An introduction to secure, scalable wireless LAN deployment

Klaas Wierenga
SURFnet
klaas.wierenga@surfnet.nl

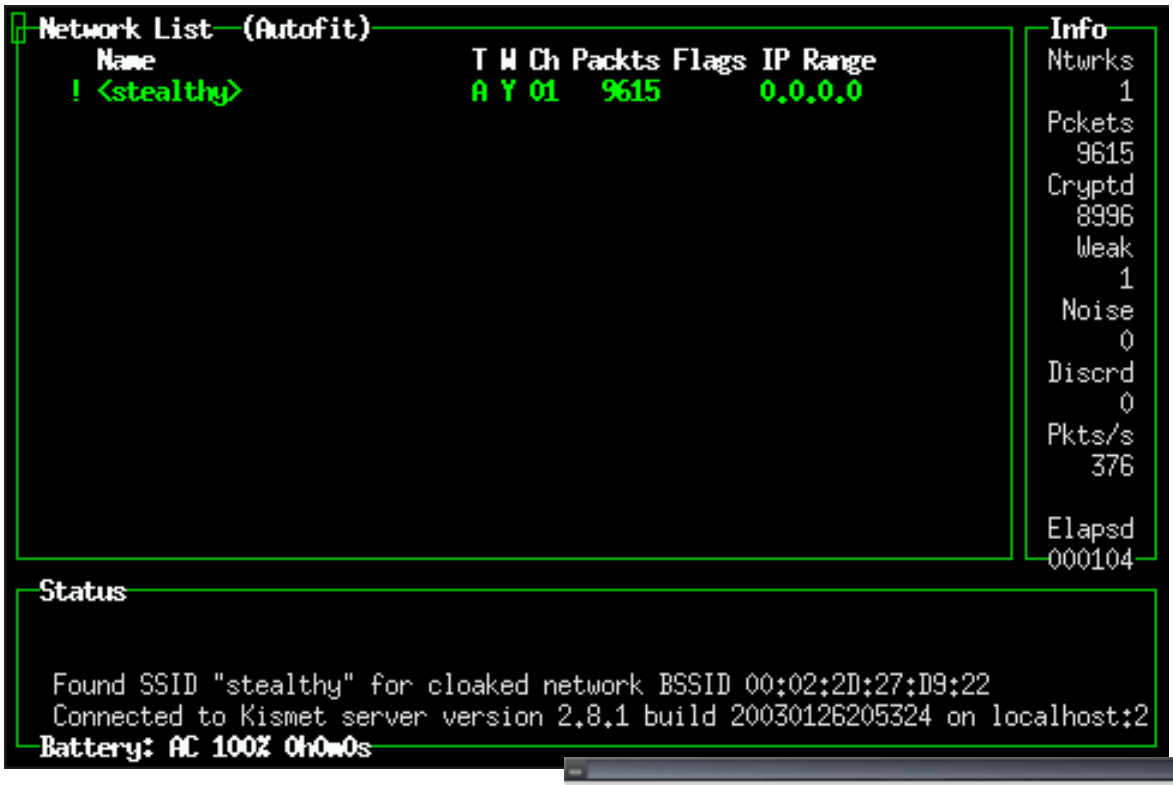
Stefan Winter
RESTENA
stefan.winter@restena.lu

Nicosia (CY), Jan 15, 2007

Contents

- Wireless network security
- IEEE 802.1X
- Conclusions

Wireless LANs are unsafe



root@ibook:~# tcpdump -n -i eth1

19:52:08.995104 10.0.1.2 > 10.0.1.1: icmp: echo request

19:52:08.996412 10.0.1.1 > 10.0.1.2: icmp: echo reply

19:52:08.997961 10.0.1.2 > 10.0.1.1: icmp: echo request

19:52:08.999220 10.0.1.1 > 10.0.1.2: icmp: echo reply

19:52:09.000581 10.0.1.2 > 10.0.1.1: icmp: echo request

19:52:09.003162 10.0.1.1 > 10.0.1.2: icmp: echo reply ^C

ifconfig eth1 hw ether 00:00:de:ad:be:ef

Requirements

- Identify users uniquely at the edge of the network
  - Prevent session hijacking
- Scalable
- Easy to deploy and use
- Open

- Give away for next part: allow for guest use

Possible solutions

Standard solutions provided by AP's:

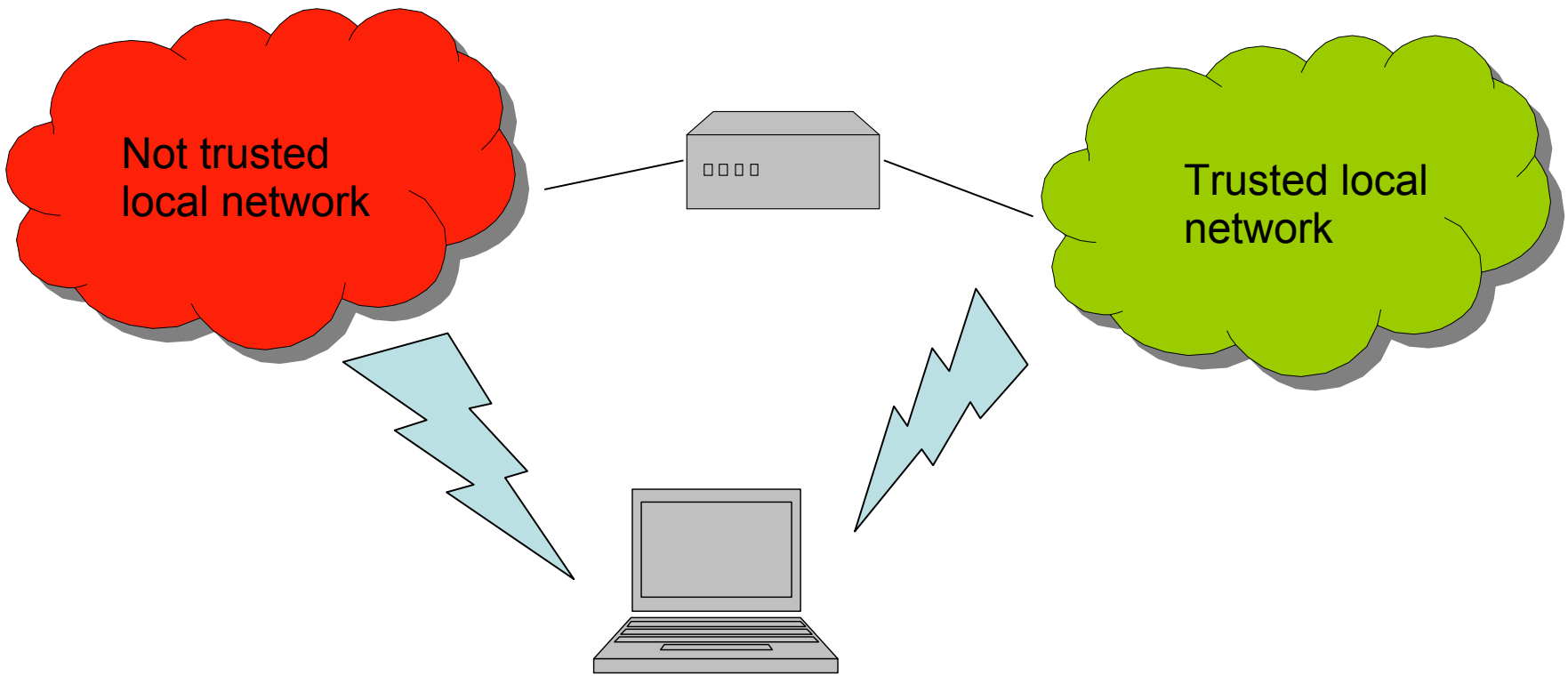
- Open access: scalable, not secure
- MAC-addres: not scalable, not secure
- WEP: not scalable, not secure

Alternative solutions:

- Web-gateway+RADIUS
- VPN-gateway

- 802.1X+RADIUS

Access to the campus WLAN



- Initial connection is either to a trusted or an untrusted network

Open network + web gateway (a.k.a. „web-redirect hotspots“)

- Open (limited) network, gateway between (W)LAN and the rest of the network intercepts all traffic (session intercept)

- Can use a RADIUS backend to verify user credentials
- Guest use easy
- Browser necessary for initial login

- Hard to maintain accountability
  - Session hijacking

Why isn't Web-Redirect good enough?

- Commercial hotspots almost exclusively use this method
- Why don't we?
  - no packet encryption on link, easily sniffable
  - user can't verify operator
  - operator doesn't care about lost/sniffed credentials as long as he gets his subscription money
- => Web-Redirect is perfect for a commercial operator
- but we should try to do better!

Open network + VPN Gateway

- Open (limited) network, client must authenticate on a VPN-concentrator to get to rest of the network

- Client software needed
- Proprietary and/or tough to setup
- Hard to scale
- VPN-concentrators are expensive
- Guest use hard (sometimes VPN in VPN)

- All traffic encrypted

- NB: VPN's **are** the method of choice for protecting data on a WAN

IEEE 802.1X

- True port based access solution (Layer 2) between client and AP/switch
- Several available authentication-mechanisms through the use of EAP (Extensible Authentication Protocol)
- Standardised
- Also encrypts all data, using dynamic keys
- RADIUS back-end:
  - Scalable
  - Re-use existing trust relationships
- Easy integration with dynamic VLAN assignment (802.1Q)
- Client software necessary (OS-built in or third-party)
- Future proof (WPA, WPA2/802.11i)
- For **wireless** and **wired**

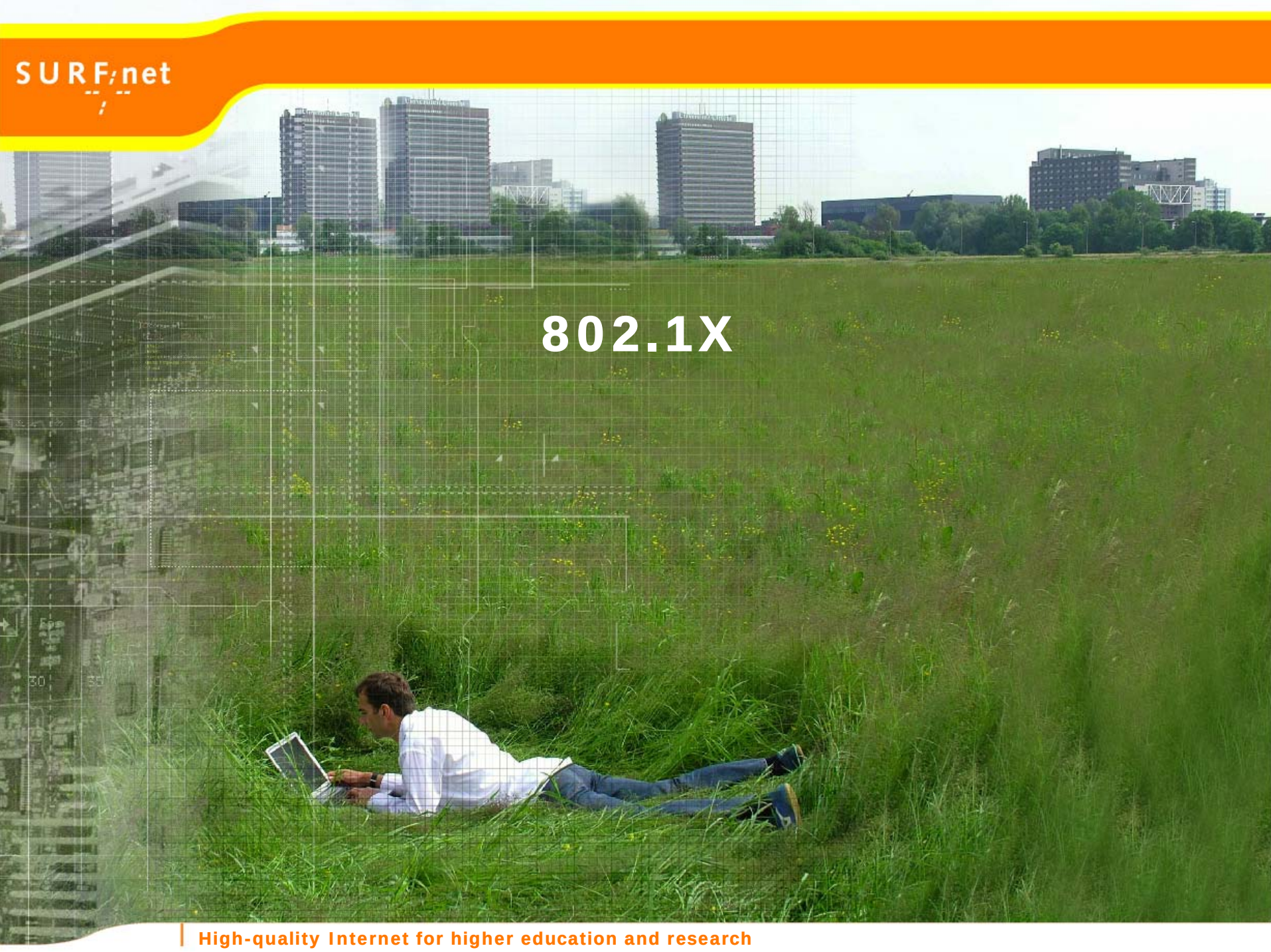
Summary

- SOHO security options of AP's don't work

- Web-redirect+RADIUS: scalable, not secure
- VPN-based: not scalable, secure
- 802.1X: scalable, secure

SURFnet

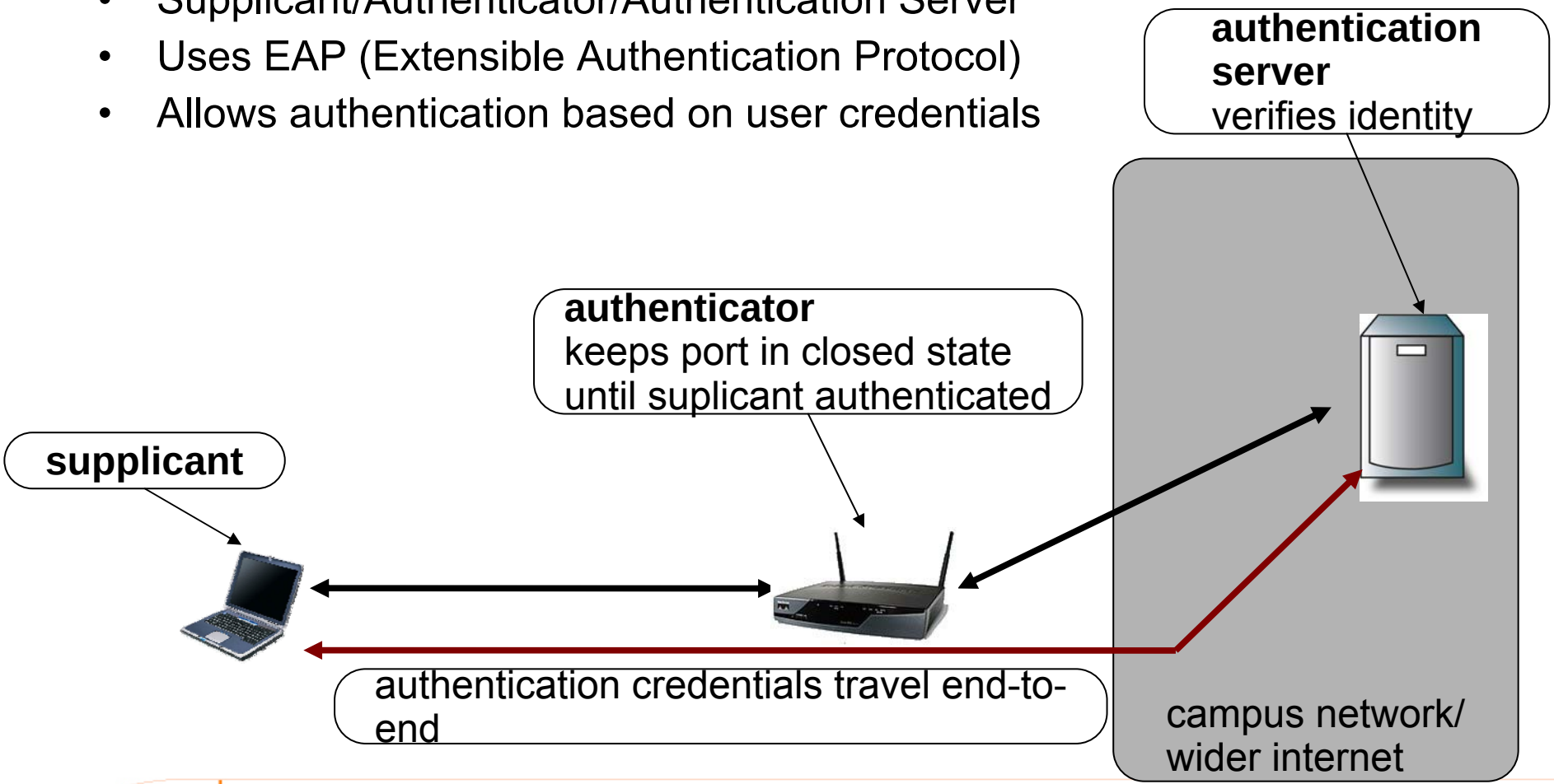
802.1X



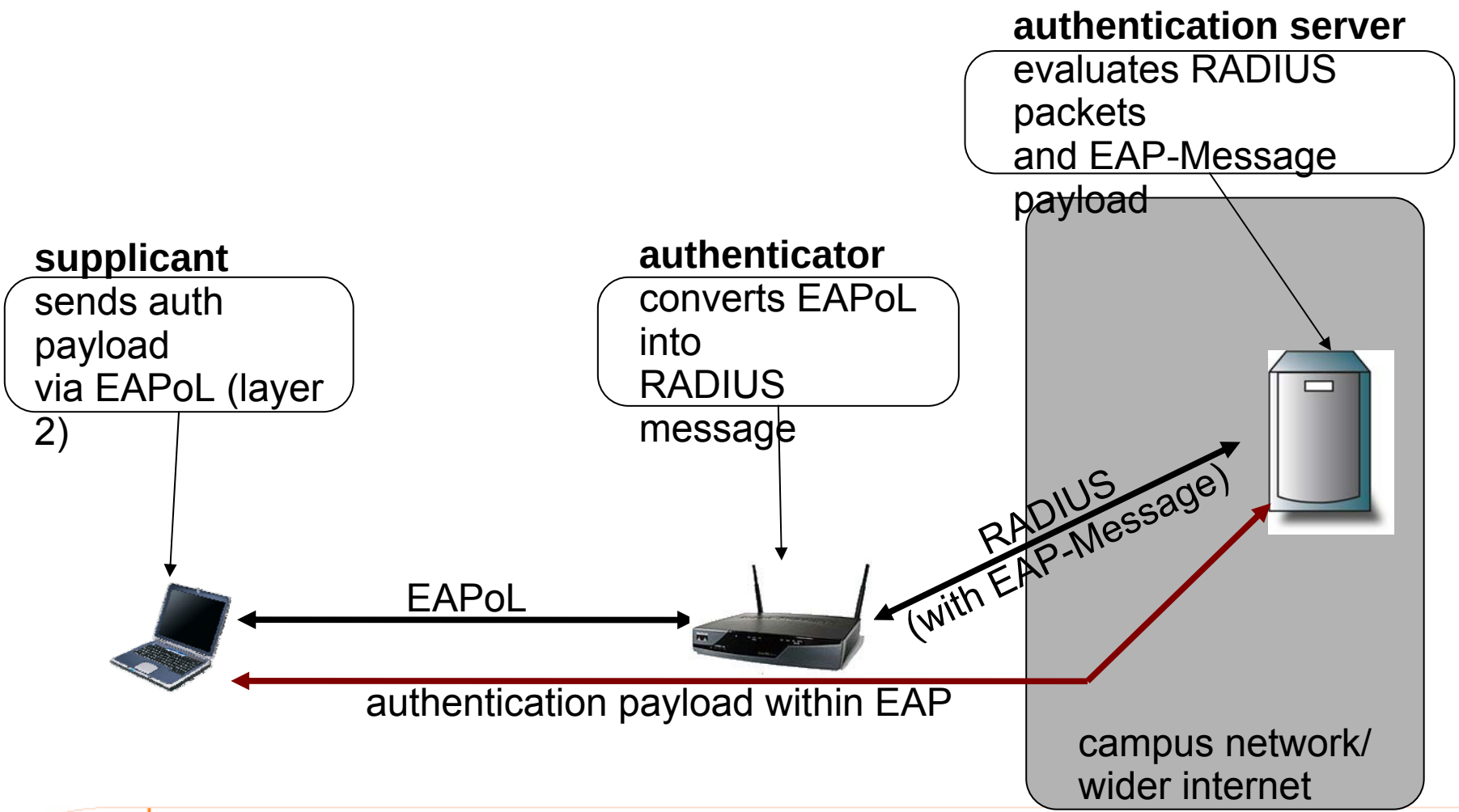
High-quality Internet for higher education and research

802.1X/EAP

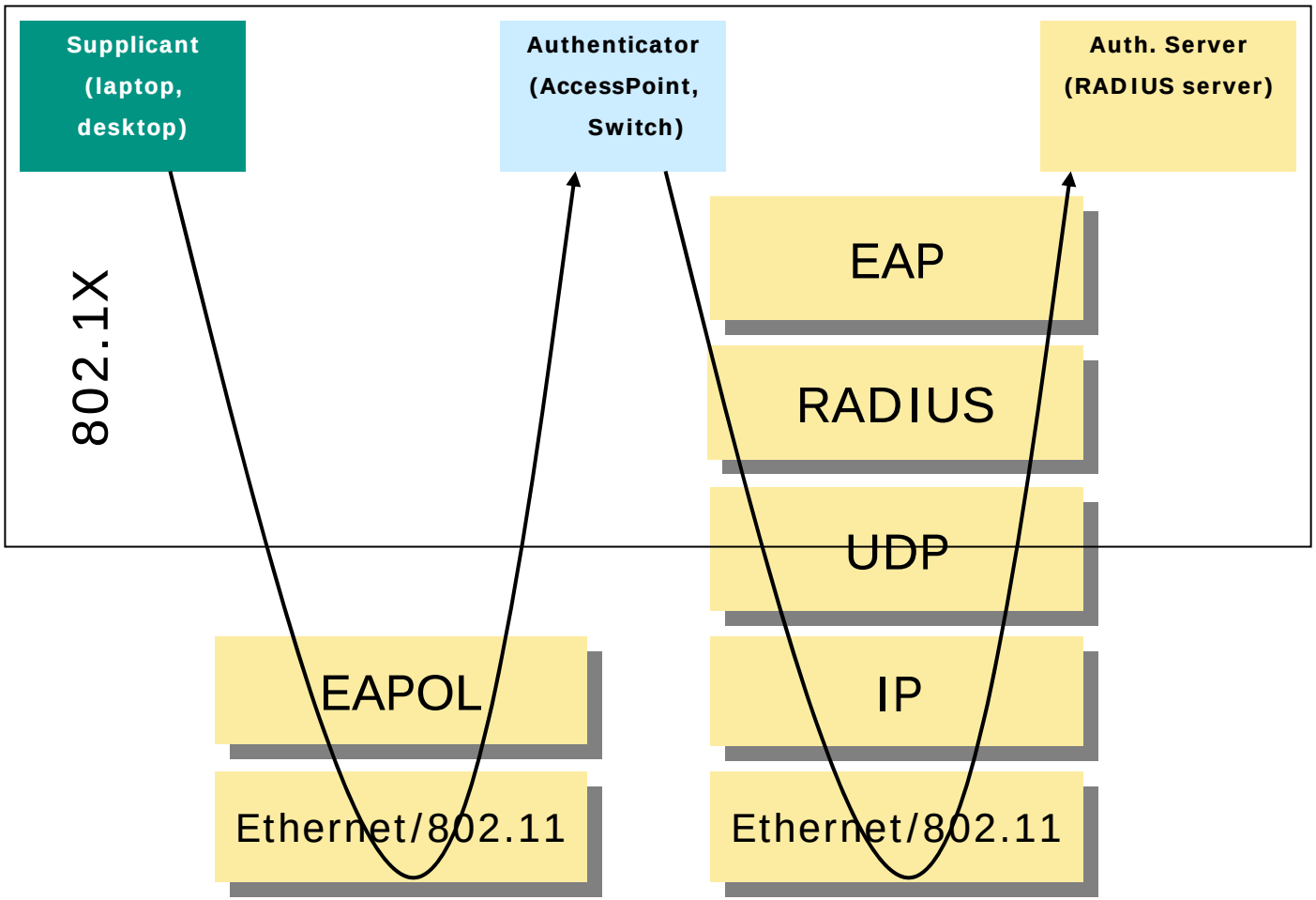
- Authenticated/Unauthenticated Port
- Supplicant/Authenticator/Authentication Server
- Uses EAP (Extensible Authentication Protocol)
- Allows authentication based on user credentials



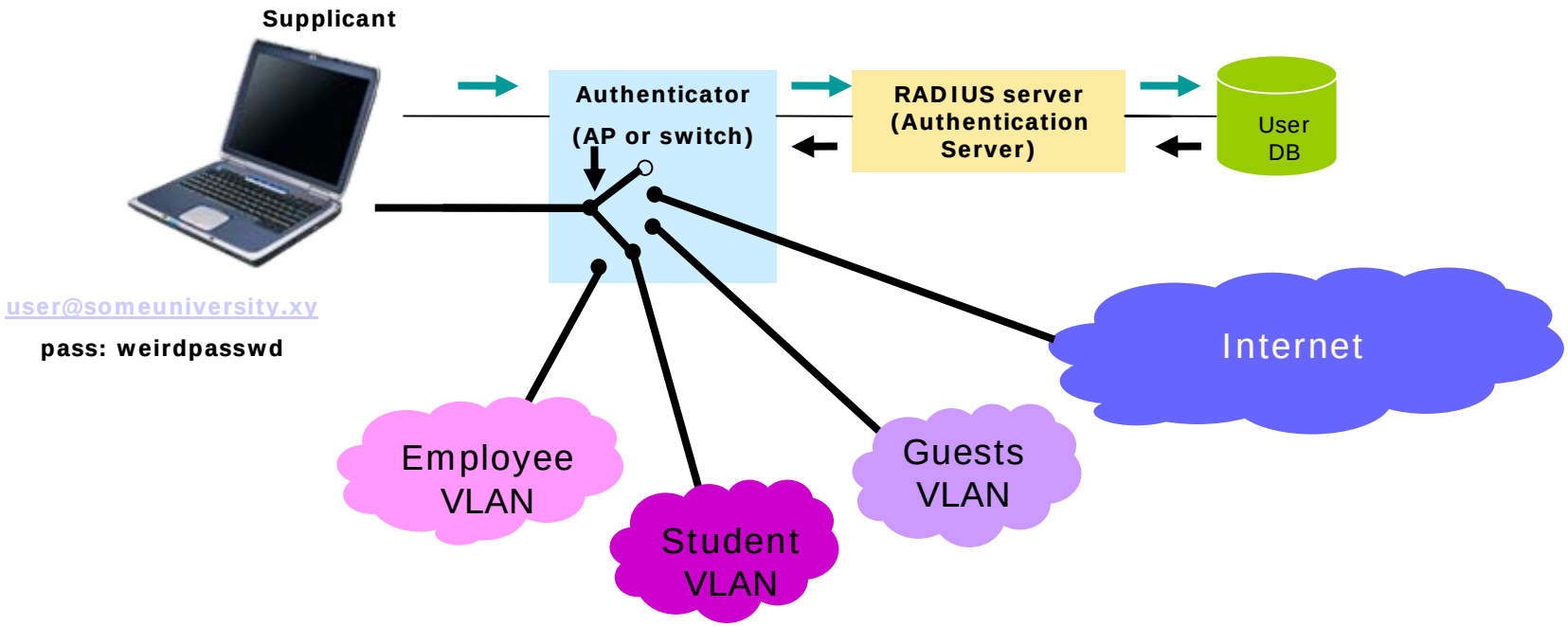
EAP over LAN (EAPOL)



Through the protocol stack



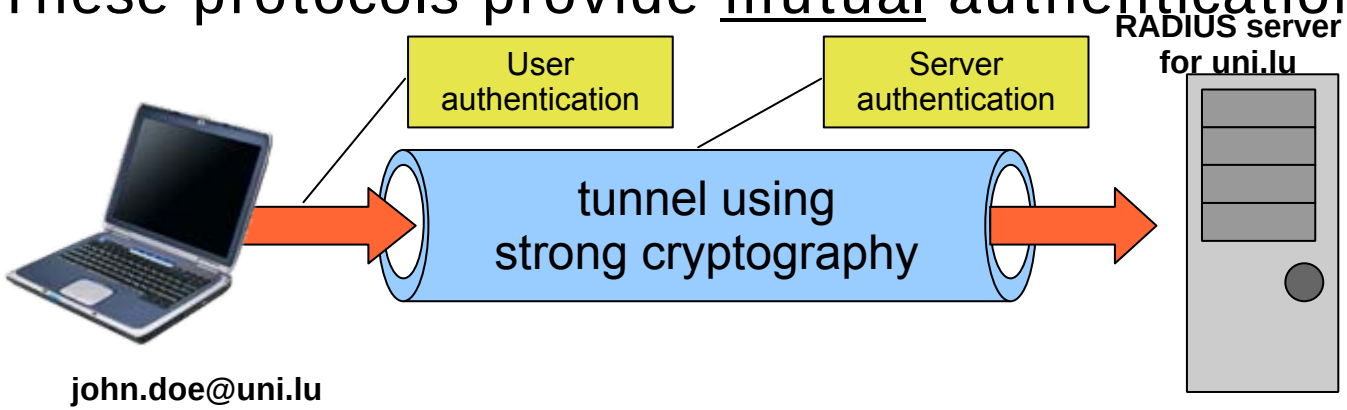
Secure access to the campus LAN with 802.1X



- 802.1X
- (VLAN assignment)

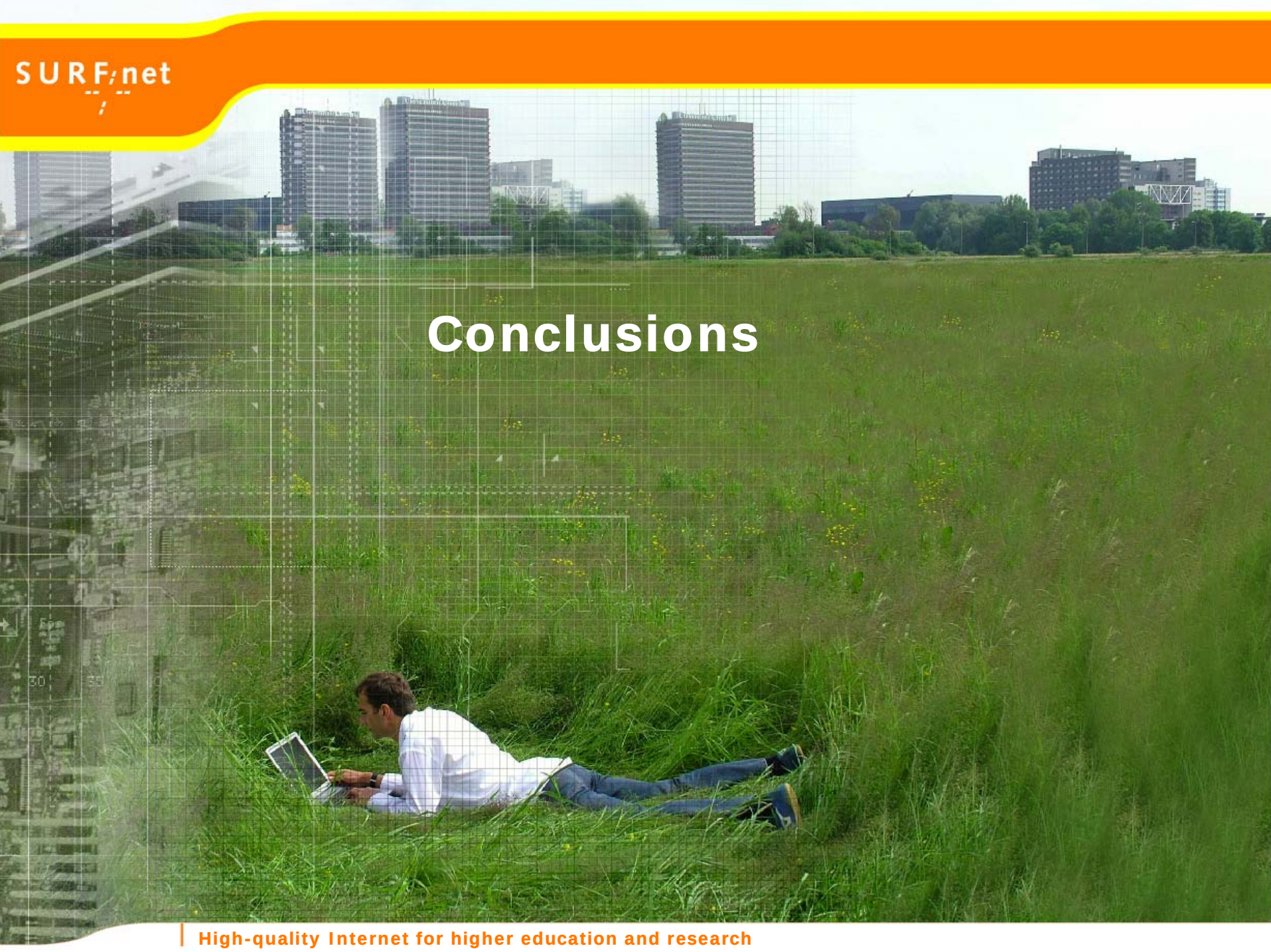
securing the authentication payload

- Common protocols within EAP:
  - EAP-TLS: both supplicant and server validate their identity with certificates
  - EAP-TTLS: server presents certificate, establishes TLS tunnel → supplicant uses username+password
  - PEAP-MSCHAPv2: similar to EAP-TTLS, but additionally encrypts username+password
- These protocols provide mutual authentication



SURFnet

Conclusions



Summary

- There is a difference between providing access to campus resources over the Internet and providing network access
- Access via the Internet: VPN

- Network access: 802.1X

- Next: How 802.1X can be leveraged for guest access