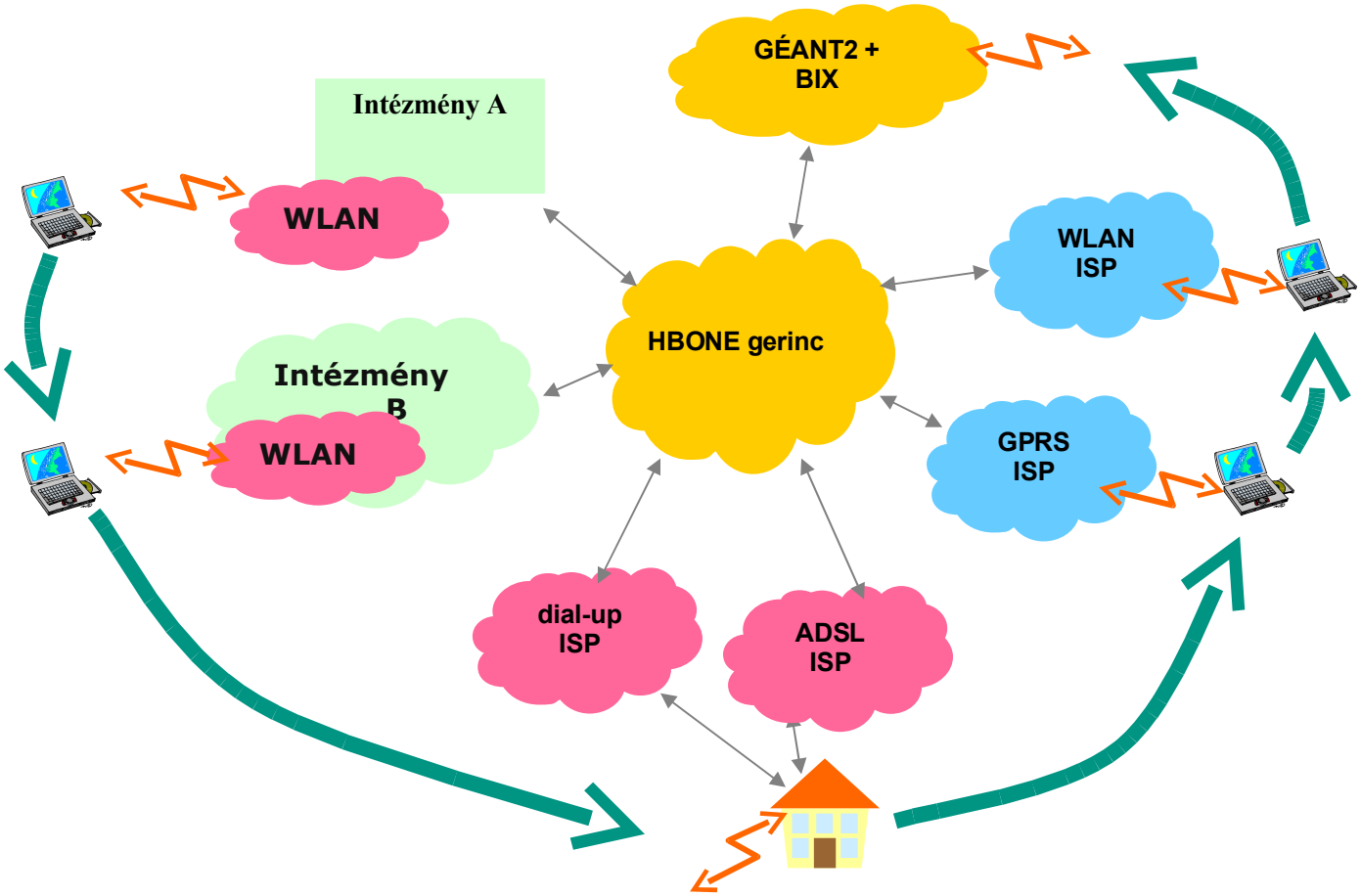
Tutamen et Simplicitas: Eduroam

Mohácsi János

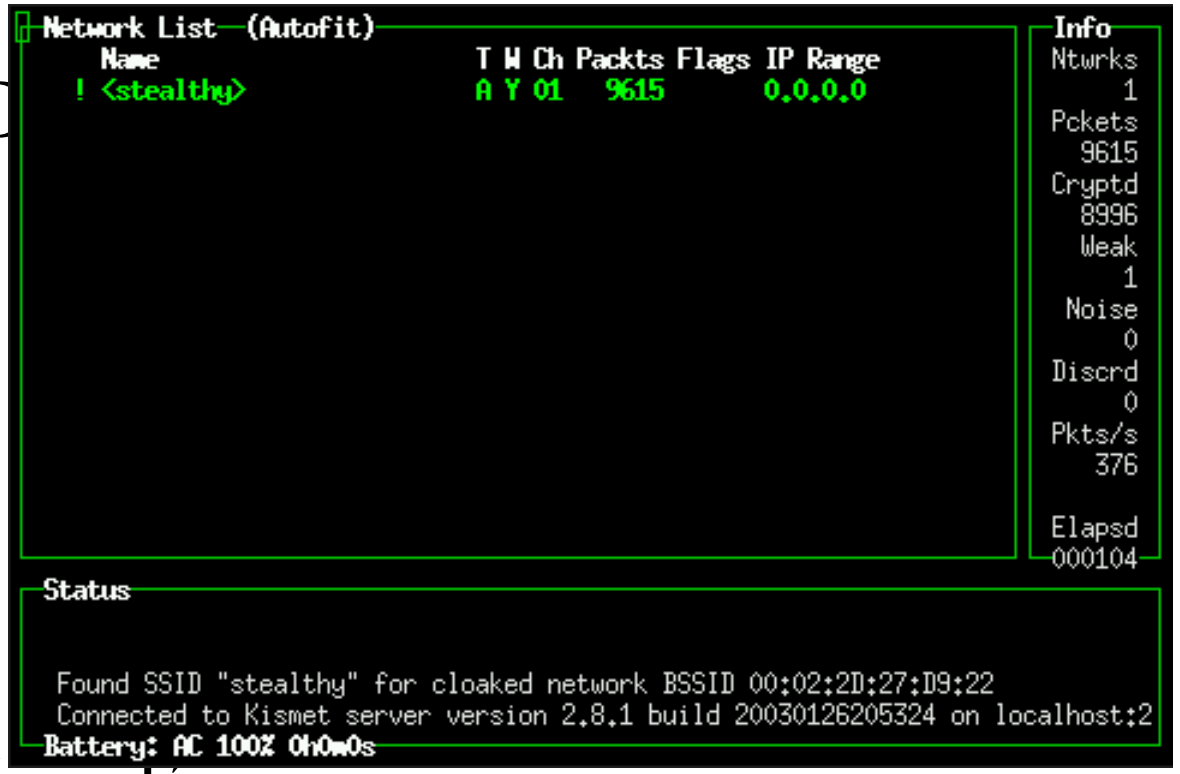
NIIF Intézet

Miért szeretjük a wireless hozzáférést?



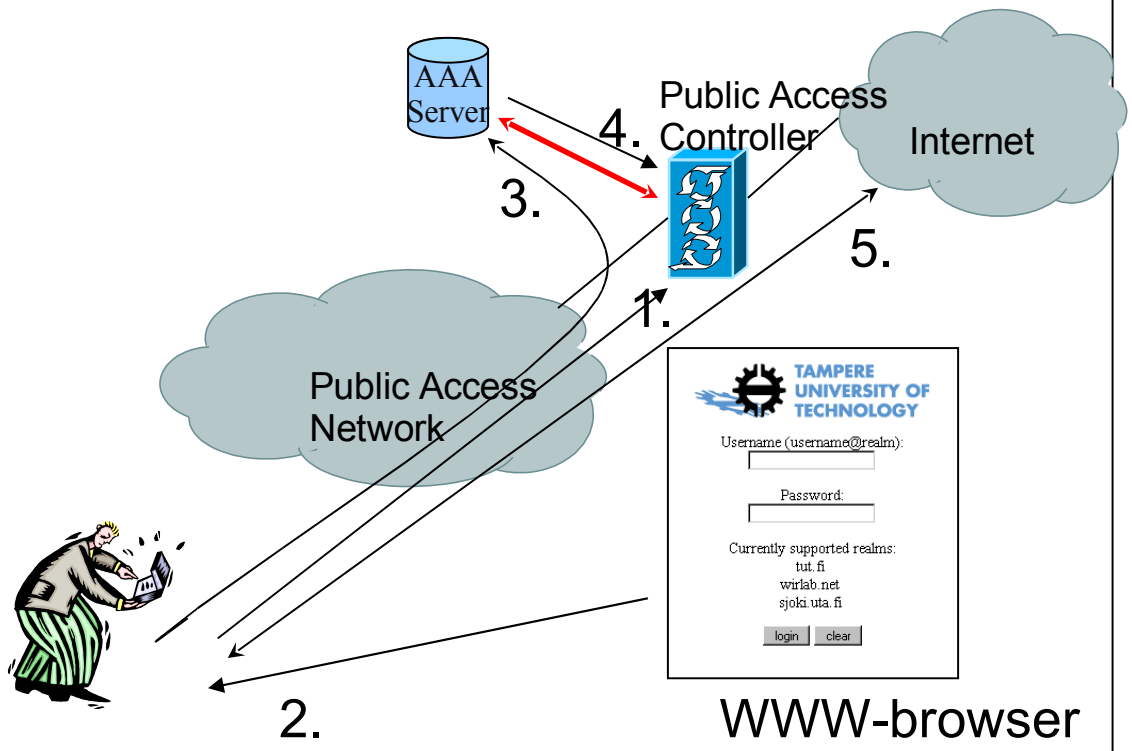
Wifi veszélyei

- Mac cím és SSID
  - TCPdump
  - Ethereal
- WEP cracking
  - Kismet
  - Airsnort
- Közbeékelődő támadás



Követelmények egy modern wireless hozzáféréssel szemben

- A felhasználók egyértelmű azonosítása a hálózat szélén
  - Nem lehet a wireless kapcsolatot “ellopni”
- Lehetőség látogatók fogadására
- Biztonságos



Követelmények egy modern wireless hozzáféréssel szemben

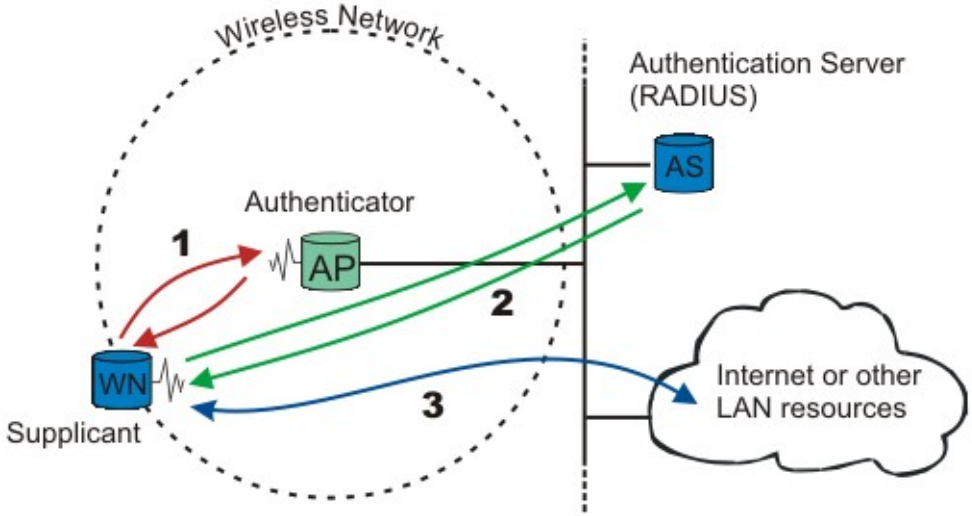
- A felhasználók egyértelmű azonosítása a hálózat szélén
  - Nem lehet a wireless kapcsolatot “ellopni”
- Lehetőség látogatók fogadására
- Biztonságos
- Skálázható
  - Anya intézményi felhasználói administráció és authentikáció – nincs központi adatkezelő!!!
  - Jó, ha tudjuk használni a már létező Radius infrastruktúrát
- Könnyen használható
- Nyitott
  - Minden operációs rendszerben támogatott
  - Szállító független
- IPv6 támogatás
- Eduroam kompatibilis

IEEE 802.1x

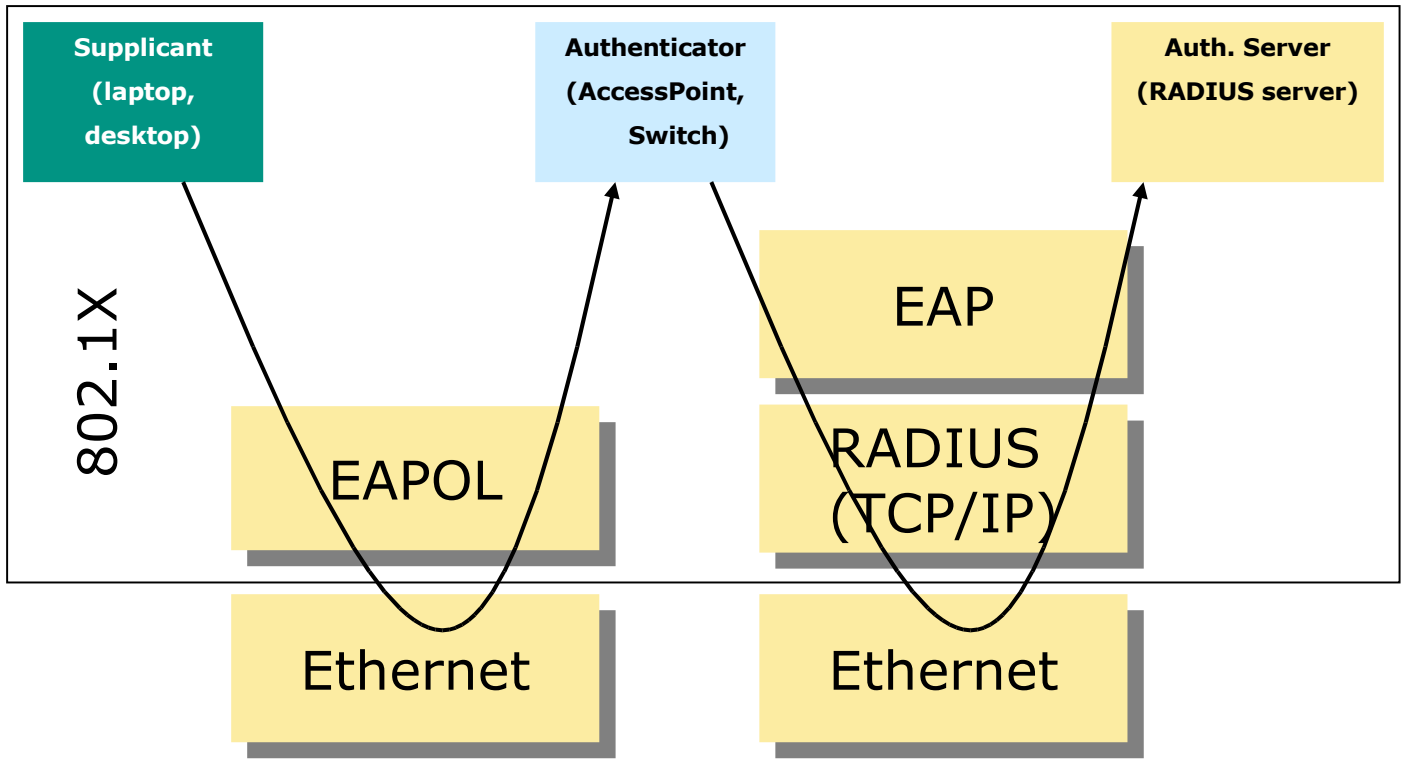
- Igazi port alapú Layer 2 azonosítás a kliens és a AP/switch között
- Többféle authentikáció lehetséges (EAP-MD5, MS-CHAPv2, EAP-SIM, EAP-TLS, EAP-TTLS, PEAP)
- Szabványos
- Titkosítja a kommunikációt dinamikus kulcsokkal
- RADIUS támogatás
  - Skálázható
- Dinamikus VLAN hozzárendelés támogatott
- Kliens szoftver szükséges (OS vagy 3rd -party)
- Vezeték nélküli és vezetékes hálózat is támogatott

802.1x és Wireless

- WPA és 802.11i ún. Enterprise módja implementálja a 802.1x-et



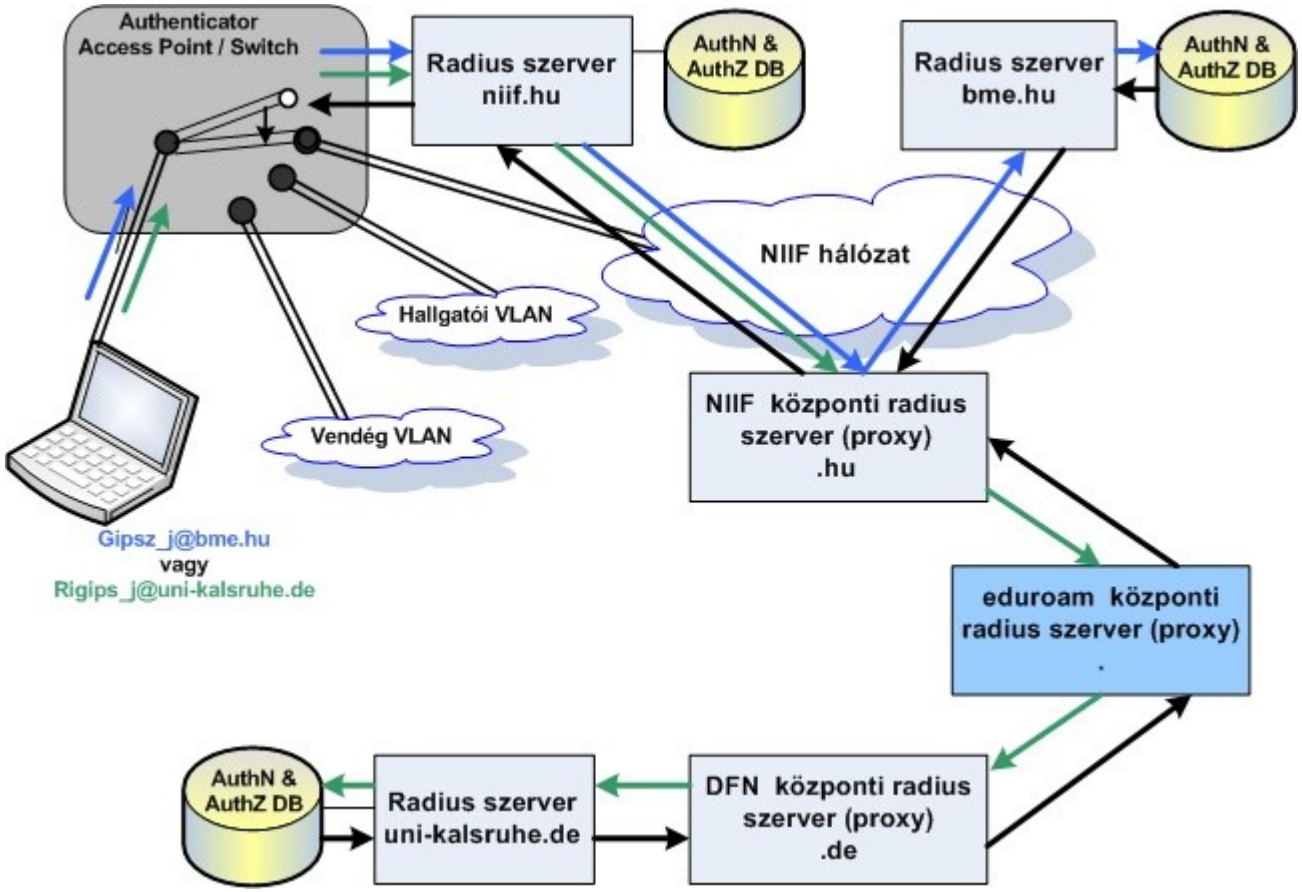
Wireless biztonság



EAP típusok

Tulajdonság	EAP MD5	LEAP,EAP-FAST	EAP TLS	PEAP	EAP TTLS
Biztonsági megoldás	Szabványos	Vendor specifikus	Szabványos	Szabványos	Szabványos
Tanúsítvány – Kliens	Nem	Nem/majdnem	Igen	Nem	Nem
Tanúsítvány – Szerver	Nem	Nem/majdnem	Igen	Igen	Igen
Azonosítás biztonsága	Semmilyen	Gyenge/Erős	Erős	Erős	Erős
Támogatott autentikációs adatbázis	Nyílt szövegű adatbázis	Active Directory, NT Domains	Active Directory, LDAP stb.	Active Directory, NT Domain, Token Systems, SQL, LDAP stb.	Active Directory, LDAP, SQL, Egyszerű jelszó fájl, Token Systems stb.
Dinamikus Kulcs Csere	Nem	Igen	Igen	Igen	Igen
Kölcsönös azonosítás	Nem	Igen	Igen	Igen	Igen

Roaming?


Authenticator
Access Point / Switch
Radius szerver
niif.hu
AuthN &
AuthZ DB
Radius szerver
bme.hu
AuthN &
AuthZ DB
NIIF hálózat
Hallgatói VLAN
Vendég VLAN
NIIF központi radius
szerver (proxy)
.hu
Gipsz_j@bme.hu
vagy
Rigips_j@uni-kalsruhe.de
eduroam központi
radius szerver (proxy)
.
AuthN &
AuthZ DB
Radius szerver
uni-kalsruhe.de
DFN központi radius
szerver (proxy)
.de

Eduroam

- Föderációs infrastruktúra a hallgató, oktatói és kutatói mobilitás támogatására
- 2004-ben jött létre – Terena TF-mobility
- 2005-től GN2 JRA5 fejlesztések
  - Monitorozás
  - Európai szolgáltatás

Eduroam - résztvevők

Eduroam résztvevők - Magyarország

- NIIF Intézet
- BME
- Debreceni Egyetem
- HIK
- Széchenyi István Egyetem
- KFKI - hamarosan
- Szegedi Tudomány Egyetem – hamarosan
- Gödöllői Egyetem -hamarosan
- ELTE?

Eduroam Magyarországon

- Teszt üzem 2006 április
  - EugridPMA meeting 2006 május
  - TF-CSIRT meeting
  - Németországi projekt megbeszélés
- Eduroam Pilot szolgáltatás
  - Több résztvevő 2006 ősze
  - TF-CSIRT/FIRST meeting - > 90 felhasználó
- NIIF Eduroam szolgáltatás – 2007 májusától

Nemzeti Eduroam policy-k

- Kölcsönös hozzáférés
- Tagok a Radius hierarchiába bekötött intézmények
- Az anyaintézmény (marad) felelős a felhasználóikért
- Az anyaintézmény felelős a helyes felhasználói nyilvántartásért
- Anya- és meglátogatott intézmény elegendő log adattal kell, hogy rendelkezzen
- A minimális biztonsági szintet garantálni kell

Szolgáltatások - Policy

- Oktatási/Kutatási intézmény közgyűtemény
- WPA-Enterprise módú authentikáció - javasolt WPA2
- Radius szerver - amely segítségével azonosítja a felhasználókat - EAP/TTLS-t, PEAP-ot, vagy EAP-TLS-t használva.
- Az eduroam SSID-ot támogatása - ha lehetséges broadcastolva is.
- A WLAN-ból el lehet érni a hálózatot - minimum a következőket
  - HTTP és HTTPS, DNS, ICMP (minden!), passive FTP,IPSec (ESP, AH, IKE), OpenVPN, SSH, POPs, IMAPs, NTP, submission (smtp/auth)
  - IPv6 tunnel broker
- IPv6 támogatása -lehetőség szerint
- Képesnek kell lennie debugolni és támogatni a saját felhasználóit
- Egy teszt account rendelkezésre álljon a teszteléshez
- AUP-vel rendelkezik

Miről szól a cím?

- Tutamen – védelem
  - WPA/WPA2 – vezeték nélküli rész védett
  - TLS (PEAP, EAP-TTLS) – TLS tunnel a supplicant és az authentikációs szerver között

- Simplicitas – egyszerűség
  - Klienst csak egyszer kell beállítani – ha az SSID mindenhol “eduroam”

Eduroam -NG

- GEANT2 roaming szolgáltatás
  - Támogatja a jelenlegi Eduroam rendszert RADIUS, 802.1X)
- Fő fejlesztési irányok
  - Dinamikus trust képzés
  - Formálisabb federáció
  - Skálázhatóság és monitorozás
  - Attributum-alapú authorizálás
  - Integráció a EduGain-el

További információk

- http://www.eduroam.org
- http://www.eduroam.hu
- http://ipv6.niif.hu/m/IPv6_Wireless_LAN_technológia

eduroam@niif.hu