EDUCATION ROAMING

Freier WLAN-Zugang für Uni-Angehörige im eduroam-Verbund

Seit Oktober 2005 ist das österreichische Wissenschaftsnetz ACOnet Teil des eduroam-Verbundes. eduroam steht für *Education Roaming*; es handelt sich dabei um ein Projekt von TERENA (dem Dachverband der europäischen Wissenschaftsnetze, siehe `www.terena.nl`), das es den Angehörigen der angeschlossenen Institutionen ermöglicht, sich mit den Zugangsdaten ihres Heimat-Netzwerks auch im WLAN (*Wireless Local Area Network*) einer anderen teilnehmenden Einrichtung anzumelden. Das bedeutet, dass z.B. Angehörige der Uni Wien mit ihrer Unet- bzw. Mailbox-UserID den Internetzugang an Bildungs- und Forschungseinrichtungen in derzeit 21 europäischen Staaten sowie in Australien und Taiwan nutzen können.

Alle Informationen zum eduroam-Projekt – auch eine Liste aller teilnehmenden nationalen Wissenschaftsnetze – erhalten Sie unter `www.eduroam.org`. Eine Übersichtsseite der beteiligten österreichischen Institutionen ist unter `www.aco.net/eduroam/` im Entstehen. Auf der Webseite `http://eduroam.univie.ac.at/` finden Sie die Zugangsmöglichkeiten (d.h. die Standorte der *Public Network Services*) im Bereich der Universität Wien.

Die Überprüfung der Zugangsberechtigungen innerhalb von eduroam erfolgt über hierarchisch organisierte Server, wobei die von TERENA betriebenen Toplevel-Server die Anfragen an die Authentifizierungsserver der teilnehmenden nationalen Netzbetreiber weiterleiten. Diese wiederum verteilen die Anfragen an die zuständigen Server der jeweiligen Mitgliedsinstitutionen. Zu beachten ist, dass die eduroam-Infrastruktur nur dann genutzt werden kann, wenn das Heimat- und das Gastgeber-Netzwerk dieselbe(n) Zugangstechnologie(n) unterstützen.

Die Nutzung von eduroam wird für drei verschiedene Zugangstechnologien ermöglicht:

- **802.1X** – ein Standard-Protokoll zur Authentifizierung in Funknetzen
- **Captive Portal** – Authentifizierung über eine Webseite, zu der jede Anfrage umgeleitet wird
- **VPN** (*Virtual Private Network*) – Verbindung zum heimischen VPN-Gateway ➠

An der Universität Wien existiert derzeit erst der Zugang über 802.1X; die SSID[1] dieses Netzes ist `eduroam`. Die Zugänge über Captive Portal und VPN werden in naher Zukunft folgen.

Kurt Bauer ■

1) Als *Service Set Identifier* (SSID) bezeichnet man die Kennung eines Funknetzwerks: Jedes Wireless LAN, das auf IEEE 802.11 basiert, besitzt eine konfigurierbare SSID oder ESSID (*Extended Service Set Identifier*), um das Funknetz eindeutig identifizieren zu können. Die SSID stellt also den Namen des Netzes dar und wird daher auch *Network Name* genannt.

DATENTANKSTELLE802.1X

Ein verschlüsseltes Funknetz für die Uni Wien

Parallel zur eduroam-Vernetzung (siehe Seite 53) wurde unter dem Namen *Datentankstelle802.1X* an der Universität Wien ein eigenes, sicheres Funknetz realisiert, dessen Zugangsmöglichkeiten unter `www.univie.ac.at/ZID/pns-standorte/` aufgelistet sind.

Es bietet 128 Bit-WEP-Verschlüsselung, wodurch Mithören sowie andere Attacken deutlich erschwert bzw. unmöglich gemacht werden. Die Authentifizierung erfolgt nicht mehr wie bei den „normalen" Datentankstellen über eine Webseite (Captive Portal), sondern wird direkt beim Verbindungsaufbau über das 802.1X-Protokoll durchgeführt. Benutzername und Passwort werden dabei in einem verschlüsselten Tunnel zum RADIUS-Server der Universität Wien übertragen (Näheres siehe Kasten *802.1X – Technischer Hintergrund*). Neben der Verschlüsselung bietet das 802.1X-Protokoll noch einen weiteren Vorteil: Da das Zugangspasswort gecacht bzw. auf dem Rechner abgespeichert werden kann, müssen die Login-Daten nicht mehr bei jedem Verbindungsaufbau eingegeben werden. Durch das Passwort-Caching wird die Verbindung zudem automatisch wiederhergestellt, wenn der Computer aus dem Ruhezustand wieder „aufgeweckt" wird.

Viele aktuelle Betriebssysteme – z.B. Windows XP SP2 oder Mac OS X 10.4 – unterstützen 802.1X nativ, d.h. man braucht keine zusätzliche Software von Drittanbietern. Sofern das verwendete System keine solche Unterstützung bietet, können diverse 802.1X-Klientenprogramme diese Funktionalität übernehmen:

- *Xsupplicant* (`http://open1x.sourceforge.net/`): kostenloser Open Source-Klient für Linux
- *Odyssey* (`www.funk.com`): kostenpflichtiger Windows-Klient, als Trial-Version erhältlich
- *Aegis* (`www.mtghouse.com`): kostenpflichtiger Klient für Windows, Mac OS X, Solaris, RedHat etc., als Trial-Version erhältlich

Die benötigten Zugangsdaten sind die eigene eMail-Adresse in der Form

- *`Mailbox-UserID`*`@univie.ac.at` (z.B. `musterm9@univie.ac.at`) für Uni-MitarbeiterInnen bzw.
- a*`Matrikelnummer`*`@unet.univie.ac.at` (z.B. `a1234567@unet.univie.ac.at`) für Studierende

sowie das dazugehörige, selbst gewählte Passwort.

Genaue Anleitungen für die Konfiguration des Zugangs zur Datentankstelle802.1X unter Windows XP bzw. unter Mac OS X sind unter dem URL `www.univie.ac.at/ZID/anleitungen/` zu finden.

Daniel Schirmer ■

802.1X – Technischer Hintergrund

Für technisch Interessierte bzw. als Hilfe zum Selbstkonfigurieren (z.B. für Linux): 802.1X basiert auf dem Client-Server-Protokoll RADIUS (*Remote Authentication Dial-In User Service*), welches zur Authentifizierung und Autorisierung von BenutzerInnen bei Einwahlverbindungen, beispielsweise über WLAN, in Computernetzwerke dient.

802.1X (bzw. RADIUS) verwendet diverse EAP-Methoden (*Extensible Authentication Protocol*). An der Universität Wien werden drei davon angeboten:

- PEAP (*Protected EAP*) – sicherer Tunnel, wird als einziges Verfahren von Windows unterstützt
- TTLS (*Tunneled Transport Layer Security*) – ähnlich PEAP
- LEAP (*Lightweight EAP*) – nicht so sicher, sollte nur verwendet werden, wenn kein anderes Verfahren möglich ist

Über eines dieser Verfahren wird die mittels MS-CHAPv2 kryptisierte Benutzername-/Passwort-Kombination übertragen. Andere Verschlüsselungstypen (z.B. TLS, MD5) bzw. Benutzerdaten-Verschlüsselungen wie MS-CHAP sowie Klartext-Passworte werden derzeit nicht unterstützt.