# 802.1x and Eduroam

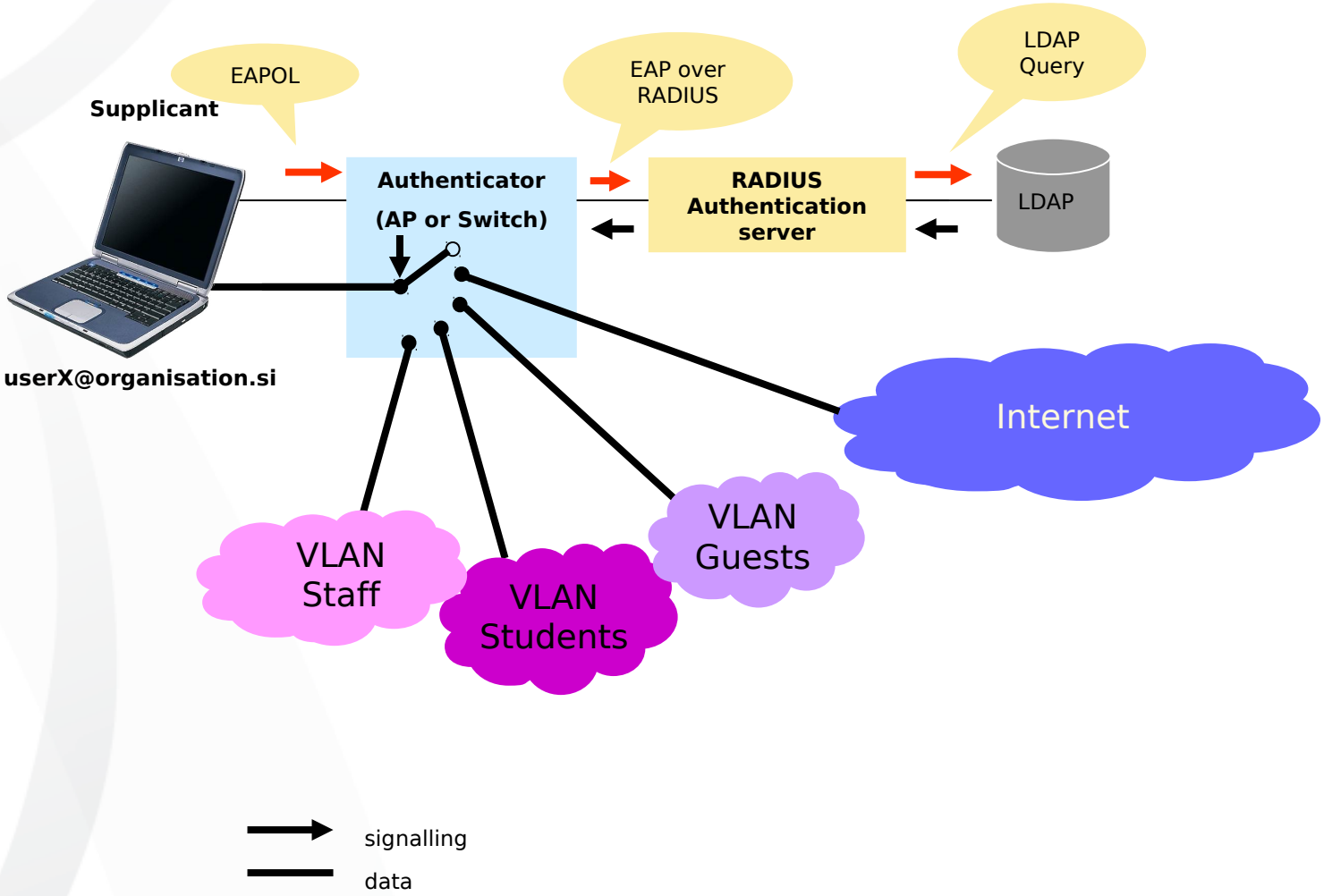
Rok Papež
Arnes, p.p. 7, SI - 1001 Ljubljana, Slovenia
aaa-podpora@arnes.si
rok.papez@arnes.si

GN3 BCP and Tf-Mobility, Belgrade
12. 09. 2011

# Ethernet network

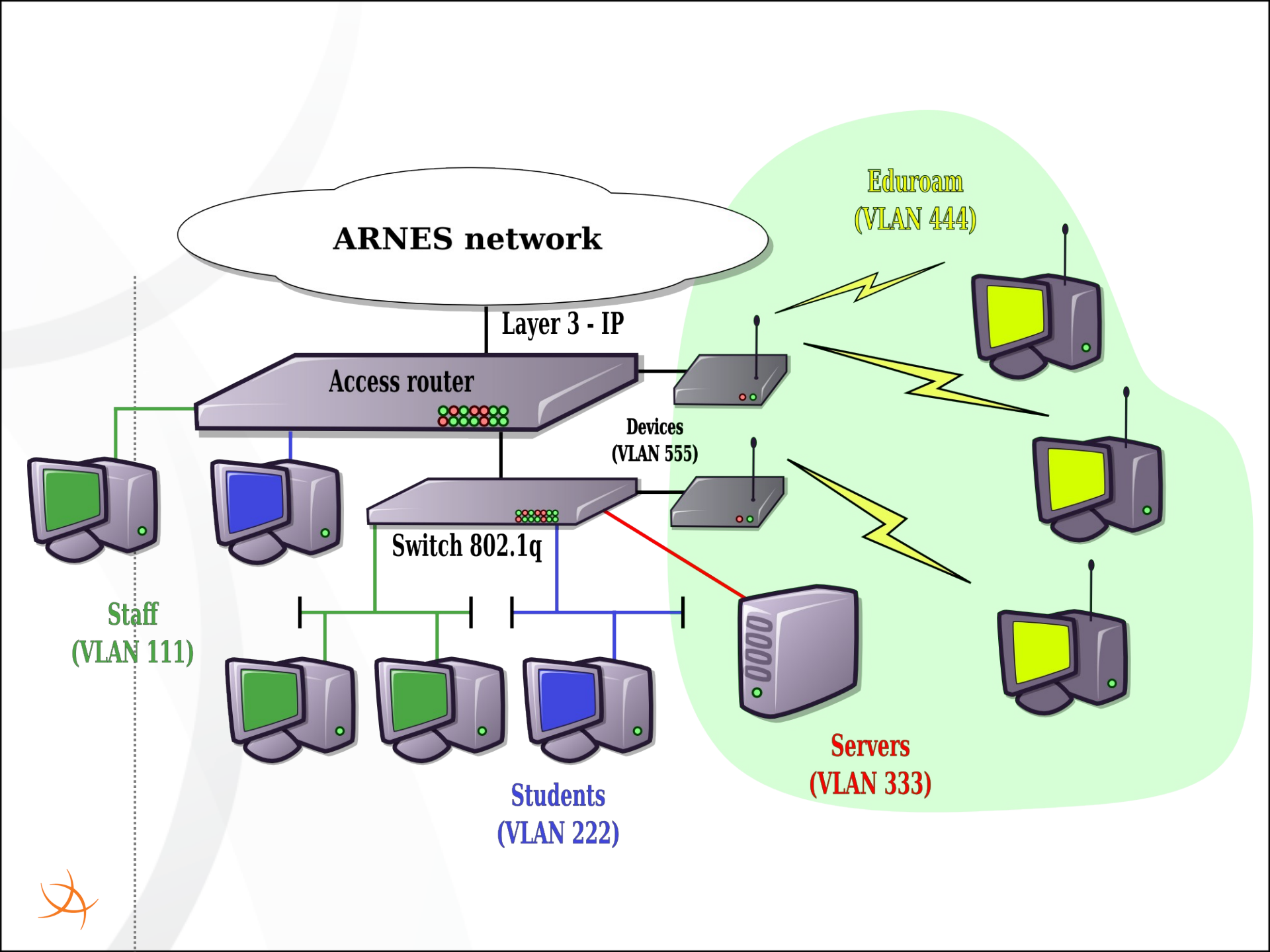
- Ethernet – old  technology
  - 1972, Xerox, Flower power - „Nice“ users
- Wired access (physical security)
- Wireless access (physical security?!)
- IEEE 802.1x
  - Device authenticates to network

# Network login - 802.1x



# 802.1x and EAP protocol stacks

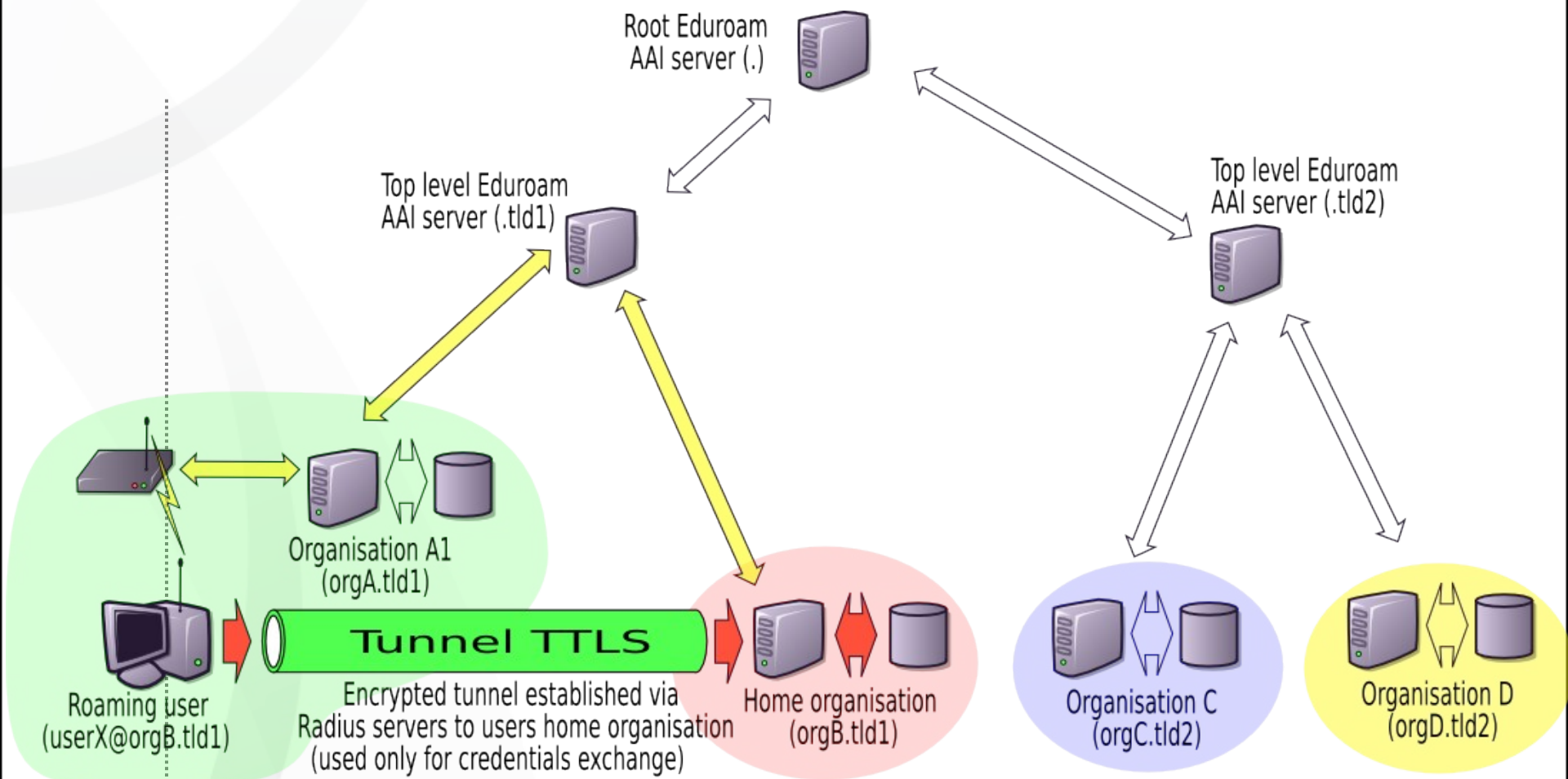
- Access Network:
  - Unauthenticated: Ethernet:EAPOL
  - Authenticated: Ethernet:IP
- Access Point / Switch to RADIUS
  - Management traffic
  - IP:UDP:RADIUS:EAP:<EAP type>
  - Authenticator == „EAP proxy“


ARNES network
Layer 3 - IP
Access router
Switch 802.1q
Eduroam
(VLAN 444)
Devices
(VLAN 555)
Staff
(VLAN 111)
Students
(VLAN 222)
Servers
(VLAN 333)

# Eduroam

- 2003, TERENA task force tf-mobility
  - Web portal (insecure)
  - VPN concentrators (unscalable)
  - 802.1x (perfect – not :-))
- Wireless + RADIUS interconnects
- Eduroam.si:
  - Internet (no NAT or fascist firewalling)
  - No fuzz (configure once, run everywhere)
  - Dynamic VLANs

# Eduroam - let's roam!



# EAP types

- Eduroam: EAP-Any-with-keys :)
  - EAP-TTLS (+ PAP, MSCHAPv2), EAP-TLS, PEAP
  - EAP-FAST, EAP-SIM, EAP-AKA
- Weak EAP types:
  - EAP-MD5, LEAP ...
- **Deployment!**
- **User support!!!**

# User database

- RADIUS supports a lot of backends
  - Static entries/files, SQL databases
  - Active Directory, LDAP directory
  - Kerberos or Samba (ntlm) authentication
- LDAP – structured database
  - Mandatory for Eduroam.si
  - Web AAI / SSO systems (simplesamlphp)
  - Schemas EduPerson and SCHAC
- Identity management

# Passwords vs. hashes

- Typically: DB hash or On-Wire hash
- Security vs. Usability
- One application DB vs. Central authentication store
- PEAP -> MSCHAPv2
- EAP-TTLS -> PAP, MSCHAPv2, ...
- http://deployingradius.com/documents/protocols/compatibility.html

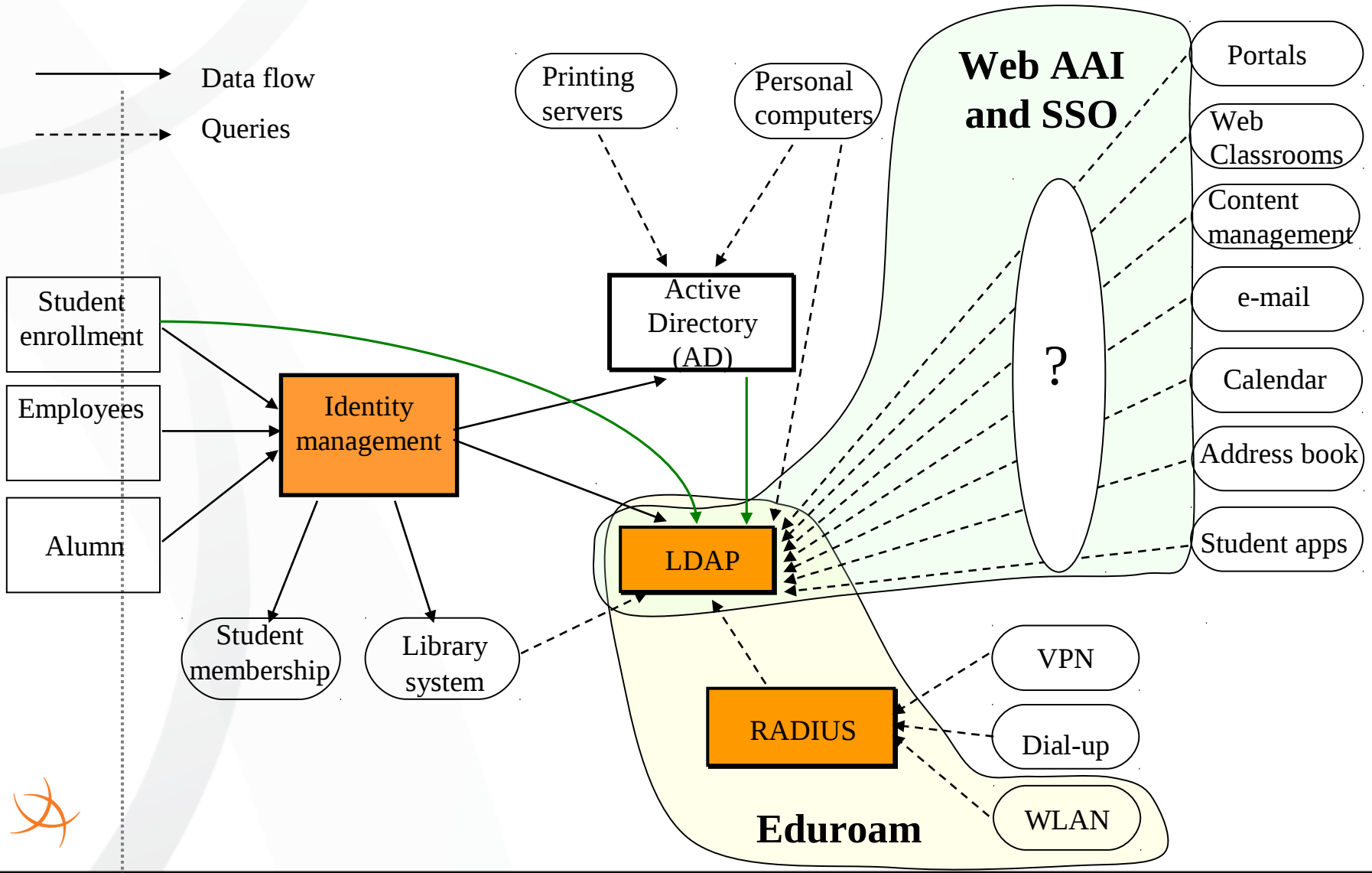
# Usability

- Eduroam:
  - SSID
  - Encryption (WEP, WPA, WPA2)
  - Supplicant
  - EAP Type
  - Credentials (user/pass or cert)
  - CA or Server certificate
- All users „devices“: different OSes
- Site deployment: SecureW2
  - ftp://ftp.arnes.si/software/eduroam

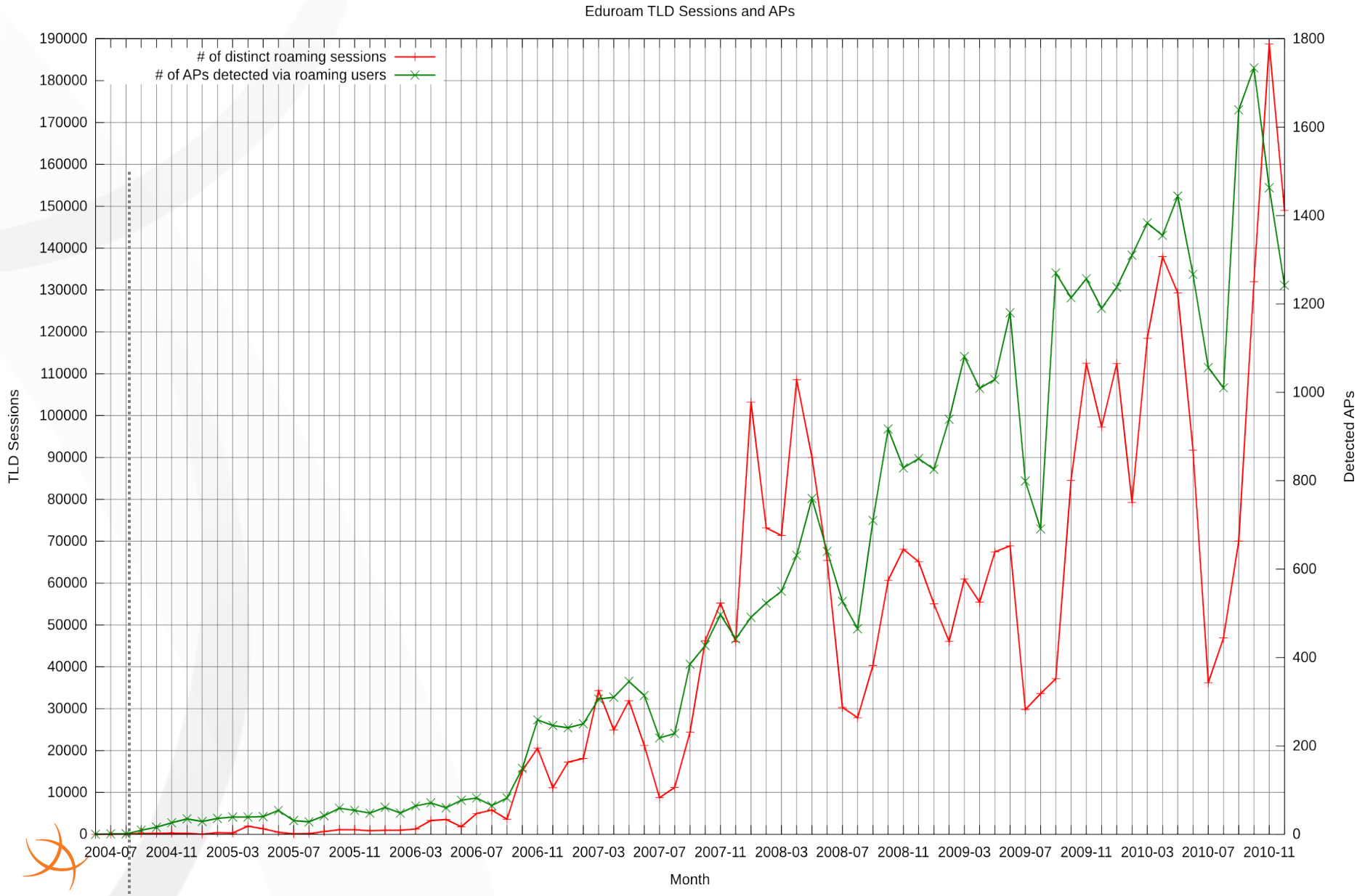
# Wired 802.1x

- Student dormitories in Ljubljana ~ 8000 beds
  - Access network: Wired 802.1x with HP ProCurve 2650/2610
  - 10GE backbone uplink to Arnes
  - Optical backbone
  - Routers Cisco Catalyst 3750/3650
  - IPv6 deployment – dual stack
  - 2 level helpdesk
- Initial government funding, now self-sustaining

# Identity management data flow



# Eduroam.si TLD stats



Arnes AAI team

aaa-podpora@arnes.si

http://aai.arnes.si

http://www.arnes.si/pomoc-uporabnikom/eduroam.html

(CC) Blackandecker/Flickr