



Rechenzentrum

Zentrale Einrichtung für Multimedia,
Kommunikationstechnik und
Informationsverarbeitung

Autor: Dipl.-Ing. Th. Keune

Datum: 11.04.2005

Grundlagen zum Wireless LAN

Die klassischen drahtlosen Netze (Wireless-LANs – WLAN) sind in der Standard-Familie IEEE 802.11 festgelegt.

Das Protokoll und die Übertragungsverfahren für drahtlose Netze wurden 1997 zunächst nur für 2 MBit/s auf dem Frequenzband von 2,4 GHz festgelegt. In mehreren Erweiterungen wurde die Spezifikation immer weiter ausgebaut. Heute sind im wesentlichen aus dieser Familie drei Standards relevant.

- IEEE802.11b
1999 wurde IEEE 802.11 auf eine Bandbreite von 11 Mbit/s erweitert und als IEEE 802.11b festgelegt.
- IEEE 802.11a
Ebenfalls 1999 wurde der Standard IEEE 802.11a verabschiedet. Danach wird das 5 GHz-Frequenzband benutzt. IEEE 802.11a stellt eine Bandbreite von 54 Mbit/s bereit. Allerdings ist die Nutzung des 5GHz-Frequenzbandes weltweit nicht einheitlich geregelt. Dadurch ergeben sich Unterschiede bei der Nutzung. Hinzu kommt ferner, dass durch die unterschiedlichen nationalen Regelungen unterschiedliche Sendeleistungen definiert sind, was auch zu unterschiedlichen Reichweiten führt. In Deutschland dürfen Geräte nach diesem Standard nur in geschlossenen Räumen eingesetzt werden
- IEEE 802.11g
Im Juli 2003 wurde der Standard IEEE 802.11g-Standard verabschiedet. Dieser Standard stellt ebenfalls eine Bandbreite von 54 Mbit/s bereit, nutzt aber wie IEEE 802.11b das 2,4GHz-Frequenzband. Der besondere Vorteil ist die Kompatibilität zu IEEE-802.11b. Werden in einem IEEE 802.11g-WLAN Geräte mit IEEE 802.11b-Standard genutzt, wird die Datenrate automatisch auf die Datenrate von IEEE 802.11b (11 MBit/s) reduziert. Access-Points, die nur IEEE 802.11b unterstützen können Geräte nach IEEE 802.11g nicht erkennen.

Standard	Bandbreite		Frequenzband
	<i>raw</i>	<i>effektiv</i>	
IEEE 802.11b	11 Mbit/s	5 – 6 Mbit/s	2,4 GHz
IEEE 802.11a	54 Mbit/s	22 – 25 Mbit/s	5,0 GHz
IEEE 802.11g	54 Mbit/s	22 – 25 Mbit/s	2,4 GHz

Tabelle 1: relevante WLAN-Standards

Verwendete Frequenzen in IEEE802.11b/g

Für Wireless-LANs nach IEEE 802.11b/g sind im Frequenzband von 2,4 GHz-Band insgesamt 14 Kanäle mit einem Trägerfrequenzabstand von nur 5 MHz vorgesehen, während der Frequenzbereich eines Kanals aber 25 Mhz beträgt.

Tabelle 2 zeigt die Frequenzbelegung in Europa, den USA und Japan:

Kanal	Trägerfrequenz	Frequenzbereich	Europa	USA	Japan
1	2412 MHz	2399,5 MHz - 2424,5 MHz	Grün	Grün	Grün
2	2417 MHz	2404,5 MHz - 2429,5 MHz	Grün	Grün	Grün
3	2422 MHz	2409,5 MHz - 2434,5 MHz	Grün	Grün	Grün
4	2427 MHz	2414,5 MHz - 2439,5 MHz	Grün	Grün	Grün
5	2432 MHz	2419,5 MHz - 2444,5 MHz	Grün	Grün	Grün
6	2437 MHz	2424,5 MHz - 2449,5 MHz	Grün	Grün	Grün
7	2442 MHz	2429,5 MHz - 2454,5 MHz	Grün	Grün	Grün
8	2447 MHz	2434,5 MHz - 2459,5 MHz	Grün	Grün	Grün
9	2452 MHz	2439,5 MHz - 2464,5 MHz	Grün	Grün	Grün
10	2457 MHz	2444,5 MHz - 2469,5 MHz	Grün	Grün	Grün
11	2462 MHz	2449,5 MHz - 2474,5 MHz	Grün	Grün	Grün
12	2467 MHz	2454,5 MHz - 2479,5 MHz	Grün	Rot	Grün
13	2472 MHz	2459,5 MHz - 2484,5 MHz	Grün	Rot	Grün
14	2477 MHz	2464,5 MHz - 2489,5 MHz	Rot	Rot	Grün

Tabelle 2: Frequenzbelegung von WLANs nach IEEE 802.11b/g

Aufgrund der dichten Kanalbelegung gibt es im Grunde nur drei Kanäle, die sich nicht mit anderen Kanälen überdecken: Kanäle 1, Kanal 7 bzw. 8 und 13 bzw. 14.

Die unterschiedliche Kanalbelegung kann bei der Nutzung von WLAN auf Reisen zu Problemen führen: Hat man eine „amerikanische“ WLAN-Karte, die nur die Kanäle 1 bis 11 „kennt“, kann es sein, dass diese in Europa keinen Kontakt zu einem Access-Point bekommt, weil der auf den Kanälen 12 oder 13 arbeitet.

Datensicherheit

Anders als bei drahtgebundener Datenübertragung kann bei einer drahtlosen Datenkommunikation jeder die Daten empfangen, die „durch die Luft schwirren“. Um den Datenverkehr innerhalb der Funkzelle, d. h. von den Clients zum Access-Point und umgekehrt zu sichern, sollten die Daten zwischen den Stationen und dem Accesspoint verschlüsselt werden. Hierzu wird WEP (Wired Equivalent Privacy) verwendet. Die Nutzdaten werden mittels des RC4-Algorithmus mit Schlüssel-Längen von 64 bzw. 128 Bit (effektiv 40 bzw. 104 Bit) verschlüsselt. Heute gilt WEP allerdings - besonders die 40-Bit-Variante - nicht mehr als besonders sicher, da der verwendete Code als gebrochen gilt.

Um dem zu begegnen, werden andere Mechanismen eingesetzt:

- ◆ VPN - virtual private Networks
Datenübertragung mit IPsec-Verschlüsselung, zusätzlich ist ein sog. VPN-Concentrator im Netz erforderlich. Dieser ist das Bindeglied zwischen z.B. WLAN und dem „normalen“ Netz.
- ◆ dynamisches WEP
- ◆ WPA
- ◆

Authentifikation

Neben der Datensicherheit der über die Funkschnittstelle übertragenen Daten selbst muß dafür gesorgt werden, das über das WLAN nur berechnigte Nutzer Zugriff auf das „dahinter“ liegende Netzwerk erhalten. Dazu gibt es neben dem klassischen VPN, dem Virtual Privat Network, mit dem Standard IEEE 802.1X eine moderne und relativ einfach zu handhabende Alternative.

IEEE 802.1X

Der Standard IEEE 802.1X definiert den Ablauf und Protokolle zur Abwicklung einer Authentifikation. Das Protokoll EAP (Extensible Authentication Protocol) stellt verschiedenen Authentifizierungsmethoden zur Verfügung, über die die eigentliche Authentifizierung abgewickelt wird.

Wie beim VPN ist zur Authentifikation nach IEEE 802.1X ein Client-Programm auf dem lokalen Rechner erforderlich. Dieses Programm wird als *Supplicant* bezeichnet.

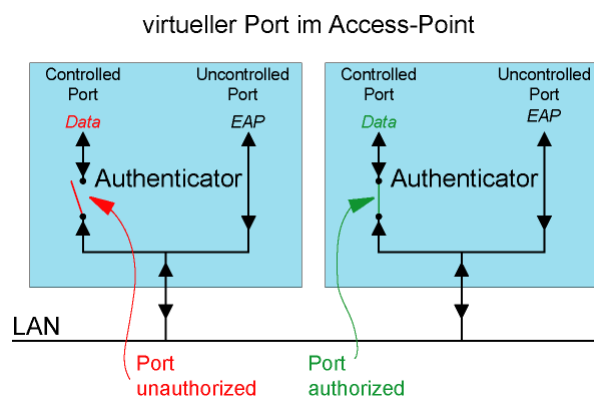


Abbildung 1: Port Based Authentication bei IEEE 802.1X

IEEE 802.1X wird auch als „Port Based Authentication“ bezeichnet. Als „Port“ wird im Zusammenhang mit Wireless-LANs der virtuelle Anschluß im Access-Point bezeichnet, zu dem der Client - Supplicant - eine Verbindung aufgebaut hat. Der Access-Point ist gleichzeitig auch Authenticator. Logisch gesehen besteht der virtuelle Port aus einem „Controlled Port“ und einem „Uncontrolled Port“: Über den „Uncontrolled Port“ wird ausschließlich die EAP-Kommunikation zwischen Supplicant und Authentifizierungs-Server abgewickelt. Erst nach erfolgreicher Authentifizierung wird der „Controlled Port“ freigegeben, über den der Zugriff auf das LAN möglich wird.

In Abbildung 2 ist der Ablauf einer Authentifizierung dargestellt:

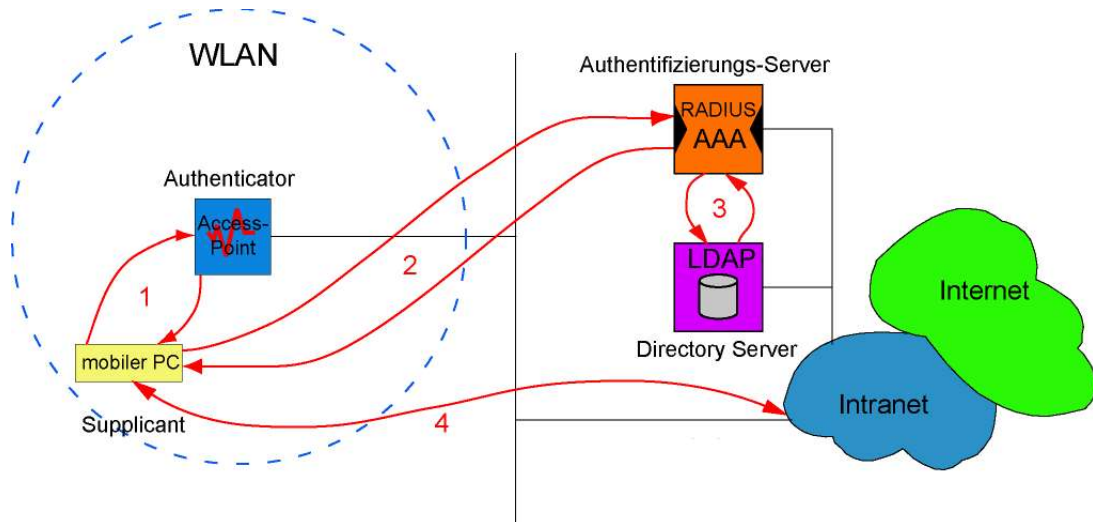


Abbildung 2: Authentifizierungsablauf bei IEEE 802.1X

Zuächst baut der Supplicant über den Access-Point (1) einen SSL-Tunnel (2) zum Authentifizierungsserver (RADIUS) auf. Während dieser Phase leitet der Access-Point nur Datenpakete zwischen dem Supplicant und dem Authentifizierungsserver weiter (Controlled Port gesperrt). Über diesen sicheren Übertragungsweg werden dann die Anmeldedaten des Benutzers übertragen. Der RADIUS entpackt die per EAP gesendeten Nutzerdaten und führt eine Überprüfung gegen den zentralen LDAP-Server (3) durch.

Konnten die Nutzerdaten erfolgreich verifiziert werden, so gibt der Access-Point die Verbindung vom mobilen PC zum Intra- und Internet frei (4) (Controlled Port freigegeben).

EAP

Das EAP-Protokoll stellt für die Authentifizierung verschiedene Authentifizierungsmethoden zur Verfügung.

EAP-Methode	Beschreibung
EAP-MD5	Benutzername/Passwort werden MD5 kodiert übertragen, nicht sehr sicher, daher in WLAN-Umgebungen nicht verbreitet.
LEAP	Lightweight EAP Zur Authentifikation ist Benutzername/Passwort erforderlich. LEAP gilt als nicht besonders sicher, daher heute von PEAP abgelöst.
EAP-TLS	Vor der Authentifizierung wird eine TLS-Session (Transport Layer Security) als „Sicherer Kanal“ zwischen Server und Supplicant erzeugt, über den dann die Authentifizierung mit Benutzername und Passwort abgewickelt wird. Sowohl auf Authentifizierungs-Server- als auf dem Supplicant ist ein eigenes X.509 Zertifikat erforderlich. Dies setzt eine Public Key Infrastruktur (PKI) voraus.
EAP-TTLS	Wie bei TLS wird vor der Authentifizierung ein sicherer TLS-Kanal erzeugt. Nur für den Authentifizierungs-Server ist ein Zertifikat erforderlich. Der Supplicant läßt sich das Zertifikat des Servers (wie bei SSH) vom Anwender als „vertrauenswürdig“ bestätigen. Innerhalb des Tunnels kann dann jede unsichere Authentifizierung, meist wird PAP verwendet, um Benutzername und Passwort zu übertragen, da der Kommunikationsweg von sich aus sicher ist.
PEAP	Protected EAP Ähnlich wie bei TTLS wird ein sicherer Tunnel aufgebaut. Für den Authentifizierungs-Server ist ein Zertifikat erforderlich, für den Supplicant optional. Prinzipell wie TTLS.
EAP-MSCHAPv2	Vom Grund her die EAP-Variante von MS-CHAPv2 Zur Authentifikation ist Benutzername/Passwort erforderlich.

WLAN-Umgebung in der Fachhochschule

Das Funknetz der Fachhochschule ist in die Netzwerk-Infrastruktur der Standorte integriert.

Als Access-Points werden Geräte von Cisco Systems eingesetzt. Bei den Geräten handelt es sich um den Typ Aironet 1231, die nach dem Standard IEEE 802.11g (54 Mbit/s) arbeiten. Die Access-Points sind kompatibel zum Standard IEEE 802.11b, es können also mobile Rechner sowohl mit 802.11b als auch IEEE 802.11g gleichzeitig auf das drahtlose Netzwerk zugreifen.

Zugang

Der Zugang in das WLAN ist nur über eine IEEE 802.1X-Authentifizierung (EAP-TTLS) möglich. Die Adresszuweisung erfolgt dynamisch per DHCP aus dem sog. privaten IP-Adressbereich 10.0.0.0 (RFC 1918). Beim Übergang in das Internet wird per Network Address Translation (NAT, RFC1631) eine Umsetzung vorgenommen.

Voraussetzung

Zur Nutzung des WLAN wird benötigt:

- eine WLAN-Karte für den Rechner. Diese sollte dem WiFi-Standard oder dem neuen IEEE 802.11g-Standard entsprechen. Neuere Notebooks mit Centrino- oder WLAN-Modul erfüllen diese Spezifikation ebenfalls.
- ein Rechner mit geeignetem Betriebssystem:
 - ◆ Windows XP oder Windows 2000
 - ◆ MAC OS X ab Version 10.3
 - ◆ Linux
 - ◆ ...
- einen gültigen Benutzeraccount der Fachhochschule.
- einen IEEE-802.1X-Supplicant.
Für Windows 2000/XP bietet RZ den OpenSource Supplicant SecureW2 an, in MAC OS ist ab Version 10.3 (Panther) ein Supplicant im Betriebssystem integriert. Für Linux bieten sich die beiden Pakete Xsupplicant bzw. WPAsupplicant an.