



WiTUC - LDAP

C. Marg, Rechenzentrum TU Clausthal

DFNRoaming-Workshop (Stuttgart, 30.11.2006)



Inhalt

- Warum LDAP?
- AAA-Profile im LDAP
- Ablauf der Benutzeranmeldung
- Ausblick

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

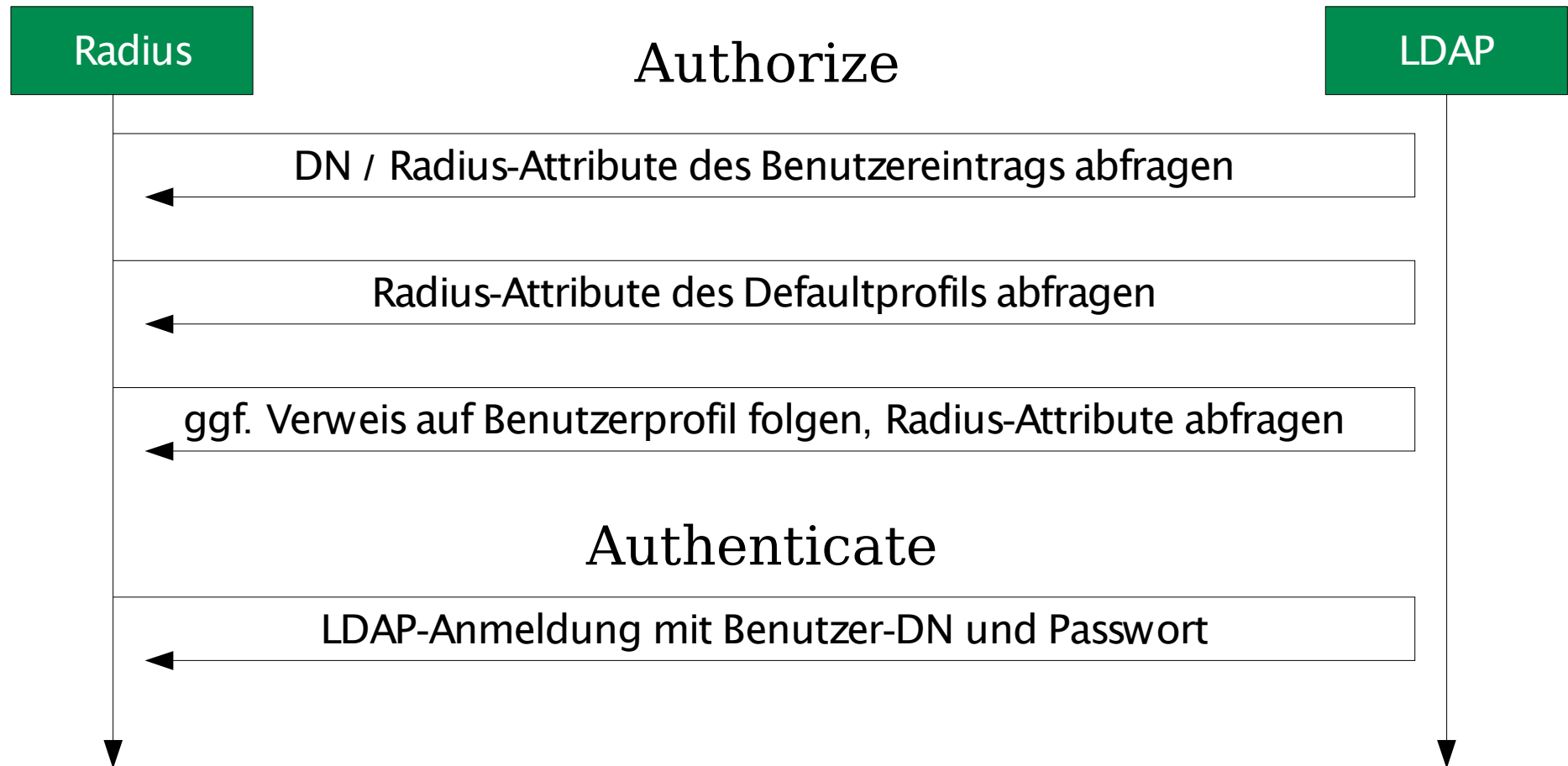
AAA-Profile im LDAP (1)

- 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)
 - radiusTunnelPrivateGroupId = 800 (VLAN-ID)
 - radiusTunnelType = VLAN (802.1q-„Tunnel“)
- Durch Verwendung von RFC2868-Attributen (**radiusTunnel***) wird die VLAN-Konfiguration von vielen Geräten verstanden.

Ablauf der Benutzeranmeldung



Ausblick

- Anschluss weiterer Geräte (VPN-Server, Wired 802.1x) an den RADIUS-Server
- Überarbeitung des Konzepts, um weitere Geräte mit spezifischen Radius-Attributen versorgen zu können
- Überlegungen bzgl. weiterer EAP-Typen



Vielen Dank für Ihre Aufmerksamkeit!



TU Clausthal

Christian Marg
Rechenzentrum

Erzstraße 51
D-38678 Clausthal-Zellerfeld

Telefon: (5323) 72-2043
Telefax: (5323) 72-3536

E-Mail: marg@rz.tu-clausthal.de
URL: <http://www.rz.tu-clausthal.de>