Projektdokumentation

Planung und Kalkulation eines Wireless-LAN

Auszubildender:
René Fischer
xxxxxxx@soft-research.de

Prüf-Nr.: 20816
Azub.-Identnr.: 3252023

Ausbildungsberuf:
IT – Systemkaufmann

Ausbildungsbetrieb:
SOFT-RESEARCH GmbH & Co. KG
Kirchenstrasse 68
81675 München

Projektbetreuer:
Michael Just
xxxxx@soft-research.de

Inhaltsverzeichnis

1. Thema 4

2. Problemstellung 4
- 2.1. Ermittlung des Ist-Zustands 4
- 2.2. Ermittlung des Soll-Zustands 5
  - 2.2.1. Vorteile eines Wireless-LAN 5
  - 2.2.2. Vorurteile, Nachteile und Gefahren des Wireless-LAN 5
  - 2.2.3. Zielsetzungen für das geplante Wireless-LAN 6

3. Planung 6
- 3.1.Gespräch mit dem Systemadministrator 6
  - 3.1.1. Technische Vorraussetzungen an das Wireless-LAN 6
    - 3.1.1.1. Die verschiedenen WLAN-Standards 6
    - 3.1.1.2. Reichweite des Wireless-LAN 7
    - 3.1.1.3. Netzwerkarchitektur 8
      - 3.1.1.3.1. Ad-hoc-Modus 8
      - 3.1.1.3.2. Infrastructure-Modus 9
    - 3.1.1.4. Sicherheitsmaßnahmen 9
      - 3.1.1.4.1. WEP 9
      - 3.1.1.4.2. MAC-Adressfilter 9
      - 3.1.1.4.3. Closed Network 10
      - 3.1.1.4.4. EAP 10
    - 3.1.1.5. Strahlenbelastung 11
- 3.2.Gespräch mit der Leitung der Finanzbuchhaltung 11
  - 3.2.1. Finanzieller Rahmen 12

4. Angebotsvergleich 12
- 4.1. Technischer Vergleich verschiedener Wireless-LAN-Lösungen 12
- 4.2. Angebotssuche/vergleich 13

5. Zusammenfassung 15

Anhang

Stockwerksgrundriss (3. OG) A1
Vorschlag zur Access Point Positionierung A2
Quellcode: WEP-Key-Generator A3
EAP-Methoden A4
Glossar A5
Quellenverzeichnis A6
Hilfsmittel A7
Genehmigter Projektantrag A8

Persönliche Erklärung

Ich versichere durch meine Unterschrift, dass ich das Projekt und die dazugehörige Dokumentation selbstständig und ohne fremde Hilfe angefertigt habe. Die Arbeit hat in dieser Form keiner anderen Prüfungskommission vorgelegen.

München, 07. Mai. 2002

Ort, Datum | Unterschrift des Prüfungsteilnehmers

1. Thema

In das bestehende LAN[1)] der Firma SOFT-RESEARCH GmbH & Co. KG soll zusätzlich ein Zugang über ein Wireless-LAN[2)] geschaffen werden. Dies ist notwendig, da sich oft Außendienstmitarbeiter und Mitarbeiter anderer Filialen im Haus aufhalten, die hier über keinen festen eigenen Arbeitsplatz verfügen. Diesen Mitarbeitern steht ein Laptop zur Verfügung, jedoch momentan kein PCMCIA-Wireless-LAN-Adapter[3)]. Jenen Mitarbeitern muss schnell und unkompliziert ein Zugang zum Netzwerk verschafft werden, ohne auf Netzwerkanschlüsse angewiesen zu sein. Damit wird die Unabhängigkeit und Mobilität gesteigert. Ebenso wird das Wireless-LAN für die Besprechungsräume im Haus benötigt, da dort jeweils nur ein Netzwerkanschluss zur Verfügung steht, und es aus ästhetischen Gründen nicht möglich ist mit einem Hub[4)] oder Switch[5)] weitere Anschlussmöglichkeiten zu schaffen. Es ist aber bei einigen Besprechungen zwingend notwendig, das alle Anwesenden über einen LAN-Zugang verfügen.

Ziel dieses Projektes ist es, einen Überblick über die unterschiedlichen sich auf dem Markt befindenden Systeme und Standards zu geben, und eine Auswahl von Lösungen als Entscheidungsgrundlage für den Systemadministrator und die Geschäftsleitung zu treffen. Damit dient dieses Projekt als Grundlage für den kommenden Aufbau eines Wireless-LAN.

Grundsätzlich zum Aufbau dieser Projektdokumentation lässt sich folgendes sagen: Die Vorgehensweise zu den Unterpunkten wird jeweils einleitend beschrieben. IT spezifische Fachbegriffe sind gesondert gekennzeichnet und werden im Glossar (Anhang A5) erklärt, sofern die Erklärung sich nicht aus dem nachfolgenden Text ergibt.

2. Problemstellung

2.1. Ermittlung des Ist-Zustands

Die Ermittlung des Ist-Zustands erfolgte mittels der Erfassungsmethode des Interviews. In einem 2stündigen Gespräch mit dem Systemadministrator wurden die Eckpunkte des Netzwerkes ermittelt. Die folgende Darstellung des Ist-Zustands basiert auf den im Gespräch enthaltenen Informationen.

Das Netzwerk der Firma SOFT-RESEARCH GmbH & Co. KG ist ein switched[6)] 100BaseTx[7)] Ethernet[8)] aufgebaut in einer Baumtopologie[9)]. Für die Verkabelung wurden Cat5-Twisted Pair[10)] Kabel verwendet. In 4 Stockwerken sind momentan ca. 70 Rechner an 60 Arbeitsplätzen an das Netzwerk angeschlossen. Der Zugang zum Internet[11)] erfolgt über eine Firewall[12)] und einen Router[13)], und wird über eine 2Mbit Standleitung[14)] hergestellt.

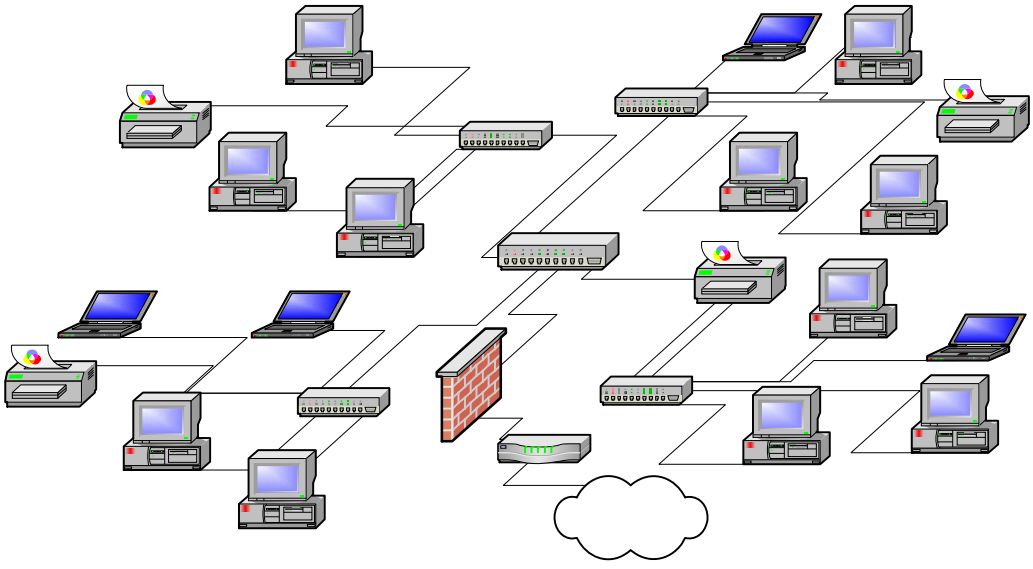


Abb.1: Vereinfachte Darstellung der Baumtopologie (ohne Server) von SOFT-RESEARCH

2.2. Ermittlung des Soll-Zustands

Die Ermittlung des Soll-Zustands stellte sich bei der Durchführung des Projektes als zeitintensiver heraus, als ursprünglich geplant. Grund für diese zeitliche Verschiebung um eine Stunde war die Aufnahme von Unterpunkten, die in dieser Komplexität nicht geplant waren, aber dem besseren Verständnis des Gesamtprojektes dienen. Die Aussagen wurde durch Recherchieren in der Quelle Q1) getroffen (siehe Quellenverzeichnis).

2.2.1. Vorteile des Wireless-LAN

Die Technik des Wireless-LAN bringt eine Menge Vorteile mit sich, von der nicht nur mobile Geräte wie Laptop oder PDA[15)] profitieren. Auch für stationäre Einrichtungen bieten sich zahlreiche Vorteile. Die lokale Verkabelung am Endgerät des Anwenders wird unnötig. Die kosten- und zeitintensive Verlegung von Kabeln entfällt und somit wird auch die Anzahl der Kabelverbindungen im Büro auf ein Minimum reduziert (je nach Ebene der Netzwerkhierarchie, die mit dem drahtlosen Übertragung abgedeckt wird). Lässt man das Funknetzwerk im Ad-Hoc-Modus[16)] laufen, muss sich kein Anwender mit den Spezifikationen des Wireless-LAN befassen, in dessen Funkzelle[17)] er sich gerade aufhält. Durch verschiedene Verschlüsselungs- und Authentifizierungsmaßnahmen kann ein Wireless-LAN zudem sehr gut gegen „Lauscher“ abgesichert werden.

Daraus ergeben sich zum Beispiel folgende Szenarien die schon seit geraumer Zeit in der Praxis Anwendung finden:

- In Meetings können alle Teilnehmer online auf sämtliche benötigten Informationen zugreifen, ohne an einen Netzwerkanschluss angeschlossen zu sein, oder Einstellungen am Laptop vorgenommen zu haben.
- Ein wesentlicher Vorteil gegenüber kabelgebundenen Systemen bietet das Funknetzwerk auch bei temporären Installationen wie z.B. auf Messen. Der Installationsaufwand ist hier um ein vielfaches geringer, der Aufbau geht viel schneller und es kommt zu weniger Ausfällen, da gerade bei Schnellaufbauten oftmals Fehler durch mangelhafte Kabelverbindungen entstehen.

So bieten Funknetzwerke eine wesentlich höhere Flexibilität als kabelgebundene Netze. Die genannten Vorteile führen zu einer höheren Produktivität und schnelleren Verfügbarkeit der Ressourcen. Ein Funknetzwerk hat allerdings auch eine Reihe von Nachteilen zu verzeichnen.

2.2.2. Vorurteile, Nachteile und Gefahren des Wireless-LAN

Jedes System hat irgendwo Schwachstellen und Nachteile. In letzter Zeit sorgte der Begriff „Wireless-LAN“ (bzw. Funknetz) vor allem deshalb für kontroverse Diskussionen, weil meist im selben Atemzug das Wort „unsicher“ fiel. Das dieses Thema früher oder später aufkommen musste, war nur eine Frage der Zeit. Bei der Akzeptanz und Verbreitung die diese Technologie in der Zwischenzeit erfahren hatte, konnten reißerische Schlagzeilen, die die Sicherheit von Funknetzen als äußerst fragwürdig darstellten, nicht ausbleiben. Betrachtet man diesen Aspekt jedoch genauer, fällt auf, dass bei entsprechender Implementierung von Verschlüsselungs- und Authentifizierungsmaßnahmen ein Funknetzwerk nicht weniger sicher oder unsicher ist als ein kabelgebundenes LAN. Untermauert wird diese Behauptung durch die Praxis - wo bereits in höchst sensiblen Bereichen, wie z.B. bei Banken, Versicherungen und Krankenhäusern, die Funk-Technik eingesetzt wird. Zur Absicherung eines Wireless-LAN stehen mindestens 3 Ebenen gegen unbefugten Zugriff zur Verfügung: a) Verschlüsselung[18)] mit 64-Bit oder 128-Bit b) Zugangsbeschränkung über die eindeutige MAC-Adresse[19)] c) Definition einer eindeutigen Gruppenidentität. Zudem existieren auf der Netzwerkebene zusätzlich die Betriebssystem-spezifischen Sicherheitsmöglichkeiten. Ein Grund ein Funknetzwerk als Standleitungsersatz zu verneinen besteht daher nicht. Bei einer Standleitung hat man keinen Einfluss auf die Verteilertechnik und die Sorgfalt des Providers[20)] in Sachen Sicherheit. Beim Einsatz der Funk-Technologie liegt es in der eigenen Hand, denn das Sicherheits-System lässt sich genau den

gewünschten Anforderungen anpassen. Alle zuvor genannten Nachteile sind daher mehr oder weniger Vorurteile, die sich relativ leicht entkräften lassen. Wirkliche Nachteile hingegen sind:

- die Bandbreite[21)], die trotz der positiven Kostenentwicklung der letzten Monate immer noch deutlich teurer und geringer als bei vergleichbaren kabelgebundenen Systemen ist.
- die Reichweite der drahtlosen Systeme, die in vielen Fällen empfindlich beschränkt ist, so dass die erhoffte Funktionalität nicht oder nur mit Abstrichen zu erreichen ist.
- der deutlich höhere Planungsaufwand für ein komplexes Funknetz, im Gegensatz zu einem vergleichbaren kabelgebundenem LAN. Der Standort des Access Points[22)] muss zudem sorgfältig gewählt werden, um eine möglichst gute Abdeckung und möglichst geringe Störung zu erzielen.
- die Vielzahl der Lösungen, welche gegenwärtig auf dem Markt verfügbar sind, wobei nur in wenigen Fällen der mittelfristige Markterfolg gesichert ist. Vor dem Hintergrund der Investitionssicherheit führt diese Situation häufig zu einer Verschiebung der Investitionsentscheidung.

2.2.3. Zielsetzungen für das geplante Wireless-LAN

Das Funknetz soll die höchstmöglichen Sicherheitsstandards verwenden, und zudem eine bestmögliche Abdeckung der Etagen erreichen, in denen es benötigt wird. Die Beschaffungs- und Installationskosten dürfen nicht über das veranschlagte Budget hinausgehen.

3. Planung

3.1. Gespräch mit dem Systemadministrator

In einem 2stündigen Gespräch mit dem Systemadministrator wurden die technischen Vorraussetzungen, die an das Wireless-LAN gestellt werden, ermittelt. Die Ergebnisse dieses Gesprächs werden nachfolgend beschrieben. Grundlage des Gesprächs war eine zuvor durchgeführte Recherche. Das Ziel dieser war, die grundlegenden technischen Informationen über Wireless-LAN und verfügbare Standards herauszufinden. Eventuell verwendete Quellen werden einleitend zu jedem Unterpunkt genannt. Die Ergebnisse und Schlussfolgerungen folgen am Ende des jeweiligen Unterpunktes. Der zeitliche Aufwand übertraf - durch die zuvor geführte Recherche - die in der Planung angegebene Stundenzahl um 1,5 Stunden. Der zeitliche Mehraufwand konnte aber bei der Angebotssuche wieder eingespart werden.

3.1.1. Technische Vorraussetzungen an das Wireless-LAN

3.1.1.1. Die verschiedenen WLAN-Standards

Die gewonnen Informationen in diesem Abschnitt beruhen auf den Quellen Q1) und Q2). Derzeit existieren eine Vielzahl miteinander konkurrierender Lösungen auf dem Markt, was im frappierenden Kontrast zum drahtgebundenen LAN mit dem dominierenden Ethernet-Standard steht. Der Markt für Wireless-LANs befindet sich momentan in der Einführungsphase. Für die nächsten Jahre werden immense Wachstumsraten prognostiziert. Deshalb versuchen viele Hersteller, sich durch die Entwicklung eigener Standards und die Ausprägung besonderer Merkmale eine aussichtsreiche Startposition auf dem Markt zu verschaffen. 1997 wurde von dem IEEE[23)] der WLAN-Standard IEEE 802.11 verabschiedet, von dem es inzwischen 2 Abwandlungen gibt, die inzwischen von fast allen namhaften Herstellern in ihre Produkte integriert wurden.

Eine kurze Übersicht der am Markt relevanten WLAN-Standards mit den wichtigsten technischen Fakten im Überblick:

- Bluetooth:
  - Frequenzbereich[24]: 2,4-GHz-ISM-Band
  - Reichweite[25]: Ohne Richtantenne[26] ca. 10 m
  - Datenraten[27]: 865,2 Kbit/s

- DECT:
  - Frequenzbereich: 1800-1900 MHz
  - Reichweite: In Gebäuden ca. 50 m, im Freien bis 300 m
  - Datenraten: Unter Ausnutzung aller Kanäle max. 20 Mbit/s

- IEEE802.11b:
  - Frequenzbereich: 2,4-GHz-ISM-Band
  - Reichweite: In Gebäuden ca. 100 m, mit Richtantenne bis 2 km möglich
  - Datenraten: Von 2Mbit/s bis 11 Mbit/s

- Wi-Fi5: ehm. IEEE802.11a
  - Frequenzbereich: 5-GHz-UNII-Bereich
  - Reichweite: In Gebäuden ca. 50 m, im Freien bis 500 m
  - Datenraten: 11 Mbit/s bis 54 Mbit/s

- HiperLAN/2:
  - Frequenzbereich: 5 GHz-ISM-Band
  - Reichweite: In Gebäuden ca. 50 m
  - Datenraten: Bis zu 54 Mbit/s

- HomeRF:
  - Frequenzbereich: 2,4-GHz-ISM-Band
  - Reichweite: In Gebäuden ca. 50 m
  - Datenraten: 1,6 Mbit/s, bei Kanalbündelung mehr

Ergebnisse/Schlussfolgerungen:

Aufgrund der niedrigen Reichweite und der geringen Datenübertragungsrate stehen Lösungen, die auf den Bluetooth-, DECT- und HomeRF-Standards basieren, nicht zur Wahl. Die Zielausrichtung dieser Systeme liegt deutlich erkennbar im Bereich der Personal Area Networks[28] (PAN). Aufgrund der noch relativ geringen Verbreitung und der im Vergleich relativ hohen Hardwarekosten und dem damit verbunden Investitionsrisiko, steht der HiperLan/2-Standard ebenso nicht zur Diskussion. Da das 5-Ghz-Frequenzband von der EU und den Mitgliedsstaaten noch nicht zur Nutzung freigegeben wurde, ist außerdem noch keine entsprechende Hardware in Europa verfügbar. Den aktuellsten Informationen nach befindet sich der Wi-Fi5-Standard zur Zeit noch in der Testphase bei der zuständigen EU-Kommission. Aufgrund des hohen Marktanteils des IEEE802.11b-Standards ist das Investitionsrisiko bei dieser Lösung als am geringsten zu beurteilen. Zudem sind Reichweite und Datenübertragungsraten im Vergleich mit den anderen Lösungen am höchsten. Die Wahl fällt also auf Systeme, die den IEEE802.11b-Standard unterstützen.

3.1.1.2. Reichweite des Wireless-LAN

Die zu erreichende Abdeckung, welche das Wireless-LAN im Haus haben soll, wurde in Absprache mit dem Systemadministrator folgendermaßen definiert:

- Im Erdgeschoss befinden sich lediglich ein Schulungsraum für Anwenderschulungen, der Empfang und das Lager. Der Zugang zum LAN über WLAN muss hier nicht zwingend erreicht werden.

- Im 1. Stock sind die Finanzbuchhaltung und Verwaltung, sowie die Abteilung „Direct Sales“ ansässig. Außerdem ist auf dieser Etage ein Vorführraum zu finden, der in erster Linie für Präsentationen und Mitarbeiterversammlungen genutzt wird (ein Präsentationsrechner mit LAN-Zugang ist vorhanden). Auch hier ist der Zugang über das Wireless-LAN in das Netzwerk nicht zwingend erforderlich.

- Im 2. Stock befindet sich die Hotline und die Systemadministration. Das Wireless-LAN muss diesen Bereich aus Administrationsgründen abdecken.

- Im 3. Stock befindet sich die Geschäftsleitung und die Entwicklung. Da besonders auf diesem Stockwerk häufig mit Geschäftspartnern, Besuchern und auswärtigen Mitarbeitern zu rechnen ist, wurde für diese Etage die höchste Erreichbarkeit des Wireless-LAN festgelegt. Die beiden auf dieser Etage befindlichen Besprechungsräume müssen ebenfalls abgedeckt werden.

Ergebnisse/Schlussfolgerungen:

Wie anhand des Grundrissplans (siehe Anhang A1) deutlich wird, überschreiten die durch das Gebäude gegebenen Raummaße die in den Spezifikationen des IEEE802.11b-Standards angegebene Reichweite der WLAN-Systeme. Daraus ergibt sich die Notwendigkeit, das Signal entweder entsprechend mit einer Antenne zu verstärken oder einen weiteren Hotspot einzurichten. Nach einer Begehung der Räumlichkeiten wird weiterhin klar, dass die Brandwände - mit einer Stärke von ca. 22,5 cm - die Funkwellen mit höchster Wahrscheinlichkeit komplett absorbieren oder so sehr schwächen werden, dass für den jeweils anderen Gebäudeteil ein extra Access Point notwendig wird. Diese Aussage beruht auf Erfahrungen verschiedenster Personen beim Einrichten eines Wireless-LAN, die u.a. in der Newsgroup „de.comp.hardware.netzwerke“ nachzulesen und zu hinterfragen sind. Genauere Angaben zur Reichweite, die das Wireless-LAN voraussichtlich erreichen wird, sind leider nicht möglich. Diese hängt sehr stark von den baulichen Gegebenheiten und den eingesetzten Baustoffen ab. Ein Vergleich mit bereits existierenden Funknetzen ist nicht zu empfehlen. Um dem Risiko von Fehlinvestitionen vorzubeugen, ist es empfehlenswert, die Reichweite eines Access Points in einem Test zu ermitteln. Bei der Positionierung der Access Points ist zu beachten, das sich die Funkzellen möglichst überlappen, um ein Wandern zwischen den Zellen zu ermöglichen (Roaming[29)]). Um die geforderte Abdeckung des Funknetzes zu erreichen, sind nach einer ersten Überlegung 3 Access Points notwendig. Die vorgeschlagene Positionierung ist dem Anhang A2 zu entnehmen.

Vorgehensweise: Reichweitenermittlung eines Access Points mittels Test:

Zuerst ist es notwendig ein Exemplar des Access Points zu kaufen, der auch später Verwendung finden soll. Dieser wird dann, der Reihe nach, an den für die Hotspots[30)] vorgesehenen Stellen im Gebäude positioniert und angeschlossen. Die beim Access Point mitgelieferten Software wird auf einem Laptop installiert und eingerichtet. Diese bietet i.d.R. verschiedene Möglichkeiten, das vorhandene Funknetz auf Qualität und Verfügbarkeit zu testen. Wurden alle vorgesehenen Positionen mit dieser Methode getestet, wird deutlich, wo das WLAN mit einem zusätzlichen Access Point bzw. einer Antenne verstärkt werden muss.

3.1.1.3. Netzwerkarchitektur

Ein Funknetz lässt sich wahlweise im „Ad-hoc“-, oder im „Infrastructure“-Modus betreiben. Dieser Abschnitt enthält den Vergleich der beiden Modi.

3.1.1.3.1. Ad-hoc-Modus

Der Ad-hoc-Modus ist im Grunde ein Wireless Peer-to-Peer[31)] Netzwerk. Dieser Modus muss bei den einzelnen Funkkarten der Clients aktiviert sein, um damit die Kommunikation der Clients ohne Access Point untereinander zu ermöglichen. Dazu ist es notwendig, auf allen Clients einen einheitlichen Namen für das Funknetz einzustellen. Der Ad-hoc-Modus eignet sich vor allem für Testzwecke oder spontane, selbstorganisierte Vernetzung untereinander. Dabei ist zu beachten, dass sich alle beteiligten Stationen gegenseitig „sehen“ müssen, da es im Gegensatz zu kabelgebundenen Netzwerken keine festgelegten Routen gibt. Der Datendurchsatz im Netz wird bei ca. 10 Rechnern ein kritisches Minimum erreichen. Der Verwaltungsaufwand für ein solches Netzwerk steigt mit jedem weiteren Rechner.

3.1.1.3.2. Infrastructure-Modus

Im Infrastructure-Modus baut ein Access Point eine Funkzelle auf, deren Abdeckung sich mit Spezialantennen und durch eine günstige Platzierung verbessern lässt. Alle WLAN-Geräte kommunizieren über den Access Point miteinander, sowie mit den anderen im LAN integrierten Geräten. Im Infrastructure-Modus bekommen die einzelnen Clients über einen Access Point Zugang zum drahtgebundenen LAN. Der Access Point dient zum einem als Bridge[32)] zum drahtgebundenen Netz, vermittelt also Pakete zwischen den Netzen hin und her. Zum anderen arbeitet er als Repeater[33)], das heißt er empfängt Pakete der Clients und leitet sie an andere weiter.

Ergebnisse/Schlussfolgerungen:

Der Ad-hoc-Modus eignet sich zum Aufbau eines einfachen Funknetzes, für kleine oder schnell aufzubauende Umgebungen. Durch die oben genannten Nachteile eignet sich dieser nicht für den angestrebten Soll-Zustand. Aus diesem Grund wird der Betrieb des Funknetzes im Infrastructure-Mode dringend empfohlen.

3.1.1.4. Sicherheitsmaßnahmen

Der größte Vorteil des Mediums Funk ist auch gleichzeitig sein Nachteil: Die Funkwellen verbreiten sich leider nicht nur im gewünschten Raum, sondern generell in der kompletten Funkzelle. Im folgenden Abschnitt werden die wichtigsten Sicherheits-Mechanismen für Wireless-LANs erläutert, ohne auf tiefergreifende technische Informationen einzugehen. Die in diesem Abschnitt enthaltenen Informationen beruhen auf Inhalten der Quelle Q3).

3.1.1.4.1. WEP

WEP steht für Wired Equivelent Privacy, einem Verfahren zur Datenverschlüsselung und Authentifizierung in Wireless-LANs. Wie der Name bereits sagt, soll das Verfahren eine vergleichbare Vertraulichkeit erzielen wie in einem drahtgebundenen LAN. Im Gegensatz zum Ethernet, wo die Datenübertragung meist unverschlüsselt erfolgt, ist WEP ein fester Bestandteil des IEEE 802.11b Protokoll-Stacks. Die WEP-Verschlüsselung erfolgt synchron[34)] mit 64 oder 128 Bit nach dem Algorithmus RC4[35)]. Die eigentliche Verschlüsselung erfolgt jedoch mit 40 bzw. 104 Bit. 24 Bit dienen nur zur Erzeugung des Paketschlüssels. Dieser wird wiederum zur Verschlüsselung eines Datenpakets[36)] verwendet. Die 24 Bit werden als eine Art „Initial Vektor“[37)] (IV) mit jedem Paket im Klartext übertragen und sind daher allgemein lesbar. Da IV-Wiederholungen auftreten, ist diese Verschlüsselung höchst unsicher und schon nach wenigen Stunden zu „knacken“. Die Authentifizierung über WEP bietet keinen hinreichenden Schutz. Im Shared Key Authentication (SKA) prüft der Access Point während der Assoziierung einer Funkstation im Challenge-Response-Verfahren, ob ein gültiger WEP-Schlüssel vorhanden ist. Erst nach erfolgreicher Prüfung können angemeldete Stationen Daten übertragen. WEP definiert keine weiteren Verfahren zum Schlüsselmanagement. Die Schlüssel müssen auf allen Clients und Access Points lokal vorhanden sein. Die Schlüsselvergabe erfolgt manuell. Alle Stationen verwenden die selben Schlüssel. Zur Erzeugung von gültigen WEP-Schlüsseln kann der WEP-Key-Generator verwendet werden. Der Quellcode für dieses, in Visual Basic geschriebene Programm, befindet sich im Anhang A3.

3.1.1.4.2. MAC-Adressfilter

Eine weiterer Sicherheitsmechanismus ist der MAC-Adressfilter. Mittels einfachen Access-Control-Listen (ACL) werden registrierte MAC-Adressen entweder zur Kommunikation zugelassen oder abgewiesen. Diese Access-Control-Listen mit den MAC-Adressen müssen auf jedem Access Point vorhanden sein. Dazu werden entweder alle Adressen fest im internen Speicher des Access Points abgelegt, oder per RADIUS-Protokoll[38)] nach Bedarf von einem zentralen Server abgefragt. Die zentrale Ablage erleichtert dabei vor allem das Management in einem Netzwerk mit vielen Teilnehmern.

3.1.1.4.3. Closed Network

Eine wichtige Funktion nimmt in einem Wireless-LAN der Netzwerkname ein, der oftmals auch als ESS-ID bezeichnet wird. An jedem Client-Rechner[39)] muss zur Auswahl des WLAN der passende Netzwerkname eingetragen werden. Allerdings besteht auch die Möglichkeit, die ESS-ID „ANY“ zu verwenden, um sich an beliebigen Access Points in der Nähe anzumelden. Einige WLAN-Adapter bieten dazu auch eine Scan-Funktion, mit der sich eine Liste aller Funknetzwerke in Reichweite ermitteln lässt. Bei einigen Produkten ist es möglich, das Senden der ESS-ID zu verhindern. Diese Funktion wird „Closed Network“ genannt. Ein Netzwerk mit eingeschalteter Closed Network-Funktion akzeptiert außerdem keine Verbindungen von Clients mit der ESS-ID „ANY“.

3.1.1.4.4. IEEE 802.1x/EAP

802.1x ist ein Standard des IEEE für lokale Netze, der im Juni 2001 veröffentlicht wurde, und insbesondere im Bereich der WLANs Furore macht. 802.1x erweitert WLANs um die Funktion einer „Port Based Network Access Control“, d.h. einer Authentifizierungsmöglichkeit für Benutzer und Stationen. EAP (Extensible Authentication Protocol) übernimmt dabei die Auswahl des Authentifizierungsmechanismus zwischen Client- und Basis-Station. Der Authenticator (Access Point) und der Supplicant (Client) tauschen per EAP (genauer gesagt: EAP-over-LAN) die Authentifizierungsdaten aus. Die tatsächliche Überprüfung der Benutzerdaten des Supplicant geschieht allerdings durch den Authentication Server. Die Kommunikation zwischen Authenticator und Authentication Server findet per RADIUS-Protokoll statt. Auch der RADIUS-Server muss die EAP-Erweiterungen unterstützen. Wie die Identität von Benutzern und Stationen tatsächlich überprüft wird, bestimmt die EAP-Methode. Die wichtigsten Methoden nutzen dazu entweder digitale Zertifikate oder Passwörter. Näheres zu den verschiedenen EAP-Methoden siehe Anhang A4.

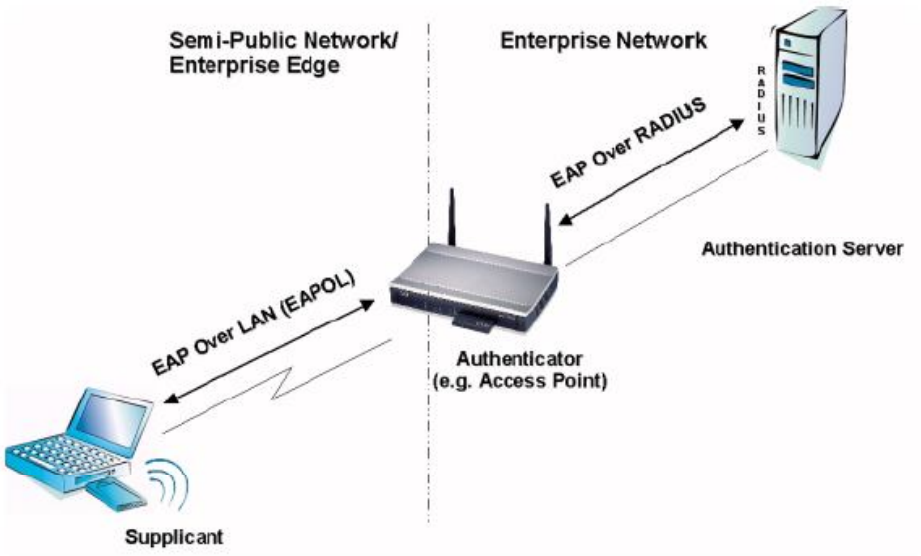


Abb.2: Anmeldeszenario einer 802.1x/EAP-Anmeldung

Ergebnisse/Schlussfolgerungen:

Es wird deutlich, das die genannten Sicherheitsmechanismen einzeln keinen ausreichenden Schutz bieten. Die WEP-Verschlüsselung kam z.B. in die Schlagzeilen, nachdem verschiedene Artikel veröffentlicht wurden, in denen auf die Verwundbarkeit von WEP hingewiesen wurde. Unter dem Titel „Weaknesses in Key Scheduling“ erschien ein Beitrag von Scott Fluhrer von Cisco Systems sowie Itsik Mantin und Adi Shamir vom Weizmann-Institut in Israel. Thema dieser Arbeit war die Möglichkeit, mit geringem Aufwand Angriffe auf so genannte „schwache“ WEP-Schlüssel auszuführen. Mit dem inzwischen im Internet zum Download verfügbaren Programm „AirSnort“[40)] ist nach einem passiven Aushorchen das unbefugte Eindringen in WEP-geschützte WLANs möglich. Der

MAC-Adressfilter ist leider schon seit geraumer Zeit, auch bei herkömmlichen LANs, keine hinreichende Sicherheitsgarantie mehr. Gängige Funknetzwerkkarten arbeiten mit einer beliebigen MAC-Adresse, die sich leicht in der Treiberkonfiguration einstellen lässt. Die Funktion „Closed Network“ versteckt das Funknetzwerk nach außen, was den Zugang erschwert, aber für versierte Leute trotzdem nicht unmöglich macht.

Es wird eine Kombination aus IEEE 802.1x mit einer WEP-Verschlüsselung von 128 Bit und einer gegenseitigen Authentifizierung auf Basis von digitalen Zertifikaten (EAP-TLS) empfohlen. Jeder Benutzer erhält für seinen Client ein digitales Zertifikat, das sowohl seine eigene Identität ausweist als auch zur Überprüfung von zulässigen Access Points genutzt wird. Die Authorisierung und die Verteilung der WEP-Schlüssel erfolgt zentral von einer Benutzerdatenbank im LAN. Somit ist gewährleistet, das die Administration die vollständige Kontrolle über Zugang und Key-Management im WLAN hat. An zentraler Stelle können Nutzungsprotokolle angelegt und ausgewertet werden. Potentielle Einbruchversuche können rechtzeitig erkannt und lokalisiert werden. Auch aus Anwendersicht ist diese Lösung sehr komfortabel, da er weiterhin seine gewohnte Netzanmeldung hat.

3.1.1.5. Strahlenbelastung

Da Wireless-LANs mit Funkwelle arbeiten, stellt sich natürlich auch die Frage nach der Strahlung die von diesen Netzen ausgeht. Die in diesem Abschnitt genannten Fakten stammen aus einem Bericht über die elektromagnetischen Strahlungen von WLAN-Komponenten (siehe Q4). Nachfolgend eine Übersicht der Ergebnisse des Berichtes:

„Das System Wireless-LAN wurde hinsichtlich seiner ausgesendeten elektrischen und der daraus abgeleiteten magnetischen Feldstärken und hinsichtlich seiner Leistungsflussdichte bei einer Speiseleistung von 100 mW mit einer sinusförmigen Frequenz von 2,46 GHz vermessen.
Sämtliche Messwerte liegen weit unterhalb der von der DIN VDE 0848, Teil 2 E/10/91 Expositionsbericht 1 und der 26. Verordnung zum Bundes Immissionsschutzgesetz vorgegebenen Grenzwerte bei Einhaltung des Mindestabstands zwischen Antenne und Person von 50 cm. Somit ist die Sicherheit von Personen im elektromagnetischen Umfeld eines Funknetzwerkes nicht nur sichergestellt, sondern weist auch große Reserven auf.“

Ergebnisse/Schlussfolgerungen:

Bekannte Probleme mit der Strahlenbelastung gibt es nicht. Entsprechen die Produkte der europäischen Norm ETS 300328, worin die Sendeleistung mit 100 mW festgelegt ist, so entspricht das einem zwanzigstel eines D-Netz-Handys. Somit sind die dabei abgestrahlten Leistungen so gering, dass das Funknetz weit weniger gefährlich als ein Mikrowellengerät, ein Handy oder ein DECT-Schnurlostelefon (mit der 10-20fachen Strahlungsleistung) ist. Die in diesem Frequenzbereich festgelegten Grenzwerte werden so weit unterschritten, dass WLAN-Karten sogar für den Einsatz im Medizinbereich zertifiziert sind. Die Access Points senden nicht permanent sondern nur wenn tatsächlich auch eine Datenübertragung stattfindet. Der Access Point ist somit, anders als Mobilfunk-Basisstationen, funktechnisch nicht aktiver als ein WLAN-Client-Rechner. Auch bei mehreren Teilnehmern, die sich in einer Funkzelle aufhalten, ist immer nur ein WLAN-Adapter zu einem Zeitpunkt aktiv, so dass auch hier keine „Vervielfachung“ der Strahlenbelastung entsteht. Es ist allerdings darauf zu achten, das der Mindestabstand von 50 cm zwischen Access Point und Person (bzw. Antenne und Person) nicht unterschritten wird.

3.2. Gespräch mit der Leitung der Finanzbuchhaltung

In einem 1stündigen Gespräch mit der Leitung der Finanzbuchhaltung wurden die finanziellen Aspekte des Projektes geklärt. Grundlage des Gesprächs waren die, zuvor mit dem Systemadministrator festgelegten, technischen Vorraussetzungen an das Wireless-LAN. Die Ergebnisse des Gesprächs werden nachfolgend aufgelistet.

3.2.1. Finanzieller Rahmen

Das Budget entspricht den Hardwarekosten für die vorgeschlagene Lösung (inkl. den Kosten für die Aufrüstung der vorhandenen Laptops mit PCMCIA-Wireless-LAN-Adaptern). Anfallende Kosten für Montagestunden werden in diesem Rahmen nicht berücksichtigt. Die für das Budget zugrunde liegenden Hardwarekosten entsprechen aufgerundeten Netto-Einkaufspreisen von am Markt befindlichen Lösungen. Sie sollen lediglich einen Überblick über die zu erwartenden Kosten geben. Die Angebotssuche erfolgt zu einem späteren Zeitpunkt.

Hardware	Anzahl	Einzelpreis	Gesamtpreis
Access Point	3	450,00 €	1.350,00 €
PCMCIA-WLAN-Adapter	8	200,00 €	1.600,00 €
		Gesamtkosten:	**2.950,00 €**

Ergebnisse/Schlussfolgerungen:

Das Budget für den Einkauf der Hardware wurde auf 3000,00 € (Netto-Einkaufspreis) festgelegt. Der Einkauf der Hardware soll zu den für die SOFT-RESEARCH GmbH & Co. KG besten Konditionen erfolgen.

4. Angebotsvergleich

Der Angebotsvergleich ist in 2 Punkte unterteilt. Der erste Punkt beschäftigt sich mit dem technischen Vergleich verschiedener WLAN-Lösungen. Im zweiten Punkt werden zu den zuvor betrachteten Systemen Angebote eingeholt, welche anschließend anhand von finanziellen Aspekten miteinander verglichen werden.

Anmerkung: Der ursprünglich geplante Vergleich von 3 Wireless-LAN-Systemen wurde mangels Alternativsystemen verworfen. Die gefundenen Lösungen entsprachen entweder nicht den technischen Anforderungen, oder waren weder über unsere Lieferanten, noch über Hardwarelieferanten im Internet zu annehmbaren Konditionen zu beziehen.

4.1. Technischer Vergleich verschiedener Wireless-LAN-Lösungen

Die Hersteller-Angaben bezüglich Reichweite und Datendurchsatz orientieren sich in der Regel an Fantasie-Welten, in denen keine Stahlbetonwände die Idylle der Übertragung stören. Da aber gerade diese Werte ein entscheidendes Merkmal für die Auswahl eines WLAN-Systems sind, war es notwendig einen objektiven Überblick über die sich am Markt befindenden Systeme zu erlangen. Um verlässliche Vergleichsdaten zu erhalten, wurde der Vergleichstest aus Quelle Q5) herangezogen. Anhand dieses Tests wurden 2 Systeme ausgewählt, die den technischen Anforderungen entsprechen, die an den Access Point gestellt werden. Da dieser Test im Oktober 2000 stattfand, und es gerade im Bereich der Wireless-LAN-Technik in relativ kurzen Abständen zu massiven Neuerungen kommt, wurden die damals getesteten Systeme durch die jeweiligen Nachfolgesysteme ersetzt. Der in Q5) ermittelte Datendurchsatz der beiden WLAN-Systeme bezieht sich auf die im Oktober 2000 getesteten Vorgängermodelle und wird deshalb in der nachfolgenden Betrachtung getrennt dargestellt. Die Durchsatzraten der damals getesteten Modelle sind allerdings durchaus mit den der Nachfolgemodellen vergleichbar. Nachfolgend eine Übersicht der beiden ausgewählten Systeme mit den wichtigsten Eigenschaften:

Access Point	Cisco AiroNet 350	Elsa LANCOM Wireless L11
Dokumentation	12 Seiten, englisch	130 Seiten, deutsch
Unterstütze Standards	802.11, 802.11b	802.11, 802.11b
LAN-Interface	10/100BaseT	10BaseT
Sonstige Interfaces	SerielI	-
Konfiguration	Terminal, Telnet, SNMP, HTTP	Telnet, SNMP, Windows Tool, HTTP
DHCP-Client	ja	ja
LAN-Protokolle	TCP/IP, ICMP, DHCP, IXP/SPX	TCP/IP, ICMP, DHCP
MAC-Filter	ja	ja
Verschlüsselung	WEP 40/128	WEP 40/128
PC-Card	Aironet 350 series AIR.PCM430	AirLancer MC-11
Betriebsarten	Ad-hoc, Infrastructure	Ad-hoc, Infrastructure
Reichweite* (in Gebäuden)	100 m	50 m
Datendurchsatz** (in KByte/s)	610, 502, 222	479, 479, 73

*) Die angegebene Reichweite sind maximale Herstellerangaben.

**) Der Datendurchsatz wurde in einem TCP-Benchmark ermittelt. Die 3 Werte entsprechen den Entfernungen des Testrechners zum Access Point (v.li.n.re.): nah (2,5 m), mittel (21 m) und fern (45 m)

System 1: Cisco AiroNet 350

Der Cisco AiroNet überzeugt im Test der c't-Redaktion vor allem durch seinen sehr hohen Datendurchsatz, der ihn von den Konkurrenzprodukten abhebt. Verantwortlich dafür ist ein integrierter „Mini-Rechner" mit einem 50Mhz 32-Bit-Mikrocontroller, 2MB Flash EPROM und 16 MB DRAM. Für die Konfiguration der Clients liegt eine Windows-Software bei. Die Power-Management-Funktion der PCMCIA-Karten ist nicht optimal.

System 2: Elsa LANCOM Wireless L11

Das Besondere am Access Point von Elsa ist wohl vor allem seine deutsche Bedienungsanleitung, mit der keiner der Konkurrenten aufwarten kann. Der Datendurchsatz ist gut, reicht aber nicht an den des Cisco AiroNet heran. Der Access Point bietet zusätzlich einen externen Antennenanschluss. Die von den PCMCIA-Karten unterstützte Power-Management-Funktion ist sehr gut.

Ergebnisse/Schlussfolgerungen:

Die technischen Unterschiede der 2 Systeme sind minimal. Beide unterstützen die WEP-Verschlüsselung mit 128 Bit und bieten die Konfiguration via Telnet[41)] und Webbrowser. Eine serielle Schnittstelle zur Konfiguration über ein Nullmodemkabel hat allerdings nur der Access Point von Cisco. Der Access Point von Elsa verfügt nur über einen 10BaseT-LAN-Anschluß, wird dafür aber mit einer umfangreichen deutschen Bedienungsanleitung ausgeliefert. Die Favorisierung eines Systems ist anhand dieser Daten nur schwer möglich, sofern diese nicht nur auf die Reichweitenangabe der Hersteller gestützt sein soll. Auch persönliche Erfahrungswerte mit einem der Hersteller sind kein aussagekräftiges Argument als Kaufentscheidung für eines der beiden Systeme. Anhand der durch die c't-Redaktion ermittelten Datenübertragungsraten lässt sich jedoch eine Empfehlung für den Cisco AiroNet 350 aussprechen.

4.2. Angebotssuche/vergleich

Durch den am 25.02.02 gestellten Insolvenzantrag[1] der Elsa AG ist ein Angebotsvergleich nur schwer zu führen. Die ungewisse Situation von Elsa führt zu rapide fallenden Preisen der Produkte, mit dem Ziel die Lagerbestände zu verkaufen, bevor etwas über die weitere Zukunft von Elsa feststeht. Die momentane Situation stellt ein sehr hohes Investitionsrisiko für alle Elsa-Produkte dar, da Garantie- und Serviceleistungen möglicherweise nicht mehr eingefordert werden können. Ähnlich verhält es sich bei Treiber- und Firmware-Updates, die wahrscheinlich ebenfalls nicht mehr zur Verfügung stehen

werden. Wie aktuell[2] auf dem Heise-Newsticker zu lesen ist, wird Elsa zum 1. Mai 2002 den Geschäftsbetrieb einstellen. Es wird möglicherweise eine Aufspaltung des Unternehmens geben, wobei der Netzwerkbereich allerdings weitergeführt werden soll. Investoren halten sich aber bisher noch zurück. Das angesprochene Investitionsrisiko bleibt daher bestehen. Es gilt abzuwägen, ob man dieses bewusst eingehen will, und möglicherweise sehr günstig an eine Wireless-LAN-Lösung kommt, die man aber unter Umständen mit dem Release[42)] der nächsten Windows-Version nicht mehr einsetzen kann. Die verwendeten Preise der beiden Systeme im nachfolgenden Angebotsvergleichs sind Netto-Einkaufspreise (ohne Verpackungs- und Transportkosten) und stammen vom 26.04.2002:

[1] siehe: http://www.heise.de/newsticker/data/tol-25.02.02-004/
[2] siehe: http://www.heise.de/newsticker/data/uma-24.04.02-001/

Cisco AiroNet 350

Access Point: AiroNet 350 (AIR-AP352E2C)
PCMCIA-Card: AIR-LMC352

Alldis

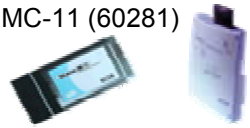
Artikel	Stück	Einzelpreis	Gesamtpreis
AIR-AP352E2C	3	1.160,00 €	3.480,00 €
AIR-LMC352	8	145,00 €	1.160,00 €
		Gesamtsumme:	**4.640,00 €**

Tech Data

Artikel	Stück	Einzelpreis	Gesamtpreis
AIR-AP352E2C	3	577,19 €	1.731,57 €
AIR-LMC352	8	123,56 €	988,48 €
		Gesamtsumme:	**2.720,05 €**

Elsa LANCOM Wireless L11

Access Point: LANCOM Wireless L11 (00655)
PCMCIA-Card: AirLancer MC-11 (60281)



Alldis

Artikel	Stück	Einzelpreis	Gesamtpreis
00655	3	325,00 €	975,00 €
60281	8	101,00 €	808,00 €
		Gesamtsumme:	**1.783,00 €**

Tech Data

Artikel	Stück	Einzelpreis	Gesamtpreis
00655	3	544,01 €	1.632,03 €
60281	8	ausverkauft	-
		Gesamtsumme:	**1.632,03 €**

Ergebnisse/Schlussfolgerungen:

Bedingt durch das sehr hohe Investitionsrisiko, das mit dem Erwerb des Elsa LANCOM Wireless L11 verbunden ist, ist die Entscheidung für den Cisco AiroNet 350 unbedingt zu empfehlen. Die unklare Lage bei späteren Supportanfragen, Garantiefällen oder Soft- und Firmware-Updates könnte sich im Nachhinein als Fehlinvestition herausstellen, die weit über den Differenzbetrag von 937,05 € hinausgeht.

Ermittlung des Differenzbetrags:

2.720,05 € Summe d. Cisco-Systems (bei Tech Data)
1.783,00 € Summe d. Elsa-Systems (bei Alldis)
937,05 €

Da die Beschaffung der Hardware zu den, für die SOFT-RESEARCH GmbH & Co. KG besten Konditionen erfolgen soll, wird der Einkauf bei Tech Data zum oben genannten Betrag von 2720,05 € empfohlen. Die Zahlung erfolgt nach den AGB der Tech Data GmbH und ist 14 Tage ab Rechnungsdatum ohne Abzug fällig. Die Abschreibung der Hardware kann aufgrund der firmeninternen Richtlinie auf 3, anstatt auf 5 Jahre erfolgen.

5. Zusammenfassung

Der gewünschte Soll-Zustand lässt sich mit den Mitteln der Wireless-LAN-Technologie sehr gut herstellen. Die dadurch entstehenden Vorteile für die Firma SOFT-RESEARCH GmbH & Co. KG und deren Mitarbeiter sprechen eindeutig für die Installation eines Wireless-LANs. Gängige Argumente die gegen ein Wireless-LAN sprechen, lassen sich mit dem aktuellen Wissensstand relativ leicht entkräften. So ist etwa die Sicherheit bei entsprechender Implementierung der vorhandenen Sicherheitsrichtlinien und sorgfältiger Betreuung des WLANs durch die Systemadministration nicht als geringer zu bewerten, als beim kabelgebundenen LAN. Auch die Gesundheitsgefährdung durch elektromagnetische Strahlung wurde inzwischen widerlegt, und darf kein Argument mehr gegen ein Wireless-LAN sein. Einzig die mit der Installation eines Funknetzes verbundenen Investitionen sind, weil immens hoch, ein Negativ-Argument. Die Vorteile die die Installation eines Wireless-LAN Systems zweifellos mit sich bringen würde, stehen Investitionskosten von 2720,05 € gegenüber. Die Entscheidung für ein Wireless-LAN muss von der Geschäftsleitung getroffen werden, und ist davon abhängig ob die Vorteile eines Wireless-LANs die hohen Kosten rechtfertigen.

Bei einer konkreten Entscheidung für ein Wireless-LAN, ist der Kauf des Access Points von Cisco zu empfehlen. Die Entscheidung für den IEEE802.11b-Standard und den Cisco AiroNet 350 ist insgesamt als zukunftssichere Investition anzusehen.

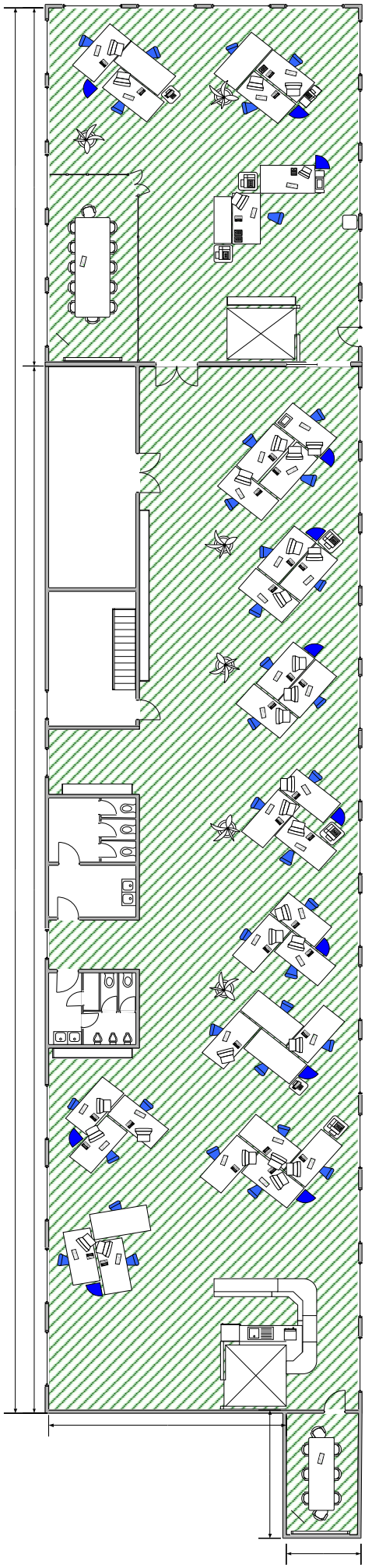


Abb.3: Raumplan des 3. Stockwerks der SOFT-RESEARCH GmbH & Co. KG

Abb.3: 3. OG, Besprechungsraum (Glaskasten). Punkt „AP2“ befindet sich nicht im Bildausschnitt.

Abb.4: 3. OG, Entwicklung. Der Punkt „AP1“ befindet sich auf dem Stahlträger, über der vorderen Säule.

Abb.5: 2. OG, Technik mit Blick auf Serverraum. Der Access Point wird im 2. Stockwerk direkt im Serverraum platziert.

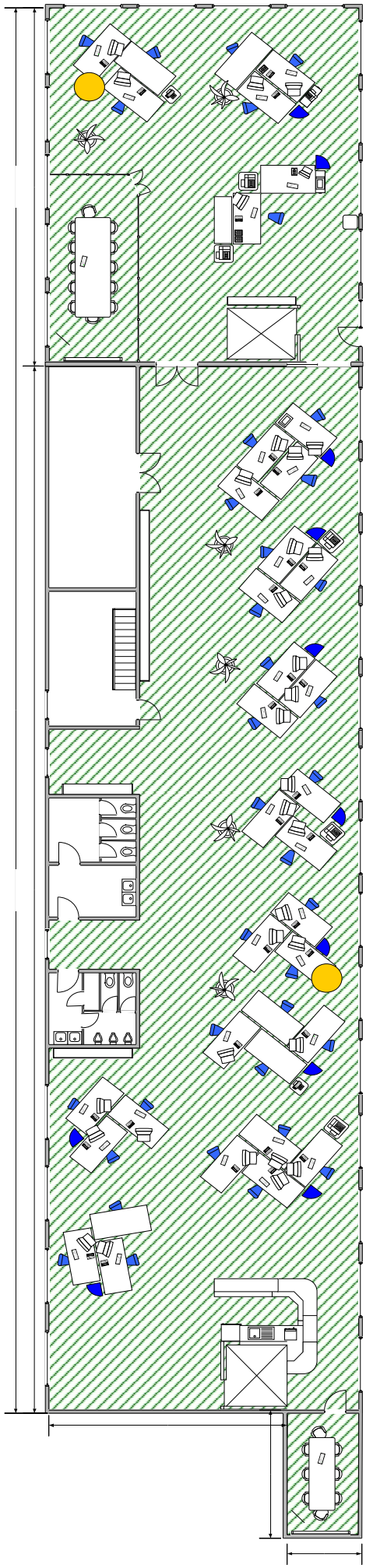


Abb.6: 3. Stockwerk mit den vorgeschlagenen Positionenen der Access Points (AP1 und AP2)

```
' Beugt Vertippern vor
Option Explicit

Private NumberOfLoops As Long

' Liefert eine Zufallszahl im Bereich RandFrom bis RandTo
' Rnd (der Zufallszahlengenerator von Visual Basic liefert eine Kommazahl im
' Bereich 0 bis 1. Diese wird mit der Höchstgrenze (RandTo) multipliziert, um eine
' Zahl im Bereich von 0 bis RandTo zu bekommen. Daraufhin wird noch die Untergrenze
' (RandFrom) addiert, damit die gelieferte Zahl dem gewünschten Zahlenbereich
' entspricht. Das Ergebnis wird noch in eine Ganzzahl konvertiert, da die
' Berechnung eine Kommazahl involviert und daher das Ergebnis eine Kommazahl wäre.

Public Function Rand(ByVal RandFrom As Long, ByVal RandTo As Long) As Long
    Rand = CLng((RandTo * Rnd) + RandFrom)
End Function

' Der Inhalt des Textfeldes txtKey wird über das globale Objekt "Clipboard",
' welches die Zwischenablage bereitstellt, als Text in selbige kopiert.

Private Sub btnCopy_Click()
    Clipboard.Clear
    Clipboard.SetText txtKey.Text
End Sub

' Unload zerstört das angegebene Objekt. Me ist ein Objekt des Type frmMain
' (das Hauptfenster dieses Programmes) und wird dadurch zerstört, was das
' Beenden des Programmes nach sich zieht.

Private Sub btnExit_Click()
    Unload Me
End Sub

' Wird aufgerufen, sobald "WEP-128 Bit" ausgewählt wird. Die Länge des Schlüssels
' muss damit 26 Zeichen betragen, welches der Einfachheit halber in der globalen
' Variablen NumberOfLoops gespeichert wird.

Private Sub rdo128_Click()
    NumberOfLoops = 26
End Sub

' Wird aufgerufen, sobald "WEP-40 Bit"  ausgewählt wird. Der Schlüssel muss hier
' allerdings nur 10 Zeichen lang sein.

Private Sub rdo40_Click()
    NumberOfLoops = 10
End Sub

' Hier wird der WEP-Schlüssel generiert. Es wird eine Schleife NumberOfLoops
' (welches in rdoXXX_Click gesetzt wurde) ausgeführt und eine Zufallszahl zwischen
' 0 und 15 (der Wertebereich einer hexadezimalen Ziffer) generiert. Diese wird dann
' in ihr Hex-Zeichen umgewandelt und an das Ergebnis (Result) angehängt. Am Ende
' wird der Wert noch in das Textfeld geschrieben.

Private Sub btnGenerate_Click()
    Dim Counter As Long
    Dim Digit As Long
    Dim Result As String: Result = ""

    For Counter = 1 To NumberOfLoops
        Digit = Rand(0, 15)
        Select Case Digit
        Case 0 To 9
            Result = Result & CStr(Digit)
        Case 10
            Result = Result & "a"
        Case 11
            Result = Result & "b"
        Case 12
            Result = Result & "c"
        Case 13
            Result = Result & "d"
        Case 14
            Result = Result & "e"
```

```
        Case 15
            Result = Result & "f"
        End Select
    Next
    txtKey.Text = Result
End Sub

' Wird beim Starten des Programms aufgerufen. Der Zufallszahlengenerator wird
' initialisiert. Standardmässig werden 128-Bit Schlüssel generiert.

Private Sub Form_Load()
    NumberOfLoops = 26
    Randomize
End Sub

' Wird aufgerufen, sobald sich der Wert in txtKey ändert. Wenn dieser gleich einer
' leeren Zeichenkette ist, wird der Kopieren-Button deaktiviert, ansonsten
' aktiviert.

Private Sub txtKey_Change()
    btnCopy.Enabled = (txtKey.Text <> "")
End Sub
```

Die Bestimmung der Identität von Benutzern und Stationen wird durch die EAP-Methode bestimmt. Die wichtigsten Methoden nutzen dazu entweder digitale Zertifikate oder Passwörter, wie die folgende Tabelle beschreibt.

EAP-Methode	Supplicant	Authenticator	Authentication Server
EAP-TLS	Zertifikat	Zertifikat	Schnittstelle zu Certification Authority
EAP-TTLS	Passwort	Zertifikat	Schnittstelle zu Certification Authority, Benutzerdatenbank
EAP-MD5	Passwort	-	Benutzerdatenbank

1) LAN – steht für Local Area Network, also ein lokales Netzwerk, an das mehrere Rechner innerhalb eines Unternehmens angeschlossen sind. Ein LAN hat eine geringe räumliche Ausdehnung und unterliegt der Verfügungsgewalt einer Firma oder Institution.

2) Wireless-LAN – abgekürzt auch WLAN genannt (im Deutschen auch Funknetz), ist eine drahtlose Anbindung an ein Netzwerk. Dadurch lässt sich beispielsweise eine Verbindung zwischen den Computern eines Unternehmens herstellen, ohne das diese über ein Patchkabel direkt miteinander verbunden sind. Das WLAN überträgt Daten per Funk entweder zwischen einem Access Point und einem Notebook oder direkt zwischen zwei Endgeräten.

3) PCMCIA-Wireless-LAN-Adapter – wird im allgemeinen auch PC-Card genannt. Einschübe für diese Karten findet man heutzutage in jedem Laptop. Die Schnittstelle ist genormt und kann verschiedene Kartentypen aufnehmen. Sie empfängt und sendet im Wireless-LAN die Datenpakete.

4) Hub – ist ein zentraler Verteiler im Netzwerk, über den man getrennte Netzwerkleitungen zusammenführen kann. Die Geräte werden einfach über eine Steckverbindung angeschlossen.

5) Switch – ist die englische Bezeichnung für einen Schalter. In der Netzwerktechnik versteht man unter einem Switch einen aktiven Hub, der wie eine Telefonvermittlungsstelle den Netzwerkverkehr zwischen Clients und Servern regelt, in dem er selbsttätig die Zieladressen der IP-Pakete auswertet und diese dann den entsprechenden Adressaten zustellt.

6) Switched – beschreibt die Vermittlungsart eines Netzwerks. Benutzer eines Netzwerks kommunizieren beliebig untereinander, wobei die Vermittlung der Datenpakete mit Hilfe von Switches realisiert wird.

7) 100BaseTx – ist eine IEEE-Spezifikation für eine Ethernet-Verkabelung, die eine Übertragungsrate von 100-MBit/s über zweipaarige UTP- und STP-Kabeln der Kategorie 5 ermöglicht.

8) Ethernet – ist das derzeit am häufigsten installierte LAN-System. Das Ethernet-Ausgangssystem 10Base5 wurde in den 70er Jahren von DEC, Intel und Xerox entwickelt und 1983 in IEEE 802.3 standardisiert.

9) Baumtopologie – ist eine so genannte Netztopologie, bei der mehrere in der Regel homogene Grundstrukturen segmentweise in vielfältiger Form entsprechend den erforderlichen Einsatzbedingungen zusammengefügt werden. Typisch ist, dass an Stelle eines Endsystems über eine Netzübergangseinheit (Bridge) ein anderes Netzsegment anschaltbar wird. Gewöhnlich werden Baumnetze aus einer Anzahl zusammengefügter Busnetze gebildet. Mit der Struktur des Baumnetzes kann unter konkreten, durch den Einsatz charakterisierten Bedingungen eine Optimierung der topologischen Struktur lokaler Rechnernetze (LAN) begünstigt werden. Baumnetze sind für Erweiterungen sehr flexibel. Bei Störungen in einzelnen Segmenten oder Netzübergängen wird der Betrieb des Gesamtsystems oft sehr eingeschränkt.

10) Cat5-Twisted Pair – beschreibt einen bestimmten Typ Netzwerkkabel, mit dem kurze Distanzen zwischen zwei Geräten überbrückt werden. Diese Verbindung ist flexibel, so dass man z.B. einen PC bei Bedarf auf dem Schreibtisch verschieben kann.

11) Internet – ist ein globales, dezentral organisiertes und strukturiertes Rechnernetz mit einheitlichem Adressierungsschema, das heute weltweit mit hohen Zuwachsraten über 300 Mio. Benutzer miteinander verbindet und neben dem ausgebauten Telefonsystem die wichtigste Basisinfrastruktur für den internationalen elektronischen Austausch von Informationen darstellt.

12) Firewall – ist die englische Bezeichnung für „Feuermauer“ oder „Brandmauer“. In der Technik beschreibt der Begriff eine Form von Hard- und/oder Software, die den Datenfluss zwischen einem privaten und einem ungeschützten Netzwerk (LAN und Internet) kontrolliert bzw. ein internes Netz vor Angriffen aus dem Internet schützt. Dazu vergleicht eine Firewall z.B. die IP-Adresse des Rechners, von dem ein empfangenes Datenpaket stammt, mit einer Liste erlaubter Sender – und weist das Paket entsprechend ab, oder lässt es in das Netz.

13) Router – beschreibt ein Rechnersystem, das eine Verbindung zu mehreren Netzwerken besitzt und Informationen zwischen diesen über eine optimale Route weiterleitet, um Netzlaufzeiten und Netzbelastung zu minimieren. Router sind ein wichtiges Bindeglied im Internet.

14) Standleitung – wird auch als Mietleitung (engl. Leased Line) bezeichnet. Eine Standleitung ist ein festgeschalteter physikalischer Übertragungsweg mit permanenter Übertragungsbereitschaft.

15) PDA – ist die Abkürzung für „Persönlicher Digitaler Assistent“ (personal digital assistant). Der PDA ist ein Computer im Westentaschenformat, und wird häufig auch als „Handheld“ bezeichnet. Die Geräte verfügen über Büro-Funktionen wie Kalender, Adress- oder Notizbuch und erlauben die digitale Kommunikation (z.B. E-Mail per Handy). Die meisten Handhelds haben außerdem ein kleine Tastatur oder einen mit einer Schrifterkennung ausgestatteten Touchscreen.

16) Ad-Hoc-Modus – ist eine mögliche Betriebsart eines Wireless-LANs (siehe 3.1.1.3.1.)

17) Funkzelle – ist der Bereich, der von einem Access Point oder einer Antenne abgedeckt wird, in dem also Netzdeckung vorhanden ist.

18) Verschlüsselung – wird auch als Kryptographierung oder Chiffrierung (engl. Encryption) bezeichnet. Verschlüsselung ist ein kryptologisches Verfahren zur Codierung von Nachrichten (im Klartext) zum Zwecke ihrer Geheimhaltung. Hierbei werden die zu verschlüsselnden Klartexte nach einer bestimmten Methode in eine scheinbar sinnlose Zeichenfolge umgewandelt, wobei die dazu verwendeten Methoden auf speziellen Verschlüsselungsverfahren (Verschlüsselungsalgorithmen) basieren.

19) MAC-Adresse – oder auch die Harwareadresse, die jedem Ethernet-System weltweit einzigartig zugeordnet ist. Die ersten 6 Bytes eines Ethernet Datenpaketes beinhalten die MAC-Adresse.

20) Provider – „to provide“ stammt aus dem englischen und bedeutet im deutschen liefern, bereitstellen oder besorgen. Es ist der Oberbegriff für einen Lieferanten oder Anbieter von Waren oder Dienstleistungen. In der Telekommunikation ist Provider eine weit verbreitete Bezeichnung für Anbieter oder Vermittler von Telekommunikationsdienstleistungen. Zusätze geben oft Hinweise auf das betreffende Marktsegment (Dienstleistungsbereich) und die betreffende Stufe der Wertschöpfungskette. Beispiele: Service Provider, Internet Service Provider (ISP), Application Provider, Internet Content Provider (ICP).

21) Bandbreite – beschreibt in der Nachrichtentechnik die Differenz zwischen der oberen und unteren Grenze einer elektrischen/elektromagnetischen Frequenz oder optischen Wellenlänge.

22) Access Point – entspricht der Zentrale einer jeden Funkzelle. Er verwaltet alle mit ihm verbundenen Clients. Es können gleichzeitig bis zu 256 Clients mit einem Access Point verwaltet werden. Die Anzahl ist jedoch Herstellerspezifisch. Der Access Point ist auch das Bindeglied zu einem bereits bestehendem IEEE 802.3 kompatiblen LAN.

23) IEEE – ist die Abkürzung für „Institute of Electric and Electronic Engineers“, ein 1963 gegründetes Institut von Elektrik- und Elektronik-Ingenieuren zur Festlegung von Normen im Netzwerkbereich, insbesondere für die Standardisierung von Bus-Topologien, Übertragungsprotokollen, der Datenübertragungsgeschwindigkeit und der Verkabelung. IEEE ist eine amerikanische Organisation. Die Standards werden dem ANSI („American National Standards Institute“) zur Billigung und Erhebung zum US-Standard vorgelegt. Die festgelegten Standards werden außerdem dem ISO („International Standardisation Organization“) zur Schaffung eines internationalen Standards vorgelegt.

24) Frequenzbereich – ist das Frequenzspektrum, angefangen bei den ultratiefen Frequenzen bis zu Frequenzen mit Mikrowellenlängen, ist eingeteilt in Bereiche mit festgelegten Frequenzgrenzen. Beim Wireless-LAN z.B. umfasst dieser Bereich 2,4 bis 2,4835 Ghz.

25) Reichweite – meint in der Funktechnik die Entfernung zwischen Sender und Empfänger(n), bis zu der mit hoher Wahrscheinlichkeit eine qualitätsgerechte Übertragung möglich ist.

26) Richtantenne – ist eine Vorrichtung zum Senden und Empfangen elektromagnetischer Wellen. Die Aufgabe der Antenne besteht in der Umwandlung der leitungsgeführten Energie des Senders in Strahlungsenergie (Sendeantenne) bzw. der Strahlungsenergie in leitungsgeführte Energie des Empfängers (Empfangsantenne). Der konstruktive Aufbau der Antenne hängt vom Anwendungsfall und vom Wellenlängenbereich (Frequenzbereich) ab.

27) Datenrate – wird allgemein auch als Übertragungsgeschwindigkeit, Bitrate oder Bitfolgefrequenz (engl. Bitrate) bezeichnet. Sie ist das Maß für die Geschwindigkeit, in der Daten in Form von Binärentscheidungen (Bits) je Zeiteinheit über ein Kommunikationssystem übertragen werden können. Die Datenrate ist das Produkt aus der Schrittgeschwindigkeit und dem Wertevorrat (Kennzustände) des betreffenden Signalparameters. Angegeben wird die Datenübertragungsrate in bit/s (Bit pro Sekunde) bzw. in den entsprechenden Zehnerpotenzen kbit/s (103 bit/s), Mbit/s (106 bit/s), Gbit/s (109 bit/s), Tbit/s (1012 bit/s), gemessen. In der englischen und amerikanischen Schreibweise verwendet man „bps“ (bits per second).

28) Personal Area Network – wird durch eine Gruppe vernetzter Geräte, z.B. einige Bluetooth-Geräte, die wechselseitig miteinander kommunizieren gebildet. Die angeschlossenen Geräte arbeiten meist im Ad-hoc-Modus. Ein solches Netzwerk ist Umgebungsunabhängig, und kann z.B. im Büro, zu Hause, im Hotel oder auch auf dem Flughafen aufgebaut werden.

29) Roaming – ist die Fähigkeit mobiler Geräte sich ohne Beeinflussung des Datenverkehrs zwischen verschiedenen Funkzellen des Netzwerkes zu bewegen. Der Roaming-Mechanismus garantiert ununterbrochene Datenübertragung. Diese Funktion wird durch die Fähigkeit des Clients erreicht, den Access Point seiner Umgebung zu wählen, der das stärkste Signal sendet.

30) Hotspot – ist englisch und beschreibt im IT-Bereich einen sensiblen Bereich (übersetzt heißer Punkt). In der Wireless-LAN-Technologie sind die Bereiche gemeint, an denen sich ein Access Point befindet.

31) Peer-to-Peer – beschreibt auf Deutsch eine so genannte Punkt-zu-Punkt-Verbindung. Angeschlossene Rechner und Systeme sind gleichberechtigt. Dies bedeutet, dass jedes System im Netz anderen Systemen Funktionen und Dienstleistungen anbieten und von anderen Systemen deren angebotene Funktionen und Dienstleistungen nutzen kann.

32) Bridge – ist englisch und heißt übersetzt Brücke. Es beschreibt ein Netzkoppelelement, das zwei oder mehrere gleichartige (homogene) Netze in der Sicherungsschicht koppelt. Dabei wird zunächst unterstellt, dass sich die zu verbindenden Netze räumlich berühren. Ist dies nicht der Fall, sind also größere Entfernungen zu überwinden, spricht man von einer Remote Bridge. Die Netzkopplung über eine Bridge ist beispielsweise dann sinnvoll, wenn die zu koppelnden Netze unterschiedliche Protokollbedingungen in der physikalischen Schicht und in der Sicherungsschicht aufweisen, in der Netzwerkschicht (Vermittlungsschicht) aber übereinstimmen; das heißt, die Netzwerkschicht kann unabhängig vom Übertragungsmedium und MAC (Medienzugangsverfahren) betrieben werden. In Bezug auf die Netzwerkschicht und die nachfolgenden Schichten arbeitet die Bridge also protokolltransparent.

33) Repeater – ist eine Hardwareorientierte Datennetzkomponente zur Verstärkung und Wiederaufbereitung von Signalen. Der Repeater wird vielfach zur Erweiterung der Übertragungsreichweite eingesetzt. Er ermöglich die physikalische Verbindung zweier LAN-Segmente desselben Typs, die auf der physikalischen Schicht des OSI-Referenzmodells identisch sind. Als Beispiel für den Repeater kann die Verbindung von Ethernet-Segmenten angesehen werden. Primäres Ziel ist dabei die Erweiterung oder die Gestaltung eines Netzes in Anlehnung an geographische Gegebenheiten. Funktionell ist der Repeater ein regenerativer Leistungsverstärker.

34) synchron – meint die zeitliche Beziehung von zwei oder mehreren Signalen, die, unabhängig von ihrer Geschwindigkeit und Frequenz eine feste Phasenbeziehung zueinander aufweisen. Diese Bedingungen liegen nur dann vor, wenn die Signale durch eine gemeinsame Taktquelle synchronisiert werden, das heißt, die Signale liegen im gleichen Zeitraster.

35) RC4 – ist ein von Ron Rivest für RSA Data Security Inc. (benannt nach Ron Rivest, Adi Shamir, Len Adleman) entwickelter Verschlüsselungsalgorithmus. Er wird auch als Stromchiffre bezeichnet. RC4 arbeitet byteorientiert mit einer variablen Schlüssellänge. Die Schlüssellänge kann von 1 bis 2048 Bit variieren. Sie ist aber oftmals in Software-Implementationen auf 40 Bit limitiert. Der RC4-Algorithmus ist nicht öffentlich verfügbar, wurde aber 1994 im Usenet durch Unbekannte veröffentlicht und findet z. B. bei der Verschlüsselung von sicheren HTTP-Verbindungen (S-HTTP) Einsatz.

36) Datenpaket – ist der Datenrahmen zur Übertragung von Nutzdaten auf virtuellen Ende-zu-Ende-Verbindungen eines paketvermittelten Netzes. Das Datenpaket besteht aus dem Paketkopf mit Kanaladresse, Paketfolgenummer usw. und dem Datenfeld zur Aufnahme der Nutzdaten.

37) Initial Vector – bedeutet auf deutsch Initialisierungsvektor und beschreibt den Startwert bei Verschlüsselungsverfahren, die einen solchen benötigen (z.B. RC4). Ein Initialisierungsvektor wird nach bestimmten Regeln mit diesem Startwert gefüllt.

38) RADIUS-Protokoll – ist ein Internet-Standard, und spielt vor allem in heterogenen Umgebungen eine wichtige Rolle. RADIUS ist ein Bestandteil von Windows 2000 und steht für „Remote Authentication Dial-in User Service“. Es ist ein für Remote-Access-Anwendungen entwickeltes Sicherheitsprotokoll, um unerlaubte externe Zugriffe auf Daten und Systeme zu verhindern. RADIUS funktioniert nach dem Client-Server-Konzept und legt die Kooperation zwischen einem AAA-Server (Authentification, Authorization and Accounting Server) und einem Network Access Server (NAS) fest. In diesem Konzept kann der AAA-Server als RADIUS-Server angesehen werden, in dem sämtliche Informationen über Remote-Benutzer zur Verfügung stehen. Der RADIUS-Client stellt ein Funktionsmodul dar, das auf dem NAS installiert wird.

39) Client – steht im englischen für Dienstnehmer. Im technischen Bereich ist damit allgemein ein Arbeitsplatzrechner gemeint, der von einem Server bereitgestellte Dienste nutzt, wie z.B. das Abrufen und Speichern von Daten.

40) AirSnort – ist ein Tool, mit dem sich Datenpakete in drahtlosen Netzwerken abfangen und entschlüsseln lassen. Mehr Infos unter: http://www.be-secure.com/airsnort.html

41) Telnet – beschreibt in der TCP/IP-Protokollarchitektur ein Anwendungsprotokoll, mit dem sich der Benutzer bei einem entfernten Rechner (Host) im Internet anmelden kann (Remote Login). Telnet realisiert eine Client-Server-Beziehung zwischen der lokalen Telnet-Software (Client) und der Software auf dem entfernten Server - d.h. der Benutzer kann sein Terminal an seinem lokalen Rechner benutzen, um auf einem entfernten Rechner zu arbeiten. Das Terminal erscheint auf dem fernen Rechner wie ein lokal angeschlossenes Terminal. Die meisten Router, Access Points, etc. unterstützen eine Konfiguration mittels Telnet.

42) Release – ist englisch und bedeutet Freigabe. Im Computerbereich wird mit diesem Begriff im Allgemeinen die Freigabe einer neuen Hard- oder Software beschrieben.

Folgende Quellen wurden für diese Projektdokumentation zu Hilfe genommen:

Q1) Vgl. Sikora, Axel.: V.: Wireless LANs im Überblick, in: WWW: http://www.tecchannel.de/hardware/750/index.html vom 05.09.2001

Q2) Vgl. Weise, Manfred.: V.: In der Welt der Funk-LAN wird gesprochen, in: WWW: http://www.computerworld.ch/domino/CWArchiv.nsf/378dd4e611038e3a412565b2005c1621/4917df0310ef7fc641256afe00489eee vom 26.10.2001

Q3) Nitzinger, René.: Whitepaper Wireless LAN Security, Rel.: draft/r2, vom 08.03.2002

Q4) Klostermann, Detlef, Dipl.-Ing.: FunkLAN im medizinischen Umfeld, vom Mai 1999

Q5) Ernst Ahlers/Dusan Zivadinovic.: Datenkuriere – 12 WLAN-Systeme für schnelle Funknetzwerke, in c't, Nr. 22/00, vom 20.10.2000

Zur Realisierung dieser Projektarbeit wurden folgende Hilfsmittel verwendet:

- Adobe Photoshop 5.5
- Microsoft Excel XP
- Microsoft Visio XP
- Microsoft Visual Basic 6
- Microsoft Word XP

Konzept: Betriebliche Projektarbeit **Prüfungsteil A**

❑ Externes Projekt

☒ Internes Projekt

Problembeschreibung (Projektbeschreibung)

In das bestehende LAN der Firma SOFT-RESEARCH GmbH & Co. KG soll zusätzlich ein Zugang über ein WLAN (Wireless-LAN) geschaffen werden. Dies ist notwendig, damit die Unabhängigkeit und Mobilität von Mitarbeiter mit einem Laptop wieder hergestellt wird. Da sich oft Außendienstmitarbeiter und Mitarbeiter anderer Filialen im Haus aufhalten, die hier im Haus keinen festen eigenen Arbeitsplatz haben, ist es notwendig, jenen Mitarbeitern schnell und unkompliziert einen Zugang zum Netzwerk zu verschaffen, ohne auf Netzwerkanschlüsse angewiesen zu sein. Ebenso wird das WLAN für die Besprechungsräume im Haus benötigt, da dort jeweils nur ein Netzwerkanschluss zur Verfügung steht, es aber bei einigen Besprechungen notwendig ist, das alle Anwesenden über einen LAN-Zugang verfügen müssen.

Projektplanung

Projektschritt	**Definition**	**Std.**
Soll/Ist-Analyse	Ermittlung des Ist-Zustands, und Erstellung des Soll-Konzepts.	3
Festlegung der technischen Anforderungen	Festlegung der technischen Anforderungen der benötigten Hardware in Zusammenarbeit mit dem Systemadministrator (z.B. Anforderungen an die Sendeleistung, die durch die Beschaffenheit des Gebäudes gegeben sind, Abhörsicherheit und Strahlenbelastung)	5,5
Festlegung des Finanzrahmens	Im Gespräch mit dem Leiter der Finanzabteilung wird das Budget festgelegt, welches für dieses Projekt zur Verfügung steht.	1,5
Einholen von Angeboten	Suche nach Angeboten die die Anforderungen erfüllen (u.a. Web-Recherche).	6
Angebotsauswahl/Kalkulation	Vergleich der Angebote nach finanziellen und technischen Aspekten und Auswahl der Hardware, die für die Anforderungen am besten geeigneten ist (Angebotsvergleich).	6
Präsentation	Erstellen einer Präsentation zur Darstellung der Fakten und Ergebnisse. Diese ist dann Grundlage zur Entscheidungsfindung.	4
Dokumentation	Erstellen der Projektdokumentation	7
Geplanter Zeitaufwand in Std.		**33**

! Höchstens 35 Stunden / **nur** Fachinformatiker, Anwendungsentwicklung 70 Stunden

Projektdokumentation

- Soll/Ist-Analyse
- Technische Anforderungen und finanzieller Rahmen
- Angebotsvergleich der eingeholten Angebote
- Auswahl von 2 Angeboten
- Vergleich: technische Details der beiden Angebote
- Fazit

! Unterschrichene Positionen werden nicht von mir selbst erstellt. Sie dienen aber dem Gesamtverständnis des Projektes.

René Fischer

Unterschrift

Prüf-Nr. **20816**