

WiFi szolgáltatás az SZTE Egyetemi Számítóközpontban I.

Borús András, Csóti Zoltán, Szabó Zsolt
Jónás Balázs

{borus, csotiz, szabozst}@cc.u-szeged.hu
bjonas@scinetwork.hu

Tartalomjegyzék

- Bevezetés
- Előzmények
- Beszerzés
- A rendszer építőelemei
- Hálózat
- Szolgáltatások
- SCIBILL Guest manager

Bevezetés

Bevezetés

- TIOP-1.3.1.-07/2/2F-2009-0004 uniós projekt
- „A Dél-alföldi Tudáspólus felsőoktatási infrastruktúrájának fejlesztése”
- Matematikai, műszaki, természettudományos és informatikai képzés számára infrastrukturális fejlesztések
- 2009. január 16. és 2012. november 30. között
- Szegedi Tudományegyetem és partnerintézményei

Bevezetés

- A pályázat „B” komponense: az oktatási-kutatási infrastruktúrát támogató, infokommunikációs technológiai fejlesztések
- A projekt részelemei:
 - informatikai központ fejlesztése
 - egyetemi gerinchálózat fejlesztése
 - egyetemi épületek aktív eszközeinek és kábelezési rendszereinek korszerűsítése
 - **egyetemi vezeték nélküli hálózat fejlesztése**
 - hálózatmenedzsment
 - szerverkonszolidáció
 - portál- és üzleti intelligencia-rendszerek fejlesztése

Célkitűzés:

ETR-azonosító WiFi minden egyetemi hallgatónak és dolgozónak

(ETR = Egységes Tanulmányi Rendszer)

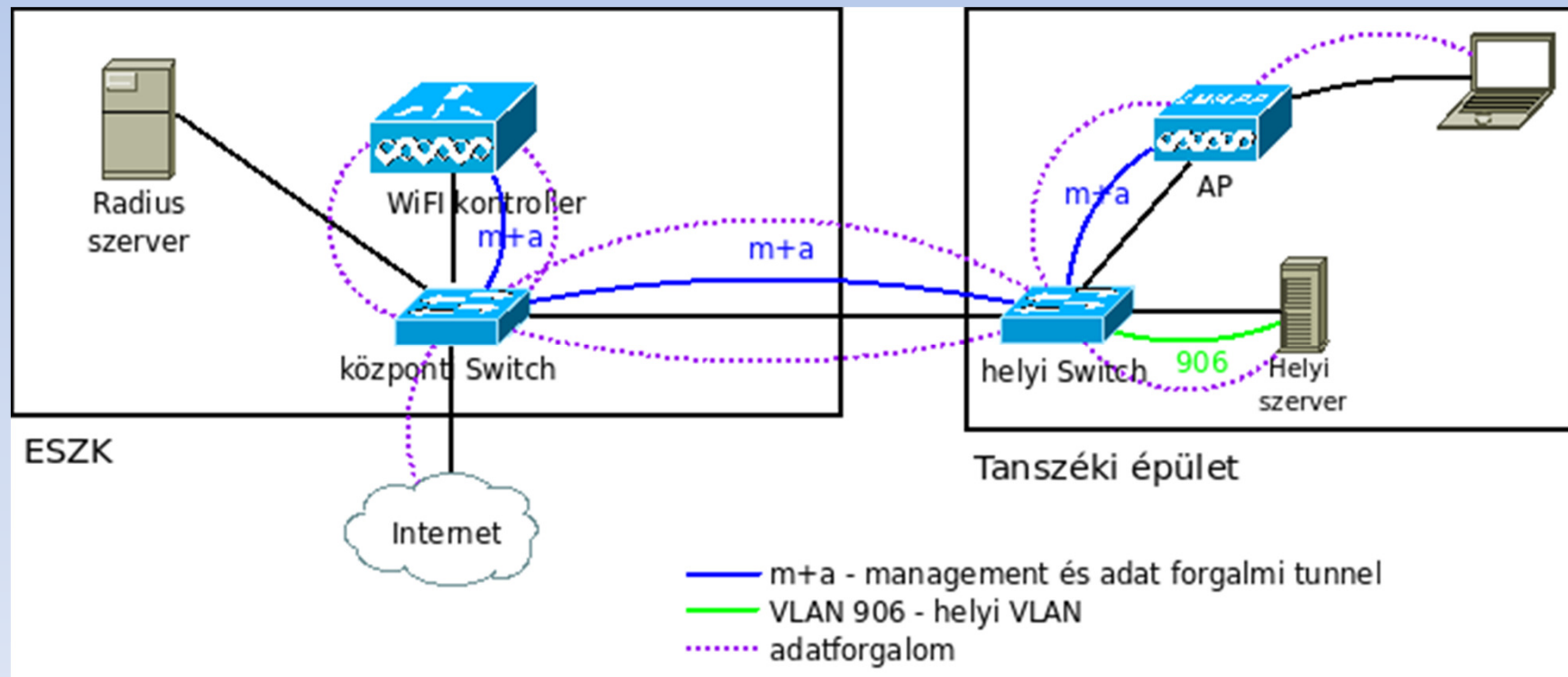
Főbb műszaki jellemzők és alapelemek:

- WPA/WPA2 Enterprise + TKIP/AES
- PEAP, MS-CHAPv2
- NPS – autentikáció (ETR AD)
- FreeRADIUS – autorizáció
- Központilag vezérelt AP-k
- Local switching (Hybrid H-REAP)

Előzmények

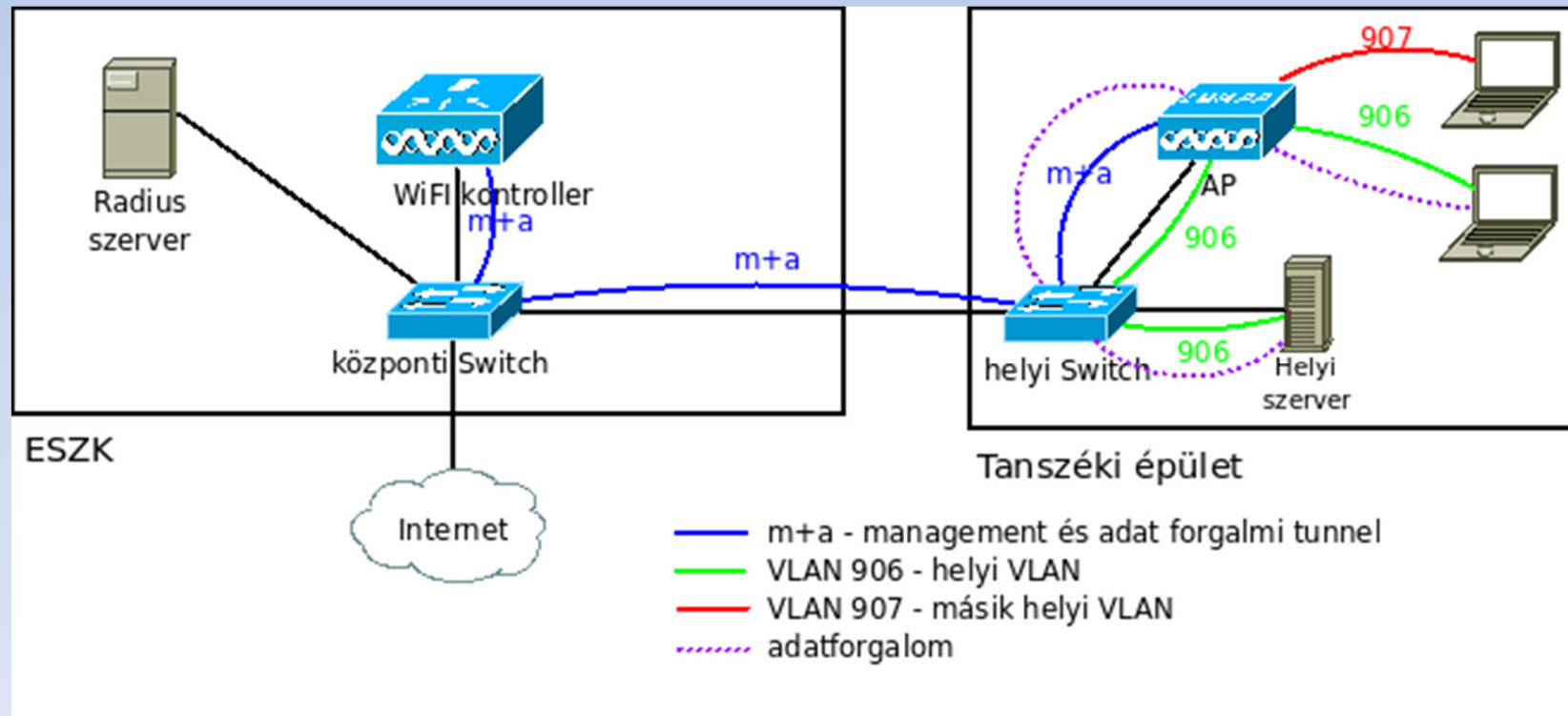
Alaprendszer

- Központi-helyi switch között L3 kapcsolat
- Minden forgalom átmegy a kontrolleren



Local switching

- Cél: Lokális erőforrások elérése WiFi-vel
- Felhasználó – „saját” épület és VLAN
- Speciális SSID megadása esetén dinamikus VLAN hozzárendelés felhasználó név és AP csoport alapján



Beszerezés

Beszerzés

A beszerzés formája: KEF-es

Megrendelés: 2012. március, szállítás: 2012. május

Szállító: SCI-Network Távközlési és Hálózatintegrációs zRt.

Típus	Beszerzett eszközök megnevezése	Mennyiség (db)
switch	HP E5406 zl Switch with Premium Software	2
kontroller	HP ProCurve MSM765zl Mobility Controller	4
kontroller	HP ProCurve E-MSM760/765 40 AP License	4
AP	HP MSM430 Dual Radio 802.11n AP (WW)	113
AP	HP MSM460 Dual Radio 802.11n AP (WW)	5
AP	HP MSM466 Dual Radio 802.11n AP (WW)	14
AP	HP In/Out Sector 8/10dBi MIMO 3 Elmt Antenna	26
Menedzser szoftver	HP PCM+ v4 S/W Platform with 50-dev Lic	1
Menedzser szoftver	HP PCM+ Mobility Manager v4 S/W Mod Lic	1
Menedzser szoftver	HP PCM+ v4 with 100-dev License	3

Garancia:

- Hardver eszközökre „life time” Next Business Day cseregarancia
- Szoftverekre 5 év 24x7 támogatás

Beszerezés

Korábbi beszerzések:

A TIOP-1.3.1.-07/2/2F-2009-0004 „A” fejezetében lévő épület felújítások során beszerzett AP-k:

Beszerezés éve	Beszert eszközök megnevezése	Mennyiség (db)
2010	HP MSM422 802.11n AP (WW)	50
2011	HP MSM430 Dual Radio 802.11n AP (WW)	47

A TIOP pályázat komponenseiből összesen 229 db AP-t vásároltunk.

Ha minden AP-t kitelepítünk, akkor több mint 10 épületben lesz elérhető a központi szolgáltatás.

Egyéb beszerzések:

Kültéri körsugárzó antenna: TerraWave Solutions 802.11n 2.4/5 GHz 6 dBi.

Jogi kar: 13 MSM 460-as AP.

AP-k vagyonvédelméhez lakat.

A rendszer építőelemei

A rendszer építőelemei

HP ProCurve 5406 zl switch:

Feladata a kontrollerek befogadása, bekötése az egyetem hálózatába

- Hálózati interfész: 2 db, illetve 1 db 8x10Gb Ethernet kártya
- Tápellátás: 2x (redundáns) tápegység modul
- Distributed-LACP port trunk-vel összekapcsolt

ProCurve MSM765zl Mobility Controller:

- HP 5406 zl switchbe telepített modul
- Hálózati interfész: backplane-re csatlakozó 2x10 Gbps Ethernet
- Egy controller által egyidejűleg kezelhető kliensek száma 2000
- 4 controllerre összesen 320 AP licenc
- A kontrollerek teaming módba kötöttek
- A teamen belül a licencek szabadon mozgathatók
- A teamben a kontrollerek szoftver frissítése automatikus
- Felügyelt AP-k frekvenciamenedzselése automatikus
- Felügyelt AP-k sugárzási teljesítménye maximum

A rendszer építőelemei

Az épületekbe kihelyezett AP-k

Elhelyezés:

- Minden AP-t épületeken belül
- Legalább 2,5 m magasra
- Lehetőleg 100%-os „data only” lefedettség
- A kültéri lefedés beltéri AP-khoz csatlakoztatott kültéri antennákkal

Típusok:

- HP MSM422 802.11n AP (WW) (300 Mbit/s)
- HP MSM430 Dual Radio 802.11n AP (WW) (300Mbit/s)
- HP MSM460 Dual Radio 802.11n AP (WW) (450Mbit/s)
- HP MSM466 Dual Radio 802.11n AP (WW) (450Mbit/s, külső antenna)

Főbb tulajdonságok:

- Hálózati interfész: 1x 802.3af PoE, 802.1q képes port
- Központilag menedzselt
- Egyidejűleg használható VLAN-ok száma 80
- Egyidejűleg használható SSID száma 16

A rendszer építőelemei

Menedzsment szoftver:

Főbb funkciók:

- A nem regisztrált (idegen) AP-k felderítése
- A forgalom monitorozása mennyiségi vonatkozásban
- A WiFi hálózat egészének, illetve az egyes eszközöknek felügyelete
- Jelentések, statisztikák készítése a kezelők számára

Beszerzett szoftver:

- HP PCM+ v4 Network Management + Mobility Manager v4 350 node licence
- HP IMC WSM modullal. 200 node licence + 350 AP licence

Operációs rendszer:

- PCM+, MM: Windows Server 2008 64bit R2 Enterprise
- IMC, WSM : Centos

Hardver:

- Blade környezetbe telepített virtuális szerver

A PCM+ „End of sale” lett az idén. Jövőre „End of support” státuszba kerül, ezért kellett váltani.

A rendszer építőelemei

Kiegészítő komponensek:

AAA szerverek:

- 2 darab, redundánsan üzemeltetett FreeRADIUS szerver
- redundáns MySQL szerver a RADIUS szolgáltatások adatbázis back endjének
- autentikációt Microsoft NPS szerver végzi az ETR AD alapján

DHCP szerverek:

- AAA szerverekre telepített egy-egy ISC DHCP kiszolgáló

Információs webszerverek (intra- és extranetes):

- tájékoztatás
- felhasználó menedzsment

(Szerver tanúsítványok: NPS és extranetes információs szerver)

SCIBILL guest manager szoftver:

- SCI-Network zRt. által fejlesztett szoftver

Hálózat

Hálózat

Az SZTENET felépítése

Ethernet hálózat

Layer3 protokoll: IPv4

Mag: Layer3-as switchek (2) rendszere

központi szolgáltatások eszközei

Blade rendszer

ETR szerverek (NPS, AD)

WiFi szerverek (RADIUS, DHCP, adminisztrációs web stb.)

WiFi szolgáltatás switch-kontroller rendszere

Az egyetemi gerinchálózat:

Épületek, alhálózatok: Layer3 „szigetek” (IP subnetek, VLAN-ok)

Switchek, tűzfalak: Layer3 demarkációs eszközök – route-olnak

A gerinchálózat felett kifeszített VLAN: NINCS

Hálózat

Célkitűzés:

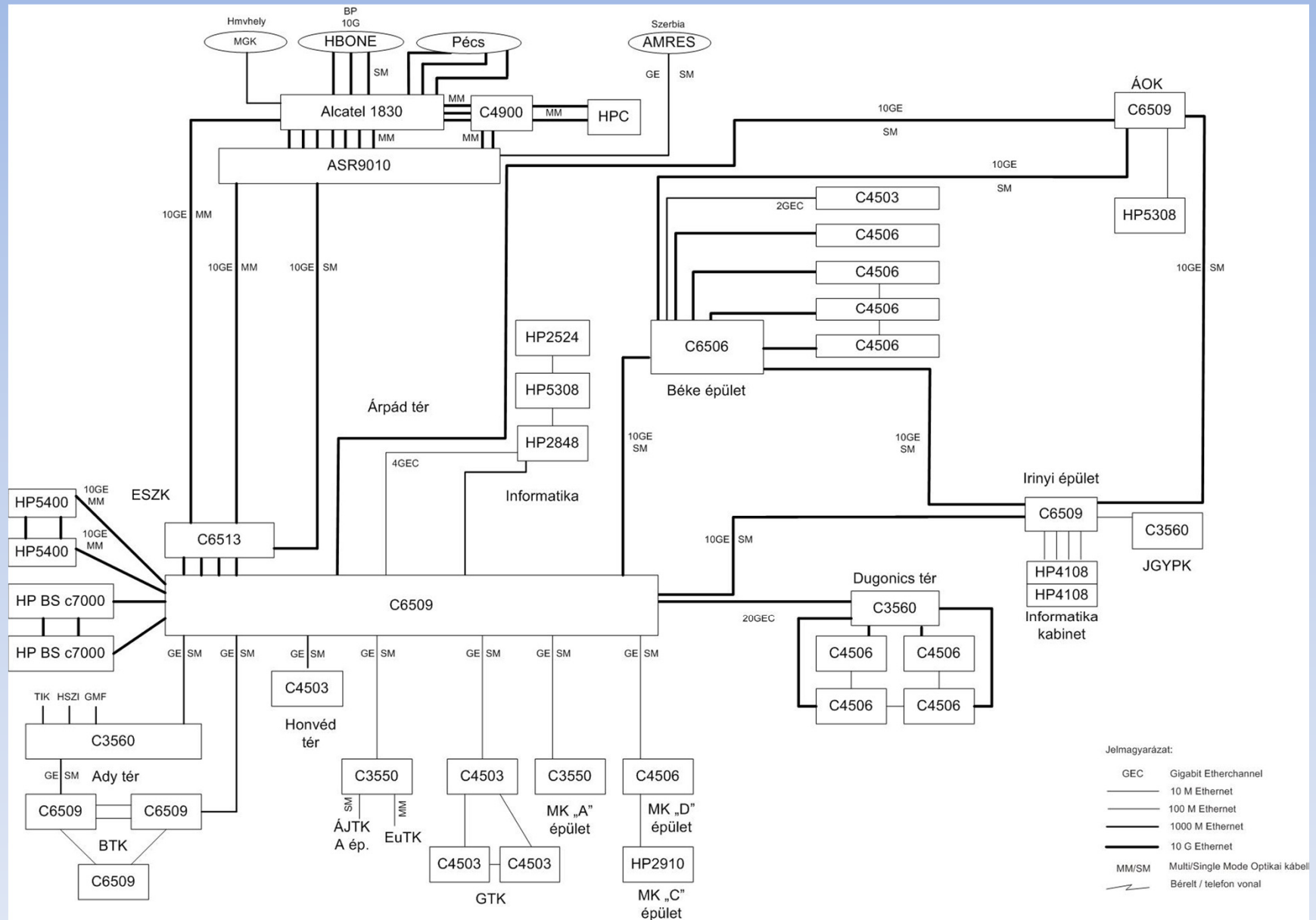
A WiFi rendszer az SZTENET – fizikai és logikai – hálózati struktúrájának módosítása nélkül telepítendő.

Lehetséges megoldás:

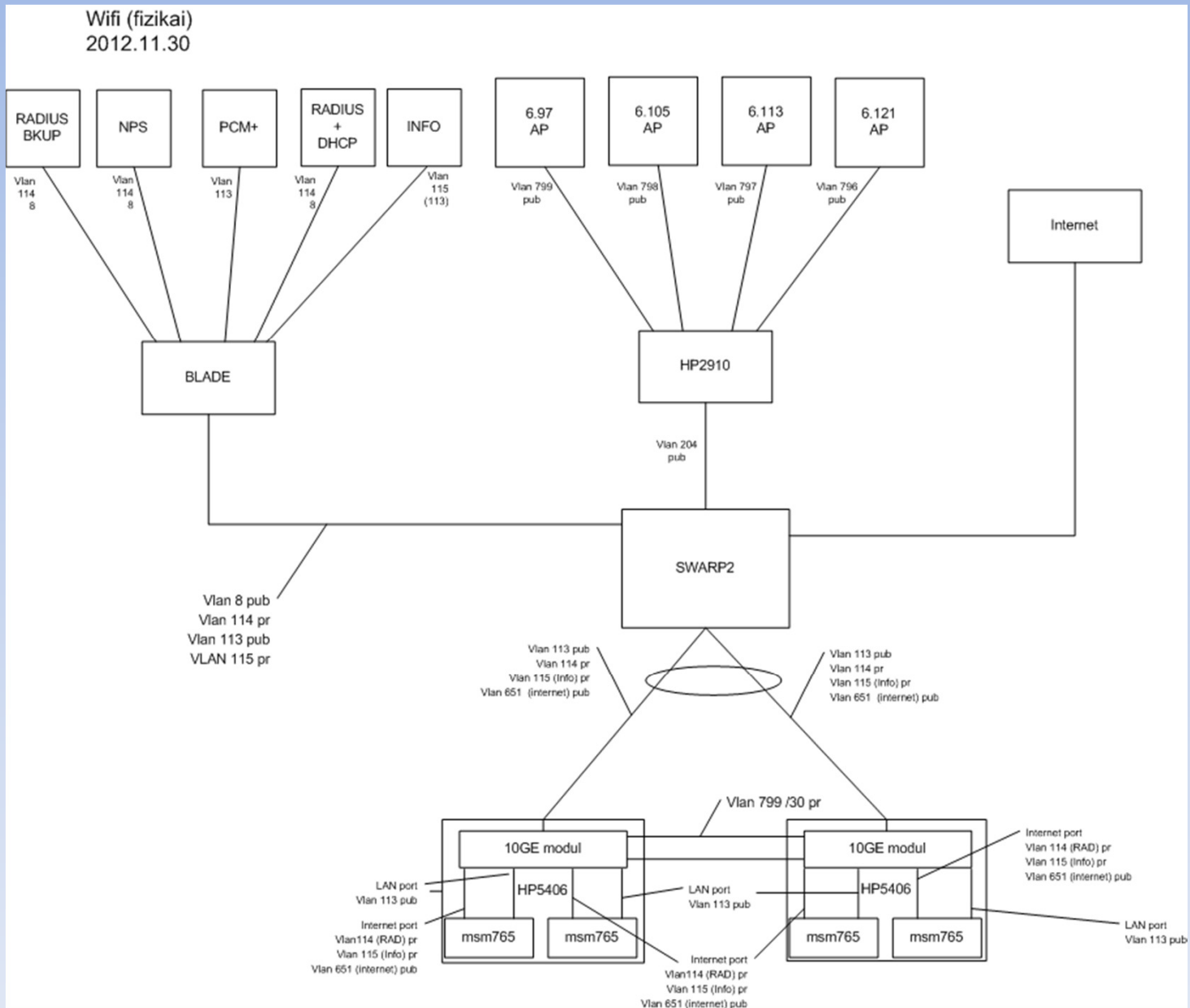
A központi controller és az épületekben elhelyezett AP-k között az egyetemi gerinchálózaton IP feletti tunnel:

Vezérlés, menedzsment és adat.

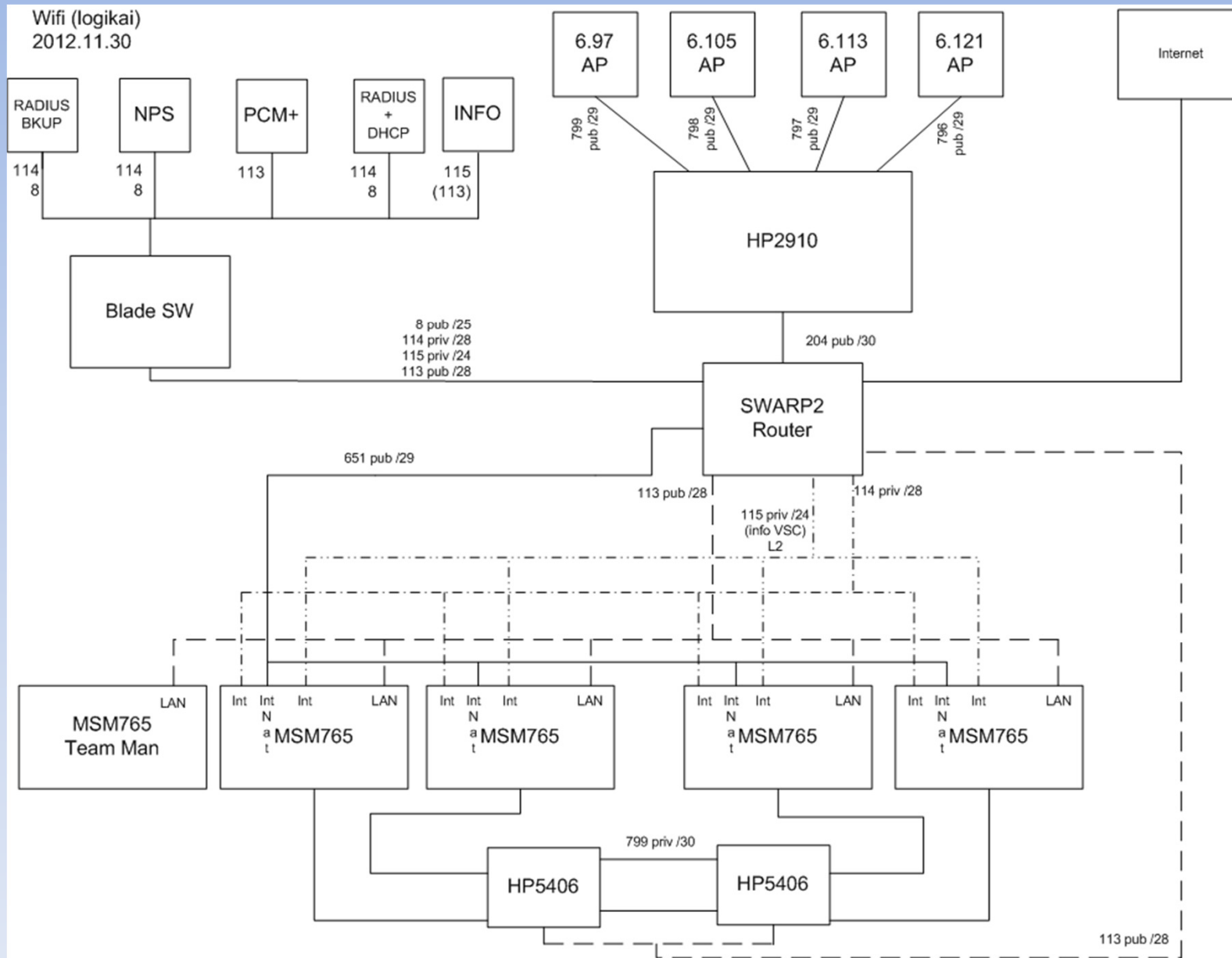
Hálózat



Hálózat



Hálózat



Hálózat

Menedzsment hálózat

Kontroller LAN port

- AP kezdeti felismerés, konfigurációs beállítások frissítése, IP tunnel
- Menedzsment: web, telnet, PCM+

Produkciós hálózat

Kontroller INTERNET port

- RADIUS és DHCP
- Információ
- NAT-olt forgalom

Hálózat

Kontroller-rendszer

teaming üzemmód

Közös menedzsment cím

NAT: külön publikus IP cím, közös privát IP tartomány

Kontroller preferencia az AP-kben

DHCP beállítások

per VSC (szolgáltatás, SSID)

NAT beállítások

per VSC (szolgáltatás, SSID)

VSC (Virtual Service Community)

- SSID
- Broadcast SSID
- Access Control (ACL és traffic shaping)
- Titkosítás: WPA/WPA2
- VSC név
- Autentikációs protokoll: 802.1x vagy HTML (captive portal)
- Kontroller user nw if (NAT privát IP tartomány)
- Egress VLAN

Szolgáltatások

Szolgáltatások

Központi szolgáltatások

- A forgalom átmegy a kontrolleren
- NAT-olt címek
- A forgalomirányító a kontroller
- Szórt SSID-k:
 - szte-wifi
 - eduroam-szte
 - szte-informacio

Local switching (LSW)

- Helyi erőforrások elérését biztosító szolgáltatás
- IP címek a helyi szokásoknak megfelelően
- A helyi tűzfal mögötti hálózat is elérhető
- A kapcsoló az AP
- Szórt SSID: szte-lan

Szolgáltatások

A felhasználók azonosítása

Felhasználónév/jelszóval

Felhasználónév:

ETR-login@wifi.u-szeged.hu

Jelszó:

Megegyezik az ETR felület belépési jelszavával

Az ETR-login az ETR elérési joggal rendelkező felhasználók nagy részénél megegyezik az EHA-kóddal.

(Nem-ETR-es kivételek: Külön DB-tábla és AD-részfa.)

Minimális szoftver követelmény :

- Bármilyen operációs rendszer WiFi támogatással
- A kliens operációs rendszer részét képező vagy külön telepített supplicant

Minimális hardver követelmény :

Egy olyan hálózati kártya, amely támogatja a következőket:

- 802.11 a/b/g/n WiFi szabványok közül legalább egyet
- WiFi titkosítás: WPA/WPA2 Enterprise TKIP/AES

Beállítási segédletek: Windows XP, Windows 7, Android 2.3.

Guest manager

Guest manager

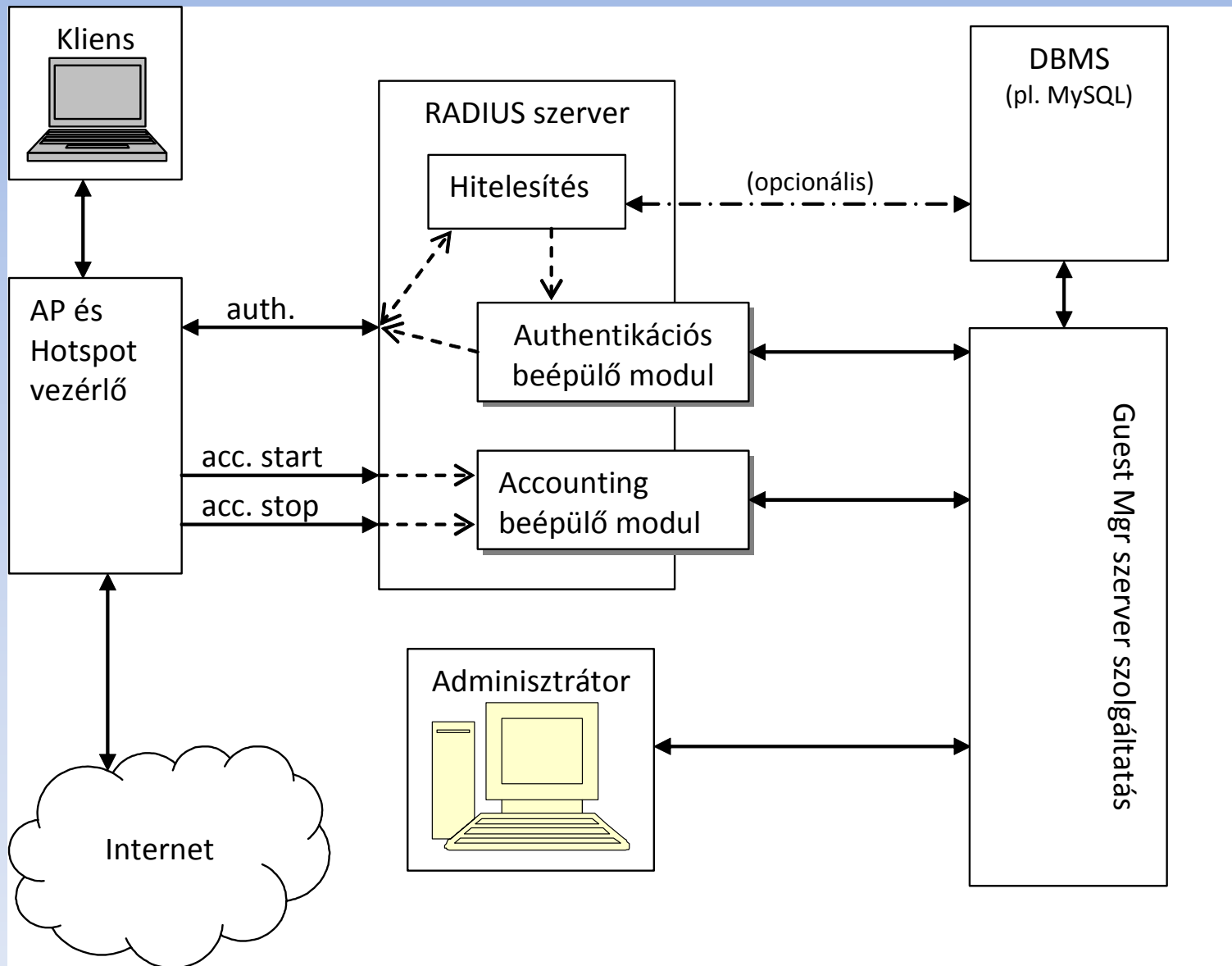
Szükségessége

- „Instant” WiFi.
- Vendégek, konferencia résztvevők számára biztonságos WiFi elérés
- A felhasználók számára egyedi azonosító/jelszó generálása – voucher

SCI-Network zRt. által fejlesztett szoftver

- FreeRADIUS alapokon
- MySQL adatbázis felhasználásával
- RADIUS szerverbe beépülő modul
- Adminisztrációs felület
- Nem csak HP-ra

Guest manager



Guest manager

RADIUS beépülő modulok

Az adatbázisban rögzítik a felhasználók tevékenységeit, ezáltal tudja a rendszer követni, hogy mennyit használhatja egy felhasználó a WiFi szolgáltatást.

Adminisztrátori felület

- Delegálható voucher kiadási jog
- Többszintű jogosultsági rendszer
 - Operator 1: Egyesével képes voucherek kiállítására
 - Operator 2: csv fájlokból felolvasott adatok segítségével egyszerre több voucher kiállítására is van lehetősége
 - Administrator
- Kétféle voucher kiadására van lehetőség:
 - „DateCard”: Egy adott időszakra érvényes (Pl. 2013. nov. 5-6.)
 - „TimeCard”: Egy adott időtartamra érvényes, az aktiválástól számítva három hónapon belül kell felhasználni (Pl. összesen 10 óra.)

**Köszönöm
a figyelmüket!**