What about 802.1X?

An overview of possibilities for safe access to fixed and wireless networks

General authentication requirements for access to networks

- Unique identification of users at the edge of the network
- Identity take-over must be impossible
- Ease of use for the end-user
- Per-institution provisioning of users in one database of the institutions network
- Low maintenance
- Ease of use for guests
- Enabling various authentication-mechanisms

Additional demands for network-access:

- Automatic VLAN-assignment per use group
- Encrypted wireless access

Overview of authentication/ authorisation-mechanisms

1. Open network
2. Open network + MAC-authentication
3. Open network + VPN-gateway
4. Open network + web based gateway
5. WEP (wireless)
6. IEEE 802.1X

Not considered: LEAP (Cisco proprietary), PPPoE (not widely deployed)

1. Open network

- Provides open ethernet connectivity, gives IP-address by DHCP (Layer 2/3 solution)
- No client software necessary (DHCP is widely spread)
- Access control is difficult
- Network is open (sniffing is possible, every client and server on the LAN is reachable)

2. Open network + MAC authentication

- Same as 1, but the MAC-address of the users' network card is checked by the network
- Operational hassle to administrate MAC addresses
- MAC addresses can be spoofed
- Guest usage is difficult

3. Open netwerk + VPN Gateway

- Open network, client must authenticate at an IP-VPN (Layer 3) gateway between the WLAN and the institutions network
- Client software necessary
- Vendor-specific
- Guest use is difficult
- Poor scalability (is getting better)
- VPN-concentrators are expensive
- VPN-concentrator is often already in place for safe access to resources from dial-in etc.

4. Open network + web based gateway

- Open network, an IP-router (Layer 3) gateway between the WLAN and the institutions network initially intercepts all traffic and presents a web page to the user on which the user must enter its ‘credentials’. If they are correct, (certain) traffic is passed through.
- Vendor-specific
- Guest logon is easy
- Poor scalability (is getting better)
- A browser must be installed, that stays active during the entire session (also when only using mail)

5. WEP

- Layer 2 encryption between Client and Access Point
- The Client must know a long string (‘password-like’) to be able to get access to a Wireless Access Points
- Operational hassle when changing WEP-keys
- Not all WEP-keys are hard to hack, but the keys must be changed regularly so a hacker cannot collect enough data to retrieve the key

6. IEEE 802.1X

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

802.1X ≠ 802.11x

802.11x is sometimes used to summarise all ethernet standards (i.e. 802.11a, 802.11b) but it is not a standard!

802.1X is a standard from the 802.1a, 1b series, developed by 3Com, HP, and Microsoft

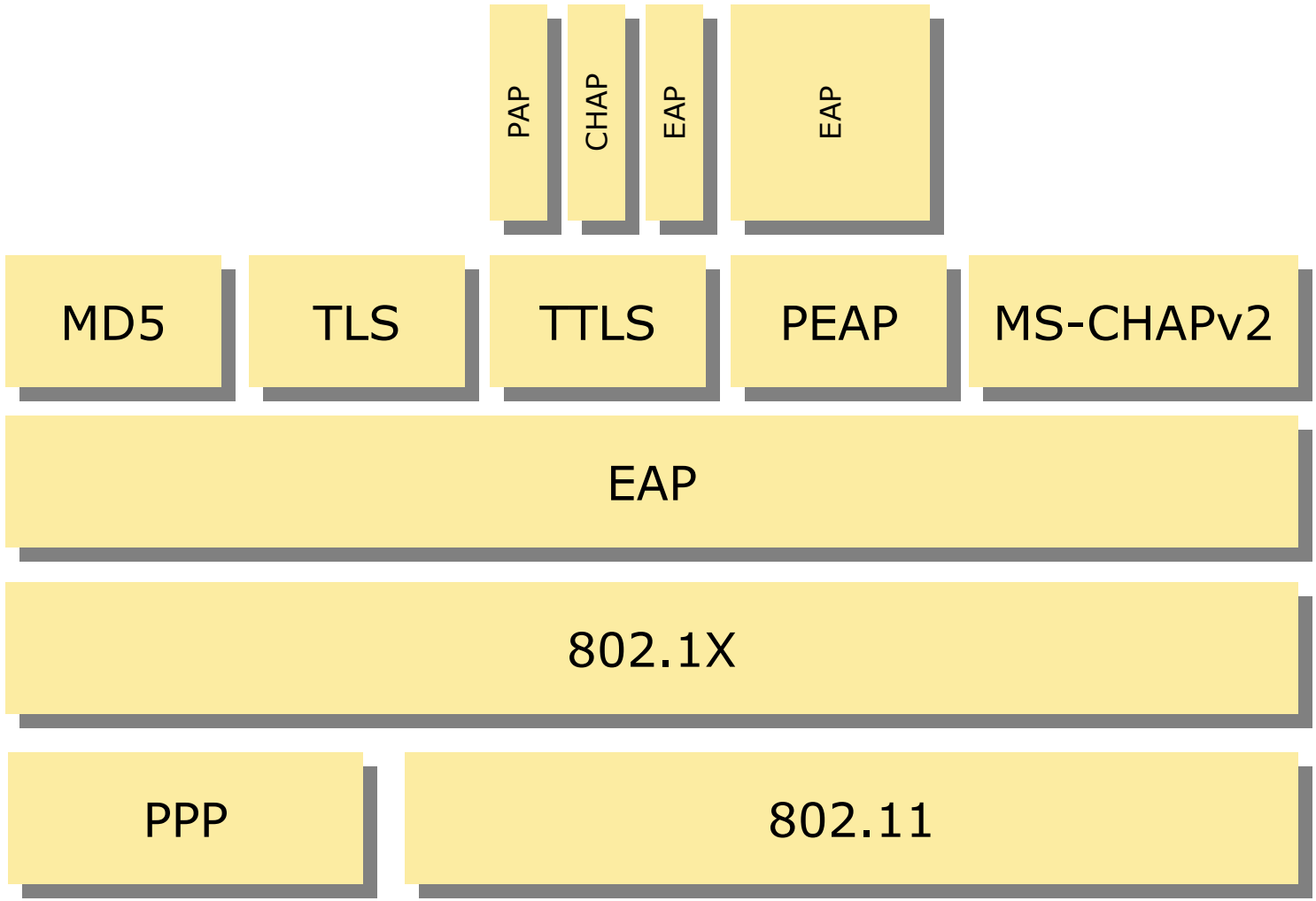
802.1X is a transport mechanism. The actual authentication takes place in the EAP-protocol on top of 802.1X.

EAP over 802.1x

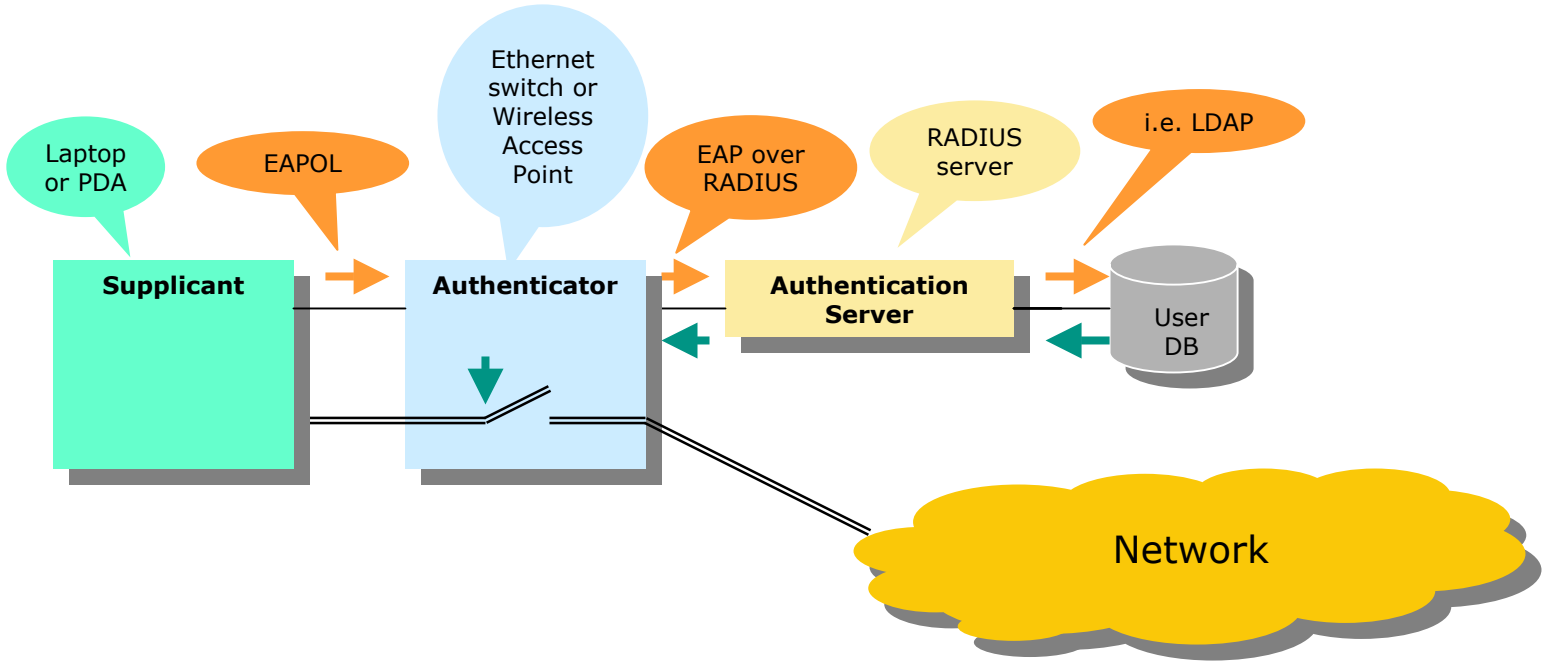
Extensible Authentication Protocol (RFC 2284) provides an architecture in which several authentication-mechanisms can be used

- EAP-MD5 Username/Password (unsafe)
- EAP-TLS PKI (certificates), strong authentication
- EAP-TTLS Username/Password (safe)
- MS-CHAPv2 Microsoft Username/Password (not safe)
- PEAP Microsoft/Cisco tunnel module for safe transport of MS-CHAPv2

Protocol-overview



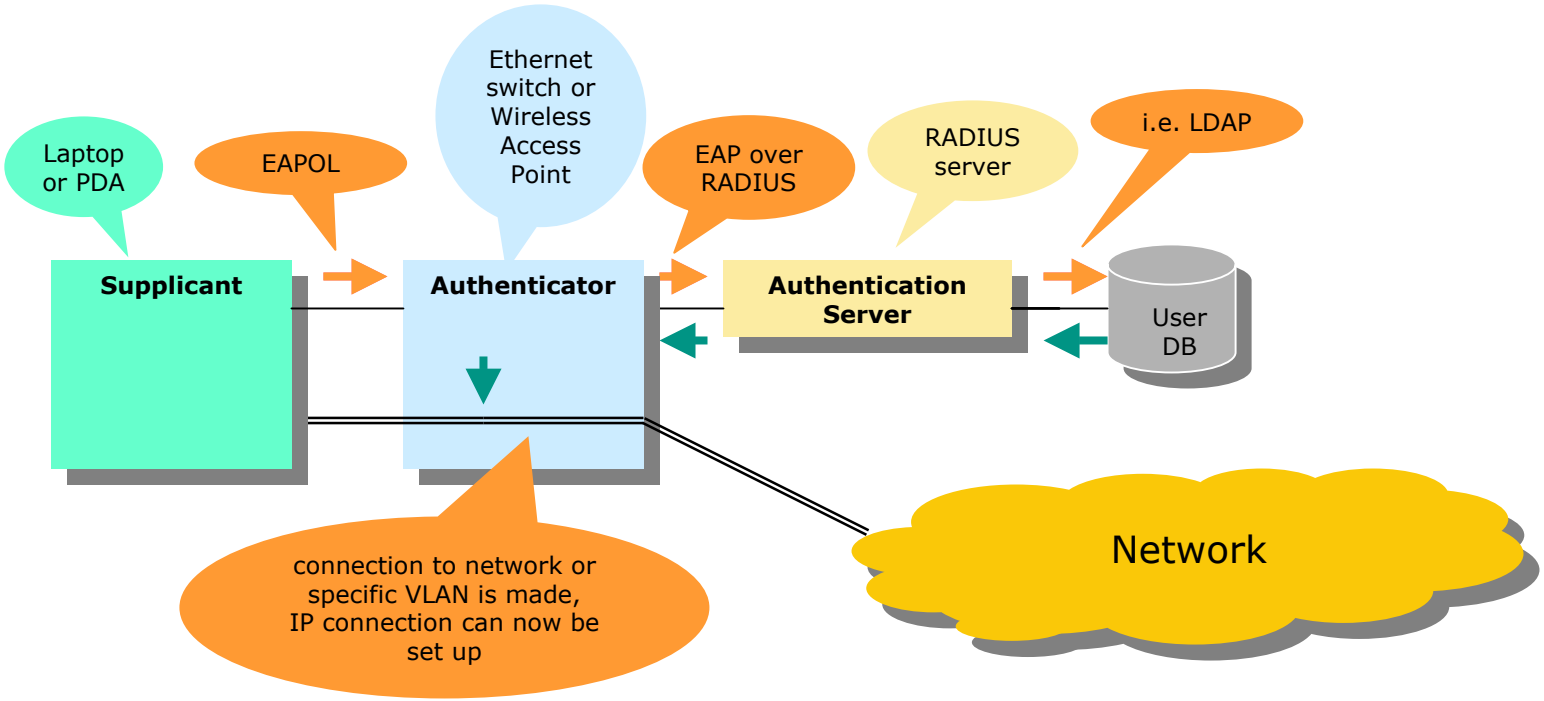
How 802.1X works



signalling

data

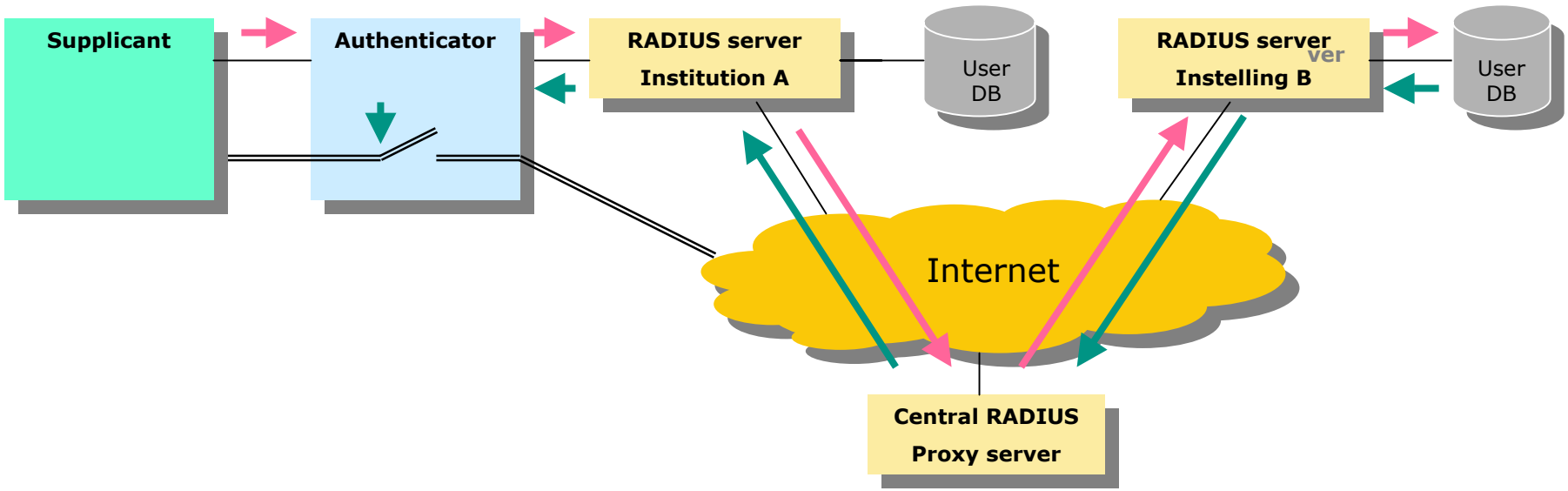
How 802.1X works



Guest usage: RADIUS-proxy

- Institution A only knows its own users (user@institution-a.nl), but trusts certain other institutions (i.e. the SURFnet community).
- To enable guest usage, the institution can transparently forward RADIUS-requests for users not in the database (user@institution-b.nl) to a central RADIUS-proxy, which forwards the request to the right institution. Whatever authentication method is used at institution B can be used in the network of institution A.

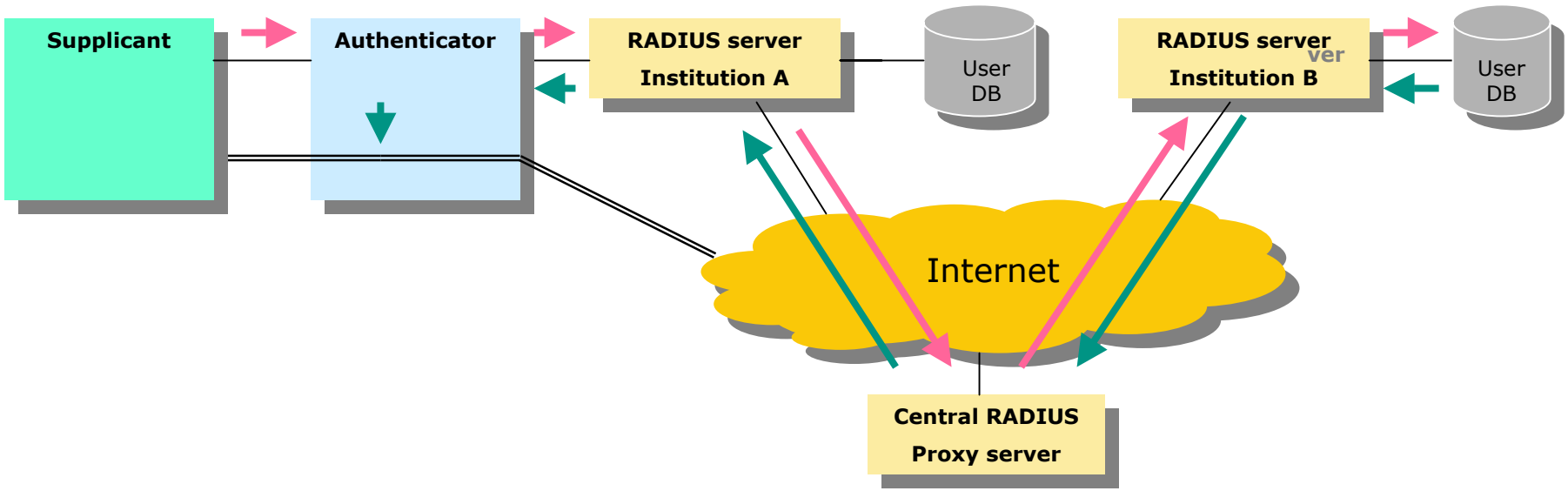
How RADIUS proxiing works



signalling

data

How RADIUS proxiing works



signalling

data

Differences wired vs wireless

- In a wireless environment, no unique, fixed and non-sniffable entry point at the edge of the network can be defined on which authorisation can take place. Therefore a temporary tunnel is necessary between the supplicant and the Access Point (‘Outer authentication’), in which the authentication takes place (‘Inner authentication’).
- A user might see multiple wireless networks. How can he be made aware of this and how will he be able to choose a network?

Status of 802.1X

- 802.1X for ‘fixed’ equipment is widely available
- Web-based access is being used by Telia for access to commercial WLAN
- Web-based systems tend to integrate 802.1x
- German and Swiss research-networks consider VPN-based access
- In the Netherlands, VPN is considered by KUB and TUD, UT has committed to 802.1x doen. RuG, UU, TuD and HvU are interested in 802.1X.
- MS and Cisco are pushing PEAP, ‘competing’ with TTLS (FUNK and Meetinghouse)

More info

802.1x	http://standards.ieee.org/reading/ieee/std/lanman/802.1X-2001.pdf

RFC's: see http://www.ietf-editor.org

EAP	RFC 2284
EAP-MD5	RFC 1994, RFC 2284
EAP-TLS	RFC 2716
EAP-TTLS	http://www.funk.com/NIdx/draft-ietf-pppext-eap-ttls-01.txt
PEAP	http://www.globecom.net/ietf/draft/draft-josefsson-pppext-eap-tls-eap-02.html
RADIUS	RFC 2865, 2866, 2867, 2868, 2869 (I/w EAP)