LANCOM™ Techpaper

802.1x

1 Einleitung

In diesem Techpaper wird die Nutzung von 802.1x für eine Zugangskontrolle und als erweiterte Sicherheitsfunktion in Wireless LANs vorgestellt. Neben 802.1x werden die Begriffe RADIUS und EAP erläutert. Den Abschluss bildet eine Installationsanleitung zum Aufbau eines hochsicheren WLANs mit Hilfe von 802.1x am Beispiel eines Funk Odyssey EAP/RADIUS-Servers mit LANCOM Access Points und AirLancer WLAN-Client-Adaptern. Dabei kommen die WLAN-Verschlüsselungstechniken WEP, WPA/TKIP und 802.11i jeweils in Verbindung mit 802.1x zum Einsatz.

2 Allgemeines zu EAP/802.1x

2.1 Die Geschichte von 802.1x

Die Idee zu 802.1x kam von Institutionen, die den Zugang zu öffentlichen Netzwerken einfach kontrollieren wollten (Universitäten, Behörden, Bibliotheken etc.).

Die gewünschte Lösung sollte kostengünstig und einfach zu implementieren sein. Dabei sollte die bestehende Netzwerk-Infrastruktur ebenso wie etablierte Protokolle verwendet werden. VPN erfüllte zwar einige der Voraussetzungen, schied aber als generelle Lösung aufgrund der hohen Ressourcen-Anforderungen und der komplexen Konfiguration aus.

Das Konzept für 802.1x wurde schließlich gemeinsam von 3Com, HP, und Microsoft entwickelt und im Juni 2001 als IEEE Standard verabschiedet. Das Modell wurde ursprünglich für Switches entwickelt (802.1d) und erst später für 802.11 erweitert.

2.2 Die Philosophie von 802.1x

Der IEEE-802.1x-Standard stellt eine wichtige Weiterentwicklung im Sicherheitskonzept für Netzwerke dar und bietet eine Möglichkeit, schon an einem Netzwerkzugangsport eine Benutzeridentifizierung vornehmen zu können. Damit werden folgende Funktionen realisiert:

- Zugangskontrolle (benutzerorientiertes Regelsystem)
- Abrechnung (Billing & Accounting)
- Bandbreitenzuweisung (QoS pro User)
- Anlegen von Benutzerprofilen (User Personalized Network, UPN)

Mit der Funktion „Single-Sign-On" können sich die Benutzer mit einer einzigen, primären Authentifizierung an verschiedenen Systemen und Anwendungen gleichzeitig anmelden, z.B. bei Einwahlservern, Firewalls, VPNs oder Wireless LANs. Dabei erfolgt die Authentifizierung des Benutzers einmalig an einem zentralen sog. RADIUS-Server.

2.3 Allgemeines über RADIUS

Alle Provider, die eine Einwahl in ein Netzwerk ermöglichen, stehen vor einem grossen Problem. Sie bieten z.B. einer Vielzahl von Benutzern an verschiedenen Orten Zugang zum Internet. Zur Gewährleistung der Sicherheit muss genauestens geprüft werden, wer Zugang zum Netzwerk bekommt, um gleich von Vornherein einen Missbrauch der Serverdienste auszuschliessen. Desweiteren benötigen die Provider möglicherweise Mechanismen, die ihnen eine Erfassung und Berechnung der Onlinezeiten für die Benutzer ermöglichen. Deshalb braucht man ein leistungsfähiges System, das die folgenden Aufgaben zentral übernehmen kann:

- Authentisierung
- Autorisierung
- Accounting

Diese Aufgabenstellungen löst der **R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice, kurz RADIUS. RADIUS ist in RFC 2865 spezifiziert und kommuniziert über UDP-Port 1812. Ein Network Access Server (NAS) fungiert als Client des RADIUS-Servers. Ein RADIUS-Server kann auch als Proxy für andere RADIUS-Server oder auch andere Arten von Authentifizierungsservern dienen. Die Kommunikation zwischen dem RADIUS-Client und -Server wird dadurch gesichert, dass sich beide Kommunikationspartner gegenseitig durch ein „Shared Secret" authentifizieren und den Datentransfer verschlüsseln können. RADIUS unterstützt eine Vielzahl von Authentifizierungsmöglichkeiten wie zum Beispiel PAP, CHAP, EAP oder UNIX-Login. RADIUS kann viele erweiterbare Attribute zu einem Benutzer verarbeiten und übermitteln (Beispiel in Abb 2.1).

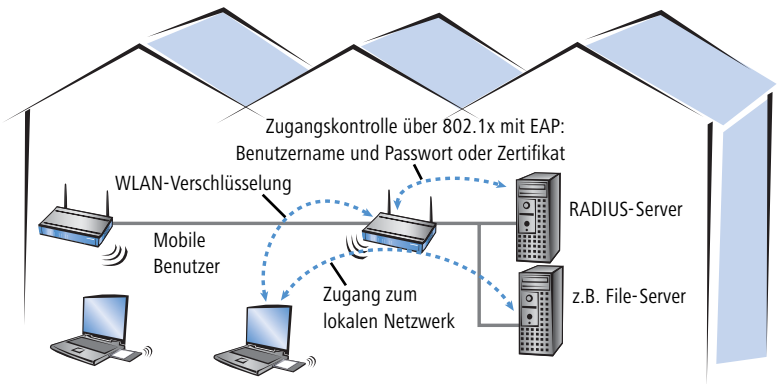

Abb. 2.1: EAP-Benutzerauthentifizierung mit 802.1x in einem WLAN

LANCOM
Systems

2.4 Das Extensible Authentication Protokoll (EAP)

EAP wurde ursprünglich für PPP entwickelt, und ist in den RFCs 2284 und 2716 spezifiziert. Mit Hilfe von EAP können zwei Kommunikationspartner vor der eigentlichen Authentifizierung aushandeln, welche Authentifizierungsmethode angewandt werden soll. Aufgrund der Ausführung als Application Programming Interface werden auch zukünftig entwickelte Authentisierungsprotokolle auf EAP aufsetzen können.

EAP beschreibt in einem einfachen Request-Response-Verfahren den Austausch der Authentifizierungsdaten vom Benutzer zum Authentisierungsserver und dessen Antwort. Dabei können beliebige Authentifizierungsmechanismen wie Kerberos, SecurI oder Zertifikate benutzt werden.

EAP wird entweder in Verbindung mit PPP verwendet oder als Protokoll-Framework zum Authentifizierungsdatenaustausch in anderen Protokollen, so etwa auch in IEEE 802.1x. Für die Anwendung von EAP über 802.1x werden die Authentifizierungsdaten mittels EAPoL (Extensible Authentication Protocol over LAN) oder im Fall von Wireless entsprechend EAPoW übertragen.

2.5 Wie funktioniert EAP?

Das EAP fordert den Benutzer auf, sich zu authentifizieren. Diese Authentisierungsinformationen werden zunächst an den Port bzw. den Authenticator weitergeleitet. Sobald der Authenticator diese Daten empfangen hat, leitet er sie an einen AAA-Server (Authentication, Authorization and Accounting), im Normalfall einen RADIUS-Server weiter. Anhand der hinterlegten Benutzerprofile authentifiziert der RADIUS-Server den User, d.h. er entscheidet, ob der User Zugriff auf die angefragten Services erhält oder nicht. In einigen Fällen übernimmt der RADIUS-Server die Authentifizierung nicht selbst, sondern leitet die Daten an eine weitere Authentifizierungseinheit weiter, im Normalfall an einen Verzeichnisdienst (LDAP-Server, Directory Server). Im Falle einer nicht erfolgreichen Authentifizierung erhält der Authenticator eine entsprechende Information, die dafür sorgt, dass der Port nicht aktiviert wird (d.h. den Modus Authentication on/Port off einnimmt) beziehungsweise das Standard Systemverhalten beibehält (Authentication on/Port on with default policy). In beiden Fällen erhält der Benutzer keinen Zugriff auf die angefragten Services. Wenn die Authentifizierung erfolgreich verläuft, wird die Erfolgsmeldung, die der RADIUS-Server an den Switch zurücksendet, mit der Funktionsbezeichnung „RADIUS/EAP Success“ versehen. Der Authenticator schaltet danach sofort den entsprechenden Port für den uneingeschränkten Datentransport frei.

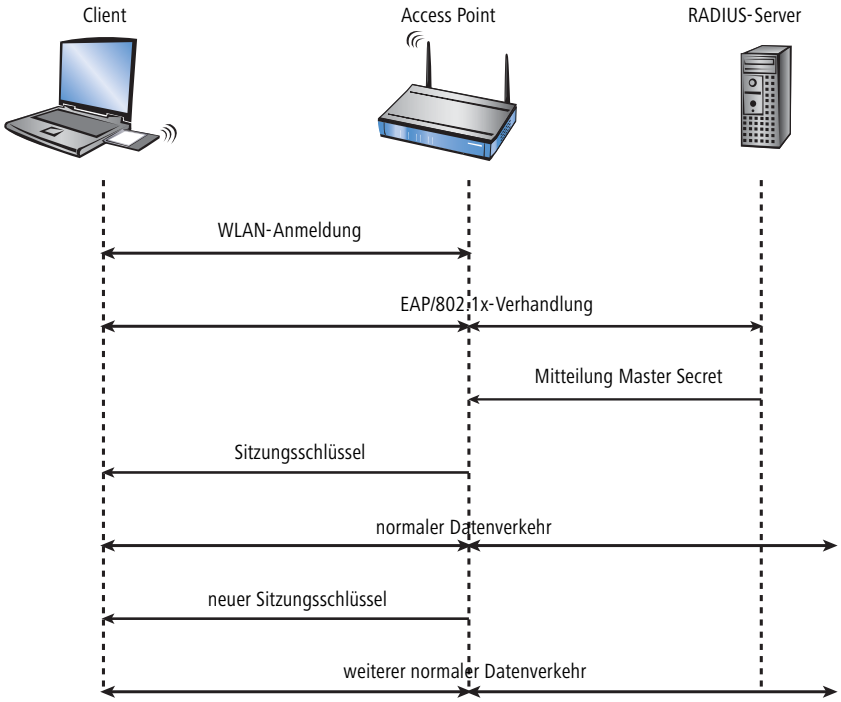

Abbildung 2.2: Schematischer Ablauf einer WLAN-Sitzung mit EAP/802.1x

2.6 EAP-TLS und EAP-TTLS

EAP-TLS (Authentifizierung durch gegenseitige Zertifikate)

Das EAP-Transport Layer Security Protokoll (eine Kombination von EAP mit SSL) verlangt eine gegenseitige zertifikatbasierte Authentisierung des Servers und des Clients auf der Transportschicht. Aktuell sind frei erhältliche Clients für EAP-TLS nur für LINUX (z.B. Open1x) und Windows XP (integriert) erhältlich. Für alle anderen Client-Betriebssysteme muss z. Zt. ein EAP-TLS Client extra lizenziert werden.

Als Vorteil von EAP-TLS kann man die Favorisierung durch Microsoft und die Integration in Windows XP sehen – die notwendige gegenseitige, zertifikatbasierende Authentisierung spricht allerdings gegen dieses Verfahren.

EAP-TTLS (Authentifizierung durch Username / Passwort und Server-Zertifikat)

Das EAP-Tunneled Transport Layer Security Protokoll erweitert EAP-TLS durch eine sehr praktische Funktion. Bevor sich der Benutzer gegenüber dem Server authentisieren muss, wird mit dem Serverzertifikat ein sicherer TLS-Tunnel zwischen WLAN-Client und Authentisierungsserver dynamisch aufgebaut. In diesem sicheren Tunnel kann sich dann der Benutzer beim Authentisierungsserver mittels Username/Passwort identifizieren. Damit entfällt die eher umständliche Notwendigkeit eines Benutzerzertifikats. Es werden – wie bei SSL (TLS) Authentisierungen über das Internet üblich – nur noch serverseitige Zertifikate zur gegenseitigen Authentisierung des Benutzers und des Servers zwingend benötigt. Das EAP-TTLS-Verfahren ist damit einfacher als EAP-TLS, da nur serverseitige Zertifikate notwendig sind.

3 Konfiguration des LANCOM Access-Points

- 802.1x mit 802.11i steht für alle WLAN-Produkten von LANCOM Systems zur Verfügung, die den Standard 802.11a oder 802.11g unterstützen
- Die Einstellungen, die für 802.1x und für 802.11i bzw. WPA eine Rolle spielen, befinden sich unter dem Unterpunkt **WLAN-Sicherheit**.
- Bei IEEE 802.1x wird die Funktion von 802.1x für den Access-Point aktiviert und dort die entsprechende RADIUS-IP, den Port (Standard-Port 1812) und das Shared Secret für die Kommunikation zwischen RADIUS und Access-Point angeben. (Abb. 3.1)

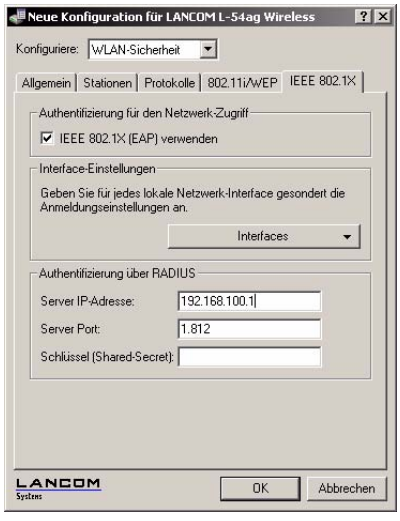

Abb. 3.1

- Für das entsprechende Interface muss man zusätzlich noch einstellen, das eine Anmeldung erforderlich ist und in welchen Zeitintervallen die Anmeldung wiederholt bzw. der Schlüssel erneuert wird. (Abb. 3.2)

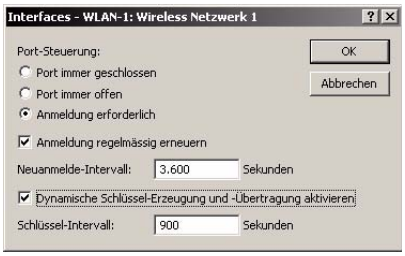

Abb. 3.2

- Bei 802.11i/WEP wird die Verschlüsselung wie in den folgenden beiden Abbildungen (Abb. 3.3 und Abb 3.4) eingestellt, wie in diesem Fall für WPA mit AES (alternativ TKIP)

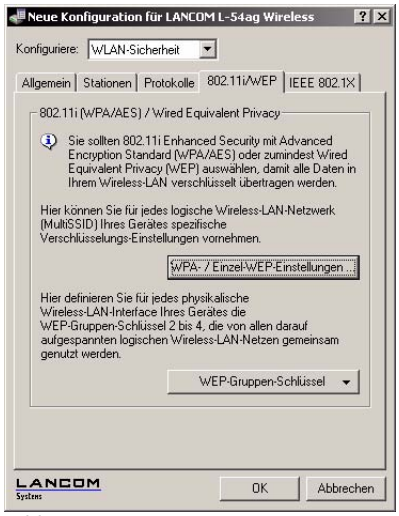

Abb. 3.3

Abb. 3.4

4 Beispiel-Szenario für 802.11i mit 802.1x/EAP-TTLS

Mittlerweile sind verschiedene RADIUS-Server mit 802.1x/EAP-Unterstützung auf dem Markt verfügbar. Hierbei reicht die Palette vom komplexen Kommandozeilentool bis hin zu benutzerfreundlicheren Servern mit eigener Konfigurations-GUI. Die Möglichkeit, einen RADIUS mit Microsoft-Servern aufzusetzen, wird aufgrund hoher Komplexität und Umständlichkeit meistens gemieden. Der Odyssey-Server bzw. Client des Entwicklers Funk (www.funk.com) ist eine Möglichkeit, die durch ihre hohe Benutzerfreundlichkeit aufgefallen ist und hier deshalb als Beispiel mit EAP-TTLS beschrieben wird.

Der Vorteil von 802.1x, die WEP-Schlüssel permanent dynamisch neu zu generieren (dynamic Re-Keying), waren ein wichtiger Sicherheitsaspekt, welche jedoch heute vom deutlich sichereren WPA mit TKIP bzw. AES abgelöst wurde. Durch die zusätzlichen Sicherheitsvorteile der mächtigen Authentifizierungs-Verfahren von 802.1x/EAP bleibt dieser Standard auch mit Unterstützung von WPA weiterhin interessant.

4.1 Konfiguration des Funk Odyssey-Server

Hier wird der schnellste Weg beschrieben, um EAP/802.1x mit WPA-Verschlüsselung basierend auf dem Funk Odyssey-Server in Betrieb zu nehmen. Als Client spielt es keine Rolle, ob man den eigenen vom Odyssey oder den Airlancer-Client nutzt.

4.1.1 Erstellung von Zertifikaten

- Sowohl bei EAP-TLS als auch bei EAP-TTLS ist mindestens ein Server-Zertifikat nötig. Einen Link zu drei verschiedene Verfahren zur Erstellung und Einrichtung des Server-Zertifikats finden Sie im Anhang.
- Zertifikate, die durch eine andere CA generiert wurden, kann man nach der Installation des Odyssey-Servers im Administrator-Tool unter **Settings** ▶ **TLS/TTLS/PEAP-Settings** auswählen.
- Das Server-Zertifikat muss dem Client bekannt sein. Dies erreicht man durch Exportierung in eine Datei, welche man dann beim Client installieren kann. Für den AirLancer-Client wird das Zertifikat z.B. unter **Security** ▶ **Configure** ausgewählt (siehe Abb. 5.4).

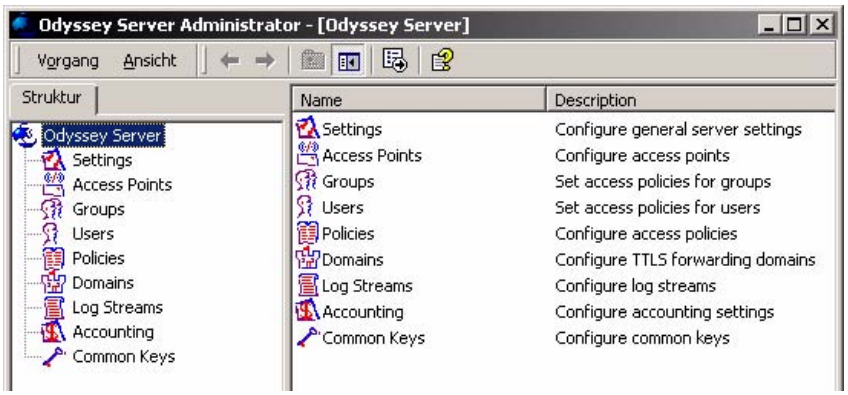

Abb. 4.1.1

4.1.2 Installation/Konfiguration des Servers

- Nach der Installation werden alle Einstellungen im Administrator-Tool vorgenommen (siehe Abb. 4.1.1).

Settings:

- **Radius-Settings** kann man Default belassen (Authentication-Port: 1812 / Accounting-Port: 1813), solange nicht andere Ports verwenden werden müssen.
- **Access Point Defaults** ist nur interessant, wenn man einen der integrierten Access-Points verwendet. Ansonsten werden alle anderen Einstellungen dafür unter **Access Points** (s.u.) vorgenommen.
- Bei **Policy Defaults** kann man die Default-Einstellung belassen.
- In **Authenticating Settings** wählt man die Authentifizierungs-Methode (z.B. TLS oder TTLS).
- In den **TLS/TTLS/PEAP Settings** werden die Zertifikate ausgewählt, ansonsten kann man die Default-Einstellungen belassen.
- Unter **User Trust** kann man das Client-Zertifikat auswählen, wenn man z.B. die Authentifizierungs-Methode EAP-TLS verwendet.
- Die Einstellungen unter **TTLS Inner Authentication, Forwarded Attributes, Returned Attributes, Self-Identication, User Identification by Certificate** und **TTLS-Accounting** können Default bleiben.

Access-Points:

- rechte Maustaste auf **Access-Points** ▶ **Add Access Point...**

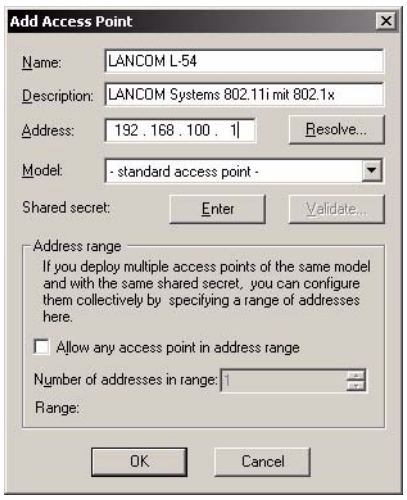

Abb. 4.1.2

- Ähnlich wie in Abb. 4.1.2 kann man IP, Name und Shared Secret vom Access-Point angeben, die natürlich entsprechend mit der Konfiguration im Access Point übereinstimmen müssen.
- Die Option, mehrere Access-Points zu nutzen ist möglich, in dem man einfach einen weiteren hinzufügt und konfiguriert.

Groups/Users:

- Damit ein Client sich im Netz hinter dem RADIUS-Server anmelden kann, muss dieser dem Server bekannt sein. Hierbei verwendet der Odyssey-Server neben den unterschiedlichen Authentifizierungsverfahren (z.B. Zertifikate) die lokalen User und Gruppen des Betriebsystems.
- Hier kann man die lokal auf dem Betriebsystem angelegten User/Gruppen im Odyssey-Server einrichten/entfernen, die Zugriff auf das Netzwerk hinter dem RADIUS haben dürfen.
- Hierzu kann man mit rechte Maustaste ▶ **Add User/Group** den jeweiligen Benutzer bzw. die jeweilige Gruppe auswählen, die lokal angelegt sind und hinzufügen.

Policies, Domains und Log-Streams:

- Die Einstellungen bleiben Default
- Unter **Log-Streams** kann man evtl. bei Bedarf Art und Aufbau der Log-Files bestimmen, falls man den ganzen Vorgang aus der Sicht des Odyssey-Servers betrachten möchte.

Accounting/Common Keys:

- Die Einstellungen bleiben Default

4.2 Konfiguration des Odyssey-Clients

- Nach der Installation kann man im **Client Manager** (Abb. 4.2.1) alle Einstellungen vornehmen.

Connection:

- Unter **Connection** wird wie in Abb. 4.2.1 den benötigten Netzwerk-Adapter und das gewünschte Netz-werk ausgewählt.
- Der Status zeigt mit **„open and authenticated"** an, dass der Radius-Server den Client erfolgreich authentifiziert hat und dass der Zugriff auf das Netzwerk hinter dem Access Point nun für dem Client offen ist. Dies lässt sich auch kontrollieren, indem man prüft, ob ggf. der DHCP-Server des Routers oder Access Points dem Client eine IP zugewiesen hat, oder ob z.B. einfach ein Ping zum Server durchkommt.
- Ansonsten kann man die Einstellungen ändern und mit **Reconnect** bzw. **Reauthenticate** den Vorgang wiederholen.

Profiles:

- Unter **Profiles** (Abb. 4.2.2) kann man verschiedene Profile für die Client-User erstellen und verwalten. In diesem Fall

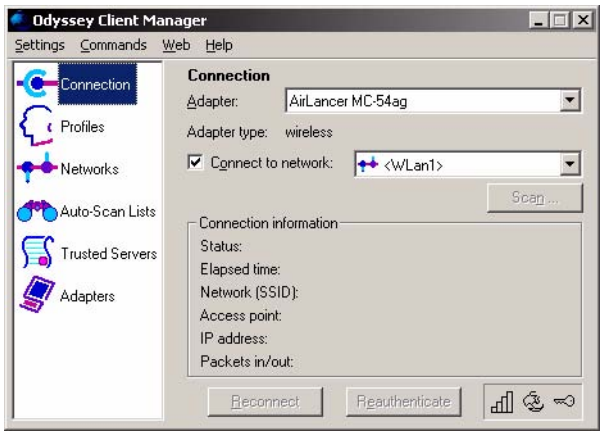

Abb. 4.2.1

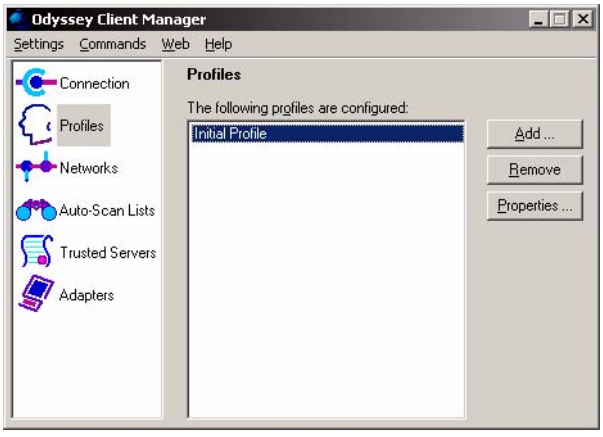

Abb. 4.2.2

wird der Einfachkeit halber das Initial Profile verwendet

- Unter **Properties** kann man das Profil verwalten (Abb. 4.2.3).

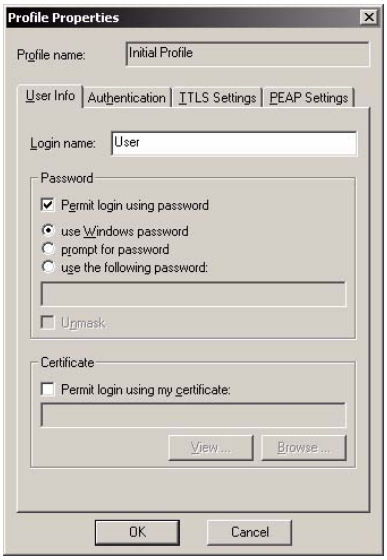

Abb. 4.2.3

- Unter **User Info** muss „**Permit login using password**" aktiviert werden. Der schnellste Weg ist „use Windows password", welche dann die Userdaten vom aktuell auf dem Client angemeldeten User nutzt. Hierbei sollte natürlich auf dem Server der entsprechende User eingerichtet sein, wobei auch das Passwort übereinstimmen muss. Alternativ kann ggf. ein anderes Passwort angegeben oder durch ein Prompt bei der Authentifizierung später abgefragt werden.
- Unter **Authentication** wählt man die Authentifizierungs-Methode aus, wie z.B. EAP/TTLS und aktiviert „**Validate server certificate**".
- **TTLS Settings** bleiben bei den Default-Werten.
- Die **PEAP Settings** spielen bei TTLS keine Rolle.

Networks:

- Unter **Networks** wird das gewünschte WLAN-Netzwerk konfiguriert (Abb. 4.2.4).

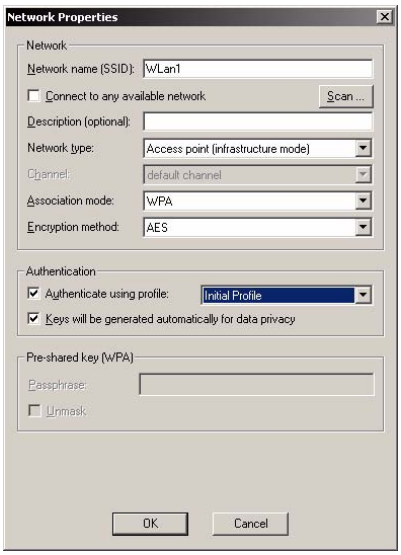

Abb. 4.2.4

- Mit **Add...** ein wird Netzwerk hinzufügt und unter **Properties...** konfiguriert.
- Im Feld **Network name (SSID)** muss man den Netzwerk-Name angeben, welches man konfigurieren möchte. Mit **Scan...** kann man eins unter den gefundenen Netzwerke auswählen.
- Unter **Association Mode** wählt man zwischen WPA, wie in diesem Fall, oder open- bzw. shared WEP.
- Bei **Encryption Method** wird dann entsprechend passend zum **Association Mode** die Verschlüsselung konfiguriert, wobei zwischen dem hochsicheren AES (802.11i) und TKIP gewählt werden kann.

Auto-Scan Lists:

- Diese Einstellungen kann man als Default belassen.

Trusted Servers:

- Wenn bei EAP-TTLS hier kein Server angegeben wird, fragt der Client explizit nach, ob der Server, wo man sich authentifizieren möchte, vertrauenswürdig ist und trägt ihn bei positiver Antwort hier ein. Dies ist auch manuell möglich und sogar empfohlen, wenn man das Server-Zertifikat besitzt.
- Per **Add...** kann man das Zertifikat auswählen und den Server-Namen angeben.

Adapters:

- Hier werden die ggf. unterschiedlichen Netzwerk-Adapter verwaltet.

5 Konfiguration des Airlancer-Clients

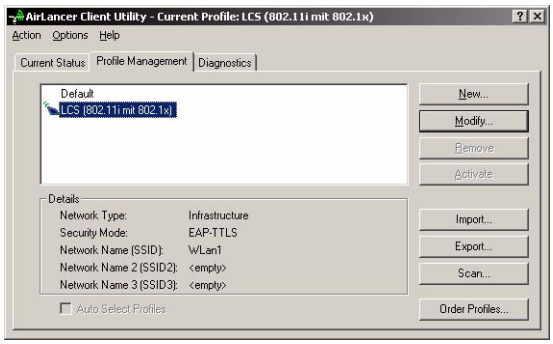

Abb. 5.1

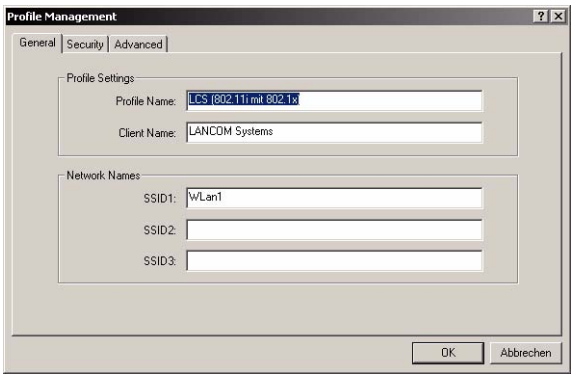

Abb. 5.2

- Um den **Airlancer Client** für 802.1x zu konfigurieren, erstellt man ein beliebiges Profil und gibt dementsprechend die SSID und den Namen des Clients an. (Abb. 5.1 und 5.2).
- Im **Profile Management** wird auf der Registerkarte **Security** WPA mit derentsprechenden EAP-Methode ausgewählt – in diesem Fall TTLS für 802.1x mit WPA (in Abb. 5.3).
- Im Gegensatz zum Odyssey-Client spielt es hier keine Rolle, ob die Verschlüsselung TKIP oder AES angewendet wird, weil der Client das selbst erkennt.

Hinweis: Die Security Option **802.1x** nutzt die WEP-Verschlüsselung mit dynamischen Re-Keying. Um 802.1x mit 802.11i zu verwenden, muss die Security Option **WPA** mit der passenden EAP-Authentifizierungs-Methode ausgewählt werden.

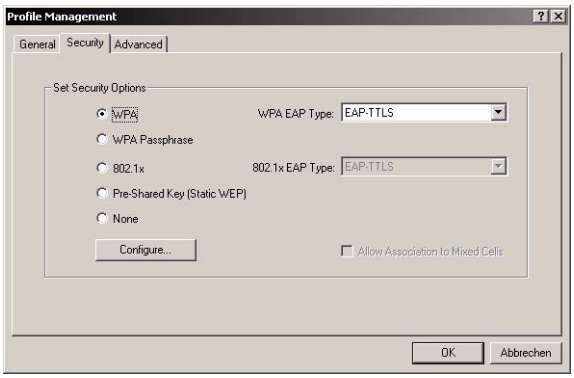

Abb. 5.3

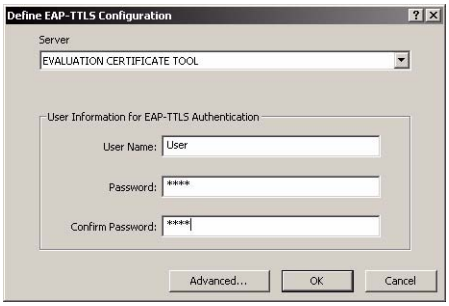

Abb. 5.4

6 Anhang

Die 802.1x-Spezifikation sind verfügbar unter:
http://www.drizzle.com/~aboba/IEEE

Bisher bekannte Schwachstellen sind zu finden bei der „University of Maryland" unter:
http://www.cs.umd.edu/~waa/1x.pdf

Verfahren zur Erstellung und Einrichtung von Server-Zertifikaten findet man unter:
http://domino.mms.de/tech.nsf/0/12f6ed456fa6b2dac1256be90029a30f?OpenDocument