Hauptseminar Telematik

– Virtual Access Points –

Michael Roßberg

Betreuer: Dr. Werner Horn
Fachgebiet Telematik
Fakultät für Informatik und Automatisierung
Technische Universität Ilmenau

19. Juni 2005

Inhaltsverzeichnis

Kapitel 1

Einleitung

Der Siegeszug der Funknetzwerke

Herkömmliche Netzwerke bewegen sich nicht, die meisten Menschen tun aber genau das den ganzen Tag. Der steigende Bedarf an Mobilität ist wohl der wichtigste Grund für den Erfolg von WLAN[1]. Aber Funknetzwerke haben noch andere Vorteile:

- relativ leicht und schnell zu installieren
- hohen Durchsatz von bis zu 108Mbit/s
- enorm flexibel einsetzbar
- sehr kostengünstige Funktechnologie

Seit ein paar Jahren sind Funknetzwerke nun in aller Munde. Wenn man der Werbung Glauben schenken kann, gibt es heute keine Geschäftsleute mehr ohne kleine Geräte, die jeden Platz auf der Welt zu einem Arbeitsplatz machen. Die Bewertung dieser Situation sei jedem selbst überlassen. Tatsache ist, dass die IEEE mit dem 802.11 Standart von 1997 dem riesigen Erfolg von Ethernet ein i-Tüpfelchen aufsetzen konnte. Selbst die katastrophalen Sicherheitsprobleme, die im Jahr 2001 den ohnehin schon schwachen WEP Schutz völlig vernichteten [FMS01], konnten dem Erfolg von Wireless LAN scheinbar nichts anhaben.

Heute sollen alleine in den Vereinigten Staaten von Amerika bereits 10 Millionen Haushalte über eigene Funknetzwerke verfügen [ITFacts05].

[1] WLAN - Wireless Local Area Network. Funknetzwerk nach IEEE802.11

Kapitel 2

Grundlagen

Was versteht man unter einem Virtual Access Point?

Der Begriff des „Virtual Access Points“ wurde maßgeblich von Bernard Aboba geschaffen. Als Mitglied der 802.11 Standardisierungsgruppe hat er im Jahr 2003 eine grundlegende Arbeit veröffentlicht [Aboba03]. Heute verwenden verschiedene Firmen den Begriff um ihre properitären Entwicklungen zu vermarkten. Eine Standardisierung liegt noch nicht vor. Der Begriff „Virtual Access Point“ wird oft als „Virtual AP“ oder einfach nur „VAP“ abgekürzt.

Definition: Ein virtueller Access Point ist eine logische Einheit in einem physischen Access Point. Dieser Access Point kann mehrere virtuelle APs unterstützen, die einem Klienten wie verschiedene APs erscheinen, auch wenn der AP nur einmal vorhanden ist. Dies kann zum einen durch eine mehr oder weniger aufwendige Simulation geschehen, oder durch eine Software auf Seite der Benutzer.

Wozu wird die Virtual Access Point Technologie benötigt?

Die VAP-Technik bietet dem Klienten grundsätzlich die Möglichkeit, Services eines Access Points explizit zu wählen. Ein naiver Ansatz ist, die Klienten ihr VLAN im Backend wählen zu lassen. Man könnte also beispielsweise Gästen einen beschränkten Zugang ohne Passwortschutz anbieten, während die Mitarbeiter einer Firma, die selben Basisstationen für kritische Aufgaben verwenden.

Weitere Anwendungsgebiete sind die Wahl von Quality of Service Eigenschaften, einer Authentifizierungsmethode oder die Möglichkeit überlappende Bereiche zwischen verschiedenen Netzwerken zu schaffen.

Das größte Potenzial wird jedoch im schnell wachsenden Hotspot[1] Markt gesehen. Dabei könnten mit Hilfe von VAPs mehrere verschiedene Anbieter gemeinsame Hardware getrennt betreiben. Ein Vorgehen wie es in der Mobilfunkbranche schon lange üblich ist. Die Vorteile sind hierbei:

- **Verbesserte Frequenznutzung**
  In den meisten Regionen der Welt gibt es nur drei nicht überlappende Kanäle im gebräuchlichen 2,4GHz Band. Das führt dazu dass sich Anbieter an hochfrequentierten

[1] Hotspot - Ein Bereich in dem Internet über Funknetz, i.d.R. gegen Bezahlung, angeboten wird.

Plätzen, wie zum Beispiel Flughäfen, sehr schnell behindern. Durch eine gemeinsame Planung könnte die Nutzung des Funkmediums in solchen Umgebungen optimiert werden.

- **Kostenreduktion**
  WLAN-Ausrüstung ist zwar wesentlich billiger, als beispielsweise Ausrüstung für den Mobilfunk, dennoch könnten Anbieter enorme Hardware- und Verwaltungskosten einsparen, wenn sie auf gemeinsame Access Points setzen würden. VAPs bieten hierbei die Möglichkeit trotzdem nicht auf spezifische Details, wie den Markennamen, verzichten zu müssen.

- **neue Geschäftsmodelle**
  Denkbar wäre beispielsweise ein hochpriorisiertes virtuelles Netzwerk für Geschäftskunden und ein kostengünstigeres für Privatanwender.

Kapitel 3

Access Point Management in 802.11

Bemerkung: *Dieses Kapitel bezieht sich ausschließlich auf Netzwerke mit reiner Basisstation-Klienten-Kommunikation, und nicht alle Aussagen sind direkt auf Ad-Hoc Netzwerke oder Wireless Distribution Systems anwendbar.*

3.1 Begriffe

Folgende Begriffe sind für das elementare Verständnis von Funknetzwerken wichtig:

- **basic service set identification (BSSID)**
  Eine BSSID ist eine global eindeutige Nummer, die das Netz um genau eine Basisstation identifiziert. Jede BSSID ist genau 6 Byte lang und wird analog zu einer MAC-Adresse gebildet.

- **extended service set (ESS)**
  Unter einem ESS versteht man mehrere Basisstationen, die über eine gemeinsame Infrastruktur verfügen. Nur innerhalb eines solchen ESS ist beispielsweise Roaming möglich.

- **service set identifier (SSID)**
  Die SSID ist im Prinzip der Name eines Netzwerks. Jede SSID ist eine bis zu 32 Bytes lange Zeichenfolge und in der Regel vom Menschen lesbar. Daher werden SSIDs benutzt um in potenziellen Klienten die Existenz von Funknetzwerken kenntlich zu machen. Laut 802.11 Spezifikation ist es vorgesehen das mehrere BSS Geräte mit einer SSID versehen werden können (die Geräte bilden dann ein ESS). Die Spezifikation behandelt jedoch nicht den umgekehrten Fall. Deshalb gehen herkömmliche Implementationen von Netzwerkkarten davon aus, dass einem Gerät immer nur eine SSID zu geordnet wird.

3.2 Management-Frames

In 802.11 wird der gesamte Verwaltungsaufwand, der mit dem Finden und dem Zugriff auf ein Funknetzwerk in Zusammenhang steht, durch so genannte Management-Frames

realisiert. Der genaue Aufbau der Pakete und die genauen Funktionsweisen können unter [IEEE80211] nachgelesen werden. Einen schönen Einstieg bietet auch [Gast05].

Die wichtigsten Management Frame Typen werden nachfolgernd kurz erläutert. Für virtuelle Access Points ist es wichtig, dass bei allen Verwaltungspaketen sowohl die BSSID des Netzwerks als auch die MAC-Adresse des Klienten mitgeschickt werden muss. Die SSID wird in fast allen Klient-zu-Basisstation Paketen sowie in den Beacons übertragen.

- **Beacons**
  Beacons sind ein Typ Management Frames, die von einem Access Point regelmäßig (in der Regel alle 100ms) ausgesendet werden. Sie haben sehr vielfältige Aufgaben und regeln unter anderem Stromspar- und Zeitsynchronisationsaufgaben. Beacons dienen aber auch dem Finden von Netzwerken und der Bestimmung der Signalqualität. Laut Standart [IEEE80211] muss in Beacons die SSID des Netzwerks erwähnt werden.

- **Probe Requests**
  Probe Requests sind explizite Aufforderungen eines Klienten an eine Basisstation ihm Verwaltungsinformationen zu schicken. Um nach bestimmten Services zu suchen enthalten Probe Requests ein SSID Informationselement. Es existiert aber auch die Möglichkeit unbestimmt zu suchen. In diesem Fall ist eine SSID der Länge 0 zu benutzen.

- **Probe Responses**
  Eine Probe Response ist die Antwort eines APs auf einen Probe Request. Sie hat prinzipiell dieselbe Struktur wie ein Beacon.

- **Authentication Requests**
  Authentification Requests werden von Klienten geschickt, um sich gegenüber einer Basisstation beziehungsweise eines ESS zu authentifizieren. [IEEE80211] kennt dabei Open und Shared Authentication. Beim Ersteren wird auf einen direkten Berechtigungsnachweis verzichtet, er kann aber implizit später stattfinden. Der Klient müsste sich dann beispielsweise über 802.1x ausweisen. Bei der Shared Authentication erfolgt die Authentifizierung mit Hilfe eines Challenge-Response-Verfahrens. Allerdings wird hierbei das unsichere WEP Verfahren eingesetzt.
  Authentification Requests enthalten kein SSID Informationselement. Sie adressieren lediglich den Access Point.

- **Association Requests**
  Mit Hilfe von Association Requests meldet sich ein Klient bei einer Basis Station an. Diese Anmeldung kann nur nach einer Authentifizierung bei einer Basisstation innerhalb des ESS erfolgen.

Kapitel 4

Implementationsmethoden für Virtual Access Points

4.1 Eine BSSID und eine SSID

Die Verwendung einer SSID entspricht zwar streng genommen nicht der Definition einer virtuellen Basisstation, jedoch erlauben auch die folgenden zwei Verfahren eine statische Zuordnung zu verschiedenen Diensten und sind zudem noch von historischem Interesse.

4.1.1 Zuordnungsunterscheidung auf MAC-Adressen Basis

Eine simple Implementierung von virtuellen Basisstationen könnte Benutzer anhand ihrer MAC-Adressen unterscheiden. MAC-Adressen haben in der Regel den Vorteil, dass sie direkt einem Benutzer zu zuordnen sind, und ausserdem in jedem Paket mitgeschickt werden müssen. Eine einfache Abbildung auf verschiedene VLANs ist so möglich. Es existieren jedoch auch gravierende Nachteile:

1. Die Verwaltung von MAC-Adresslisten bedeutet gerade in großen Institutionen einen riesigen Aufwand. Häufig auftretende Änderungen führen zu wenig Transparenz.
2. Jede allein auf MAC-Adressen basierende Authentifizierung ist unsicher.
3. Zuordnungen sind statisch, das bedeutet der Benutzer kann nicht ad-hoc wählen welche Dienste er in Anspruch nehmen möchte.
4. Es existieren ungeklärte Fragen bezüglich Broadcast und Multicast Paketen. Wie bei einem Hub, der vor einem VLAN-fähigen Switch steht, werden alle Rundrufpakte aus verschiedenen Subnetzen an alle Teilnehmer des Funknetzwerks geschickt. Bei Multicast Paketen führt das nur zu dem Problem, dass manche Klienten unnötig belastet werden. Bei Broadcast Paketen ist das Problem grösser. Unter Umständen werden hier Pakete interpretiert, die nicht für den Teilnehmer bestimmt waren. Ein Beispiel wären zwei Windows-Computer, die an zwei verschiedene VLANs senden, aber die selben privaten IP-Adress-Bereiche verwenden. Ein vernünftiges Arbeiten mit der Netzwerkumgebung wäre nicht mehr möglich.
   Das Problem relativiert sich aber mit dem Einführen von Sicherheitsmechanismen.

Durch Kryptographie mit unterschiedlichen Verfahren oder Schlüsseln lassen sich beide VLANs vollständig von einander trennen.

5. Beacons stellen ein nicht so simpel zu lösendes Problem dar. Auch sie sind Broadcast Pakete, im Unterschied zu den eben genannten handelt es sich aber hierbei nicht um Daten- sondern um Management-Frames. Die wichtigste Folge ist: Verwaltungsinformationen dürfen nicht verschlüsselt werden, somit ist eine gezielte Unterscheidung von Klienten nicht mehr möglich.
   Einige Hersteller umgehen dieses Problem in dem sie Informationen, wie die einzelnen verwendeten SSIDs und Verschlüsselungsverfahren, von den Administratoren fest in die mobilen Geräte konfigurieren lassen. Eine sehr unflexible und fehlerträchtige „Lösung“.

4.1.2 Zuordnungsunterscheidung auf Basis von Benutzeridentifikationen

Beim Einsatz von verschiedenen Benutzerkennungen oder verschiedener Gruppenschlüsseln ist es möglich auf Basis dieser Daten verschiedene Dienste zur Verfügung zustellen. Dieses Verfahren behebt allerdings nur die ersten zwei Mängel an der MAC-Authentifizierung, und setzt außerdem ein EAP-basiertes Verfahren voraus. Von einer Unterscheidung durch vier festkonfigurierte WEP Schlüssel, wie immer noch von manchen Institutionen betrieben, ist abzuraten.

4.2 Eine BSSID und mehrere SSIDs

Ein Funknetzwerk mit mehreren SSIDs zu betreiben, bietet eine mehr oder weniger transparente Möglichkeit die Auswahl der in Anspruch genommenen Dienste dem Benutzer zu überlassen. Jeder einzelne Netzwerkname könnte dann zum Beispiel einem Provider oder einer Sicherheitsklasse zugeordnet werden.
Alle folgenden Ansätze könnten in der Praxis mit ein paar Einschränkungen funktionieren. Allerdings stellt [Melville04] klar, dass das Betreiben von mehreren SSIDs über eine BSSID laut [IEEE80211] eigentlich nicht erlaubt ist:

> *So while there is no explicit ban on sharing a BSSID among multiple SSIDs, the specification implicitly denies it.*

4.2.1 Guest-Mode

Bei dem Guest-Mode Verfahren gibt es mehrere SSIDs mit denen sich Klienten bei einer Basisstation assoziieren können. Auf Probe Requests mit den einzelnen SSIDs wird mit Probe Responses der entsprechenden Dienste geantwortet.
Probleme entstehen erst wenn man die SSID nicht kennt: es ist für Basisstationen in der Regel nur vorgesehen genau eine SSID bekannt zu geben. Jetzt erklärt sich auch der Name „Guest-Mode“. Mit diesem Verfahren ist es nur möglich den Dienst für Gäste zu annoncieren. Alle anderen Dienste müssen manuell durch den Administrator zu den Benutzergruppen

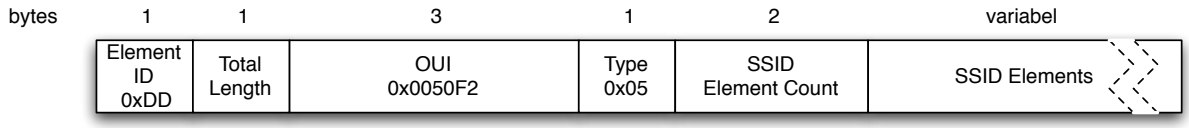
gelangen.
Hier gibt es Parallelen zur Zuordnung auf MAC-Adressenbasis; ein solcher Prozess ist fehlerträchtig und unbefriedigend für alle Beteiligten.

4.2.2 mehrere SSID Tags

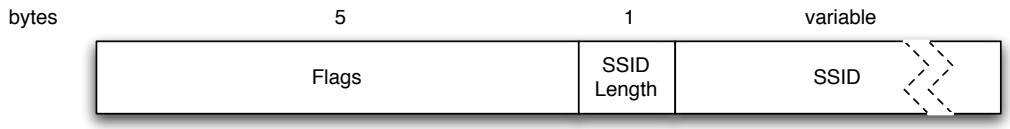
Auch wenn heutige Implementationen von Funknetzwerksoftware davon ausgehen, dass in Beacons genau ein SSID-Informationselement auftaucht, so spricht nichts dagegen einfach mehrere solcher Elemente anzuhängen. Im Standart finden sich auch in diesem Fall keine expliziten Verbote, aber Applikationen, die mit einer solchen trickreichen Auslegung nicht rechnen, werden zu unvorhersehbaren Effekten neigen.

4.2.3 SSID Listen von Cisco

Einen offiziell tragbareren Weg hat die Firma Cisco eingeschlagen. Durch das Anhängen eines herstellerspezifischen Informationselements an Beacons und Probe Responses werden hier SSIDs bekannt gegeben. Leider neigt Cisco dazu properitäre Entwicklungen nicht zu standardisieren und öffentlich bekannt zu geben. So auch bei der Dokumentation der SSID Listen. Sie ist nur für OEM Hersteller im Rahmen des [CCX] Programms verfügbar. Alle folgenden Informationen sind daher durch „Reverse Engineering“ gewonnen worden.



Die äußere Struktur des Informationselements folgt einem inoffiziellen Schema des Wi-Fi Konsortiums. Dabei wird als Element-ID 0xDD angegeben. Diese Nummer ist extra für herstellerspezifische Erweiterungen reserviert worden. Im folgenden Byte steht die gesamte Länge des Elements, um Klienten das Springen zum nächsten Element zu ermöglichen. Als nächstes wird ein 3 Byte „Organizationally Unique Identifier“ übertragen. Dieser OUI ist eine global eindeutige Nummer, die eigentlich zur MAC-Adressvergabe genutzt und von der IEEE vergeben wird. In unserem Fall ist die ID 0x0050F2. Das Type Feld dient der Unterscheidung von mehreren Erweiterungen eines Herstellers. Das letzte benötigte Feld gibt die Anzahl der SSID Elemente an, die bekannt gegeben werden sollen. Diese werden einfach konkateniert nach dem bekannten Muster an das Listenelement angehangen.



Der prinzipielle Aufbau des SSID-Elements ist einfach. Jedes Element beginnt mit 5 Byte Statusbits, die Konfigurationsinformationen für das virtuelle Funknetz enthalten. Dem folgt die Länge der SSID sowie die SSID selbst.

Die Bitmaske spiegelt vor allem Sicherheitseinstellungen wieder. Von rechts-nach-links gelesen ergeben sich folgende Bedeutungen:

Ciphersuite	
Bit 1	• 40-bit RC4 Schlüssel kann verwendet werden
Bit 2	• 104-bit RC4 Schlüssel kann verwendet werden
Bit 3	• AES Schlüssel kann verwendet werden • kann nicht mit RC4 Verschlüsselung kombiniert werden

Verschlüsselung (Bits nicht kombinierbar)	
Bit 5	• Keine Verschlüsselung
Bit 6	• WEP-40 Verschlüsselung
Bit 7	• WEP-104 Verschlüsselung
Bit 8	• TKIP wird benutzt • Indikation des Algorithmus über Bit 1 & 2

prä-WPA Erweiterungen (Bits nicht kombinierbar)	
Bit 10	• Cisco MIC und Per Packet Keying ist aktiviert. • Indikation des Algorithmus über Bit 10 und 11 • Bit 1, 2 und 3 scheinen eine besondere Bedeutung zu haben. Sie sind fest auf 1, 0, 1 gesetzt.
Bit 11	• Per Packet Keying ist aktiviert und CMIC ist deaktiviert. • Indikation des Algorithmus über Bit 10 und 11 • Bit 1, 2 und 3 sind fest auf 1, 1, 0 gesetzt.
Bit 12	• CMIC ist aktiviert und Per Packet Keying ist deaktiviert. • Indikation des Algorithmus über Bit 10 und 11 • Bit 1, 2 und 3 sind fest auf 1, 1, 1 gesetzt.

Schlüsselverwaltung (Bits beliebig kombinierbar)	
Bit 16	• Eine Schlüsselverwaltung findet statt. Dieses Bit muss gesetzt werden, falls irgendeine der folgenden Optionen aktiviert wurde.
Bit 26	• Schlüsselverwaltung mit WiFi Protected Access Version 1 im Enterprise Modus
Bit 27	• WiFi Protected Access Version 1 im Preshared Key (PSK) Modus
Bit 28	• WiFi Protected Access Version 2 im Enterprise Modus
Bit 29	• WiFi Protected Access Version 2 im Preshared Key Modus
Bit 30	• Cisco Centralized Key Management mit WEP
Bit 31	• Cisco Centralized Key Management im AES Modus

Verschiedenes (Bits beliebig kombinierbar)	
Bit 33	• Möglichkeit der EAP-Authentisierung vorhanden
Bit 34	• Wireless Provisioning System (WPS) wird verwendet

4.2.4 Verbleibende Probleme

Bei der Verwendung von mehreren SSIDs über eine BSSID verbleiben einige Probleme. Wie auch bei den anderen bisher vorgestellten Lösungen bleibt die Verwendung von Rundrufpaketen problematisch, weil sie von allen Klienten der physischen Basisstation empfangen und verarbeitet werden.
Durch die Verwendung von mehreren SSIDs werden aber auch zwei zusätzliche Probleme eingeführt. Zum einen erfordern die letzten beiden Lösungen veränderte Software auf Seiten der Teilnehmer. Die Modifikationen halten sich aber in Grenzen und durch einen offenen Standart ließe es sich relativ einfach bewerkstelligen.
Das andere Problem ist, das keine 802.11 konforme Authentifizierung nach der „shared key“ Methode mehr möglich ist. Dabei findet normalerweise vor der Assoziierung ein Challenge-Response-Verfahren mit WEP statt; allerdings wird hierbei noch nicht die SSID übertragen und die Basisstation kann somit keine Überprüfung der Antwort durchführen. Mögliche Auswege wären eine verzögerte Überprüfung mit einer Deauthentifizierung im Falle eines Fehlschlags oder ein vollständiger Verzicht auf „shared key“, was angesichts der Sicherheitsprobleme von WEP sicherlich keinen Verlust darstellt.

4.3 Mehrere BSSIDs und mehrere SSIDs

Die inzwischen von vielen Firmen bevorzugte Methode, der Implementierung von virtuellen Access Points, ist vollständig konform zu [IEEE80211]. Bei der Verwendung von mehreren SSIDs und mehreren BSSIDs kann auf der Funkschnittstelle kein Zusammenhang zwischen den Netzen mehr erkannt werden.
Bei schlechten Funkbedingungen wird aber gerade diese Transparenz zu einem Problem werden. Bei 802.11 führen solche Bedingungen zu häufigen Handover Vorgängen. Mit der Einführung von virtuellen Funknetzwerken wird auch zwischen diesen ständig gewechselt werden, denn Klienten können nicht erkennen, dass es sich immer um dieselbe Basisstation handelt.
Der offensichtlichste Nachteil des Ansatzes ist aber klar die Verschwendung von Funkressourcen. Damit die einzelnen virtuellen Netze gut reagieren muss das Sendeintervall der Beacons konstant bleiben. Das bedeutet für vier virtuelle Funknetzwerke vervierfacht sich der Beaconverkehr. Diese Vervielfachung bedeutet aber auch eine höhere Belastung für die Basisstationen. Durch die harten Echtzeitforderungen, die an Beacons gestellt werden, setzen moderne softwareseitige Implementierungen auf Interrupts, die dann auch wesentlich öfter auftreten müssen.
In der Präsentation zur Entwicklung des Madwifi-Treibers [Leffler05] werden auch noch weitere Hardwareprobleme beschrieben. Um einen schnellen Transport zu gewährleisten werden Unicast-Datenpakete in Funknetzwerken von den Prozessoren der Netzwerkkarten bestätigt. Diese Prozessoren sind jedoch in der Regel dazu ausgelegt nur eine einzige BSSID zu überwachen. Die Basisstation muss aber alle ihre BSSIDs überwachen können. Für die Entschlüsselung mit Hilfe der Hardware müssen die Prozessoren außerdem eine Zuordnung von Chiffriermethode und -schlüssel auf Basis von MAC-Adressen erlauben. Es wird noch einige Zeit dauern bis diese Forderungen selbstverständlicher Weise erfüllt werden.
Bleibt die Frage nach der „Verschwendung“ von BSSIDs. Wenn an jedes Gerät, was in der Lage ist eine Basisstation zu betreiben, sehr viele MAC-Adressen vergeben werden, dann könnte es in ein paar Jahren eine Analogie zur Knappheit der Internet-Adressen geben.

Kapitel 5

Zusammenfassung

Virtuelle Basisstationen sind eine sehr interessante Technologie. Allerdings stellt sich die Frage warum die IEEE ihren Fehler bei der Einführung von Ethernet noch einmal wiederholt hat. Damals musste der Standart 802.1q nachgereicht werden, der virtuelle LANs eingeführt hat. Meiner Meinung nach wäre auch jetzt eine Standardisierung zu befürworten, um die Verwaltung schlank zu halten und Inkompatibilitäten Einhalt zu gebieten.
Bis dahin wird jedoch die einzige Methode eine virtuelle Basisstation zu implementieren auf die vollständige Emulation der Luftschnittstelle, mit mehreren SSIDs und BSSIDs, hinauslaufen.

Literaturverzeichnis

[CCX] Cisco Systems.
Cisco Compatible Extensions Program for Wireless LAN (WLAN) Devices
http://www.cisco.com/en/US/partners/pr46/pr147/partners_pgm_concept_home.html

[Leffler05] Sam Leffler.
FreeBSD Wireless NetworkingFreeBSD Wireless Networking, 2005
http://people.freebsd.org/~sam/BSDCan2005.pdf

[FMS01] Scott Fluhrer, Itsik Mantin and Adi Shamir.
Weaknesses in the Key Scheduling Algorithm of RC4, 2001
http://www.wisdom.weizmann.ac.il/~itsik/RC4/Papers/Rc4_ksa.ps

[IEEE80211] IEEE Std 802.11-1999
Information technology– Telecommunications and information exchange between systems– Local and metropolitan area networks– Specific requirements–
Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 1999
http://standards.ieee.org/getieee802/download/802.11-1999.pdf

[ITFacts05] IT Facts
10 mln US households have WLAN, 2005
http://www.itfacts.biz/index.php?id=P3062

[Melville04] Graham Melville.
Virtual Access Point Definition, 2004
http://www.drizzle.com/~aboba/IEEE/
11-04-0238-00-0wng-definition-virtual-access-point.doc

[Aboba03] Bernard Aboba.
Virtual Access Points, 2003
http://www.drizzle.com/~aboba/IEEE/11-03-154r1-I-Virtual-Access-Points.doc

[Gast05] Matthew Gast.
802.11 Wireless Networks: The Definitive Guide
Second Edition, O'Reilly, 2005