



# WiTUC – Radius, LDAP, Accounting & DFNRoaming

C. Höfft, Rechenzentrum TU Clausthal  
(Autor: C. Strauf)

DFNRoaming-Workshop (Berlin, 26.04.2007)



# Agenda

- „WiTUC“ - WLAN an der TU Clausthal
- Technik hinter WiTUC
- AAA-Infrastruktur von WiTUC
- Fußangeln bei AAA
- DFNRoaming und eduroam
- Literaturhinweise



# „WiTUC“ - WLAN an der TU Clausthal

# „WiTUC“ - WLAN an der TU Clausthal

- „WiTUC“: Anlehnung an **Wireless TU Clausthal**
- Ziele:
  - Sicherer Zugang für TU-Angehörige
  - Zugang möglichst einfach gestalten (Dokumentation)
  - Nicht flächendeckend (Kosten!) aber an strategisch möglichst günstigen Stellen Hotspots
  - Roaming auch an anderen F&L-Standorten in Deutschland oder sogar in Europa



# Technik hinter WiTUC

# Technik hinter WiTUC

- WLAN-Switch:  
Cisco/Airspace 4402  
Wireless LAN Controller
- Access-Points:  
Cisco/Airspace  
1010/1020
- Management: Cisco  
WCS 4.0



## Technik hinter WiTUC (2)

- Verbindung Thin APs ↔ WLC: Layer3 LWAPP
- Unterstützte Standards: 802.11 a/b/g
- Autorisierung und Authentisierung: 802.1X mit EAP-TTLS + PAP (ausschließlich)
- Verschlüsselung: WPA2+AES bzw. WPA+TKIP (SSIDs „WiTUC“ & „eduroam“), WEP mit Schlüsseltausch über 802.1X (SSID „WiTUC2“)
- Accounting per Betriebsregelung verpflichtend für TU-Angehörige (Sicherung der Ressourcen)

## Technik hinter WiTUC (3)

- Unterstützte Clients (offiziell):
  - Windows mit SecureW2-Supplikant
  - MacOS X 10.4 mit eingebautem Supplikant
- Unterstützte Clients (inoffiziell):
  - Unix-Derivate mit wpa\_supPLICant
  - andere Endgeräte mit EAP-TTLS+PAP-fähigen Supplikanten
- Hotspots: in allen Campus-Teilen identisch konfiguriert (SSIDs „WiTUC“, „eduroam“ & „WiTUC2“)



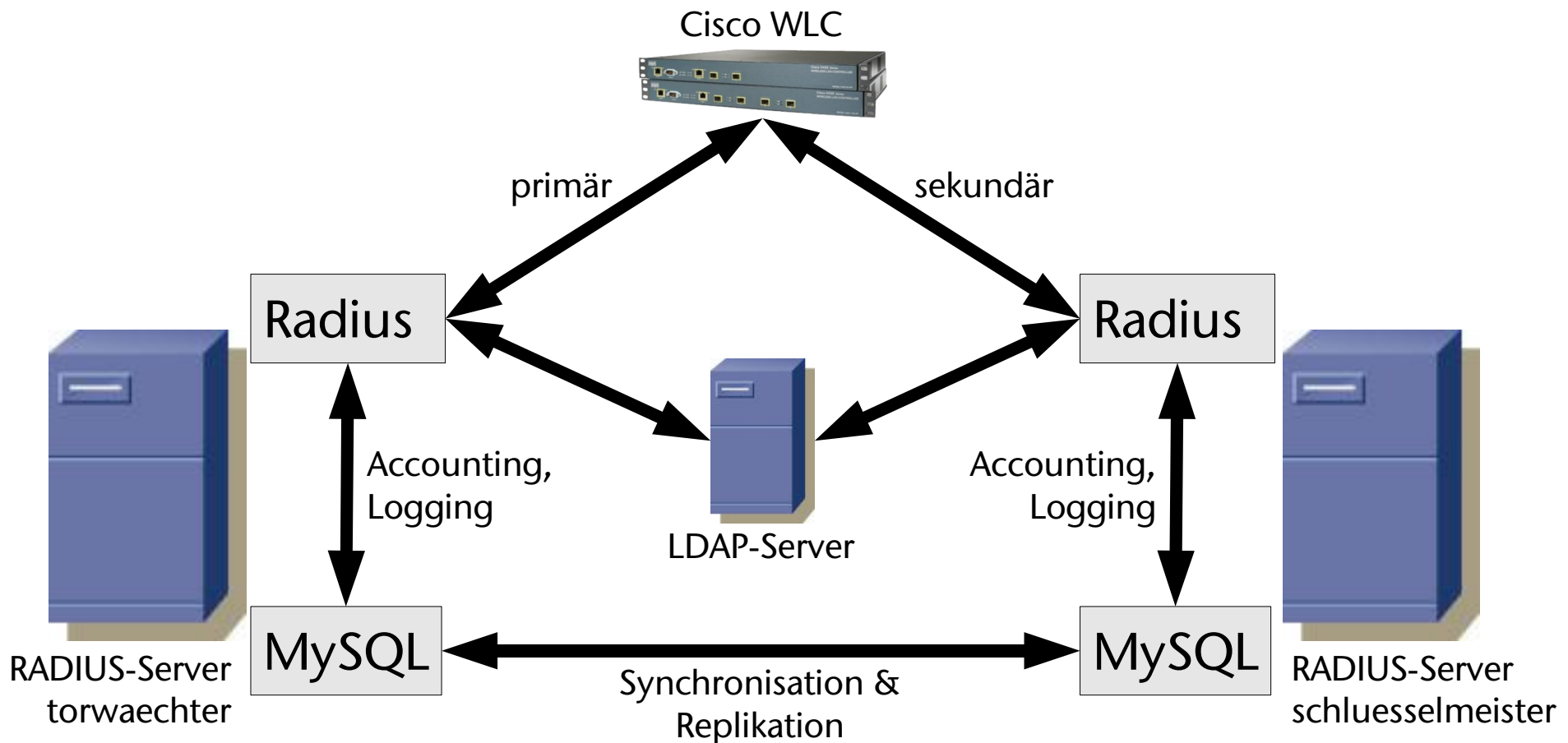
# AAA-Infrastruktur von WiTUC

# AAA-Infrastruktur von WiTUC

- Autorisation, Authentisierung und Accounting (AAA) mit folgender Software unter FreeBSD:
  - FreeRADIUS: Kommunikation zwischen WLC, LDAP, MySQL und DFN-Radius-Proxies
  - OpenLDAP: Nutzerdaten, Radius-Attribute (VLAN, QoS, Traffic-Limit, etc.)
  - MySQL: Accounting-Daten und Login-Daten (werden zu Beginn jeden Monats gelöscht)
- Verwendete Hardware:
  - 2x Dell Poweredge 850

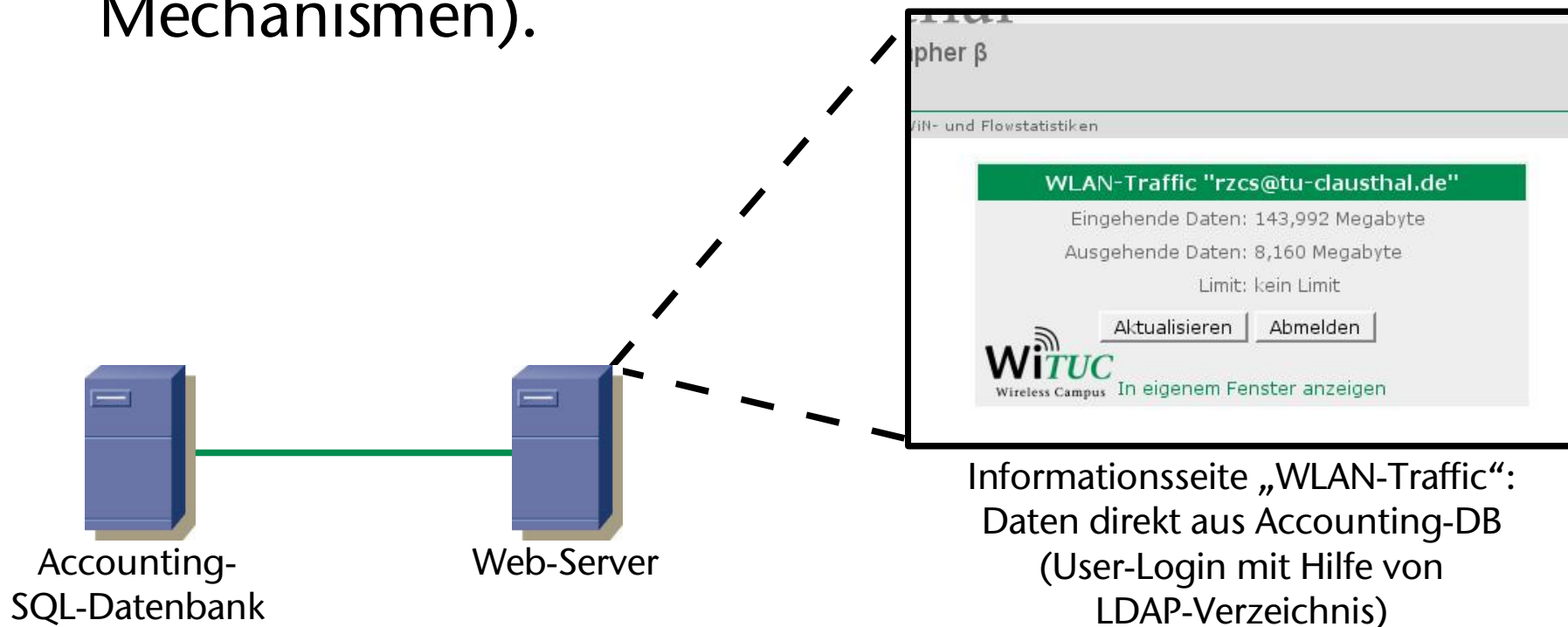
# AAA-Infrastruktur von WiTUC (2)

- Redundanzkonzept Radius:



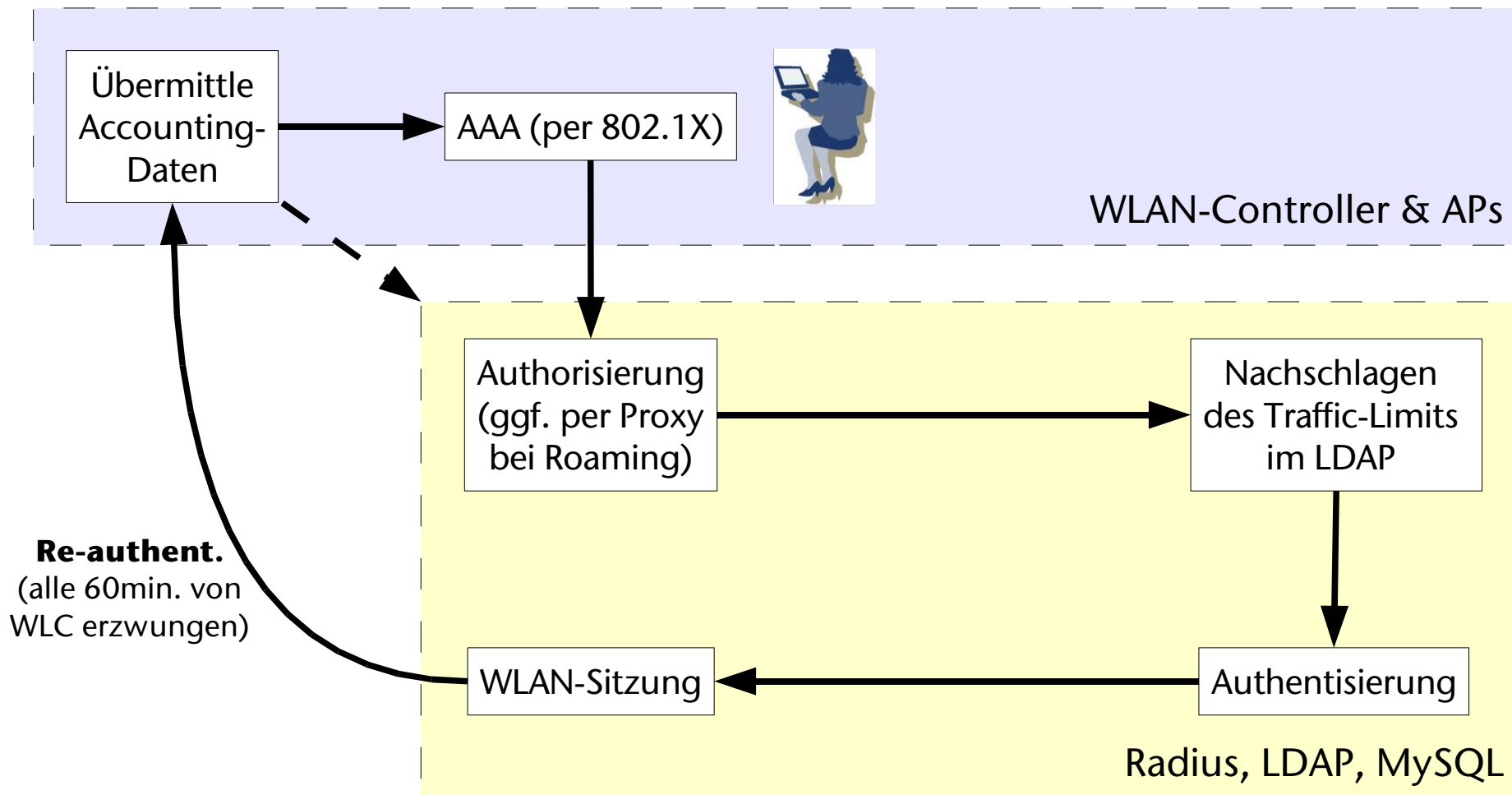
## AAA-Infrastruktur von WiTUC (3)

- Warum Accounting-DB in Form von MySQL?
- Antwort: einfache Anbindung anderer Dienste, einfach realisierbare Redundanz (MySQL-Mechanismen).



# AAA-Infrastruktur von WiTUC (4)

- Ablauf einer Sitzung:



## Warum LDAP?

- LDAP wird bereits als zentrale Benutzerdatenbank gepflegt.
- Sinnvollster Speicherort für benutzer- und/oder gruppenspezifische Konfigurationsdaten
- Nach Erweiterung mit Radius-Schema ist die Speicherung von Radius-Attributen direkt möglich

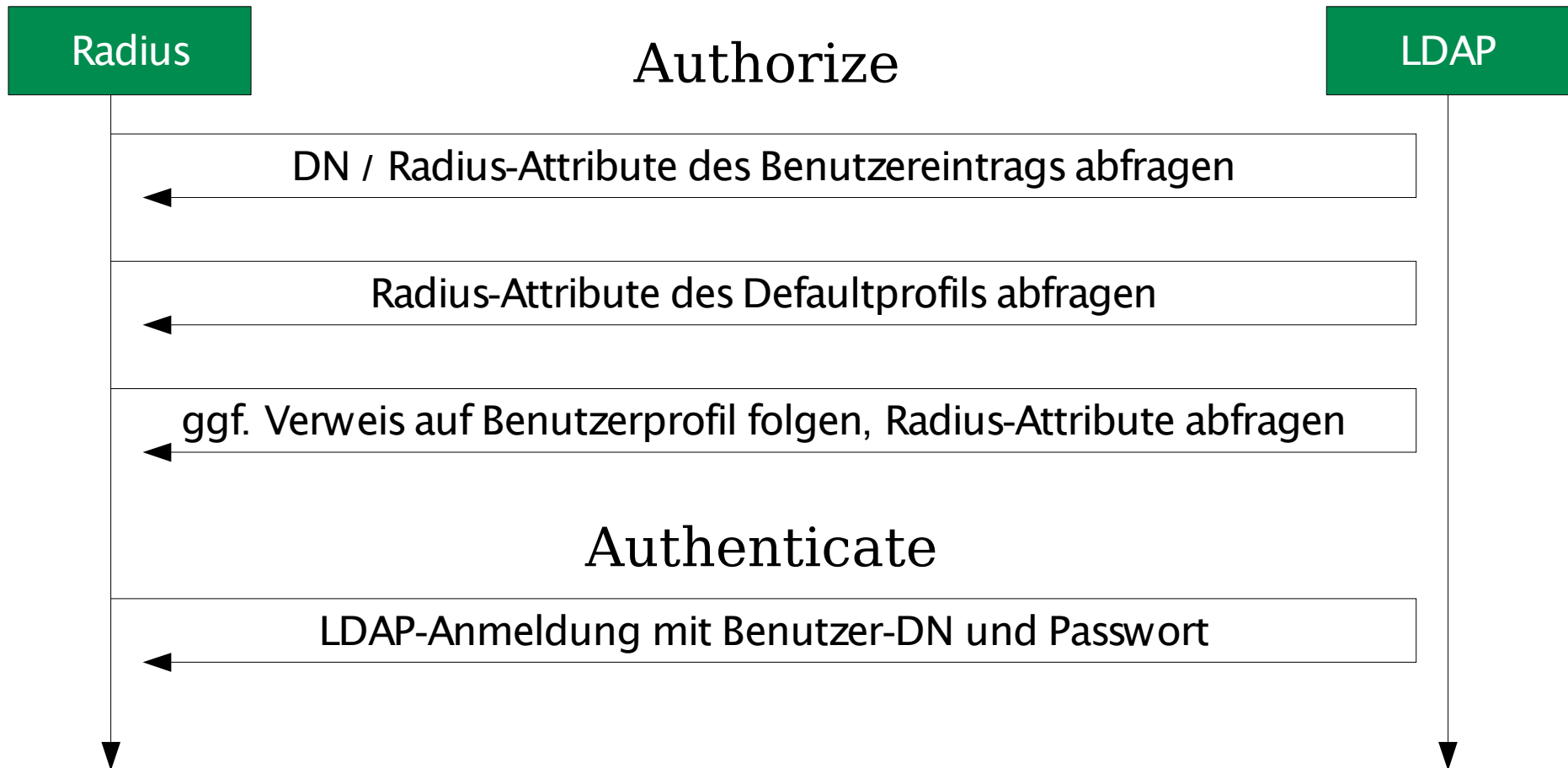
## AAA-Profile im LDAP (1)

- LDAP enthält bereits Benutzerkonten mit Passwortattribut nach dem **inetOrgPerson**-Schema
- Benutzerkonten können einen Verweis auf ein Radiusprofil enthalten (**radiusProfileDN**)
- Radiusprofile stehen in eigener Organisationseinheit.

## AAA-Profilen im LDAP (2)

- In Profilen verwendete Radius-Attribute (am Beispiel „Student“):
  - radiusReplyItem = (setzt Traffic-Limit & QoS)
    - Traffic-Limit := 3221225472
    - Aire-QOS-Level := Bronze
  - radiusTunnelMediumType = IEEE-802 (Ethernet-Verbindung)
  - radiusTunnelType = VLAN (802.1q-„Tunnel“)
  - radiusTunnelPrivateGroupid = 800 (VLAN-ID)
- Durch Verwendung von RFC2868-Attributen (**radiusTunnel\***) wird die VLAN-Konfiguration von vielen Geräten verstanden.

# Ablauf der Benutzeranmeldung



## AAA-Infrastruktur von WiTUC (5)

- Einbindung MySQL: nach Beschreibung in FreeRADIUS-Dokumentation Include von sql.conf
- Benutzung der DB:
  - Accounting-Daten (Start / Stop / Update) werden in DB eingetragen
  - Traffic wird automatisch per SQL aufsummiert
  - Perl-Modul in FreeRADIUS (Skript von RZ-TUC erstellt) liest bei Autorisierung Traffic-Limit aus LDAP aus und prüft, dass Volumina in DB das Traffic-Limit nicht überschreiten (ansonsten Reject!)

## AAA-Infrastruktur von WiTUC (6)

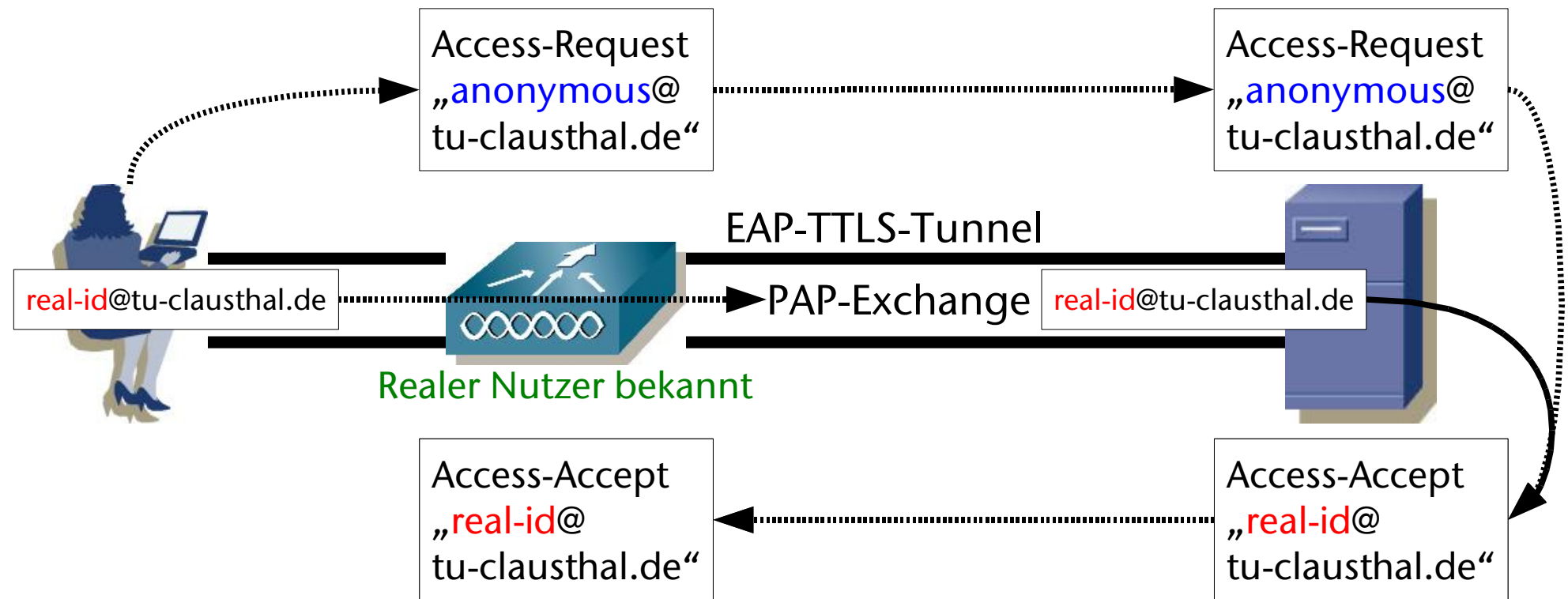
- Accounting an der TUC:
  - Accounting-Daten werden am ersten jeden Monats gelöscht
  - Sessions sind auf Cisco WLC auf 60min. eingestellt, danach erfolgt (für den Nutzer transparente) Re-authentisierung, um „frische“ Accounting-Daten zu erhalten und Limit zu forcieren



# Fußregeln bei AAA

# Fußangeln bei AAA

- Radius-Accounting bei EAP-TTLS+PAP: Username in Access-Accept-Message kopieren, realer Nutzer sonst unbekannt!



## Fußregeln bei AAA (2)

- FreeRADIUS-Einstellungen, um innere Identität in Access-Accept zu kopieren:

### eap.conf:

```
...
    ttls {
        ...
        use_tunneled_reply = yes
        ...
    }
...
```

### users-File:

```
...
DEFAULT Realm == tu-clausthal.de, Freeradius-Proxyed-To == 127.0.0.1
    User-Name == "%{User-Name}",
    Fall-Through = yes
...
```

## Fußangeln bei AAA (3)

- X.509-Zertifikate für Radius-Server bei EAP-TTLS:
  - Selbst signierte Zertifikate führen zu *erheblichen* Sicherheitsproblemen (Spoofing von Hotspots und des Radius-Servers, Abhören von Nutzerdaten)!
  - Von CA signierte Zertifikate verwenden; folgende Optionen existieren:
    - Von DFN-CA signierte Zertifikate verwenden
    - Von kommerzieller CA signierte Zertifikate verwenden
  - Bei SecureW2 (Windows) und MacOS X lassen sich Root-Zertifikate von DFN-CA sehr leicht (teilweise automatisch – Stichwort „INF-Datei“) importieren

## Fußregeln bei AAA (3)

- Passwortprüfung bei verschiedenen EAP-Typen:
  - Fast alle Methoden (mit Ausnahme von PAP und – über Umwege – MSCHAPv2) erfordern Klartextpasswörter im LDAP oder im users-File des Radius-Servers
  - Möglichkeiten für PAP: beliebig, PAP überträgt Klartextpasswörter die vom Radius-Server im richtigen Format gehasht werden können
  - MSCHAPv2: Passwörter können als LAN-Manager-Hash vorliegen (klartextäquivalent)



# DFNRoaming und eduroam

# DFNRoaming und eduroam

- Problem: wie bekommen Gäste Zugang zum lokalen WLAN?
- Antwort: über ein systematisch organisiertes Roaming (Stichwort: Radius-Proxies)!
- TUC ist an DFNRoaming angeschlossen, der DFN-Verein wiederum nimmt am „eduroam“-Projekt teil  
⇒ europaweites Roaming möglich



## DFNRoaming und eduroam (2)

- Wichtige Voraussetzungen für DFNRoaming:
  - Äußere EAP-Identitäten müssen sog. „Realms“ enthalten (z.B. „@tu-clausthal.de“), damit „Heimat-Radius-Server“ des Benutzers bekannt ist
  - Auf lokalem Radius-Server:
    - Authentisiere lokalen Realm / Null-Realm selbst
    - Leite Anfragen mit unbekanntem Realms (z.B. „@uninett.no“ aus Norwegen) als Proxy an hierarchisch übergeordneten Radius (DFN-Radius-Server) weiter

## DFNRoaming und eduroam (3)

- Zu erledigende Arbeitsschritte zur Teilnahme an DFNRoaming/eduroam:
  - Kontakt mit Herrn Paffrath (DFN) aufnehmen
  - Radius-Konfiguration anpassen
  - Tests durchführen, ob Radius-Proxying funktioniert
  - Anpassung der lokalen Dokumentation für die Benutzer
- TU Clausthal testete Roaming mit Hilfe von K. Barmen von UNINETT in Norwegen

# DFNRoaming und eduroam (4)

- FreeRADIUS-Einträge (Proxying einschalten!):

```
proxy.conf:
...
#
# Eintraege fuer das DFN-Roaming
#
realm DEFAULT {
    type                = radius
    authhost            = radius1.dfn.de:1812
    accthost            = radius1.dfn.de:1813
    secret              = XXXXXXXXXXXXXXXXXXXX
    nostrip
}

realm DEFAULT {
    type                = radius
    authhost            = radius2.dfn.de:1812
    accthost            = radius2.dfn.de:1813
    secret              = XXXXXXXXXXXXXXXXXXXX
    nostrip
}...
```

## DFNRoaming und eduroam (5)

- DFN-Radius-Server in FreeRADIUS als Clients bekannt machen:

### clients.conf:

```
...
client radius1.dfn.de {
    secret          = XXXXXXXXXXXXXXXXXXXX
    shortname       = top-level-radius1
    nastype        = other
}

client radius2.dfn.de {
    secret          = XXXXXXXXXXXXXXXXXXXX
    shortname       = top-level-radius2
    nastype        = other
} ...
```

## DFNRoaming und eduroam (6)

- Zur korrekten Behandlung von Roaming-Identitäten („anonymous@einrichtung.de“) folgende Einträge in FreeRADIUS machen:

### users-File:

```
...  
DEFAULT User-Name == "^[Aa][Nn][Oo][Nn][Yy][Mm][Oo][Uu][Ss]$"
Auth-Type := Reject  
  
DEFAULT User-Name == "^[Aa][Nn][Oo][Nn][Yy][Mm][Oo][Uu][Ss]@.*$"
Auth-Type := EAP  
  
DEFAULT Realm == NULL, Auth-Type := Reject  
...
```

## DFNRoaming und eduroam (7)

- **Wichtig:** Radius-Attribute fremder Radius-Server filtern, sonst mögliche Sicherheitsprobleme:
  - In radiusd.conf im „post-proxy“-Abschnitt den „attr\_filter“ einbinden
  - „attrs“-File wie folgt anpassen:

### attrs-File:

```
...  
DEFAULT  
    EAP-Message =* ANY,  
    Message-Authenticator =* ANY,  
    User-Name =~ ".+",  
    Reply-Message =* ANY,  
    MS-MPPE-Recv-Key =* ANY,  
    MS-MPPE-Send-Key =* ANY,  
    State =* ANY
```

# Literaturhinweise

- [http://wiki.freeradius.org/Main\\_Page](http://wiki.freeradius.org/Main_Page) – Doku zu FreeRADIUS
- <http://www.ietf.org/rfc/rfc2868.txt?number=2868> – Dokumentation der IETF-Attribute zum Übermitteln von VLAN-Zuordnungen
- <http://dev.mysql.com/doc/refman/5.1/de/replication-howto.html> – Dokumentation der automatischen MySQL-Replikation (für redundante Accounting-Datenbank)
- `doc/examples/openldap.schema` im FreeRADIUS-Tarball – Dokumentation des Radius-Schemas für OpenLDAP
- <http://www.rz.tu-clausthal.de/wituc/> – Dokumentation des WLAN der TU Clausthal
- <http://www.dfn.de/content/dienstleistungen/dfnroaming/> – DFN-Seite zum DFN-Roaming
- <http://www.eduroam.org> – Seite des eduroam-Projektes



Vielen Dank für Ihre Aufmerksamkeit!



**TU Clausthal**

**Christian Höfft**  
Rechenzentrum

Erzstraße 51  
D-38678 Clausthal-Zellerfeld

Telefon: (5323) 72-2007  
Telefax: (5323) 72-3536

E-Mail: [hoefft@rz.tu-clausthal.de](mailto:hoefft@rz.tu-clausthal.de)  
URL: <http://www.rz.tu-clausthal.de>