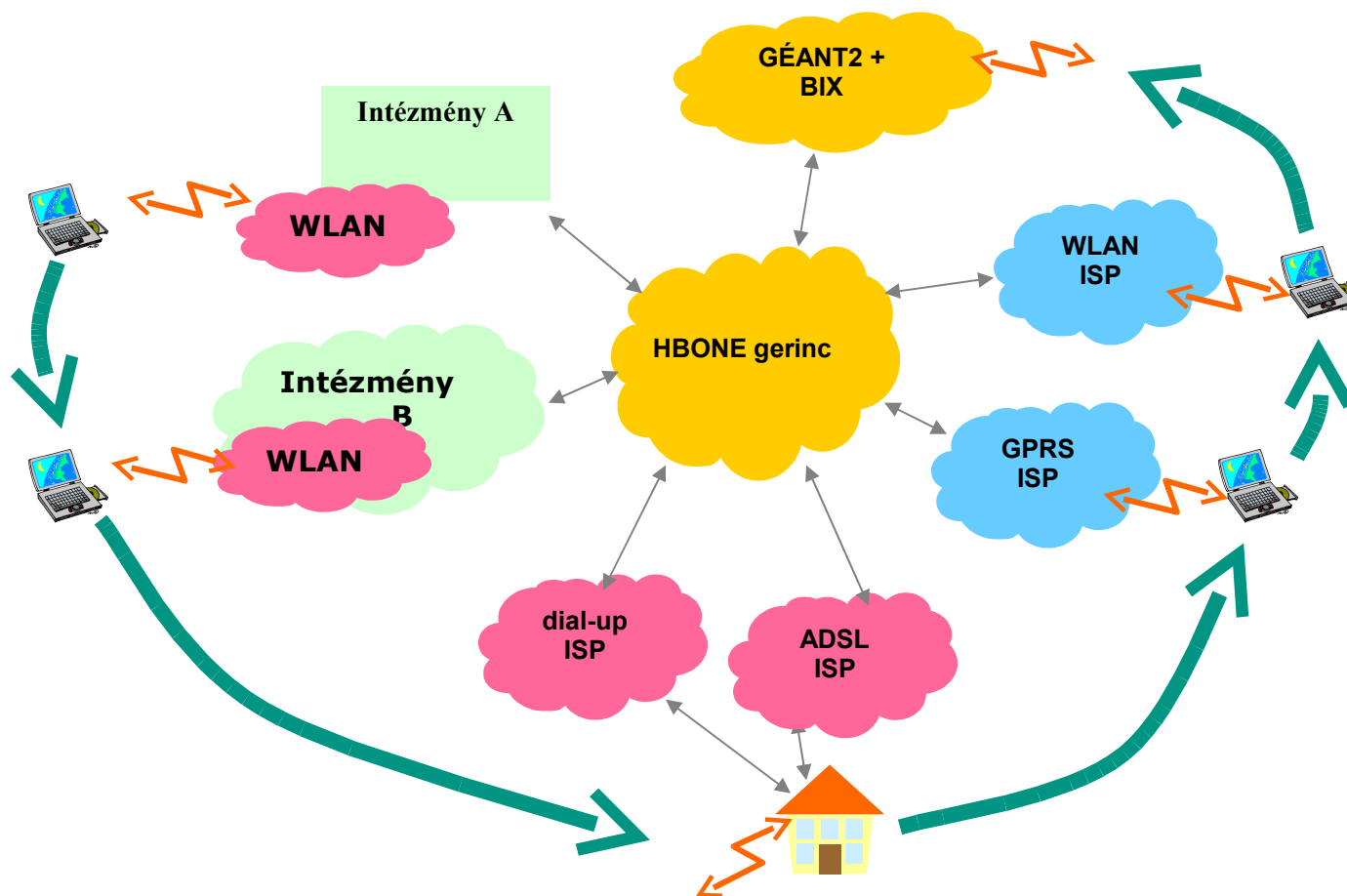




# Univerzális IPv4 és IPv6 hozzáférés biztosítása wireless technológiával

Mohácsi János  
NIIF/HUNGARNET

# Miért szeretjük a wireless hozzáférést?





# Wifi veszélyei

- Mac cym és SSID felderítés
  - TCPdump
  - Ethereal
- WEP cracking
  - Kismet
  - Aircrack-ng
- Közbeékelődő támadás



# Követelmények egy modern wireless hozzáféréssel szemben

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

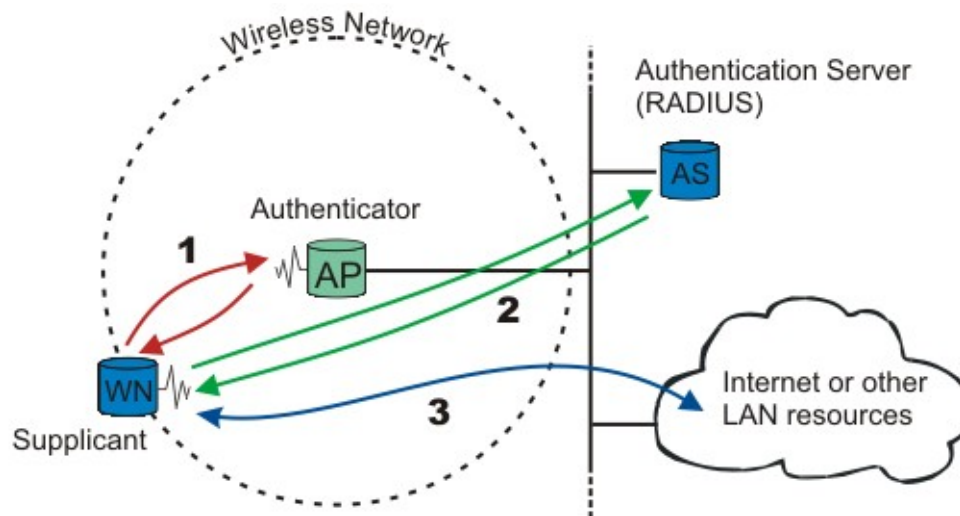


# IEEE 802.1x

- Igazi port alapú Layer 2 azonosítás a kliens és a AP/switch között
- Többféle autentikáció 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 3<sup>rd</sup> -party)
- Vezeték nélküli és vezetékes hálózat is támogatott

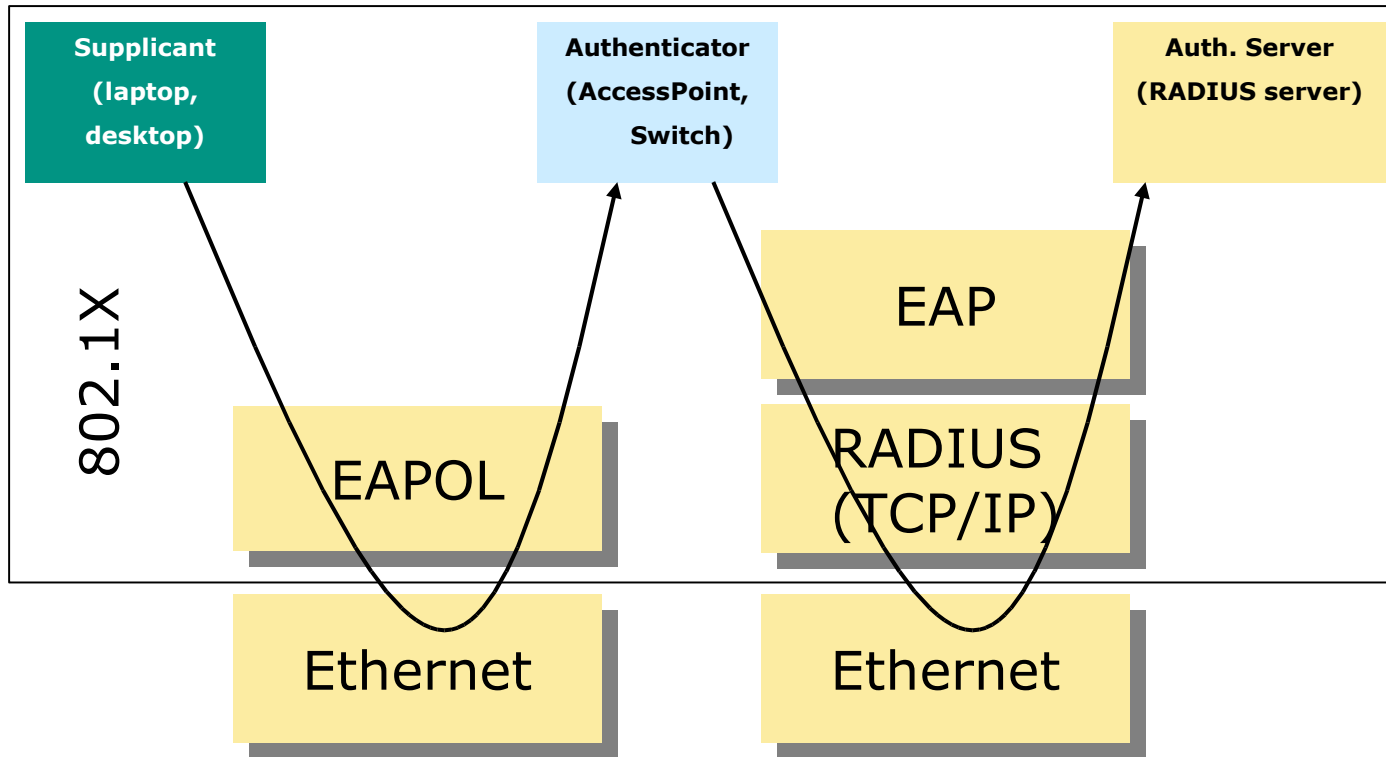
# 802.1x és Wireless

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





# Wireless biztonság



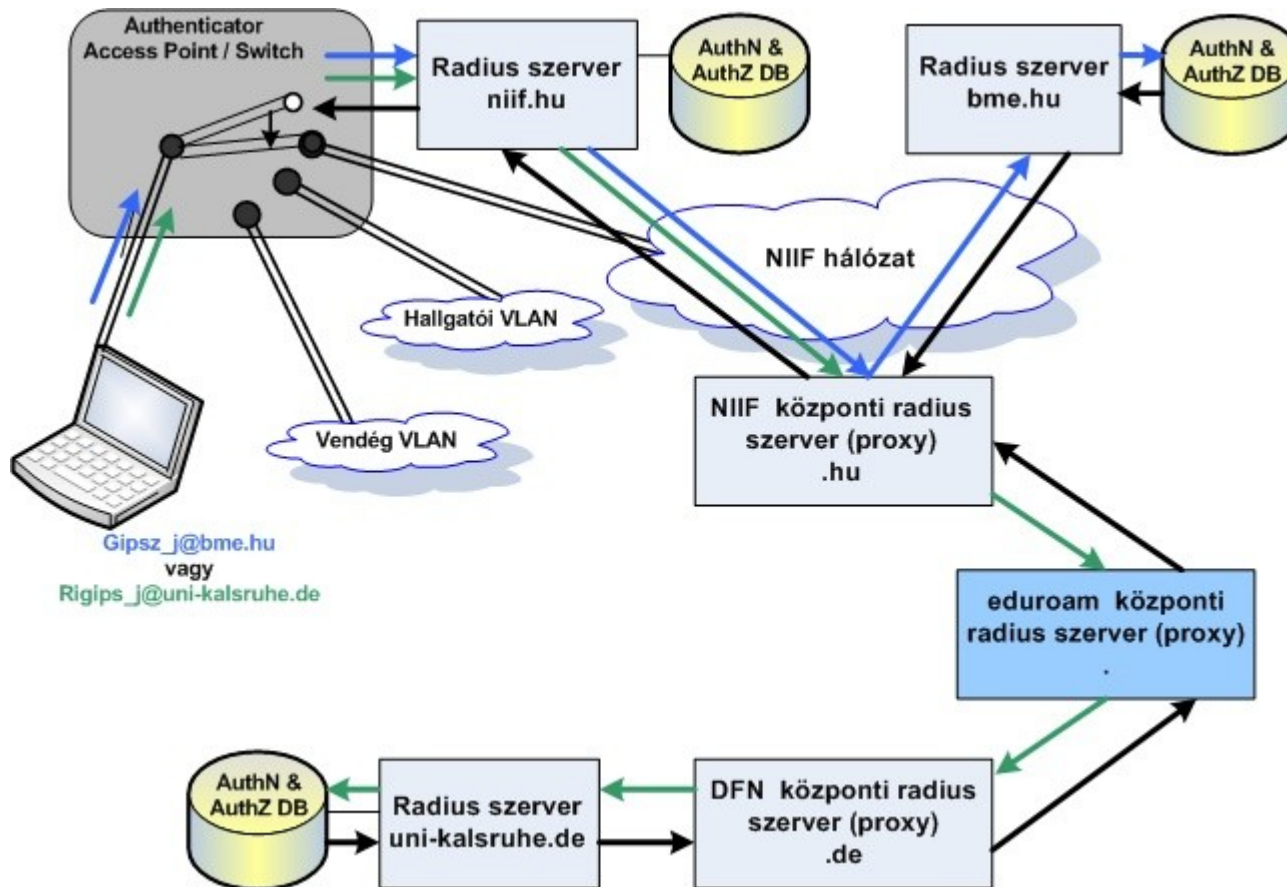


# EAP típusok

Tulajdonság	EAP MD5	LEAP	EAP TLS	PEAP	EAP TTLS
<b>Biztonsági megoldás</b>	Szabványos	Vendor specifikus	Szabványos	Szabványos	Szabványos
<b>Tanúsítvány – Kliens</b>	Nem	?	Igen	Nem	Nem
<b>Tanúsítvány – Szerver</b>	Nem	?	Igen	Igen	Igen
<b>Azonosítás biztonsága</b>	Semmilyen	Gyenge	Erős	Erős	Erős
<b>Támogatott autentikációs adatbázis</b>	Nyílt szüvegű 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.
<b>Dinamikus Kulcs Csere</b>	Nem	Igen	Igen	Igen	Igen
<b>Kölcsönös azonosítás</b>	Nem	Igen	Igen	Igen	Igen



# Roaming?



# Eduroam - résztvevők



# Eduroam résztvevők - Magyarország

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



# Szolgáltatások - Policy

- Oktatási/Kutatási intézméyn közgyűtemény
- WPA-Enterprise módú autentikáció - 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
- Képesnek kell lennie debugolni és támogatni a saját felhasználóit
- Egy teszt account rendelkezésre álljon a teszteléshez
- AUP-vel rendelkezik



# Tesztek

- EugridPMA meeting 2006 május
- TF-CSIRT meeting
- Németországi projekt megbeszélés

# Eduroam -NG

- GEANT2 roaming szolgáltatás = eduroam-NG
- Támogatja a jelenlegi Eduroam rendszert (RADIUS, 802.1X)
- Fő fejlesztési irányok
  - Dinamikus trust képzés
  - Formálisabb federáció
  - Integrált 802.11i és WPA/WPA2
  - Skálázhatóság és monitorozás
  - Attributum-alapú autorizálás
  - Integráció a EduGain-el



# További információk

- <http://www.eduroam.org>
- <http://www.eduroam.hu>
- [http://ipv6.niif.hu/m/IPv6\\_Wireless\\_LAN\\_technológia](http://ipv6.niif.hu/m/IPv6_Wireless_LAN_technológia)

[eduroam@niif.hu](mailto:eduroam@niif.hu)