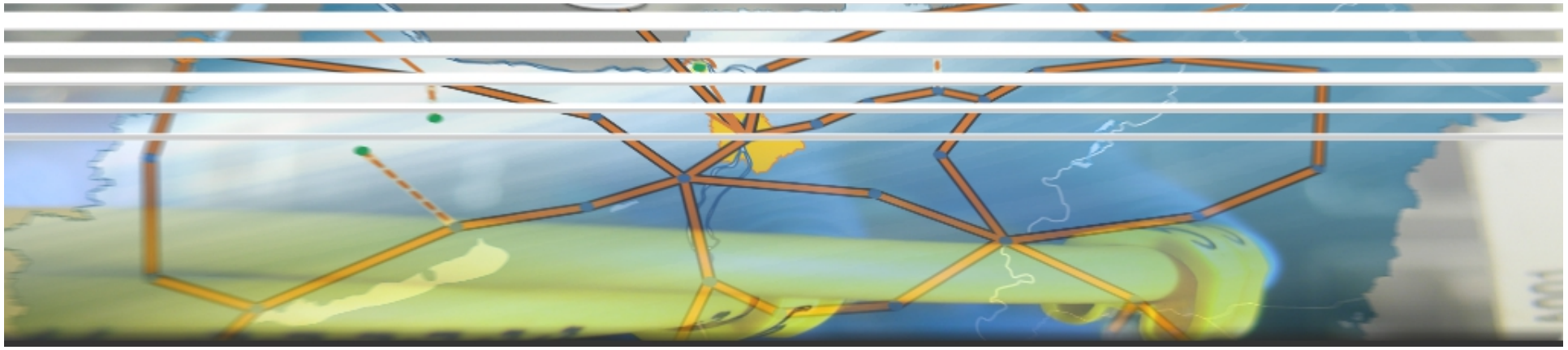
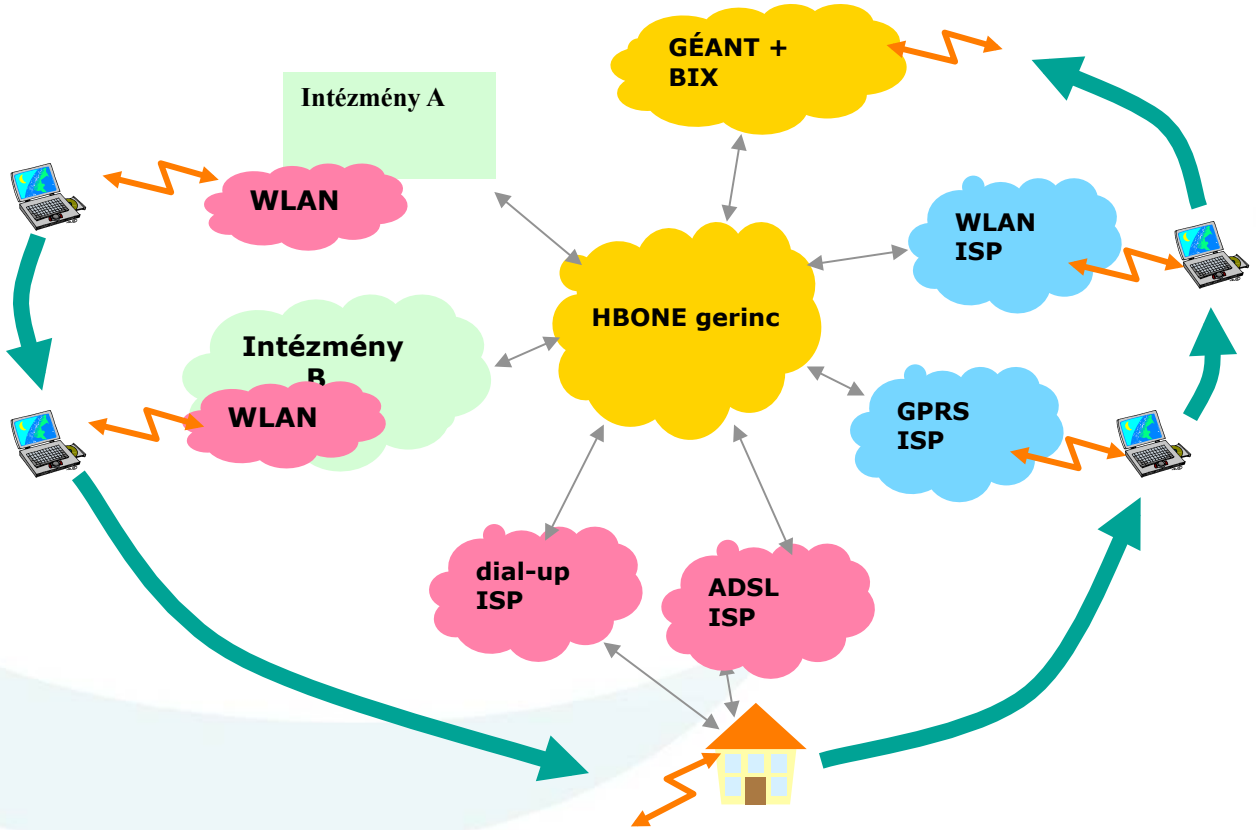
eduroam konfiguráció workshop



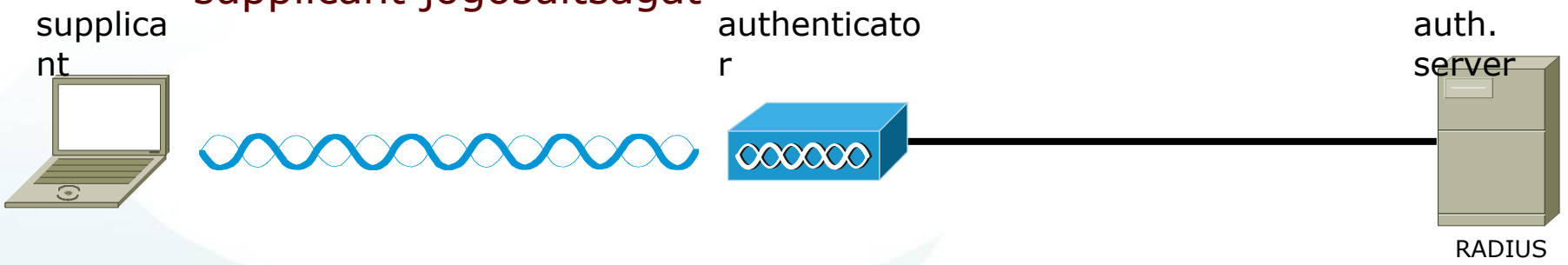
Mohácsi János
NIIF Intézet

Miért szeretjük a wireless hozzáférést?



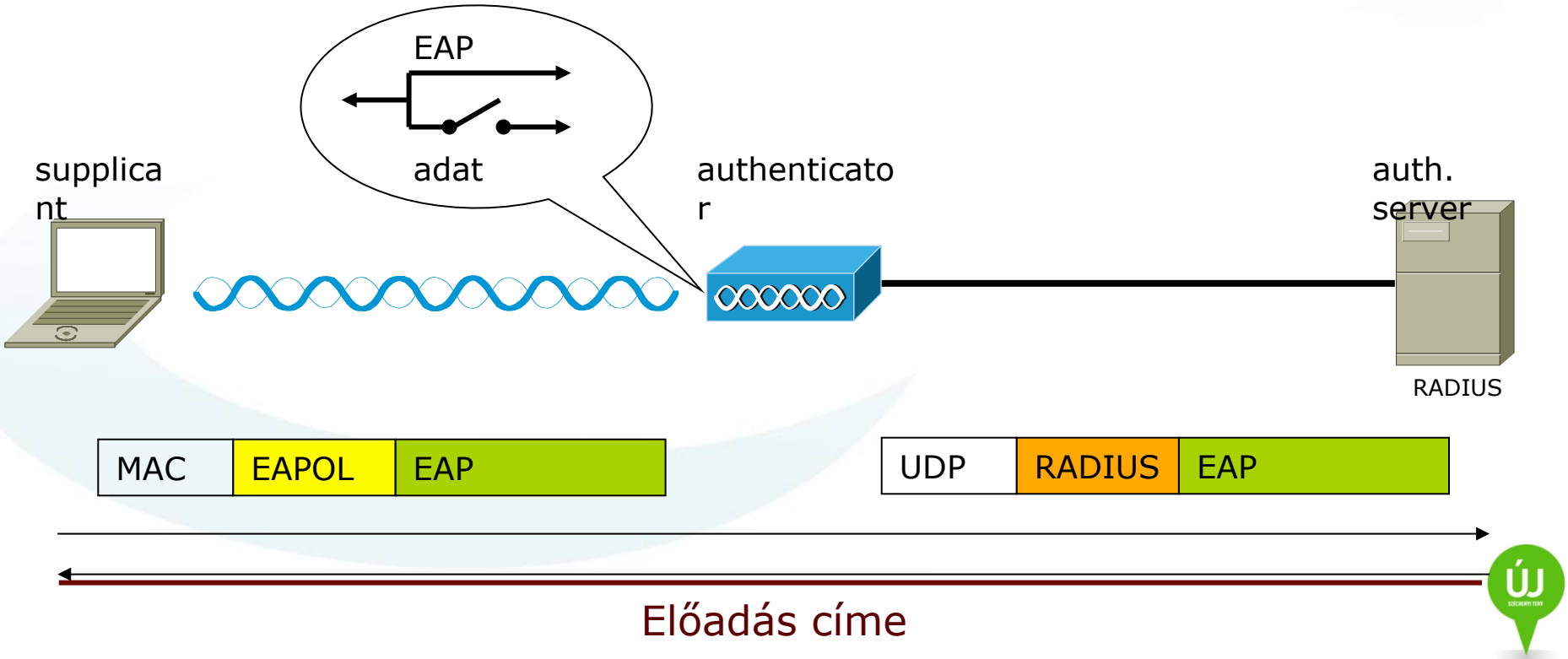
IEEE 802.1x

- EAPOL – EAP over LANs (néha EAPOW)
  - EAP csomagok átvitele 802.3 LAN-ok adatkapcsolati rétege felett
- szereplők:
  - supplicant – hozzá akar férni a hálózathoz
  - authenticator – ellenőrizni akarja a supplicant jogosultságát
  - authentication server – az authenticator számára ellenőrzi a supplicant jogosultságát



IEEE 802.1x (folyt.)

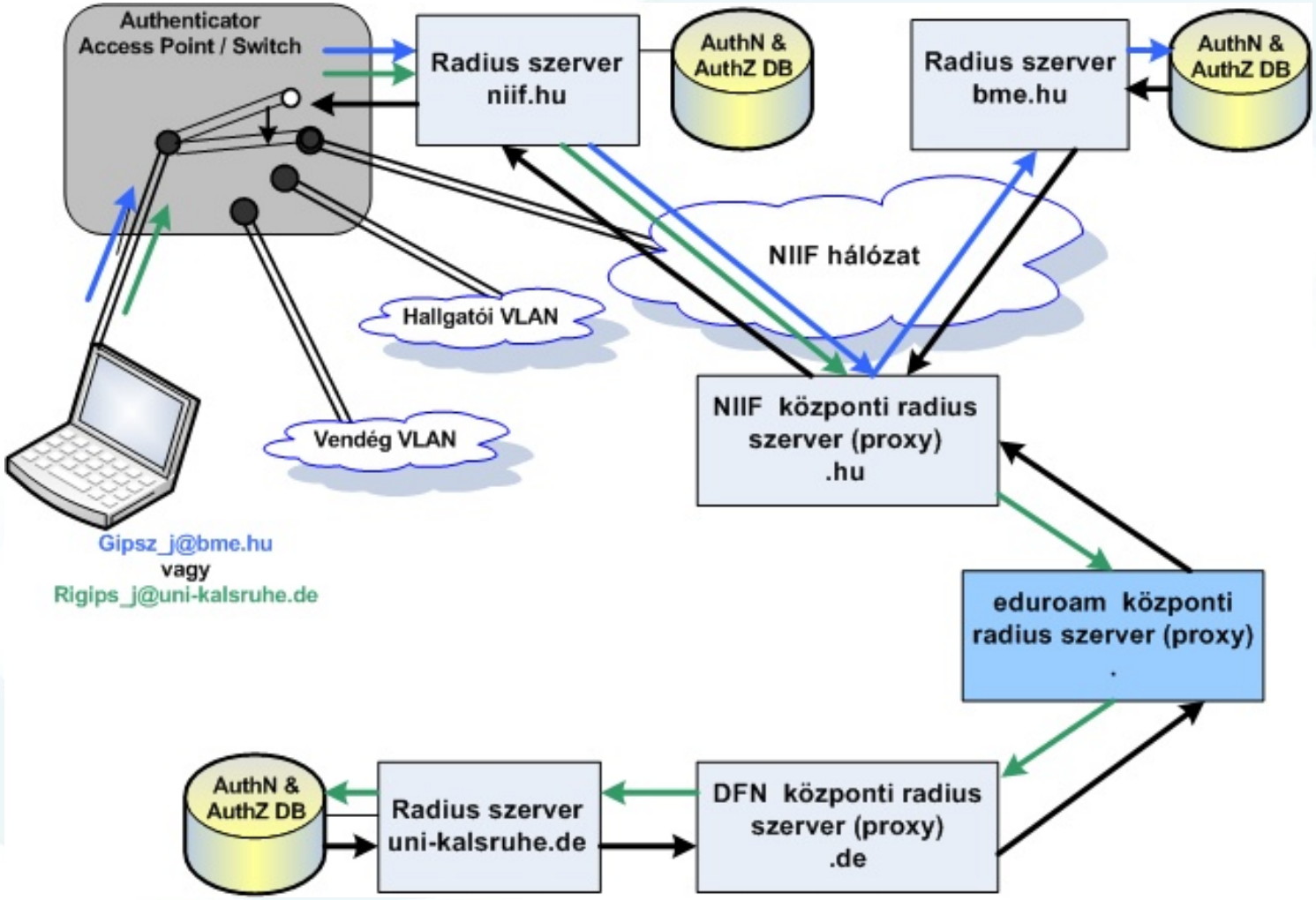
- amíg a supplicant azonossága nincs igazolva, addig az authenticator csak EAP forgalmat enged át a supplicant portján
  - WLAN esetén ez az Association ID-hez rendelt virtuális port



EAP típusok

Tulajdonság	EAP MD5	LEAP	EAP TLS	PEAP	EAP TTLS
Biztonsági megoldás	Szabványos	Vendor specifikus	Szabványos	Szabványos	Szabványos
Tanúsítvány – Kliens	Nem	?	Igen	Nem	Nem
Tanúsítvány – Szerver	Nem	?	Igen	Igen	Igen
Azonosítás biztonsága	Semmilyen	Gyenge	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

Hogyan csatlakozzunk az Eduroam-hoz?

- Előfeltételek:
  - Működtessünk egy karbantartott felhasználói adatbázist
  - Működtessünk helpdesk-et ahol a felhasználói és biztonsági problémákat tudjuk kezelni
  - Legyen felhasználói szabályzatunk és/vagy AUP-nk
- Állítsunk fel helyi vezeték nélküli hálózati szolgáltatást amely a fenti felhasználói adatbázist használja felhasználói azonosításra (802.1x)

Hogyan csatlakozzunk az Eduroam-hoz? /2

- Állítsuk be a helyi 802.1X infrastruktúrát, hogy
  - A my-domain.hu realmről érkező kéréseket helyiként dolgozza fel
  - Továbbítsa a nem helyi kéréseket (proxy) a nemzeti szerverre
- Egyeztessünk az NIIF-el:
  - Nemzeti radius szerverek FQDN neveiről és IP címeiről
  - RADIUS szerverek közötti shared secretről – biztonságos csatornán
  - Intézményi vezetéknélküli/eduroam website URL-je
  - test-accountról – biztonságos csatornán
  - Adminisztrátor elérhetősége
- Írjuk/írassuk alá a föderációs szerződést

Hogyan válaszunk Access Pointot?

- Alapvető
  - 802.1x támogatás
  - WPA- Enterprise, WPA2-Enterprise – 802.11i,
  - Logolás, konfigurálhatóság, SNMPv2c
- Ha komolyan gondoljuk
  - 802.11 - rádió
    - Több SSIDs támogatás a Beacon-ben
    - 802.11 MIB
  - 802.1X - 802.1X MIB
  - SNMPv3
  - RADIUS Authentication and accounting
- Jó ha van
  - Dynamic VLAN support
  - Wireless Controllel – ha nehany tucatnál több AP-t kell menedzselni

802.1x ~ RADIUS

- RADIUS autentikáció szükséges EAP-hoz
- Szervernek támogatni kell a választott típust (EAP-TLS, EAP-TTLS, PEAP)
- Több szerver lehetséges, hogy redundáns legyen
- Szerverek:
  - Cisco ACS – egészen a 4.2-es változatig gyatra EAP támogatás
  - FreeRADIUS – manuál gyenge, de a levelezési listán mindenre válaszolnak
  - IAS 2003 – csak PEAP, viszont integrálva van a Microsoft Active Directory-val
  - Radiator – nagyon jó támogatás
  - Infoblox
  - Funk Steel-belted
  - És még sok más

RADIUS konfiguráció

- Access point konfiguráció – IP cím + shared secret
- EAP mód konfiguráció – és választás!
  - EAP-TTLS – tetszőleges jelszó adatbázis
  - PEAP – a felhasználói név/jelszó adatbázisuknak vagy Microsoft AD-ben, vagy NTLM hash-ben, vagy nyílt szövegben kell lennie
  - Mind két esetben szükségünk van a RADIUS szerveren szerver tanusítványra (TLS!) – pl. NIIF TERENA SCS

RADIUS konfiguráció

- NIIF Eduroam Proxy konfiguráció – 2 IP, + shared secret
- Realm-el ellátott (username@realm) azonosítók feldolgozásának konfigurálása
  - Saját realm
  - Forward a NIIF Edurom proxy-nak
- Teszt/monitoring account konfigurálása

Freeradius konfiguráció

- Ha több realm szükséges lehethet (unlang) – javasolt
  - http://ipv6.niif.hu/m/Wireless_Eduroam_FreeRadius
    - Szerzők: Jákó András, Kadlecsik József,Mohácsi János
- Ha csak 1 realm (Fallback to default)
  - https://confluence.terena.org/display/H2eduroam/How+to+deploy+eduroam+on-site+or+on+campus

802.1x supplicant ~ EAP Compatibility

Kliens	98/ ME	XP/ 2K	OS X	Li nux	Pckt PC	TLS	PEAP	TTLS	Licensz
Win beépített	✗	✓	✗	✗	✗	✓	CHAP v2	✗	beépített
OSX beépített	✗	✗	✓	✗	✗	✓	✓	✓	beépített
SecureW2	✗	✓	✗	✗	✓	✗	✗	✓	$$/ ingyenes
Odyssey (J)	✓	✓	✗	✗	✓	✓	✓	✓	$$
AEGIS (C)	✓	✓	✓	✓	✓	✓	✓	✓	$$
wpa_supp	✓	✓	✗	✓	✗	✓	✓	✓	ingyenes
Xsupplicant	✗	✗	✗	✓	✗	✓	✓	✓	ingyenes

Reference: LIN 802.1x factsheet

Kérdések

eduroam@niif.hu