Patrick Postel

Sebastian Schünemann

Jaroslaw Zdrzalek

Sicherheit in kommerziellen WLAN-Systemen

Diplomarbeit eingereicht im Rahmen der Diplomprüfung
im Studiengang Technische Informatik
am Fachbereich Elektrotechnik und Informatik
der Hochschule für Angewandte Wissenschaften Hamburg

Betreuender Prüfer : Prof. Dr. Kai von Luck
Zweitgutachter : Prof. Dr.-Ing. Martin Hübner

Abgegeben am 29. Januar 2004

Patrick Postel, Sebastian Schünemann und Jaroslaw Zdrzalek

Thema der Diplomarbeit

Sicherheit in kommerziellen WLAN-Systemen

Stichworte

WLAN, Sicherheit, Greenspot-Roaming

Kurzzusammenfassung

Diese Arbeit beschäftigt sich mit der Planung, dem Design und der Umsetzung einer WLAN-Lösung für den kommerziellen Einsatz. Dabei steht vor allem das Thema Sicherheit im Vordergrund, da es die derzeit schwächste Stelle im WLAN-Standard ist. Vorgestellt wird dabei ein System, das aus zwei Komponenten besteht, einer Hardware vor Ort und einem zentralen Server, der diese verwaltet. Die Lösung ist so konzipiert, in verschiedenen Konfigurationen mehrerer unterschiedliche Zielgruppen und Einsatzszenarien bedienen zu können.

Patrick Postel, Sebastian Schünemann and Jaroslaw Zdrzalek

Title of the paper

Security for comercial WLAN-Systems

Keywords

WLAN, Security, Greenspot-Roaming

Abstract

This thesis covers planning, design and implementation of a wireless LAN system for commercial usage. One topic handles security aspects as the weakest part of actual WLAN standards, the other one tackles roaming problems. Our proposed solution consists of two components. On the one hand we designed a LINUX based router and access point, one the other hand a server is proposed for control and management. The system is designed for flexible handling different user groups and usages by easy change some configuration parameters.

INHALTSVERZEICHNIS

1. EINLEITUNG 7

1.1. Road Map 9

2. DATENÜBERTRAGUNG 11

2.1. Der Übertragungsweg 11

2.2. Kabel vs. Funk 12

2.3. Fazit 13

3. EINSATZSZENARIEN 15

3.1. Zielgruppen 16

3.1.1. Finanzdienstleistungen 16

3.1.2. Gesundheit 19

3.1.3. Außendienst 21

3.1.4. WLAN-Betreiber 23

3.2. Lösungsansätze 24

3.2.1. Office / Privat 25

3.2.2. Gebäudekomplexe, teils öffentlich 26

3.2.3. HotSpots 28

3.2.4. Zusammenfassung 29

3.3. Schlussfolgerung 30

4. MOBILE TECHNIKEN 31

4.1. Mobilfunk 31

4.1.1. GSM 31

4.1.2. HSCSD 32

4.1.3. GPRS 33

4.1.4. UMTS 33

4.2. Bluetooth 37

4.3. WLAN Überblick 39

4.4. Vergleiche 41

4.5. Schlussfolgerungen 46

5. WLAN 47

5.1. Die physikalische Ebene 50
5.1.1. DSSS - Direct Sequence Spread Spectrum 50
5.1.2. FHSS (Frequency Hopping Spread Spectrum) 51
5.1.3. OFHS (Orthogonal Frequency Division Multiplexing) 51

5.2. Standards 53
5.2.1. Allgemeines 53
5.2.2. Standardreihen 54
5.2.3. Erweiterungen 56
5.2.4. Fazit 58

5.3. Gesundheitsrisiken 60

5.4. Probleme im kommerziellen WLAN aus Anwendersicht 62
5.4.1. Sicherheit 62
5.4.2. Zugangskontrolle / Roaming 63

5.5. Roaming 63
5.5.1. Roaming von HotSpots 63
5.5.2. Greenspot 64

5.6. Schlussfolgerung 66

6. SICHERHEIT 67

6.1. Was bedeutet Sicherheit 67
6.1.1. Verfügbarkeit 67
6.1.2. Integrität 68
6.1.3. Vertraulichkeit 68
6.1.4. Authentizität 69
6.1.5. Autorisierung 70
6.1.6. Verbindlichkeit 70

6.2. Angriffe 70
6.2.1. „Sniffing“ 71
6.2.2. Spoofing 72
6.2.3. Man-in-the-middle 73
6.2.4. Session Hijacking 74
6.2.5. Denial Of Service 75

6.3. Protokolle zur Datensicherung in konventionellen, kabelgebundenen Netzwerken 75

6.3.1. PPTP ... 75
6.3.2. L2TP ... 84
6.3.3. SSH ... 84
6.3.4. IP-SEC ... 86
6.3.5. SSL/TLS ... 91
6.3.6. Kerberos ... 95
6.3.7. Firewall ... 99

6.4. Native WLAN-Sicherheit ... 104
6.4.1. WARUM WEP & co, wenn es VPN und IPSec gibt? ... 104
6.4.2. Was gibt es an Sicherungsmethoden und wozu sind sie geeignet? ... 105
6.4.3. Die Verfahren im Einzelnen ... 107
6.4.4. Die Varianten des EAP ... 110
6.4.5. WPA ... 115
6.4.6. WPA2 (802.11i) ... 117

6.5. Gegenüberstellung der Sicherungsmethoden ... 118
6.5.1. Allgemeine Netzwerksicherungsmethoden ... 118

7. IMPLEMENTIERUNG EINES KOMMERZIELLEN WLAN-SYSTEMS ... 121

7.1. Anforderungen an das Gesamtsystem ... 121

7.2. Das Access-Gateway, die Box ... 123
7.2.1. Anforderungen, was für Komponenten werden benötigt? ... 123
7.2.2. Design, Softwarekomponenten im Überblick ... 126
7.2.3. Implementierung des Access Gateways ... 135

7.3. Server ... 153
7.3.1. Anforderungen ... 153
7.3.2. Gateway-Server-Kommunikation ... 158
7.3.3. Benutzerverwaltung ... 170
7.3.4. Administration GUI ... 176
7.3.5. Roaming ... 178

8. RESÜMEE ... 183

8.1. Wurden die Anforderungen erfüllt ? ... 183
8.1.1. Sicherheit ... 183
8.1.2. Einfachheit der Bedienung ... 184
8.1.3. Flexibilität/Erweiterbarkeit ... 185
8.1.4. Kommerzieller Einsatz ... 185
8.1.5. Skalierbarkeit ... 186

8.2. Fazit 188

8.3. Ausblicke 189

1.Einleitung

Mobilität ist seit je her ein Grundbedürfnis des Menschen. Mit Mobilität verband man bisher vor allem die physische Freiheit, sich von Ort zu Ort bewegen zu können. Durch die Techniken der modernen Datenübertragung jedoch, ist in den letzten Jahren eine weitere Ausprägung hinzugekommen, die Mobilität in der Kommunikation.
Zwei Aspekte gilt es zu betrachten, zum einen die Möglichkeit auf die eigenen Kommunikationskanäle auch von „unterwegs“ aus zuzugreifen, zum anderen dabei nicht von störenden Kabeln abhängig zu sein.
Ein Statement von einer der führenden „Denkfabriken“ der achtziger und neunziger Jahre, dem XEROX – PARC, soll an dieser Stelle angebracht werden. Genauer die Gedanken von Marc Weiser, einem der „Väter“ der Idee von „Ubiques Computing“ oder auch der dritten Computergeneration. Er dachte schon Ende der achtziger Jahre über die Zukunft der Computer innerhalb der Gesellschaft nach und stellte einige für damalige Zeiten visionäre Modelle auf. Unter anderem beschrieb er die unterschiedlichen Zyklen, die die Rechner in unserer Gesellschaft durchlaufen werden. Eine erste Generation, in der viele Terminals mittels eines Rechners bedient werden, sprich sich viele Nutzer einen Rechner teilen, eine zweite Generation, in der jeder Nutzer über einen eigenen Rechner verfügt und eine dritte Generation, in der auf einen Nutzer mehrere Rechner kommen - eine Vorhersage, die exakt eingetroffen ist. Über eine vierte Generation schwieg er sich allerdings aus und da er leider bereits verstorben ist, wird es auch dabei bleiben. [Weiser] Der Siegeszug dieser dritten Computergeneration wird dabei maßgeblich von zwei entscheidenden Elementen abhängen, zum einen von mobiler Rechenpower, die zu ständig fallenden Preisen verfügbar ist, und zum anderen von den digitalen, mobil verfügbaren Kommunikationsnetzen.
Ist eine Konnektivität zu diesen Netzen einmal sichergestellt und verfügbar, so wäre dies der Schritt in die mobile, multimediale Kommunikation, die das Abfragen von Informationen jeder Art, zu

jeder Zeit und von jedem Ort aus ermöglicht. In Kombination mit tragbaren Endgeräten ist so für einige Berufsgruppen ein Arbeiten von quasi jedem beliebigen Ort aus möglich.
Ein Kandidat diese Aufgabe zu lösen, ist die Technik „Wireless LAN“ (WLAN). Allerdings leiden die bisherigen Pilotprojekte zumeist unter einem von drei verschiedenen Symptomen:

a) Sie sind zu teuer, so dass der Dienst nicht attraktiv ist. (z.B. Telekom, 7,95 Euro pro Stunde)

b) Sie sind kostenlos, was sich für keinen Betreiber auf Dauer rechnen kann. (z.B. HotSpot Hamburg)

c) Sie sind von einem „normalen“ Benutzer nicht zu bedienen, da eine Reihe von technischen Kenntnissen vorausgesetzt wird. (z.B. aufwendige Konfigurationen)

Die Zielsetzung dieser Arbeit soll es sein, eine Lösung zu erarbeiten, die den Anforderungen des kommerziellen Einsatzes von WLAN entspricht. Es gilt dabei ein sicheres, zuverlässiges und erschwingliches System zu kreieren, das sich durch einfache Handhabung auch für den Massenmarkt eignet.

Der Consumer-Bereich, soll hier also außer Acht gelassen werden, in ihm geht es vornehmlich um die bequeme Handhabung innerhalb der eigenen vier Wände. Ob im Garten, im Bett oder im Arbeitszimmer, überall soll eine einfache Nutzung gewährleistet sein. Die Anforderungen an die Technik sind in diesem Bereich eher niedrig, da es sich um klar definierte Aufgaben und Nutzergruppen handelt.
Im kommerziellen Umfeld hingegen, gilt es eine Vielzahl von Aufgaben und ständig wechselnde Benutzergruppen unter einen Hut zu bringen. Dies erfordert zwar komplexere und aufwendigere Systeme, aber dafür bedienen diese dann auch einen sehr lukrativen Markt, die Business-Kunden.
Einer der wichtigsten Punkte im kommerziellen Umfeld ist das Thema Sicherheit. Firmendaten sind zumeist vertraulich und wenn

diese auch noch durch die Luft übertragen werden, ist deren Schutz elementar.

Zwei unterschiedliche Ansätze sind innerhalb der mobilen Datennetze zu erkennen. Zum einen die PAN's (Personal Area Networks), die die Kommunikation zwischen verschiedenen Geräten abbilden und mittels „spontaner Netzwerkbildung" tatsächlich als eine neue Netzform gesehen werden könnten und zum anderen die hier thematisierten Netze, die es zum Ziel haben, Geräte mit vorhandener Infrastruktur zu verbinden.
Dabei geht es um einen drahtlosen Zugriff auf das Intra- oder Internet unter Zuhilfenahme der bereits vorhandenen, kabelgebundenen Kanäle. Dieses zusätzliche „Angebot" wird allen die „berechtigt" sind zur Verfügung gestellt. Wobei die Berechtigung in bestimmten Bereichen auch mittels Geld erworben werden kann. Für diese Nutzer kommt, neben dem bedeutenden Thema der Sicherheit, eine weitere Anforderung hinzu, diejenige der Existenz von Bezahlsystemen und Bezahlmöglichkeiten.
Zu erwähnen ist noch, dass es wahrscheinlich nicht einen einzelnen Betreiber dieser Zugangspunkte geben wird, sondern mehrere oder gar viele. Um es für die zahlenden Kunden dennoch möglichst einfach zu halten, wird es nötig sein, für Systeme zu sorgen, die einen einheitlichen Zugriff bei allen Betreibern ermöglichen, ähnlich wie die meisten es vom Mobiltelefon gewöhnt sind. Damit ist eine dritte wichtige Anforderung angesprochen: das Thema Roaming.

1.1. Road Map

Im Verlaufe dieser Arbeit werden wir darlegen, welche Gründe uns bewogen haben, eine Lösung wie die unsrige zu kreieren. Dabei soll nachvollziehbar werden, welche Indikatoren uns zu den jeweiligen Entscheidungen geführt haben. Beginnen werden wir in Kapitel 2 mit der Frage, ob wir auf stationäre oder mobile Übertragungswege setzten wollen. Auch wenn vieles für das Kabel spricht, so gibt es dennoch gute Gründe für den Einsatz drahtloser Techniken.

Im dritten Kapitel werden wir evaluieren, für welche Zielgruppen eine mobile Datenübertragung interessant ist. Wir werden von einigen exemplarischen Beispielen abstrahieren und diese auf drei grundsätzliche Einsatzszenarien herunterbrechen. Die Büros, die HotSpots und die halb-öffentlichen Gebäudekomplexe. In einem weiteren Abstraktionsschritt wird dann gezeigt, dass diese wiederum von einem System mit nur zwei Komponenten bedient werden können: einer „Hardware vor Ort“ und einer Zentraleinheit, die eine Vielzahl dieser Geräte verwalten kann.
Im 4. Kapitel werden die in Betracht kommenden Verfahren zur mobilen Datenkommunikation gegenübergestellt, sowie eine Begründung für unsere Wahl, WLAN, geliefert. Ein Verfahren das dann im Kapitel 5 etwas genauer vorgestellt wird.
Wie bereits kurz angerissen, ist die Sicherheit, der zentrale Punkt im kommerziellen Umfeld. Eine Thematik, die im Zusammenhang mit Datenübertragung zwar noch nicht in alle Köpfe vorgedrungen ist, aber sich anschickt, dies zu tun. Schon deshalb darf sie in keiner anspruchsvollen Lösung fehlen. Welche Standards es auf diesem Sektor gibt und wo die jeweiligen Stärken und Schwächen liegen, wird in Kapitel 6. näher erläutert. Dieses Kapitel schließt dann auch den theoretischen Grundlagenteil ab, so dass wir uns im Kapitel 7 der Praxis zuwenden können. Hier soll eine konkrete Umsetzung der beiden benötigten Komponenten, „Hardware vor Ort“ und „Zentraleinheit“, anhand des Beispieles „HotSpot“ vorgestellt werden. Diese wird dann im abschließenden Kapitel 8 noch einmal mit etwas Abstand betrachtet und zusammengefasst.

2.Datenübertragung

Seit einigen Jahren reden Gesellschaftswissenschaftler jeglicher Ausrichtung davon, dass ein neues Zeitalter der Menschheitsgeschichte angebrochen ist, das Kommunikationszeitalter !

Für die Einsicht, dass diese Aussage nicht jeglicher Grundlage entbehrt, bedarf es keines Hochschulstudiums, ein Blick in unsere nähere Umgebung genügt. Nicht nur die Massenmedien wie Rundfunk, Presse, Fernsehen und Werbeplakate umgeben uns wo immer wir auch sind, die Kommunikation hat auch in unsere Hosentasche Einzug gehalten. Das Mobiltelefon gehört für einen Großteil der Menschen in Mitteleuropa beim Verlassen des Hauses genauso zur alltägliches Ausstattung wie die Schlüssel oder die Brieftasche.
Auf der anderen Seite wird auch der Gebrauch von PDA's, die wahrscheinlich irgendwann mit den Mobiltelefonen verschmelzen werden, und den Laptops als Arbeitsmittel, immer alltäglicher, was zusammenfassend bedeutet, dass in naher Zukunft ein nicht unerheblicher Teil der europäischen Bevölkerung Geräte zur elektronischen Datenverarbeitung ständig bei sich tragen wird.
Betrachtet man diese Tendenz liegt eine Schlussfolgerung auf der Hand, Datennetze, die diese Geräte dann mit „Aktualität" versorgen, werden in Zukunft noch wichtiger, als sie heute schon sind.

2.1. Der Übertragungsweg

Um eine Datenübertragung zu etablieren, müssen drei wesentliche Dinge vorhanden sein, ein Sender, ein Empfänger und eine Strecke die Sender und Empfänger verbindet. Für die Strecke ist dabei wichtig, dass sie sowohl vom Sender als auch vom Empfänger unterstützt wird und dass sich beide Seiten auf eine einheitliches Verfahren geeinigt haben, wie die Daten übertragen werden und wie

sie nach dem Empfang zu interpretieren sind. Dies wird in der Regel von Protokollen geleistet, die auf beiden Seiten arbeiten. In der Praxis handelt es sich dabei meist nicht um eines, sondern um mehrere Protokolle, die verschiedene Aufgaben erledigen. Zum Beispiel regelt eines die physikalische Ebene mit Details zur Signalübertragung, den Pegeln, dem Timing usw., während ein anderes die Interpretation der Daten auf der Anwendungsebene regelt. Die beteiligten Protokolle arbeiten dabei völlig getrennt voneinander, denn es ist für sie nicht wichtig, von wem sie Daten bekommen und welcher Art diese Daten sind. Ihre Aufgabe ist es, die „Roh-Daten“, die irgendjemand bereit stellt, auf der einen Seite zu verpacken, auf die „Reise“ zu schicken, und auf der anderen Seite wieder auszupacken, sowie die dann in „1 zu 1 Kopie“ vorhandenen „Roh-Daten“ wieder an die auf der anderen Seite wartende Anwendung zu übergeben.
Um die Prozesse einer Kommunikation zwischen Anwendungen abzubilden, wurde das OSI-Schichtenmodell entwickelt, auf das hier nicht näher eingegangen werden soll. Näheres zu dem OSI-Schichtenmodell und Protokollen findet man zum Beispiel in [Tanenbaum].

Die eventuell vorhandenen Protokolle und Verfahren auf Anwendungsebene sollen hier erst einmal keine Betrachtung finden, es geht im ersten Schritt um die physikalische Ebene.
Zur Übertragung von Daten gibt es auf physikalischer Ebene grundsätzlich zwei unterschiedliche Wege: Diejenigen per Kabel oder per Funk.

2.2. Kabel vs. Funk

Das Kabel ist der Veteran auf diesem Sektor und immer noch das am häufigsten genutzte Medium zur Datenübertragung. Seine Vorteile liegen ganz klar in den beiden elementaren Punkten Zuverlässigkeit und Sicherheit. Sicherheit, da die Daten, die mittels eines Kabels übertragen werden, von außen ohne großen Aufwand nicht zugänglich sind, da man sich physikalischen Zugriff auf das

Kabel selbst verschaffen müsste, Zuverlässigkeit, da nur extrem große Störeinflüsse die Datenübertragung mittels eines Kabels beeinträchtigen. Diese sind wiederum relativ leicht ausfindig zu machen und zu beseitigen.
Der Funk hingegen, hat genau an diesen beiden elementaren Punkten große Nachteile zu verzeichnen. Die Summe der Störeinflüsse ist groß, da der „Äther“ immer voller wird, und der „Wunde Punkt“ beim Thema Sicherheit ist die Tatsache, dass nicht nur der gewünschte Empfänger die Nachricht bekommt, sondern auch jeder andere, der sich in Sendereichweite befindet.
Darüber hinaus ist auch die maximale Datenrate bei kabelgebundenen Strecken höher, so dass man zusammenfassend sagen kann, dass das Kabel aus Übertragungssicht nur Vorteile bietet - wäre da nicht das in den letzten Jahren immer stärker werdende Thema: „Mobilität“.
In den letzten wenigen Jahrzehnten wurde eine Tendenz sichtbar, die mit einer steigenden Nachfrage an mobiler Datenübertragung in der breiten Masse zu umschreiben ist. Ein erster Ausdruck dieser Entwicklung war die Fernbedienung für den Fernseher und es gipfelt derzeit im Boom der Mobiltelefone. Der nächste Schritt ist jetzt der Zugriff über mobile Wege auf das Intra-/Internet und auch hier gibt es die ersten Lösungen, sowohl für unterwegs, als auch für das Büro oder daheim.
Die Nutzer haben einen neuen „Wert“ entdeckt, den „Wert“ der Mobilität. Eben diese Mobilität ist es auch, die die Anforderungen an kabellose Übertragungswege bestimmt. Dies bedeutet natürlich einen größeren Anspruch an die zu Grunde liegende Technik, denn es gilt die oben angesprochenen Probleme, Sicherheit, Zuverlässigkeit und Datenrate zu lösen.

2.3. Fazit

Auch wenn die Übertragung per Kabel viele Vorteile birgt, geht der Trend derzeit deutlich dahin, sich vom Kabel weitestgehend zu lösen, sowohl was die Stromversorgung (AKKU/Batterie), als auch was die Übertragung der Daten angeht. Es ist auch nur ein Grund

vorstellbar, der diesen Trend in den nächsten Jahren aufhalten könnte. Eine „Massenangst“ vor den uns umgebenden Funkwellen und Zweifel in Bezug auf deren Gesundheitsverträglichkeit. Allerdings sind es nur die großen Medienkonzerne, die diese Angst schüren könnten und die haben ein eher entgegengesetztes Interesse. Daher werden wir uns an dieser Stelle dafür entscheiden, einen kabellosen Ansatz zu verfolgen.

3.Einsatzszenarien

Die Möglichkeit eine schnelle und mobile Datenkommunikation anbieten zu können hat vor einigen Jahren die großen Telekommunikationsunternehmen dazu veranlasst, während der UMTS- Lizenz-Versteigerung sehr viel Geld in dieses Vorhaben zu investieren.
Mittlerweile haben sich allerdings auch andere Verfahren herauskristallisiert, die ein ähnliches Angebot mit wesentlich geringeren Kosten zur Verfügung stellen könnten. So sind z.B. WLAN und Bluetooth mittlerweile ernst zu nehmende Konkurrenten geworden, zumal sie auch von Seiten der Hardwarehersteller starke Unterstützung erfahren. Es sind heutzutage praktisch alle neueren Notebooks sowie auch die ersten PDA (z.B.: HP5550) serienmäßig mit diesen Technologien ausgerüstet und auch die Mobiltelefone bilden hier keine Ausnahme. Viele schwierige Klippen bei der Dienstbereitstellung wie z.B. Sicherheit und Roaming sind im UMTS-Umfeld bereits umschifft, da diese Probleme schon für GSM gelöst wurden. An der Fähigkeit der anderen Systeme diese Schwierigkeiten ebenfalls adäquat zu lösen wird sich die Zukunft des mobilen Datenmarktes entscheiden. Das Spiel um die Marktvorherrschaft wird demnächst beginnen, sein Ausgang ist noch ungewiss. Eine große Zielgruppe für diese Dienstleistungen wird aber auf jeden Fall die der „Knowledge-Worker“ sein, diese potentiellen Nutzer können Ihre Tätigkeiten an praktisch jedem Ort der Welt ausüben und brauchen dafür nur ihre eigene kleine „Kommunikationszentrale“ (Laptop, Handy). Aus dieser Gruppe werden sich wahrscheinlich auch die „Early-Adapters“ der einzelnen Dienstleistungen ergeben.
Neben diesen gibt es noch diverse potentielle Kunden-und Nutzergruppen, von denen einige im Folgenden exemplarisch vorgestellt werden sollen. Ziel der Vorstellung ist es, konkret auftretende Probleme und Bedürfnisse zu isolieren und im Verlauf der weiteren Arbeit Lösungsansätze anzubieten.
Dabei sollen erst unterschiedliche Dienstleistungssektoren und deren zukünftige Anforderungen an die mobile Datenübertragung vorgestellt werden und anschließend Systeme, um diesen

Anforderungen übergreifend zu begegnen. Zur Begrifflichkeitsklärung bleibt zu sagen, dass es auf drei grundlegende Systeme hinauslaufen wird: Office, Gebäudekomplexe und HotSpots. Im Office-Bereich wird das Netz nur festgelegten Nutzern zugänglich gemacht, in Gebäudekomplexen gibt es einen definierten Benutzerkreis, der das interne Netz nutzen darf und eine öffentliche Gruppe, die gegen Bezahlung auf externe Netze zugreifen kann und im Bereich der HotSpots geht es nur um die Bereitstellung von Netzwerkdienstleistungen gegen Bezahlung. Aber zuerst sollen ein paar potentielle Zielgruppen vorgestellt werden, die an verschiedenen Bereichen der drahtlosen Kommunikation Interesse haben.

3.1. Zielgruppen

3.1.1. Finanzdienstleistungen

Finanzdienstleistungen werden im aufkommenden Markt der mobilen Multimediadienste eine zentrale Rolle spielen. Ob nun aus Sicht der reinen Transaktionen, die voraussichtlich ein erhebliches Volumen haben werden, oder als „Infrastruktur“, um andere kostenpflichtige Dienstleistungen erst zu ermöglichen.
Es lassen sich dabei zwei grundsätzliche Typen von Finanzdienstleistungen unterscheiden: Zum einen die direkten, mobilen Bezahlfunktionen, zum anderen der mobile Zugang zu den verschiedenen Leistungen der Banken und Sparkassen.
Aus Sicht der Kunden lassen sich fünf interessante Dienste herausstellen:

- mobile Micropayments
- mobile Macropayments
- mobile Überweisungen
- mobiler Aktienhandel
- mobile Beratungsdienste für Kunden

Micropayments

Das Bezahlen von digitalen Werten wie etwa Downloads oder kostenpflichtigen Informationsangeboten wird in Zukunft wahrscheinlich ebenfalls auf digitalem Wege erfolgen

Dies ist in mehrerer Hinsicht zu begrüßen. Zum einen werden die Kunden so an diese Form der Bezahlung herangeführt, zum anderen entsteht bei der gesamten Wertschöpfungskette kein Medienbruch mehr. Die entsprechenden Systeme können komplett digital abgebildet werden. Auch das Bezahlen von Waren im Internet wird wahrscheinlich in absehbarer Zukunft auf diesem Wege abgewickelt. Eine andere Form des Einsatzes von Micropayment wird das Bezahlen vor Ort via SMS oder Anruf sein. So könnten z.B. Getränke- oder Zigarettenautomaten bedient werden.

Macropayments

Bei den Macropayments geht es um die Übertragung von Kreditkartenfunktionen auf mobile Endgeräte. An manchen Stellen haben sie einige Berührungspunkte mit den Micropayments, erweitern diese jedoch um den Erwerb von nahezu allen Produkten und Dienstleistungen in der „realen“, nicht digitalen Welt.

Überweisungen

Zum Angebot der Sparkassen und Banken über mobile Datenkanäle wird ein Abbild des heutigen Online-Bankings auf entsprechende Endgeräte gehören. Abfragen des eigenen Kontostandes, Überweisungen, aber auch Statusabfragen zu eigenen Geldgeschäften werden demnächst auch mobil angeboten.

Aktienhandel

Der mobile Aktienhandel wird eher einen kleineren Nutzerkreis ansprechen, denn nur ein Bruchteil der Bankkunden machen täglich Börsengeschäfte. Auf der anderen Seite sind die dort getätigten Umsätze allerdings auch dementsprechend groß, so dass ein durchaus lukrativer Markt zu erwarten ist. Auch könnte die Möglichkeit diesen Dienst in oben erwähnten Standzeiten zu nutzen dazu beitragen, mehr Kunden in diesem Segment zu gewinnen.

Mobile Beratung

Ein persönlicher Ansprechpartner, mit dem auch ein Austausch von digitalen Dokumenten zeitgleich möglich ist, wird ein weiteres Angebot der Sparkassen und Banken an ihre mobilen Kunden sein, sei es der Aktienberater, Anlageberater oder ein Versicherungsexperte. Die gewünschten Informationen sind jederzeit, wahrscheinlich gegen eine entsprechende Gebühr, verfügbar.

Ein wesentlicher Vorteil in diesen mobilen Möglichkeiten liegt in dem Ausnutzen von Standzeiten. Beispielsweise im Stau oder beim Warten auf, bzw. in einem öffentlichem Transportmittel können so bereits Arbeiten, die getan werden müssen, erledigt werden ohne wirkliche Freizeit dafür aufzuwenden.

Neben einer möglichst günstigen, mobilen Datenübertragung, sind allerdings noch einige weitere wichtige Vorraussetzungen zu erfüllen, bevor diese Dienstleistungen in das tägliche Leben Einzug halten können und werden. Als erstes gilt es hier ein gutes und vollständiges Sicherheitskonzept zu erwähnen, dem von den Kunden auch Vertrauen entgegen gebracht wird. Denn die Themen Datenschutz und Datenfälschung sind im Zusammenhang mit Bezahlvorgängen hoch sensitiv. Des Weiteren wird eine leichte Bedienbarkeit der mobilen Endgeräte eine große Rolle spielen, da von der Mehrzahl der heutigen Nutzer keine allzu große Affinität zur Technik vorausgesetzt werden kann. Als dritter Punkt ist dann noch eine große Verbreitung von Akzeptanzstellen im In- und Ausland zu nennen, vornehmlich auch für die alltagsüblichen Transaktionen und all dies mit möglichst geringen anteiligen Kosten für Nutzer und Anbieter sowie einer möglichst hohen Verfügbarkeit des mobilen Datendienstes.
Zwei Einsatzgebiete für mobile Datenübertragungen sind in diesem Sektor ausfindig zu machen: Zum einen müssen die oben genannten Dienste den Endkunden ja irgendwie erreichen, sprich bei Benutzung des Internets zum Datentransport muß die „letzte Meile“ überbrückt werden (→ HotSpot), zum anderen sind mobile Datendienste auch für die hausinternen Arbeitsplätze interessant (→Office). [IZT]

3.1.2. Gesundheit

Der Gesundheitssektor befindet sich in vielerlei Hinsicht im Umbruch. Die mobile Datenkommunikation wird Ihren Teil dazu beitragen, in der Zukunft überhaupt noch eine gute medizinische Versorgung in den Industrienationen zu gewährleisten, denn bei der immer weiter steigenden Zahl älterer Menschen auf der einen Seite und den immer kleiner werdenden Budgets auf der anderen Seite, wird man um eine Automatisierung von größeren Teilen des Gesundheitssystems nicht mehr herumkommen.
Der Einzug der mobilen Datenkommunikation in diesen Sektor ist also unausweichlich und wird darüber hinaus noch einige neue Möglichkeiten mit sich bringen.
Zwei große Einsatzfelder gilt es zu unterscheiden: Die häusliche und die stationäre Pflege. Daneben gibt es davon unabhängige Themen wie etwa die mobile Patientenakte, die von den jeweiligen behandelnden Ärzten eingesehen werden kann und die, da alle Ärzte gemeinsam auf einem Datenstamm arbeiten, stets die aktuellsten Informationen enthält. Wichtig ist allerdings, dass der Patient die Kontrolle behält, wer in seine Akte sehen darf und auch was er sehen darf. Denn Details über die gesundheitliche Vergangenheit der einzelnen Patienten dürften neben den Ärzten auch Arbeitgeber und Versicherungen interessieren, was sehr negative Konsequenzen haben könnte. Ein gutes Sicherheitskonzept von der Speicherung über die Authentifizierung der Nutzer, bis hin zur Datenübertragung ist von größter Wichtigkeit, denn es handelt sich um hoch sensible Daten.

Häusliche Pflege

Zur häuslichen Pflege gehört die Behandlung von Älteren und chronisch Kranken, sowie die Überwachung von Risikoschwangerschaften und anderen temporären Patienten.
Die wichtigsten mobilen Dienstleistungen in diesem Bereich sind Notruf – und Informationsdienste sowie die Übertragung von Messdaten.

Notruf:
Ein mobiler Sender, den der Patient ständig bei sich trägt, fungiert als Notrufmelder. Im Ernstfall aktiviert der Patient den Sender und eine ständig besetzte Zentrale kann die weiteren Schritte veranlassen. Moderne Geräte können auch eine Sprechverbindung aufbauen und somit eine genauere Einschätzung der Situation ermöglichen, darüber hinaus sind sie häufig mit GPS ausgerüstet, um den Patienten auch außerhalb seiner Wohnung lokalisieren zu können.

Informationsdienste:
Erinnerungen für Diabetiker oder andere chronisch Kranke zur Medikamenteneinnahme, Änderung der Dosierung von Tabletten oder die Beantwortung von Patientenfragen, sei es automatisch bei häufig gestellten oder mittels einer Zentrale bei spezielleren, sind nur einige der Möglichkeiten von Informationssystemen. Sie sollen dazu dienen, die Ärzte dauerhaft zu entlasten.

Messdaten:
Wenn Messdaten medizinischer Geräte in Zukunft direkt an eine Zentrale zur Auswertung übertragen werden, könnte das eine Vielzahl von Arztbesuchen überflüssig machen. Bei Dauerüberwachungen könnte zudem eine sofortige Reaktion eingeleitet werden, wenn die Daten von den Sollwerten abweichen.

Im Umfeld der häuslichen Pflege steht die mobile Datenübertragung mit einer an 100% grenzenden Zuverlässigkeit des Systems im Vordergrund, denn es geht um Menschenleben.

Stationäre Pflege
Zur Stationären Pflege gehören vor allem Krankenhäuser, Rehakliniken und Pflegeheime. In allen Bereichen lassen sich zwei Gruppen von Nutzern mobiler Datendienste herausstellen: die Patienten und das Personal.
Für das Personal gilt es dabei die derzeitigen Arbeitsabläufe und Verwaltungsprozesse zu optimieren um wieder mehr Zeit für die einzelnen Patienten zu haben. So könnte durch den Einsatz von

PDA's ein Großteil des täglichen „Papierkrames" geregelt und durch den Einsatz von Laptops und mobilen Patientenakten die Visiten optimiert werden.
Für die Patienten gibt es neben den schon bei der häuslichen Pflege beschriebenen Funktionen zudem die Möglichkeit das bestehende Netz für eine lokale Kommunikation und das Bereitstellen von Zusatzdiensten zu nutzen. Angefangen vom Internetzugang über „Videos on Demand", bis hin zur Kontakt- und Spielplattform auf der die Patienten gemeinsam Ablenkung finden. Denn die Langeweile ist ein häufiges Problem bei längeren stationären Aufenthalten. Ein solches Dienstleistungsangebot könnte zudem große Teile des Gesamtsystems durch zusätzliche Einnahmen von den Patienten refinanzieren. Dabei ist darauf zu achten, dass die vom Personal übertragenen Daten in einem sicheren Datentunnel fließen und auch eine höhere Priorität als die Patientendaten genießen. Eine ganzheitliche Gebäudelösung ist hier von Nöten (→ Gebäudekomplexe) [IZT]

3.1.3. Außendienst

Viele Firmen greifen auf ein großes Netzwerk von Außendienstlern zurück um ihre Produkte zu vertreiben, diese müssen in regelmäßigen Abständen in die jeweiligen Zentralen zurückkehren, um neues Material zu bekommen und ihre Zwischenergebnisse abzuliefern. Das erwähnte Material kann im Bezug auf Außendienstmitarbeiter vielschichtig sein. Es sind die neusten Werbeunterlagen genau so wie neuere Verträge, neues Adressmaterial oder neue Firmen- und Produktpräsentationen. Die Fahrten zur Zentrale sind dabei nicht selten mit weiten Strecken verbunden, da viele Außendienstler in Gebieten eingesetzt sind, in denen die jeweilige Firma keine eigene Niederlassung besitzt. Auch müssen Arbeitsplätze vorgehalten werden, die in der überwiegenden Zeit nicht genutzt werden, denn nur wenige Firmen setzten bisher auf die dynamische Zuteilung von Büroräumen. (→ Office)

Die mobile Datenkommunikation ist ein Weg, diesen Kostenfaktoren zu begegnen.
Der Außendienstler ist im Gegensatz zu vielen anderen Zielgruppen nicht auf eine ständige Verfügbarkeit angewiesen. Es ist für ihn nur wichtig, innerhalb einiger Stunden, gewisse Bereiche ansteuern zu können, an denen er ungestört übertragen kann. Wichtiger sind für ihn die Faktoren Sicherheit, Preis und Übertragungsrate. Die Sicherheit muss natürlich während der gesamten Übertragung gewährleistet sein, da er vornehmlich wichtige Firmendaten transferiert. In vielen Konzernen wird daher die Möglichkeit ein VPN aufzubauen ein grundsätzliches Kriterium sein. Da die Datenmengen bei Präsentationen leicht in die zweistelligen Megabytes gehen können, ist zudem eine schnelle Anbindung von Bedeutung und wenn man dann noch die Gesamtmenge der Außendienstler betrachtet, ist natürlich auch der Preis ein wichtiger Faktor. (→ HotSpot) Neben diesen klassischen Außendienstlern ist eine weitere Nutzergruppe in diesem Umfeld zu isolieren. Dabei geht es um Arbeiter, die sich vorwiegend auf Montage befinden. Die dortigen Anforderungen sind vor allem eine mobile Personalplanung und eine zeitnahe Abrechnung der geleisteten Arbeiten. Es geht also eher um reine Infodienste an die Zentrale, die überwiegend keine hohen Bandbreiten benötigen werden.
Im Idealfall kann man den Datentransfer mit alltäglichen Tätigkeiten verknüpfen, um weitere Zeit zu sparen.
Wenn die Firmen sich auf eine verbreitete Technologie verlassen könnten, die zudem preisgünstig angeboten würde, könnten diese ihre gesamte Infrastruktur bezüglich der Außendienstler umstellen und in den oben erwähnten Kostenstellen enorme Summen einsparen. Ein weiteres wichtiges Problem, das allerdings noch gelöst werden muss, ist die Vorgabe, dass die Firmen natürlich nur mit einem Anbieter eine vertragliche Beziehung eingehen möchten. Denn nur mit diesem könnten sie über bessere Konditionen oder Festpreise auf Grund ihrer hohen Gesamtvolumina verhandeln. Damit also auch Lokationen, die von verschiedenen Betreibern versorgt werden, in das Angebot integriert werden können, ist ein übergreifendes Roamingabkommen von großer Wichtigkeit.

3.1.4. WLAN-Betreiber

Bisher wurden nur Dienstleistungssektoren betrachtet, die zwar auf eine zukünftige mobile Datenkommunikation angewiesen, aber nicht auf eine bestimmte Technologie festgelegt sind. Beim WLAN-Betreiber ist dies, wie der Name schon verrät, anders. Er setzt in seinem Businessmodell voll auf den Siegeszug der WLAN-Technologie. Sein Ziel ist es als WISP (Wireless Internet Service Provider) zu fungieren und die Bereitstellung von mobilen Internetzugängen zu vermarkten. An dieser Stelle muss erwähnt werden, dass sich die Rolle der WISP's derzeit im Wandel befindet. Auf Grund der bisherigen Struktur mit eher sporadischen Lokationen, an denen dieser Dienst angeboten wird und der ebenfalls noch sehr geringen Zahl an Nutzern ist das derzeit meist genutzte Verfahren der Verkauf von Prepaid-Karten vor Ort. Der WISP, verdient also direkt an den Kunden sein Geld.
Mit der zunehmenden Verbreitung von WLAN, sowohl was die Nutzer, als auch was die Zugangspunkte angeht, wird sich eine völlig andere Struktur ergeben.
In dem neuen Geschäftsfeld des WISP wird es neben anderen WISP's noch drei weitere Akteure geben. Erstens die Standortbetreiber, die den Zugang vor Ort ermöglichen, zweitens die Serviceprovider, die die Kundenbeziehungen pflegen und die Dienstleistung verkaufen und drittens natürlich die Nutzer selbst. Die Rolle eines WISP's wird es sein, möglichst viele Standorte zu vereinen und diese den Serviceprovidern gegen eine entsprechende Gebühr zur Verfügung zu stellen. Viele WISP's werden wahrscheinlich gleichzeitig als Standortbetreiber fungieren und die größten sogar auch als Serviceprovider.
Diese Rolle wird allerdings wohl nur Großkonzernen, die auf dem Sektor der Telekommunikation tätig sind und über wirklich viele funktionierende Kundenbeziehungen verfügen, zufallen. Hintergrund für diese Prognose ist die Einschätzung, dass es den meisten Menschen sehr lästig sein wird, von immer anderen Betreibern immer neue Prepaid-Karten zu erwerben, wenn sie diesen Dienst nicht nur sporadisch sondern regelmäßig nutzen. Darüber hinaus sind die meisten Menschen auch nicht bereit mit mehreren Firmen vertragliche Bindungen einzugehen. Sie würden es vorziehen diesen

Dienst einfach nur als Zusatzdienstleistung eines ihrer bestehenden Dienstleister einzukaufen und über den schon vorhandenen Weg in Rechnung gestellt zu bekommen. Die Vermutung liegt nahe, dass die großen Mobilfunk- und Telekommunikationsbetreiber hier das Rennen machen werden.
Unter diesen Gesichtspunkten muss der WISP folgende Leistungen erbringen, um ein dauerhaftes Geschäftsmodell zu etablieren:

- Er muss mit den Zugangssystemen vor Ort kommunizieren können oder diese direkt selber aufstellen und betreiben.
- Er muss die einzelnen Lokationen einzeln verwalten können und Statistiken führen, diese müssten ggf. auch als Abrechnungsgrundlage mit dem Standortbetreiber fungieren.
- Er muss die Nutzung einzelnen Kunden erfassen und diese entweder selbst Abrechnen (auch Prepaid) oder geeignete Abrechnungsdaten erzeugen um diese elektronisch an den jeweiligen Serviceprovider zu übergeben.

Darüber hinaus sind weitere Faktoren wichtig, um die Kosten auf mittelfristige Sicht klein zu halten :

- Leichte Anbindung von Sekundärsystemen. Denn die Chance, dass sich in den nächsten Jahren z.B. ein Roamingstandard etablieren wird ist recht hoch, das System sollte also so ausgelegt sein, das es diesen später ohne große Probleme einbinden kann.
- Die eingesetzten Systeme, vor allem die vor Ort, sollten vom Ansatz her so wartungsarm wie möglich konzipiert sein. Dabei sollten sie wenn möglich schnell aufgebaut werden können und leicht aufrüstbar sowie aus der Ferne von zentraler Stelle her updatefähig sein, denn die nächsten technologischen Standards befinden sich bereits in der Pipeline der Hersteller.

Die Anforderungen der WISPS sind also recht komplex und vielschichtig, für die meisten wird sich wie so oft die Frage stellen: „Kaufen oder selber bauen…?“ (→HotSpot)

3.2. Lösungsansätze

Obwohl nur ein kleiner Teil der real existierenden potentiellen Nutzergruppen von mobilen Datendiensten vorgestellt wurde (weitere z.B. Bürokomplexe, Fabrikhallen, Lagerhäuser, Fuhrparks, Hafenlogistik,…) und obwohl die jeweiligen Interessen und Anwendungsgebiete grundverschieden sind, lässt die Faktenlage darauf schließen, dass all diese Nutzergruppen mit einer überschaubaren Anzahl an Lösungen befriedigt werden können. In jedem der verschiednen Fälle geht es ja lediglich darum Daten zu übertragen und dafür muss eine entsprechende Infrastruktur zur Verfügung stehen. Die verschiedenen involvierten Nutzerkreise definieren demnach die verschiedenen Lösungsszenarien.

3.2.1. Office / Privat

Für die Nutzung innerhalb von Büroräumen oder im privaten Umfeld bietet die mobile Datenkommunikation für alle Personen mit Laptops eine Reihe von Vorteilen: angefangen vom Wegfall der lästigen Kabel im Hinblick auf die kommenden multifunktionalen Büros über die freie Beweglichkeit der Mitarbeiter bis hin zum einfachen Angebot der Netzwerknutzung für Gäste. Allerdings sollte ein solches internes, mobiles Datennetz einige Grundanforderungen erfüllen, die je nach Art der Geschäftsräume unterschiedlich sind. Die Themen der Sicherheit bei der Datenübertragung und der funktionierenden Zugangskontrolle sind allerdings bei allen Einsatzgebieten von größter Wichtigkeit wohingegen ein überregionales Roaming generell uninteressant ist.

3.2.1.1. Home und Small Office (SOHO)

Für diesen Bereich kommt es vor allem auf die leichte Bedienbarkeit an, dabei ist es gleichfalls wichtig, verschiedene Funktionen abzudecken und zwar durch eine Lösung im „standalone“-Betrieb. Nicht ganz so hohe Priorität genießen dagegen Funktionen wie die Leistungsfähigkeit, da es in der Regel nur sehr wenige gleichzeitige

Nutzer gibt und meist auch kein Server oder ein hausinternes Netz zu bedienen ist, denn es handelt sich vornehmlich um die Bereitstellung des vorhandenen Internetanschlusses über drahtlose „Wege“.

3.2.1.2. Größere Bürokomplexe

In größeren Firmen sieht es da anders aus, hier ist vor allem die Performance, die Administrierbarkeit und die Updatefähigkeit einer Lösung gefragt, denn zum einen soll das interne Datennetz ebenfalls drahtlos bereit gestellt werden und zum anderen ist meist nur eine Person oder eine Abteilung für die Wartung und Pflege der Netze zuständig, was natürlich eine zentrale Verwaltung voraussetzt.

3.2.1.3. Verteilte Standorte einer Firma

Viele Firmen haben mehrere Standorte in einem Land bzw. weltweit. Für diese könnte es zumindest national wichtig sein, die Systeme über eine Zentraleinheit steuern zu können und dort eine gemeinschaftliche Administration, Nutzerverwaltung und Updateeinspeisung vorzunehmen. So könnte der Mitarbeiter aus München auch in Hamburg mit seinen normalen Zugangsdaten und Rechten ins lokale Netz. In den einzelnen Standorten gelten dann entweder die Anforderungen von 3.2.1.1 oder 3.2.1.2 je nach dem wie groß die einzelnen Außenstellen sind.

3.2.2. Gebäudekomplexe, teils öffentlich

Neben den Büros, wo nur Mitarbeitern der drahtlose Zugriff auf bestehende Netze angeboten werden soll, sind halböffentliche Gebäudekomplexe eine weitere potentielle Interessentengruppe.

Dabei geht es um die Bereitstellung eines kostenpflichtigen Zuganges für ständig wechselnde Nutzer und außerdem um die Möglichkeit die vorhandenen Systeme auch intern nutzen zu können. Zumindest für den internen Bereich ist dabei eine Sicherung der Datenübertragung unabdingbar.
Da dasselbe System von internen und externen Nutzern gleichzeitig bedient wird und da die internen Anwendungen meist eine größere Priorität genießen, sind zusätzlich die Themen der Zugangskontrolle, der Bandbreite und des „Quality of Service“ von gesteigerter Wichtigkeit.
Außerdem ist bei der Entwicklung der Zugangs– und Sicherheitssysteme darauf zu achten, dass auch nicht so leistungsstarke Endgeräte, die so genannten „Thin-Clients“, zum Einsatz kommen werden.

3.2.2.1. Hotel

Für Hotels wird es in absehbarer Zeit zum Standard gehören müssen, den Kunden einen Zugang zum Netz (in diesem Fall dem Internet) anzubieten. Gerade für bestehende Häuser, die die entsprechende Technologie nachrüsten müssen, bietet sich eine drahtlose Lösung an. Alle kabelgebundenen Varianten sind nicht nur sehr kostenintensiv, sie verursachen auch Baulärm, der den Betrieb stört.
Hotels wollen mit dem Betrieb des Netzes in erster Linie einen Mehrwert schaffen, mit dem man auch noch Geld verdienen kann. Dazu muss es möglich sein, Gästen erst nach deren Anmeldung den Zugang zu gewähren und ihnen die Nutzung anschließend in Rechnung zu stellen, entweder auf Basis eines Festpreises pro Tag oder je nach Nutzung. Da es sich bei den Nutzern vornehmlich um Geschäftsreisende handeln wird, ist darüber hinaus eine Sicherung der Daten auf der Funkstrecke von größter Wichtigkeit.
Die Möglichkeit das entstehende Hausnetzwerk auch selbst oder für Zusatzdienste (z.B. Video-On-Demand) zu nutzen, ist derzeit als eher Sekundär einzustufen, dies mag sich allerdings in Zukunft ändern.

3.2.2.2. Krankenhaus/ Rehakliniken

Kliniken, für die das Angebot an die „Kunden“ und die damit verbundenen Zusatzdienste, ähnlich wie bei den Hotels, sehr interessant ist, haben darüber hinaus ein deutlich größeres Interesse an einem Inhausnetzwerk. Nicht nur, dass ein Chat oder eine Spielplattform den Patienten zusätzlich angeboten werden könnten, gerade die Einbindung von PDAs und Laptops in den Ablauf des Arbeitstages birgt ein großes Potential für Zeiteinspaarungen. Diese könnte dann den Patienten zugute kommen.
Im ersten Schritt sind es vor allem die Schreibarbeiten und der Verwaltungsaufwand der optimiert werden könnte, in Zukunft ist natürlich auch die Einbindung von Medizintechnik denkbar. Bei diesen hoch sensitiven Daten ist es natürlich von größter Wichtigkeit, dass niemand unbefugt Zugriff erhält. Ein durchgehendes Sicherheits- und Authentifizierungskonzept ist unabdingbar.

3.2.3. HotSpots

Mit dem Begriff HotSpots werden derzeit Lokationen bezeichnet, an denen der drahtlose Zugang zum Internet mit eigenen Endgeräten möglich ist. So soll über die nächsten Jahre ein Netzwerk entstehen, das eine fast komplette Abdeckung der „interessanten“ Lokationen ermöglicht. Ziel ist es, im ersten Schritt vor allen den Businesskunden diesen Service anzubieten, natürlich gegen Bezahlung. Wenn so ein Netz einmal großräumig verfügbar ist, werden die Möglichkeiten groß sein, denn das Wissen, dass jeder Mitarbeiter problemlos und in absehbarer Zeit einen breitbandigen Internetzugang nutzen kann, ist für viele Firmen ein Angebot, aus dem sich neue Einsparpotentiale ableiten lassen.
Bevor es aber soweit ist, muss noch viel geschehen, vom Aufbau des Netzes, über entsprechende Roamingabkommen bis hin zu den Preisen und Geschäftsmodellen. Sicher ist allerdings, dass ein verteiltes System mit einer Zentraleinheit und einer Lösung, die den

drahtlosen Zugang vor Ort bereitstellt, gebraucht wird, um diesen Dienst zu ermöglichen. Die Zentralsysteme sollten untereinander vernetzbar sein, um die Roaming und Billingproblematik zu lösen, eine sehr einfache Bedienbarkeit ist von größter Wichtigkeit, denn es soll ja eine möglichst große Gruppe von Menschen angesprochen werden, auch die nicht technisch Begeisterten, und abgesehen davon möchte der Kunde natürlich seine Daten in guten Händen wissen, auch hier ist die Sicherheit Thema. Was in diesem Bereich dagegen eher zweitrangig ist, ist die Bandbreite. Nur sehr wenige HotSpots werden in den nächsten Jahren mit großer Bandbreite an das Internet angebunden werden, denn dafür besteht kein Grund, da nicht zu erwarten ist, dass es in naher Zukunft eine große Zahl gleichzeitiger Nutzer geben wird. Die „normale“ HotSpot-Installation dürfte so mit 768 kbit/s bis 2 Mbit/s angebunden sein- eine Bandbreite die aus technischer Sicht keine großen Probleme verursachen sollte.

3.2.4. Zusammenfassung

Die Vielzahl der denkbaren Einsatzszenarien und Nutzergruppen konnte erfolgreich in drei Klassen mit jeweils gleichen Merkmalen und Anforderungen aufgeteilt werden.
Wenn man die so klassifizierten Lösungsansätze jetzt etwas näher betrachtet, fällt auf, dass man im Wesentlichen nur zwei Komponenten braucht um all diese Anforderungen zu bedienen. Zum einen eine Lösung vor Ort, die den eigentlichen Zugang bereitstellt und die so flexibel ist, dass sie je nach Leistungsanforderungen auf verschiedenen Hardwarekomponenten läuft, um so je nach Anforderung an die Performance zu skalieren (von klein, kompakt und billig zu leistungsstark, robust und hochpreisig) und zum anderen eine Steuerkomponente, die über Intra- oder Internet eine Vielzahl der „Vor Ort Lösungen“ kontrollieren, managen und updaten kann. Zu erwähnen ist darüber hinaus, dass bei all den technischen Möglichkeiten und Lösungsansätzen eines nicht vernachlässigt werden darf: der spätere Nutzer. Und für diesen ist natürlich eine einfache

Bedienbarkeit der Lösung von größter Wichtigkeit. Ohne eine einfache Bedienbarkeit wird der Massenmarkt nie adressierbar sein und nur dort sind die Umsätze zu erzielen, die die Investitionen in diesem Bereich auch refinanzieren und lukrative Gewinne in Aussicht stellen.

3.3. Schlussfolgerung

Wie gezeigt, kann man die Bedürfnisse von fast allen Zielgruppen auf nur drei verschiedene Klassen von Lösungsansätzen herunterbrechen. Denn auch wenn natürlich Kriterien wie Größe und Leistung je nach Zielgruppe und selbst innerhalb einer Zielgruppe stark variieren, gibt es nur drei wesentliche Szenarien für kabellose Netzwerke: Die Nutzung unterwegs, im Büro bzw. Privat und innerhalb von halböffentlichen Gebäudekomplexen. Die Anforderungen zu den drei Szenarien wiederum weisen ebenfalls einige Gemeinsamkeiten auf. Herauszustellen sind hier die Themen: Zugangskontrolle mit zentraler Nutzerverwaltung, Sicherheit der übertragenen Daten, die Einfachheit der Bedienung, das Roaming und das Anbinden von Sekundärsystemen, um den Nutzen und die Zukunftsfähigkeit des Systems zu maximieren.
Gelingt es diesen Anforderungen mittels zweier in sich modularen Komponenten (Server und Hardware vor Ort) zu begegnen, so erhält man eine Lösung, die einen Großteil aller derzeit denkbaren Zielgruppen bedienen wird.

4. Mobile Techniken

Unter dem Oberbegriff der mobilen Techniken sind alle technischen Ansätze zusammengefasst, die eine örtlich nicht gebundene Datenkommunikation, also eine auf Funk-Basis beruhende, ermöglichen. Die einzelnen Ansätze sind dabei höchst verschieden, sei es in Punkto Bandbreite, Sicherheit, Hardwareanforderung oder Preis. Die individuellen Schwächen und Stärken sollen im Folgenden betrachtet und bewertet werden.

4.1. Mobilfunk

4.1.1. GSM

GSM (Global System for Mobilecommunication) ist der Mobilfunkstandard der 2ten Generation. Die erste Generation ist an dieser Stelle nur aus Kuriositätsgründen der Erwähnung wert. Zwar wurde schon 1926 auf einer Bahnstrecke die erste mobile Sprachkommunikation realisiert. Doch selbst Jahrzehnte später waren die ersten frei verfügbaren Geräte nicht wirklich als „mobil“ zu bezeichnen. Mit 18 Kg Gewicht und 2,5 Minuten Akkuzeit, mit heutigen Maßstäben nicht mal mehr zu messen. Etwas besser wurde es dann mit dem C- Netz der Telekom, dessen Geräte primär als Autotelefone eingesetzt wurden, aber auch diese sollen hier keine Erwähnung finden, denn erst mit GSM trat das Handy europa-, ja weltweit seinen Siegeszug an. Mittels GSM wurde die digitale Kommunikation möglich, was zur Folge hatte, das auf der einen Seite die Endgeräte sehr klein und auch sehr günstig wurden und auf der anderen Seite sich die Sprachqualität enorm verbesserte. Aufkommende Zusatzdienste wie Internet und vor allem SMS trugen ihren Teil zur explosionsartigen Verbreitung des Handys bei. Der Begriff Handy, der nichts mit dem englischen Original „mobile“ zu tun hat, ist im übrigen ein Kunstwort. Erstmalig von einem süddeutschen Radiosender bei einer Reportage benutzt ist es mittlerweile in aller Munde und zu einem Bestandteil der deutschen Sprache geworden, genau wie das Gerät ein fester Bestandteil der

heutigen Kommunikationsgesellschaft geworden ist. Parallel zu GSM stießen auch andere Datendienste wie z.B. das Internet auf gesellschaftliche Akzeptanz. Es war daher wichtig, in absehbarer Zukunft auch diesen Dienst über Mobilfunk anbieten zu können. Im Jahre 2000 konnten mittels CSD (Circuit Switched Data) nur eine Datenübertragung von 9,6 kbit/s über die GSM-Netze angeboten werden. Um den Übergang in die Dritte Mobilfunkgeneration einzuleiten wurden daher 1998 zwei neue Standards der Datenübertragung definiert. HSCSD (High Speed Circuit Switched Data) und GPRS (General Packet Radio Service). HSCSD ist dabei genau so wie CSD ein leitungsorientiertes (CS – Circuit Switched) und GPRS ein paketorientiertes (PS – Packet Switched) Übertragungsverfahren. GPRS erfordert allerdings im Gegensatz zum HSCSD eine komplett neue eigenständige Netzstruktur im Core Network (Vermittlungsnetz), die für ein Routing von Paketen geeignet ist. Der Vorteil von paketorientierten Diensten ist, dass ein logischer Übertragungskanal von mehreren Teilnehmern gemeinsam benutzt werden kann. [UMTS-Report][GSM-World]

4.1.2. HSCSD

HSCSD ist die wohl vorerst letzte Evolutionsstufe der leitungsorientierten Übertragungsverfahren. Um den Datendurchsatz gegenüber CSD zu steigern, werden mehrere auf einander folgende Zeitschlitze innerhalb des GSM- Netzes belegt. So kann eine Geschwindigkeit von bis zu 57,6 kbits/sec erreicht werden. Mittels HSCSD wird eine permanente Verbindung zwischen Sender und Empfänger etabliert. Dieses hat, im Hinblick auf Videokonferenzen, einen deutlichen Vorteil gegenüber paketorientierten Übertragungsverfahren, da eine feste Bandbreite garantiert werden kann. [UMTS-Report] [GSM-World]

4.1.3. GPRS

GPRS ist die erste Implementierung eines paketorientierten Übertragungsprotokolls, das über die GSM Netze funktioniert, denn diese sind im Kern leitungsorientiert und mussten daher umgestellt werden.
Der große Vorteil dieses Verfahrens gegenüber denen mit einer festen Verbindung liegt darin, dass das Netzwerk nur dann beansprucht wird, wenn es auch Daten zum versenden gibt, außerdem teilen sich mehrere Teilnehmer eine physikalische Leitung, was enorme Leitungskapazitäten einspart. Mit GPRS lassen sich Übertragungsraten von bis zu 115 kbit/s erzielen, was in einem Netz der 2. Generation durchaus akzeptabel ist.
Der größte Vorteil von GPRS liegt allerdings in seiner Kompatibilität zum Protokollstack des ISO/OSI-Schichtenmodelles, es ist also für TCP/IP- Übertragungen bereit [Tanenbaum]. Da auch die Netzwerke der 3. Generation mit packetorientierten Diensten arbeiten werden, war GPRS eine gute Vorbereitung in diese Richtung. Da ein großer Teil der Investitionskosten für GPRS durch einen geringeren Aufwand bei der Einführung der 3. Generation kompensiert wird, ist es allen Betreibern leicht gefallen diesen Schritt zu gehen. [UMTS-Report][GSM-World]

4.1.4. UMTS

UMTS ist der Mobilfunkstandard der dritten und neusten Generation und wird somit in Zukunft die 2. Generation (GSM) ablösen. Diese Ablösung wird allerdings nicht ganz so schnell vonstatten gehen, wie sich das die Netzbetreiber gewünscht hätten. Denn zum einen fehlt ihnen aufgrund der enormen Summen, die bei der Lizenzversteigerung ausgegeben wurden, das Geld den nötigen Netzaufbau so zügig wie gewünscht voranzutreiben, zum anderen sind auch die Mobiltelefonhersteller noch nicht so weit, eine große Auswahl an Geräten der 3. Generation vorzustellen. Man darf dabei nicht vergessen, dass zur Zeit der Versteigerung der Hype der „New Economy“ in vollem Gange war und damit verbunden natürlich auch

die Euphorie gegenüber dieser neuen Technologie entsprechend groß. Nun, da alle wieder auf den Boden der Tatsachen zurückgekehrt sind, ist das Frohlocken gewichen und die Netzbetreiber suchen händeringend nach Anwendungen, die auf Dauer ihren Invest doch noch refinanzieren. Allerdings ist die Suche nach diesen so genannten „Killer Anwendungen“ noch nicht so recht erfolgreich gewesen. Das beste Zugpferd innerhalb GSM war die SMS, etwas ähnliches gilt es jetzt auch für UMTS zu finden.

Vom technischen Standpunkt her ist der Ansatz, den UMTS verfolgt, durchaus zu begrüßen.

So war es die Zielsetzung des 1992 von der ITU (International Telecommunications Union) verabschiedeten Standards IMT-2000 (International Mobile Telecommunications at 2000 MHz), die Bandbreiten für den Datentransport extrem zu vergrößern, eine optimale Implementierung paketorientierter Datendienste zu gewährleisten und einen längst überfälligen weltweiten Standard zu etablieren.

Um dabei allen Nationen und vor allen den Netzinhabern entgegenzukommen und damit auch Teile der bestehenden Netze der 2. Generation für den neuen Standard wieder verwendet werden können, wurden mehrere länderspezifische Varianten (siehe Bild 1) eingegliedert und die angestrebten Ziele somit aufgeweicht. Auch wenn der Standard es vorsieht, dass die verfügbaren Endgeräte alle einzelnen Ausprägungen unterstützen, wird dies zumindest in der Anfangsphase wohl nur ein Wunsch bleiben. Bevor also ein echter weltweiter Standard etabliert ist, wird es noch einige Zeit dauern.

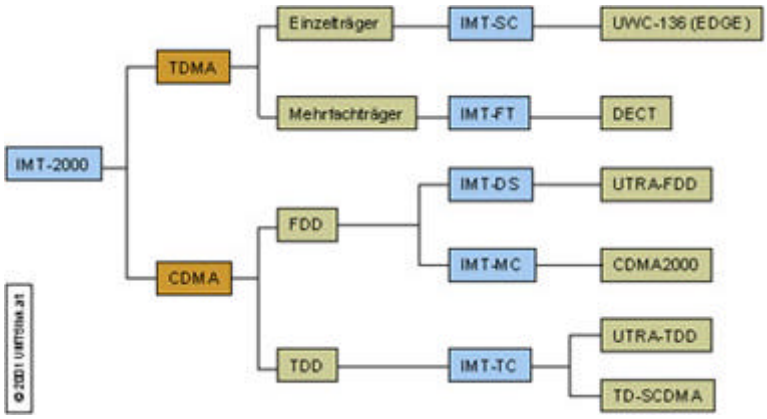


Abbildung 1 IMT-2000, [UMTS-Report]

Für UMTS, also primär für den europäischen Raum, sind die zwei Technologien UTRA-FDD (UMTS Terrestrial Radio Access – Frequency Division Duplex) und UTRA-TDD (UMTS Terrestrial Radio Access – Time Division Duplex) relevant. Der Begriff „Terrestrial“ bezieht sich dabei auf Bodenstationen, bei IMT-2000 ist prinzipiell auch an Satellitenanbindung gedacht und dafür sind auch eigene Frequenzbereiche reserviert worden. Die Normen für die Satellitenkommunikation sind jedoch noch nicht entschieden.
Die einzelnen mobilen Dienste, die im IMT-2000 Standard zusammengefasst wurden, sind verschiedenen Frequenzbereichen zugeordnet. Unter „Uplink“ versteht man die Kommunikationsrichtung vom Mobiltelefon zur Bodenstation und unter „Downlink“ den umgekehrten Weg vom Netz zum Mobiltelefon.

Frequenzbereich [MHz]	Verwendungszweck
1710 – 1785	DCS-1800 Uplinkband (Digital Cellular System = GSM 1800)
1805 – 1880	DCS-1800 Downlinkband
1880 – 1900	DECT - Digital Enhanced Cordless Telecommunications
1900 – 1920	UTRA-TDD (4x 5MHz-Bänder)
1920 – 1980	UTRA-FDD Uplink (12x 5MHz Bänder für Uplink)
1980 – 2010	MSS Uplink (Mobile Satellite Service)
2010 – 2020	UTRA-TDD unlizenzierter Betrieb (2x 5MHz Bänder)
2020 – 2025	UTRA-TDD (1x 5MHz Band)
2110 – 2170	UTRA-FDD Downlink (12x 5MHz Bänder für Downlink)
2170 – 2200	MSS Downlink (Mobile Satellite Service)

Tabelle 1 UMTS-Frequenzbänder, [UMTS-Report]

Bei dem innerhalb von UMTS so wichtigen UTRA-FDD System besteht jedes Frequenzpaket aus einem eigenen Uplink- und einem Downlink Frequenzband von je 5MHz, ein Band für das „Sprechen“ und ein Frequenzband für das „Hören“. Daher spricht man bei UTRA-FDD auch von „gepaarten“ Frequenzpaketen. Das ebenfalls relevante UTRA-TDD System besteht hingegen aus nur einem 5MHz Frequenzband, über das Uplink- und Downlink-Kommunikation per Zeitmultiplex realisiert werden und das daher als „ungepaartes“ Frequenzpaket bezeichnet wird. Fasst man die obere Tabelle (Tabelle 1 UMTS-Frequenzbänder) ins Auge, so sind für UMTS zwei mal 60MHz für FDD-Dienste und insgesamt 25MHz für lizenzierte TDD-Dienste reserviert. Es können daher für die UMTS-Frequenzlizenzen genau 12 gepaarte (60MHz/5) und 5 ungepaarte Frequenzpakete versteigert werden. Dabei sind jedoch für einen effizienten Netzbetrieb mindestens zwei gepaarte Frequenzpakete notwendig. Somit blieben für die Versteigerungen im Jahre 2001 nur 6 Lizenzen. Da es aber 11 Bieter gab, erklärt das die enormen Summen die erzielt wurden.

Was die zukünftigen Nutzer angeht, wird es wohl erstmalig verschiedene „Klassen“ von Mobilfunknutzern geben. UMTS sieht drei verschiedne Gruppen vor: Gold-, Silber- und Braun– Kunden. Den Goldkunden wird eine Datenrate von 384 kbits zur Verfügung gestellt und eine von 144kbits garantiert, ausserdem werden sie bei der Kanalvergabe bevorzugt behandelt. Den Silber-Kunden sowie den Braun-Kunden wird eine maximale Datenrate von 144 kBit/s zugestanden, dabei wird den Silber-Paket-Inhabern 64 kBit/s garantiert, den „Braunen“ ganze 16 kBit/s. Die Maximaldatenrate von 2MBit/s wird vorerst wohl nur an sehr wenigen Orten überhaupt zur Verfügung stehen und noch seltener nutzbar sein. [UMTS-Report] [GSM-World]

4.2. Bluetooth

Bluetooth wurde entwickelt, um unsere hoch moderne Kommunikationsgesellschaft von einem der letzten „Fossilien“ zu befreien, dem Kabel. Bereits 1994 von der Firma Ericsson angedacht, wurde Bluetooth 1998 von der Spezial Interest Group (SIG), die von den Großkonzernen Ericsson, IBM, Intel, Nokia und Toshiba gegründet wurde, umgesetzt. Benannt ist es übrigens nach einem dänischen König (Harald Blåtand (Bluetooth)), der während seiner Zeit (911-986) die verschiedenen Stämme zu einem Königreich einte. Die symbolische Analogie zu dem, was mit Bluetooth bewirkt werden soll, liegt auf der Hand, denn ähnliches hat Bluetooth mit der Kommunikation zwischen PC’s, Peripherie und portablen Geräten vor: sie zuvereinheitlichen.
Wie die verschiedenen Einsatzgebiete schon andeuten, geht es dabei primär um die übergreifende Kommunikation von verschiedensten Geräten. Von der Maus, über den Druckeranschluss, bis zum Display, vom Handy über den PDA, bis zum Laptop. Die einzelnen Geräte, wenn entsprechend konfiguriert, bauen dabei ihre drahtlosen Netzwerkverbindungen ganz automatisch auf, denn Bluetooth-Geräte suchen einander. In der Regel wird dem Nutzer signalisiert, dass ein anderes Gerät den Wunsch hat, eine Verbindung aufzubauen. Der Nutzer muß die Verbindung dann akzeptieren, doch dieser Prozess ist zwischen bekannten Geräten auch automatisierbar. Durch weltweit einmalige Seriennummern (48 bit), findet dabei die Identifizierung des Gegenübers statt. Es können bis zu 8 Geräte gleichzeitig, wechselseitig miteinander kommunizieren und bilden so genannte „Pico-Netze“. Insgesamt können 127 Geräte in einem Netzwerk miteinander verbunden sein. Der Initiator des Ganzen (erstes Gerät, das Verbindungsaufbau wünschte) ist automatisch der Master.
Als Frequenzband benutzt Bluetooth das lizenzfreie ISM-Band im 2,45 GHZ Bereich mit einer maximalen Abstrahlleistung von 100mW. Diese wird allerdings nur mittels zusätzlicher Leistungsverstärker erreicht und hat eine maximale Reichweite von 100 m bei einer Übertragungsgeschwindigkeit von bis zu einem MBit. Da Bluetooth praktisch in allen elektronischen Geräten zum

Einsatz kommen soll, wurde bei der Entwicklung auf vier wesentliche Punkte Wert gelegt:

1. extrem kleine Baugröße
   ca. 9 mm Kantenlänge der „Platine“ (siehe Bild)
2. sehr geringer Energiebedarf
   vom Sleep-Modus mit 30 Mikroampere bis zum Sende-Modus mit 3 bis 30 Milliampere
3. niedrige Produktionskosten
   derzeit bei um die 5 Dollar pro Modul
4. eingebaute Sicherheit
   Realisiert durch ein Frequenzhopping von 1600 Hops pro Sekunde, die im Challenge/Response – Verfahren mit bis zu 128 bit verschlüsselt werden können

Die Verbreitung von bluetooth-fähigen Geräten schreitet schnell voran, eine gute Aussicht für die Zukunft dieser Technologie. [UMTS-Report][GSM-World]

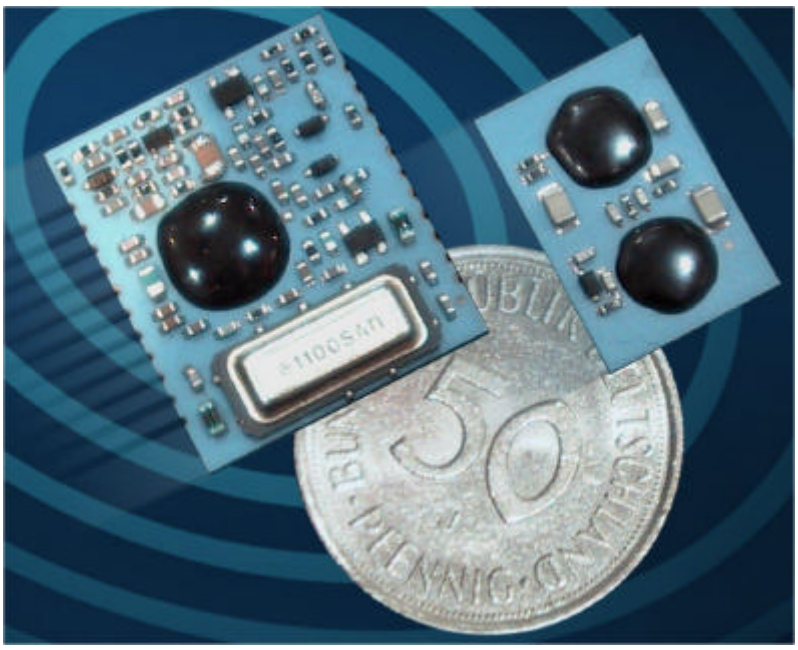


Abbildung 2 Baugröße Bluetooth [Storz]

4.3. WLAN Überblick

WLAN ist ein weltweiter Standard, der eine schnelle, kabellose Übertragung von Daten innerhalb einer bestimmten Zone erlaubt. Das System besteht aus einem Funkverteiler (AccessPoint, AP) und einer Empfangs/Sendekarte. Diese Karte gehört mittlerweile zum festen Bestandteil jeder neuen PDA- und Laptopgeneration und wird so innerhalb weniger Jahre eine fast vollständige Verbreitung erreichen. Es gibt zwei grundsätzliche Systemmodi, den „adhoc“ – Modus, der direkt zwei Endgeräte über zwei Karten miteinander verbindet und den Infrastrukturmodus, bei dem ein oder mehrere Endgeräte über die Karte mit einem Funkverteiler kommunizieren und über diesen ein gemeinsames Netzwerk bilden. Auf Seite der Zugangspunkte (Funkverteiler) gibt es verschiedne Einsatzszenarien. Zum Ersten sind da die privaten AccessPoints, die ihrem Besitzer den drahtlosen Zugang zum eigenen, hausinternen Datennetz ermöglichen. Zum Zweiten nutzen immer mehr Firmen diese Technologie, um ihren Mitarbeitern einen nicht ortsgebundenen Zugang zum Netzwerk bereit zu stellen und gleichzeitig die Flexibilität ihrer Büroräume zu erhöhen. Zum Dritten gilt es die öffentlichen Zugänge zu erwähnen. Die so genannten „HotSpots“ entstehen an immer mehr Orten mit viel Publikumsverkehr und sollen dort in Zukunft allen interessierten Nutzern, gegen ein gewisses Entgelt, einen Zugang zum Internet ermöglichen.

Alle drei Einsatzgebiete weisen derzeit starke Zuwachszahlen auf, in Kombination mit der weiter wachsenden Verbreitung der Empfangskarten und der Tatsache, dass ein paar große „Player“ auf dem IT-Markt diese Technologie derzeit extrem „pushen“[1], ist die Chance einer großen Marktdurchdringung von WLAN extrem hoch.

Ein weiterer Pluspunkt ist, dass nicht nur eine Reihe von Herstellern bereits in die Produktion der Hardware eingestiegen sind und daher die Preise in den beiden letzten Jahren um mehr als 500% gefallen sind, sondern dass auch die Datenraten immer höher werden. Dabei kann WLAN als „Ethernet über die Luft“ betrachtet werden und ist

[1] Namentlich Intel mit seiner „Centrino“ Technologie und Microsoft, die WLAN, im Gegensatz zu Bluetooth, standardmäßig unterstützen.

somit von der Grundlage her für die eingesetzten Anwendungen und Programme keine völlig neue Technologie, die es zu integrieren gälte. Dies bringt auf der einen Seite zwar eine größere Akzeptanz mit sich, die sich natürlich positiv auf zu treffende Kaufentscheidungen auswirkt, ist auf der anderen Seite allerdings auch gefährlich, da über den kleinen Zusatz „über die Luft“ und die damit verbundenen Risiken und Sicherheitslücken nicht alle Verantwortlichen in den Firmen und noch weniger Heimanwender nachdenken.
Leider wurde bei der Standardisierung von WLAN manches nicht bedacht, z.B. die Ausrichtung auf Echtzeitanforderungen und ein „Quality of Service“ fehlen komplett. Natürlich war dieser Schritt aufgrund der Kompatibilitätsanforderung zum Ethernet nur schwer zu gehen, aber vielleicht hätte man sie als Zusatzfunktion für geschlossene WLAN-Netze mit vorsehen können. Wie dem auch sei, Tatsache ist, dass heutzutage einige Firmen versuchen, eben diese Funktionalitäten „nachzurüsten“, aber bisher ohne Erfolg. Das Ethernet ist nun einmal per Definition nicht echtzeitfähig und damit sind die Chancen seiner drahtlosen Erweiterung ebenfalls sehr gering.
An dieser Stelle sei eins noch angemerkt: WLAN wird des Öfteren fälschlicherweise mit WI-FI in einen begrifflichen Topf geworfen. Dies ist allerdings mitnichten so, denn Wi-Fi ist lediglich eine Non-Profit-Organisation, die für eine Hersteller übergreifende Interoperabilität der einzelnen WLAN-Produkte eintritt und somit „nur“ den Weg für eine schnelle Verbreitung dieser Technologie ebnet. [TOM1]

4.4. Vergleiche

Zunächst soll eine Grafik die unterschiedlichen Einsatzgebiete und Datendurchsatzraten der Technologien nochmals verdeutlichen
:

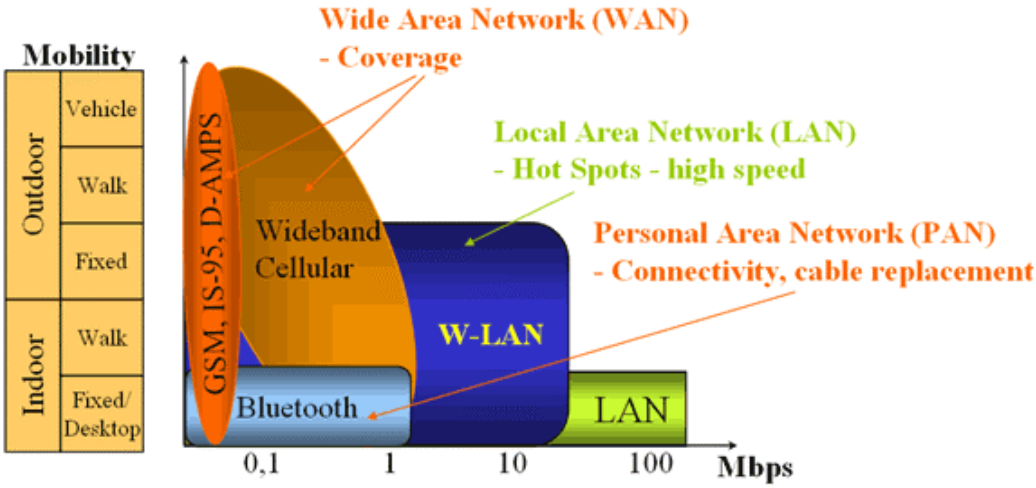


Abbildung 3 Einsatzgebiete mobiler Übertragungstechniken, [TOM1]

Bereich/ Technologie	Mobilfunk	Bluetooth	WLAN
Kosten	Sowohl die Sendeantennen, die Endgeräte und die Datenübertragung sind derzeit noch sehr teuer. Da darüber hinaus die Lizenzkosten für UMTS extrem hoch waren, wird	Das Sendeequipment ist extrem billig (ca. 5 Euro) die Datenübertragung kostet prinzipiell ebenfalls nichts, selbst der Stromverbrauch ist zu vernachlässigen.	Die Funkverteiler und die Empfangskarten sind im mittleren Preisniveau. Der Traffic ist im eigenen Netz natürlich kostenlos, wird in Zukunft „unterwegs“, also an HotSpots wohl aber Geld kosten.

	vermutet, das sich daran auch in Zukunft nichts ändern wird.		
Verfügbarkeit	Die Netzabdeckung ist in Mitteleuropa fast als komplett zu bezeichnen. Nur sehr entlegene Gebiete sind noch nicht erschlossen.	Es bestehen derzeit noch keine echten Bluetoothnetze, die eine Abdeckung garantieren. Die Verfügbarkeit ist allerdings sofort vorhanden, sobald sich 2 bluetooth-fähige Geräte innerhalb der Reichweite befinden.	Bis dato existieren nur die ersten HotSpots an ausgewählten Plätzen, die eine Nutzung des Internets für jedermann ermöglichen. Allerdings gehen fast alle Experten davon aus, dass sich dies in der näheren Zukunft ändern wird.
Datenrate	114 kBit/s im GPRS, zukünfitg bis zu 2 MBit/s mit UMTS	Bis zu 1MBit/s	Verbreitet ist derzeit 11 und 22 MBit/s, 54 MBit/s ist im kommen, über 100 MBit/s bereits in Vorbereitung.
Reichweite	Ca. 500-2000m um die Sendemasten herum. Allerdings sinken mit steigender Teilnehmerzahl auch die Bandbreiten.	10 m (100 m mit Verstärker)	Je nach Bebauung der Umgebung zwischen 30 und 300 m. Auch hier teilen sich alle Teilnehmer die Bandbreite.

Einsatzmöglichkeiten	Bis dato für den Mobilfunk und die Kurzkommunikation (SMS) eingesetzt, soll UMTS auch das Internet mobil verfügbar machen.	Vor allem bei der Kommunikation auf kurzen Wegen. z.B. vom Mobiltelefon zum Headset oder zwischen zwei Mobiltelefonen(PAN, Gerät zu Gerät), allerdings auch um Daten vom PDA mit einer Basisstation abzugleichen. Die Nutzung von Internet über Bluetooth ist aber wohl vorerst nicht zu erwarten.	Im Privat- und Firmenumfeld wird es Teilwiese wohl das kabelgebundene Ethernet ablösen, mit einer zunehmenden Verbreitung an öffentlichen Orten wird es darüber hinaus wohl UMTS bei der Bereitstellung von Internet Konkurrenz machen. Die Verbindung mobiler Geräte mit einer vorhandenen Infrastruktur wird wahrscheinlich ihre Hauptaufgabe sein.
Störanfälligkeit	Da die Funkfrequenzen nur für die Mobilfunkstandards reserviert sind, wird diese Technik nur durch viel Metall oder dicke Wände gestört.	Da es im Lizenzfreien ISM (Industrie, Scientific, Medicine) – Band sendet, gibt es eine gewisse Störanfälligkeit durch Quellen die das gleiche Band nutzen. Durch das extreme Frequenzhopping hält sich diese allerdings in Grenzen.	Wie auch Bluetooth benutzt WLAN das ISM-Band. Da es aber kein Frequenzhopping oder andere ähnliche Mechanismen gibt, ist die Störanfälligkeit als recht hoch zu bezeichnen. Gerade auf längeren Strecken reicht manchmal schon ein großer Gegenstand aus Metall, um die Übertragung zu beeinträchtigen.
Sicherheit	Durch die SIM-Karte ist eine gute	Neben dem Frequenzhopping, sieht Bluetooth	Das mit in die Spezifikation integrierte Verfahren (WEP) ist als

	Authentifizierung möglich, zudem findet atandardmäßig eine Verschlüsselung der Daten auf der Funkstrecke statt	optional eine starke Verschlüsselung der Daten vor.	unsicher einzustufen. Allerdings steht einer Nutzung anderer Verschlüsselungs-techniken und Rahmensysteme nichts im Wege.
Roaming	Da es nur recht wenige Mobilfunkprovider gibt, haben diese sich mittlerweile selbst international auf entsprechende Abkommen geeinigt. Das Roaming von Funkzelle zu Funkzelle ist ebenfalls kein Problem.	Roaming ist für Bluetooth derzeit noch kein Thema, da die Verbindungen immer direkt zwischen den Teilnehmern bestehen.	Das Roaming zwischen zwei AP's ist kein Problem, solange sie sich in einem gemeinsamen Netz befinden. Sind verschiedene Netze, verschiedener Betreiber involviert ist noch keine Lösung in Sicht. Woran allerdings gearbeitet wird, ist der Versuch, die Netze verschiedener Betreiber für alle Kunden zugänglich zu machen
Quality of Service	Die benötigten Bandbreiten werden durch den Standard zugesichert. Wenn nicht durch äußere Umstände die Übertragung unterbrochen wird, sind	Sogar höhere Bandbreiten als die, die für eine einfache Sprachqualität benötigt würden, können durch den Standard zugesichert werden, Bluetooth verfügt	Es ist im WLAN keine Priorisierung und keine feste Bandbreitenzusicherung vorgesehen. Cisco ist derzeit der einzige Hersteller, der natürlich nur in Verbindung mit entsprechenden Cisco-Empfangskarten, einen Accesspoint mit QoS

	Responsezeiten für Sprachqualität garantiert	unter anderem sogar über drei komplette Sprachkanäle.	anbietet.
Unterstützung der Big-Player (IBM, Microsoft, Intel ….)	Alle Mobilfunkgerätehersteller setzen ausschließlich auf diesen Standard. Allerdings ist die Einbettung und Unterstützung von GSM-Modulen in Notebooks und PDA's bisher noch kaum vorangeschritten. Dies könnte sich allerdings mit UMTS ändern.	Bluetooth wurde in der vergangenen Zeit sehr Stiefmütterlich behandelt, wenn es um entsprechende Softwareunterstützungen ging. Mittlerweile findet es aber zunehmend Verbreitung und damit steigt auch die Beachtung	WLAN wurde in den letzten Jahren extrem „gepusht". Sowohl was die Unterstützung von Softwareseite angeht, als auch die Hardwareintegration in Notebooks und PDA's. Intel hat im Chipsatz „Centrino" sogar WLAN fest integriert, und somit den Stromverbrauch extrem minimiert.
Fazit	In vielen Bereichen der mobilen Datenkommunikation wird vorerst kein Weg am Mobilfunk vorbeiführen. Da die entsprechenden Frequenzen allerdings kostenpflichtig und vergeben	Bluetooth wird im Bereich der PersonalAreaNetworks noch allerlei zu Wege bringen. Das Bedienen vieler verschiedener technischer Haushaltsgeräte über nur ein Kontrollgerät wird wahrscheinlich dazu gehören.	WLAN hat einige Schwächen, die allerdings zum großen Teil durch entsprechende Rahmensysteme kompensiert werden können. Wenn eine sinnvolle Erweiterung der Standards gelingt, hat WLAN durchaus die Chance, UMTS in vielen Bereichen die Show zu stehlen. Ob dies allerdings gelingt, wird erst die Zukunft zeigen.

	sind, werden sich auch in Zukunft nur wenige auf diesem Markt agieren. Das Interesse diese Technologie voran zu treiben, wird bei allen anderen dementsprechend gering sein.	Auch auf anderen Sektoren der Kurzstrecken-kommunikation wird Bluetooth eine Zukunft haben.	Jedenfalls die extrem wichtigen Faktoren „Preis“ und „Bandbreite“ sprechen für diese Technologie; ob UMTS diese durch entsprechende Angebote wie z.B. Flatrates kompensieren kann und will bleibt ebenfalls abzuwarten.

[UMTS-Report] [GSM-World] [TOM1]

4.5. Schlussfolgerungen

Alle drei Technologien haben, wie nicht anders zu erwarten war, ihre Stärken und ihre Schwächen. Dabei ist vom heutigen Standpunkt aus nur schwer zu sagen, welche der Technologien das Rennen machen wird, zumal sie ja nicht in allen Bereichen direkte Konkurrenten sind, sondern sich in einigen Fällen eher ergänzen. Für unsere Zielgruppen und angedachten Einsatzgebiete jedoch fällt die Entscheidung relativ leicht.

UMTS ist ein Feld, das zum einen nur die großen Telkos bestellen dürfen, da diese die Lizenzen innehaben, und zum anderen ist UMTS eine Technologie, die flächendeckend zum Einsatz gebracht wird. Dies ist zwar prinzipiell keine schlechte Sache, es wird von unserer Seite jedoch bezweifelt, dass es derzeit eine Notwendigkeit für schnelle Datenkommunikation an jedem beliebigen Ort gibt. Es werden wohl eher gewisse Lokalitäten und Ballungszentren sein, an denen auf ein solches Angebot zurückgegriffen wird. Die Wirtschaftlichkeit einer solchen Unternehmung ist also zumindest in den nächsten Jahren zu bezweifeln. Daher entscheiden wir uns dagegen.

Bluetooth hat zwar einige sehr schöne Features, aber die Reichweiten sowie die Übertragungsraten sind nicht in dem Bereich, wie es unsere Zielgruppen erfordern, man müsste mit Bluetooth sehr viele Zugangspunkte schaffen, die dann wiederum mit Hilfe von Kabeln verbunden werden müssten. Der Vorteil gegenüber dem Kabel wäre dann eher klein.
Bleibt WLAN. WLAN hat zwar ebenfalls einige Schwächen, aber für uns überwiegen die Vorteile der hohen Datenraten in einem lizenzfreien Frequenzband gepaart mit dem starken Engagement großer „Player“ für diese Technik, die weltweit standardisiert ist. Letzteres will heißen, dass die Empfangskarten aus Japan funktionieren auch in Deutschland, was wiederum bedeutet, dass jede damit verbundenen Dienstleistung ohne Probleme auch den internationalen Kunden und Reisenden angeboten werden kann. Zudem liegt, unserer Meinung nach, das Haupteinsatzgebiet für schnelle Übertragungen von großen Datenmengen immer noch in lokal begrenzten Räumlichkeiten, in denen man zwar mobil ist (Gehen), aber nicht gleichzeitig beispielsweise Auto fährt. Ausserdem ist der WLAN-Markt nicht reglementiert und jeder hat auf ihm die gleichen Rechte und Möglichkeiten. All diese Kriterien lassen für uns das Pendel in Richtung WLAN ausschlagen. [UMTS-Report] [GSM-World] [TOM1]

5. WLAN

Nun also der etwas genauere Blick auf die Technologie Wireless LAN.
Hinter dem Begriff Wireless LAN (WLAN) verbirgt sich eigentlich nur ein Vertreter der Produktgruppe der Radio-LANs (R-LAN), zu der auch noch Systeme wie z.B. das HiperLAN gehören. Allerdings können die anderen Systeme derzeit getrost vernachlässigt werden, da sie entweder in der Entwicklung eingestellt wurden oder es für sie kaum Produkte gibt, die den Markt ankurbeln könnten.
WLAN und die anderen Verfahren basieren auf dem Standard IEEE802.11 der nach der stolzen Arbeitszeit von zwölf Jahren 1997 beschlossen und publiziert wurde.

Dieser erste drahtlose WLAN-Standard definierte die technologischen Grundlagen für die Produktion von Geräten und wurde mit sieben grundsätzlichen Zielvorgaben ins Leben gerufen:

1. Es sollte eine Entfernung zwischen 3 und 300 Metern überbrückt werden können, um den typischen Ausdehnungen von Arbeitsgruppen gerecht zu werden.
2. Die Datenraten sollten mindestens denen des klassischen Shared-Ethernet entsprechen, die bei 1 MBit/s liegen.
3. Die Kompatibilität zu Ethernet IEEE802.3 sollte gewährleistet sein, damit eine einfache Integration via Bridges in bestehende Netzwerkstrukturen ermöglicht wird.
4. TCP/IP Unterstützung
5. Die Nutzung eines möglichst weltweit lizenzfrei verfügbaren Frequenzbandes war eine wichtige Vorgabe, denn nur so konnte eine rasche Marktpenetration mit großen Stückzahlen und damit einhergehend moderaten Preisen erzielt werden.
6. Ein robustes Übertragungsverfahren sollte gefunden werden.
7. Ein in weiten Bereichen akzeptierter Industriestandard sollte Verwendung finden.

Dabei beschränkte man sich auf die Definition der unteren beiden Ebenen des OSI-Schichtenmodells. Neben dem gemeinsamen Medienzugriffsprotokoll (Media Access Protocol) wurden so drei physikalische Schichten definiert :

- Infrarot (IR)
- Frequency Hopping Spread Spectrum (FHSS)
- Direct Sequence Spread Spectrum (DSSS)

Diese wurden später noch um eine vierte erweitert, dem OFDM (Orthogonal Frequency Division Multiplexing). Dieses Verfahren war nötig, um höhere Datenübertragungsraten zu realisieren.

Es gibt zwei nebenläufige Standards, die in verschiedenen Frequenzbändern senden. Eine „a“-Reihe, die im 5 GHz Bereich arbeitet und von Beginn an auf den Einsatz von OFDM setzte und

eine „b“- Reihe, die im 2,4 GHz Bereich arbeitet und anfänglich auf DSSS oder FHSS setzte, aber in ihrer Erweiterung, dem „g“ – Standard durch die Anforderung an eine höhere Datenrate ebenfalls auf OFDM umschwenken musste. Sowohl auf die Übertragungstechnologien, als auch auf die verschiedenen Standards soll in den nächsten Kapiteln noch näher eingegangen werden.

Allen Standards ist allerdings gemein, dass ein WLAN-System aus mindestens zwei Komponenten besteht: einem Funkverteiler und einer Empfangskarte (oder zwei Empfangskarten). Der Funkverteiler, Accesspoint genannt, sorgt dabei für einen „Übergang“ zwischen der kabelgebundenen- und der kabellosen Übertragung. Er wird mit standardkonformen Ethernet versorgt und stellt dieses dann über die Luft bereit. Das Gegenstück, die Empfangskarte, kann als Extramodul an gängige Endgeräte angeschlossen werden (z.B. via USB, PCI, miniPCI, PCMCIA, …) und ist mittlerweile bei vielen neueren Modellen schon serienmäßig integriert. (Laptop, PDA).

Ein Accesspoint kann dabei stets mehrere Empfangskarten gleichzeitig bedienen (1:N, wobei N je nach Hersteller variiert) eine Karte hingegen, kann zu einem Zeitpunkt immer nur mit einem Accesspoint kommunizieren. Es gibt zwei unterschiedliche Modi, den Infrastrukturmodus, der wie gerade beschrieben die Bereitstellung eines vorhandenen Netzwerkes über einen Accesspoint an die Karten vorsieht und den „Ad-Hoc“ – Modus, bei dem zwei Karten (und damit zwei Endgeräte) direkt miteinander kommunizieren, ohne dass ein Accesspoint oder eine weitere Netzwerkkomponente im Spiel wäre.

Im Infrastrukturmodus ist ferner vorgesehen, dass die Karten automatisch zu einem weiteren Accesspoint wechseln, wenn dieser sich im gleichen Netz befindet und eine bessere Erreichbarkeit hat. (z.B.: niedrigere Auslastung oder höhere Sendestärke). Hierbei spricht man vom „Roaming“ zwischen Accesspoints innerhalb eines Netzes, das für den Nutzer völlig transparent von statten geht. Dieses hat mit dem Roaming zwischen den Netzen verschiedener WLAN-Anbieter, wie es unter Punkt 5.5 dargelegt ist, allerdings nichts zu tun. [TOM1]

5.1. Die physikalische Ebene

Infrarot ist zwar im Standard 802.11 als Übertragungsmedium definiert, kommt aber im WLAN-Umfeld nicht zum Einsatz, daher soll an dieser Stelle nicht näher darauf eingegangen werden[2]. Die im WLAN – Umfeld zum Tragen kommenden Verfahren sind in erster Linie das FHSS, das DSSS und das OFDM, die jetzt im einzelnen etwas näher vorgestellt werden sollen.

5.1.1. DSSS - Direct Sequence Spread Spectrum

Das DSSS ist ein Spreizbandverfahren, was bedeutet, dass das eigentliche Datensignal auf eine größere Bandbreite aufgefächert und dann als solche übertragen wird. In der Praxis wird idealerweise ein Faktor von (mindestens) 10 benutzt. Um die Toleranz gegenüber Störungen weiter zu maximieren, wird jedes einzelne Bit als 11 bittige Codesequenz übertragen (hier Barker Code), wobei der normale Code die digitale „0“ wiedergibt und der Inverse die digitale „1“. Ein Nachteil sticht sofort ins Auge: die nicht optimale Ausnutzung der Bandbreite. Auf der anderen Seite gibt es aber auch einige entscheidende Vorteile:

Als erstes wäre hier die Toleranz gegen Störungen zu nennen. Im Gegensatz zu Frequenzhopping-Verfahren ist es meist möglich, das Signal selbst bei einer 3 Mal so großen Störgröße noch sicher zu demodulieren. Zudem ist das DSSS ein sehr energiesparendes Verfahren, das darüber hinaus sehr schnell beim Verbindungsaufbau ist. Die weiteren Tatsachen, wie eine größere Reichweite und vor allem eine höhere maximale Bandbreite (bis zu 11 MBIT) als FHSS haben dazu geführt, dass es der „Quasi-Standard“ im WLAN–Umfeld geworden ist. [DAFU][CCC1]

[2] Weiterführende Informationen finden Sie z.B. auf www.irda.org

5.1.2. FHSS (Frequency Hopping Spread Spectrum)

Ähnlich wie das DSSS ist auch das FHSS ein Spreizbandverfahren mit den schon genannten Vorteilen. Der größte Unterschied beider liegt im Frequenzhopping. Das FHSS wechselt pseudozufällig mindestens 20 mal pro Sekunde seine Sendfrequenz, was ein komplexeres Synchronisationsverfahren erfordert. In einem Szenario ergibt sich allerdings auch ein Vorteil in Bezug auf die Störanfälligkeit: Bei feststehenden Störquellen, wie z.B. Mikrowellengeräte oder anderen FHSS- Sendern, kommt es zu weit weniger Verlusten, da nur sehr wenig auf der „gestörten“ Frequenz übertragen wird. Die Vor- und Nachteile zu DSSS sind fließend, aber die etwas geringere Reichweite und die maximale Bandbreite von 2Mbit haben dazu geführt, dass sich DSSS durchgesetzt hat. Beide Verfahren, werden auch heute noch im 2,4 GHz Bereich eingesetzt, DSSS bei WLAN, FHSS bei Bluetooth. [CCC2]

5.1.3. OFHS (Orthogonal Frequency Division Multiplexing)

Da sich DSSS für 802.11b am oberen Limit der Leistungsfähigkeit bewegt, der Markt aber nach höheren Bandbreiten ruft, musste für den ebenfalls im 2,4 GHz Bereich arbeitenden 802.11g Standard auf das eigentlich im 5 GHz Bereich eingesetzte Verfahren OFHS ausgewichen werden.

Das theoretische Konzept von OFHS ist schon recht alt (ca. 30 Jahre), allerdings konnte erst durch die enormen Forschritte in der Mikroelektronik und der Signalverarbeitung an einen Einsatz in der Praxis gedacht werden (ca. seit 10 Jahren). Mittlerweile ist das Verfahren recht weit verbreitet[3]. Es beruht, wie andere Mehrträgersysteme auch, auf dem grundsätzlichen Prinzip, die Übertragung eines (oder mehrerer) breitbandigen Signale in die

[3] Das Verfahren wird unter Aanderem eingesetzt in: Digital Video Broadcasting (DVB), Digital Audio Broadcasting (DAB), x Digital Subscriber Line (xDSL), Power Line Communications (PLC)

Übertragung von vielen schmalbandigen orthogonalen Signalen zu überführen.

Der Datenstrom wird in viele parallele kleinere Datenströme zerlegt und jeder einzelne dieser Teilströme wird auf einem eigenen Unterträger gesendet. Die Unterträger sind orthogonal zu einander und da ein bestimmter Frequenzabstand eingehalten wird erreicht man, dass sich die einzelnen Träger überlappen dürfen, denn die Orthogonalität stellt eine Unterscheidbarkeit dar. Durch diesen Effekt, wird deutlich weniger Bandbreite benötigt, um die selben Dateninhalte zu übertragen. Dazu hier ein Beispiel, das den Vergleich von OFDM und FDM darstellt, statt FDM könnten dabei auch andere nicht Mehrträgerverfahren herangezogen werden. Man sieht, daß OFDM bedeutend weniger Bandbreite braucht, je mehr Unterträger man hat:

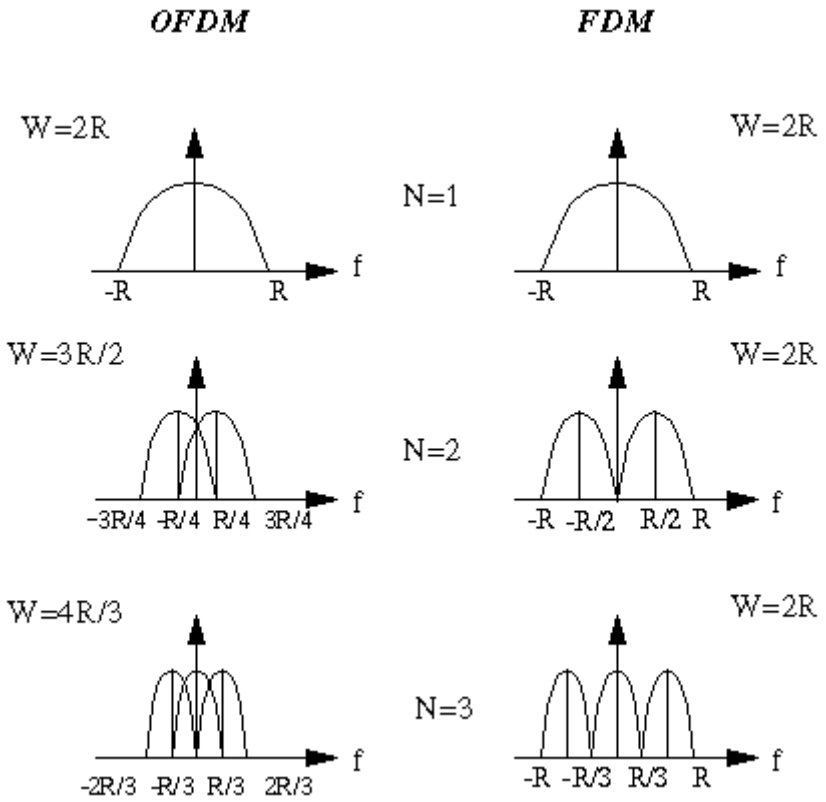


Abbildung 4 Vergleich OFDM-FDM, [UNI KI]

Natürlich hat dieser Gewinn an Bandbreite auch seinen Preis. Die Störanfälligkeit ist deutlich größer als bei den Spreizbandverfahren, aber dies wird gern akzeptiert, wohl nicht zuletzt, da man große Zahlen bei der Bandbreite (gleichgültig wie die Realität letztlich aussieht) einfach viel besser verkaufen kann als geringe. [UNI Kl]

5.2. Standards

5.2.1. Allgemeines

Wie bereits in dem Vorwort zu Kapitel 5 angesprochen, gibt es unter 802.11 zwei grundsätzlich verschiedene Standardreihen und mittlerweile auch einige Erweiterungen, die sich mit Themen wie „Quality of Service“, Sicherheit oder Interoperabilität beschäftigen. Doch erst zu den beiden Standardreihen, die einige Gemeinsamkeiten, aber auch einen wesentlichen Unterschied aufweisen. Sie funken in verschiedenen Frequenzbändern. Während 802.11b das weltweit lizenzfreie ISM (Industrial, Scientific, Medical)– Band (2,4 GHz) nutzt, ist 802.11a im 5Ghz- Band tätig. Zu beiden Standards gibt es bereits Nachfolger, so dass man getrost von zwei verschiedenen, „konkurrierenden“ Standardreihen reden kann. Wer von beiden allerdings das Rennen machen wird, ist in diesem Fall schon abzusehen. Da das 5Ghz Band nicht in allen Ländern frei ist und da außerdem die maximal zulässigen Abstrahlleistungen im 5 GHz Bereich nur ein Fünftel derer im 2,4 GHz- Band beträgt (20mW zu 100mW am Antennenausgang), geht zumindest der Massentrend derzeit ganz deutlich Richtung 2,4 GHz, sprich 802.11g, das zu 802.11b abwärts kompatibel ist. Das einzige, was den 5 GHz – Standard zu Gute kommen könnte, ist die Tatsache, dass das freie 2,4 GHz-Band in Zukunft immer mehr überlaufen sein wird und bei einem steigenden Datenaufkommen vielleicht auf weitere Frequenzbänder ausgewichen werden muss. [TOM1]

5.2.2. Standardreihen

Wie bereits erwähnt, gibt es zwei konkurrierende Standardreihen, die jetzt etwas genauer vorgestellt werden sollen.

5.2.2.1. Die „a“ Reihe

Die „a“- Standardreihe oder 802.11a (in der Erweiterung 802.11h) benutzt das weltweit bisher nicht freigegebenen Lizenzband 5 GHz, um seine Daten zu übertragen. Ein Vorteil daran ist die relative Freiheit. Nur sehr wenige Dienste sind derzeit in diesem Band tätig, was eine hohe Verfügbarkeit zur Folge hat. Im Gegensatz dazu, sind die bereits aktiven Dienste in diesem Band leider auch sehr sensitiv, da es zumeist Flugleitsysteme oder militärische Anwendungen sind. Deren Unversehrtheit ist dann auch ein Faktor in der Regulierung der maximalen Abstrahlleistung gewesen, woraufhin eine Obergrenze von 20mW festgelegt wurde.
Und da die Wellen im 5 GHz Bereich schon per se eine geringere Reichweite haben als die im 2,4 GHz – Bereich - ein Effekt, der durch die geringere erlaubte Abstrahlleistung noch unterstützt wird - ist dies in Summe einer der entscheidenden Nachteile gegenüber der „b“ – Standardreihe, denn man bräuchte wesentlich mehr Accesspoints (und damit auch Verkabelung), um eine äquivalente Abdeckung zu erzielen.
Zur Technik: Die „a“- Reihe setzte von vornherein auf den Einsatz von OFDM als Übertragungstechnik und war deshalb von Anfang an in der Lage, höhere Bandbreiten anzubieten. (54 MBit/s). [TOM1]

5.2.2.2. Die „b“ – Reihe

Die „b“ – Standardreihe oder 802.11b benutzt das weltweit lizenzfreie 2,4 GHz ISM- Band (Idustrial, Medical, Scientific). Ein wesentlicher Vorteil, da so sofort die ganze Welt als potentieller Absatzmarkt erschlossen war, aber auch ein kleiner Nachteil, da

natürlich sehr viele Dienste in diesem Band arbeiten und so entsprechende Interferenzen an der Tagesordnung sind. Auch ist nicht abzusehen, wer sich in Zukunft noch alles in diesem Bereich „tummeln“ wird. Die Übertragung der Daten wird bei 802.11b mittels FHSS oder DSSS (überwiegend) realisiert, allerdings sind diese Dienste auf eine maximale Geschwindigkeit von 11 MBit begrenzt, was den Wunsch nach einer Erweiterung mit höheren Datenraten auslöste. Diese Wünsche wurden dann mit dem 802.11 g – Standard befriedigt. Er setzt wie die 802.11a Variante auf OFMD als Übertragungstechnik und bietet so ebenfalls Datenraten bis zu 54 MBit/s an. Da allerdings eine Abwärtskompatibilität gefordert wurde, verfügt jeder Accesspoint, der diesen Standard benutzt, eigentlich über zwei getrennte Übertragungstechniken, denn es gilt DSSS ebenfalls mit zu bedienen. Der Accesspoint und die Empfangskarte handeln dann vor Beginn der Übertragung aus, wozu die Karte in der Lage ist und senden je nach Ergebnis mit 11 oder 54 MBit/s.

Im Gegensatz zu der „a“-Reihe, ist die Übertragung unter „b“ in 13 Kanäle unterteilt, die sich mangels entsprechender Bandbreite leider nicht gegenseitig ausschließen sondern überlappen.

Wenn zwei Quellen auf dem gleichen Kanal senden, kommt es zu vielen Störungen und damit zum Verlust von vielen Paketen (und daraus resultierend dem Verlust von viel Bandbreite). Diese ist möglichst zu verhindern. Leider interferieren durch die Überlappung auch benachbarte Kanäle in einem hohen Maße, so dass eine störungsfreie, gleichzeitige Übertragung nur auf drei Kanälen möglich ist (optimal 1, 7, 13). Ein weiterer Nachteil ist, dass nicht alle 13 Kanäle in jedem Land frei gegeben sind, was die Möglichkeiten nochmals einschränkt. Hier nun die konkrete Überlappung der Kanäle

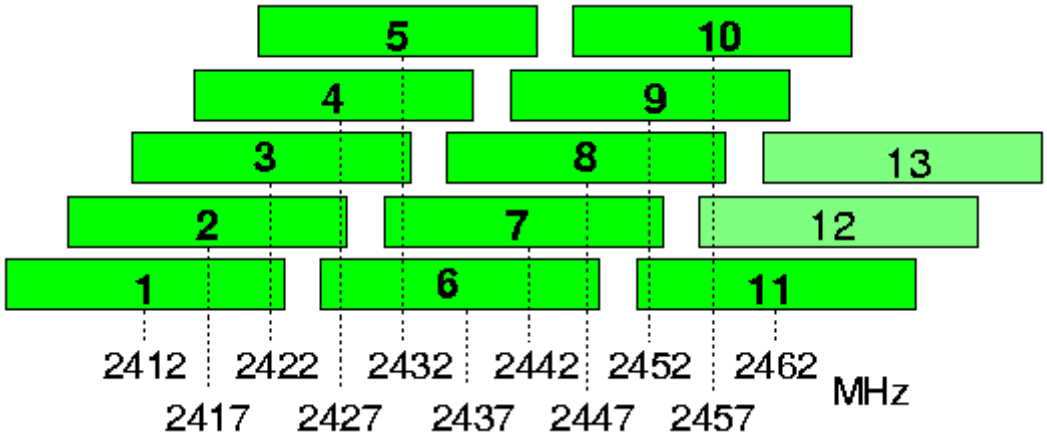


Abbildung 5 - Frequenzeinteilung der Funkkanäle bei 802.11b, [TOM1]

Trotz dieser Nachteile, zeichnet sich ein klarer Sieg dieses Systems auf dem Weltmarkt ab, da die Vorteile als schwerwiegender eingestuft werden. [TOM1]

5.2.3. Erweiterungen

Auf die kommenden Erweiterungen soll an dieser Stelle nicht allzu detailliert eingegangen werden. Einige davon sind bereits Ratifiziert, einige stehen unmittelbar davor und andere sind noch in der Endphase der genauen Spezifikation. Wichtig soll hier sein, welche grundsätzlichen Probleme von welchen kommenden (oder bereits aktiven) Standards adressiert werden. [TOM1]

5.2.3.1. IEEE802.11d

Der von Cisco als "World Mode" bezeichnete IEEE-Standard dient in erster Linie der Harmonisierung von Access Points, um ihnen die weltweit höchst unterschiedlichen Regularien für die Nutzung der knappen Ressource Frequenz sowie die daran geknüpften jeweils spezifischen Sendeleistungen beizubringen. Ziel des 11d-Stadnards ist es, für die verschiedenen Länder der Welt die gleichen Access

Points einzusetzen, und die landesspezifischen Regularien lediglich software-seitig durch schlichte Eingabe des jeweiligen Betriebsstandortes zu aktivieren und den örtlichen Gegebenheiten somit anzupassen.
Für die Mobile Stations ändert sich indes nichts, denn im Infrastruktur-Modus teilen die Access Points den angeschlossenen Mobile Stations unter anderem die Parameter für den Kanal und die Sendeleistung mit, mit denen die Kommunikation mit dem Access Point abgewickelt wird. IEEE802.11d soll also ein nahtloses Verwenden der Clients zwischen den WLANs in verschiedenen geographischen Regionen mit der gleichen drahtlosen Client-Hardware ermöglichen. [TOM1]

5.2.3.2. IEEE802.11e

IEEE802.11e ist eine geplante Erweiterung für die beiden OFDM-Standards des IEEE: 802.11a und 802.11g um das Merkmal Quality of Service (QoS), das für Voice-over IP (VoIP) respektive die drahtlosen Variante der Sprachübertragung über WLAN, VoWLAN, und Streaming-Multimedia-Verfahren unerlässlich ist. Mit 11e und - siehe unten 11h, tastet sich das IEEE also vorsichtig an das heran, was HiperLAN/2 bereits "ab Werk" beherrscht. [TOM1]

5.2.3.3. IEEE802.11f

Dies ist eine Erweiterung für die beiden IEEE-Standards IEEE802.11a sowie IEEE802.11g, um das Roaming mobiler Clients zwischen verschiedenen Access Points explizit festzulegen und die einzelnen Fähigkeiten von APs exakt zu definieren. Dieser IAPP[4]-Zusatz zum Standard IEEE802.11 soll die Interoperabilität von Access Points unterschiedlicher Hersteller verbessern, die heute noch keineswegs gegeben ist. [TOM1]

[4] Inter Access Point Protocol

5.2.3.4. IEEE802.11i

Dies ist eine Erweiterung für die beiden IEEE Standards IEEE802.11a, IEEE802.11b sowie IEEE802.11g, um die bekannten Sicherheitslücken des Wired Equivalent Privacy-Verfahrens (WEP) zu schließen. Dazu ist geplant, WEP durch das Temporal Key Integrity Protocol (TKIP) und den AES-Algorithmus zu ersetzen. Das TKPI-Verfahren fußt auf rotierende Schlüsseln, die jeweils nach einer relativ kurzen Lebensdauer durch neue ersetzt werden. [TOM1]

5.2.3.5. IEEE802.1x

Dies ist ein bereits verabschiedetes Protokoll, das in erster Linie eine Authentifizierungsmethode für Back-End-Systeme darstellt. Dabei wird auf multiple Authentifizierungsmöglichkeiten eingegangen. [TOM1]

5.2.4. Fazit

Abschliessend ist zu den Techniken innerhalb von 802.11 noch zu erwähnen, dass die in Realität erzielten Datenraten sehr viel geringer sind als die angegebenen (11 MBit/s bzw. 54 MBit/s), denn dazu müssten wirklich ideale Bedingungen herrschen: niemand stört, man ist allein, befindet sich in 10 cm Abstand, hat keine Reflexionen von Gegenständen usw… Anhand des Faktors „Entfernung zur Quelle“ soll hier gezeigt werden, welche Einschränkungen nur dieser eine Faktor schon mit sich bringt, selbst wenn alles weitere in Idealform betrachtet wird. Wenn Sie in Realität mittels einer 54 MBit/s - Karte den halben Durchsatz auch tatsächlich erzielen, sollten sie sich sehr glücklich schätzen.

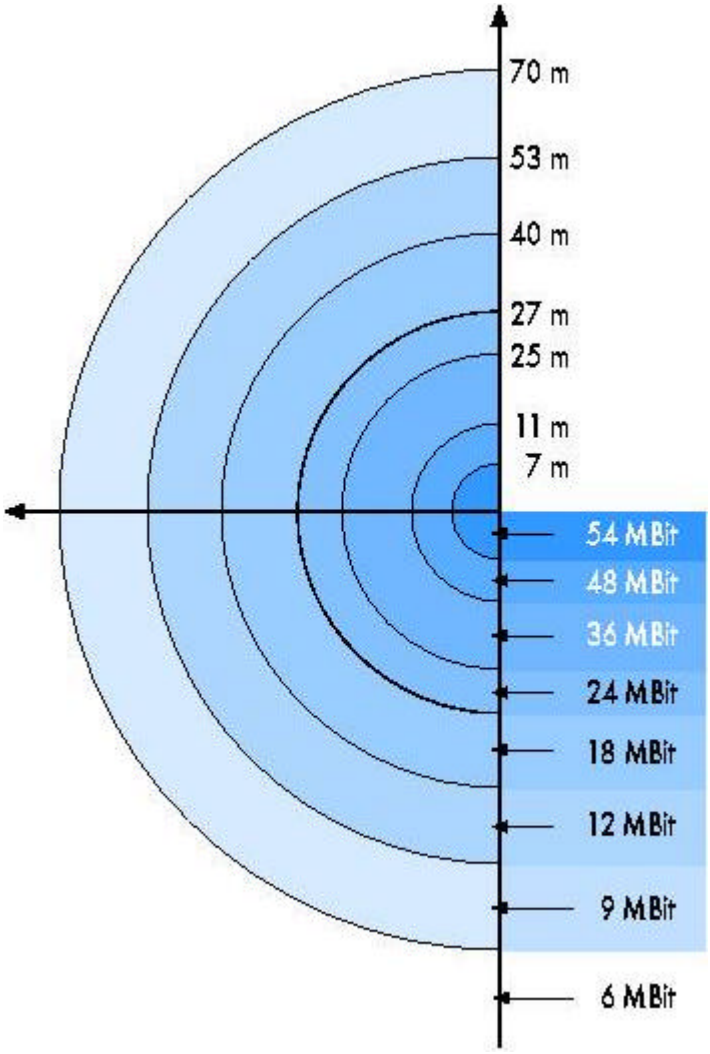


Abbildung 6 – Bandbreiteneinbußen, [TOM1]

5.3. Gesundheitsrisiken

Über die grundsätzliche Frage, ob Gesundheitsrisiken von elektromagnetischer Strahlung ausgehen, soll an dieser Stelle nicht diskutiert werden, es geht vielmehr darum, die Emissionen von WLAN mit denen anderer Sendequellen zu vergleichen und in Relation zu setzten, denn das Gefährdungspotential steigt üblicherweise mit der Energiemenge, die abgestrahlt wird.
Bei Durchsicht der einschlägigen Literatur und der veröffentlichten Gutachten zu diesem Thema fällt auf, dass die einzelnen Quellen doch zu recht unterschiedlichen Ergebnissen kommen. In einigen Kernaussagen, stimmen sie jedoch überein und auf die soll hier eingegangen werden, da ein genauer Vergleich der einzelnen Gutachten den Rahmen sprengen würde.

Die Abstrahlung von digitalen Funkdiensten wie GSM-Mobilfunk, DECT-Schnurlostelefone und WLAN weisen hohe Gemeinsamkeiten auf, dabei handelt es sich in allen Fällen um periodisch gepulste Strahlung, wobei die Basisstationen der Systeme auch dann senden, wenn gar keine Nutzdaten zu übertragen sind. Es sind mehrere grundsätzliche Faktoren zu isolieren, die die Emissionen beeinflussen. Zu nennen sind hier die Intensität der Strahlung, deren Dauer und der Abstand zum Menschen, jeweils sowohl für die Basisstation als auch für das Mobilteil.
Durch die maximal zugelassenen Abstrahlleistungen der einzelnen Systeme ist klar definiert, dass WLAN mit seinen erlaubten 100mW am wenigsten Grundemissionen verursacht, dicht gefolgt von DECT (200mW) und mit weitem Abstand gefolgt vom Mobiltelefon (2000 mW). DECT und Mobilfunk erreichen diese Werte allerdings nur im Übertragungsfall, eine WLAN-Karte hingegen, die sich im Notebook oder im PDA des Nutzers befindet, sendet nach ihrer Aktivierung fast kontinuierlich. Alle Basisstationen senden in jedem Fall kontinuierlich, allerdings ist der Abstand zu ihnen weit größer als der zum Mobilteil und da der Abstand quadratisch in die Berechnungsformel einfließt, also bei einem 10 fachen Abstand (z.B. 10 cm zu 1m) gleich eine hundertfache Wirkung auftritt, sind es die Mobilteile, die hier betrachtet werden sollen. Dabei soll keinesfalls

der Eindruck entstehen, dass nicht für alle, auch für diejenigen, die diese Systeme nicht benutzen, durch die Basisstationen eine Grundstrahlung permanent emittiert wird, deren Summe durchaus nicht gering ist. Allerdings ist es schwierig bei dem Gemisch aus Radio -, Fernseh -, Mobilfunk -, DECT -, WLAN- und noch vielen weiteren uns umgebenden Wellen einen „Schuldigen“ festzumachen. Sicher ist nur, dass WLAN dabei seinen Teil zu den Emissionen beiträgt.

Ein weiterer Grund, der die Betrachtung erschwert, ist der Einfluss auf die empfindlichen Regelsysteme des menschlichen Organismus (z.B. Nerven-, Hormon- und Immunsystem, Zellkommunikation), die bisher noch nicht vollständig bekannt sind. Alle bisherigen Grenzwerte beziehen sich einzig auf die Wärmewirkung von hochfrequenter Strahlung und diese werden bei WLAN nicht annähernd erreicht.

Fazit:

WLAN „verstrahlt“ seine Umgebung und damit seine Nutzer kontinuierlich, allerdings mit einem Strahlungsniveau, das nur einen Bruchteil dessen entspricht, was ein Mobilfunkgerät während des Verbindungsaufbaus erreicht.

Hierzu ein Rechenbeispiel: Geht man davon aus, dass sich die WLAN-Karte innerhalb eines Laptops oder eines PDA’s in einem Abstand von 25 cm zum Nutzer und sich ein Mobiltelefon direkt am Kopf (1cm) befindet, ergibt sich allein durch den Abstand ein Unterschiedsfaktor von 625. Hinzu kommt, dass die abgestrahlte Leistung abermals um den Faktor 20 kleiner ist. Kumuliert ergibt sich also ein Unterschied von Faktor 12500!

Die Bewertung, ob nun eine schwache permanente oder eine temporäre starke Emission eine größere Gefährdung birgt, soll jedem selbst überlassen werden. Anzumerken bleibt noch, dass wir alle seit Jahren ständig einer „Verstrahlung“ des Äthers ausgesetzt sind, deren tatsächliche Folgen sich wohl erst in vielen Jahren abschätzen lassen. [TOM1][Virnich]

5.4. Probleme im kommerziellen WLAN aus Anwendersicht

Neben den Gesundheitsrisiken gibt es noch zwei wichtige weitere Themen, die die Nutzer interessieren. Die Einfachheit der Handhabung und die Sicherheit ihrer Daten.
Die WLAN- Technologie bietet für den Nutzer den Bedienvorteil, dass sich die Karte im Endgerät und der Accesspoint automatisch finden. Ferner sind die Karten mittlerweile oft bereits in die Endgeräte integriert und die Betriebssystemsoftware erkennt die gängigen Modelle automatisch. Die grundsätzliche Bedienung ist also ohne Aufwand gewährleistet. Für den kommerziellen Einsatz sind allerdings noch weitere Systeme notwendig, wie die Sicherheit und die Zugangskontrolle. Zur Zugangskontrolle gehört im Umfeld der öffentlichen HotSpots auch das Thema Roaming.

5.4.1. Sicherheit

Auf die technischen Realisierungen und Empfehlungen soll im Kapitel 6.5 noch näher eingegangen werden.
Aus Sicht der Nutzer allerdings ist es wichtig, dass die Sicherheit mit einem möglichst geringen zusätzlichen Aufwand erreicht werden kann. Außerdem wäre es schädlich, wenn bei kommenden Weiterentwicklungen immer wieder ein neues Prozedere erlernt werden müsste. Entweder sollte die Sicherheit also automatisch funktionieren oder es sollte ein übergreifendes Sicherheitskonzept Anwendung finden, das für diverse Netzwerklösungen verwendbar ist. Dies gilt sowohl für Sicherheit innerhalb von Büros oder anderen geschlossenen Systemen, als auch für den Bereich der öffentlichen HotSpots.

5.4.2. Zugangskontrolle / Roaming

Nicht öffentliche Netze - wie Firmennetzwerke - sind in der Regel nur für einen bestimmten Personenkreis zugänglich. Da WLAN meist nur eine Erweiterung bzw. Ergänzung der kabelgebundenen Netze darstellt, gilt hier gleiches. Eine in der Regel von einem Administrator verwaltete Nutzerdatenbank regelt die Zugriffe und das Rechte-Management, der Nutzer authentifiziert sich über ein Login und erhält dann Zugriff.
Im Bereich der öffentlichen HotSpots ist es mit einem einfachen Login nicht getan, zwar sollte es für den Nutzer so aussehen, idealerweise sollte sogar der gleiche Login immer und überall funktionieren. Die Realität sieht allerdings anders aus: Derzeit entstehen viele verschiedene HotSpot-Systeme von unterschiedlichen Anbietern. Ob die Nutzer in Zukunft allerdings verstärkt auf diese Möglichkeit der Nutzung des Internets zugreifen werden, wird nicht nur von der Sicherheit und dem damit verbundenen Vertrauen abhängen, sondern auch von der Möglichkeit, an jedem Zugangspunkt auch Zugang zu erhalten und sich vor allem dabei nicht jedes Mal um neue Zugangsdaten kümmern zu müssen. Es muß also eine für den Nutzer transparente Möglichkeit geben, die eben dieses gewährleistet: ein Roamingsystem.

5.5. Roaming

5.5.1. Roaming von HotSpots

Unter dem Begriff Roaming versteht man im Zusammenhang mit HotSpots nicht das Roaming unter mehreren Accesspoints, die im gleichen Netz aktiv sind, sondern ein System, das den Nutzern einen transparenten Zugang an HotSpots verschiedenster Betreiber ermöglicht. Es gibt derzeit von verschiedenen Seiten Bestrebungen ein solches System zu etablieren, allerdings gibt es hier grundsätzlich zwei verschiedene Ansätze: den kommerziellen und

den nicht kommerziellen. Im kommerziellen Umfeld versuchen verschiedene Firmen ein solches System auf die Beine zu stellen, denn es liegt auf der Hand, dass es natürlich sehr lukrativ wäre, eben diese Vermittlungsplattform zu betreiben und an jedem Zugriff mitzuverdienen. Genau deshalb soll an dieser Stelle vermutet werden, dass die konkurrierenden Unternehmen nicht zulassen werden, dass nur eine Firma sich diese lukrative Position sichert. Die andere Möglichkeit wäre eine übergreifende Kooperation mehrerer Firmen, aber das wird definitiv einige Koordinationsprobleme mit sich bringen. Diesen Möglichkeiten gegenüber steht die Alternative, auf eine nicht kommerzielle Lösung zu setzten. Also das Szenario, dass ein nicht kommerzieller Verein diese Plattform aufbaut und betreibt. Eben ein solches System befindet sich derzeit in der letzten Realisierungsphase und zwar vom ECO-Verband der Internetwirtschaft, das Projekt heißt „Greenspot“.
An dieser Stelle soll nicht das gesamte technische Konzept von Greenspot erläutert, sondern vielmehr die grundsätzlichen Überlegungen dargelegt werden[5].

5.5.2. Greenspot

Grundsätzlich geht Greenspot davon aus, dass es mehrere Akteure auf dem Markt der WISPS (Wireless Internet Service Provider) geben wird: die Betreiber vor Ort (genannt Operator), diejenigen, die mehrere dieser Operatoren zusammenfassen (genannt Konzentratoren) und diejenigen, die den Endkundenkontakt besitzen (genannt Serviceprovider). Dabei ist nicht ausgeschlossen, dass einzelne Parteien auch mehrere oder alle Rollen einnehmen.
Die Operatoren sind dabei das letzte Glied in der Kette. An den so erschlossenen Endpunkten können die Kunden auf das Internet zugreifen. Dabei werden sie entweder direkt an Ort und Stelle mit

[5] Für mehr: www.eco.de / Stichwort :Greenspot, allerdings ist es notwendig vor Erhalt der technischen Specs und des Vertragswerks einen NDA zu unterschreiben

Zugangsdaten versorgt, gegen entsprechende Bezahlung versteht sich, oder über Greenspot.
Die Konzentratoren vereinen mehrere dieser Endpunkte unter einem System zur einheitlichen Zugangskontrolle. Sie sind es auch, die mit dem Greenspot-System kommunizieren und die erforderlichen Daten übermitteln. Für die einzelnen Operatoren würde dies keinen Sinn machen, da der erforderliche Aufwand zu groß wäre. Sie stellen also die eine Seite des Greenspot Systems dar. Die andere Seite des Systems bilden die Serviceprovider. Sie sind es, die die Endkundenbeziehungen haben und sich um das Inkasso kümmern. Dabei haben sie alle Freiheiten in der Preisgestaltung. In der Praxis wird davon ausgegangen, dass die großen Telekommunikationsanbieter ihren Kunden dies als Extraservice anbieten werden. Sie haben die entsprechenden Kunden inkl. vorhandener Inkassoanbindungen, sie arbeiten in der richtigen Branche und sie haben die notwendige Reichweite, ihre Kunden über das neue Angebot zu informieren. Um dabei sowohl ihnen als auch den Operatoren und Konzentratoren eine gewisse Kalkulationssicherheit zu geben, gibt es eine „Interconnection-Fee“. Die regelt, wer im Falle einer Vermittlung über Greenspot wieviel Geld bekommt.
Der gesamte Ablauf würde dann wie folgt von Statten gehen:
Die Serviceprovider geben ihren Kunden die entsprechenden Zugangsdaten. Die Zugangsdaten bestehen aus einem Passwort und einem Username, dieser Username besteht im Falle von Greenspot wiederum aus einem individuellen Teil und einem Teil, der den entsprechenden Serviceprovider identifiziert. Im Falle von Greenspot getrennt durch ein „ @“. (Beispiel: postel@telekom).
Wenn sich jetzt einer dieser Kunden an einem beliebigen an Greenspot angeschlossenen HotSpot registrieren möchte, werden die Daten vorerst an den betreibenden Konzentrator weitergeleitet. Dieser prüft dann zunächst, ob die Zugangsdaten zu seinen eigenen gehören, ansonsten leitet er die Daten an Greenspot weiter und wartet auf die Antwort. Greenspot identifiziert anhand der Kennung den entsprechenden Provider und leitet die Daten an ihn weiter. Dieser trifft dann die Entscheidung, ob die Daten akzeptiert werden sollen oder nicht. Diese Antwort geht zurück an Greenspot und dann weiter an den entsprechenden Konzentrator, der den Zugang oder

die Ablehnung einleitet. Nach Beendigung der Verbindung geht diese Information erneut den Weg zum Serviceprovider, um die unterschiedlichen Abrechnungssysteme zu synchronisieren.
Für den Nutzer bietet dieses Verfahren den Vorteil, sich nicht um neue Passwörter oder den Zahlungsweg kümmern zu müssen. Sie haben fortan die Möglichkeit, überall (in Zukunft auch weltweit geplant) auf das Internet zugreifen zu können und das zu mit ihrem Provider ausgehandelten und für sie kalkulierbaren Preisen.
Für die Konzentratoren bietet Greenspot den Vorteil, eine viel größere Nutzergruppe erreichen zu können. Da sie das technische System aufgebaut haben, ist natürlich jeder weitere zahlende Kunde willkommen. Diese größere Reichweite ist auch für den Operator interessant, weil sie ihren Standort attraktiver macht.
Für die Serviceprovider bietet Greenspot die Möglichkeit, ohne jegliche Investitionen nur ihren Kundenstamm zu nutzen, um zusätzliches Geld zu generieren.
Und all dies wird bereitgestellt von einer nicht kommerziellen Plattform, von der für alle Beteiligten keine Konkurrenzgefahr ausgeht - ein Modell, was tatsächlich aufgehen könnte.

Auch wenn es am Ende nicht das Greenspot- System sein sollte, das sich durchsetzt, so steht doch eines fest:
Wenn WLAN wirklich massentauglich und eine echte UMTS-Konkurrenz werden soll, muß ein vergleichbares System geschaffen werden. [eco]

5.6. Schlussfolgerung

Einige Aspekte innerhalb von WLAN sind verbesserungswürdig. Einige davon können mit entsprechenden Rahmensystemen und im Zusammenspiel von mehreren involvierten Gruppen in den Griff bekommen werden, wie zum Beispiel das hier angesprochene Thema Roaming, andere können von jedem Lösungsanbieter selbst angegangen werden. Der Kernaspekt ist hier die Sicherheit.
Sicherheit ist eine Geisteshaltung, die mehr und mehr in den Köpfen der Computernutzer Einzug hält. Vereinfacht könnte man sagen,

ohne Sicherheit wird es im WLAN-Umfeld aufgrund fehlenden Vertrauens schwierig Kunden zu gewinnen, ohne Kunden wiederum gibt es keine Refinanzierung, ohne Refinanzierung wird WLAN nicht lange am Markt bleiben. Dies gilt natürlich vor allem für den öffentlichen Bereich (HotSpots). Innerhalb von geschlossenen Systemen, wie Firmennetzen oder dem SOHO-Markt wird der Vorteil der „Kabellosigkeit“ zumindest in einigen Zonen dazu führen, dass WLAN zum Einsatz kommen wird. Der Erfolg von WLAN als System soll hier also gar nicht in Zweifel gezogen werden, doch für den öffentlichen Bereich gilt es noch viele Hürden zu überwinden.

6.Sicherheit

6.1. Was bedeutet Sicherheit

Betrachtet man beim Entwurf oder Einsatz von IT-Systemem deren Sicherhait, ist zuvor zu klären, was unter dem Begriff der Sicherheit in diesem Kontext zu verstehen ist. Das Bundesministerium für Sicherheit in der Informatiomstechnik (BSI), dessen zentrale Aufgabe die Förderung der IT-Sicherheit ist, veröffentlicht in regelmäßigen Abständen das sogenannte „IT-Sicherheitshandbuch“, als Leitfaden zur Risikoanalyse und Entwurf von Sicherheitskonzepten, in diesem wird der Begriff IT-Sicherheit wie folgt definiert [BSI 1992]:

„Zustand eines IT-Systems, in dem die Risiken, die beim Einsatz dieses IT-Systems aufgrund von Bedrohungen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß beschränkt sind.“ [BSI 1992, Anhang F Glossar]

Unter Bedrohung eines IT-System wird der Verlust von Verfügbarkeit, Integrität und/oder Vertraulichkeit verstanden.

6.1.1. Verfügbarkeit

„Mit Verfügbarkeit bezeichnet man den Tatbestand, daß Funktionen eines IT-Systems ständig bzw. innerhalb einer vorgegebenen Zeit, die von Funktion zu Funktion unterschiedlich sein kann, zur Verfügung stehen und die Funktionalität des IT-Systems nicht vorübergehend bzw. dauerhaft beeinträchtigt ist. In diesem Zusammenhang kann auch die Verfügbarkeit von Informationen bzw. Daten bedeutend sein.“ [BSI 1992, Kapitel 3.1]

6.1.2. Integrität

„Unter der Integrität von Informationen versteht man die Tatsache, daß Informationen nur von Befugten in beabsichtigter Weise verändert und nicht unzulässig modifiziert werden können. Von dieser Grundbedrohung sind auch Programme betroffen, da die Integrität der Daten nur bei ordnungsgemäßer Verarbeitung und Übertragung garantiert werden kann. Häufig wird unter dem Begriff "Integrität" außer der Unversehrtheit auch noch die Vollständigkeit, die Widerspruchsfreiheit und die Korrektheit verstanden. Vollständig bedeutet, daß alle Teile der Information verfügbar sind. Korrekt sind Informationen, wenn sie den gemeinten Sachverhalt unverfälscht beschreiben.“ [BSI 1992, Kapitel 3.1]

6.1.3. Vertraulichkeit

„Unter der Vertraulichkeit von Informationen versteht man die Tatsache, daß die Information nur Befugten zugänglich ist und kein unbefugter Informationsgewinn stattfinden kann. Von dieser Grundbedrohung können auch Programme als Informationen im weiteren Sinne betroffen sein, z. B. wenn ein Verfahren, dessen Vorschrift durch ein Programm dargestellt wird, geheim gehalten werden soll.“ [BSI 1992, Kapitel 3.1]

In anderen Quellen wird dieses gelegentlich noch um die Begriff Authentizität, Autorisierung und Verbindlichkeit erweitert:

6.1.4. Authentizität

Die Sicherung der Authentizität hat zwei Aspekte: Authentizität in Bezug auf einen Kommunikationspartner oder Benutzer (auch *entity authentication* genannt) bedeutet, dass dessen Identität zweifelsfrei festgestellt werden kann. Bevor ein IMAP-Server einem Benutzer Zugriff auf seine E-Mails gibt, muß dieser erst beweisen, daß er wirklich der berechtigte Nutzer ist. Der zweite Aspekt von Authentizität betrifft Nachrichten (*data origin authentication*): Hier fordert man, daß für den Empfänger (und evtl. weitere Beteiligte) feststellbar ist, ob eine Nachricht authentisch ist, also der angebliche Absender mit dem tatsächlichen Absender übereinstimmt.

6.1.5. Autorisierung

Die meisten Dienste und Daten dürfen nur von autorisierten Personen (oder Prozessen, Rechnern etc.) genutzt beziehungsweise zugegriffen werden (*access control, authorization*). Wenn sich zum Beispiel ein Benutzer mit seinem Paßwort an einem Unix-System anmeldet (authentifiziert), heißt das noch lange nicht, daß er dann auch die Festplatte formatieren oder das System herunterfahren darf. Zugriffskontrolle ist von funktionierenden Benutzer-Authentifikationsmechanismen abhängig, da der anfragende Nutzer zuverlässig erkannt werden muß, um seine Berechtigung für die gewünschte Aktion überprüfen zu können.

6.1.6. Verbindlichkeit

Nachrichten sind verbindlich, wenn der Absender im Nachhinein nicht bestreiten kann, eine Nachricht tatsächlich abgeschickt zu haben (*non-repudiation*). Genauso soll der Empfänger später nicht leugnen können, eine bestimmte Nachricht erhalten zu haben. Diese Zurechenbarkeit (*accountability*) des Absendens schützt einen Online-Händler beispielsweise davor, daß ein Käufer bei der Lieferung nicht unwiderlegbar behaupten kann: "Ich habe nichts bestellt!". Der verbindliche Nachweis des Empfangs entspricht demgegenüber in etwa einem eingeschriebenen Brief.

6.2. Angriffe

Durch die Kommunikation über Netzwerke bietet ein IT-System Unterschiedliche Angriffspunkte, der folgende Abschnitt beschreibt die bekanntesten [Raepple 1998]:

6.2.1. „Sniffing“

Durch IP oder TCP werden keine Mechanismen zur Verschlüsselung des Datenstromes bereit gestellt. Bei Anwendungen, welche diese Protokolle zum Datentransfer nutzen, ohne eigene Verschlüsselungsmechanismen zu verwenden, finden sich diese Information als Klartext in den Paketen wieder. In sogenannten Shared Media Netzwerken haben nicht nur Sender und Empfänger der Nachricht Zugriff auf die gesendeten Datenpakete. Weitere Teilnehmer, die Zugang zum übertragenden Medium (Ethernet-Kabel, Luft bei WLAN) haben, können durch Modifikation der Netzwerkkarte (promiscous mode) auch ohne besonderen Aufwand Daten mitlesen, welche nicht an ihre Adresse gerichtet sind.
Betroffen sind hiervon eine Vielzahl weit verbreiteten Anwendungsprotokolle, wie z.B. POP3, SMTP, Telnet oder FTP, welche von Haus aus über keine zureichenden Sicherheitsmerkmale verfügen. Neben der Gefahr, die vom Mitlesen der übertragenen Informationen, sowie der von diesen Protokollen benutzen Passwörtern ausgeht, stellt das Sniffing durch Ausspionieren der IP/TCP-Protokoll-Header (Absender-/Empfängeradresse/-port, Sequencenummer) auch die Basis weiterer Angriffe dar.

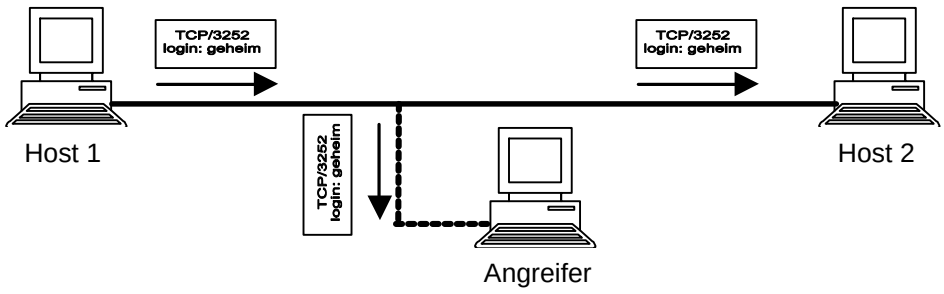


Abbildung 7 Sniffing, Mitlesen von Paketen

WLAN ist hier besonders gefährdet, da das übertragende Medium Luft für Jedermann zugänglich ist.

6.2.2. Spoofing

Unter Spoofing versteht man die Art von Angriffen, bei denen der Angreifer die Identität eines anderen Netzteilnehmers vortäuscht. Im Falle des IP-Spoofing wird dieses erreicht, indem das IP-Paket mit einer gefälschten Absenderadressen versehen und an das Zielsystem gesendet wird. Eine besondere Gefahr besteht hier in Verbindung mit Diensten, die eine Authentifizierung über die IP-Adresse vornehmen (siehe Hijacking) , wie z.B. rsh, X-Windows oder nfs. Ein ähnliches Vorgehen kann auch auf weitere Schichten das OSI-Modells angewendet werden. Mittels ARP wird hier eine Zuordnung der MAC-Adressen (Netzwerkkarte) zu IP-Adressen vorgenommen, jeder Rechner führt hierzu eine Tabelle, die diese Zuordnungen enthält, lässt sich eine bestimmte Zuordnung nicht aus der Tabelle entnehmen, sendet der Rechner einen sogenannten ARP-Broadcast ins Netz, der von allen Rechnern in diesem empfangen wird. Im Normalfall sendet daraufhin der Rechner mit der nachgefragten IP-Adresse ein ARP-Antwort-Paket, die fehlende Zuordnung kann der ARP-Tabelle des anfragenden Rechners daraufhin hinzugefügt werden. Da die Anfrage an alle Teilnehmer im Netz geht, kann ein Angreifer auf ein solches Paket reagieren, indem er selber ein Antwort-Paket sendet, in dem er seine MAC der angefragten IP zuordnet. Dieses hat zur Folge, dass der Rechner, von welchem die Anfrage kam, die IP-Adresse des erfragten Teilnehmers mit der MAC-Adresse des Angreifers assoziiert und alle Pakete an diesen sendet.

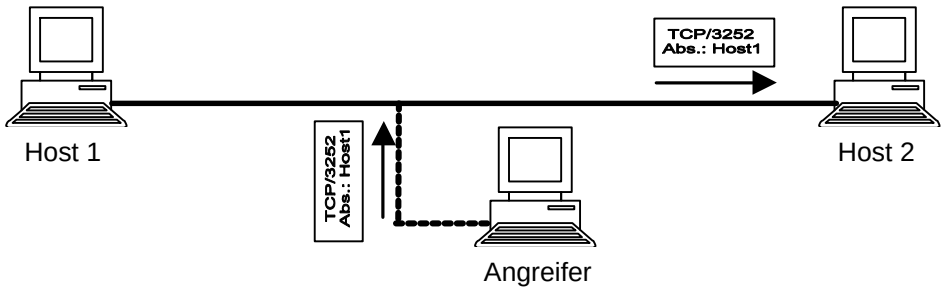


Abbildung 8 Spoofing

6.2.3. Man-in-the-middle

Bei Angriffen, die unter dem Begriff "man-in-the-middle" zusammengefasst werden, versucht ein Angreifer sich so in den Kommunikationsfluß zwischen zwei Kommunikationspartnern zu hängen, dass die gesendeten Daten zuerst an den Angreifer gesendet werden, welcher sie anschließend an den Zielrechner weiterleitet. Durch den Angreifer muss der Datenaustausch beider Rechner so manipuliert werden, dass beide ihre Daten an ihn senden und in dem Glauben gelassen werden, dies sei die gewünschte Gegenstelle.
Der Angreifer hat so die Chance alle Daten einzusehen, bevor diese an den eigentlichen Empfänger gehen, zuvor können diese durch den Angreifer verändert worden sein. Man spricht hier von einem aktiven „man-in-the-middle"-Angriff.

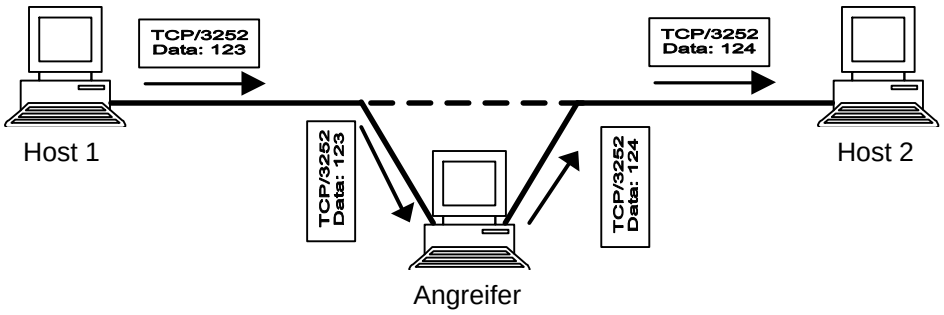


Abbildung 9 Man-in-the-middle Angrif

Der konkrete Ablauf eines solchen Angriffs hängt von den Protokollen, die Ziel der Attacke sind, ab. Beispielhaft sei im folgenden Abschnitt das Session Hijacking als Man-In-the-Middle Angriff auf IP-basierte Dienste wie Telnet erwähnt.

6.2.4. Session Hijacking

Die durch das Sniffing und Spoofing beschriebenen Möglichkeiten, stellen die Grundlage von Angriffen dar, welche zum Ziel haben, eine aktive Verbindung zwischen zwei Kommunikationspartnern zu übernehmen (oder zu stören), man spricht hier von Hijacking. Der Angreifer hört den Datenverkehr auf seinem Netzwerksegment ab, bis eine aktive Verbindung, z.B. eine Telnet-Session entdeckt wurde. Aus den abgehörten Daten stellt der Angreifer ebenfalls ein Paket zusammen, welches die Absenderadresse des ursprünglichen Teilnehmers enthält und sendet dieses an den Telnet-Server, die Sequencenummer dieses Paketes wird anhand der abgehörten Paket erraten, so dass der Server davon ausgeht ein weiteres Paket des Clients zu empfangen. Erreicht das original Client-Paket den Server wird dieses als fehlerhaft verworfen, da aufgrund des bereits empfangenen „gefälschten“ Paketes die Sequencenummer nicht mehr korrekt ist, die original Telnet-Session ist hierdurch unterbrochen.

Prinzipiell ist dieses Vorgehen auf alle Protokolle anwendbar, die eine aktive Session lediglich über die Absender-IP-Adresse sicherstellen. Im Falle von Telnet können über die eingespeisten Pakete Kommandos transportiert werden, die besonders im Falle einer übernommenen Session des root-users verheerende Auswirkungen haben können (z.B. rm –rf /*).
Aufgrund der erforderlichen Kenntnisse zur Durchführung dieses Angriffes, galt dieser lange Zeit als schwer durchführbar, dieses gilt nicht mehr, seit auch hierfür Tools existieren, die diesen Angriff automatisieren (e.g. juggernaut).

6.2.5. Denial Of Service

Die unter dem Begriff Denial of Service–Attacke zusammengefassten Methoden haben das gemeinsame Ziel Rechner an der Ausführung ihrer Dienste zu hindern. Dieses erfolgt oft durch Ausnutzung von Schwachstellen der Netzwerkprotokolle und/oder der Implementierungen der eingesetzten Betriebsysteme.
Stellvertretend soll hier das Syn-Flooding (welches auch als Ping-of-Death bekannt ist) beschrieben werden, welches Schwächen einiger TCP-Implementierungen ausnutzt. Beim Aufbau einer TCP-Verbindung sendet der Initiator ein SYN-Paket an den gewünschten Kommunikationspartner. Dieser reagiert darauf, indem er ein SYN/ACK an den anfragenden Rechner zurücksendet und auf eine Bestätigung des Empfangs zum entgültigen Aufbau der Verbindung wartet. Hier setzt das SYN-Flooding an, unterstützt durch entsprechende Tools werden ununterbrochen SYN-Pakete an eine Rechner gesendet, ohne die darauf folgenden SYN/ACK-Antworten zu bestätigen. Die TCP-Implementierung des angegriffenen Rechners muß sich sämtliche Anfragen merken, um auf die Bestätigung zu warten (welche ausbleibt). Folge dessen ist, dass immer mehr Speicher verbraucht wird, und es (bei entsprechend fehlerhaften Implementierung) zu einem Stack-Overflow kommen kann. Der Rechner ist jetzt nicht mehr in der Lage, seine eigentlichen Aufgaben auszuführen.
Verstärkt werden kann der Effekt durch sog. Distributet Denial of Service-Attacken werden, hier die angreifenden Programme auf mehreren Rechner platziert und starten ihren Angriff gleichzeitig, sozusagen mit vereinter Kraft, gegen das Zielsystem.

6.3. Protokolle zur Datensicherung in konventionellen, kabelgebundenen Netzwerken

6.3.1. PPTP

6.3.1.1. Was ist PPTP

PPTP ist ein Netzwerkprotokoll für Punkt-zu-Punkt-Verbindungen.[6]
Das Point to Point Tunneling Protokol erlaubt plattformübergreifende Kommunikation über das Internet auf einfache und dennoch recht sichere Weise.
Entgegen der Suggestion, die der Name impliziert, eignet sich PPTP sowohl für die Punkt zu Punkt als auch für Punkt zu Mehrpunkt Verbindungen. Das eröffnet die Möglichkeit, sich von unterwegs über das Internet in das eigene Firmennetzwerk „einzuwählen“ gleichermaßen wie zwei Standorte oder zwei Rechner miteinander zu verbinden.[7]

PPTP ist neben L2TP (Layer 2 Tunneling Protokoll) und L2F (Layer 2 Forwarding) ein Layer-2 VPN. Das heißt, es wird ein virtuelles Netzwerkgerät (und Kabel) zur sicheren Kommunikation erzeugt, das eine vorhandene IP-Infrastruktur (z.B. das Internet) benutzt, um transparent ein lokales Netzwerk herzustellen. Dadurch werden Sicherheistprobleme, welche aus dem Einsatz von nicht für drahtlose Kommunikation ausgelegter Anwendungen entstehen, ohne deren Modifikation behoben. Das Verfahren bietet zudem gegenüber Verfahren auf OSI Layer 3 und der Anwendungsebene den Vorteil, protokollunabhängig zu sein; es können zahlreiche Protokolle wie IP, IPX, NetBEUI, etc. „durchgetunnelt“ werden.

PPTP ist durch das Microsoft-Betriebssystem weit verbreitet und auch bei anderen Betriebssystememem wie Unix und MacOS gibt es Implementierungen. Durch den bereits recht langen Einsatz sind die Stärken und Schwächen genau untersucht worden.

6.3.1.2. Wie setzt sich PPTP zusammen?

---

[6] Es wurde von einem Konsortium bestehend aus K. Hamzeh - Ascend Communications, G. Pall - Microsoft Corporation, W. Verthein - 3Com, J. Taarud - Copper Mountain Networks, W. Little - ECI Telematics, G. Zorn - Microsoft Corporation, im Juli 1999 erarbeitet und ist ein RFC-Draft (2637) allerdings kein IETF Standard, vielmehr ein Industriestandard.

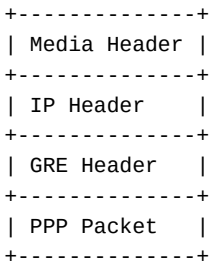
[7] Hierfür müssen aber beide Router entsprechend eingerichtet werden: Routen, Proxyarp, etc.

PPTP besteht aus zwei Komponenten, einer Kontrollverbindung auf Basis von TCP und einem IP-Tunnel, der über GRE PPP-Pakete transportiert wird.

Die Kontrollverbindung ist zuständig für den Aufbau, das Management und das Trennen des Tunnels. Es wird das Link Control Protokoll (LCP) benutzt. Die wesentlichen Merkmale des LCP [RFC 1548/1570] sind:

- Verkapselungsoptionen
- Paketgrößen
- Auffinden von Konfigurationsfehlern
- Senden von „keep alive packets“
- Funktionstest des Tunnels
- Trennung des Tunnels

Der Tunnel ist mittels GRE implementiert. Um mehrere Verbindungen am Server unterscheiden zu können, wird eine eindeutige ID/Session vor dem Aufbau des Tunnels über die Kontrollverbindung vereinbart. Über den GRE-Tunnel werden PPP-Pakete transportiert. PPP regelt schließlich die Authentifizierung sowie den eigentlichen Datenaustausch sowie optional/modular die Verschlüsselung und Komprimierung.



6.3.1.3. Verbindungsaufbau

PPTP sieht Mechanismen vor, die die Authentifizierung und Verschlüsselung abwickeln.
Bei dem Verbindungsaufbau werden 5 Phasen durchlaufen:

1. Linkaufbau
2. Authentifizierung
3. Callback Option
4. Aktivierung des Network Layer
5. Datenaustausch

Link Aufbau
Es wird das Unterprotokoll LCP (Link Control Protokol) benutzt, um die verschiedenen Optionen auszuhandeln. Es wird dabei untersucht, welche Parameter von beiden Seiten unterstützt oder gar gefordert werden. Typische Parameter beinhalten die Optionen für die Authentifizierungsart, die Verschlüsselung, Kompression sowie die Zuweisung von IP-Adressen.

Authentifizierung
Während der Authentifizierungsphase tauschen sich der PEER und der AUTHENTICATOR aus, um die Identität der Endpunkte des Tunnels zu verifizieren.
Dabei können verschiedene Protokolle verwendet werden, die da seien: PAP, CHAP, MS-CHAPv1, MS-CHAPv2 sowie allgemein EAP, auf die später näher eingegangen wird.
Bei allen hier aufgeführten Protokollen besteht die Möglichkeit, die Identität des Benutzers festzustellen, d.h. der Benutzer muss seinen Loginnamen und das Passwort eingeben. Das erlaubt im Allgemeinen ein höheres Sicherheitsniveau als allein den Transportendpunkt, d.h. z.B. die Netzwerkschnittstelle, zu authentifizieren.

Callback Option
Microsoft sieht vor, nach der Authentifikation die Verbindung zu trennen, um dann die Verbindung durch den AUTHENTICATOR, den NAS (Network Access Server) aufzubauen. Dabei wird unter Benutzung des Callback Control Protocol (CBCP) eine

Wählverbindung über das Telefonnetz vom NAS zum PEER unter Berücksichtigung der in Phase 2 übermittelten Telefonnummer aufgebaut. Durch dieses Verfahren wird zusätzlich sichergestellt, dass der PEER valide ist.

Aktivierung des Network Layer

Die in Phase 2 ausgehandelten Optionen für die IP-Verbindung werden hier benutzt, um eine IP-Verbindung aufzubauen. Wurde Verschlüsselung ausgehandelt, wird das MPPE-Modul mit den Schlüsseln initialisiert, die während der Authenifizierungsphase berechnet wurden.

Datenaustausch

Die Anwendungsdaten werden in PPP-Pakete eingekapselt und optional komprimiert und verschlüsselt. PPP benutzt wiederum GRE (Generic Routing Encapsulation), ein Protokoll, welches ursprünglich durch CISCO entwickelt wurde und welches eine Vielzahl von Netzwerkprotokollen transportieren kann, u.a. ipv4, ipv6, unicast und mulicast sockets, etc..

6.3.1.4. Die Authentifizierungprotokolle im Einzelnen

PAP – Password Authentication Protocol.

Auf dieses Protokoll wird nicht näher eingegangen, da es mit Klartextpassworten arbeitet und deshalb für den Einsatz im WLAN-Umfeld nicht geeignet ist. Eine andere Bedeutung erlangt es im Zusammenhang mit EAP-TLS, wo der Transport durch eine darunter liegende Schicht gabgesichert wird und auch bei Verwendung von „One Time Passwords“, kurz OTP, die über einen alternativen Weg bereitgestellt werden (z.B. SMS).

CHAP

Das Challenge Handshake Authentication Protocol bietet erstmals eine Möglichkeit zur Authentifizierung ohne Klartext-Passwörter. Dieses Protokoll wurde weiterentwickelt und praktisch durch MSCHAP verdrängt.

MSCHAP Microsoft Challenge Handshake Authentication Protocol

Diese Variante des CHAP-Protokolls weist trotz des Eratzes der Klar-Text-Passworte durch einen Hash immer noch wesentliche Schwächen auf.

Bei der Generierung des RESPONSE-Pakete werden zwei Hashes mit demselben Schlüssel erstellt: der LAN-Manager-Hash und der NT-Hash, wobei der erstere ein leichter zu hackender Hash ist. Dadurch wird es für Angreifer einfacher, den NT-Hash abzuleiten.

Des weiteren, wird bei der Herstellung des Hashes ein Bereich davon mit Nullen aufgefüllt. Dadurch wird der Bruteforce und Dictionary Attacken vereinfacht, da man von einer geringeren Entropie (Menge an Möglichkeiten) für das Passwort und dessen Hash ausgehen kann. Bei Heterogenen Systemen mit Linux ist des Weiteren die Passwortlänge auf acht Zeichen begrenzt, was die Menge der Passworte weiter reduziert.[PPTP2]

Wie bei allen passwortbasierten Authentifizierungsverfahren liegt eine große Schwäche in der Komplexität der Passwörter, welche sensibel gegenüber dictionary- und brute force Attacken sind. Hier taucht auch das Dilemma auf, entweder oft die Passworte ändern zu müssen oder Passworte von hoher Komplexität und Länge zu verwenden.

In einem Drei-Wege-Challenge-Response-Handshake-Verfahren wird ein CHALLENGE (eine Zufallszahl) verschickt, die vom Peer mit dem Secret verhasht wird. Die Antwort wird vom Authenticator mit einem eigen generierten Hash verglichen, der dann mit Accept oder Reject antwortet.

Möglich ist auch die Überprüfung des Authenticators durch den Peer, wodurch beide Seiten verifiziert werden können (mutual authentication), falls die Authentizität des Einwahlservers nicht durch eine dedizierte Leitung/Verbindung bereits sichergestellt ist.

Die Mindestanforderung an den Chiffrierer ist der HMAC-MD5 Algorithmus (Keyed-Hashing for Message Authentication).

MS-CHAP ist weitestgehend Rückwärtskompatibel mit CHAP.

Die wesentlichen Unterschiede beziehen sich hauptsächlich auf Kompatibilitätserhaltung zu bereits etablierten Produkten von MS und beinhalten:

- Verwendung von Passwort-Hash statt des Klar-Text-Pasworts
- Wiederholte Abfrage des Passworts bei Fehleingaben
- Ein Satz von Fehlercodes für den Benutzer

MSCHAP v2 - Microsoft PPP CHAP Extensions, Version 2

Diese Erweiterung beinhaltet im Wesentlichen die „mutual authentication“ in einem 3-Wege-Verfahren und die Veränderung der Länge des Challenge-Strings, wodurch zusätzliche Sicherheit ermöglicht wird.

Die „stateful encryption“, bei der die Schlüssel nicht wechseln, wurde durch eine stateless encryption abgelöst. Hier arbeitet der Authenticator mit einem anderen Schlüssel als der PEER, wobei beide ihre Schlüssel von dem gleichen Passwort-Hash (Secret) ableiten. Der LAN-Manager-Hash wurde komplett durch den kryptografisch stärkeren NT-Hash verdrängt, wobei das Verfahren an sich beibehalten wurde.

Sicherheitserwägungen

Die durchaus praktische Erweiterung um Fehlercodes und die Wiederholung der Passwortaufforderung birgt jedoch auch Gefahren. Es wird möglich, durch Ausprobieren das richtige Passwort zu erraten, weshalb die Anzahl der Wiederholungen begenzt werden sollte. Weiterhin bietet die Klartextübertragung des Challenge dem potenziellen Angreifer die Möglichkeit, durch Ausprobieren Rückschlüsse auf den Passwort-Hash zu ziehen. Die Möglichkeit den Umstand zu mildern besteht darin, ein komplexes Passwort zu wählen und es oft zu wechseln. Ein weiteres Problem stellt die Übertragung des Loginnamens im Klartext dar. Dadurch wird ein wesentlicher Teil der Logindaten offebanbart und ein potenzieller Angriff erleichtert. [PPTP1]

6.3.1.5. MPPE-Verschlüsselung

Im Rahmen des PPP besteht die Möglichkeit mit MPPE [RFC3078] (Microsoft Point to Point Encryption) zu verschlüsseln. Dieses Protokoll verwendet den RSA/RC-4 Stromchiffrierer, um mit 40, 56 oder 128-bit langem Schlüssel zu verschlüsseln. Damit lässt sich zusätzlich zur Authentifizierung der Benutzer auch eine Vertraulichkeit der Daten und deren Konsistenz erreichen. In Verbindung mit MSCHAPv2 kann eine periodische Reinitialisierung der Schlüssel ausgehandelt werden, wodurch zusätzliche Sicherheit erzielt werden kann. Es sind aber auch andere Verfahren zur Erzeugung der Initialschlüssel vorgesehen, so z.B. Kerberos und TLS.

Auch wenn von der Integrität der Daten ausgegangen werden kann, ist das MPPE-Verfahren, bzw. dessen Metadaten dagegen nicht geschützt. So könnte ein Angreifer über das Kontrollprotokoll den Parteien suggerieren, die Stärke der Verschlüsselung, also die Schlüssellänge, herabzusetzen, falls diese schwächere Verschlüsselungen durch eine entsprechende Konfiguration akzeptieren. Weiterhin sind auf diesem Wege DoS-Attacken möglich, indem permanent die Resynchronisation erzwungen wird.
Außerdem zeigt sich eine Schwäche in dem „stateful mode“, wo es vorkommen kann, dass mehrere Pakete mit dem selben Schlüssel chiffriert werden können. Dadurch wird es dem Angreifer erleichtert, in Besitz von mehr Daten für eine Kryptoanalyse zu kommen. Aus diesem Grund sollte „stateful encryption“ durch „stateless“, wo für jedes Paket ein neuer Schlüssel ausgehandelt werden kann, abgelöst werden.

6.3.1.6. Vergleich der Authentifizierungs-Verfahren im PPP

Die verschiedenen Authentifizierungverfahren des PPP wurden im Laufe der Zeit weiterentwickelt und deren meisten Schwächen beseitigt. Das MS-CHAPv2-Verfahren bietet einen brauchbaren und gleichzeitig einfach zu verwendeten defakto-Standard, der einzig empfehlenswert im PPTP-VPN-Umfeld ist; die Vorgängerverfahren wurden hauptsächlich aus Kompatibilitätsgründen beibehalten.
Ein Nachteil aller hier erwähnten PPP-Authentifizierungsprotokolle, der insbesondere im WLAN-Umfeld von Bedeutung ist, ist der Fakt, dass der Benutzername im Klartext übertragen wird. Dadurch wird ein Teil der zur erfolgreichen Authentifizierung benötigten Information in einem ansonsten ungeschützten Netzwerk preisgegeben. Eine Abhilfe schafft die Benutzung von WEP, was aber technisch gesehen absurd ist, da der Datenstrom dann mit dem gleichen Verfahren zweimal chiffriert würde.
Es wird deutlich, dass PPTP eine praktikable Komponente zur Absicherung des WLAN's ist, jedoch nicht der maßgeschneiderte Anzug. Andere, native Verfahren werden auf lange Sicht den Vorzug bekommen.

6.3.2. L2TP

Das Layer 2 Tunneling Protokoll [RFC2661] vereinigt viele Vorteile des PPTP mit Ciscos Eigenentwicklung L2F erweitert um die Sicherheit des IPSec.
So werden zusätzlich zu IP auch andere Protokolle wie IPX und NetBios unterstützt.
Die Verbreitung ist ähnlich PPTP durch das Microsoft Betriebssystem benutzerseitig weit gegeben. Zu den Nachteilen gehören:

- Komplizierte Einrichtung (Clientzertifikate erforderlich für eine sichere Kommunikation)
- Hoher Verwaltungsaufwand (PKI mit CRL's)
- CA angreifbar
- NAT-Traversal nicht durchgängig für alle Betriebssysteme implementiert
- Langer Protokollstack und dadurch großer Overhead
- Wenige open-source Implementierungen

Die Vorteile:

- Einfache Benutzung
- Hohe Sicherheit
- Weite Verbreitung

[L2TP1][MS2]

6.3.3. SSH

SSH ist eine Anwendung auf Schicht 7 des OSI-Modells. Es gestattet für gewöhnlich eine sichere Konsole auf einer entfernten Maschine. Es kann aber eben auch dazu genutzt werden, TCP-Sockets durchzutunneln. So ist SSH eine alternative Möglichkeit, den WLAN-Transport abzusichern, denn für jede Anwendung, beziehungsweise Dienst, kann ein SSH-Tunnel aufgebaut werden. X11-Anwendungen können im grafischen Modus auch remote ausgeführt werden, wobei eine Dosktop-Verbindung von lokal zum entfernten Rechner aufgebaut wird.

SSH benutzt die Public-Key-Verfahren mit den Algorithmen von RSA und DSA.

Die Version 2 sichert die Vertraulichkeit durch Verfahren wie: 3DES, Blowfish, CAST-128 und Arcfour. Der Zuwachs an Chiffrierern bringt zunächst eine bessere Performance in Bezug auf den Durchsatz durch optimierte Verfahren wie Blowfish, sowie Verbesserungen in der Sicherung der Integrität des Transports durch hmac (-md5 und -sha1) mit sich, im Vergleich zu Version 1. Abgerundet wird das Paket durch eine Kompression nach dem Zip-Verfahren, die jedoch nur bei langsamen Verbindungen sinnvoll erschein, da ansonsten größere Verzögerungen auftreten können.

SSH ist vor allem in der *nix Welt angesiedelt, wobei Implementierungen für alle gängigen BS existieren. Durch anerkannte, bereits länger bestehende Kryptografieverfahren, wird ein hohes Maß an Sicherheit erzielt. Die openSSL-Bibliothek, die Grundlage für viele Implementierungen hat erlangt immer mehr einen fortgeschrittenen „Reifezustand“.

Da SSH primär für remote-Anwendungen ausgelegt ist, mangelt es an Praktikabilität beim Einsatz als Transportsicherung. Das Public-Key-Verfahren erfordert, dass Client und Server sich noch vor der Aufnahme der Session kennen müssen, damit ein bestimmter Grad an Sicherheit erzielt werden kann. Dies ist hinderlich in einem HotSpot-System. SSH wird dennoch vereinzelt in dem Sinne eingesetzt, w.g. der genannten positiven Eigenschaften und in Ermangelung anderer Standards im WLAN-Sektor.

SSH’s Open-Source-Implementierungen haben sehr zur Beliebtheit dieser Software beigetragen und sie ist gut dokumentiert. Mit Hilfe einer guten Anleitung ist auch das TCP- und X11-Forwarding „in Gang zu bringen“, was für öffentliche Zugänge aber nicht Praktikabel erscheint, da es mit einigen mühen bei der Einrichtung verbunden ist und auch Fachkenntnisse erfordert.

6.3.4. IP-SEC

Eine Vielzahl von Angriffen auf Netzwerkkommunikation beruht auf der Tatsache, dass bei der Spezifikation des Internet Protokolls (IPv4) keine Methoden zur Sicherstellung von Authentizität, Vertraulichkeit und Integrität definiert wurden. Um diesen Mangel zu beheben wurden zwei Protokollerweiterungen erarbeitet, welche einen Standart zur Realisierung sicherer Kommunikationswege beschreiben [RFC 2401]. Entsprechend der gestellten Sicherheitsanforderungen können die beiden Protokolle ESP (Encapsulating Security Payload [RFC2406]) und AH (Authentication Header [RFC2402]) eingesetzt werden. Die primäre Aufgabe von ESP ist die vertrauliche Datenübertragung mittels kryptografischer Verfahren, während es die Aufgabe von AH ist, die Authentifizierung der kommunizierenden Systeme zu ermöglichen. Beide Protokolle bieten Möglichkeiten, die Integrität der gesendeten Pakete zu verifizieren. Zur Sicherung der Datenstrecke kann eines der beiden Protokolle oder eine Kombination beider eingesetzt werden.

Der Einsatz der Protokolle ist in zwei verschiedenen Betriebsmodi möglich, dem Tunnel- und dem Transportmodus.

6.3.4.1. Transport mode

Im Transport mode werden die durch die Protokolle gegebenen Sicherheits-Dienste zwischen zwei Host etabliert. Auf IP Pakete, welche zwischen zwei Rechnern versendet werden, werden auf der gesamten Übertragungsstrecke die Sicherungsmechanismen (ESP-Verschlüsselung und/oder AH-Authentifizierung) angewandt.

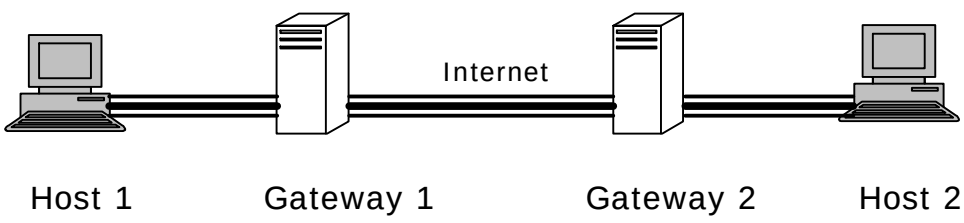


Abbildung 10 Transport mode

6.3.4.2. Tunnel mode

Beim Betrieb der Protokolle im Tunnel mode, werden Pakete, welche zwischen zwei Teilnehmern (Host 1 und Host 2) versendet werden, als Nutzlast in weitere IP-Pakete verpackt (Tunneln), welche auf einer Teilstrecke die ESP/AH–Mechanismen nutzen. Eine Verschlüsselung erfolgt hier nur auf der entsprechenden Teilstrecke. Da die ursprüglichen IP-Pakete eines Hosts in IP-Pakete mit ESP/AH eingeschlossen werden, greifen hier die Sicherheitsmechanismen für das komplette Ursprungspaket, so dass hier z.B. auch IP-Header-Information wie Ziel- / Absenderadresse der Kommunikationspartner verschlüsselt werden können, dieses Vorgehen wird als „Tunneln“ bezeichnet.

Wird beispielsweise ein IP-Paket von Host 2 an Host 1 gesendet, geschieht dieses mit der dem Host 2 bekannten IP-Adresse von Host 1 als Zieladresse des Paketes. Eingeschlossen in ein gesichertes IP-Paket erreicht dieses Gateway 1 und wird von diesem entpackt und wie von Host 2 abgesendet an Host 1 zugestellt.

Die Aufgabe von IPSec-Gateways ist es, das Ver- und Entpacken der IP-Pakete vorzunehmen und die Zustellung an das entsprechende Partner-Gateway sicherzustellen. IPSec wird im Tunnel mode betrieben, wenn mindestens ein Gateway an der Verbindung teilnimmt (Abbildung b zeigt den Einsatz des Tunnel mode zwischen einem Host und einem Gateway, der Tunnel wird hier direkt durch Host 2 aufgebaut und terminiert auf Gateway 1)

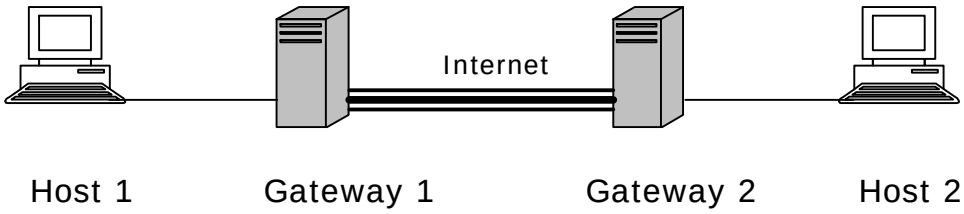


Abbildung 11 a) Tunnel mode Gateway - Gateway

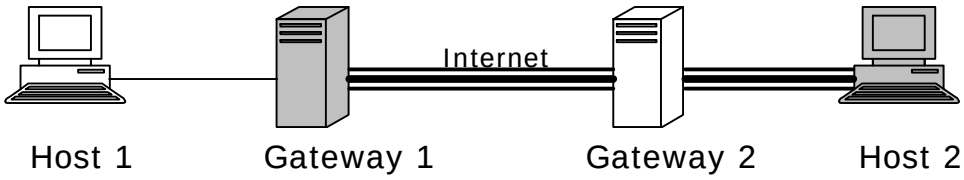


Abbildung 11 b) Tunnel mode Host - Gateway

In der IP-Sec Spezifikation wird der Begriff der Security Association (SA) geprägt, diese beschreibt die Parameter einer IP-Sec gesicherten Verbindung zweier Teilnehmer. Eine Verbindung wird hierbei durch das Tripel SPI (Security Parameter Index), der Ziel-IP-Adresse und dem verwendeten Protocol (ESP und AH verfügen über separate SAs) definiert. Beim SPI handelt es sich um eine zufällig generierte 32-bit Zahl, welche für die Verbindung generiert wurde, diese wird in dem Protokoll-Header übermittelt. Die durch die SA assoziierten Informationen einer Verbindung enthalten Angaben über den Verwendeten Algorithmus (Verschlüsselung, Authentifizierung), von den Algorithmen benötigte Informationen (Zertifikat, Schlüssel) sowie angaben zur Gültigkeitsdauer der Verbindung.

Diese Informationen werden beim Aufbau einer IP-Sec-Verbindung ausgehandelt, für eine detailierte Beschreibung des Verbindungsaufbaus und dem damit in Verbindung stehenden Austausch von Schlüsseln sei auf die Literatur verwiesen ([RFC 2408; RFC 2409]).

6.3.4.3. Authentication Header

Der Authentication Header befindet sich in einem IP-Paket hinter dem IP-Header, vor den Daten der Transportschicht (TCP/UDP), und hat folgenden Aufbau:

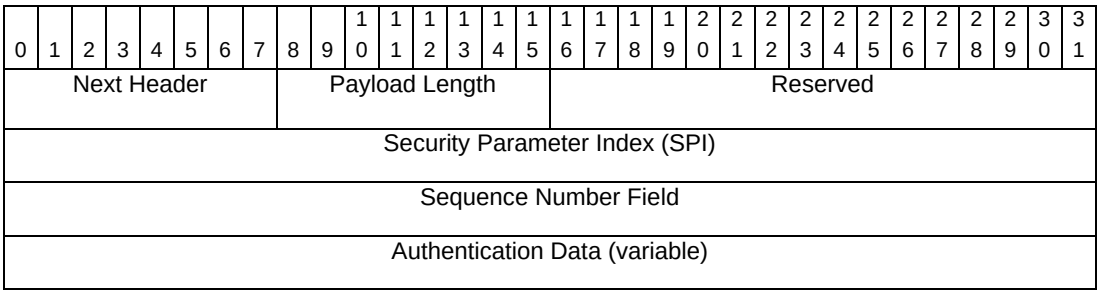


Abbildung 12 AH – Header Daten

Mittels eines geeigneten Algorithmus wird über die Daten des IP-Paketes (Transportschichtdaten [TCP-/UDP – Pakete], Daten des AH-Headers, sowie alle unveränderlichen IP-Header-Felder) ein Hash-Wert errechnet, eingesetzt werden hierfür Algorithmen wie MD5 oder SHA-1. Der errechnete Wert wird im Feld Authentication Data des AH-Headers übermittelt. Erreicht das Paket den Zielrechner, wird über die Daten des empfangenen Paketes erneut die Prüfsumme errechnet und mit dem übermittelten Wert verglichen. Wurden Daten des Paketes verändert, stellen die verwendeten Algorithmen sicher, dass dieses durch Unterschiede der Prüfsummen erkennbar ist.

original IP-Paket:

IP-Header	Nutzdaten

mit AH im Transportmodus:

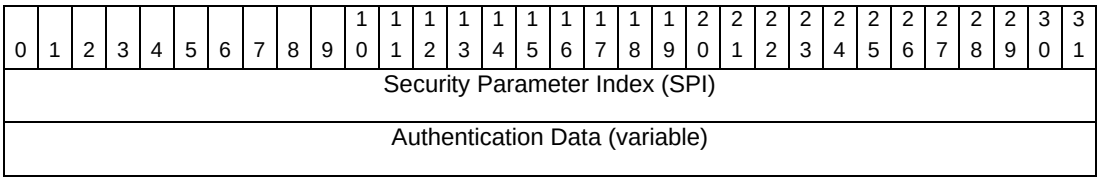
IP-Header	AH-Header	Nutzdaten

mit AH im Tunnelmodus:

IP-Header neu	AH-Header	IP-Header	Nutzdaten

6.3.4.4. Encapsulating Security Payload

ESP kommt zum Einsatz, wenn die Vertraulichkeit der übertragenen Daten mittels Verschlüsselung gesichert werden soll. Der Einsatz ist auch hier in beiden Betriebsmodi möglich. Im Transport bleibt der original IP-Header erhalten, nur die Nutzdaten (Daten der Transportschicht) werden verschlüsselt. Wird ESP im Tunnelmodus betrieben wird das komplette original IP-Paket verschlüsselt und dieses als Nutzdaten eines neuen IP-Paketes an den Tunnelendpunkt (Gateway) gesendet. Das Gateway stellt das getunnelte IP-Paket wieder her, entschlüsselt dieses und stellt es dem Zielrechner zu.



original IP-Paket:

IP-Header	Nutzdaten

mit ESP im Transportmodus:

IP-Header	ESP-Header	Nutzdaten	ESP-Trail	ESP-Auth

mit ESP im Tunnelmodus:

IP-Header neu	ESP-Header	IP-Header	Nutzdaten	ESP-Trail	ESP-Auth

Verbindungen, die durch Authentication Headers (AHs) geschützt sind, können nicht übernommen werden, da der Angreifer nicht in der Lage ist, gültige AHs zu erzeugen. Für die Generierung gültiger AHs benötigt er den geheimen Schlüssel.

Als Protokoll, welches die bisherigen Sicherheitslücken des Internet-Protokolls beseitigen soll, wird die IPSec-Protokollfamilie intensiv auf Schwachstellen untersucht. Eine detaillierte Analyse von Schwächen im Protokoll ist dem von Bruce Schneier und Niels Furguson verfassten Dokument „A Cryptographic Evaluation of IPSec“ zu entnehmen [Schneier 1999]. Ein wesentlicher Kritikpunkt

ist die Komplexität des Protokolls und deren schlechte Dokumentation, die eine fehlerfreie Umsetzung, sowie den Einsatz des Protokolls erschwert (hier seien nur der Parallele Betrieb von AH und ESP mit teilweise überschneidenden Funktionen erwähnt).

Obwohl auch für IPSec einige Schwachstellen identifiziert wurden, gilt es gegenwärtig als eines der sichersten, verfügbaren Protokolle.

6.3.5. SSL / TLS

Mit dem ursprünglich von Netscape entwickelten Protokoll SSL (Security Socket Layer) steht eine weitere Methode zur Verfügung, Daten verschlüsselt zu transferieren. Im Unterschied zu IP-Sec ist SSL im Protokoll-Stack zwischen den Protokollen der Transportschicht (wie z.B. TCP) und den Anwendungsprotokollen positioniert (siehe Abbildung 13). Bei den Anwendungen, welche auf das SSL-Protokoll aufsetzen, ist HTTP sicherlich das verbreitetste (und wird von allen gängigen Browsern unterstützt), der Einsatz von SSL ist aber auch mit anderen Protokollen, wie SMTP oder POP3 möglich.
Das Record Protokoll stellt innerhalb des SSL-Protokolls die untere Schicht dar, welche den Datenaustausch mit der darunter liegenden Transportschicht ermöglicht. Durch das Record Protokoll wird die Authentizität der versendeten Daten, sowie, durch Verschlüsselung, deren Geheimhaltung gesichert. Zu den weitern Aufgaben gehört die Fragmentierung der durch die Anwendung versendeten Datenpakete und deren (optionale) Komprimierung.
Die vom Record Protokoll versendeten Pakete haben die in Abbildung 13 dargestellte Struktur, die von der Anwendung zu versendenden Daten werden mittels eines geeigneten Algorithmus verschlüsselt und bilden den Nutzdatenbereicht des Record-Paketes. Zur Sicherung der Integrität wird weiterhin eine Prüfsumme über die Daten errechnet (MAC) und zur Überprüfung beim Empfänger mitgesendet, die Verschlüsselung schließt diesen Wert mit ein.

Die Verfahren zur Verschlüsselung und Berechnung der Prüfsumme, sowie die benötigten Schlüssel werden im Vorfeld zwischen Client und Server ausgehandelt, häufig verwendete Algorithmen sind z.B. DES, Triple-DES (Verschlüsselung) und MD5, SHA-1 (Prüfsumme), zur genauen Funktionsweise sei an dieser Stelle auf entsprechende Literatur zum Thema Kryptographie verwiesen.

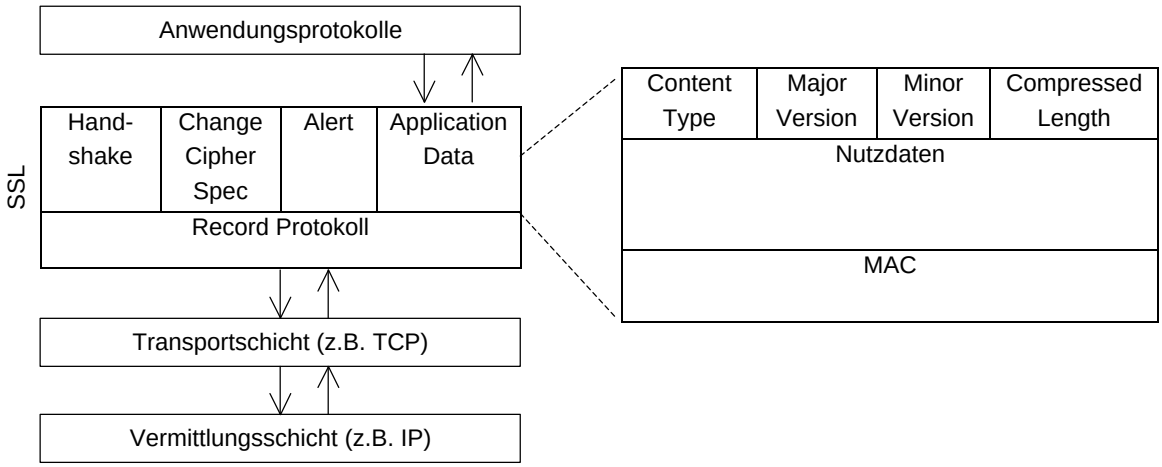


Abbildung 13 SSL/TLS Position im Protokoll-Stack (Record Protokoll)

Die zweite Schicht wird durch die SSL-Subprotokolle Handshake-, Change-Cipher-Spec-, Alert- und Apllication Data – Protokoll gebildet, wobei letztere den Datenaustausch mit der Anwendung realisiert. Die Aufgabe des Handshake-Protokolls ist es, beim Aufbau einer Verbindung die Verfahren zur Verschlüsselung und Prüfsummenerrechnung auszuhandeln, sowie die benötigten Schlüssel auszutauschen. Folgende Abbildung zeigt den Ablauf der während des Handshakes ausgetauschten Nachrichten.

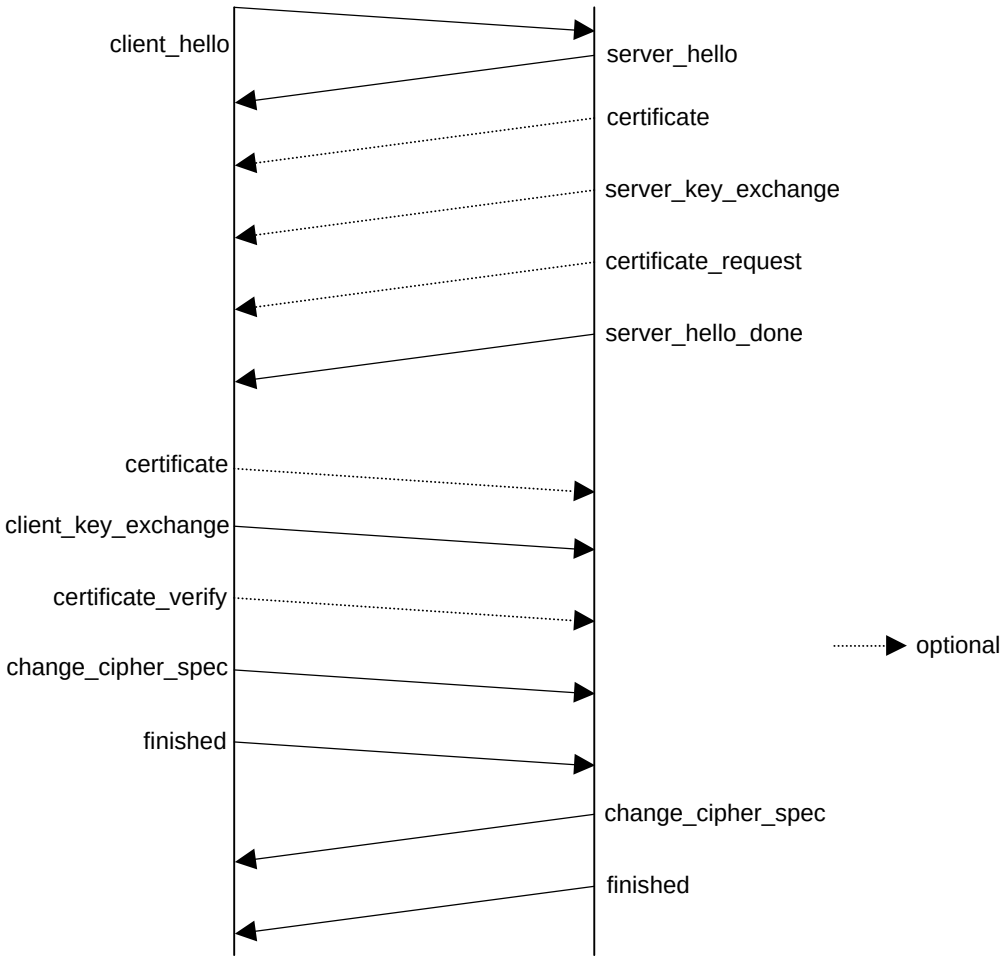


Abbildung 14 SSL-Handshake

Die Bedeutung der einzelnen Nachrichten zeigt folgender beispielhafter Ablauf eines SSL- Verbindungsaufbaues (die Authentifizierung erfolgt über ein X.509 - Zertifikat und RSA-Schlüssel) :

client_hello	Der Client signalisiert den Wunsch eines Verbindungsaufbaues, das client_hello-Paket enthält Angabe über die unterstützten SSL-Versionen, sowie die verfügbaren Verfahren zur Verschlüsselung und Prüfsummenberechnung (opt. Komprimierung).
server_hello	Die Antwort des Servers enthält die Festlegung auf die SSL-Version, sowie die verwendeten Algorithmen zur

	Verschlüsselung und Prüfsummenberechnung. Der Server teilt dem Client weiterhin einen Sitzungsnummer mit, welche die Sitzung im folgenden identifiziert.
Certificate	Zur Authentifizierung des Servers sendet dieser sein Zertifikat (X.509), welches seinem öffentlichen Schlüssel enthält, an den Client.
server_hello_done	Informationsaustausch seitens des Servers ist abgeschlossen.
client_key_exchange	Der Client generiert einen zufälligen Sitzungsschlüssel, welchen er verschlüsselt mit dem öffentlichen Schlüssel des Servers an diesen sendet. Dieser Schlüssel wird für den synchronen Verschlüsselungsalgorithmus der aufgebauten Verbindung verwendet.
change_cipher_spec	Mittels dieser Nachricht signalisieren Client und Server die umstellung der Kommunikation auf die ausgehandelten Parameter.
Finished	Diese Nachricht wird sowohl vom Client, als auch vom Server versendet. Der Verbindungsaufbau ist jetzt abgeschlossen, die Kommunikation erfolgt mit den ausgehandelten Parametern, dieses gilt bereits für die finished-Nachricht.

In der Regel wird bei einer SSL-Verbindung der Authentizität eines Servers (z.B. Web-Server) über dessen Zertifikat sichergestellt, ebenso ist aber auch die Authentifizierung des Clients möglich. Der Server fordert hierzu mittels eines „certificate_request“-Paketes während des Handshakes ein Zertifikat des Clients ein und überprüft dieses.

Die verschlüsselte Übertragung von Daten mittels SSL kann, sofern geeignete Algorithmen und ausreichende Schlüssellänge verwendet werden, als relativ sicher betrachtet werden. Schwachstellen sind eher während des Verbindungsaufbaus, dem Handshake zu finden. Ein Man-In-The-Middle Angreifer, der von Beginn des Handshakes

alle Pakete abfängt und eigene weiterleitet, kann sich so dem Server gegenüber als Client und dem Client als Server ausgeben, der Angreifer kann die gesendeten Daten einsehen und modifiziert weiterleiten. Die Durchführbarkeit solcher und ähnlicher Angriffe hängt oft von der eingesetzten SSL Implementierung ab (detaillierte Angriffsbeschreibungen sind unter [Schneier 1996] nachzulesen).

6.3.6. Kerberos

Wie bereits herausgestellt, ist eine zentrale Anforderung an (verteilte) IT-Systeme die gegenseitige Sicherstellung der Authentizität der teilnehmenden Personen und Systeme. Eine Infrastruktur bereitzustellen, die dieses möglichst unabhängig von den genutzten Diensten ermöglicht, ist Aufgabe sogenannter Authentisierungssysteme. Ein solches System ist das Mitte der 80er Jahre am MIT entwickelte Kerberos [MIT Kerberos] [Hübner 2003].

Die zentrale Rolle in einem Kerberos-System spielt das Key-Distribution-Center (KDC, auch Kerberos Server), welches die geheimen Schlüssel aller Teilnehmer (Benutzer und Dienste/Server) kennt. Die Nutzung eines Dienstes innerhalb eines durch Kerberos gesicherten Netzes setzt das Vorhandensein eines gültigen Tickets voraus, dieses stellt die Authentizität des Teilnehmers sicher. Die Aufgaben des Kerberos-Servers werden in die Dienste Authentication Server (AS) und Ticket-Granting-Server (TGS) unterteilt. Bei der ersten Anmeldung eines Benutzers im System kommuniziert dieser, bzw. der von ihm verwendete Client, mit dem Authentication Server, konnte der Benutzer sich authentifizieren (e.g. Passwort) wird ihm durch diese Aktion ein Ticket-Granting-Server-Ticket übermittelt. Um einen bestimmten Dienst in Anspruch zu nehmen braucht der Benutzer ein Ticket, welches explizit für die Nutzung dieses Dienstes durch ihn ausgestellt wurde, die Erstellung dieser Tickets ist Aufgabe des Ticket-Granting-Servers. Der Benutzer übermittelt zunächst das erhaltenen TGS-Ticket und den Namen des gewünschten Dienstes an den Ticket-Granting-Server, durch das Ticket (und dem ebenfalls vom AS zuvor erzeugten Sitzungsschlüssel) ist eine Eindeutigkeit des Benutzers

sichergestellt. Der Ticket-Granting-Server stellt jetzt ein Ticket für die Nutzung des gewünschten Dienstes aus. Der genaue Ablauf und die ausgetauschten Daten zwischen den teilnehmenden Systemen werden im folgenden dargestellt:

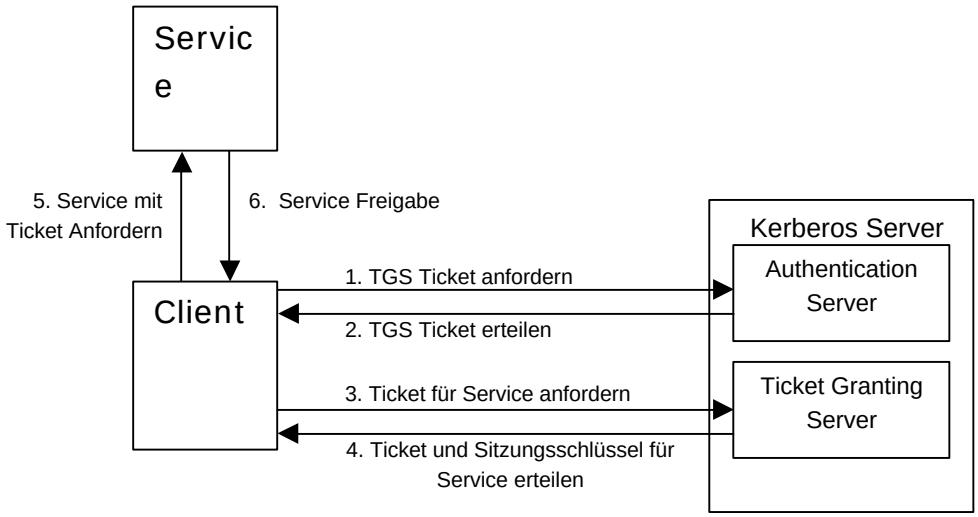


Abbildung 11 Ablauf Kerberos Authentifizierung

1.	ID_{Client}, ID_{TGS}, $T_{current}$	Der Client beginnt die Authentifizierung durch Senden seines (eindeutigen) Namens, denjenigen des Ticket Granting Servers, sowie die aktuelle Zeit. AS
2.	$\{K_{Client,TGS}, T_{current}\}_{K_{Client}}$, $\{Ticket(ID_{Client}, ID_{TGS}, K_{Client,TGS}, T_{current})\}_{K_{TGS}}$	Der Server generiert einen Sitzungsschlüssel für die Kommunikation zwischen Client und TGS ($K_{Client,TGS}$). Diesen sendet er verschlüssel mit dem geheimen Schlüssel des Clients (K_{Client}) an diesen zurück. Desweiteren sendet er ein Ticket für den TGS, welches den Namen des Clients, des TGS und den erzeugten

		Sitzungsschlüssel enthält, dieses Ticket wurde mit dem geheimen Schlüssel des TGS verschlüsselt. Hat der Client diese Daten erhalten, entschlüsselt er mittels seines geheimen Schlüssels den Sitzungsschlüssel.
3.	$\{ID_{Client}, T_{current}\}_{K_{Client,TGS}}$, $\{Ticket(ID_{Client}, ID_{TGS}, K_{Client,TGS}, T_{current}\}_{K_{TGS}}$, $ID_{Service}$	Um ein Ticket für den gewünschten Service zu erhalten, sendet der Client an den TGS seine Identifikation sowie einen Timestamp, verschlüsselt mit dem vom AS erhaltenen Sitzungsschlüssel für die Kommunikation mit dem TGS. Die Nachricht enthält des weiteren das vom AS ausgestellte Ticket für die Kommunikation mit dem TGS sowie den Namen das Services.
4.	$\{\{Ticket(K_{Client,Service}, Id_{Client}, T_{current})\}_{K_{Service}}$, $K_{Client,Service}$, $ID_{Service}$, $T_{current}\}_{K_{Client,TGS}}$	Der TGS entschlüsselt das vom Client gesendete Ticket mit seinen privaten Schlüssel und entnimmt ihm den Sitzungsschlüssel, mit welchem er versucht die Identifikationsdaten des Clients zu entschlüsselt. Wurden die Client-Angaben verifiziert, erzeugt der TGS ein Ticket für den angeforderten Service, mit dessen privaten Schlüssel ($K_{Service}$) verschlüsselt. Dieses Ticket enthält einen neu generierten Sitzungsschlüssel für die Kommunikation zwischen dem Client und dem Service, dieses wird dem Client ebenfalls übermittelt. Die gesamten Daten werden mit dem Sitzungsschlüssel $K_{Client,TGS}$ chiffriert übertragen.
5.	$\{ID_{Client}$, $T_{current}\}_{K_{Client,Service}}$, $\{Ticket(K_{Client,Service}, Id_{Client}, T_{current})\}_{K_{Service}}$	Zur Nutzung eines Dienstes wird das für diesen ausgestellte Ticket, sowie die Identifikation des Benutzers

		(verschlüsselt mit dem für diese Kommunikation vom TGS erstellten Sitzungsschlüssel) übermittelt.
6.	$\{T_{current}\}_{K_{Client,Service}}$	Wurden die Angaben vom Service erfolgreich verifiziert, kann die eigentliche Nutzung (e.g. E-Mail senden) beginnen. Der Service signalisiert dieses durch Senden des Zeitstempels verschlüsselt mit dem gemeinsamen Sitzungsschlüssel.

Die in den Schritten 1. und 2. beschriebenen Authentifizierung gegenüber dem AS und die damit verbundene Benutzerinteraktion (Eingabe Passwort) erfolgt einmal zu Beginn der Nutzung des Systems. Wurde das TGS-Ticket ausgestellt, ist die Anmeldung an spezielle Dienste und die dafür erforderliche Anfrage eines Tickets für den Benutzer transparent, da dieses vom Kerberos-Client ohne erneute Passworteingabe durch das TGS-Ticket möglich ist (Single Sign On).

Der Austausch von Daten innerhalb das Kerberos-Protokolls (Tickets, Zeitstempel, Ids) erfolgt, wie bereits in der Ablaufbeschreibung erwähnt, verschlüsselt. Neben der Verschlüsselung der Tickets mit dem Privaten Schlüssel des Adressierten Servers erfolgt eine Verschlüsselung mit dem Sitzungsschlüssel, welcher vom AS bzw. TGS erzeugt wurde. Zum Einsatz kommen hier symmetrische Verfahren wie DES/3DES. Soll der Datenaustausch mit dem vom Benutzer angeforderten Dienst ebenfalls verschlüsselt erfolgen, kann der Sitzungsschlüssel auch hierfür verwendet werden, sofern die Implementierung dieses ermöglicht.

6.3.7. Firewall

Bei den zuvor beschriebenen Methoden zur Sicherung der Kommunikation zwischen IT-Systemen erfolgte dieses durch entsprechende Modifikationen der durch die kommunizierenden Systeme eingesetzten Methoden zum Datenaustausch (Einsatz eines geeigneten Protokolls). Der durch den Einsatz einer Firewall verfolgte Ansatz ist die Kontrolle des Datenstroms zwischen den Systemen, diese bleiben davon weitestgehend unberührt. Zum Einsatz kommt eine Firewall, wenn der Datenstrom zwischen zwei (oder mehreren) Netzen mit unterschiedlichem Sicherheitsniveau kontrolliert werden soll. Die Schnittstelle zwischen Netzwerken wird gewöhnlich durch einen Router gebildet, welcher auf der Netzwerkschicht Pakete zwischen diesen vermittelt. Da dieses eine geeignete Stelle ist, um den Datentransfer mittels einer Firewall weiterer Kontrollen zu unterziehen, ist häufig eine Verbindung von Firewall und Router anzutreffen.
Eine gebräuchliche Struktur eines durch eine Firewall gesicherten Netzwerkes zeigt Abb. 16, es wird anhand des geforderten Sicherheitsniveaus zwischen dem „internen Netz“, der sogenannten DMZ (Demilitarisierte Zone) in welcher sich öffentlich zugängliche Systeme, wie z.B. ein Webserver befindet und dem Zugang zum Internet unterschieden. Es wird ein Regelwerk erstellt, welches festlegt, in welchem Umfang zwischen den Netzen Daten ausgetauscht werden dürfen, dieses wird von der Firewall umgesetzt.

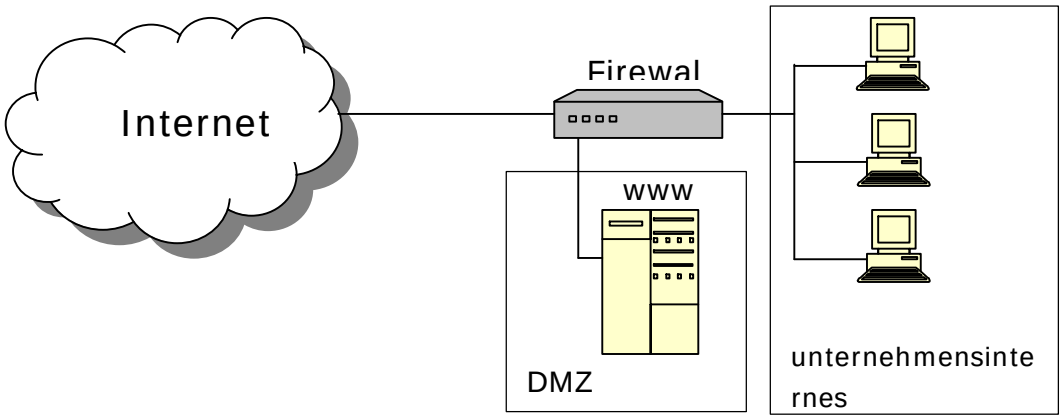


Abbildung 16 Firewallgesichertes Netzwerk

Firewall-Systeme lassen sich in zwei Kategorien unterteilen, Paketfilter und Proxy-Gateway, welche sich im wesentlichen durch die Protokollebenen unterscheiden, auf welchen sie den Datenstrom kontrollieren.

6.3.7.1. Paketfilter

Ein Paketfilter kontrolliert den Datenfluss zwischen den einzelnen, angebundenen Netzwerkabschnitten auf der Netzwerk- und Transportschicht. Für die Kombination Eingangsnetzwerk (über welche Schnittstelle kommt des Paket rein?) und Ausgangsnetzwerk (wohin soll es weitergeleitet werden?) werden Regeln definiert, welche anhand folgender Paketeigenschaften festlegen, ob eine Weiterleitung erfolgen darf:

- IP-Header Daten:
    - IP-Ursprungsadresse
    - IP-Zieladresse
- Daten des gekapselten Paketes der Transportschicht:
    - Art des Protokolls (TCP, UDP, ICMP)
    - TCP/UDP-Absender-Port
    - TCP/UDP-Ziel-Port
    - Flags des TCP-Headers (ACK, SYN, ...)
    - ICMP message type

Oft wird das Regelwerk eines solchen Paketfilters als Auflistung der Filterregeln in tabellarischer Form, wie in folgender Abbildung auszugsweise zu sehen, erstellt:

Nr.	Interface	IP-Quelle	IP-Ziel	Protokoll	Ziel-Port	Aktion
1	Internet	*.*.*.*	www in DMZ	http	80	ACCEPT
2	Internet	*.*.*.*	ftp in DMZ	ftp	21	ACCEPT
3	Internes Netz	212.23.1.*	Internet	HTTP	ALL	ACCEPT
4	ALL	ALL	ALL	ALL	ALL	DENY

Beispielsweise wird hier geregelt, dass der Zugriff aus dem Internet nur auf Rechner in der DMZ, und zwar die dort befindliche Server mit www- und ftp-Diensten erlaubt ist. Aus dem internen Netz dürfen alle Rechner eines Netzwerksegmentes uneingeschränkt auf das Internet zugreifen. Wird ein Paket durch den Filter analysiert werden die Regeln sequentiell abgearbeitet, entsprechen die Eigenschaften des Paketes denen einer Regel, wird die zugeordnete Aktion ausführt. Folge dieser Aktion ist, dass das Paket passieren darf (ACCEPT) oder verworfen wird und somit keine Verbindung zustande kommt. Hier wird häufig zwischen REJECT und DENY unterscheiden. Wird durch die Regel REJECT vorgegeben, wird das Paket verworfen und eine Fehlermeldung zurückgesendet (ICMP). Im Gegensatz dazu wird bei DENY auf eine Fehlermeldung verzichtet. „Alles was nicht erlaubt ist, ist verboten“, ist eine der wichtigsten Grundregeln beim Erstellen von Firewallregeln. In dem gezeigten Beispiel wird diese durch den letzten Eintrag realisiert. Wird ein Paket analysiert und es trifft keine der Regeln auf dieses

zu, trifft der Paketfilter auf die letzte Regel, welche alle Pakete, die bis zu dieser Regeln nicht als „akzeptabel“ erkannt wurden verworfen werden.

Für den Einsatz eines Paketfilters als Firewall spricht dessen leichte Verfügbarkeit, oft bieten bereits vorhandene Router Möglichkeiten zur Erstellung von Filterregeln. In größeren Netzwerken erreicht das Regelwerk allerdings schnell einen unübersichtlichen Umfang. Die Tatsache, dass die Analyse auf Internet-/Transportschicht erfolgt bringt einige protokollbedingte Schwächen mit sich, so ist es nicht möglich, auf bekannte Muster innerhalb der Pakete, die Angriffe auf bestimmte Applikationen bedeuten können, zu reagieren.

6.3.7.2. Proxy-Gateway

Im Gegensatz zu Paketfiltern erfolgt die Kontrolle des Datenstroms bei Proxy-Gateways auf Applikations-Ebene. Hierzu ist eine Trennung der Verbindung an der Schnittstelle des zu schützenden (Unternehmens-)Netzwerkes vorzunehmen, diese erfolgt im Gateway.

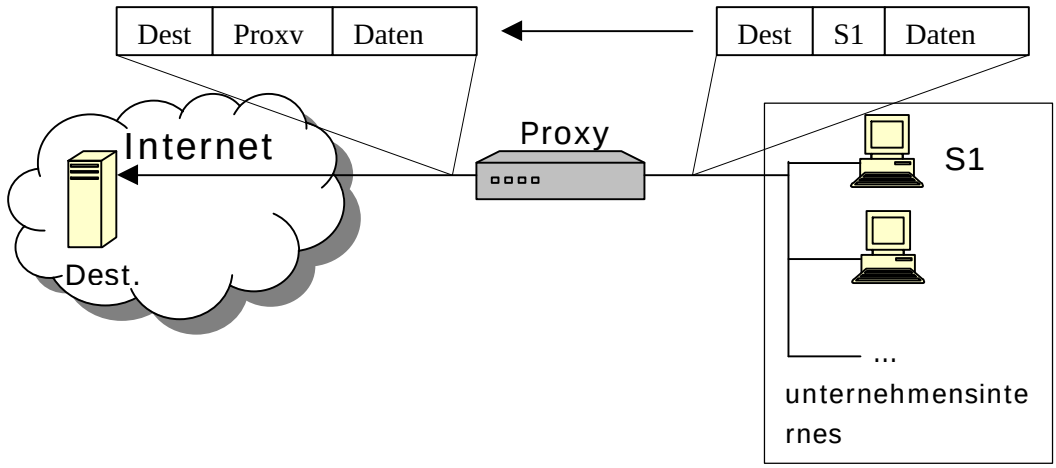


Abbildung 17 Proxy-Gateway

Der Proxy nimmt das Paket entgegen und sendet es stellvertretend an den Zielrechner, dabei wird die original Absender-Adresse des Rechners im geschützten Unternehmensnetzwerk durch die Adresse des Proxys ersetzt. Die Antwort-Pakete gelange so zunächst an den Proxy zurück. Dieser ordnet es dann dem Rechner, der die ursprüngliche Anfrage gestellt hat, zu und leitet es weiter. Nach außen bleiben die internen Adressen somit verborgen. Das Proxy-Gateway hat somit nicht nur die Möglichkeit zu kontrollieren, welche Verbindungen aufgebaut werden dürfen, es kann den Inhalt der ausgetauschten Daten auch auf Applikationsebene untersuchen. Der Aufwand für dieses Verfahren ist allerdings um einiges höher als eine Paketfilterung, was sich auf die Performance auswirkt.

6.4. Native WLAN-Sicherheit

In Zeiten, in denen die Preise für WLAN-Eqipment ständig fallen und mittlerweile fast schon das Niveau von Ethernet-Komponenten erreichen, ist die Frage „was soll ich kaufen“ wohl leicht beantwortet. Die Käufer aus dem Consumer-Bereich entscheiden sich für das Internet im Garten, wie die Werbung verspricht und nicht so schnell für eine oft kostspielige Kabelfestinstallation. Dementsprechend soll die Einrichtung und Wartung solcher Komponenten möglicht einfach sein und dennoch ein Maß an Sicherheit bieten.

6.4.1. WARUM WEP & co, wenn es VPN und IPSec gibt?

Neben den allgemeinen Sicherungsprotokollen für Netzwerke wie IPSec,
gibt es speziell für WLAN entwickelte, native Absicherungsmöglichkeiten.
Der hauptsächliche Grund für die weiteren Maßnahmen liegt darin, dass das physikalische Übertragungsmedium Luft, im Gegensatz zu Kabelnetzwerken, überall „anzapfbar“ ist. Dieses ist durch IPSec (PSK) oder andere VPN’s nicht ganz zu beheben. Es bleiben offene Stellen wie Dateifreigaben oder andere offene Ports.[Hill][KNIG]

Die Verkabelung bietet von Haus aus einen gewissen Grad an Sicherheit, u.z. dadurch, dass die Kabelinstallationen in geschützten Bereichen gemacht werden. Ob Zuhause oder im Rechenzentrum, ein Zugriff auf diese Netzwerke erfordert einen direkten Zugriff auf das Kabel. Bei WLAN ist das grundverschieden. Jedermann kann mittels im Internet vorhandener Tools, wie z.B. tcpdump, den unverschlüsselten Datenverkehr des Nachbars abhören und missbrauchen.

Viele der Hersteler der WLAN-Hardware tendieren eher dazu, schnell ein funktionierendes Produkt bereitzustellen, als auf die Risiken hinzuwesen. So werden Sicherheitsfragen oft in den Benutzeranleitungen kaum angegangen und der Kunde benutzt letztendlich ein System, welches von Haus aus keinerlei Schutz bietet und andere dazu einlädt, den eigenen Datenverkehr abzuhören oder das Internet mitzubenutzen.

Dabei ist das WEP bereits ein Kompromiss zwischen Sicherheit und einfacher Einrichtung. Das WEP bietet ein Mindestmaß an Sicherheit, ohne weitere Software oder Geräte kaufen zu müssen. Dieses Verfahren soll den Unterschied zwischen kabelgebundenen und drahtlosen Netzen egalisieren, ohne dabei gleich einen IT-Fachmann hinzuziehen zu müssen. Dieser Anspruch wurde durch WEP allein zwar nicht erfüllt, ist aber dennoch ein Baustein für mehr Sicherheit. [WiFi1-6]

6.4.2. Was gibt es an Sicherungsmethoden und wozu sind sie geeignet?

Der Standard IEEE 802.11 umfasst Methoden, die zu mehr Sicherheit in einem natürlicherweise angreifbarem Übertragungsmedium beitragen sollen. Das Mehr an Sicherheit will man hier, auf OSI-Schicht 2 [Tanenbaum], der Sicherungsschicht angehen. So kann die Assoziation einer Basisstation mit einem Client unterbunden werden, indem keine SSID gesendet wird. Diese einfache Schutzvorkehrung setzt die Kenntnis des Netzwerknamens durch den Client (Station/Host) voraus, anderenfalls müsste er erst erraten werden. Dies ist eine erste Hürde, welche vergleichbar damit ist, die passende Dose im Kabelnetzwerk zu finden.

Weiter bleibt die Möglichkeit, den Zugriff auf das WLAN Netzwerk einzuschränken, zu erwähnen, die auf Access Control Listen setzt. Hierbei werden entweder nur bekannte Netzwerkadapter zugelassen oder bestimmte ausgeschlossen.

Die Authentifizierung und Verschlüsselung wird mittels WEP durchgeführt. Die anfänglich mit 40 bit angesetzte Schlüssellänge wurde mehrfach erhöht und liegt zur Zeit bei bis zu 152 bit, wobei die ursprüngliche Schlüssellänge von 40 bit nach wie vor, aus Gründen der Exporteinschränkungen in manche Länder der Welt, beibehalten wurde, um einen großen Absatzmarkt für WLAN-Produkte zu haben.

Die manuelle Einrichtung der „pre-shared secret“ wird durch den Standard 802.1x 802.1x (Port Based Access Control) in Verbindung mit EAP (Extensible Authentication Protokoll) verbessert. Hierbei werden einige Probleme des autorisierten Zugriffs auf das Netzwerk auf Schicht 2 angegangen und der WEP-Schlüsselaustausch automatisiert.

Die Vertraulichkeit und Integrität der Daten werden aber erst durch die Kombination aus einer der EAP-Methoden (Token, Zertifikate, One-Time Passwörter, Radius, ...) und, auf der anderen Seite, einer Verschlüsselung hergestellt. Das WEP wird durch dynamische Schlüssel erst ernsthaft im Geschäftsumfeld möglich, wobei grundlegende Probleme aber nicht gelöst wurden.

Zukünftige Sicherheitsstandards der WECA namens WPA und WPA2 [WiFi] setzen auf eine Software-Aktualisierung der Produkte (firmware update), um die Schwächen des ursprünglichen WEP auszugleichen. Letzteres setzt auf AES (Advanced Encryption Standard), welches einen erheblichen Rechenaufwand bei zahlreichen Chiffrierern erfordert, der wiederum in den meisten Fällen einen Coprozessor auf der WLAN-Karte und in der Basisstation erfordert (zumindest bei älteren reinen 802.11b-Modellen). Die kommenden Generationen des WLAN-Equipments nach 802.11a/b/g verfügen bereits über AES-Hardwarebeschleuniger.

6.4.3. Die Verfahren im Einzelnen

6.4.3.1. SSID, MAC-ACL

Grundsätzlich ist ein dreistufiges Zugangsmodell vorgesehen, das zwischen nicht verbundenen, assoziierten und authentifizierten Stationen unterscheidet.
Die Assoziation erfolgt aufgrund der Übereinstimmung des SSID (Service Set Identifier).
Möglich ist aber auch die Eintragung des Bezeichners ANY oder eines leeren Strings, wodurch diese Identifikation mittels diesen Verfahrens außer Kraft gesetzt wird.

Je nach Größe und Anzahl der Komponenten eines drahtlosen LANs bestehen verschiedene Identifizierungsmöglichkeiten für ein drahtloses LAN:

Der Netzwerkname oder die SSID (Service Set Identifier oder Servicegruppenkennung) – Sie Identifiziert das drahtlose Netzwerk. Alle drahtlosen Geräte im Netzwerk müssen dieselbe SSID verwenden.

ESSID (Extended Service Set Identifier oder erweiterte Servicegruppenkennung) - Dies ist eine gesonderte SSID, die zur Identifizierung eines drahtlosen Netzwerks verwendet wird, das Zugriffspunkte (AccessPoints) enthält.

IBSSID (Independent Basic Service Set Identifier oder unabhängige Basis-Servicegruppenkennung) - Dies ist eine besondere SSID, die zur Identifizierung eines Netzwerks von drahtlosen Computern verwendet wird, die für die direkte Kommunikation untereinander (Peer to Peer, AdHoc-Netzwerk) ohne Zugriffspunkt konfiguriert wurden.

BBSSID (Basic Service Set Identifier oder Basis-Servicegruppenkennung) - Eindeutige Kennung für jedes

drahtlose Gerät. Die BSSID ist die Ethernet MAC-Adresse des Geräts.

Broadcast SSID - Ein Zugriffspunkt kann auf Computer reagieren, die Testpakete mit der Broadcast SSID senden. Wenn diese Funktion auf dem Zugriffspunkt aktiviert ist, kann jeder drahtlose Benutzer sich mit Hilfe einer leeren SSID (Null-SSID) mit dem Zugriffspunkt verbinden.

6.4.3.2. WEP (Wired Equivalent Privacy)

Der Standard 802.11 definiert ein Authentifizierungs- und Verschlüsselungsverfahren, das die gleiche Sicherheit bieten soll, wie eine Kabel-Festinstallation. Die Sicherung soll durch eine Verschlüsselung der Daten mit einem 40-bit langem Schlüssel (später 104-bit und nicht standardkonforme 152 bit) erfolgen. Es wird aber auch ein s.g. „Initialisation Vector“ (IV) als Teil des Schlüssels im Klartext übertragen. Der IV dient als dynamische Komponente bei der Verschlüsselung und hat eine feste Länge von 24 bit. Dies hat sich als unzureichend herausgestellt, da durch die Erhöhung der Übertragungsrate der IV schneller überläuft als ursprünglich vorgesehen, so werden oft gleiche Schlüssel verwendet, was dem Hacker den Angriff erleichtert. Es wurden Verfahren entwickelt, welche u.a. den Überlauf diesen Zählers ausnutzen, um den Schlüssel aus passiv ausgelesenen Netzwerkdaten zu extrahieren. Die Schwäche von WEP liegt ferner nicht in dem eingesetzten Verschlüsselungsverfahren (RSA/RC-4), sondern beruht auf einer mittelmäßigen Umsetzung des Verfahrens, das kaum Dynamik zuläßt. WEP wurde auf dem Technologiestand der frühen 90-er Jahre entwickelt und seit dem nicht wesentlich verbessert, obwohl sich die äußeren Umstände geändert haben (z.B. Übertragungsrate von 2 auf über 54Mbit/s, höhere Sicherheitsanforderungen in Unternehmen). Hier wird es auch deutlich, dass eine Verlängerung des Schlüssels nur bedingt zu mehr Sicherheit führt. Nichtsdestotrotz ist WEP eine Hürde, ohne die wirklich jeder erfahren könnte, was andere im Netz so treiben. Leider ist dieses Verfahren durch die Medien so in Verruf geraten, dass die Anwender davon Abstand nehmen, es überhaupt noch einzusetzen. Dazu hat aber auch die Industrie im erheblichen Maße durch mangelhafte Aufklärung verleitet. So wird in den Handbüchern oftmals nicht hinreichend auf Risiken hingewiesen. Andererseits ist der Schutz mittels reinem WEP nur in geschlossenen Benutzergruppen möglich, da nur ein Schlüssel (-Set) existiert, den ja alle Teilnehmer kennen müssen.[8]

[8] Weitere Informationen zum Thema finden sich bei [INTN]

6.4.3.3. 802.1x (Port Based Access Control) und EAP (Extensible Authentication Protocol)

Die Schwächen des WEP wurden kurz nach dessen Bekanntgabe publik. Die Hersteller reagierten daraufhin mit zwei weiteren Verfahren, die das WEP entscheidend verbessern.
Das 802.1x-Protokoll [IEEE802.1x] dient hierbei dem kontrollierten Zugriff auf Netzwerkressourcen am AccessPoints. Nicht authentifizierte Benutzer haben lediglich die Möglichkeit, sich am AccessPoint anzumelden. Alle Netzwerk-Aktivitäten auf der IP-Schicht werden unterbunden. Zur Authentifizierung wird eines der EAP-Verfahren eingesetzt, wobei der Authentifizierungsserver meist nicht der Accesspoint selbst ist, sondern der AAA-Server des Unternehmens wie z.B. der RADIUS-Server.
Dadurch wird es erstmals möglich, Sicherheitsregeln pro Benutzer zu führen. Außerdem wird das Problem des statischen Schlüssels durch ein dynamisches Schlüssel-Distributionsverfahren behoben. Der Hacker bekommt so kaum ausreichend Daten für einen offline-Angriff. Der Benutzer freut sich letztlich über die Einfachheit der Benutzung und über ein signifikantes Mehr an Sicherheit.

6.4.4. Die Varianten des EAP

EAP [EAP] ist ein offener Standard für den es mehrere Implementierungen gibt. Letztlich ist die Industrie hier gefragt, Verfahren für die unterschiedlichen Bedüfnisse zu finden und umzusetzen, entsprechend viele Varianten gibt es auf dem Markt[9]:

- LEAP
- EAP-TLS
- EAP-MD5
- EAP-TTLS
- PEAP

[9] Eine gute Quelle für weitere Informationen stellt [METH] dar.

6.4.4.1. LEAP (Lightwight-EAP)

Cisco reagierte als erster großer Hersteller im WLAN-Umfeld auf die Schwächen von WEP mit dem Lightwight-EAP. Diese Lösung war zumindest anfänglich noch sehr proprietär und funktionierte nur mit Cisco-Equipment: WLAN-Adapter und Accesspoints sowie dem ACS-Radius-Server. Die vorhandene Infrastruktur auf Basis von Windows-Servern oder LDAP ließ sich leicht anbinden, so dass eine schnelle Integration möglich war. Eine Schwäche zeigt dieses Protokoll gegenüber Man-In-The-Middle-Attacken, durch die das gesamte Netzwerk kompromitiert werden könnte.

6.4.4.2. EAP-TLS (Transport Layer Security)

Diese Vaiante setzt auf eine Erweiterung des SSL-Protokolls, das TLS. Die Stärke des TLS liegt in der PKI (Public Key Infrastructure). Es werden Zertifikate auf Seiten des Benutzerrechners und des AAA-Servers eingesetzt, um die Authentifizierung sicher zu gestalten. Andererseits bedeutet das einen nicht zu vernachlässigenden administrativen Aufwand, die Zertifikat-Infrastruktur zu gestalten. Microsoft lindert mit dem Server-Betriebssystem das Problem, indem es die Verwaltungsmöglichkeiten darin integriert, einen Radius-Server mit ausliefert aber auch einen Client in die neuen Versionen seines Benutzer-Betriebssystems integriert.[EAP-TLS]

6.4.4.3. EAP-MD5

Dies ist das am wenigsten sichere Verfahren Es ist nicht für einen dynamischen Schlüsselaustausch geeignet. Weiterhin ist der MD5-Hash verwundbar gegen Wörterbuch-Angriffe. Der Server wird nicht authentifiziert, was das Risiko von Session Hijacking und Man-In-

The-Middle-Attaken erhöht. Das Verfahren ist vergleichbar mit der CHAP-Authentifizierung des PPP-Protokolls.

6.4.4.4. EAP-TTLS (Tunneled Transport Layer Security)

Dieses Protokoll bietet ein Höchstmaß an Sicherheit in Drahtlosen Netzwerken.
Zu den herausragenden Merkmalen von EAP-TTLS gehören:

- Login-Daten werden durch starke Verschlüsselung innerhalb von TLS geschützt
- Beide Endpunkte werden durch eine „mutual authentication“ sicher Identifiziert
- Das Verfahren erzeugt dynamische Schlüssel für Station und AccessPoint
- Die Verifizierung der Logindaten kann extern, z.B. durch Radius erfolgen
- Es kann eine Vielzahl an Authetifizierungsmethoden eingesetzt werden, so RSA/securID, Client-Zertifikate und auch proprietäre Mechanismen, welche zum Authentifizierungsserver durchgetunnelt werden können (PAP,CHAP,MSCHAPv1 und v2)
- TKIP (Temporal Key Integrity Protocol) und AES (Advanced Encryption Standard) verhindern Session Hijacking
- Schnelles Roaming zwischen Basisstationen durch „fast reconnect“

Dieses Verfahren zeichnet sich insbesondere dadurch aus, dass seitens des Clients keine Zertifikate erforderlich sind. Es hat eine breite Unterstützung seitens der Hersteller gefunden, insbesondere existieren zahlreiche Clients für alle erdenklichen Betriebssysteme. Die Serverkomponenten werden primär durch „Funk Software“ angeboten.

6.4.4.5. PEAP (Protected Extensible Authentication Protocol)

Diese Variante setzt sich zum Ziel, ähnlich EAP-TTLS ohne Client-Zertifikate auszukommen. Es soll vielmehr eine Infrastruktur für den sicheren Transport von Passwortdaten etabliert werden. Dazu soll ein Tunnelverfahren vor fremden Zugriff schützen.

PEAP beitet folgende Sicherheitsaspekte

- “Mutual authentication“
- dynamische Schlüsselerzeugung
- Gesicherte Benutzerauthentifizierung
- Fast reconnect“, z.B. beim Wechsel der assozierten Basisstation
- Paketfragmentierung und Zusammensetzung

Das Authentifizierungsverfahren ist mehrfach gesichert. Das Szenario beinhaltet folgende Schritte:

Teilnehmer:
Peer – Der Rechner des Benutzers
Authenticator – Network Access Server oder im einfachsten Fall ein AccessPoint
Authentication Server – Ein Server mit der Benutzerdatenbank, der die Logindaten verifiziert

1. Es wird ein TLS-Tunnel zwischen dem Client und dem Authentikator hergestellt. Durch die Verwendung von Zertifikaten kann sichergestellt werden, dass beide Tunnelendpunkte vertrauenswürdig sind.

2. Innerhalb des Tunnels werden Benutzer-Logindaten übertragen, die durch ein beliebiges EAP oder proprietäres Verfahren verifiziert werden.

3. Es werden Schlüsselpaare für beide Teilnehmer erzeugt, von denen Sitzungsschlüssel für weitere Verwendung mittles TLS-PRF abgeeitet werden.

4. Das Roaming kann auf drei Wegen erfolgen: durch erneue Authentifizierung, durch Wiederaufnahme der Sitzung oder durch einen Kontexttransfer zwischen den NAS/Aps

Zur Zeit ungeklärt ist das Roaming zwischen verschiedenen Netzen/Anbietern und das Verhalten bei Störungen durch gefälschte EAP-Pakete.

Beide Verfahren , d.h. PEAP und TTLS, nutzen die gleiche Technologie, setzten sie aber anders um. Die Inkompatibilität rührt daher, dass der Nachrichtenaustausch durch unterschiedliche Hersteller definiert wurde. Letztendlich wird sich wohl nur ein Verfahren durchsetzen, das die höhere Akzeptanz seitens der Nutzer findet.[10]

[10] Weitere Quellen zum Thema PPP und EAP
http://www.ietf.org/proceedings/02mar/206.htm
http://www.ietf.org/proceedings/02mar/slides/eap-5/sld001.htm
http://www.ietf.org/rfc/rfc2759.txt?number=2759
ftp://ftp.nordu.net/internet-drafts/draft-ietf-pppext-eap-ttls-02.txt

6.4.5. WPA

WPA ist ein Vorschlag der Wi-Fi-Alliance, mit Hilfe vorhandener Standards die Sicherheit im WLAN weiter zu verbessern. Dieser Vorschlag wurde unterbreitet angesichts der Schwächen im WEP und auf Druck der Industrie, um die Zwischenzeit bis zur Ratifizierung des entgültigen Standards 802.11i zu überbrücken. So ist WPA „zukunftskompatibel“.

WPA stellt eine Untermenge an Sicherheitsaspekten des zukünftigen 802.11i - Standards dar und erweitert das WEP.
WPA = 802.1X + EAP + TKIP + MIC [WiFi4]

	WEP	WPA	802.11i /WPA2
Verschlüsselung	RSA/RC-4	RSA/RC-4	AES
Schlüssellänge	40 bit und mehr	128Bit (64bit für Authentifizierung)	128 bit
Länge des IV	24 bit	48 bit	48 bit
Schlüssel-IV-Verh.	Zufammenfügen	Alternierende Funktion	Nicht benötigt
Datenintegrität	CRC32	MIC	CCM
Header-Integrität	Keine	MIC	CCM
Reply-Angriff	Keine	IV-Sequenz	IV-Sequenz
Schlüssel-Management	Keins	EAP	EAP
Verfügbarkeit	Jetzt	Wird etabliert	Ende 2004

Die wesentlichen Verbesserungen bzgl. der Sicherheit im Vergleich zu WEP sind durch die Einführung des „Port Based Access Control“ nach 802.1x und der EAP-Methoden erzielt worden. Die Schwäche in der Implementierung der Verschlüsselung soll durch einen Ausbau des „Initialization Vector“ (IV) in Verbindung mit einer Mix-Funktion erzielt werden. Die dynamische Schlüsselerzeugung und Distribution wird unter dem Begriff TKIP (Temporal Key Integrity Protocol) zusammengefasst. Hierbei sind zwei Szenarien vorgesehen. Eine

vereinfachte Variante ohne einen Authentifizierungsserver für den Heimbereich (WPA-PSK, Pre-Shared-Keys) und eine Enterprise-Version für Unternehmen mit einem AAA-Server, vorzugsweise Radius. Der PSA-Modus reduziert die WEP-Schlüsselverwaltung auf die Eingabe eines gewöhnlichen Passwortes. Das Passwort ist dann auch für alle Teilnehmer gleich, was potenziell ein Sicherheitsrisiko darstellt, jedoch ist dies ein Kompromiss zwischen Sicherheit und einfacher Handhabung, der im Heimbereich als akzeptabel erscheint (bei WEP gibt es weder eine einheitliche Methode die Schlüssel einzugeben, noch eine gemeinsames Format für die Schlüssel).
Eine Erweiterung um MIC (Message Integrity Check, Michael) stellt mittels einer Mathematischen Funktion sicher, dass gefälschte Pakete durch beide Wireless-Teilnehmer abgelehnt werden.

Das WPA-Update soll als Software-Aktualisierung für Betriebssysteme sowie als Firmware auf vorhandene Hardwarekomponenten aufgespielt werden können, was den Übergang erleichtern dürfte. Die Verschlüsselung mittels AES erfordert aber eine enge Bindung an die Hardware und soll dermaßen viele Ressourcen beanspruchen, dass dessen Implementierung einen Coprozessor benötigen wird, weshalb AES kein Bestandteil des WPA ist.
WPA beinhaltet nicht die z.Zt. in 802.11i spezifizieten Merkmale:

- Sicherer Ad-Hoc-Modus (IBSS)
- Roaming
- Deauthentifizierung und Disassoziation
- AES

WPA beinhaltet die zwei genannten Modi, die jedoch mit dem ursprünglichen WEP nicht kompatibel sind. Aus dem Grunde kann es anfänglich zu Integrationsschwierigkeiten kommen, da erst auf WPA umgeschaltet werden kann, wenn alle Geräte dies unterstützen. Die Hersteller versuchen durch ihre derzeitige Haltung, zunächst die nächste Generation des Equipments mit höheren Datenraten nach 802.11g und 802.11a zu etablieren und das Problem der Aktualisierung der Firmware und Treiber dadurch zu umgehen.
Weiterhin ist keine sichere Kommunikation im Ad-Hoc (peer-2-peer Netzwerk, IBSS) definiert, wodurch außer dem gewohnten Szenario

auch manche AP-Bridges betroffen sind, die diesen Modus verwenden.
Die Erweiterung um das MIC bringt auch Probleme mit sich, wie das ja schon von IPSec bekannt ist. Eine Übertragung der Session-Daten zum nächsten AccessPoint während des Roamings wird erschwert, wenn nicht gar unmöglich.

6.4.6. WPA2 (802.11i)

Der IETF Standard soll 2004 ratifiziert werden.
Viele Bestandteile des zukünftigen Standards sind im Vorfeld durch die WECA in WPA integriert. Die offenen Punkte beziehen sich auf schwer zu lösende Probleme im Bereich des Roamings und in Bezug auf den Ad-Hoc-Modus (IBSS).
Die Problematik im Ad-Hoc-Modus rührt daher, dass die verschärfte Sicherheit zum großen Teil durch eine Verlagerung der Logik in das Backendsystem (z.B. Radius-Server) zu erfolgen hat, dieser Modus aber ohne solche Systeme auskommen muss und deshalb einer Vereinfachung bedarf, die jedoch wieder Lücken in das Konzept reißt.
Bzgl. des Roamings liegt eine Ursache für Kopfzerbrechen darin, eine aufgebaute Session zügig auf einen anderen Zugriffspunkt zu übertragen, da das Verfahren an sich stark in der Komplexität zugenommen hat.[11]

[11] Die Entwicklung des 802.11i Standards befindet zur Zeit der Veröffentlichung der Arbeit immer noch in Arbeit. Weiterführende Information kann bei IEEE eingeholt werden. Des Weiteren empfiehlt sich als Lektüre [METH]

6.5. Gegenüberstellung der Sicherungsmethoden

6.5.1. Allgemeine Netzwerksicherungsmethoden

Diese Methoden haben eine lange Tradition und wurden dafür entwickelt, im einfachsten Fall, zwei Rechner miteinander über einen virtuell direkten Weg zu verbinden. Die Authentifizierung der beiden Partner ist ein gemeinsames Merkmal aller Protokolle. Zusätzlich bieten die meisten auch noch einen Grad an Sicherheit an. Die Unterschiede rühren daher, dass in verschiedenen Einsatzszenarien spezielle Anforderungen an die Authentifizierungsart und geforderte Verschlüsselung gestellt werden.

Speziell für den HotSpot-Einsatz wird gefordert, dass die Authentifizierungsart möglichst an HotSpots unterschiedlicher Serviceprovider durchführbar ist. Somit werden Protokolle, die mit einem Shared Secret oder Zertifikaten arbeiten kaum durchsetztbar sein, u.z. deshalb, weil es für alle HotSpots eine gemeinsame CertificateAuthority geben müsste, die alle verwendeten Zertifikate signiert. Das ist nicht praktikabel. Shared Secret ist aus gleichen Gründen in dem Szenario gar nicht denkbar.
Abhilfe schaffen aber Protokolle, die eine Passwortauthentifizierung verwenden, also MSChap Version2 und OneTimePasswort-Systeme z.B. über SMS.

Ein weiteres Unterscheidungsmerkmal bildet die OSI-Layer-Positionsierung der Protokolle. So sind Protokolle wie SSH und SSL auf der Anwendungsebene angesiedelt. Sie können somit einzelne Anwendungen wie http-Browsen und Mail-Anwendungen absichern. Leider obliegt diese Aufgabe aber dem Nutzer, der ja nicht immer in der Lage ist, die Anwendungen entsprechend zu konfigurieren. Oft ist es gar unmöglich, da die clientseitige oder serverseitige Anwendung dies nicht beherrscht. Somit müssten mobile Nutzer ihr Equipment mit speziellen Softwareprodukten ausstatten, was den Nutzern nur selten plausibel gemacht werden kann.

Andere Protokolle arbeiten auf Layer3, so z.B. IPSec. Hier fallen die meisten Einschränkungen, die für die Anwendungsebene bekannt sind, weg. Es werden alle Protokolle oberhalb der Vermittlungsschicht und IP selbst geschützt. Andere werden dadurch nicht abgedeckt: Netware, IPX, etc.
IPSec bereitet z.Zt. noch Probleme mit NAT-Firewalls, die oft im Zusammenhang mit dynamischen IP-Adressen verwendet werden. Das NAT-Traversal, eine patentierte Lösung, löst jedoch das Problem. Die für HotSpot-Einsatz geeignete IPSec-Konfiguration ist der Transportmodus mit ESP. Authenticated Header kann mit einer NAT-Firewall nicht ohne Weiteres eingesetzt werden. Sinnvoll ist auch der Einsatz spezieller Client-Einwahl-Software, die mit Passworten arbeitet. Hinderlich sind hingegen Konfigurationen, die mit Zertifikaten arbeiten, da eine Zertifikate-Infrastruktur (PKI) HotSpot-Anbieter übergreifend aufgebaut werden müsste. Insbesondere die Erfordernis von Benutzerzertifikaten bereitet Probleme, da sich diese oft ändern können (CRL-Problematik und Probleme bei der Einrichtung wg. der Administratorrechte bei Windows). Zudem existieren Clientimplementierungen noch nicht für alle Betriebssysteme oder sie sind nur als kommerzielle Kauf-Software erhältlich, was eine Einheitlichkeit verhindert.
Auf Layer 2, dem Link-Layer, gibt es kaum Einschränkungen bzgl. der zu transportierenden Protokolle, was aber bei einem HotSpot-Einsatz nicht so sehr ins Gewicht fällt. Ein wichtiges Kriterium stellt aber die weite Verbreitung dieser Protokolle aufgrund der langen Bestandsdauer dar. So gibt es PPTP-Implementierungen für alle gängigen Betriebssysteme meist „von Haus aus“. Es muss praktisch nichts käuflich erworben werden und die Software ist auch bereits fertig installiert. L2TP in Verbindung mit IPSec erfordert aber noch einen unerheblichen Installationsaufwand, vergl. IPSec. Die Handhabung ist aber sehr simpel und die meisten Nutzer kennen es bereits, da es nach dem gleichen Prinzip wie eine DFÜ-Einwahl funktioniert. Im Punkto Sicherheit gilt eine einfache Einrichtung gegen zusätzliche Sicherheit und Mehraufwand bei der Einrichtung und Verwaltung abzuwägen.
Für einen unkomplizierten und dennoch recht sicheren Zugriff auf das Internet unabhängig vom Ort ist PPTP mit MS-Chap v2 und

MPPE-Verschlüsselung letztendlich die unserer Meinung nach einzige z.Zt. mögliche Methode.

Im Folgenden wird ein Versuch unternommen, die sehr verschiedenen Protokolle trotz der nicht direkten Vergleichbarkeit gegenüberzustellen, u.z. im Hinblick auf eine ansonsten ungesicherte WLAN-Verbindung im Falle eines Hotspots, also für unvorbereitete User in einer fremden Umgebung.

	PPTP	L2TP[12]	SSH	IPSec	SSL/TLS
Verschlüsselung	+-	++	++	++	++
Schlüssellänge	+-	++	++	++	++
Authentizität	+	+	+	++	+
Datenintegrität	+-	++	++	++	++
Header-Integrität	--	++	+	+	--
Schlüssel-Management	+[13]	+-	+-	+-	+
Administration	++	-	--	-	+-
Usability	++	+-	-	+-	+-

[12] Eine Gegenüberstellung der beiden von MS eingesetzten Verfahren findet sich bei [MS2]

[13] Beschränkt sich auf die Verwaltung der Passwörter, was im Vergleich zu einer PKI wenig aufwendig ist.

7. Implementierung eines kommerziellen WLAN-Systems

7.1. Anforderungen an das Gesamtsystem

Ein HotSpot besteht im Wesentlichen aus drei Teilnehmern bzw. Komponenten

- Client-PC
- AccessGateway (AG)
- AccessServer (AS)
- Service Provider[14]

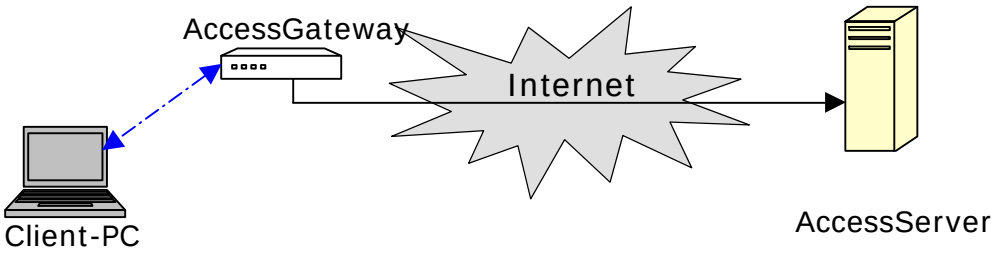


Abbildung 18 Komponenten des Hotspotsystems

Somit ist das im Verglich zu einer Stand-Alone Appliance, wie z.B. ein Home-WLAN-Router, ein erweitertes Szenario, in dem zusätzlich noch ein Zentral für viele Instanzen des AG agierenden Server vorkommt. Die Rolle des AG hat in unserem System die Box, und unser Hotspot-Server hat die Rolle des Access-Servers. Die Boxen versorgen die Nutzer des Systems mit Internet, ob per Kabel oder drahtlos, während der Hotspot-Server vor allem Verwaltungsaufgaben abwickelt.

[14] Der Service Provider, wie in 3.1.4 beschrieben, spielt bei der Implementierung des HotSpots nur marginal im Zusammenhang mit dem Thema Roaming eine Rolle, wie im Kapitel 7.3.5 beschrieben.

Im Vergleich dazu sind die anderen Szenarien, auf die in Kapitel 3.1 eingegangen wurde, im Prinzip mit einer Untermenge der für ein HotSpot benötigen Komponenten realisierbar, insofern ist das HotSpot-Szenario das komplexeste.
Wir haben uns deshalb für den HotSpot entschieden, da wir so Einblick in die meisten Komponenten an einem Beispiel bieten können.

Bei der Implementierung eines HotSpots spielen zwei Aspekte eine besonders wichtige Rolle: Praktikabilität und möglichst große Zielgruppe/Klientel.
Sicherheit ist unbedingt auch ein Thema, wie es bereits in der Vorstudie deutlich geworden ist, jedoch nützt einem ein absolut sicherer HotSpot nichts, wenn man es nicht schafft, sich dort einzuloggen. Es muss also ein Kompromiss gefunden werden, bei dem die Absicherung des WLANs mittels gängiger Verfahren statt findet.
Ein weiterer Aspekt ist die Durchmischung der User. An einem public-HotSpot soll möglichst jeder teilhaben können. Nicht jeder ist aber bereit, sich bei jedem in Frage kommenden HotSpot-Anbieter einen Zugang zu besorgen. Insofern müssen Möglichkeiten gefunden werden, entweder ein System zu schaffen, das alle potenziellen HotSpot-Anbieter bedient oder alternativ kann man ein Roaming-Verfahren entwickeln oder beides.

7.2. Das Access-Gateway, die Box

7.2.1. Anforderungen, was für Komponenten werden benötigt?

Das AccessGateway definiert sich durch folgende Funktionalitäten:

- Implementierung des Zugangs zum Internet mittels eines geeigneten Transfermediums
- Einsatz als AccessPoint
- Routen zwischen den beiden Übertragungsmedien
- Authentifizierung der Benutzer
- Sicherung der Funkstrecke
- Traffic Shaping
- Accounting
- Firewall-Funktionalität
- WEB-gestützte Konfiguration
- Live-Update
- Parameteraustausch mittels der Schnittstelle zum Access-Server

Beginnend mit Grundfunktionalitäten wie der Internetverbindung bauen andere Module darauf auf und stellen neue, komplexere Dienste zur Verfügung.

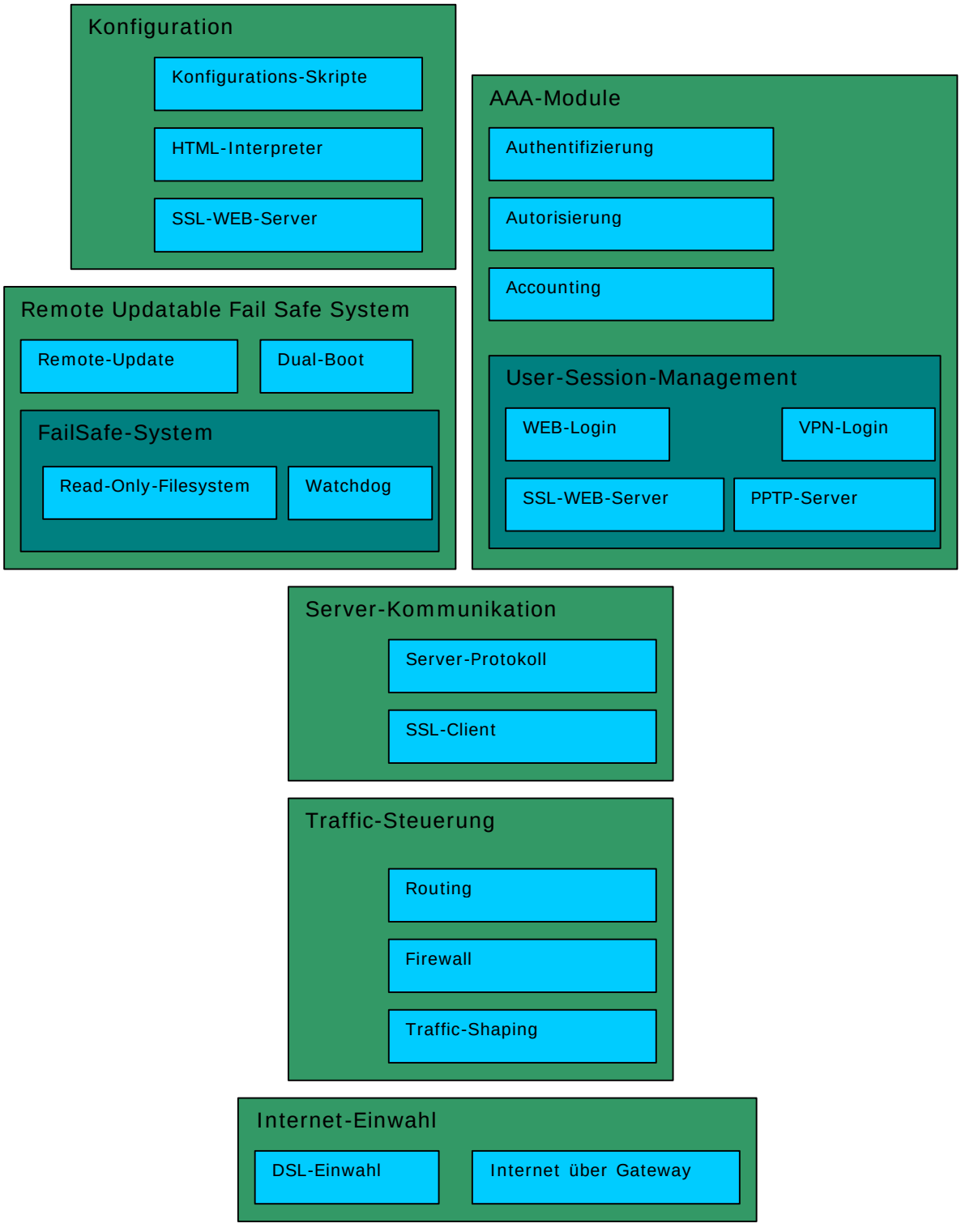


Abbildung 19 Module AccessGateway

Die im vorigen Kapitel genannten Anforderungen an das AG können zu Funktionsgruppen, wie in der Abbildung zu sehen, zusammengefasst werden. Das sind insbesondere:

- Internet Einwahl oder permanente Verbindung
- Traffic Steuerung
- Server Kommunikation
- Remote Updatable Fail Safe System
- AAA-Module
- Konfiguration

Die so bezeichneten Module arbeiten trotz der Trennung eng zusammen. Es wird ein Nachrichtenaustausch zwischen den Modulen stattfinden und ein entsprechendes Protokoll muss ggf. gefunden bzw. entwickelt werden, das allen Modulen gemeinsam ist.

Die Box erfüllt vor allem die Funktion eines Routers, der jedoch in der einen oder anderen Hinsicht angepasst wird. Zugrunde liegen also Standardfunktionen des Betriebssystems, wie das Routing und Firewalling. Es wird ein Weg gesucht, die benötigte Funktionalität vor allem mit vorhandenen Komponenten abzudecken. Das Bindeglied muss ggf. entwickelt werden, wenn es kein solches für diesen Anwendungsfall gibt. Weitere eigenentwickelte Module ergänzen das Basissystem zu einem Ganzen. Bei der Wahl des Grundgerüsts wird klar, dass viele der Anforderungen kosteneffektiv durch freie Software erfüllt werden können. So kann Linux als ernsthafte Konkurrenz zu kommerziellen Produkten auf dem Sektor der Server-Betriebssysteme angesehen werden. Zudem bietet OpenSource-Software die Möglichkeit zu individuellen Anpassungen, die in Verbindung mit der Vielfalt an frei vorhandenen Tools erst ein Gesamtsystem ermöglicht. Dabei möchte man im Prinzip „nur“ einen sicheren Internetzugang, jedoch wird das „nur“ hier und da schnell zu einem „etwas mehr“, denn ein sicherer WLAN-Zugang ist z.Zt. nichts, was man als ein fertiges Produkt, ob in Hardware oder als Softwarelösung „von der Stange“ kaufen kann. Es ist vielmehr eine Kombination aus vorhandenen Produkten bzw. Verfahren, die einen sicheren Zugang möglich macht.

7.2.2. Design, Softwarekomponenten im Überblick

7.2.2.1. Die Einwahl

Die Software soll vor allem dem Nutzer ermöglichen, sich am Hotspot ins Internet einzuwählen. Der Vorgang lässt sich mittels des folgenden Use-Case-Diagramms veranschaulichen.

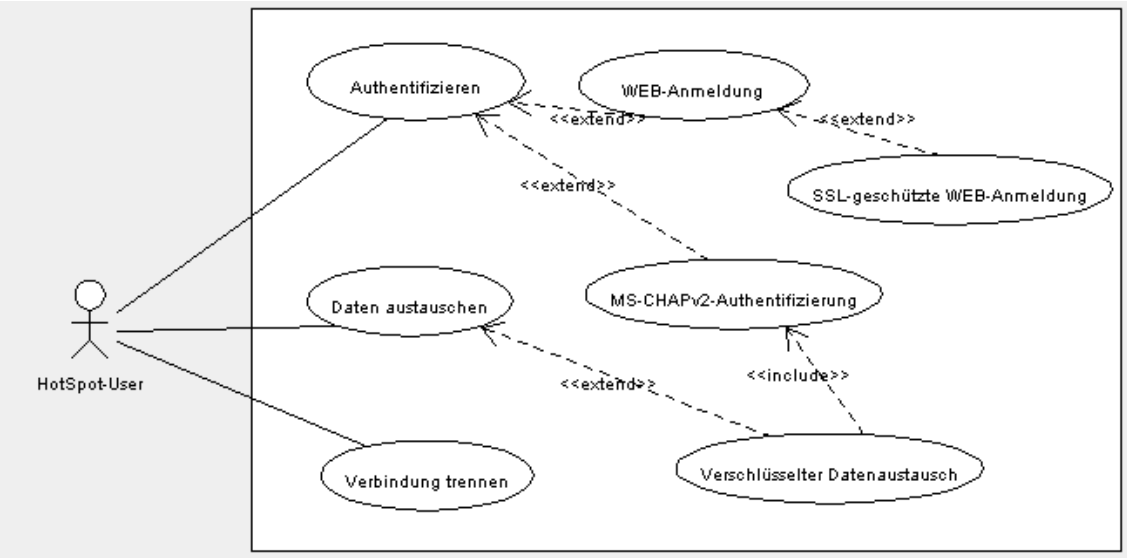


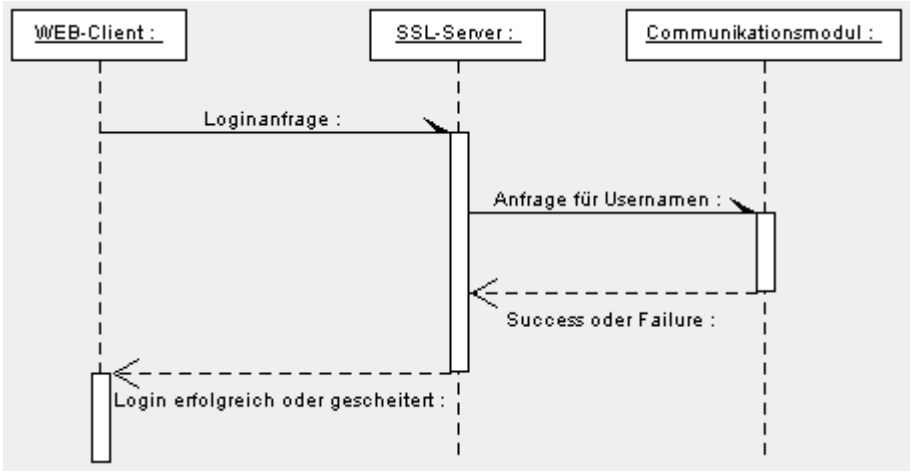
Abbildung 20 Use-Case-Diagramm AccessGateway

Die WEP-Verschlüsselung ist wegen der sicherheitstechnischen Bedenken und der Problematik des Managements, wie im Vorwege erläutert, nicht ohne weiteres für öffentliche HotSpots geeignet. Deshalb werden Alternativern angeboten: hier exemplarisch eine SSL/TSL-gesicherte Anmeldung oder eine VPN-Verbindung incl. Verschlüsselung.

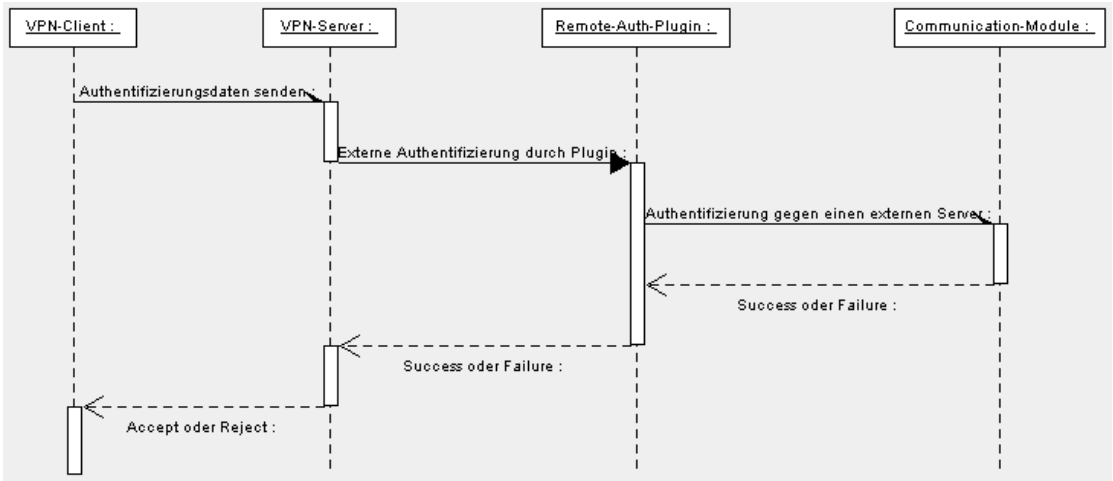
Die Authentifikation erfolgt für beide Verfahren gegen einen entfernten Server.
Dazu werden die Anfragen an ein Kommunikationsmodul delegiert. Die Antworten des AS werden an die Authentifizierungsmodule zugestellt.

So lässt sich das gleiche Verfahren sowohl auf die WEB-Login, wie auf die VPN-Anmeldung anwenden, obwohl die Module dann völlig anders funktionieren.
Der modulare Aufbau verhilft hier zum Wiederverwenden des Codes. Noch wichtiger ist aber, dass durch die gemeinsame Basis, das Server-Kommunikationsprotokol, u.a. viele Standard-Authentifizierungsverfahren angebunden werden können, je nach den Bedürfnissen.

WEB-Anmeldung



VPN-Anmeldung



Die Abbildungen verdeutlichen, dass die gemeinsame Schnittstelle sowohl von dem PPP-Server als auch von dem WEB-Server für die Remote-Authentifizierung benutzt wird.

7.2.2.2. Autorisierung

Das Thema Autorisierung ist nur von Bedeutung, wenn tatsächlich unterschiedliche Dienstqualitäten je nach Login unterschieden werden sollen. Für den gewöhnlichen Fall der Gewährung oder Verweigerung des Internetzugangs kann man hingegen noch nicht viel darüber sagen, außer dass authentifizierte Benutzer im Gegensatz zu Nicht-Teilnehmern einen Zugang erlangen.
Im Fall des AG kann man von Autorisierung sprechen, da jedem Login auch individuelle Qualität anhaftet:

- Ortsgebundenheit oder Unabhängigkeit
- Download-Bandbreite
- Upload-Bandbreite
- Priorität gegenüber anderen Nutzergruppen

Die Dienstmerkmale hängen vom Nutzerprofil ab, je nach dem für welches WLAN-Produkt-Paket er sich entscheidet, kann der User mehr oder weniger Dienstleistung in Anspruch nehmen. In dem verteilten System aus AG, AS und dem User kommt dem AG die Rolle des Türstehers zu, während alle benutzerspezifischen Informationen, das User Profile, serverseitig zu speichern sind. Die Autorisierung erfolgt parametrisiert durch den AS. Hierzu dienen diverse AG-AS-Protokol-Parameter.

7.2.2.3. Accounting

Von essentieller Bedeutung für ein kommerzielles System ist die zuverlässige Abrechenbarkeit der Benutzer gegenüber dem Dienstanbieter. Dazu werden Nutzungsdaten erhoben, zentral gespeichert und zur Rechnungstellung herangezogen. Dem AG kommt hierbei die Rolle des Sammlers zu.
Beginnend mit dem Login werden die Nutzungsdaten bestehend aus den Transfermengen für Downloads und Uploads, sowie die Nutzungsdauer pro Sitzung einzeln erfasst.
Die Erfassung endet mit einem expliziten Logout, d.h. durch einen der drei Auslöser:

- User-Logout
- Session-Timeout
- Kontroliertes Logout beim Aufbrauchen des Guthabens

Der Logout durch ein Session-Timeout soll nach einer bestimmten Zeitdauer erfolgen, wenn innerhalb dieser keine Daten mehr vom Benutzer übertragen wurden.
Es wird also das Ende der letzten Übertragung zeitlich erfasst. Weitere Netzwerkaktivität setzt den Zähler zurück; keine Aktivität über eine bestimmte Dauer führt zum Session-Timeout.
Diese Zeit fließt nicht in die Sitzungsdauer ein.
Es kommt aber auch vor, dass während einer Sitzung z.B. das Guthaben verbraucht wird, woraufhin die Verbindung unterbrochen werden muss. Diese Information wird vom AS bereitgestellt und während der Sitzung durch den AG mit dem aktuellen Verbrauch verglichen. Dadurch wird es möglich auch Mehrfachlogins sicher zu terminieren.
Die gesammelten Daten werden zusammengefasst und periodisch an den AS geschickt, auf jeden Fall aber auch am Ende einer Sitzung. Das ist insbesondere für eine Nutzung in Verbindung mit einem WEB-Login wichtig, da hier nur so das Sitzungsende zuverlässig erkannt werden kann, falls sich ein Benutzer nicht abmeldet. Auch kommuniziert der Server die verbleibende Zeit oder Datenmenge in den Antwortpaketen auf Verbrauchsmeldungen, woraufhin die Sitzung beendet werden kann.

Diese Daten werden nicht weiter ausgewertet, sondern gelangen zum AS, wo sie analysiert und entsprechend dem Nutzerprofil bewertet werden.

7.2.2.4. Internet Einwahl oder permanente Verbindung

Die eigentliche Ware, der Internetzugang, wird bezogen über xDSL oder alternativ über ein LAN. Diese Einstellung wird am AG vorgenommen, da es zum Installationszeitpunkt noch keine Verbindung zum AS gibt. Denkbar ist aber auch nach dem try&error-Verfahren zunächst die LAN-Verbindung zu testen. Wenn nämlich ein DHCP-Server im Netzwerk existiert, der die Parameter IP-Adresse, Standard-Gateway und Nameserver den Clients mitteilt, kann man auch von einer Plug&Play-Installation des AG sprechen. Anderenfalls sind diese Parameter einzustellen oder die DSL-Einwahl zu konfigurieren.
Die DSL-Einwahl wird dem Einrichter gegenüber auf wenige einzustellende Parameter reduziert: Login-Name und Passwort. Die restlichen entsprechen einer permanenten Verbindung mit Wiedereinwahl beim ISP-seitigen Trennen der Verbindung. Für den einfachen Fall, dass nur ein DSL-Modem am Ethernet-Segment angeschlossen ist, kann man von dieser Annahme ausgehen.
In Hinsicht auf die Systemarchitektur besteht der Unterschied zwischen den beiden Anbindungsarten darin, dass die Einwahl ein Punkt-zu-Punkt-Überbau auf der Ethernet-Verbindung ist [PPPoe], während bei der Variante über ein LAN-Gateway IP direkt auf Ethernet aufbaut.

7.2.2.5. Traffic Steuerung

Die Traffic-Steuerung ist das Herz des AG. Hier kommen so essentielle Aspekte zum Tragen wie das Routing, die Firewall und nicht zuletzt das Traffic Shaping. Der Datenverkehr von den Clients, der über VPN und über WLAN-Basisverbindung eingeht wird gefiltert, rationiert und je nach Internetanbindung über das eine oder andere Gerät ausgegeben.

Die Firewall setzt Network-Address-Translation [NAT] ein, damit sich Verbindungen über das Internet auch mit nur einer öffentlichen IP-Adresse von mehreren Clients herstellen lassen, ohne dass jeder dieser Clients eine öffentliche IP-Adresse bekommen muss. Das Szenario ist sowohl für den Einsatz im LAN als auch mit xDSL praktikabel und ermöglicht eine dynamische Zuordnung der Adressen zu den Clients, ohne feste? Adressen vorhalten zu müssen. Das spart letzten Endes kostbare Ressourcen. Zudem enthält die Firewall Regeln, die typische Angriffe verhindern. Sie regelt den Zugriff für authentifizierte Benutzer auf das Internet und ermöglicht es andererseits nicht eingeloggten Usern, beim Ansurfen einer beliebigen Internet-Seite auf die Loginseite zu gelangen, ohne sie zu kennen.
Die Firewall spielt auch beim Thema Accounting eine gewichtige Rolle, denn alle IP-Pakete die sie passieren, werden gezählt und einer User-Session zugeordnet.
Sie regelt also den Zugriff und die Nutzung des Netzwerks für User die das WEB-Login nutzen.

Je nach Autorisierung können unterschiedliche Bandbreiten bzw. Prioritäten für Client-Verbindungen festgelegt werden. Die Umsetzung dieser Aufgabe obliegt dem Traffic-Shaper.
Ziel sollte sein, zwei unterschiedliche Kombinationen aus Download- und Upload-Bandbreiten sowie eine Priorisierung der Pakete je nach Type-Of-Service-Wert zu erreichen.

7.2.2.6. Server Kommunikation

Zu einem verteilten HotSpot-System gehört neben dem AG auch der AS. Die gemeinsame Sprache ist das Kommunikationsprotokoll, welches das Bindeglied darstellt.
Die Einzelheiten zum Protokoll werden im Kapitel 7.3. erläutert.
Die Server-Kommunikation wird von anderen Modulen in Anspruch genommen, die alle eine einheitliche Schnittstelle zum Nutzen dieses Dienstes erhalten sollen. Da die Kommunikation immer durch

das AG angestoßen wird[15], kann sie durch ein Request-Response abgebildet werden.

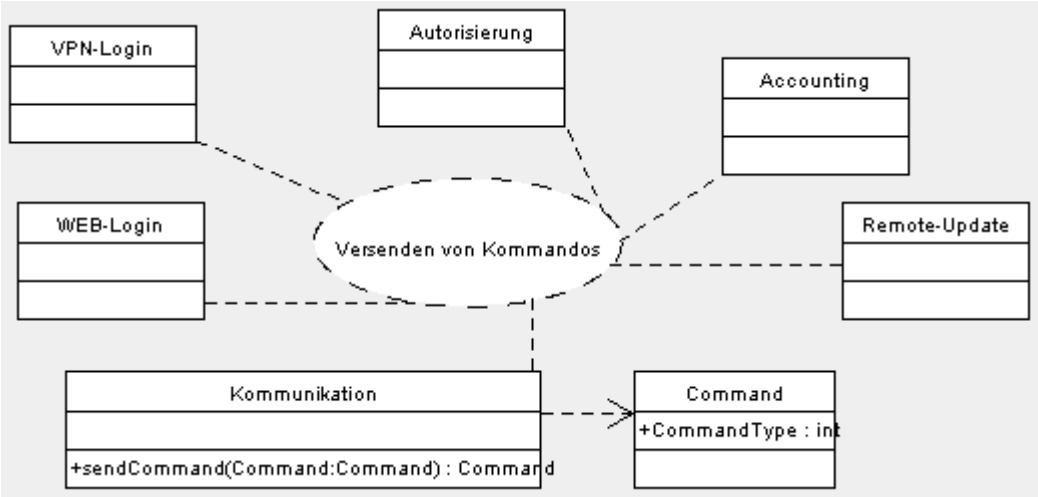


Abbildung 21 Klassendiagramm Kommunikation AccessGateway

Die Kommunikationsklasse übersetzt die eingehenden Kommandos in die Kodierung des Kommunikationsprotokolls und dekodiert die Antwort-Nachrichten des AS zu Kommandos, die von den Modulen verstanden werden. Die Servernachrichten sind http-Konform als Parameter im „search“-Teil des Requests und im Response-Body eingebettet. Die internen Datenstrukturen jedoch entsprechen der Implementierung und können Klassen oder Strukturen sein.

[15] Aufgrund der DSL-Einwahl eines AccessGateways wird dessen IP dynamisch zugeordnet und ist dem Server somit nicht bekannt

7.2.2.7. Konfiguration

Bevor das AG in Betrieb gehen kann, müssen noch einige Einstellungen vorgenommen werden. So soll mindestens die Art und die Parameter der Internet-Anbindung von Fall zu Fall anders eingestellt werden können. Als angemessene Benutzerschnittstelle erscheint vor allem eine WEB-Browser gestützte Konfiguration, die sich durch ein genormtes Design und Übersichtlichkeit auszeichnet. Dadurch werden unnötige Hürden genommen und der Benutzer findet sich schnell zurecht durch den Wiedererkennungseffekt. So hat dieses Verfahren die Vorteile auf seiner Seite im Vergleich z.B. zu einem Telnet- oder einem anderen Shell-Zugang. Durch eine SSL/TLS-Verschlüsselung des Kanals, kann die Administration auch ohne WEP oder VPN sicher über WLAN durchgeführt werden.
Der Zugang zur Administrationsoberfläche muss aber gesondert geschützt werden, damit es nur autorisierten Usern erlaubt bleibt, ein AG zu administrieren. Der Zugangsschutz kann mittels Zertifikate erfolgen.
Für die Konfiguration wird ein WEB-Server benötigt, der zusätzlich dynamische Seiten und SSL unterstützt.
In der Konfiguration soll vorgesehen sein, zunächst zwischen einer xDSL-Einwahl und einem Zugang über einen Gateway-Rechner zu wählen. Die Parameter haben eine Schnittmenge sind jedoch teilweise verschieden. Der DSL-Zugang erfordert einen Login, sowie teilweise DNS-Informationen, während der Zugang über ein Gateway dessen IP-Adresse, anstelle des Logins erfordert. Die DNS-Einstellungen werden günstigstenfalls durch das Gateway bzw. den ISP übermittelt und sind somit optional.

7.2.2.8. Remote Updatable Fail Safe System

Diese Bezeichnung steht für den Anspruch, servicearm zu sein und dadurch langfristig günstig im Betrieb, was insbesondere für ein kommerzielles System unerlässlich ist.
Man stelle sich vor, die AccessGateways werden an unzugänglichen Orten, weit vom nächsten Serviceort installiert. Ein Softwareupdate wird früher oder später fällig und u.U. eben auch sehr kostspielig, wenn viele dieser Geräte aktualisiert werden sollten. Ein Remote-Update löst diese Problematik. Es ermöglicht, von einem Server aus, mehrere AG mit einer neuen Softwarerevision zu versorgen, wie man es z.B. von Virenscannern gewohnt ist, die ihre Virusdefinitionsdateien ständig aus dem Internet aktualisieren.
Um dieses Feature sinnvoll einsetzen zu können, ist es wichtig, Problemfälle im Vororteinsatz zu erkennen und diagnostizieren zu können (natürlich geschehen die größten Katastrophen nicht im Testbetrieb, sondern im live-Einsatz). Dazu empfiehlt es sich ein Logging-System zu betreiben, das flexibel genug ist, gezielt auf Abruf Statusinformationen von ausgewählten AG einholen zu können. Wird ein Problem erst ein mal erkannt, kann so das Fehlverhalten mittels gezielter Statusabfrage oder Einsicht in Laufzeitkonfiguration bzw. Logfiles eingegrenzt werden. Daraufhin kann ein Update erarbeitet werden und an alle betroffenen AG über das Distributionssystem zugestellt werden.
Es darf aber nicht vergessen werden, dass viele Fehler im Allgemeinen erst durch die s.g. Bugfixes erzeugt werden. Um auch diesem Problem zu begegnen, kann man ein Zweitsystem, ein FailOver- /Backup-System, neben dem Live-System auf jedem AG einrichten. Das Backup-System kommt zum Einsatz, wenn das Live-System nicht alle Parameter erfüllt, die ein funktionierendes System kennzeichnen. Ein funktionierendes System definiert sich vor allem durch laufende Module, die wiederum einzeln für deren Funktionsprüfung verantwortlich sind und sich im Fehlerfall einfach beenden oder stehen bleiben. Die Ausnahme bildet natürlich der Betriebssystemkern, der sich einer solcher Prüfung entzieht. Einzig durch einen Hardware Watchdog, der noch vor dem Boot-Vorgang aktiviert wird kann man solchen Problemen begegnen. Der

Watchdog aktiviert das Backupsystem. In diesem Zustand können nur rudimentäre Funktionen wahrgenommen werden. Das AG signalisiert den Fehlerzustand an den Server und versetzt sich in einen Wartezustand, bis der Fehler durch einen Servicetechniker über ein neues Update behoben wird. Es können also nur neue Updates akzeptiert werden.
Fehlerzustände sollten außer am Server auch an dem AG durch entsprechende Kodierung der Leuchtsignale an einer Error-LED angezeigt werden.

7.2.3. Implementierung des Access Gateways

Bei der Implementierung spielt die Wiederverwendung von vorhandenen Ressourcen und die Einhaltung von Standards eine zentrale Rolle.
Natürlich muss eine Entwicklung auch der Wirtschaftlichkeit Rechnung tragen.
Diese Vorgaben werden ausgezeichnet durch freie Software erfüllt. Insbesondere eignet sich das Linux-Betriebssystem für unsere Zwecke:

- Frei erhältlich
- Source-Pakete vorhanden
- Hervorragende Netzwerk-Unterstützung
- Anpassbar in jeder Hinsicht

Als eines der am meisten verbreiteten freien Betriebssysteme bietet es eine nahezu unüberschaubare Vielfalt an Anwendungsprogrammen und Serverdiensten, aus denen sorgfältig eine harmonierende Auswahl zu treffen ist, die auf die hier formulierten Anforderungen passt.

7.2.3.1. DSL-Einwahl

Der typische DSL-Zugang erfolgt über ein ADSL-Modem. Das Modem ist über Ethernet angeschlossen und kommuniziert mit dem angeschlossenen Rechner über ein Protokoll namens PPPoE, das einer seriellen Übertragung ähnelt. Die bekannteste Client-Software kommt von der Software-Schmiede Roaring Penguin und ist sowohl in einer Kernelversion als auch als UserLand-Programm verfügbar. Letzteres ist eine Erweiterung des PPPD-Dienstes, der ebenfalls für VPN-Tunnel eingesetzt wird.
Die Verbindungsparameter sind für eine permanente Verbindung eingestellt. Bei häufigen Fehlern auf der Ethernet-Strecke oder falls der ISP die Verbindung trennt, beendet sich der Dienst implementierungstechnisch bedingt. Deshalb sorgt ein kleines Skript für die automatische Wiedereinwahl und die Anzeige des Zustands der Verbindung über eine LED.

7.2.3.2. Routing, Firewall und Traffic Shaping

Das Routing erfolgt bei Linux im Kernel. Für die bescheidenen Bedürfnisse unseren AG's sind wenige statische Routen vollkommen ausreichend.[16]
Interessanter ist die feine Steuerung des Datenverkehrs durch die Firewall, die das gewohnte Routing beeinflusst. Das Standardwerkzeug für diesen Zweck ist das IPTABLES-Paket [Netfilter]. Es besteht aus einer Kernel-Erweiterung, die in das Routing eingreift und Steuer- und Dienstprogrammen für die Benutzer.
Es existiert eine hervorragende Anleitung zu diesem Thema[17].
Hier sei nur auf die wesentlichen Aspekte eines Firewall-Systems eingegangen.
IPTables/ Netfilter stellt mit das flexibelste und gut durchdachteste Werkzeug dar, um den Paketfluss effizient zu steuern. Es ermöglicht uns den Eingriff in das Routing an entscheidenden Stellen.
Durch entsprechende Regeln wird sichergestellt, dass:

- Viele Clients sich eine öffentliche IP-Adesse teilen
- Und der direkte Zugriff aus dem Internet auf die Clients nicht möglich ist
- Nur autorisierte Nutzer über WLAN Zugriff auf das Internet haben
- Alle VPN-Nutzer ebenfalls auf das Internet zugreifen können
- Gängige Angriffe aus dem Internet abgewährt werden
- Alle nicht eingeloggten Surfer auf die Web-Login-Seite gelangen
- Die geflossenen Datenmengen für jeden User einzeln erfasst werden
- Die IP-Pakete entsprechend dem User-Profile für den Traffic-Shaper klassifizieren

[16] Einen tiefen Einblick in das Routing gibt Anderw S. Tanenbaum
[17] Anleitungen zum Thema Netfilter: http://people.netfilter.org/~rusty/unreliable-guides/

In Zusammenarbeit mit dem Authentifizierungsmodul werden nach einem erfolgreichen Login neue Regeln in der Firewall angelegt, die den Internetzugang auf IP-Ebene gestatten. In diesem Fall greift das Routing, und die Pakete können passieren. Pakete von nicht autorisierten IP-Quelladressen werden hingegen auf die lokale Adresse des AG verändert, wodurch alle Anfragen von dem AG selbst beantwortet werden. Dieses Verhalten verhilft uns zu einer drastischen Vereinfachung bei der Herstellung der Verbindung: Sowohl bei dem Web-Login als auch bei dem VPN-Login mit PPTP oder L2TP muss man eine IP-Adresse des Servers oder seinen Namen eingeben. Durch den o.g. Trick kann man bei Unsicherheit eine beliebige Adresse angeben, das Ziel ist immer das AG, solange man nicht angemeldet ist.

Die Vorgaben aus dem User-Profile bzgl. der Bandbreiten und Prioritäten lassen sich wohl am besten mit klassenbasierten Bandbreitenmanagement-Tools wie iproute2 und entsprechenden Queuing Disciplines regeln.[18] Die von der Firewall markierten Pakete werden einer Queue zugeordnet und entsprechend der dort definierten Disziplin getrimmt.
Die Vorgehensweise bei Anlegen einer Queue entspricht der von Firewall-Regeln: sobald ein Client erfolgreich eingeloggt hat, werden CBQ-Klassen an passender Stelle im Baum angehängt, beim Logout können Sie wieder entfernt werden.

[18] Eine wohldokumentierte Anleitung und Hintergründe findet man im Linux Documentation Project: http://www.tldp.org/HOWTO/ADSL-Bandwidth-Management-HOWTO/implementation.html

7.2.3.3. WLAN

Was normalerweise in der Firmware der AccessPoints stattfindet, lässt sich unter bestimmten Voraussetzungen auch in Software realisieren. Das prominenteste Projekt ist meines Wissens HostAP[19]. Diese Software macht sich den Umstand zu Nutze, dass sich WLAN-Hardware, die auf dem Prism-Chipsatz[20] basiert, in einen Modus versetzen lässt, in dem für den AccessPoint wichtige Funktionen in der Software anstatt in der Firmware abgewickelt werden. Dies erlaubt höchste Flexibilität in Bezug darauf, welche Funktionalität in der Hardware und welche auf dem Hostrechner ausgeführt wird. So ist der Funktionsumfang ständig gewachsen und hat einen ansehnlichen Umfang erreicht:

- Betrieb in BSS und IBSS-Modus
- Betrieb als Station und AccessPoint
- WDS-Modus (Wireless Distribution System)
- Authentifizierung/Deauthentifizierung
- Assoziation/Reassoziation/Disassoziation
- Energiesparfunktionen
- IEEE 802.1X
- Dynamische WEP-Schlüssel
- Radius-Support
- MAC-Adressen basierte Zugriffsteuerung (ACL)

Darüber hinaus bietet der Treiber in Verbindung mit den Wireless Tools eine gute Plattform zur Evaluierung des 802.11 Standards und der Möglichkeiten der Hardware. Mit Hilfe der zahlreichen Managementtools lassen sich verschiedene Konfigurationen der Hardware und des Treibers leicht finden. Die Kombination aus dem HostAP-Treiber und den universellen Wireless Extensions und Wireless Tools schafft eine solide und zukunftssichere Basis für Entwicklungen auf diesem Gebiet.

---

[19] Nähere Informationen sind auf der Hopage des Authors: Jouni Malinen erhältlich: http://hostap.epitest.fi/

[20] Copyright/TM: Intersil

Folgende Konfiguration erfüllt die Anforderungen an ein WLAN-HotSpot:

- Betrieb im Master-BSS-Modus
- WEP-Verschlüsselung aus
- ACL aus (open policy)
- Bridging zwischen Wireless Clients aus

Durch diese Konfiguration ist der HotSpot durch einen Scan nach verfügbaren drahtlosen Netzen auffindbar und jeder kann sich mit ihm assoziieren. Die Zugriffssteuerung erfolgt nicht durch WLAN-Authentifizierung, da einerseits hierfür noch keine einheitliche Methode vorhanden ist[21], andererseits die WEP-Authentifizierung für öffentliche Zugänge ihren Zweck nicht erfüllt und auch den Zugang erschwert[22]. Deswegen wird der Zugriff durch das WEB-Login über SSL und VPN gesteuert.

7.2.3.4. VPN

Wie aus dem Kapitel 6 hervorgeht, halten wir zwei VPN-Arten für geeignet, an öffentlichen Zugangsstellen die WLAN-Verbindung abzusichern: PPTP und L2TP.
PPTP wird z.Zt. noch von uns favorisiert, da es für die Nutzer einfacher in der Einrichtung und unter den Betriebssystemen weiter verbreitet ist. Dafür existieren erwiesenermaßen einige Lücken im Konzept[23], die jedoch zumindest teilweise durch eine geeignete serverseitige Konfiguration ausgeglichen werden können.

Die bekannteste Linux-Implementierung des PPTP-Protokolls heißt PoPToP.

---

[21] WEP-Authentifizierung und WPA/ TKIP können implementierungsbedingt nicht zusammen betrieben werden.
[22] Vergleiche Kapitel 6
[23] vergl. Kapitel 6.x.x.x

Es handelt sich hierbei um einen Serverdienst, der das Kontrollprotokoll implementiert. Das eigentliche Arbeitspferd ist aber PPPD und die Kernelkomponenten, die den Rest der Arbeit erledigen, angefangen bei der Aushandlung der Verbindungsparameter bis hin zur Verschlüsselung. Entsprechend fällt auch der Aufwand bei der Installation und Einrichtung der Quellpakete aus. Zumindest bei PPP ist man auf die neuesten Quellen aus dem CVS in der Version 2.4.3 angewiesen. Für eine sauber funktionierende Verschlüsselung nach dem MPPE-Verfahren wird noch ein zusätzlicher Kernel-Patch benötigt[24], da die CVS-Version offensichtlich bei eingeschalteter Verschlüsselung die MTU-Werte nicht korrekt berechnet, was sich darin äußert, dass große Pakete nicht ankommen und die Verbindung hängt.
Der Patch löst das Problem und erlaubt zudem auch den Einsatz der MPPC-Komprimierung, die jedoch patentiert ist[25], und in dem AG nicht eingesetzt wird.
Die Konfiguration für PPPD sollte mindestens diese Optionen beinhalten:

- Stateless Encryption
- RC4 128bit
- MS-Chap v2 – Authentifizierung

Durch das Schlüsselwort require wird sichergestellt, dass der Server die Verbindung trennt, falls der Client eine dieser Optionen verweigert. Typischerweise sind Clients aber eher liberal konfiguriert, so dass eine schärfere Richtlinie auf jeden Fall schon durch die Standardkonfiguration abgedeckt ist. Kommt eine Verbindung trotzdem nicht zustande, ist das meist ein Hinweis auf eine clientseitige Misskonfiguration.

Mit dieser Konstellation aus Kernel-Treibern und Dienstprogrammen kann man einen PPTP-Server zum Laufen bringen. Jedoch fehlt noch die Anbindung an das Authentifizierungs- und Accounting-Modul.

---

[24] PolBox-Link: http://www.polbox.com/h/hs001/

[25] Patent liegt bei HiFn

Dank des modularen Aufbaus des PPPD-Dienstes ist es möglich ein Plugin zu konstruieren, das die Authentifizierung, abweichend von dem gewohnten Weg über eine Passwortdatei auf dem Datenträger, über eine Serverabfrage realisiert. Hier macht man sich CallBack-Funktionen (Hook) und Notifier-Funktionen zu Nutze, um das gewohnte Verhalten bei der Abfrage der Passwörter zu verändern und außerdem auf unterschiedliche Ereignisse, wie z.B. Link-UP, IP-UP, Link-Down etc. zu reagieren. So wird z.B. bei einer Login-Anforderung der Einsprungspunkt chap-check-hook aufgerufen. Die übergebenen Parameter werden in Form eines LOGIN-REQUEST-Kommandos an das Kommunikationsmodul übergeben. Die Antwort des AS entscheidet letzten Endes über den Rückgabewert des Hooks und über den Erfolg der Login-Anfrage.
Eine Goldgrube an Accountinginformation erschließt sich durch die pppd.h Headerdatei, durch die das Plugin Zugriff auf globale Variablen des PPP-Dienstes erhält.
So lassen sich nicht nur relevante Daten zu den übertragenen Datenmengen abrufen, sondern auch effizient begrenzen. PPP kann so auf das Guthaben eines Kunden eingestellt werden wie eine Eieruhr – eine sehr elegante Möglichkeit.

7.2.3.5. Dual-Boot

Das Dual-Boot-System macht sich die Kenntnis der Soft und Hardware zu Nutze.
Um ein solches System zu implementieren, braucht man zunächst genaue Information über das Laufzeitverhalten des Gesamtsystems, insbesondere über die Anzahl und den Zustand der Prozesse. Diese Information fließt in ein Überwachungsprogramm ein, das im Fehlerfall das Backup-System startet[26]. Sinnvollerweise erfolgt das über einen Hardware-Watchdog, der wiederum die Funktionsfähigkeit des Überwachungsprogramms verifiziert.

[26] Das Backupsystem ist eine unveränderliche Installation, die allein den Zweck erfüllt, ein Live-System mit Updates vom AS zu versorgen.

Über ein Flag, das in einem nicht flüchtigen, zur Bootzeit lesbaren Speicher abgelegt ist[27], lässt sich die Entscheidung treffen, welche der beiden Installationen zu booten ist.
Vor dem Boot-Vorgang wird das Flag grundsätzlich auf „dirty“ gesetzt und nur nach einem komplett erfolgreichen Boot des Live-Systems wieder auf „clean“ zurückgesetzt.
Eine solche Unterscheidung bietet leider kein uns bekannter Boot-Loader, weshalb eine Anpassung am LILO-BootLoader vorgenommen werden musste.

[27] Es bietet sich z.B. eine ungenutzte Stelle im CMOS-Speicher an

7.2.3.6. HTTP-Server und Client mit SSL und dynamischen Inhalten

Für die Implementierung eines WEB-Logins und der WEB-gestützten Konfigurationsoberfläche wird jeweils ein WEB-Server benötigt.
Zudem empfiehlt es sich angesichts der Tatsache, dass es sich hierbei um ein minimalistisches System handelt, einen schlanken WEB-Server einzusetzen.
Die Erfahrung im Studium zeigte, dass sich solch ein WEB-Server mit relativ wenig Aufwand erstellen lässt. Die Vorkenntnisse ergänzen wir hier durch den Einsatz der openSSL-Bibliothek, um den WEB-Server mit Verschlüsselung auszustatten.
Dabei wird ein Abstraktionslayer, das BIO-System, verwendet, mit dem man gut arbeiten kann, ohne Detailkenntnisse über diese Bibliothek haben zu müssen.
Der Hauptaufwand bei der Programmierung der SSL-Anbindung liegt somit in der Konfiguration der SSL-Umgebung. Dazu gehört das Anlegen von Zertifikaten und deren Verwaltung.
Zertifikate werden von uns eingesetzt, um sicher zu stellen, dass sich beide Kommunikationspartner bei der Konfiguration und dem Nachrichtenaustausch mit dem Server gegenseitig identifizieren. Zusätzlich werden in das Administrations-Zertifikat integrierte Attribute durch den SSL-WEB-Server abgefragt. So wird erreicht, dass ein Betreiber nur seine eigenen HotSpot administrieren kann, obwohl alle Zertifikate von einer einzigen CA signiert werden [Hübner-Folien].

Der so entstandene WEB-Server ist nun in der Lage statische Inhalte, wie HTML-Dateien und Grafiken zu „serven“. Zu Konfiguration des AG wird noch eine Möglichkeit benötigt, die in einem http-Request übermittelten Anfrage-Parameter zu deuten und umzusetzen.
Angesichts des begrenzten Umfangs der Konfigurationsoptionen erfolgt die Auswertung nicht durch eine Skriptsprache, sondern wird im Quellcode fest einprogrammiert.
Die präparierten HTML-Seiten übermitteln also wohl bekannte Variablen.

Bei der Konfiguration werden sie z.B. in einer Konfigurationsdatei abgelegt.

Für den Fall, dass der User über kein passendes Zertifikat verfügt, gibt es Anwendungslogik, die die Loginseite für HotSpot-User anzeigt, ohne dass der User in den Entscheidungsprozess involviert wird. Lediglich Administratoren werden zur Auswahl eines Administrations-Zertifikats aufgefordert, für den Fall, dass sie mehrere Betreiber supporten.

7.2.3.7. Accounting-Komponenten

Basierend auf den beiden Zugangsmöglichkeiten: WEB-Login und VPN, hat das Accountingmodul also die Anfgabe, Verbrauchsinformationen der aktiven Sessions auszulesen und periodisch dem AS mitzuteilen. Es arbeitet ferner mit der Firewall eng zusammen und übt so Kontrolle über den Datenfluss über die WLAN-Internet-Route. Das Funktionsprinzip beruht darauf, auf bestimmte Ereignisse mit der Umprogrammierung der Firewall zu reagieren. Außerdem werden Zählerständer der einzelnen Sessions ausgelesen und der Inactvity-Timeout ausgelöst. Die Firewallregeln können über eine iptables-Bibliothek (libiptc) injiziert werden. Um User-Sessions in der Firewall abzubilden, bedienen wir uns eines Tricks: Für jede Session wird eine eigene Chain erstellt, die mindestens zwei Regeln enthält, eine für eingehende Pakete und eine für ausgehende Pakete mit dem Target RETURN. So brauchen nicht alle Einträge durchlaufen zu werden.

7.2.3.8. Kommunikationskomponente

Das Kommunikationsmodul für Nachrichtenaustausch mit dem AS implementiert eine SSL-gestützte Kommunikation mittels Nachrichten. Der Initiator eines Nachrichtenaustausches ist topologiebedingt die Box, u.z. aus dem Grund, weil die Boxen hinter einer NAT-Firewall agieren oder an eine ADSL-Leitung mit u.U. einer dynamischen IP-Adresse angeschlossen sind. Dies macht es dem Server unmöglich, die Box anzusprechen. Die Nachrichten sind z.Zt. noch rein textueller Natur, es können aber auch Binärdaten übertragen werden. Bestimmte Events werden in ein dem Server zukömmliches Textformat übersetzt und an diesen geschickt. Der Server antwortet seinerseits mit einer passenden Nachricht, die das Event bestätigt oder es ablehnt. Im Fehlerfall können aber auch Nachrichten erzeugt werden, welche das Format nicht einhalten. Solche Nachrichten werden als Fehler interpretiert und verworfen.
Die SSL-Verbindung erfordert seitens der Box ein gültiges CA- und Server-Zertifikat.
Nur authorisierte Systeme können an solch einer Kommunikation teilnehmen, alle anderen kommen nicht über die SSL-Handshake-Phase hinaus, die noch vor jedem Übermitteln einer Nachricht stattfindet.
Auf der anderen Seite der Kommunikation, nämlich intern, nimmt das Modul Kommandos entgegen. Nach einer Übersetzung in das Messageformat des Kommunikationsprotokolls werden sie verschickt, von dem verarbeitet und beantwortet. Die Antwort wird in die interne Struktur, also wieder ein Kommando zurückübersetzt und an den Initiator des Nachrichtenaustausches weitergeleitet oder intern verarbeitet. In der Zwischenzeit nimmt das Modul keine weiteren Nachrichten entgegen, es arbeitet single-threaded.
Die interne Kommunikation ist hier mit Hilfe von Messagequeues implementiert, eine der drei wesentlichen Möglichkeiten zwischen Prozessen Informationen auszutauschen (neben Semaphoren und SharedMemory). Dazu existieren Datenstukturen, welche den Messages entsprechen, jedoch aus Performancegründen C-Strukturen sind. (In naher Zukunft sollen auch in der Kommunikation zwischen dem Server und den Boxen eben diese

Strukturen eingesetzt werden. Die Rechenlast würde sich dann zu Gunsten der Boxen verschieben, was auch im Sinne eines embedded Device ist).

Im Fall einer nicht Erreichbarkeit der Server-Services kann ein alternativer AS angesprochen werden. Dies wird durch einen Test ermittelt, bei dem der Dienst durch öffnen und schließen eines Ports auf eben diesem Server verifiziert wird.

Neben der Bereitstellung der Kommunikationsdienste für andere Module nimmt das Modul selbst auch noch zwei weitere Funktionen wahr: Die Übermittlung des Status der Box an den Server in einer Art Echo-Funktion und das Anfordern von Box-Updates vom Server.

Das Echo dient dem Zweck, aktuelle Log-Informationen an den Server zu übertragen, die dann zentral für jede Box abgerufen werden können. Die Log-Informationen beinhalten wichtige Fehlermeldungen sowie Warnungen, die auf Missbrauch des Systems hindeuten können. So kann rechtzeitig auf sich anbahnende Probleme reagiert werden und das System erhält gewissermaßen einen Hauch Leben: es gibt im live-Betrieb Lebenszeichen von sich, die eine ständige Verbesserung erst möglich machen.
Die Übertragung findet periodisch statt, sodass am Server auch erkennbar ist, wenn eine Box ernsthafte Probleme bekommt, die es unmöglich machen, den Server zu kontaktieren.
Die Periode ist am Server für jede Box einzeln einstellbar und wird durch das Echo der Box mitgeteilt, so dass diese über den Zeitpunkt der Übertragung des nächsten Echos stets Bescheid weiß.

Die zweite Funktion innerhalb des Moduls ist die Update-Funktion.
Jede Box hat eine Software-Version, welche beim Echo dem Server mitgeteilt wird.
Liegt dem Server eine neuere Version vor und ist der Zeitpunkt für das Update eingetreten, so wird das in der Antwort auf das Echo der Box mitgeteilt. Die Box fordert daraufhin die neue Softwareversion am Server an und quittiert ggf. den erfolgreichen Empfang. Im Fehlerfall wird die neue Version nicht quittiert und die Box kann

beim nächsten Echo die Software noch einmal anfordern. Die Software wird in einem dafür vorgesehenen Ort abgelegt und entsprechende Skripte werden aufgerufen, die die Installation und das Update der Softwarekomponenten umsetzten.

7.2.3.9. Die Hardware des Access Gateways

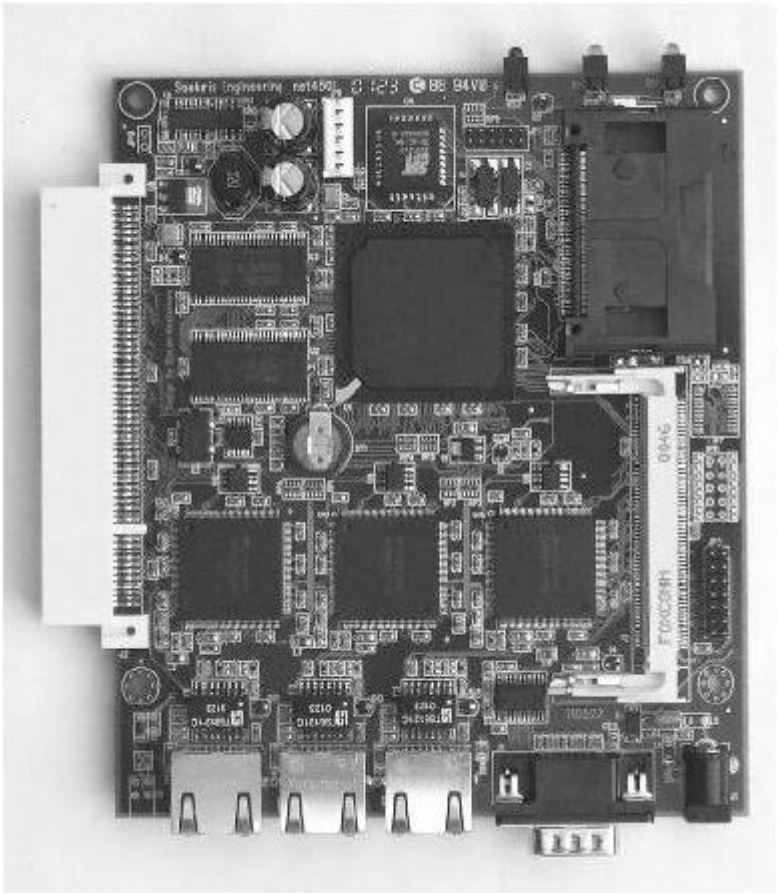
Die Vorgabe an die Hardware ist es vor allem minimal zu sein.
Die Gründe dafür liegen in der Wirtschaftlichkeit des Systems, wo es viele AccessGateways und wenige AccessServer gibt. Die Hardwarekomponenten sind so zusammenzustellen, dass möglichst wenig Serviceaufwand vor Ort besteht, da die Boxen oft an entlegenen oder unzugänglichen Orten platziert sind wie z.B. Dach- und Deckeninstallationen. So sind mechanische Bauteile wie Festplattenlaufwerke oder Lüfter oft Verursacher von Problemen. Auch ist die Anzahl vorhandener Schnittstellen minimal zu halten. Lediglich 2-3 Ethernetports, eine oder mehrere Wlan-Funkgeräte, Stomanschluss und eine Buchse für serielle Kommunikation sind für ein AG völlig ausreichend und minimieren die Risiken einer Fehlkonfiguration der Anschlüsse. Bei der Auswahl geeigneter Hardware wurden verschiedene „embedded pc's" evaluiert.
So sind Systeme auf Basis des PC104-Standards zwar sehr kompakt und modular, jedoch wegen der Vielzahl erforderlicher Steckverbindungen und überflüssiger Platinen vorwiegend zur Evaluierungszwecken geeignet. Für die Massenfertigung ist ein einziges Board deshalb von Vorteil. Miniatur-PC's wie z.B. die BareBones bieten den Vorteil, durch Massenfertigung recht erschwinglich und gleichzeitig leistungsfähig zu sein, jedoch sind sie nichts anderes als Heim-PC's, die durch zahlreiche onboard-Komponenten verkleinert werden konnten.
Die Lösung ist ein System selbst zu assemblieren oder ein Minimalsystem, das die Anforderungen befriedigt, zu finden. Bei der Recherche nach einem solchen System fanden wir eine kleine Hardware-Schmiede, die eine Reihe von passenden embedded Netzwerk-PC's anbietet: Soekris NET45xx- embedded network PC's.

Spezifikationen:

100/133 Mhz AMD ElanSC520
64 Mbyte SDRAM on board
1 Mbit BIOS/BOOT Flash
CompactFLASH Type I/II socket bestückt mit einem 64Mbyte Modul
3 10/100 Mbit Ethernet ports, RJ-45
1 serieller Port, DB9.
Power LED, Aktivitäts LED, Fehler LED
Mini-PCI type III socket. (t.ex for optional hardware encryption.)
PCI Slot
8 bit GPIO, 14 pins
Hardware watchdog
Abmmesungen des Boards 4.85" x 5.7"
Stromversorgung entweder 5V DC doder7-20V DC, max 10 Watt
Umgebungstemperatur 0-60 °C

Software:

comBIOS für eine Menagement Konsole
PXE boot rom für Booten vom Netzwerk



Der AMD-Elan Prozessor ist ein Vertreter der bekannten i486 Architektur. Er wurde unter dem Aspekt entwickelt, speziell für embedded appliances besonders gut geeignet zu sein. Dazu tragen Faktoren wie: ein geringer Stromverbrauch, integrierte Funktionalitäten wie PCI-Controller, Memory-Controller, Serial-Controller, Watchdog, Interrupt-Controller, DMA-Controller und niedrige Hitzeemmision wesentlich bei.
Die Bestückung mit 64Mbyte SDRAM erfüllt zeitgemäße Maßstäbe an Speicherdurchsatz und Größe für Embedded Devices im Router/Firewall-Sektor.
Auch mangelt es nicht an Erweiterungsmöglichkeiten. Durch den Standard PCI-Steckplatz und die miniPCI-Variante lassen sich gängige Erweiterungen anbinden. Besonders interessant im Umfeld der Emmbeded Devices ist der miniPCI –Steckplatz. Hier kann man auf eine breite Palette von Zubehör aus dem Notebook-Sektor zugreifen, welches ähnliche Voraussetzungen zu erfüllen hat, also niedrige Verbrauchswerte und Platzersparnis. So sind z.B. WLAN-,

ISDN- und Beschleunigerkarten für Verschlüsselung im entsprechendem Format von unterschiedlichen Herstellern erhältlich.
Durch das Vorhandensein von drei Ethernetports sind typische Routeranwendungen mit den Schnittstellen LAN, WAN und DMZ oder Managementport leicht realisierbar. WLAN lässt sich durch eine PCI-, miniPCI-Karte oder in einer anderen Version der Hardware durch PCMCIA/PC-Card ebenfalls anschließen.
Die GPIO's lassen sich frei verwenden. Eine typische Anwendung dafür wäre, weitere LED's anzusteuern oder Schalter vorzusehen.
Letztenendes trägt die externe Stromversorgung durch einen geregelten oder ungeregelten Trafo zu noch mehr Flexibilität beim Einsatz in unterschiedlichen Ländern der Welt mit individuellen Stromversorgungen. Auch reduziert und verteilt sich die Hitzeleistung der Box durch den Einsatz einer externen Stromversorgung, was sich gut in das Gesamtkonzept eines langlebigen und stromsparenden Embedded Device eingliedert.

7.3. Server

7.3.1. Anforderungen

Im Kapitel 3.2 wurden unterschiedliche Szenarien beschrieben, in welchen WLAN-Systeme zum Einsatz kommen. Wie bereits herausgestellt, gibt es hier Überschneidungen im Funktionsumfang. Als Maßstab für das zu entwickelnde System wird das Szenario einer durch einen Wireless Service Provider betriebenen Infrastruktur von WLAN-Zugängen herangezogen (siehe 3.1.4 WLAN-Betreiber), die sich hieraus ergebenen Anforderungen sind zu einem Großteil auch in den anderen Szenarien wiederzufinden.
In diesem Szenario wird davon ausgegangen, dass durch den Betreiber des Systems an unterschiedlichsten Orten ein Internetzugang für dessen Kunden bereitgestellt wird, diese Orte werden als Hotspot bezeichnet (siehe 3.2.3 Hotspots). Dem Betreiber soll eine zentrale Verwaltung des kompletten Systems ermöglicht werden, der Zugang für die Benutzer soll unabhängig vom gewählten Hotspot möglich sein. Hieraus ergibt sich eine Verteilung des Systems in einerseits viele, an unterschiedlichen Orten befindliche Zugangspunkte (den AccessGateways) und einer zentralen Verwaltung (dem AccessServer).
Kernaufgabe des zu entwickelnden Servers ist die Bereitstellung eines Kommunikationsprotokolls, welches den erforderlichen Austausch von Informationen zwischen dem Server und den Zugangspunkten ermöglicht. Der Umfang dieses Protokolls ergibt sich aus den Anforderungen des erwähnten Szenarios. So wird z.B. gefordert, dass Benutzer sich vor Zugangsgewährung zu identifizieren haben oder, dass die Nutzung des Internetzuganges zum Zwecke der Abrechnung erfasst werden muss. Die folgende Abbildung 22 skizziert grob, wie sich dieses in einer Kommunikation zwischen dem AccessGateway und dem AccessServer wiederspiegeln könnte:

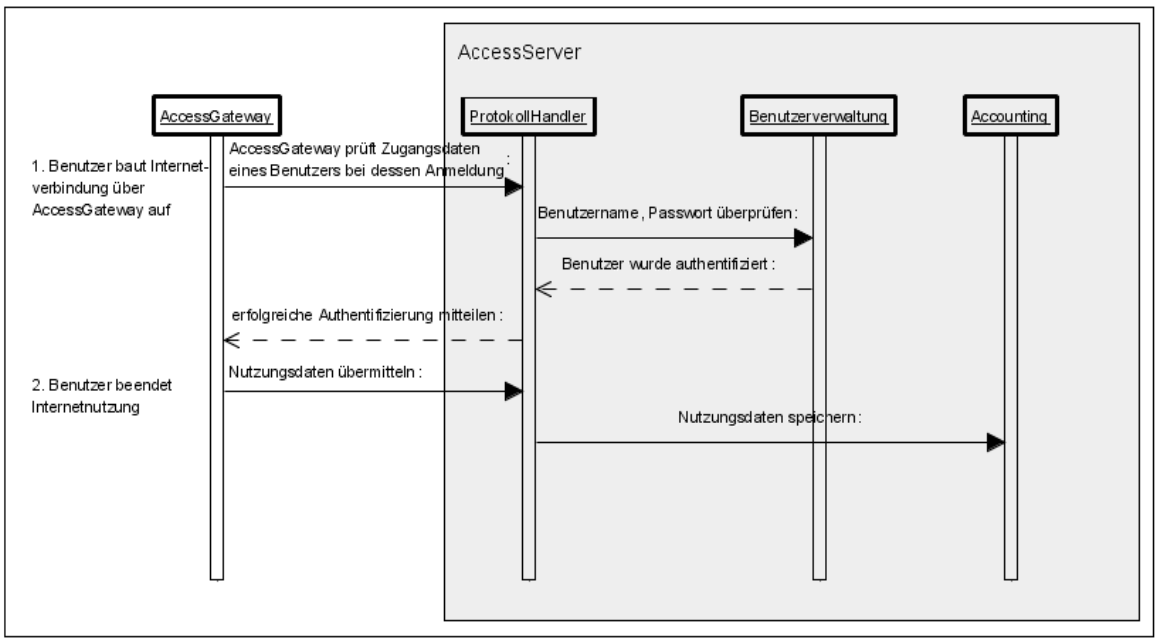


Abbildung 22 Ablauf Anwendungsfall Authentifizierung / Accounting

Für den Anwendungsfall eines Verbindungsaufbaus zum Internet über das AccessGateway (1) durch einen Benutzer am Hotspot, richtet dieses zunächst eine Anfrage an den Server, um die Identität des Benutzers und dessen Berechtigung zum Verbindungsaufbau zu überprüfen. Beendet der Benutzer später seine bereitgestellte Internetverbindung wieder, teilt das AccessGateway dem Server Informationen über den Umfang der Nutzung (Dauer, Transfervolumen) mit.

Auch wenn die Vorgänge sehr vereinfacht dargestellt wurden, können bereits neben der reinen Protokoll-Verarbeitung (ProtokollHandler) weitere Teilfunktionalitäten identifiziert werden, welche auch für andere Anwendungsfälle von Bedeutung sein können (Benutzerverwaltung, Handling der Accounting-Daten).

An weiterer Anwendungsfall ergibt sich aus der Forderung für den produktiven Einsatz eines solchen Systems, durch einen Wireless Service Provider, eine einfache Administration aller hierfür erforderlichen Daten bereitzustellen, dieses betrifft z.B. die Verwaltung der Kunden (Zugangsdaten, Nutzungsdaten) oder der einzelnen AccessGateways. Der AccessServer stellt hierzu ein Web-Interface bereit, die Administration kann so über den Web-Browser erfolgen. Folgende Abbildung zeigt beispielhaft die Vorgänge für den

Abruf der Nutzungsdaten eines Benutzers über die Administrations-Oberfläche:

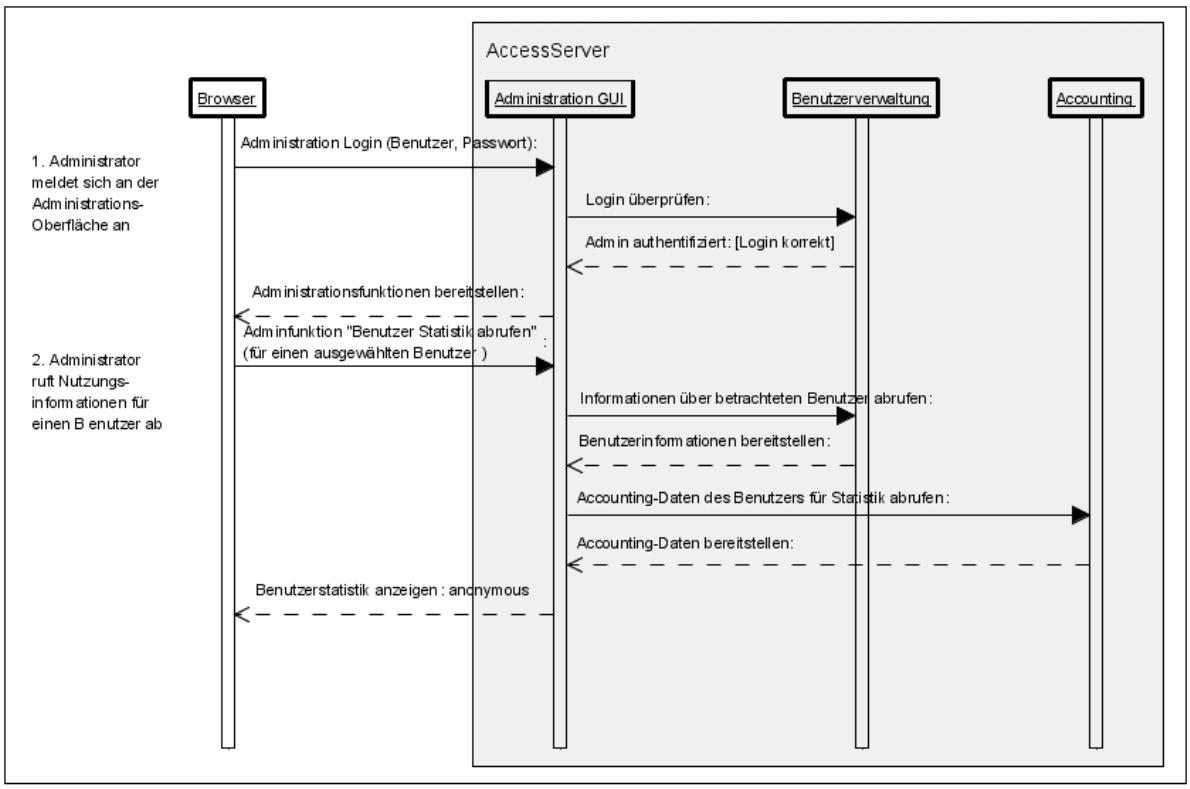


Abbildung 23 Ablauf Anwendungsfall Administration, Abruf der Nutzungsdaten eines Benutzers

Auch der Zugriff auf die Administrationsoberfläche muss abgesichert werden, ein Anwender, der diese nutzt, authentifiziert sich daher zunächst (1), z.B. mittels Benutzername und Passwort. Auf der Oberfläche startet der Mitarbeiter den Abruf der Daten eines Benutzers, das System stellt die erforderlichen Informationen zusammen und präsentiert sie, in diesem Fall werden sie im Browser dargestellt.

Bei der Identifizierung der Teilfunktionalitäten wird deutlich, dass auch in diesem Anwendungsfall auf ähnliche Funktionsbereiche, wie der Verwaltung von Benutzern zugegriffen werden muss.
Für die Umsetzung des AccessServers werden daher folgende Teilaufgaben definiert, diese werden im folgenden detaillierter untersucht und eine Lösung erarbeitet:

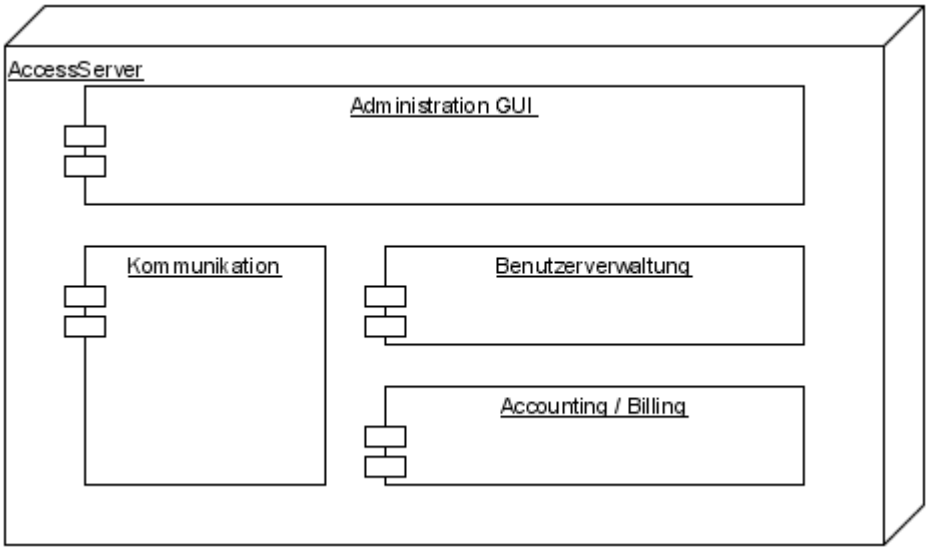


Abbildung 24 Komponenten des AccessServers

Die Abbildung 24 zeigt die anhand der bekannten Anforderungen identifizierten funktionalen Komponenten des AccessServers.
Die Umsetzung der einzelnen Komponenten, sowie deren Interaktion soll im Folgenden erarbeitet werden. Die Komponenten sind:

Gateway-Server-Kommunikation

Das zu entwickelnde System besteht aus einer Vielzahl örtlich verteilter Zugangspunkte (AccessGateways) unter einer zentralen Verwaltungseinheit (AccessServer), zur Erfüllung der geforderten Aufgaben ist eine Kommunikations-Protokoll zwischen diesen zu entwickeln. Dieses muss einem AccessGateway die Authentifizierung eines Benutzers ermöglichen, ebenso müssen vom Gateway Daten über die Nutzung des Zugangs übermittelt werden. Weiterhin wird gefordert, dass der AccessServer Administrations- bzw. Monitoring-Funktionen für einzelne Gateways bereitstellt, auch hierfür ist ein Datentransfer erforderlich.

Accounting / Billing

Die vom AccessGateway erfassten Nutzungsdaten einer Internetnutzung müssen zur Kostenermittlung erfasst werden.

Benutzerverwaltung

Es sind geeignete Verwaltungsmöglichkeiten der teilnehmenden Benutzer zu erarbeitet, hierbei sollte berücksichtigt werden, dass die Verwaltung von Benutzern eine in vielen Systemen auftauchende Problemstellung ist und auf eventuell vorhandene Benutzerdaten zugegriffen werden kann.

Administrations-Oberfläche

Die Administration des Systems sowie die Verwaltung aller relevanter Daten (Benutzer, AccessGateways) erfolgt über den AccessServer, um diese Aufgaben durch einen Betreiber durchführbar zu machen, ist eine geeignete Oberfläche bereitzustellen.

7.3.2. Gateway-Server-Kommunikation

7.3.2.1. Authentifizierung, Autorisierung, Accounting (AAA)

Die Infrastruktur der Hotspot-Lösung entspricht im wesentlichen der konventioneller, kabelgebundener Internet Service Provider. Die Verbindung des Benutzers zwischen seinem Rechner und dem internetbereitstellenden Zugangspunkt (Network Access Server, NAS) des ISP wird über das Telefonkabel mittels Modem hergestellt. Die Abbildung 25 zeigt den prinzipiellen Aufbau eines solchen ISP Zugangs (ähnlich kann auch ein Zugang ins Firmennetz realisiert werden). Die Aufgabe des Network Access Servers ist es, vor Bereitstellung eines Zuganges den Benutzer zu überprüfen (Authentifizierung, Autorisierung) sowie die Nutzung des Zugangs durch ihn zu protokollieren (Accounting).

Authentisierung
Bevor dem Benutzer ein Verbindungsaufbau ermöglicht wird ist dessen Identität sicherzustellen.

Autorisierung
Zu überprüfen, in welchem Umfang der Zugang genutzt werden darf, ist Aufgabe der Autorisierung. Denkbar sind hier z.B. Einschränkungen im Umfang der Nutzungsmöglichkeiten.

Accounting
Ziel des Accountings ist es, eine quantitative Erfassung der Zugangsnutzung eines Benutzers zu erfassen (z.B. Dauer der Verbindung, transferiertes Datenvolumen). In kommerziellen Systemen bilden die erfassten Daten die Grundlage der Kostenermittlung.

Übertragen auf das Hotspot-System werden die Aufgaben des Network Access Servers vom AccessGateway wahrgenommen. So wie ein ISP über mehre Einwahlknoten verfügt, ist auch den Hotspot-Nutzern der Zugang an allen AccessGateways zu ermöglichen. Dazu müssen alle NAS Zugriff auf die Benutzerdaten haben, diese im NAS bzw. AccessGateway zu verwalten erscheint in Hinblick auf den damit verbundenen Synchronisationsaufwand zwischen den einzelnen AccessGateways/NAS als wenig sinnvoll.
Im Bereich der Internet Service Provider wurde dieser Problemstellung mit dem Entwurf sogenannter AAA-Protokolle (**A**uthentifizierung, **A**uthorisierung, **A**ccounting) begegnet, welche den Datenaustausch zwischen einem Einwahlknoten/NAS und der zentralen Datenbank (AAA-Server) definieren.

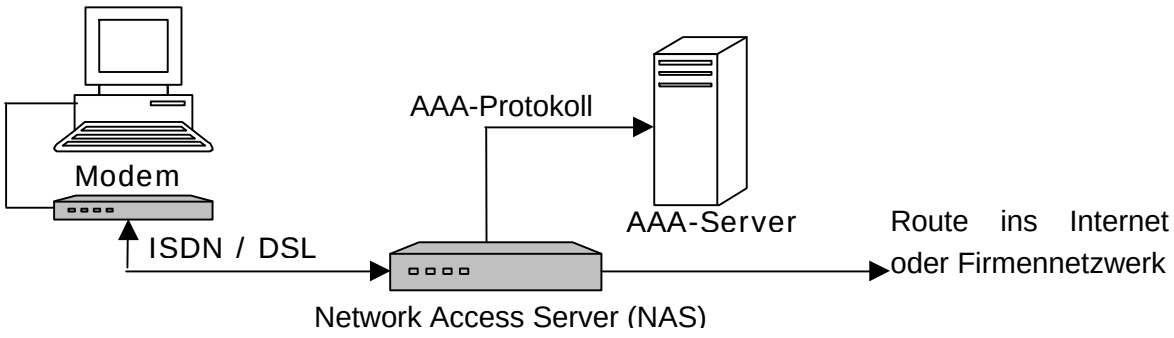
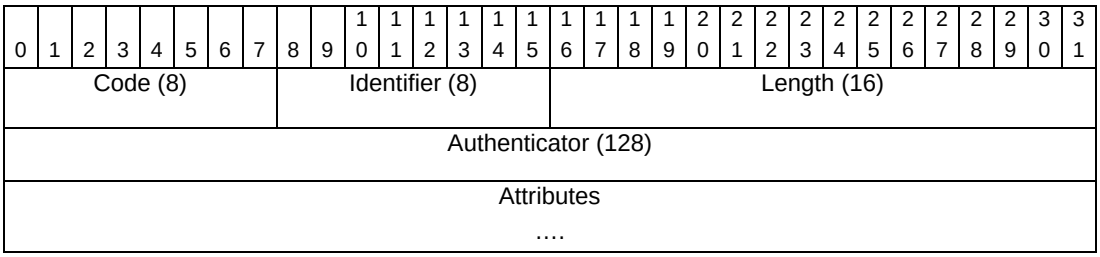


Abbildung 25 Struktur Wählzugang zum Provider / Firmennetz

7.3.2.2. Radius

Der bekannteste Vertreter der AAA-Protokolle ist das von der Firma Livingston (heute Lucent) entwickelte RADIUS (Remote Authentication Dial-In User Service). Hierbei handelt es sich um ein Client-/Server-Protokoll, die Position des Clients übernimmt in diesem Szenario der NAS. Im Folgenden sollen die durch Radius gegebenen Möglichkeiten in Hinblick auf eine Verwendung innerhalb des Hotspot-Systems beschrieben werden. RADIUS verwendet UDP zum Versenden der Nachrichten zwischen NAS und dem (RADIUS-)Server, die Pakete haben dabei folgenden Aufbau:



Der Verwendungszweck eines gesendeten Paketes wird durch die Code-Angabe kenntlich gemacht, dieses Feld kann folgende Werte annehmen:

Code	Bedeutung
1	Access-Request
2	Access-Accept
3	Access-Reject
4	Accounting-Request
5	Accounting-Response
11	Access-Challenge
12	Status-Server (experimental)
13	Status-Client (experimental)
255	Reserved

Über das Identifier-Feld erfolgt die Zuordnung von Anfrage- und Antwort-Paket.
Jedes RADIUS-Paket kann über eine variable Anzahl von Attributen verfügen, welche Attribute in einem Paket vorhanden sind richtet sich nach dem jeweiligen Verwendungszweck. Neben den Standard-RADIUS-Attribute ([RFC2865]), können auch herstellerspezifische Attribute eingesetzt werden. Ein Attribut innerhalb des Paketes hat folgende Struktur:

Type (1 Byte)	Length (1 Byte)	Value (Length – 2 Bytes)

Die maximale Länge eines Attributes ist so auf 254 Bytes beschränkt. Für die Längenangabe des gesamten Paketes ist ein Maximal-Wert von 4096 vorgesehen (incl. Code, Length, Identifier, Authenticator und Attribute), was den Umfang der gesendeten Attribute ebenfalls einschränkt.

Zunächst soll der Vorgang der Benutzeranmeldung näher betrachtet werden, von Bedeutung sind hier die RADIUS-Pakete mit den codes 1,2,3 und 11. Auf das Accounting wird noch an späterer Stelle eingegangen. Das folgende Sequence-Diagramm zeigt den prinzipiellen Ablauf einer Benutzerauthentifizierung beim Verbindungsaufbau mit einem Zugangsknoten:

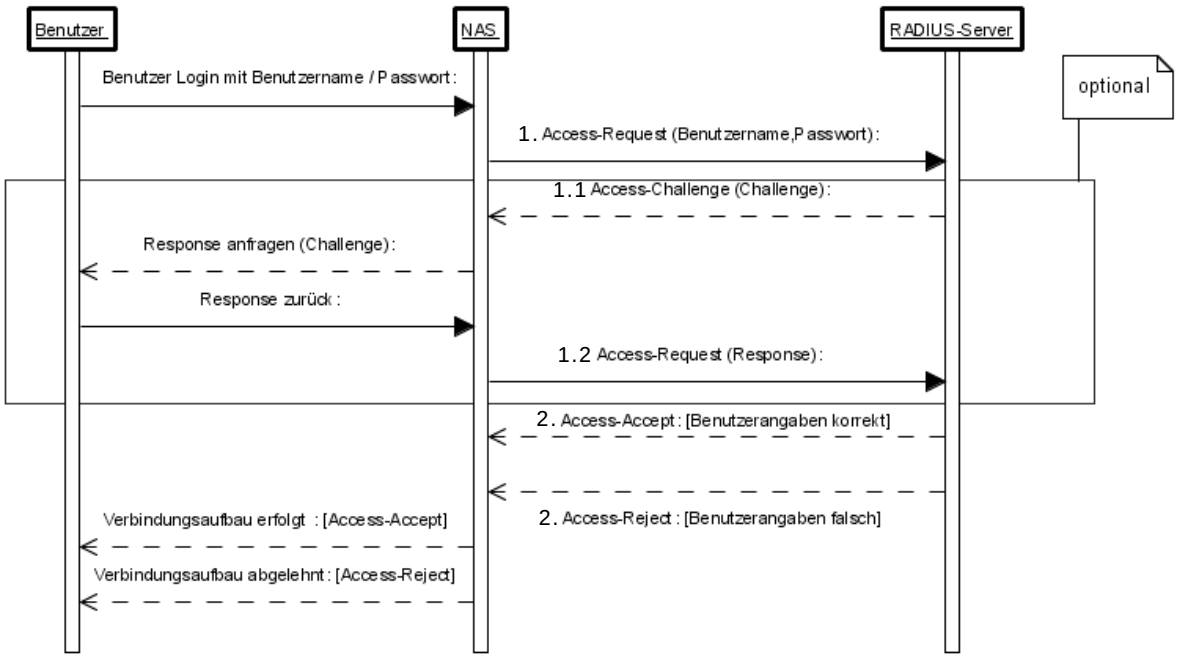


Abbildung 26 RADIUS Authentifizierung

1. Access-Request

Der zu authentifizierende Benutzer versucht sich am NAS anzumelden und übergibt zu diesem Zweck seinen Benutzernamen und sein Passwort (PAP). Der NAS erzeugt ein Access-Request Paket unter der Verwendung der RADIUS-Attribute „User-Name“ und „User-Password“ und sendet dieses an den RADIUS-Server. Das Passwort allerdings wird zuvor unter Zuhilfenahme des geheimen Schlüssels zwischen NAS und RADIUS-Server und dem generierten Request-Authenticator verschlüsselt (MD5(shared secret + RA), Details unter [RFC2865])

2. Access-Reject / Access-Accept

Der RADIUS-Server überprüft die Angaben unter Verwendung einer Benutzerdatenbank, existiert der angegebene Benutzername und ist das Passwort korrekt, sendet der RADIUS-Server ein Access-Accept-Paket zurück, dieses kann Attribute enthalten, welche die Nutzungsmöglichkeiten, entsprechend eines Benutzerprofils, genauer definieren.

Optional kann vom Server ein Challenge/Response-Verfahren zur Authentifizierung gefordert werden:

1.1 Access-Challenge
Erzwingt die Konfiguration des RADIUS-Servers für den zu authentifizierenden Benutzer die Verwendung einer Challenge/Response-Authentifizierung, reagiert der Server auf den ersten Access-Request des NAS mit einem Access-Challenge-Paket. Das Paket enthält einen zufällig genierten Wert (Challenge), welcher vom NAS an den Benutzer weitergereicht wird. Der Benutzer muss diesen Wert mit seinem privaten Schlüssel (e.g. Passwort) verschlüsseln, dieses kann durch geeignete Software (Login-Client) oder zusätzliche Hardware (e.g. SecureID-Karte) erfolgen. Das Ergebnis (Response) wird an den NAS übergeben, welcher mit diesen Angaben erneut ein Access-Request generiert und dem RADIUS-Server zur Überprüfung zusendet.

1.2 Access-Request, Access-Reject
Der RADIUS-Server führt die Operation auf dem Challenge mittels des ihm bekannten Passwortes des Benutzers ebenfalls durch und überprüft ob des Ergebnis mit dem Response des Benutzers übereinstimmt. Abhängig vom Ergebnis wird jetzt, wie zuvor beschrieben, entweder mit einem Access-Accept oder Reject geantwortet.

Der Verbindungsaufbau zwischen den Benutzer und dem NAS und der damit einhergehende Datenaustausch zur Authentifizierung ist nicht Gegenstand des RADIUS Protokolls. Es existieren unterschiedliche Verfahren um dieses zu realisieren (PAP, CHAP hier sei auf 6.3.1.4). Durch den flexiblen Einsatz der Attribute innerhalb des RADIUS-Protokolls ist eine Interoperation mit verschiedenen Methoden möglich (siehe [RFC 2865, Kapitel 2.2 Interoperation with PAP and CHAP]).

Accounting

Wird davon ausgegangen, dass das Hotspot-System von einem Wireless Service Provider, wie im Szenario unter 3.1.4. beschrieben, betrieben wird, wurde bereits herausgestellt, dass es erforderlich ist, eine Kostenermittlung vor der Nutzung des Zugangs durch einen Kunden durchzuführen. Es ist somit nicht nur erforderlich die Identität eines Benutzer bei der Anmeldung sicherzustellen, sondern auch die quantitative Nutzung des Zugangs zu ermitteln. Für eine Kostenermittlung sind Angaben, wie die Dauer der Nutzung und das transferierte Datenvolumen von Interesse. Für die Erfassung dieser Accountingdaten wurden beim Entwurf des RADIUS-Protokolls die Pakettypen Accounting-Request und Accounting-Response vorgesehen (Erweiterung der ursprünglichen RADIUS-Spezifikation, in separatem RFC beschrieben [RFC 2866]). Bei Bereitstellung der Verbindung sowie bei deren Beendigung durch den Benutzer signalisiert der Zugangsknoten (NAS / Access-Gateway) dieses dem Server, im Falle des RADIUS-Protokolles werden die Pakete wie folgt versendet:

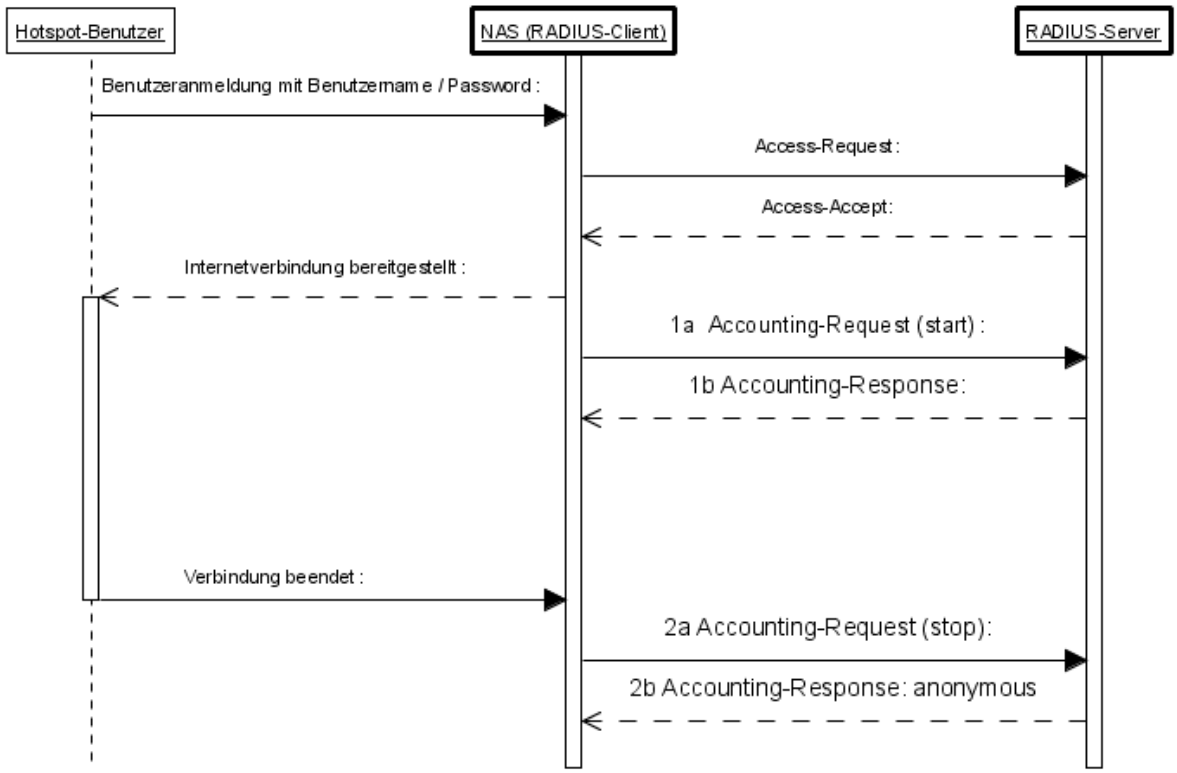


Abbildung 27 RADIUS - Accountig

1. Bereitstellung des Zugangs

Der Network Access Server, welcher den Dienst (Internetzugang) für den Benutzer bereitstellt, übermittelt Accounting-Informationen durch ein mit erforderlichen Parametern versehenes Accounting-Request-Paket, dieses erfolgt zu Beginn und am Ende einer Dienstnutzung (das Attribut Acct-Status-Type nimmt hierfür den Wert start bzw. Stopp an).

Zunächst authentifiziert sich der Benutzer für die Inanspruchnahme des Dienstes, wie dieses unter 7.1.2 Radius beschrieben wurde (Access-Request). War dieses erfolgreich, wird das Accounting-Start-Paket an den zuständigen RADIUS-Server gesendet (1a), das Paket enthält unter anderem Angaben über den NAS, über welchen der Zugang erfolgt (NAS-IP-Address), eine Identifizierung der zu protokollierenden Sitzung (Acct-Session-Id) und natürlich den Benutzer, der den Dienst in Anspruch nimmt (User-Name).

Der erfolgreiche Empfang eines Accounting-Request-Paketes wird vom RADIUS-Server mit einem Accounting-Response-Paket quittiert (1b).

2. Beendigung der Zugangsnutzung

Während der Nutzung des Zugangs durch den Benutzer ist es Aufgabe des Network Access Servers, den Umfang der Inanspruchnahme festzuhalten (siehe Kapitel 7.1.2.3 und 7.1.3.7) und diesen nach Beendigung der Verbindung an den RADIUS-Server zu übermitteln. Zu diesem Zweck wird ein Accounting-Request-Paket mit einem auf „Stop“ gesetzten Acct-Status-Type übermittelt (2a), welches über die Dauer der Verbindung (Acct-Session-Time) und die transferierten Datenmengen (Acct-Input-Octets, Acct-Output-Octets) Auskunft gibt. Nach Verarbeitung der Daten durch den RADIUS-Server quittiert dieser den Erhalt durch ein Accounting-Response (2b).

Der RADIUS-Server ist dafür verantwortlich die ihm übermittelten Nutzungsdaten in geeigneter Form, z.B. in einer Datenbank, zu speichern. Die Daten aller Nutzer des Systems liegen so, unabhängig vom genutzten Zugangspunkt, an zentraler Stelle vor und können zu weiteren Auswertungen herangezogen werden. Die Kosten, die ein Service-Provider dem Kunden für die Nutzung des Internetzuganges über das System in Rechnung stellt, können anhand dieser Daten ermittelt werden. Darüber hinaus ermöglichen diese Daten dem Betreiber auch Rückschlüsse auf die Auslastung des Systems.

7.3.2.3. Erweiterte Anforderungen

Eine weitere Anforderung, die eine Kommunikation zwischen den AccessGateways und dem Server erforderlich machen würde, ist die Überwachung der Funktionstüchtigkeit der einzelnen Gateways. Diese müsste hierzu Status-Informationen in regelmäßigen Abständen an den Server senden (oder der Server müsste diese Abfragen). Diese Aufgabe wird vom RADIUS-Protokoll nicht adressiert, hier sind andere Lösungen zu finden.

7.3.2.4. Realisierung

Es hat sich herausgestellt, dass mit dem RADIUS-Protokoll bereits ein Lösungsansatz existiert, welcher einen Großteil der an das Hotspot-System gestellten Anforderungen in Bezug auf die Kommunikation zwischen dem Server und den Gateways erfüllt. Dieses führt zu der Überlegung eine vorhandene Implementierung eines RADIUS-Servers, z.B. freeRadius (www.freeradius.org), einzusetzen und entsprechend zu modifizieren. Aufgrund der hier geltenden Lizenz-Bedingungen (GPL, http://www.fsf.org/licenses/gpl.html) ist eine kommerzielle Verwertung des entstehenden Hotspot-System schwer möglich. Weiterhin wäre man in die Architektur des verwendeten Servers

sowie die verwendete Programmiersprache (in diesem Fall C) gebunden.
Daher fiel die Entscheidung auf die Entwicklung eines eigenen Protokolls und der dazugehörigen Verabreitung durch einen Server. Da der durch das RADIUS-Protokoll vorgegebene Datenaustausch sich bereits in der Praxis bewärt hat, wird sich die Lösung an diesem orientieren.
Während RADIUS von einer Übertragung mittels UDP-Paketen ausgeht, setzen wir eine SSL-Verbindung als Basis für die Kommunikation zwischen Gateway und Server ein, im Gegensatz zu UDP ist dieses ein verbindungsorientiertes Protokoll, was das Handling (Timeout, Retransmission) wesentlich vereinfacht. Ein weiterer Vorteil gegenüber RADIUS ist der Wegfall der Begrenzung des Umfangs transferierter Parameter, auch wird mittels SSL die gesamte Nachricht verschlüsselt übertragen, während das RADIUS-Protokoll hier nur Mechanismen zur Verschlüsselung der im Paket übertragenen Passwörter vorsieht. Ein AccessGateway kann zusätzlich mit einem Zertifikat ausgestattet werden, mittels welchem es sich beim Verbindungsaufbau authentifiziert, zudem kann die Identität eines AccessGateways zweifelfrei festgestellt werden.

Die Entwicklung des Servers erfolgt in der Programmiersprache Java, als Laufzeitumgebung wird ein J2EE (Java 2 Enterprise Edition) konformer Application–Server eingesetzt. Mit J2EE wurde durch SUN eine Spezifikation [SUN1] erstellt, die grundlegende Funktionen für die Erstellung von Server-Applikationen definiert, diese werden von Applikation-Servern unterschiedlicher Hersteller implementiert[28]. Die Verarbeitung von http bzw. HTTPS–Anfragen gehört zu den Aufgaben, bei denen Unterstützung vom Applikation-Server bereitgestellt wird, hierzu wurden in J2EE sogenannte Servlets definiert (für weiterführende Informationen zur Servlet-Programmierung sei auf [SUN3] verwiesen). Ein Klasse, die eine HTTP(S)-Anfrage verarbeiten soll, erbt hierzu von der abstrakten

[28] Zu den verbreitetsten Application-Servern gehören der WebLogic Server von Bea Systems (http://www.bea.com), der WebSphere Application-Server von IBM (http://www.ibm.com/de/software/websphere/) oder der Oracle 9iAS (http://www.oracle.com)

Klasse javax.servlet.http.HttpServlet. Die AccessGateways bauen eine SSL-Verbindung zum Server auf, das Handling der SSL-Connection (Verbindungsaufbau, Zertifikathandling) wird hierbei vom Application-Server übernommen, dem Servlet wird Zugriff auf den Request (javax.servlet.http.HttpRequest) und auf ein Objekt zum Senden der Antwort (javax.servlet.http.HttpResponse) ermöglicht. Die Kommunikation zwischen Gateway und Server folgt dem Request-Response-Verfahren. Wie beim RADIUS-Protokoll geht die Kommunikation vom AccessGateway aus, die Attribute der gesendeten Anfrage werden hierbei im http-Request übermittelt. Die Anfrage wird von einem Servlet (ProtocolHandlerServlet) verarbeitet, dieses sendet die Antwort im HTTP-Response zurück.
Für die unterschiedlichen Pakete wird auf das Attribut-Set aus dem RADIUS-Protokoll zurückgegriffen.
Abbildung 28 und Abbildung 29 zeigen die an der serverseitigen Verarbeitung beteiligten Klassen bzw. den Ablauf der Request-Verarbeitung am Beispiel einer eingehenden AuthRequest-Anfrage. Die Implementierung der Requestverarbeitung orientiert sich an den Design-Pattern „Command“ und „Command Dispatcher“ [Gamma 1994]. Die unterschiedlichen Pakete werden auf konkrete Klassen abgebildet, welche von der abstrakten Klasse Protocol_Command erben, eine jede dieser Klassen ist für die Behandlung des entsprechenden Paketes zuständig. Das ProtocolHandlerServlet nutzt eine Factory (ProtocolCommandFactory), um aus dem eingehenden HTTP-Request die dazugehörige Instanz eines ProtocolCommands zu erzeugen (z.B. ProtocolCommand_AuthRequest), das Servlet wird so von der Verarbeitung der Anfrage entkoppelt.
Das erzeugte Kommando wird vom ProtokolHandlerServlet ausgeführt (execute()), das Kommando greift hierzu auf die benötigten Resourcen des Servers zu (z.B. Benutzerverwaltung zum überprüfen eines Logins). Das Ergebnis dieser Ausführung ist erneut ein Protocol_Command, welches zusätzlich das Interface ReturnableCommand implementiert und über die Fähigkeit verfügt sich, mit seinen Attributen als Anfrageergebnis an des AccessGateway zurückzusenden, die Attribute werden dabei im http-Response-Body hinterlegt.

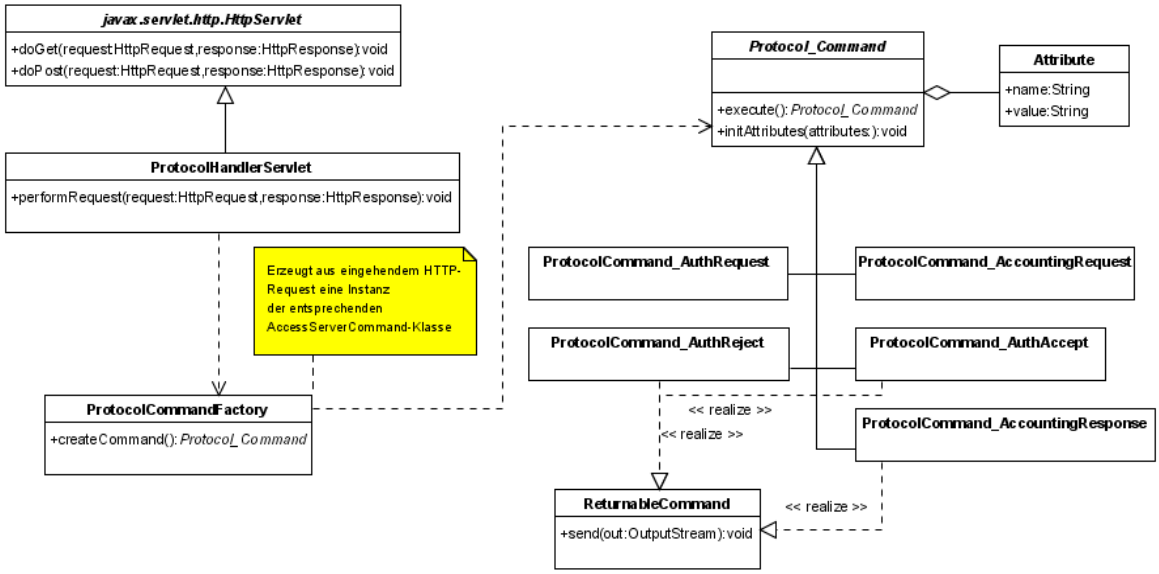


Abbildung 28 Klassendiagramm Protokollverarbeitung

Der in Abbildung 29 geschilderte Ablauf zeigt die Umsetzung des bereits in Kapitel 7.3.1 beschriebenen Vorganges der Benutzerauthentifizierung auf diese Architektur.

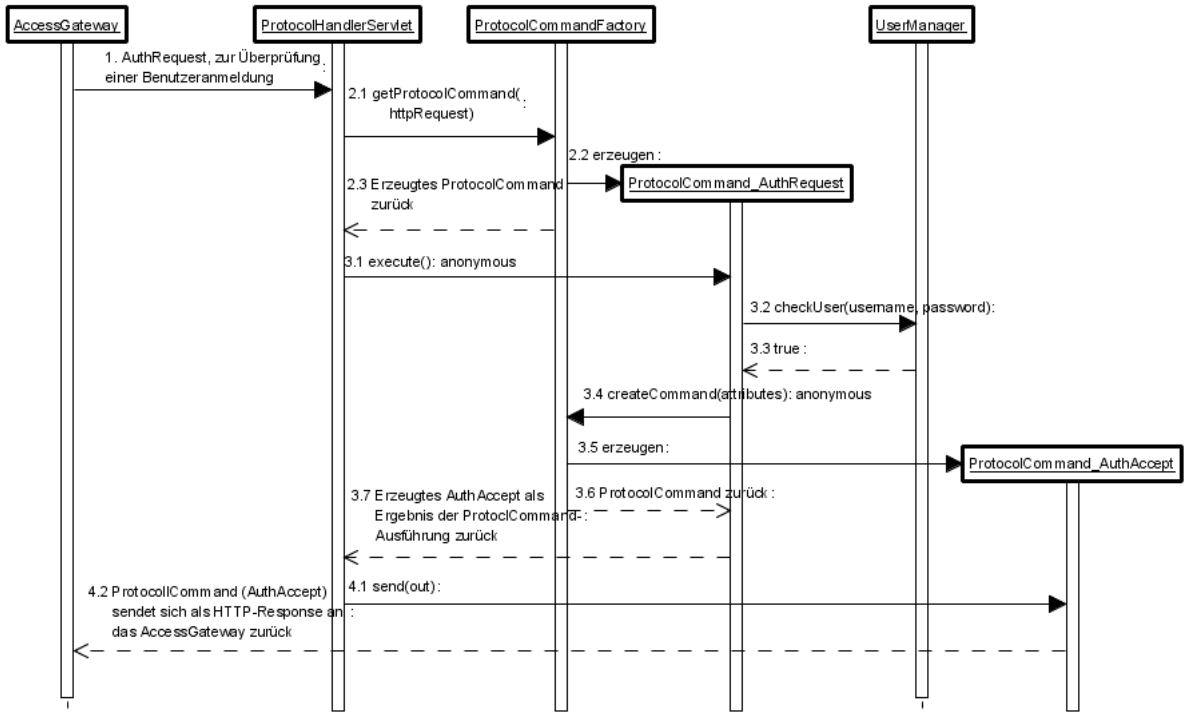


Abbildung 29 Ablauf Protokollverarbeitung

Neben den durch RADIUS vorgegebenen Pakten für Authentifizierung, Autorisierung und Accounting ist dieses Verfahren auch auf weitere Anwendungsfälle, wie zum Beispiel die Übermittlung von Statusinformationen der einzelnen AccessGateways an den Server möglich. Auch kann ein Nachrichtentyp dazu verwendet werden, das ein AccessGateway ein Software-Update vom Server anfragt und dieses, sofern vorhanden, als Antwort übermittelt bekommt.

Ein weiterer Vorteil, der sich aus der Entscheidung für J2EE als Plattform für das System ergibt, ist die Möglichkeit, die Anwendung mit überschaubarem Aufwand geclustert, also auf mehrer physikalische Server verteilt, zu betreiben. So kann einer steigenden Anzahl von AccessGateways durch entsprechende Skalierung der Server-Applikation begegnet werden.

7.3.3. Benutzerverwaltung

Es hat sich in den vorherigen Abschnitten bereits gezeigt, dass der Verwaltung von Benutzern, die über das System Zugang zum Internet erhalten, eine zentrale Funktionalität des Servers ist, welche in unterschiedlichsten Anwendungsfällen benötigt wird. Es gilt ein Modul zur Benutzerverwaltung zu erstellen, welches die unterschiedlichen Operationen im Umgang mit Benutzern bereitstellt. Hierzu gehört das Anlegen, Löschen und Bearbeiten von Benutzern im System oder die Überprüfung von Benuzteridentitäten.

7.3.3.1. X.500 / LDAP

Die Verwaltung von personenbezogenen Daten ist im Bereich vernetzter Systeme eine häufige Aufgabenstellung. Angaben zu Personen werden für unterschiedliche Zwecke und in unterschiedlichem Umfang verwaltet, so z.B. für Benutzerkonten zur Zugangsbeschränkung bei Betriebsystemen, in Personaldatenbanken oder Adressverzeichnissen. Oft führt dies zu einer Situation, in der für jede Anwendung eine eigene Benutzerdatenbank in einer spezifischen Form angelegt wird. Dieses bringt einen enormen Verwaltungsaufwand mit sich, für identische Personen müssen mehrfach Daten gepflegt werden, ändert sich eine Angabe zur Person muss diese ggf. in allen Benutzerdatenbanken gepflegt werden.
Um eine solche Situation zu vermeiden, werden sogenannte Verzeichnisdienste eingesetzt. Verzeichnisdienste ermöglichen die strukturierte Verwaltung von Informationen und stellen eine Schnittstelle zum Zugriff auf diese bereit. Die Verwaltung ist hierbei nicht auf personenbezogene Daten beschränkt. Durch eine Standardisierung von Verzeichnisdiensten wird eine gemeinsame Nutzung durch verschiedene Anwendungen ermöglicht, mit X.500 liegt ein internationaler Standard vor, der im Folgenden kurz umrissen werden soll, um die Nutzung zur Benutzerverwaltung zu erläutern [Klünter 2003].
Die in einem nach X.500 realisierten Verzeichnis gespeicherten Informationen, werden aus sicht des Anwenders hierarchisch, in Form eines Verzeichnisbaumes (Directory Information Tree) verwaltet, in Abbildung 30 wird ein solcher exemplarisch veranschaulicht. Die Einträge (Knoten und Blätter) in diesem Baum stellen Objekt dar, welche über verschiedene Eigenschaften verfügen. Hier abgelegte Objekte können z.B. Unternehmen, Personen eines Unternehmens oder auch Geräte in einem Netzwerk repräsentieren. Jedes Objekt verfügt über ein oder mehrere Attribute, über sogenannte Objektklassen wird definiert über welche Attribute ein Objekt verfügen kann, von welchem Typ diese sind und ob deren Vorhandensein Pflicht ist oder nicht. Ein Objekt kann hierbei mehreren Klassen zugeordnet sein. Es existieren

Standardklassen, mit denen häufig verwendete Objekt-Strukturen abgebildet werden können, zum Aufbau einer Benutzerverwaltung steht z.B. die Klasse „Person“ zur Verfügung[29]. Durch die Verwendung der standardisierten Klassen können diese Daten von unterschiedlichen Anwendungen genutzt werden.
Alle Objekte einer Hierarchieebene, also alle Kinder eines gemeinsamen Knotens, müssen anhand der Ausprägung ihrer Attribute unterscheidbar sein (Relative Distinguished Name, RDN), für Personen wird häufig der Name (Common Name, CN) verwendet. Über den RDN und den Pfad zu einem Objekt kann eine eindeutige Identifizierung vorgenommen werden, diese wird durch die RDNs der einzelnen Knoten von der Wurzel bis zum betrachteten Objekt , gebildet . Im gezeigten Beispiel ist der RDN der Person „CN=Klaus Mustermann“, die eindeutige Bezeichnung im Verzeichnisbaum, der Distinguished Name, ist „C=DE, O=BeispielFirma, OU=Vertrieb, CN=Klaus Mustermann“.

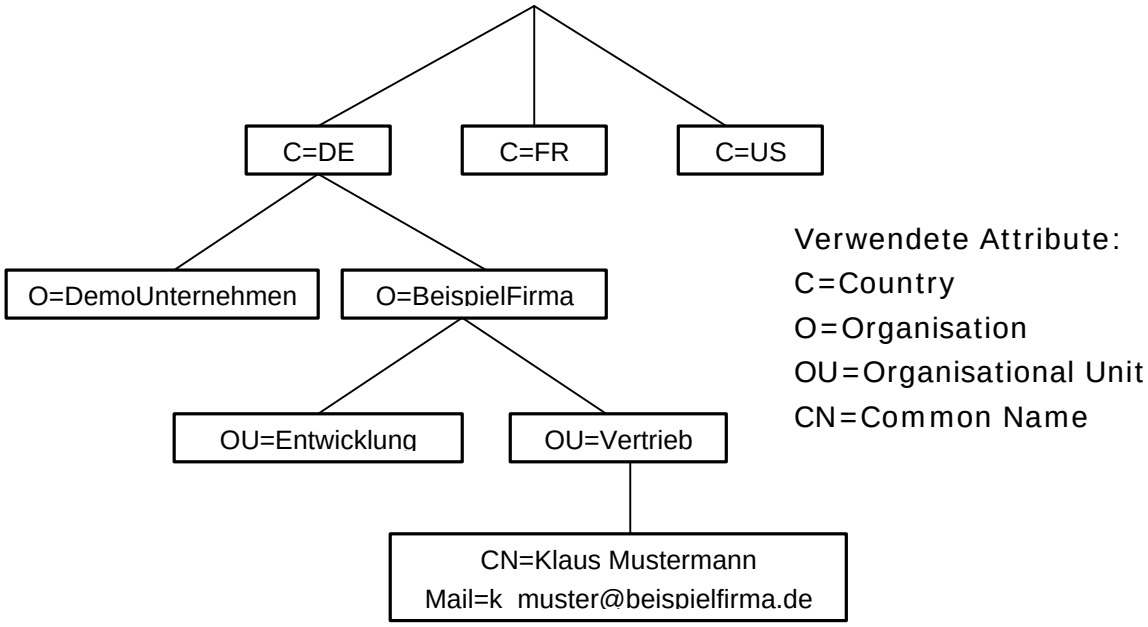


Abbildung 30 Auszug aus Verzeichnisbaum

[29] Für weitere Informationen zu Standardklassen sei auf RFC2256 „A Summary of the X.500 User Schema for use with LDAPv3“ oder RFC2798 „Definition of the inetOrgPerson LDAP Object Class“ verwiesen.

Um auf die Informationen eines nach X.500 organisierten Verzeichnisses zuzugreifen, wird im Standard auch ein Zugriffsprotokoll definiert, das Directory Access Protocol, DAP. Dieses deckt den sehr komplexen Funktionsumfang eines X.500 Directorys ab, wobei dieses auf dem ISO-Schichtenmodell aufsetzt und RPC-Mechanismen (Remote Procedure Call) zur Kommunikation nutzt. In der Praxis hat sich das auf den IP-Protokollen aufsetzende Lightweight Directory Protocol, LDAP durchgesetzt. Dieses Client-Server-Protokoll stellt die erforderlichen Operationen zum Zugriff auf den Verzeichnisbaum bereit, hierzu gehört das Erzeugen, Berabeiten oder Löschen von Objekte, ebenso Methoden zur Suche nach Objekten im Baum anhand ihrer Attribute.
Im Falle einer auf LDAP basierenden Benutzerverwaltung des AccessServers, würde die Komponente zur Realisierung der benötigten Funktionen im Umgang mit Benutzern als LDAP-Client agieren und die Anfragen (Benutzer anlegen, löschen, bearbeiten, suchen) an den LDAP-Server senden.

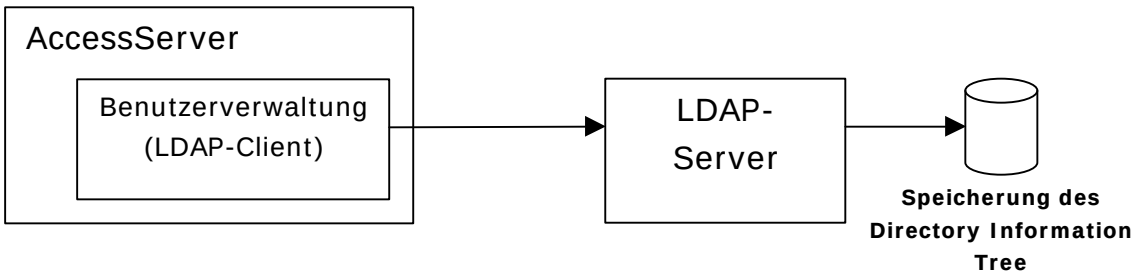


Abbildung 31 AccessServer Benutzerverwaltung mittels LDAP-Server

Die hier gegebenen Beschreibung von X.500 und LDAP umschreibt nur grob die gegebenen Möglichkeiten, für eine detaillierte Beschreibung sei auf die Spezifikation[30] und weiterführende Literatur verwiesen [LDAP].

7.3.3.2. Eigene Benutzerdatenbank

Neben der Verwaltung von Benutzern in einem Verzeichnisdienst ist ein verbreitetes Vorgehen das Speichern von Benutzerdaten in der gleichen (relationalen) Datenbank, welche auch die weiteren anwendungsrelevanten Daten enthält. Im Vergleich zu einer LDAP-Lösung geht hier die Flexibilität verloren, da die so gespeicherten Benutzer in der Regel nur von einer Anwendung, also dem AccessServer genutzt werden (können). Auf der anderen Seite bietet eine solche Lösung die Vorteile einer relationalen Datenbank, werden Operationen durchgeführt, welche auf Benutzer- und weitere Anwendungsdaten zugreifen, können diese in einer Transaktion durchgeführt werden. Ebenso kann die referentielle Integrität von zu Benutzern in Beziehung stehenden Daten sichergestellt werden.

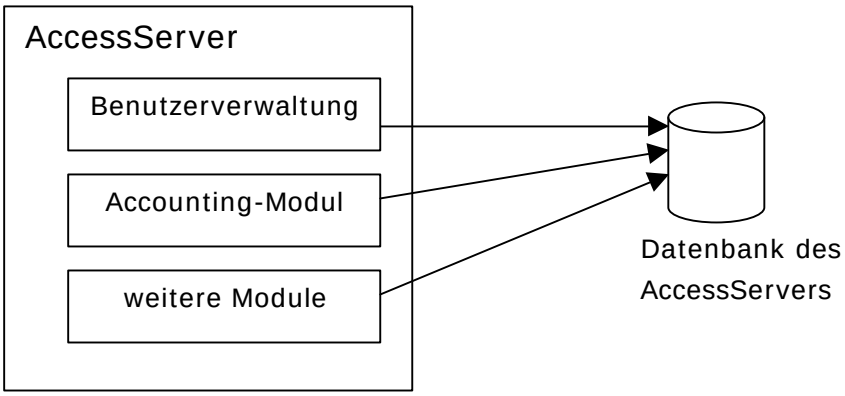


Abbildung 32 AccessServer Benutzerverwaltung in eigener Datenbank

[30] Die komplette Spezifikation von X.500 kann entgeldlich von der ISO bezogen werden (www.iso.org) und ist unter ISO/IEC9594-X zu finden. Die wichtigsten Spezifikationen für LDAP sind RFC 2251 bis 2256.

7.3.3.3. Realisierung

Die Realisierung der Benutzerverwaltung in Form einer Anbindung an einen LDAP-Server stellt sicherlich eine der flexibelsten Lösungen dar und ist von besonders großem Vorteil, wenn das System in eine Infrastruktur integriert wird, in der bereits eine Benutzerverwaltung mittels LDAP erfolgt. Die Realisierung der Benutzerverwaltung des Hotspot-Systems erfolgt aus Gründen der einfacheren bzw. schnelleren Umsetzung allerdings zunächst in Form einer eigenen Benutzerdatenbank des AccessServers. Beim Entwurf wird darauf geachtet, dass das vom AccessServer verwendete System zur Verwaltung von Benutzern austauschbar ist, dieses sollte sich dabei nicht auf das Verhalten anderer Komponenten auswirken. So kann die Implementierung einer LDAP-basierten Lösung zu einem späterem Zeitpunkt erfolgen.

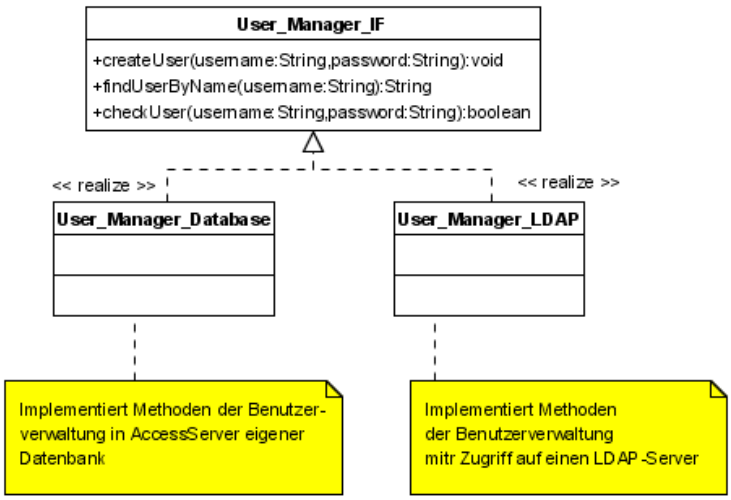


Abbildung 33 Klassendiagramm Benutzerverwaltung

Das Verhalten, welches von einer Benutzerverwaltung erwartet wird, wird in einem Interface definiert (User_Manager_IF). Die bereitgestellten Methoden ergeben sich hierbei aus der Analyse der Anwendungsfälle, bei welcher deutlich wurde, welche Module mit der Benutzerverwaltung interagieren und welche Operationen durchgeführt werden müssen (z.B. Anlegen eines Benutzers oder verifizieren der Login-Daten). Abhängig von der Art der Realisierung

der Benutzerverwaltung wird dieses Interface von konkreten Klassen implementiert, die Benutzerverwaltung in einer eigenen Datenbank z.B. von der Klasse User_Manager_Database. Weitere Varianten können so im Nachhinein hinzugefügt werden, welches Verfahren zum Einsatz kommt, ist für die restlichen Komponenten des AccessServers transparent.

7.3.4. Administration GUI

Zur Administration des Systems wird eine Web-Oberfläche bereitgestellt, die Bedienung erfolgt hier über bereitgestellte HTML-Seiten, zur Bedienung ist daher nur ein Web-Browser erforderlich. Es ist somit kein zusätzlicher Aufwand zur Verteilung von Client-Anwendungen erforderlich, ebenso entfällt das Verteilen von Updates, da die Oberfläche auf dem Server generiert wird und Änderungen sofort allen Nutzern bereitstehen. Sofern eine Netzwerkanbindung vorhanden ist, besteht keine örtliche Beschränkung beim Zugriff, dieser kann auch über das Internet erfolgen. Die Übertragung der Daten zwischen Server und Browser basiert auf HTTP, zur Absicherung der Verbindung kann hier in der Regel ohne Beeinträchtigung der Server-Implementierung auf HTTPS (SSL) gewechselt werden, um die Daten verschlüsselt zu übertragen.
Auch hier stellen J2EE-Applikation-Server entsprechende Mechanismen bereit, die das Erzeugen einer dynamischen Web-Oberflächen ermöglichen, diese kann so in der gleichen Laufzeitumgebung wie die restlichen Komponenten des AccessServers betrieben werden und auf diese zugreifen.
Zur Realisierung hat sich hier das Model-View-Cotroller (MVC) Muster bewährt, welches eine Trennung von Anwendungsdaten und deren Präsentation ermöglicht [SUN 2]. Der Controller verarbeitet die eingehende Anfrage (HTTP-Request) und sorgt für die Bereitstellung der erforderlichen fachlichen Daten, welche angezeigt bzw. manipuliert werden sollen, das Model (dieses sind z.B. Stammdaten der Nutzer des Hotspot-System). Um diese im Browser des Administrators zur Anzeige zu bringen, wird durch den

Controller der entsprechende View gewählt, dieser ist als JSP realisiert. Mit JSP steht in J2EE eine Skriptsprache zur Verfügung die sich auf die Präsentation von Anwendungsdaten (Model), z.B. in Form von HTML-Seiten, konzentriert.

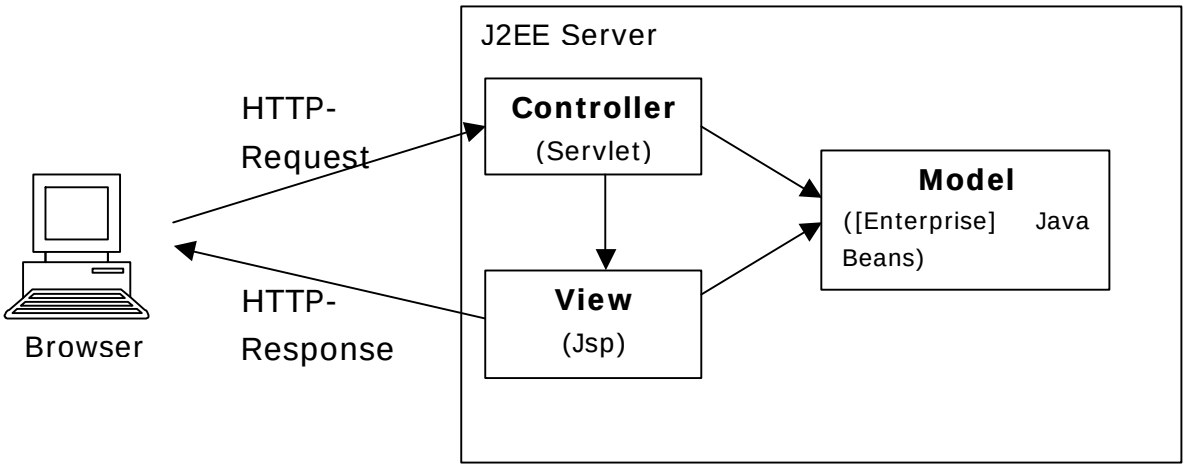


Abbildung 34 MVC in J2EE Application Server

Die Umsetzung dieses Muster ist kein Bestandteil von J2EE, sondern ist als Vorschlag basierend auf Erfahrungen in der Entwicklung von Benutzeroberflächen zu verstehen. Es existiert eine Vielzahl von Frameworks, die bei der Entwicklung von MVC-orientierten Oberflächen unterstützen, zu den bekanntesten (OpenSource-Lösungen) gehören z.B. Struts oder Turbine. Auf die Implementierung kann im Rahmen dieser Diplomarbeit nicht weiter eingegangen werden, weitere Informationen sind unter http://jakarta.apache.org/struts/ oder http://jakarta.apache.org/turbine/ zu finden.

7.3.5. Roaming

In den bisherigen Betrachtungen ist davon ausgegangen worden, das ein Nutzer, der über ein AccessGateway Zugang zum Internet erhält, im zuständigen AccessServer registriert wurde. Somit ist der Benutzer auf die Hotspots beschränkt, welche über diesen abgewickelt werden. Um diese Einschränkungen zu umgehen, wird an Lösungen gearbeitet, die eine betreiberübergreifende Abwicklung der Zugangsnutzung ermöglichen, dieses wird als Roaming bezeichnet. Bekannt ist dieses bereits aus dem Bereich des Mobilfunks: Verlässt man den Bereich, der vom Provider, dessen Kunde man ist, abgedeckt wird, kann auf die vorhandene Infrastruktur eines anderen Providers zugegriffen werden. Die Provider tauschen Informationen über diese Nutzung untereinander aus, die Abrechnung erfolgt über den Provider, bei dem man Kunde ist (so kann das Mobiltelefon auch im Ausland genutzt werden, entsprechende Roaming-Verträge zwischen den Providern vorausgesetzt).

7.3.5.1. Greenspot

Dieses auf WLAN-Zugänge zu übertragen hat sich (in Deutschland) das eco-Forum (Electronic Commerce Forum – Verband der deutschen Internetwirtschaft e.V.) mit dem Greenspot-Projekt zum Ziel gesetzt [Greenspot].
Die Spezifizierung der Greenspot-Lösung ist zum gegenwärtigen Zeitpunkt noch nicht vollständig abgeschlossen, die Lösungsansätze sollen im Folgenden beschrieben werden und eine Übertragung auf die im Rahmen der Diplomarbeit erarbeitete Lösung gezeigt werden.

Bei Greenspot wird von einem Szenario ausgegangen, in dem folgende Rollen unterschieden werden:

WISP-Operator

Der WISP-Oparator stellt den Internetzugang am Hotspot zur Verfügung. Der Operator ist vertraglich an einen WISP-Concentrator gebunden, welcher für Authentifizierung der Nutzer sowie für das Clearing der aus der Nutzung entstandenen Abrechnung verantwortlich ist. Übertragen auf die im Rahmen der Diplomarbeit erarbeitete Lösung entspricht der WISP-Operator dem AccessGateway (Die Hardware wird im Greenspot-Sprachgebrauch „Public Access Control Gateway“ genannt).

WISP-Concentrator

Der WISP-Concentrator wird von den WISP-Operatoren zum Zwecke der Authentifizierung und des Accountings kontaktiert. Wird der Benutzer, auf den sich diese Aktionen beziehen, nicht von diesem WISP-Concentrator, sondern von einem andern Service-Provider verwaltet, werden die Anfragen an einen Greenspot-Server weitergereicht. Der Datenaustausch erfolgt mittels RADIUS. Der WISP-Concentrator entspricht dem AccessServer unserer Lösung.

Greenspot

Greenspot übernimmt die Vermittlerrolle zwischen den einzelnen Parteien.

Service-Provider

Die Roaming-Nutzer sind Kunden der Service-Provider, diese haben die Hoheit über die Preisgestaltung und rechnen die Zugangsnutzung gegenüber ihren Kunde ab (Kandidaten für diese Rolle sind Unternehmen wie Acor, Telekom oder AOL).

Der Anwendungsfall des sich anmeldenden Benutzers, auf die Greenspot-Architektur abgebildet, läuft wie in Abbildung 35 gezeigt ab:

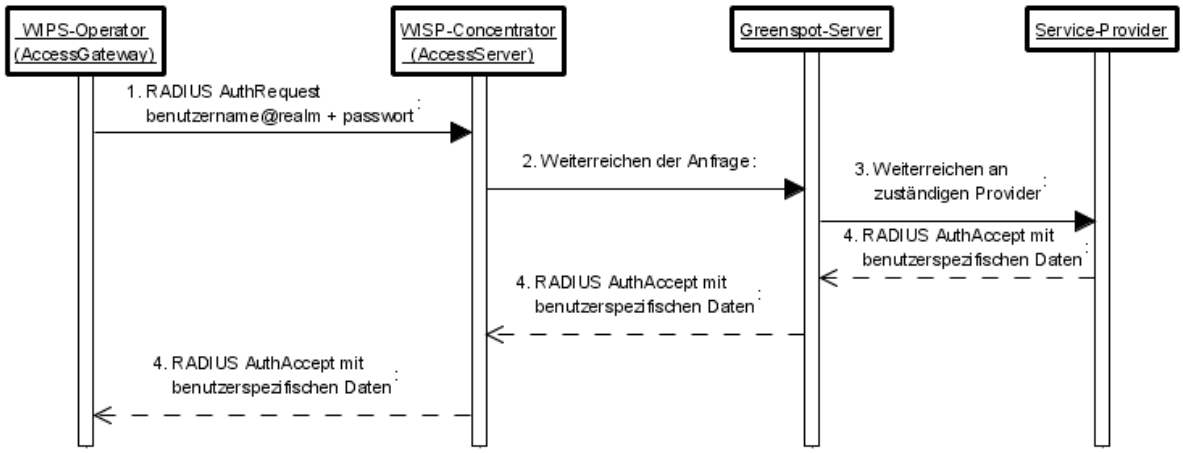


Abbildung 35 Nutzer-Authentifizierung mit Greenspot

1. Der Benutzer meldet sich zur Internetnutzung beim WISP-Operator an, zusätzlich zu Benutzernamen und Passwort wird noch der Realm angegeben, welcher den Service-Provider identifiziert, bei dem der Benutzer Kunde ist. Dieses wird als RADIUS „AuthRequest“-Paket an den WISP-Concentrator gesendet.
2. Der WISP sendet die Anfrage, sofern der Benutzer nicht direkt beim Concentrator authentifiziert werden kann, an einen Greenspot-Server weiter.
3. Der Greenspot-Server kann anhand des Realms den zuständigen Service-Provider ermitteln und sendet die Anfrage an diesen weiter.
4. Der Service-Provider kann die Authentifizierung der Benutzerangaben vornehmen, war diese erfolgreich, wird eine AuthAccept-Nachricht an den WISP-Operator zurückgereicht, dieser kann jetzt den Zugang bereitstellen.

Beim Accounting wird ähnlich verfahren, die Zugangsnutzung wird beim WISP-Operator erfasst und ebenso an die Greenspot-Server weitergeleitet (RADIUS AccountingRequest). Im Greenspot Clearinghouse werden diese Daten aufbereitet (Usage Dateil Records) und zur Abrechnung der Kunden durch die Service-Provider bzw. der einzelnen Parteien untereinander genutzt.

7.3.5.2. Umsetzung des Greenspot-Ansatzes

Die im Greenspot definierten Aufgaben des WISP-Operators und WISP-Concentrators entsprechen dem AccessGateway bzw. AccessServer der hier erarbeiteten Lösung. Sollte sich das Roaming-Verfahren durchsetzen, muss eine Integration in dieses Szenario möglich sein. In der beschriebenen Zusammenarbeit der einzelnen Parteien bei der Authentifizierung des Benutzers erfolgt eine RADIUS-Authentifizierung über mehrere Zwischenschritte, wobei diese als Proxy dienen. Dieses Verfahren wird in den AccessServer übernommen, allerdings unter Beibehaltung des entwickelten Protokolls zwischen AccessGateway und Server, der AccessServer übersetzt die Nachrichten in ein äquivalentes RADIUS-Paket und sendet dieses an den Greenspot-Server weiter. Auf Seite des AccessGateways ist somit lediglich eine Erweiterung um die Angabe des Service-Provider-Realms erforderlich, weitere Anpassungen entfallen.
Wie in Kapitel 7.3.2.4 beschrieben werden die Nachrichten des AccessGateways serverseitig in Protocol_Command-Klassen transferiert, welche die Anfrage behandeln (Abbildung 28 und Abbildung 29). Für den Greenspot-Einsatz werden zusätzlich Klassen implementiert (z.B. ProtocolCommand_AuhtRequest_Greenspot), diese greifen nicht auf die Komponenten des AccesServers zu, sondern operieren als RADIUS-Client und senden ein entsprechendes RADIUS-Paket an den Greenspot-Server. Das Ergebnis dieser Anfrage (z.B. RADIUS AuthAccept) wird an das entsprechende ProtocolCommand umgewandelt und an das AccessGateway zurückgegeben.

Da die Instanzeierung über eine Factory gelöst ist, bleibt der restliche Server-Implementierung davon unberührt. Die ProtocolCommandFactory kann z.B. anhand des Vorhandenseins einer Realm-Angabe entscheiden, welche ProtocolCommand-Instanz zu erzeugen ist.

8. Resümee

Die Arbeit hatte zum Ziel die Planung und Umsetzung einer sicheren WLAN-Lösung für kommerzielle Zwecke aufzuzeigen. Im Verlauf der Anforderungsanalyse ist dann herausgestellt worden, dass man im Wesentlichen nur zwei Komponenten braucht, um ein fast universell einsetzbares WLAN-System zu erstellen: eine Lösung vor Ort (auch AccessGateway), die einen Teil der Logik übernimmt und eine zentrale Serverkomponente, die die Lösungen vor Ort bedient und Anbindungsmöglichkeiten für Sekundärsysteme bereitstellt. Damit das System den kommerziellen Ansprüchen gerecht wird, sind darüber hinaus eine Reihe von Zusatzfunktionalitäten geschaffen worden, die den Nutzen für die Kunden erhöhen.
Ein konkretes Einsatzszenario:
Jemand betreibt als WISP (Wireless Internet Service Providern) eine Serverkomponente und platziert an möglichst vielen interessanten Lokationen (Restaurants, Bars, Hotels, Marinas, Campingplätze ….) die „Lösung vor Ort“. Die Besitzer der Lokationen betreiben diese an ihrer DSL-Leitung, bieten ihren Kunden einen Mehrwert an und werden am Umsatz beteiligt.
Im Folgenden sollen die Anforderungen an das kommerzielle System kurz mit deren Realisierungen zusammengebracht werden:

8.1. Wurden die Anforderungen erfüllt ?

8.1.1. Sicherheit

Die von uns im HotSpot-Bereich gebotene Sicherheit ist aus reiner Sicherheitssicht keine perfekte Lösung, da das PPTP- Protokoll durchaus als angreifbar gilt. Doch hier mußte ein Kompromiss mit der einfachen Bedienbarkeit eingegangen werden. Einen VPN – Tunnel einzurichten, kann den meisten Nutzern noch zugetraut werden, zumal auf der „Lösung vor Ort“ ein Programm zum herunterladen hinterlegt ist, das eben diese Verbindung für Windows automatisch einrichtet. Was dem durchschnittlichen Nutzer hingegen nicht zugemutet werden kann, ist das Einrichten von IP-SEC – Strecken, die mittels Zertifikaten gesichert sind.

Eine aus rein sicherheitstechnischer Sicht sehr zu empfehlende Variante, aber noch nichts für den Massenmarkt. Auf dem Massenmarkt ist es wichtig, dass für den Nutzer nur sehr wenig zusätzlicher Aufwand nötig ist, um Sicherheit zu gewährleisten. Anders ist dies bei Systemen für geschlossene Nutzergruppen wie etwa dem „Office-Bereich“, wo ein Administrator die Grundinstallation vornehmen kann. In unserer Lösung für diesen Bereich wird das Sicherheitsmodul „PPTP“ einfach durch das Sicherheitsmodul „IP-SEC“ ersetzt.

8.1.2. Einfachheit der Bedienung

Um die einfache Bedienbarkeit des Systems zu zeigen, soll hier kurz der Bedienablauf für den Nutzer dargelegt werden.
Sobald der Nutzer sich in Reichweite eines AccessGateways begibt, assoziiert sich ggf. seine WLAN-Karte mit dem AG. Bei einem Versuch im Internet zu surfen wird er auf Loginseite umgeleitet, wo er sich mit seinen Zugangsdatgen sofort per WEB-Login einloggen kann oder alternativ ein Installationsprogramm für eine sichere Verbindung mittels VPN downloaden und installieren kann. Hier kann er jetzt seine Zugangsdaten sofort eingeben und anschließend surfen oder er nutzt eine Verknüpfung auf dem Desktop, die nach dem Öffnen ebenfalls die Eingabe der Zugangsdaten ermöglicht. Ein einfacher klick auf „Verbinden“ initiiert dann den für den Nutzer transparenten Prozess aus Authentifizierung und Aufbau des Sicherheitstunnels. Ein Browser öffnet sich und der Nutzer kann sicher surfen. Ein weiterer Vorteil dieses nur einmal zu installierenden Programms ist die Speichermöglichkeit der Zugangsdaten. Von nun an reicht dem Nutzer beim Erreichen der HotSpot-Zone ein einfaches Klicken auf „Verbinden“ und alles, selbst das Öffnen eines Browsers, funktioniert automatisch.

8.1.3. Flexibilität/Erweiterbarkeit

Für die unterschiedlichen Einsatzszenarien, bestehen im Hinblick auf die Anbindung an Sekundärsysteme extrem unterschiedliche Anforderungen. Die Bandbreite der denkbaren Möglichkeiten reicht hier von den gezeigten Sekundärsystemen für Hotspots (Roaming, Accounting) bis zu dem Anbinden von firmen- und branchenspezifischen Softwaresystemen und bestehenden Nutzerverwaltungen. Alle diese denkbaren Ansätze zu betrachten würde an dieser Stelle den Rahmen der Arbeit sprengen, denn sie betreffen nicht das Kernthema.
Es wurde anhand des Beispieles „HotSpot“ gezeigt, dass die Architektur flexibel genug ist, weitere Systeme zu integrieren und eben diese Flexibilität ist es ja, die alle späteren Erweiterungen und Anpassungen erst ermöglicht. Ein weiterer Pluspunkt unter diesem Gesichtspunkt ist die Verwendung der Programmiersprache Java und eines Applikationsservers. Eine Kombination, die größtmögliche Flexibilität gewährleistet.

8.1.4. Kommerzieller Einsatz

Um die gebotenen Leistungen und den Komfort für den Betreiber und die Möglichkeiten für die Nutzer weiter zu steigern, haben wir noch einige Funktionalitäten hinzugenommen, die nicht direkt als notwendige Anforderungen herausgestellt wurden, aber dennoch sehr
zur Abrundung des Systems beitragen.
Es ist sinnvoll, ein HotSpot–System so zu konzipieren, dass der Aufwand vor Ort so minimal wie möglich ist. Denn gerade Besuche bei allen Außenstellen sind sehr zeit- und kostenintensiv. Deshalb wurde bei der Hardware darauf geachtet, dass keine beweglichen Teile im Einsatz sind, das System fußt also auf einer lüfterfreien CPU und einer CompaqFlash–Karte als Festspeicher. Die Hardware wird vorkonfiguriert ausgeliefert, so dass der Aufbau vor Ort von jedem Laien innerhalb von 5 Minuten vorgenommen werden kann. Es ist lediglich notwendig das Strom- und das DSL-Kabel einzustecken und das Gerät ist betriebsbereit. Im Fehlerfall kann so einfach eine Ersatzhardware per Paketdienst überbracht und die alte abgeholt werden, auch hier ist kein Personaleinsatz vor Ort nötig. Als Letztes sind die mit Sicherheit von Zeit zu Zeit notwendigen Software-

Updates zu nennen, auch diese können, wie bereits beschrieben, von zentraler Stelle auf die Boxen eingespielt werden. Im Normalfall kommt der komplette Betrieb des Systems also ohne Einsatzkräfte vor Ort aus.
Weitere Funktionalitäten sollen den Nutzen für den Kunden weiter erhöhen, so ist die Hardware mit drei Ethernetports ausgestattet, einen für den DSL-Zugang, einen für den PC oder das Netzwerk des Betreibers (einfache Routerfunktion), denn dieser möchte ja nicht für die Benutzung seiner eigenen DSL-Leitung bezahlen, und einen, der zur Vergrößerung der Abdeckung dient. Hier können zusätzliche einfache Accesspoints ohne weitere Logik angeschlossen werden, da alle von der Hardware vor Ort versorgt werden, ist zwischen ihnen ein örtliches Roaming aktiv und auch die Authentifizierung und die Sicherheitsmerkmale unterscheiden sich nicht von der Basislösung. Es ist auch möglich, diesen Port nicht dazu zu nutzen, die Abdeckung zu vergrößern, sondern um den Dienst „Internetbereitstellung“ auch mittels anderer Verfahren anzubieten. So kann zum Beispiel eine handelsübliche Bluetooth-Basisstation angeschlossen werden, um auch alle PDA – Besitzer als potentielle Kunden zu gewinnen.
Da die Hardware wie erwähnt auch als Router arbeitet, war es nur sinnvoll auch eine Firewall mit in die Lösung zu integrieren. So sind Kunden und Betreiber zusätzlich vor Angriffen aus dem Internet geschützt.

8.1.5. Skalierbarkeit

Als letzte Anforderung, die herausgestellt wurde, ist noch eine gute Skalierbarkeit der Lösung zu betrachten. Was bedeutet, dass es möglich sein muß, sowohl die Serverkomponente als auch die „Lösung vor Ort“ ohne große Probleme an schwankende Leistungsanforderungen anzupassen.
Im vorgestellten System beruht die Serverkomponente auf Java unter Verwendung eines Applikationsservers. Dieser bietet unter anderem die Möglichkeit, das System zu „clustern“ und somit je nach Bedarf, die Rechenleistung zu erhöhen.
Auf Seiten der Hardware vor Ort wird, wie beschrieben, mit einem Linuxderivat und einer darauf basierenden Software gearbeitet. Auch hier ist die Lösung ohne Probleme auf größeren Rechnern lauffähig, wenn es an einigen Standorten zu Leistungsengpässen kommen sollte. Da zudem

der einzig rechenintensive Vorgang, die Verschlüsselung, auf die Außenstellen verlagert wurde, entsteht auch beim Betrieb von sehr vielen Außenstellen über einen Server (10000+) kein Engpass, die Hardware vor Ort muss dann nur den jeweiligen Gegebenheiten angepasst werden. Damit sehen wir auch das letzte Kriterium als erfüllt an.

8.2. Fazit

Als Ganzes stellt unsere Lösung einen guten Kompromiss aus allen gewünschten Anforderungen dar, der zugunsten kommerzieller Aspekte gewichtet wurde.
So kommt weder das Leistungsspektrum zu kurz, noch ist das System für die Nutzer kompliziert im Umgang. Der Spagat zwischen einem sicheren und gleichzeitig unkomplizierten WLAN-System ist gelungen, soweit es die heutigen Möglichkeiten zulassen.
Der modulare Aufbau des Systems und die Schaffung klarer Schnittstellen und Protokolle erlaubte uns während der Implementierung mit hoher Flexibilität Erweitrungen vorzunehmen und Aufgaben zu teilen. Zudem können viele Module der Lösung vor Ort und der Serverkomponente für die Realisierung anderer WLAN- Systeme „Eins zu Eins“ wieder verwendet werden, sei es für den Einsatz in großen oder kleinen Bürolösungen, aber auch halböffentlichen Gebäudekomplexen. Die Entwicklungsarbeit wurde also einmal getätigt und steht jetzt für diverse Anwendungen zur Verfügung. Ein rundes System, das für zukünftige Erweiterungen bereit ist.

8.3. Ausblicke

Der weltweite WLAN-Markt, befindet sich derzeit innerhalb einer rasanten Entwicklungsphase, die von allen großen Teilnehmern gemeinsam vorangetrieben wird. Da sind auf der einen Seite die Hardwarehersteller, die sich immer mehr auf die Produktion von Standardkomponenten verlegen, da die Nachfrage dafür ständig steigt. Da sind auch die Hersteller von Notebooks, PDA's und Telefonen, die beginnen diese Technologie „ab Werk" in ihre Geräte zu integrieren. Des weiteren sind da die Netzbetreiber, die bisher noch eher zögerlich anfangen, eine Infrastruktur zu schaffen, da die meisten zunächst abwarten, ob sich das System wirklich durchsetzt, und die kleineren und mittleren Firmen, die in WLAN eine Zukunftschance sehen, individuelle Lösungen schaffen und auf den großen Durchbruch hoffen, zuletzt sind die Standardisierungsgremien zu nennen, die dem Ruf nach mehr Geschwindigkeit, mehr Sicherheit und größerer Interoperabilität versuchen nachzukommen. Und natürlich die Endkunden, die all dies in Zukunft refinanzieren sollen.
Die Affinität zur Technik und zur mobilen Kommunikation ist in den letzten Jahren ständig gestiegen und wenn dieser Trend anhält, was zu erwarten ist, hat WLAN eine gute Chance im beginnenden Kommunikationszeitalter eine interessante Rolle zu spielen. Welche Systeme sich allerdings letztendlich in welchem Zusammenspiel durchsetzen werden, wer diese betreibt und wer die Endkunden betreut steht heute noch in den Sternen. Als sicher anzusehen ist lediglich, dass dem Internet wohl die Zukunft gehören wird, welche Systeme das Internet dann allerdings zu den Endkunden transportieren, bleibt abzuwarten.
Der WLAN-Markt befindet sich noch in einer so frühen Phase, dass Prognosen und Zukunftsausblicke sehr schwierig sind. Derzeit trifft das hier vorgestellte System die Anforderungen des Marktes, ob es in Zukunft allerdings durch neue Hardwarestandards in Punkto Sicherheit und durch Lösungen großer Firmen in Punkto Management und Verwaltung überholt wird bleibt ebenfalls abzuwarten.
Wenn allein die Technik darüber entscheiden würde, ob das System ein Erfolg wird, hätten wir aus unserer Sicht gute Chancen, leider ist es in der Realität viel wichtiger, ein System gut zu vermarkten. Und der Standardweg etwas gut zu vermarkten läuft meist über große Anfangsinvestitionen für Werbung und Vertrieb.

Ein letzter Gedanke bei allen Zukunftsausblicken sollte stets der Vorstellung gewidmet sein, was man an der Arbeit anders gemacht hätte, wenn sie in drei bis fünf Jahren geschrieben worden wäre. Die ehrliche Antwort ist, wir wissen es nicht, da die dann zu erfüllenden Anforderungen zum jetzigen Zeitpunkt noch nicht absehbar sind. Absehbar ist für uns nur, dass unser System die jetzigen Anforderungen bedient und durch seine modulare Struktur genügend Flexibilität aufweist, mit zukünftigen Anforderungen zurechtzukommen.

Abbildungsverzeichnis

Abbildung 1 MIT-2000 36
Abbildung 2 Baugröße Bluetooth 39
Abbildung 3 Einsatzgebiete mobiler Übertragungstechniken 42
Abbildung 4 Vergleich OFDM-FDM 53
Abbildung 5 Frequenzeinteilung der Funkkanäle bei 802.11b 57
Abbildung 6 Bandbreiteneinbußen 60
Abbildung 7 Sniffing, Mitlesen von Paketen 72
Abbildung 8 Spoofing 73
Abbildung 9 Man-in-the-middle Angrif 74
Abbildung 10 Transport mode 87
Abbildung 11 a) Tunnel mode Gateway – Gateway 89
Abbildung 11 b) Tunnel mode Host – Gateway 89
Abbildung 12 AH – Header Daten 90
Abbildung 13 SSL/TLS Position im Protokoll-Stack (Record Protokoll) 93
Abbildung 14 SSL-Handshake 94
Abbildung 15 Ablauf Kerberos Authentifizierung 97
Abbildung 16 Firewallgesichertes Netzwerk 101
Abbildung 17 Proxy-Gateway 103
Abbildung 18 Komponenten des Hotspotsystems 122
Abbildung 19 Module AccessGateway 125
Abbildung 20 Use-Case-Diagramm AccessGateway 127
Abbildung 21 Klassendiagramm Kommunikation AccessGateway 132
Abbildung 22 Ablauf Anwendungsfall Authentifizierung / Accounting 155
Abbildung 23 Ablauf Anwendungsfall Administration, Abruf der Nutzungsdaten eines Benutzers 156
Abbildung 24 Komponenten des AccessServers 157
Abbildung 25 Struktur Wählzugang zum Provider / Firmennetz 160
Abbildung 26 RADIUS Authentifizierung 163
Abbildung 27 RADIUS – Accountig 165
Abbildung 28 Klassendiagramm Protokollverarbeitung 169
Abbildung 29 Ablauf Protokollverarbeitung 169
Abbildung 30 Auszug aus Verzeichnisbaum 173
Abbildung 31 AccessServer Benutzerverwaltung mittels LDAP-Server 174
Abbildung 32 AccessServer Benutzerverwaltung in eigener Datenbank 175
Abbildung 33 Klassendiagramm Benutzerverwaltung 176
Abbildung 34 MVC in J2EE Application Server 178
Abbildung 35 Nutzer-Authentifizierung mit Greenspot 180

Literaturverzeichnis

[BSI 1992] Bundesamt für Sicherheit in der Informationstechnik (BSI):
IT-Sicherheitshandbuch, Handbuch für die sichere Anwendung der Informationstechnik
Version 1.0: BSI 1992

[CCC1] „Chaos Computer Club“ Hanau:
DSSS
https://www.ccc-hanau.de/~jensb/wavelan/dsss.html
Stand:17.08.03

[CCC2] „Chaos Computer Club“ Hanau:
FHSS
https://www.ccc-hanau.de/~jensb/wavelan/fhss.html
Stand: 17.08.03

[DAFU] DAFU – Datenfunk:
DSSS
http://www.dafu.de/rechts/dsss.html
Stand:15.08.03

[EAP] IETF RFC 2284, Larry Blunk John Vollbrecht
PPP Extensible Authentication Protocol (EAP)
Stand: März 1998

[EAP-TLS] IETF RFC 2716, Bernard Aboba, Dan Simon
PPP EAP TLS Authentication Protocol
Stand: October 1999

[eco] Verbandes der deutschen Internetwirtschaft e.V., ECO:
Greenspot
http://www.eco.de/servlet/PB/menu/1185128_l1/index.html
Stand:12.12.03

[Eisi] Jochen Eisinger, University of Freiburg
Exploiting known security holes in Microsoft's
PPTP Authentication Extensions (MS-CHAPv2)
Stand: 23.7.2001

[Gamma 1994] Erich Gamma, Richard Helm, Ralph E. Johnson, John Vlissides:

Design Patterns: Elements of Reusable Object-Oriented Software
1.Auflage: Addison-Wesley Verlag, 1994

[Greenspot] Verband der deutschen Internetwirtschaft, AK WLAN, AG Roaming:

Greenspot WLAN Roaming
http://www.eco.de/servlet/PB/show/1206439/GS-WhitePaper-030506.pdf
Stand: 5.1.2004

[GSM-World] GSM-World:

Infoportal zum Thema GSM und mobile Techniken
http://www.gsmworld.com/technology/glossary.shtml
Stand:13.06.03

[Hill] Jürgen Hill:

Computerwoche, Wie schützt man das eigene WLAN?
Stand: 15.01.2003

[Hübner 2003] Prof. Dr.-Ing. Martin Hübner:

IT-Sicherheit, Kapitel 4 Sicherheitsmaßnahmen in Betriebsystemen
Hamburg, Hochschule für angewandte Wissenschaften, 2003

[IEEE802.11] IEEE Standard 802.11

IEEE Standard for 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
Stand: 1999

[IEEE802.1x] IEEE Standard 802.1x

IEEE Standard for Local and metropolitan area networks – Port-Based
Network Access Control

Stand: Juni 2001

[INTN] Interlink Networks, Inc.
EAP Methods forWireless Authentication
Stand: 2.4.2003

[IZT] IZT Institut für Zukunftsstudien und Technologiebewertung, SFZ Sekretariat für Zukunftsforschung, IAT Institut Arbeit und Technik:
Entwicklung und zukünftige Bedeutung mobiler Multimediadienste
Werkstattbericht 49, Berlin, Dezember 2001

[Klünter, Laser 2003] Dieter Klünter, Jochen Laser:
LDAP verstehen, OpenLDAP einsetzen
1. Auflage, Heidelberg: dpunkt.Verlag GmbH, 2003

[KNIG] Eric Knight, C.I.S.S.P.
Computer Vulnerabilities
Stand: 8.3.2000, Revision 4

[L2TP1] Phoram Mehta, Trabon Solutions
Secure Remote Access With L2TP
Stand: 04 June, 2002 auf ITsecurity.com

[METH] Dr. Paul Goransson, President, Meetinghouse, Inc.
802.11… A Standard for the Present and Future
Stand: 1.2.2003

[MIT1] The MIT Kerberos Team:
Kerberos: The Network Authentication Protocol"
Massachusetts institutes of technology
http://web.mit.edu/kerberos/
Stand: 20.12.2003

[MS1] Microsoft Corporation
Step-by-Step Guide for Setting Up Secure Wireless Access in a Test Lab
Stand: Mai 2003

[MS2] Microsoft Corporation
Virtual Private Networking in Windows 2000: An Overview
White Paper

[PPTP1] Kory Hamzeh, G. Singh Pall, William Verthein, Jeff Taarud, W. Andrew Little:
Point-to-Point Tunneling Protocol—PPTP
draft-ietf-pppext-pptp-00.txt
Stand: Juni 1996, abgelaufen

[PPTP2] Bruce Schneier, Mudge, David Wagner:
Cryptanalysis of Microsoft's PPTP Authentication Extensions (MS-CHAPv2)
Stand: 19.10.1999

[Raepple 1998] Martin Raepple:
Sicherheitskonzepte für das Internet
1. Auflage, Heidelberg: dpunkt.Verlag GmbH, 1998

[RFC1510] Network Working Group:
RFC 1510 T,he Kerberos Network Authentication Service (V5)
http://www.ietf.org/rfc/rfc1510.txt
Stand: 5.1.2004

[RFC 2865] Network Working Group:
RFC 2865, Remote Authentication Dial In User Service (RADIUS)
http://www.ietf.org/rfc/rfc2865.txt
Stand: 5.1.2004

[RFC 2866] Network Working Group:
RFC 2866, RADIUS Accounting
http://www.ietf.org/rfc/rfc2866.txt
Stand: 5.1.2004

[RFC 2402] Network Working Group:
RFC 2402, IP Authentication Header
http://www.ietf.org/rfc/rfc2402.txt
Stand: 5.1.2004

[RFC 2406] Network Working Group:
RFC 2406, IP Encapsulating Security Payload (ESP)
http://www.ietf.org/rfc/rfc2406.txt
Stand: 5.1.2004

[RFC 2408] Network Working Group:
RFC 2408, Internet Security Association and Key Management Protocol (ISAKMP)
http://www.ietf.org/rfc/rfc2408.txt
Stand: 5.1.2004

[RFC 2409] Network Working Group:
RFC 2409, The Internet Key Exchange (IKE)
http://www.ietf.org/rfc/rfc2409.txt
Stand: 5.1.2004

[Schneier 1996] Bruce Schneier, David Wagner:
Analysis of the SSL 3.0 Protocol
http://www.schneier.com/paper-ssl-revised.pdf
Stand: 10.12.2003

[Schneier 1999] Bruce Schneier, Niels Ferguson:
A Cryptographic Evaluation of IPSec
Counterpane Internet Security, Inc., 1999
http://www.schneier.com/paper-ipsec.pdf
Stand: 11.12.2003

[Some] Nicko van Someren, nCipher Ltd
The risks of short RSA keys for secure communications using SSL
Stand: 22.4.2002 auf ITsecurity.com

[Storz] Jakob Storz:
Bluetooth
Seminararbeit AIS, SS 2002, Hochschule für angewandte Wissenschaften Hamburg
http://www.informatik.fh-hamburg.de/~ais/ss2002/abstr/abstr.html
Stand: 15.10.2003

[SUN 1] Sun Microsystems, Inc:

Java 2 Platform Enterprise Edition Specification, v1.4
Final Release, Santa Clara, California USA: Sun Microsystems
http://java.sun.com/j2ee/j2ee-1_4-fr-spec.pdf
Stand: 24.11.2003

[SUN 2] Sun Microsystems, Inc:
Guidelines, Designing Enterprise Applications with the J2EE Platform
Sun Microsystems, Inc
http://java.sun.com/blueprints/guidelines/designing_enterprise_applications/
Stand: 14.12.2003

[SUN 3] Stephanie Bodoff:
Java Servlet Technology
Sun Microsystems, Inc
http://java.sun.com/j2ee/tutorial/1_3-fcs/doc/Servlets.html
Stand: 21.12.2003

[Tanenbaum] Andrew S. Tanenbaum:
Computernetzwerke
3. redigierte Auflage: Pearson Education Deutschland GmbH, 2000

[TLS] IETF RFC 2246, Tim Dierks, Christopher Allen
The TLS Protocol Version 1.0
Stand: Januar 1999

[TOM1] Tom's Hardware:
Grundlagen: Drahtlose Netzwerke
http://www.de.tomshardware.com/network/20030310/wlan-09.html
Stand:10.06.03

[UMTS-Report] UMTS-Report:
Infoportal rund um das Thema UMTS
http://www.umts-report.com
Stand:13.06.03

[UNI Kl] TU Kaiserslautern, Fachbereich Nachrichtentechnik:
Orthogonal Frequency Division Multiplexing
http://nt.eit.uni-kl.de/wavelet/ofdm.html

Stand: 25.08.03

[Virnich] Dr. –Ing. Martin H. Virnich:
WLAN-Anwendungen für „HotSpots“
http://www.baubiologie.net/docs/wlan1.html
Stand: 20.11.03

[Weiser] Marc Weiser:
Ubiquitous Computing
http://www.ubiq.com/hypertext/weiser/UbiHome.html
Stand: 12.12.03

[WiFi1] Wi-Fi Alliance
Enterprise Solutions for Wireless LAN Security
Stand: 6.2.2003

[WiFi2] Wi-Fi Alliance
Securing Wi-Fi Wireless Networks with Today's Technologies
Stand: 6.2.2003

[WiFi3] Wi-Fi Alliance
Wi-Fi Protected Access:
Strong, standards-based, interoperable security for today's Wi-Fi networks
Stand: 29.4.2003

[WiFi4] Wi-Fi Alliance
Wi-Fi Protected Access Web Cast
Stand: 11.6.2003

[WiFi5] Wi-Fi Alliance
Wi-Fi Protected Access:
Strong, standards-based, interoperable security for today's Wi-Fi networks
Stand: 29.4.2003

[WiFi6] David Cohen, Wi-Fi Alliance
Networld + Interop
Stand: 29.4.2003

Versicherung der Selbständigkeit

Hiermit versichern wir, dass wir die vorliegende Arbeit im Sinne der Prüfungsordnung Technische Informatik PO 98 nach §24 (5) ohne fremde Hilfe selbständig verfasst und nur die angegebenen Hilfsmittel verwendet haben.

Die Kapitel 1,2,3,4,5 und 8 wurden von Patrick Postel bearbeitet.
Die Kapitel 6.1, 6.2, 6.3.4, 6.3.5, 6.3.6, 6.3.7 und 7.3 wurden von Sebastian Schünemann bearbeitet.
Die Kapitel 6.3.1, 6.3.2, 6.3.3, 6.4, 6.5, 7.1 und 7.2 wurden von Jaroslaw Zdrzalek bearbeitet.

Hamburg den 29.01.04

(Patrick Postel)

(Sebastian Schünemann)

(Jaroslaw Zdrzalek)