802.1X in SURFnet

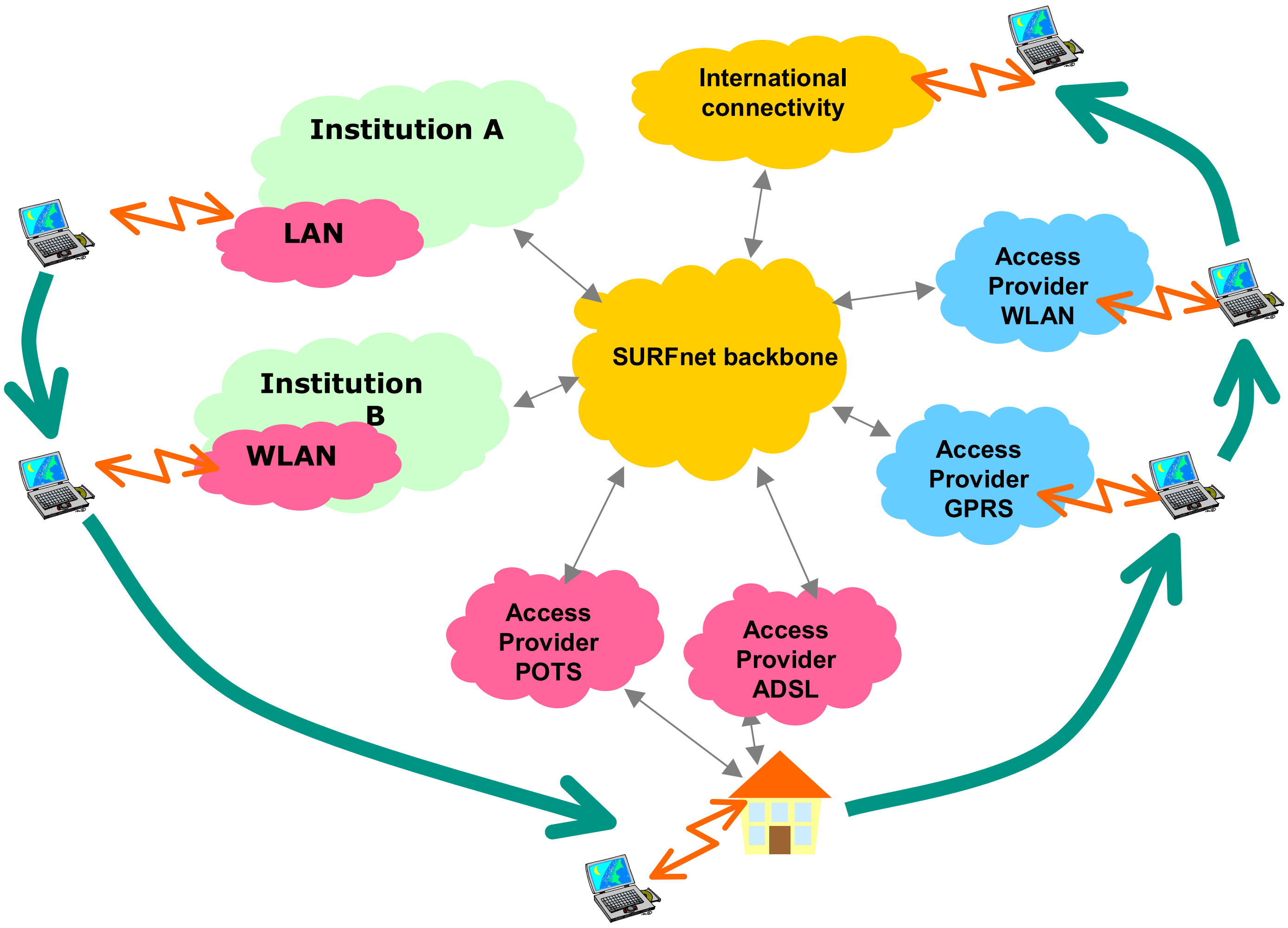
Klaas.Wierenga@SURFnet.nl

22 May 2003

TOC

- Background
- Requirements
- Various solutions investigated
- 802.1X in SURFnet, the Netherlands and Europe
- Lessons learned
- The future
- Conclusion

Background


International connectivity
Institution A
LAN
SURFnet backbone
Access Provider WLAN
Institution B
WLAN
Access Provider GPRS
Access Provider POTS
Access Provider ADSL

Requirements

- Identify users uniquely at the edge of the network
  - No session hijacking
- Allow for guest usage
- Scalable
  - Local user administration and authN!
  - Using existing RADIUS infrastructure
- Easy to install and use
- Open
  - Support for all common OSes
  - Vendor independent

- After proper AuthN open connectivity

Various solutions

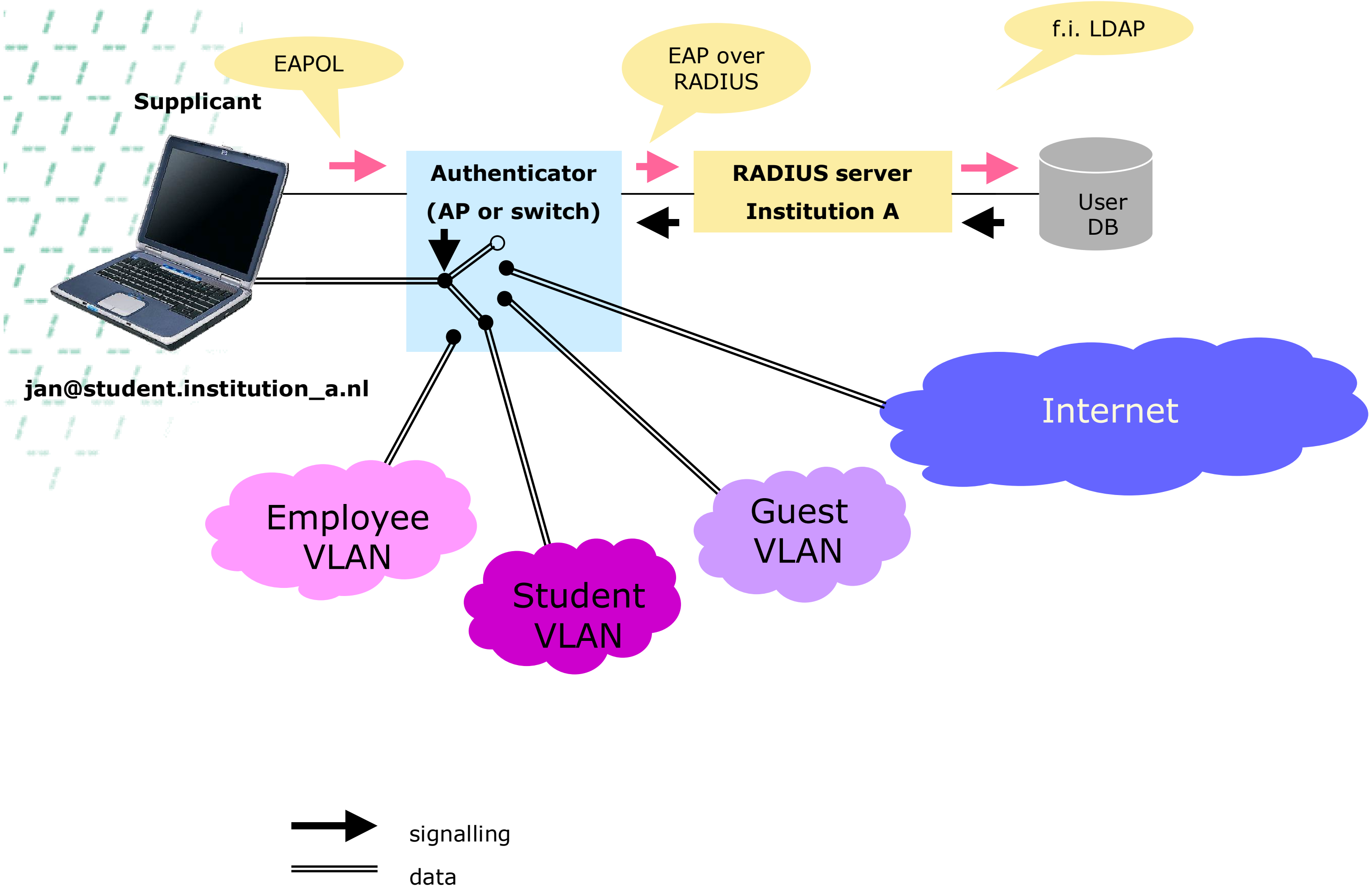
- WEP (unsafe)
- MAC-address (unsafe)
- LEAP (proprietary)
- Web-gateway (hard to make safe)
- VPN-gateway (hard to make scalable)

- 802.1X
  - Pilot with University of Twente and Alfa&Ariss

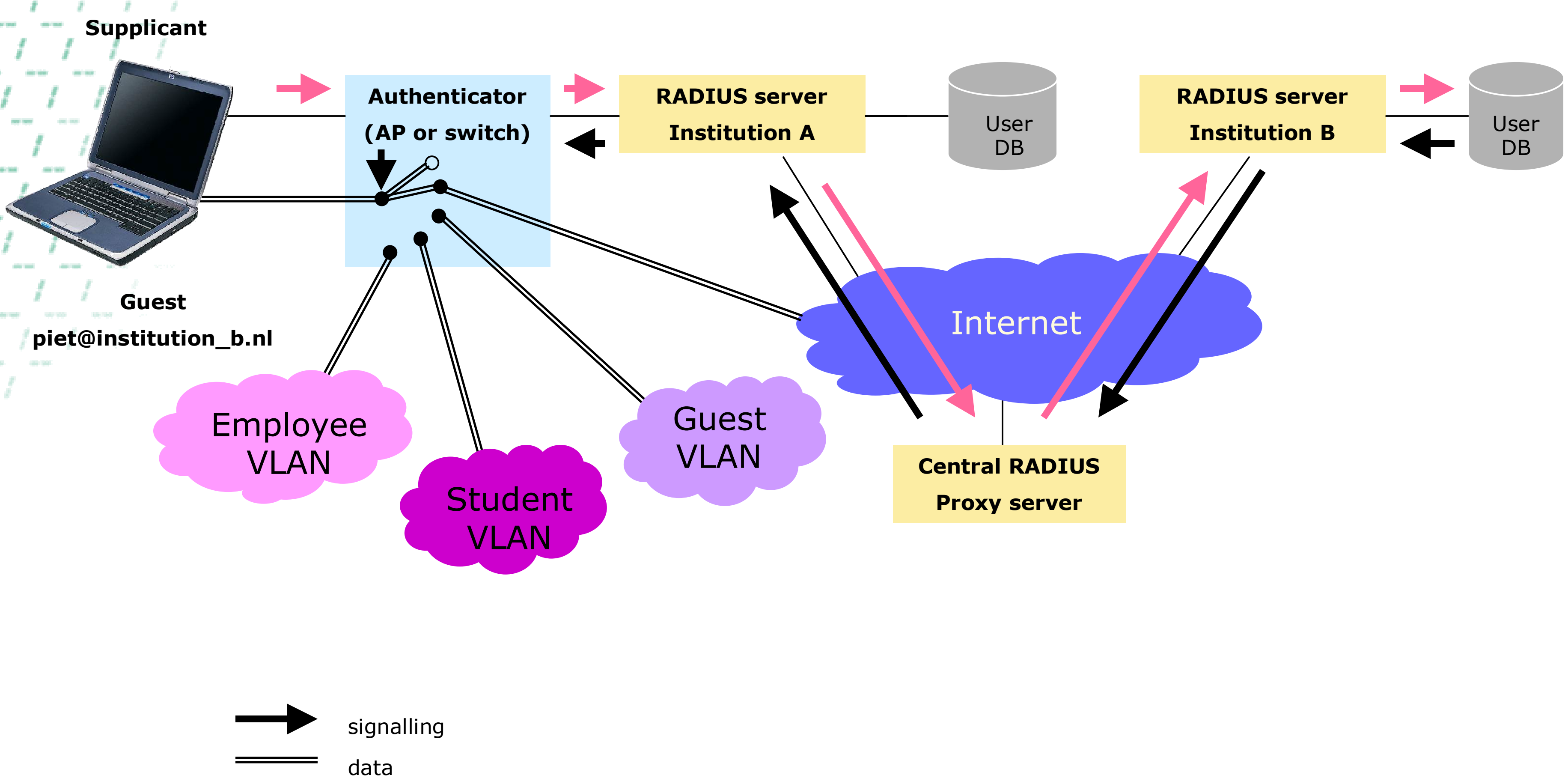
6. IEEE 802.1X

- True port based access solution (Layer 2) between client and AP/switch
- Several available authentication-mechanisms (EAP-MD5, MS-CHAPv2, EAP-SIM, EAP-TLS, EAP-TTLS, PEAP)
- Standardised
- Also encrypts all data, using dynamic keys
- RADIUS back end:
  - Scaleable
  - Re-use existing Trust relationships
- Easy integration with dynamic VLAN assignment
- Client software necessary (OS-built in or third-party)

802.1X in action



Cross-domain 802.1X with VLAN assignment



Current status

- Wireless
  - University of Twente, University of Amsterdam, Hogeschool van Amsterdam currently use 1X, most others are considering this.
- Fixed
  - Delft University, University of Tilburg currently use 1X, most others are considering this
- Software
  - Freeware tool SecureW2

…in the rest of the Netherlands (Freeband)

- Hotspots at public places near SURFnet locations
- WLAN connectivity on the move, i.e. trains, automobiles (planes yet to come)
- 802.1X connecting to SURFnet RADIUS infrastructure
- Open for whole SURFnet community

- Hotspots will be made available in Amsterdam, Utrecht, Groningen, Enschede, Eindhoven, Delft, Rotterdam, Leiden

… and beyond (TF-Mobility)

- European scale WLAN roaming
- Currently comparing
  - Web-based
  - VPN-based
  - 802.1X based
- In summer testbed definition

Lessons learned

- It’s all about scalability
- EAP types are either unsafe (MD5, MS-CHAPv2), hard to deploy (TLS) or not ready (PEAP) so the choice is easy: TTLS
- 2-way RADIUS infrastructure introduces possible problems
  - Prevent loops
- AUP needed for guest usage
- Logging is needed
- The more you see about 1X the more you like it

Future

New standards

- 802.11*
- WPA (pre standard 802.11i, TKIP)
- 802.11i: 802.1x + first TKIP, later AES

Application integration

- A-select (TNC session 8c)
  - OTP via SMS is available

Conclusion

- 802.1X is available
- 802.1X works
- 802.1X scales
- 802.1X is secure
- 802.1X is extensible
- 802.1X allows for guest usage
- 802.1X is the future

So what are you waiting for....

More information

- http://www.surfnet.nl/innovatie/wlan
- http://a-select.surfnet.nl
- http://www.freeband.nl