ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Chris Welti
Beat Döbeli

Empfehlungen zur

Kabellosen Vernetzung von Computern an Schulen

2. Auflage

September 2001

Einleitung

Wireless LAN (kurz WLAN) scheint eine Wunderlösung (auch) für Schulen zu sein! Allerorten werden die Einfachheit, Mobilität und Geschwindigkeit gelobt. Man müsse keine Kabel verlegen – Funksysteme seien schnell zu installieren, und sie überbrückten im Handumdrehen auch Gebäude- oder Grundstücksgrenzen und ermöglichten so Internetzugang auf dem ganzen Schulhausgelände. In denkmalgeschützten Gebäuden mit entsprechenden Bauauflagen dürften sie gar die einzig mögliche LAN-Technologie darstellen. Ausserdem sollen sie sich hervorragend für vorübergehende Vernetzung eignen, etwa für eine spezielle Unterrichtsstunde: Keine störenden Kabel, über welche die Schüler stolpern, weniger Rechner, da die Stationen ja alle mobil sind...
So die Idealvorstellung. Doch wie sieht es in der Realität aus?

Worum geht es in diesem Leitfaden?

Dieser Leitfaden zeigt in übersichtlicher Weise die für Schulumgebungen wichtigsten Eigenheiten von WLAN auf, um einen Entscheid pro/contra WLAN zu ermöglichen. Funknetzwerke sind nicht für jeden Einsatzzweck geeignet: Die gegenüber modernen drahtgebundenen Netzen sehr geringe Geschwindigkeit und die kaum vorhandene Sicherheit gegen Mithörer stellen die wohl grössten Einschränkungen dar.

Was bieten wir?

Was genau bietet WLAN? Wo liegen die Unterschiede zum herkömmlichen LAN? Wo liegen die Tücken bei Beschaffung, Installation und Betrieb? Wir bieten 29 Empfehlungen, die Hilfestellung bei der Beschaffung und dem Betrieb eines WLAN geben sollen. Diese sind thematisch geordnet nach dem üblichen Ablauf einer Beschaffung (s. nächste Seite).
Aufgrund der raschen technologischen Entwicklung wurde bewusst auf system- und produktspezifische Details verzichtet.

Wen sprechen wir an?

- InformatikverantwortlicheundSystembetreuerInnen von Schulen
- Schulleitungen und Schulbehörden

Grundbegriffe der Netzwerktechnik werden als bekannt vorausgesetzt.

Hintergrund

Dieser Leitfaden ist das Ergebnis einer Semesterarbeit von Chris Welti am Departement Informatik der ETH Zürich unter der Leitung von Prof. Dr. C. A. Zehnder und Beat Döbeli. Die Empfehlungen stützen sich neben intensiven Internetrecherchen auf Interviews mit Fachleuten aus Schweizer Schulen und WLAN-Projekten an der ETH Zürich.

Bezug des Dokuments

Dieser Leitfaden kann kostenlos als PDF-Dokument per Internet unter

http://www.educeth.ch/informatik/berichte/wireless/

bezogen werden.

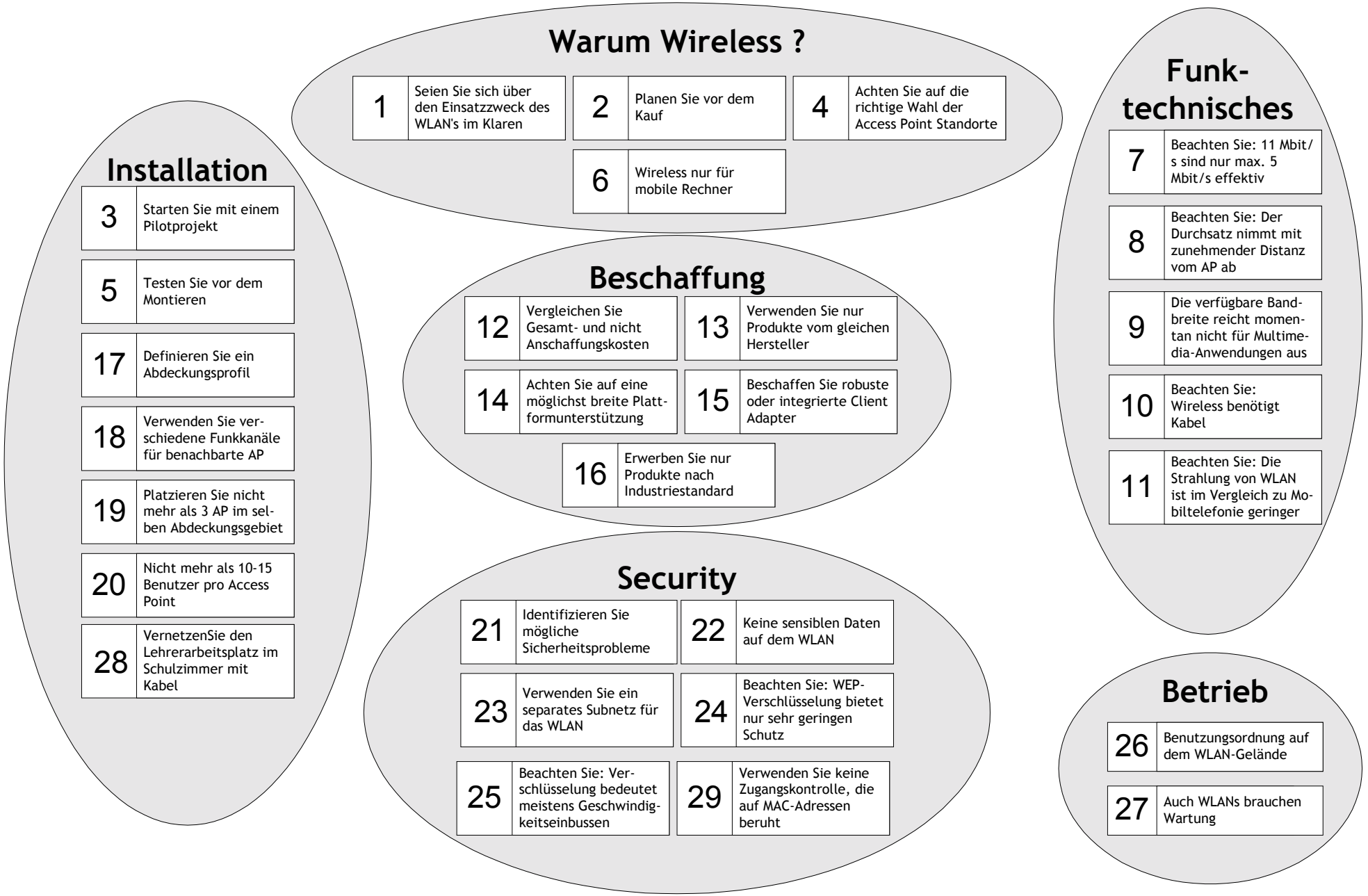
Feedback

Wir sind an konstruktiven Anregungen, Bemerkungen und Erfahrungsberichten interessiert. Bitten senden Sie Ihre Kommentare per E-Mail an:

doebeli@inf.ethz.ch

Änderungen in der 2. Auflage

In der 2. Auflage sind die Sicherheitsempfehlungen aufgrund der gebrochenen WEP-Verschlüsselung angepasst sowie die Empfehlungen 28 und 29 hinzugefügt worden.


Warum Wireless ?
1 Seien Sie sich über den Einsatzzweck des WLAN's im Klaren
2 Planen Sie vor dem Kauf
4 Achten Sie auf die richtige Wahl der Access Point Standorte
6 Wireless nur für mobile Rechner
Installation
3 Starten Sie mit einem Pilotprojekt
5 Testen Sie vor dem Montieren
17 Definieren Sie ein Abdeckungsprofil
18 Verwenden Sie verschiedene Funkkanäle für benachbarte AP
19 Platzieren Sie nicht mehr als 3 AP im selben Abdeckungsgebiet
20 Nicht mehr als 10-15 Benutzer pro Access Point
28 VernetzenSie den Lehrerarbeitsplatz im Schulzimmer mit Kabel
Beschaffung
12 Vergleichen Sie Gesamt- und nicht Anschaffungskosten
13 Verwenden Sie nur Produkte vom gleichen Hersteller
14 Achten Sie auf eine möglichst breite Plattformunterstützung
15 Beschaffen Sie robuste oder integrierte Client Adapter
16 Erwerben Sie nur Produkte nach Industriestandard
Security
21 Identifizieren Sie mögliche Sicherheitsprobleme
22 Keine sensiblen Daten auf dem WLAN
23 Verwenden Sie ein separates Subnetz für das WLAN
24 Beachten Sie: WEP-Verschlüsselung bietet nur sehr geringen Schutz
25 Beachten Sie: Verschlüsselung bedeutet meistens Geschwindigkeitseinbussen
29 Verwenden Sie keine Zugangskontrolle, die auf MAC-Adressen beruht
Funk-technisches
7 Beachten Sie: 11 Mbit/s sind nur max. 5 Mbit/s effektiv
8 Beachten Sie: Der Durchsatz nimmt mit zunehmender Distanz vom AP ab
9 Die verfügbare Bandbreite reicht momentan nicht für Multimedia-Anwendungen aus
10 Beachten Sie: Wireless benötigt Kabel
11 Beachten Sie: Die Strahlung von WLAN ist im Vergleich zu Mobiltelefonie geringer
Betrieb
26 Benutzungsordnung auf dem WLAN-Gelände
27 Auch WLANs brauchen Wartung

Inhaltsverzeichnis

Vorbemerkung 1 Was verstehen wir unter kabelloser Vernetzung ?

Wir betrachten in diesem Leitfaden nur Wireless LAN („WLAN"), die mit Funktechnik arbeiten. Weder Infrarot- noch Wireless WAN (Wide Area Network) Produkte werden berücksichtigt.

Unter einem Wireless LAN („WLAN") verstehen wir ein kabelloses lokales Netzwerk, das im Unterschied zu einem drahtgebundenen LAN Daten per Funk überträgt. Systeme für Übertragungen im Weitbereichsverkehr sowie Systeme die mit Infrarot arbeiten, werden hier nicht berücksichtigt.

Client Adapter (CA):

Wie eine herkömmliche Netzwerkkarte ermöglicht der CA den Anschluss ans Netzwerk. Da wir uns hier in einer Funkumgebung befinden, enthält jeder CA anstatt eines Kabelanschlusses eine Antenne. CA sind als PCI-Karte, PCMCIA-Slot Karte und USB Version erhältlich. Besonders empfehlenswert sind direkt in Notebooks integrierte WLAN-Adapter. Diese bieten gegenüber den anderen Versionen einerseits eine bessere Antenne, wodurch sich die Reichweite erheblich verbessert; andererseits ist durch die Integration die Beschädigungsgefahr viel kleiner.

Access Point (AP):

Gerät, das den Datenverkehr von allen Stationen entgegennimmt bzw. an alle Stationen verteilt, bzw. ans LAN weiterleitet. Enthält meistens einen Anschluss für Ethernet LAN (RJ45, 10/100 Mbit/s). Einzelne Modelle enthalten auch einen integrierten Router mit ISDN oder 56K Modem, der direkte Einwahl zu einem Internet Provider ermöglicht. Wird normalerweise an die Decke montiert. Entspricht einem Hub in einem LAN.

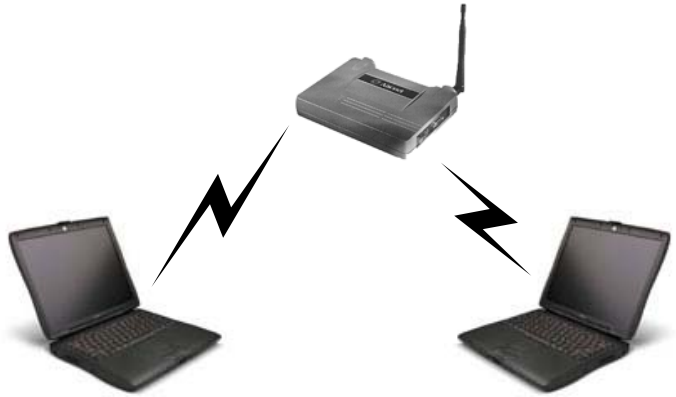
Extension Point (EP):

Funktioniert ähnlich wie ein Verstärker, erweitert das Abdeckungsgebiet eines AP. Hat keinen herkömmlichen RJ45 Ethernet LAN Anschluss. Wird jedoch nur selten eingesetzt, da sich die Übertragungsgeschwindigkeit reduziert und die Verzögerungszeiten zunehmen.

Ad-Hoc Modus: Peer to Peer WLAN:

Es werden nur CA eingesetzt. Der Datenverkehr erfolgt direkt zwischen den einzelnen CA, ohne über einen AP zu gehen. Eine spezielle Konfiguration der CA ist in diesem Fall nicht nötig. Die Reichweite ist jedoch eingeschränkt (ca. 20-30 m) und ein Zugriff auf ein bestehendes Wired LAN ist nicht möglich. Es kann nur auf die Ressourcen der sich in Reichweite befindlichen CA zugegriffen werden.

Infrastruktur-Modus: WLAN mit einem AP:



Jeglicher Datenverkehr wird zuerst vom Client zum AP übertragen und von dort aus an alle übrigen angeschlossenen Stationen weitergeleitet. Gegenüber einer Peer to Peer Konfiguration wird rund eine Verdoppelung der Reichweite erreicht. Es ist je nach Umgebung eine Abdeckung im Umkreis von ca. 20-100 m möglich.

Infrastruktur-Modus mit mehreren AP:

Die einzelnen AP werden über einen Hub bzw. Switch miteinander verbunden (über Kabel !). Eine umfassende Abdeckung eines gesamten Gebäudes, mit nahtlosem, unterbruchsfreiem Übergang zwischen den einzelnen APs („Roaming“) ist somit möglich. (Sofern sich die Abdeckungsgebiete der APs leicht überschneiden !)

Airport / Wavelan:

Airport und Wavelan sind Produktbezeichnungen für IEEE 802.11 Produkte der Firmen Apple bzw. Lucent/Orinoco.

Weitere Fachbegriffe finden Sie im Glossar.

Quellen / Weiterführende Literatur:

Introduction to Wireless LANs
http://www.wlana.com/intro/introduction/customer.html

Introduction to Wireless LANs (II)
http://www.wireless-nets.com/whitepaper_wireless_lan_intro.htm

What is a Wireless LAN ?
http://www.proxim.com/wireless/whiteppr//whatwlan.shtml

How WLANs Work
http://www.wlana.com/intro/introduction/work2.html

Wireless Local Area Networks (WLAN)
http://www.pcs-tech.com/body_wlan.htm

Vorbemerkung 2 Wir geben keine Einführung in Netzwerktechnik

Erläuterungen zu netzwerkspezifischen Themen werden in diesem Leitfaden bewusst ausgelassen. Wireless LANs unterscheiden sich von „normalen", drahtgebundenen LANs durch die Verwendung von Funktechnik anstelle von Kabel zur Bitübertragung. Daher wird ein grundlegendes Verständnis von Netzwerktechnik vorausgesetzt.

Weiterführende Literatur:

Andrew Tanenbaum, Computernetzwerke, 3. Auflage

Vorbemerkung 3 Beachten Sie auch unsere anderen Broschüren!

Sie halten die erste Auflage unserer „Wirelessbroschüre" in den Händen. Diese Broschüre ist ein Folgeprodukt des Leitfadens zu „Beschaffung und Betrieb von Informatikmitteln an allgemeinbildenden Schulen".

Wartungsbroschüre

In der 1999 erstmals veröffentlichten Broschüre „Empfehlungen zur Wartung von Informatikmitteln an allgemeinbildenden Schulen" haben wir allgemeine Empfehlungen zu Beschaffung und Betrieb von Informatikmitteln im Schulbereich gesammelt. Diese werden hier nicht wiederholt, lassen sich aber auch im WLAN-Bereich umsetzen. Als Ergänzung zur vorliegenden Wirelessbroschüre lohnt sich deshalb die Lektüre der Wartungsempfehlungen. Sie können als PDF-Dokument unter der Adresse

http://www.educeth.ch/informatik/berichte/wartung/

kostenlos bezogen werden.

Weitere Broschüren

Das Interesse und die Rückmeldungen zur ersten Auflage des Wartungs - Leitfadens haben unsere Absicht bekräftigt, weitere Empfehlungen im Umfeld Schule und Informatik zu erarbeiten. Weitere Themen sind geplant.

Aktuelle Informationen über unsere Empfehlungen finden Sie unter

http://www.educeth.ch/informatik/berichte/

Empfehlung 1 Seien Sie sich über den Einsatzzweck des WLANs im Klaren

WLAN bietet nicht nur Vorteile! Der Einsatzzweck und die Bedürfnisse der Benutzer sollten als erstes abgeklärt werden.

Bevor Sie ein WLAN planen oder einrichten, sollten Sie sich darüber klar werden, wozu es eingesetzt werden soll:

- Mobilität von Notebooks erhöhen ?
- Vernetzung in schwierigem Umfeld (Asbest, Denkmalschutz)
- Vernetzung zweier Gebäude über eine Strasse oder fremden Boden

Die Vor- und Nachteile eines WLANs gegenüber einem drahtgebundenen LAN sollten sorgfältig gegeneinander abgewägt werden.

Der Einsatz von WLANs für den mobilen Zugriff auf Netzwerkressourcen (z.B. Internet) ist empfehlenswert, solange die Anforderungen an die Übertragungsgeschwindigkeit und Verzögerungszeit gering sind.

Normalerweise ist für Stationen mit festem Standort eine Verkabelung gegenüber dem Einsatz von WLAN-Technologie vorzuziehen, da eine viel bessere Performance mit weniger technischen Problemen erreicht werden kann. Der Einsatz von WLAN Technologie ist allenfalls für entfernte stationäre Rechner, deren Verkabelung zu teuer wäre, gerechtfertigt.

	Kupfer-Kabel LAN (802.3) Fast Ethernet	Wireless LAN IEEE 802.11b	Wireless LAN 802.11a / Hyperlan2 (ca. 2002)
Verkabelungskosten	Hoch	gering	gering
Hardwarekosten	niedrig	hoch	hoch
Sicherheit	rel. hoch (switched)	gering	gering
Reichweite	150 m	25-100 m	25-100 m
Nominalbandbreite	100 Mbit/s	11 Mbit/s	22-55 Mbit/s
Durchsatz	~90 Mbit/s	~5 Mbit/s	10-25 Mbit/s
Verzögerung	sehr niedrig	mittel	mittel
Zuverlässigkeit	Hoch	rel. gering	rel. gering
Strahlung	Praktisch keine	gering	gering

Tabelle 1: Vergleich aktueller LAN-Technologien

Empfehlung 2 Planen Sie vor dem Kauf

Ein kleines, temporäres WLAN mit einem einzigen AP mag relativ schnell eingerichtet sein. Für eine permanente Installation ist jedoch eine sorgfältige Planung unumgänglich!

Auch nachdem man den Entschluss gefasst hat, ein WLAN einzusetzen, gibt es weitere Dinge die man beachten sollte:

- **Abdeckungsprofil:** Eine Gebäudekarte mit der benötigten Muss- und Soll– Abdeckung (unbedingt nötig <-> erwünscht) ermöglicht das ungefähre Abschätzen der Anzahl benötigter APs. Die genaue Anzahl ist aber erst nach praktischen Tests eruierbar.
- **Anzahl Benutzer für ein bestimmtes Gebiet:** Sollen mehr als 15-20 Benutzer gleichzeitig auf einen AP zugreifen müssen, oder ein erhöhter Bandbreitebedarf herrschen, kann es sinnvoll sein, parallel weitere AP im selben Gebiet zu installieren.

Diese Angaben sollten Ihnen helfen, die benötigte Anzahl der zu erwerbenden AP abzuschätzen. Testen Sie in jedem Falle vor dem Kauf, ob Ihre Anforderungen erfüllt werden.

Verwandte Empfehlungen:

Empfehlung 3: Starten Sie mit einem Pilotprojekt
Empfehlung 4: Achten Sie auf die richtige Wahl der Access Point Standorte
Empfehlung 17: Definieren Sie ein Abdeckungsprofil
Empfehlung 18: Verwenden Sie verschiedene Funkkanäle für benachbarte APs
Empfehlung 19: Platzieren Sie nicht mehr als 3 AP im selben Abdeckungsgebiet

Empfehlung 3 Starten Sie mit einem Pilotprojekt

Der Einstieg in die WLAN-Welt mittels eines kleinen Pilotprojektes hilft Ihnen, die anfänglichen Kosten klein zu halten und Erfahrungen zu sammeln, ohne unter Druck zu stehen.

Beginnen Sie klein. Testen Sie zuerst in einem kleinem Teilgebiet. Mit einer äusserst eingeschränkten Benutzergruppe. Treten dann Probleme auf, so ist der Betroffenenkreis eingeschränkt und der dadurch entstehende Schaden gering. Zudem werden Sie nicht mit Fragen überflutet. Der Wartungs- und Support-Aufwand hält sich in Grenzen. Nicht zuletzt sind so auch Beschaffungskosten tief.

Testen Sie unter realen Nutzungsbedingungen. Sonst ergeben sich eventuell beim produktiven Einsatz neue Probleme, die im Testbetrieb nicht festgestellt werden konnten.

Es ist empfehlenswert, ein WLAN Schritt für Schritt aufzubauen. Sobald ein Bereich ohne Fehler in Betrieb ist, kann eine Erweiterung durchgeführt werden.

Verwandte Empfehlungen:

Empfehlung 2: Planen Sie vor dem Kauf

Empfehlung 5: Testen Sie vor dem Montieren

Empfehlung 4 Achten Sie auf die richtige Wahl der Access Point Standorte

Folgende Punkte spielen bei der Wahl von AP-Standorten eine Rolle:

- Funkabdeckung
- Leichte Erreichbarkeit (Wartung)
- Schutz vor Sabotage und Diebstahl
- Benötigte Verkabelung bis zum AP

Die Montage von AP's an leicht zugänglichen Orten hat den Vorteil, dass bei Problemen Manipulationen an den AP's (Reset) rasch und unkompliziert vorgenommen werden können.

Die Gefahr von Diebstahl und Sabotage darf aber bei der Wahl von AP-Standorten nicht vernachlässigt werden !

Diebstahl lässt sich durch Diebstahlsicherungen erschweren, Sabotageakte sind jedoch nur sehr selten durch bauliche Massnahmen zu unterbinden.

Verwandte Empfehlungen:

Empfehlung 1: Seien Sie sich über den Einsatzzweck des WLANs im Klaren

Empfehlung 5 Testen Sie vor dem Montieren

Glauben Sie bei WLAN weder den Herstellerangaben noch den Erfolgsmeldungen anderer Installationen! Testen vor Ort unter realen Bedingungen ist unumgänglich.

Sowohl Reichweite als auch Durchsatz variieren je nach Produkt und Hersteller. Die Bausubstanz und sonstige Hindernisse haben ebenfalls einen grossen Einfluss auf die Reichweite von Funkwellen. Bevor Sie zu Bohrmaschine und Meissel greifen, um Geräte fix zu montieren und Kabel zu verlegen, sollten Sie das WLAN ausgiebig unter den zu erwartenden Nutzungsbedingungen testen.

Vereinbaren Sie mit Ihrem Händler einen Testbetrieb von einigen Wochen. Falls Ihr Händler von seinem Produkt überzeugt ist, sollte es eigentlich ein Leichtes sein, ihn von einer solchen Testphase zu überzeugen. Falls nicht, sollten Sie sich vielleicht einen neuen Händler suchen.

Beginnen Sie beim Testen mit einem AP. Wenn diese Konfiguration zuverlässig funktioniert, können bei Bedarf zusätzliche APs in den Test integriert werden.

Arbeiten Sie mit Schnur und Klebeband. Erst wenn das Netz stabil funktioniert, wird definitiv montiert.

Verwandte Empfehlungen:

Empfehlung 3 Starten Sie mit einem Pilotprojekt

Empfehlung 6 Wireless nur für mobile Rechner

Kupferkabel bieten dem Benutzer dedizierte Leitungen und Übertragungsraten von momentan 100 Mbit/s zu einem sehr attraktiven Preis. Wo eine Funkverbindung aus Gründen der Mobilität oder der zu hohen Installationskosten nicht benötigt wird, ist eine feste Verkabelung vorzuziehen.

Setzen Sie für festinstallierte Rechner eine normale, drahtgebundene LAN Verkabelung ein. Sie erhalten eine viel höhere Übertragungskapazität (bis zu 1 Gbit/s), eine viel geringere Fehlerrate und höhere Sicherheit. WLAN bietet dagegen eine höhere Mobilität und Flexibilität. Bei fix montierten Rechnern sind diese Vorteile hinfällig.

Es ist, wenn immer möglich, eine Verkabelung vorzuziehen. Ausnahmen bilden Orte, an denen Kabel aus technischen, finanziellen oder rechtlichen Gründen nicht möglich sind (Asbestwände, Denkmalschutz etc.)

Auch das Verbinden eines Rechners in einem nahegelegenen Gebäude mit dem eigenen LAN über einen WLAN AP und eine Client Card ist in diesem Zusammenhang nochmals zu überdenken.

Sollte trotzdem ein Funknetz eingesetzt werden, ist unbedingt eine Richtstrahlantenne einzusetzen, um den ungewollten Abstrahlbereich minimal zu halten (Mithörer). Grundsätzlich ist der WLAN Einsatz nur für Notebooks beziehungsweise mobile Desktopstationen zu empfehlen. Setzen Sie sonst wo immer möglich Kupferkabel oder Glasfaser ein.

Verwandte Empfehlungen:

Empfehlung 1: Seien Sie sich über den Einsatzzweck des WLANs im Klaren

Empfehlung 7 Beachten Sie: 11 Mbit/s sind im Maximum nur ca. 5 Mbit/s effektiv

Die Übertragungsgeschwindigkeit von 11 Mbit/s beim WLAN Standard 802.11b ist nur eine Rohdatenrate. Der im realen Betrieb nutzbare Datendurchsatz beträgt maximal 5 Mbit/s.

Obwohl in allen Werbebroschüren und Medienberichten beim WLAN Standard 802.11b immer von 11 Mbit/s gesprochen wird, stehen effektiv nur maximal 5 Mbit/s an nutzbarer Bandbreite zur Verfügung. Das liegt vor allem am eingesetzten Zugriffsprotokoll CSMA/CA. Dieses Verfahren soll die Kollision von Datenpaketen verhindern, führt jedoch zu relativ langen Wartezeiten vor dem Senden eines Paketes. Dadurch geht ein grosser Teil der theoretisch verfügbaren Bandbreite verloren. Ein weiterer Grund sind die gegenüber drahtgebunden LANs hohen Fehlerraten, die bei der Funkübertragung auftreten.

Die besagten 5 Mbit/s sind nur bei optimalem Empfang und einem einzigen verbundenen Benutzer erreichbar.

Verwandte Empfehlungen:

Empfehlung 8 Beachten Sie: Der verfügbare Durchsatz nimmt mit zunehmender Distanz vom AP ab

Quellen / Weiterführende Literatur:

iX 1/2001, S.50, c't 18/2001, S 127

Empfehlung 8 Beachten Sie: Der verfügbare Durchsatz nimmt mit zunehmender Distanz vom AP ab

So banal das tönen mag; Sie haben bei einem WLAN nur optimalen Durchsatz, wenn Sie direkte Sichtverbindung zum AP haben und nicht zu weit weg sind. Je weiter Sie sich vom AP entfernen, desto schwächer wird das übertragene Signal und entsprechend sinkt der Datendurchsatz. Deshalb ist der AP an möglichst zentraler Stelle zu montieren.

Durch Dämpfung wird das übertragene Signal geschwächt und es treten Fehler bei der Decodierung auf, worauf das System mit einer niedrigeren Datenübertragungsrate reagiert.

Verwandte Empfehlungen:

Empfehlung 4: Achten Sie auf die richtige Wahl der Access Point Standorte

Empfehlung 7: Beachten Sie: 11 Mbit/s sind im Maximum nur ca. 5 Mbit/s effektiv

Quellen / Weiterführende Literatur:

c't 18/2001, S. 134-136

Empfehlung 9 Beachten Sie: Die verfügbare Bandbreite reicht (momentan) nicht für Multimedia-Anwendungen aus

Aufgrund der relativ geringen realen Durchsatzraten von WLAN's und den diesbezüglichen hohen Anforderungen von Multimedia-Anwendungen ist ein Einsatz von WLAN-Technologie für diese Zwecke nicht zu empfehlen.

Für Multimedia-Anwendungen wie z. B. Videoübertragungen ist die momentan verfügbare Bandbreite zu gering. Vor allem ist beim gleichzeitigen Zugriff von vielen Benutzern auf dasselbe Medium ist ein rapides Absinken der Bandbreite pro Person zu beobachten. Das bedeutet, dass beispielsweise ein WLAN für den Unterricht, in dem viele Schüler praktisch gleichzeitig auf ein bestimmtes Programm zugreifen, meistens ungeeignet ist. Es gibt inzwischen zwar Produkte, die sich diesem Problem angenommen haben und höhere Bandbreiten (ca. 24 - 54 Mbit/s) und Quality of Service (QoS) – Garantien aufweisen, jedoch entsprechen diese nicht der 802.11b Norm. Somit ist man dann auf den jeweiligen Hersteller alleine angewiesen und kann nicht im Problemfall auf Konkurrenz-Produkte ausweichen, ohne die gesamte Installation zu erneuern.

Das Laden von Programmen über das Netz oder gar das Kopieren ganzer System-Images über ein WLAN ist nicht zu empfehlen.

Die effektiv erreichbare Durchsatzrate von 5 Mbit/s entspricht nur 625 KByte/s. Dies ist in etwa mit der Übertragungsrate eines 4x CD-ROMs vergleichbar.
Insbesondere beim Einsatz von Multimedia-Lern-Programmen, welche meistens gewisse Minimalanforderungen an die Übertragungsrate stellen

(Bild, Ton, Video), muss die im Gegensatz zu geswitchtem Ethernet geringe Übertragungsrate übers WLAN im Auge behalten werden.

Verwandte Empfehlungen:

Empfehlung 1: Seien Sie sich über den Einsatzzweck des WLANs im Klaren

Empfehlung 7: Beachten Sie: 11 Mbit/s sind im Maximum nur ca. 5 Mbit/s effektiv

Empfehlung 8: Beachten Sie: Der verfügbare Durchsatz nimmt mit zunehmender Distanz vom AP ab

Quellen / Weiterführende Literatur:

iX 1/2001, S.50

Empfehlung 10 Beachten Sie: Wireless benötigt Kabel

Trotz Funktechnologie lassen sich Verkabelungen mit WLAN nicht ganz vermeiden. Ein Access Point braucht mindestens ein Stromkabel; bei mehreren AP mit Roaming sind zusätzlich noch Netzwerkkabel erforderlich. Einzig im Ad-hoc-Modus, wo nur die CA untereinander kommunizieren, werden keine zusätzlichen Kabel benötigt.

WLANs werden meistens als eine Ergänzung zum bestehenden LAN eingesetzt. Da das WLAN mit dem LAN verbunden werden muss, ist mindestens ein Netzwerkkabel vom Access Point zum LAN nötig. Allgemein kann man sagen, dass für jeden eingesetzten AP ein Netzwerkabel benötigt wird, nämlich um die Access Points miteinander zu verbinden (via Hub/Switch), um ein Roaming zu ermöglichen; Deshalb sollte bei einer Neuverkabelung grundsätzlich jedes Zimmer mit mindestens einem Netzwerkanschluss versehen werden. Hinzu kommt natürlich, dass jeder AP auch ein Stromkabel besitzt. Also gibt es zu jedem AP sicher zwei Kabel. Zudem sind die Kabelschächte meistens nicht gerade dort, wo man Sie haben möchte. Für APs wäre ein Kabelschacht mit Deckenzugang ideal, da diese meistens an der Decke montiert werden.

Also: Pro AP eine Strombuchse + ein Netzwerkanschluss

(Einige Anbieter liefern spezielle Adapter, bei denen die AP über das Netzwerkkabel mit Strom versorgt werden können.)

Empfehlung 11 Beachten Sie: Strahlung des WLANs im Vergleich zu Mobiltelefonie geringer

Diskussionen über die Schädlichkeit der Strahlung von WLANs sind kaum zu vermeiden. Es soll hier nur darauf hingewiesen werden, dass sich bei Benutzung von Mobiltelefonen im selben Einsatzgebiet, die Frage nach der Schädlichkeit von WLANs eigentlich erübrigt.

Es gibt noch sehr wenige Untersuchungen zu Gesundheitsrisiken von Funknetzwerken. Die Mehrheit der bisher veröffentlichten Berichte stützen sich auf Versuche mit Funkwellen im Bereich der Mobiltelefone (900/ 1800 Mhz), wobei als Versuchstiere meistens Ratten eingesetzt werden.

Bis jetzt gibt es noch keine wissenschaftliche Studie die belegt, dass WLAN-Funkwellen im 2.4 Ghz Bereich eine für den Menschen schädliche Wirkung haben.

Natürlich ist eine solche nicht auszuschliessen, jedoch sollte man Folgendes beachten:

- Die sich heute im Verkauf befindlichen WLANs weisen im Vergleich zu den Mobiltelefonen eine deutlich geringere Strahlungsemission auf (WLAN: ca. 1 bis 30mW, Mobiltelefone: 1-2 Watt). Also bis zu einem Faktor 1000 kleiner !
- Während beim Handy während der gesamten Gesprächsdauer eine konstante Strahlungsleistung herrscht, beschränkt sich der Datenverkehr in WLANs zumeist auf kurzzeitige Anhäufungen, wobei zwischenzeitlich praktisch keine Strahlung abgegeben wird. Ausserdem ist beim Benutzen von Mobiltelefonen die Antenne nur wenige mm vom Kopf entfernt, während beim WLAN-Adapter immerhin 20-30cm dazwischen sind. (Wobei die Strahlenintensität mit $1/r^2$ abnimmt)

Quellen / Weiterführende Literatur:

Do Wireless LANs pose a health or safety risk to the consumer ?
http://www.wlana.org/resource/lan_health_risk.html

Empfehlung 12 Vergleichen Sie Gesamt- und nicht Anschaffungskosten

Obwohl die Beschaffungskosten für WLAN-Equipment noch höher sind als die für drahtgebundene LANs, kann der Einsatz von WLANs durch geringere Installations- und Betriebskosten durchaus auch günstiger sein.

WLAN-Adapter sind im allgemeinen teurer als herkömmliche Ethernet-Karten für drahtgebundene LANs. Obwohl die Preise für WLAN-CA am fallen sind (speziell bei integrierten CA), werden WLAN-Produkte vermutlich immer teurer bleiben als die drahtgebundenen Pendants. Ausserdem werden WLAN-Karten immer langsamer bleiben als entsprechende drahtgebundene Produkte. Sie sollten jedoch beachten, dass zu den Anschaffungskosten noch der Installationsaufwand (Verkabelung) und die Betriebskosten hinzukommen. Je nach Gebäude und benötigter Installation kann dieser Betrag durchaus ins Gewicht fallen.

Es ist zu erwarten, dass die nächste Generation von WLAN Geräten nach dem 802.11a Standard (~ 24 Mbit/s) bzw. Hiperlan-Norm (~54 Mbit/s) in etwa 1-3 Jahren zu ähnlichen Preisen erhältlich sein wird. Diese werden NICHT abwärtskombatibel sein, da sie im Bereich von 5 Ghz arbeiten. Sie werden dann also wahrscheinlich sowohl neue AP als auch CA benötigen.

Verwandte Empfehlungen:

Wartung 5: Kaufen Sie Qualität!

Wartung 6: Beachten Sie: Computerkosten ≠ Beschaffungskosten

Empfehlung 13 Verwenden Sie nur Produkte vom gleichen Hersteller

WLAN ist eine junge Technologie. Trotz Standardisierung arbeiten Geräte unterschiedlicher Hersteller nicht immer problemlos zusammen. Verwenden Sie daher möglichst nur Produkte vom selben Hersteller oder testen Sie die Kompatibilität vor dem Kauf.

Unglücklicherweise treten trotz Standardisierung (z.B. 802.11b für die aktuellsten Produkte) noch Schwierigkeiten bei der Kommunikation von Produkten unterschiedlicher Hersteller auf (z.B. bei Roaming, WEP, Ad-Hoc Modus). Es ist deshalb von Vorteil, sich beim Kauf möglichst auf einen Hersteller zu beschränken. Weitere Gründe, weshalb Sie möglichst homogene Produkte einsetzen sollten finden Sie in Wartung Empfehlung Nr.2.

Eine Kompatibilitätsliste mit WLAN-Produkten verschiedener Hersteller finden sie unter www.wi-fi.com.

Verwandte Empfehlungen:

Wartung 2: Halten Sie Ihren Computerpark so homogen wie möglich

Quellen / Weiterführende Literatur:

Wireless Ethernet Compatibility Alliance (WECA) http://www.wi-fi.com
iX 1/2001, c't 18/01

Empfehlung 14 Achten Sie auf eine möglichst breite Plattformunterstützung

Die Unterstützung vieler Plattformen durch das Produkt eines Herstellers erleichtert den Einsatz in heterogenen Umgebungen wesentlich.

Stellen Sie sich vor, Sie schaffen sich jetzt ein WLAN an, das nur Ihren jetzt installierten Rechnertyp unterstützt. In einem Jahr stellen Sie fest, dass Sie für eine bestimmte Anwendung neue Rechnertypen benötigen, die jedoch nicht von ihrem WLAN-Hersteller unterstützt werden. Jetzt bleibt Ihnen kaum etwas anderes übrig, als das ganze WLAN neu zu installieren, bzw. die AP und CA auszutauschen. Sie tun also gut daran, schon von Anfang an auf weitere Anwendungszwecke vorbereitet zu sein.

Es kann deshalb nur empfohlen werden, darauf zu achten, dass möglichst viele Plattformen von dem zu kaufenden Produkt unterstützt werden.

Empfehlung 15 Beschaffen Sie robuste oder integrierte Client Adapter

Gerade in einer Schulumgebung ist es wichtig, Geräte zu kaufen, die eine gewisse Resistenz gegen grobe Behandlungen durch Schüler besitzen.

Seien Sie sich bewusst, dass die Client Adapter bei täglichem Einsatz in einer Schulumgebung stark beansprucht werden. Speziell die Antennen der Client Adapter sollten darauf ausgerichtet sein, dass sie nicht gleich bei der kleinsten Belastung Schaden nehmen. Sind die Antennen austauschbar? Oder muss bei einer defekten Antenne gleich die ganze Client Card ausgetauscht werden?

Halten Sie auf jeden Fall immer einige Ersatzkarten bereit !

Immer mehr Hersteller von Notebooks bieten auch Modelle mit integriertem WLAN-Client Adapter an. Diese besitzen eine bessere Antenne und somit grössere Reichweite. Ausserdem ist diese Lösung robuster, da die Antenne direkt im Gerät integriert ist.

Verwandte Empfehlungen:

Wartung 5: Kaufen Sie Qualität!

Empfehlung 16 Erwerben Sie nur Produkte nach Industriestandard

Da die Kommunikation zwischen Geräten verschiedener Hersteller nur funktioniert, wenn sich diese an gewisse Vereinbarungen halten, sollten sie darauf achten, nur Produkte nach Industriestandard zu kaufen.

Somit sind Sie nicht abhängig von einem bestimmten Hersteller. Der momentan aktuelle Standard bei WLANs ist IEEE 802.11b (11 Mbit/s). Die verschiedenen Client Adapter nach dieser Norm sollten eigentlich mit jedem beliebigen AP nach 802.11b Standard funktionieren. Eventuell ist eine Unausgeglichenheit bei der Bandbreitenzuteilung unterhalb der Benutzer eines APs zu beobachten, falls Client Adapter von verschiedenen Herstellern eingesetzt werden.

Jedoch ist trotz Standardisierung eine enge Zusammenarbeit von APs verschiedener Anbieter nicht garantiert (z.B. erweitertes Roaming).

Verwandte Empfehlungen:

Empfehlung 13: Verwenden Sie nur Produkte vom gleichen Hersteller

Wartung 4: Vermeiden Sie gemischte Umgebungen!

Empfehlung 17 Definieren Sie ein Abdeckungsprofil

Eine 100% Abdeckung des Gebäudes ist praktisch nicht zu erreichen. Welche Gebiete müssen versorgt werden ? Wo ist eine Versorgung wünschbar, aber nicht unbedingt notwendig ?

Es ist ein Leichtes, 50% eines Gebäudes mit einem WLAN abzudecken, aber 100% sind praktisch unmöglich. Funkwellen reagieren sehr sensibel auf (insbesondere metallene) Gegenstände und Personen.

Deshalb ist im Pflichtenheft ein Abdeckungsprofil mit MUSS und SOLL-Abdeckung sinnvoll. (Wo ist eine gute Abdeckung notwendig ? Wo ist sie wünschenswert, kann aber nötigenfalls vernachlässigt werden ?)

Die genaue Reichweite eines AP lässt sich nicht genau vorhersagen, man ist daher mehr oder weniger auf praktische Tests angewiesen. Ausserdem sollte man beachten, dass der Durchsatz mit zunehmender Distanz abnimmt.

Somit muss nicht nur beachtet werden, wo eine Versorgung benötigt wird, sondern auch in welcher Qualität (Durchsatz).

Verwandte Empfehlungen:

Empfehlung 2: Planen Sie vor dem Kauf

Empfehlung 8: Beachten Sie: Der verfügbare Durchsatz nimmt mit zunehmender Distanz vom AP ab

Empfehlung 18 Verwenden Sie verschiedene Funkkanäle für benachbarte APs

Damit sich die APs nicht gegenseitig stören, sollten die Funkkanäle für benachbarte APs möglichst überschneidungsfrei gewählt werden.

Gemäss dem IEEE 802.11b Standard stehen insgesamt 13 Funkkanäle für die APs zur Verfügung. Damit sich die AP nicht gegenseitig stören, sollte man für benachbarte APs verschiedene Funkkanäle wählen. Von den verfügbaren 13 Kanälen sind jedoch nur drei Kanäle verfügbar, die sich im Frequenzbereich nicht überschneiden. Hier in Europa sind dies Kanal 1, 7 und 13.

Gegeben drei Access Points AP1, AP2 und AP3. Alle sind benachbart. Eine gute Wahl der Kanäle wäre hier Kanal 1 für AP1, Kanal 7 für AP2 und Kanal 13 für AP3.
Dies gilt natürlich nur, falls sich nicht noch weitere AP im „Einzugsgebiet" befinden.

Beachten Sie auch, dass wir in einer 3-dimensionalen Welt leben! Auch ein AP im Stockwerk unter- bzw. oberhalb kann eine Störung verursachen.

Verwandte Empfehlungen:

Empfehlung 19: Platzieren Sie nicht mehr als 3 AP im selben Abdeckungsgebiet

Empfehlung 19 Platzieren Sie nicht mehr als 3 AP im selben Abdeckungsgebiet

Um auch grössere Bandbreitebedürfnisse zu befriedigen, werden manchmal mehrere AP im gleichen Raum platziert, um so den Durchsatz zu vervielfachen. In diesem Falle ist unbedingt die Empfehlung 18 zu beachten!

Erfahrungsgemäss beschränkt sich die maximale mögliche Anzahl APs im selben Abdeckungsgebiet eines AP (=Zelle) auf 3 Stück, damit ein störungsfreier Betrieb möglich ist. Dies hängt damit zusammen, dass sich die APs zu stören beginnen, wenn sie in derselben Zelle liegen. Deshalb ist es notwendig, die Kanäle der APs überschneidungsfrei zu wählen (Kanäle 1, 7, 13). Dies führt dann zur oben angemerkten Einschränkung auf 3 APs pro Zelle.

Da die minimale Reichweite pro AP innerhalb eines Raumes ca. 20m beträgt, lässt sich zur Zeit (mit 802.11b) auf diesem Gebiet max. 3 x 11 Mbit/s = 33 Mbit/s realisieren.

Von diesem sind dann maximal etwa 3 x 5 Mbit/s effektiv nutzbar.

Verwandte Empfehlungen:

Empfehlung 18: Verwenden Sie verschiedene Funkkanäle für benachbarte APs

Quellen / Weiterführende Literatur:

iX 1/2001, S.60

Empfehlung 20 Nicht mehr als 10-15 Benutzer pro AP

Da WLAN-AP schon von Haus aus nicht gerade grosszügig mit Geschwindigkeit versorgt sind, ist der Zugriff auf den AP auf wenige Benutzer zu beschränken.

Obwohl es theoretisch kein Limit von Anzahl Clients an einem AP gibt, nimmt die Performance mit zunehmender Anzahl Clients ab.

Um eine wenigstens einigermassen vernünftige Geschwindigkeit bieten zu können, ist gemäss Erfahrungswerten ungefähr pro 10-15 gleichzeitiger Benutzer derselben Zelle ein AP vorzusehen. Aufgrund der Ausführungen von Empfehlung Nr. 10 ist dementsprechend innerhalb einer Zelle die maximale Anzahl gleichzeitiger Benutzer auf ca. 30-45 beschränkt.

Dabei ist zu beachten, dass dies nur bei gleichzeitiger Nutzung der Ressourcen zutrifft, das bedeutet, dass im Durchschnitt nicht mehr Benutzer zugreifen sollten. Da beispielsweise beim Surfen im Internet nur ab und zu ein Burst von Datenpaketen anfällt, stellt das dort kaum ein Problem dar. Sind aber zur gleichen Zeit viele FTP-Transfers oder sonstige kontinuierliche Datenströme am Fliessen, ist ein Engpass kaum zu vermeiden.

⇨ **Hinweis für Universitäten:**

Der Einsatz von WLAN mit der Absicht, dass mehr als 50 Studierende in einem Vorlesungssaal gleichzeitig live auf das Netzwerk zugreifen können, ist mit heutiger Technik (IEEE 802.11b) nicht realisierbar.

Empfehlung 21 Identifizieren Sie mögliche Sicherheitsprobleme

Gerade im Sicherheitsbereich liefern WLANs immer wieder Gesprächsstoff. Deshalb muss man wissen, woher bei einem WLAN in einer Schulumgebung Gefahr droht.

Ohne Schutzmassnahmen ist ein WLAN so offen wie ein unbewachter Hub mit freien Steckdosen:

- Jeder kann sich ins Netzwerk einhängen
- Jeder kann allen Datenverkehr auf dem Subnet mithören (unverschlüsselte Daten, Passworte)

In einer Schulumgebung sind folgende Gefahren zu betrachten:

Nachbarn:

- „unfreiwilliges" Mithören von Daten (-> kein Datenschutz).
- unerlaubte Nutzung von Netzwerkressourcen: Der Schaden äussert sich hier durch die entstehenden Kosten (z.B. Internet Datentransfer) bzw. durch strafbare Handlungen, für die dann die Schule verantwortlich gemacht wird.

Schüler:

- Unerlaubter Zugriff auf Daten des Administrationsnetzes. Abhilfe: **Kein Wireless für das Administrationsnetz !!!**

Es muss jedoch angemerkt werden, dass auch drahtgebundene LANs keineswegs per se sicher sind, da auch Kabel Strahlung abgeben. Zudem sind viele Netzwerke als sogenannte Shared LANs realisiert, die alle Datenpakete an alle angeschlossenen Stationen senden. Diese „picken" sich jeweils die an sie adressierten Pakete hinaus. Mit geeigneter Software ist es aber ein Leichtes, alle ankommenden Daten zu analysieren.

Folgende Tabelle soll Ihnen dabei helfen, diese Sicherheitsprobleme anzugehen:

	SSID	WEP	MAC-Filterung	Authentifizierung	VPN mit Verschlüsselung
Externes Abhören möglich	JA	JA (s. Empfehlung 24)	JA	JA	NEIN
Mitbenutzung durch Externe	NEIN	JA (s. Empfehlung 24)	JA (s. Empfehlung 29)	NEIN	NEIN
Abhören durch Interne	JA	JA	JA	JA	NEIN
Vorteile	einfache Installation	Im 802.11 Standard und somit bei allen entsprechenden Produkten integriert.	Schutz vor Mitbenutzung durch unautorisierte Clients	an Benutzer gebunden	an Benutzer gebunden, sehr sicher
Nachteile	SSID sind leicht herauszufinden und daher für die Sicherheit nicht zu gebrauchen. Änderungen müssen bei allen CA nachgeführt werden	WEP-Verschlüsselung lässt sich durch Abhören von einigen Stunden WLAN-Daten knacken. (s. Empfehlung 24)	Gebunden an physische Karte, nicht an den Benutzer. Grosser Aufwand für die Nachführung der MAC-Adressliste. Unsicher. (s. Empfehlung 29)	Da die Übertragung unverschlüsselt erfolgt, werden Benutzername und Passwort im Klartext übertragen! Deshalb Einsatz von Verschlüsselungstechnologien (SSH, SSL) notwendig !	grosser Installationsaufwand und kaum verfügbare Unterstützung der Hersteller
Bemerkungen	Nur für die Segmentierung (Zugriffsunterteilung) von APs gedacht			Ist nur über die Verwendung von RADIUS Servern per SSH zu empfehlen	

Quellen / Weiterführende Literatur:

W. A. Arbaugh et al. : **Your 802.11 Wireless Network has No Clothes**
http://www.cs.umd.edu/~waa/wireless.pdf

A. Stubblefield et al: **Using the Fluhrer, Mantin and Shamir Attack to break WEP**: www.cs.rice.edu/~astubble/wep/

c't 2000, Heft 22, S. 62 sowie S.260-273,
c't 2001, Heft 18, S.122-124

Empfehlung 22 Keine sensiblen Daten auf dem WLAN !

Da die Daten bei WLANs per Funk übertragen werden, lassen sich die Empfänger nicht so leicht einschränken. Deshalb haben sensible Daten auf einem WLAN nichts zu suchen!

Als die Redaktion der Fachzeitschrift c't (c't 2000, Heft 22) einige WLAN-Produkte testete, staunte sie nicht schlecht, als sie plötzlich Zugriff auf das Netzwerk der benachbarten Medizinischen Hochschule bekam. Diese hatten Access Points (AP) ohne Verschlüsselung und ohne MAC- Adressenfilterung eingesetzt. Man stelle sich vor, welchen Skandal ein freier Zugriff auf geschützte Patientendaten nach sich ziehen würde!

Aber selbst die zum IEEE 802.11-Standard gehörende WEP-Verschlüsselung und die Authentisierung mittels MAC-Adressen hat sich als unsicher erwiesen (s. Empfehlung 24 und Empfehlung 29).

Denken Sie also nicht mal im Traum daran, das Verwaltungsnetz der Schule mit WLAN auszurüsten, es sei den, Sie wollen den Schülern bereitwillig Zugriff auf Schulnoten oder ähnliche interne Informationen geben.

Verwandte Empfehlungen:

Empfehlung 21	Identifizieren Sie mögliche Sicherheitsprobleme
Empfehlung 24	Beachten Sie: WEP-Verschlüsselung bietet nur sehr geringen Schutz
Empfehlung 29	Verwenden Sie keine Zugangskontrolle, die auf MAC-Adressen beruht
Wartung 1:	Trennen Sie das administrative Netz vom Schulnetz!

Empfehlung 23 Verwenden Sie ein separates Subnetz für das WLAN

Sollten Sie das WLAN als eine Erweiterung ihres bestehenden drahtgebundenen LANs einsetzen, verwenden Sie ein eigenes Subnetz für das WLAN.

Sie benötigen zwar einen Router, um das Wireless-Subnetz mit dem restlichen Netzwerk zu verbinden, jedoch gibt es mehrere gute Gründe, dies zu tun:

- ***Performance***
  Da das WLAN nicht ständig auch alle Pakete des LAN erhält (Broadcasts, Verkehr innerhalb LAN), steht ein grösserer Teil der Bandbreite für die Wireless-Benutzer zur Verfügung.
- ***Security***
  Benutzer des WLANs können durch geeignete Massnahmen vom Zugriff aufs LAN gesperrt werden, solange sie sich nicht entsprechend authentifizieren.
- ***Wartung/Fehlersuche***
  Beim Ausfall des einen Netzwerks ist das andere nicht betroffen. So ist bei einem Fehler im WLAN ein normales Arbeiten im drahtgebundenen LAN weiterhin möglich.

Empfehlung 24 Beachten Sie: WEP-Verschlüsselung bietet nur sehr geringen Schutz

Die WEP-Verschlüsselung lässt sich mit geeigneten Programmen innerhalb von wenigen Stunden knacken und bietet keinen Schutz gegenüber am selben AP eingeloggte Benutzer.

Die von den Herstellern ursprünglich als Schutz vor externem Abhören gedachte WEP-Verschlüsselung hat versagt. Im Laufe des Jahres 2001 sind zuerst theoretische Angriffe [1] und bald darauf Implementationen von Angriffen [2] [3] veröffentlicht worden, die eine seit 1995 bekannte Schwäche des in WEP verwendeten RC4-Algorithmus ausnützen. Durch genügend langes Abhören des Netzwerkverkehrs kann mit Hilfe dieser Programme der WEP-Schlüssel geknackt werden. Je nach Datenaufkommen sind für das Knacken des Schlüssels 4 Stunden bis einige Tage nötig. Mit den sich zur Zeit in Entwicklung befindlichen Programmen ist bald kein Spezialwissen mehr notwendig, um WEP zu knacken.

Wired Equivalent Privacy = einer Verkabelung entsprechende Sicherheit

Als weitere Einschränkung ist zu beachten, dass WEP definitionsgemäss bereits vor Bekanntwerden der aktuellen Schwächen keinen Schutz gegen das Abhören durch rechtmässig am gleichen AP eingeloggten Benutzer bot. Die Sicherheit entsprach in etwa derjenigen eines Hub-Anschlusses.

Quellen / Weiterführende Literatur:

[1] Security of the WEP algorithm
www.isaac.cs.berkeley.edu/isaac/wep-faq.html
[2] Using the Fluhrer, Mantin and Shamir Attack to break WEP:
www.cs.rice.edu/~astubble/wep/
[3] AirSnort: airsnort.sourceforge.net

Empfehlung 25 Beachten Sie: Verschlüsselung bedeutet meistens Geschwindigkeitseinbussen

Durch aktivierte WEP-Verschlüsselung wird der Datendurchsatz bei den meisten Produkten verringert.

Da durch die Verschlüsselung zusätzlicher Aufwand im AP sowie dem Endsystem bedeutet und zudem weiterer Protokoll-Overhead hinzu kommt, wird durch eine aktivierte WEP-Verschlüsselung die Performance merkbar verringert (bis zu 30%). Es ist jedoch nur eine Frage der Zeit, bis optimierte Versionen der Verschlüsselungstechniken angeboten werden, die in etwa dieselbe Geschwindigkeit wie die unverschlüsselte Übertragung erreichen.

Quellen / Weiterführende Literatur:

iX 1/2001, S.50

Empfehlung 26 Erstellen Sie eine Benutzungsordnung auf dem WLAN-Gelände.

Für einen störungsfreien Betrieb des WLANs ist es notwendig, mögliche Interferenzen so gering als möglich zu halten. Deshalb ist es unter Umständen ratsam, den Einsatz von bestimmten Geräten im WLAN-Gebiet zu verbieten.

Betroffen sind alle Geräte, die im selben Frequenzbereich wie das WLAN operieren.

Im Falle von 802.11b betrifft das den 2.4 Ghz Bereich. In diesem Frequenzband arbeiten z.B. Funktelefone, Mikrowellen und Bluetooth Geräte. Wobei anzumerken ist, dass die meisten WLAN-Hersteller die Störungen von Mikrowellengeräten bewusst in ihre Produktegestaltung mit einbeziehen und diese somit nicht so ein grosses Problem darstellen. Besonders störend sind natürlich andere APs, die nicht zum eigenen WLAN gehören. Solche sind in jedem Falle zu verbieten beziehungsweise ins eigene Netz mit einzubinden.

Quellen / Weiterführende Literatur:

Benutzungsordnung an der Carnegie Mellon University (USA)
http://www.cmu.edu/computing/wireless/airspace.html

Empfehlung 27 Auch WLANs brauchen Wartung

WLANs benötigen zwar keine Kabel, aber trotzdem Wartung. Deshalb ist es notwendig, das WLAN ins Wartungskonzept zu integrieren.

Wer ist wofür verantwortlich ? Welche Teile des WLANs werden vom Lieferanten gewartet, welche intern ?

Es muss zumindest an der Schule ein Systembetreuer bestimmt werden, der in Zusammenarbeit mit dem Informatikteam und dem Lieferanten das WLAN in Betrieb hält.

Zudem soll eine klar definierte Anlaufstelle vorhanden sein, welche die Benutzer bei Problemen aufsuchen können. Diese sollte in der Lage sein, Hilfe bei der Installation von CAs bzw. der Beseitigung von bekannten Problemen zu leisten.

Dementsprechend muss sie mit dem Systembetreuer in engem Kontakt stehen. (Üblicherweise wird in einer Schule wohl der Systembetreuer selbst diese Anlaufstelle sein. Es können jedoch auch vorerst Power-User eingesetzt werden, die dann erst bei grösseren Problemen den Systembetreuer zu Hilfe nehmen)

Verwandte Empfehlungen:

Wartung 14: Planen Sie die Wartung Ihres Schulnetzes!

Wartung 16: Achten Sie auf die Verfügbarkeit von Ansprechpersonen

Empfehlung 28 Vernetzen Sie den Lehrerarbeitsplatz im Schulzimmer mit Kabel

Trotz Funkvernetzung im Schulzimmer lohnt sich der Aufwand, den Lehrerarbeitsplatz zu verkabeln.

Es gibt verschiedene Gründe, warum der Arbeitsplatz der Lehrperson traditionell mit Kabel vernetzt werden sollte:

- **Datendurchsatz:** Auf dem Computer der Lehrperson ist rasch ein höherer Datendurchsatz erforderlich als bei den SchülerInnen. Ist der Lehrercomputer verkabelt, so können bandbreitenhungrige Dinge am Lehrer-Computer / Beamer gezeigt werden.
- **Zuverlässigkeit:** Auch wenn WLAN immer zuverlässiger werden, so können sie doch nicht mit bewährter Kabeltechnologie mithalten. Für die LehrerIn ist es angenehm, eine mögliche Fehlerquelle weniger überprüfen zu müssen.
- **Sicherheit:** Auch wenn wir nicht empfehlen, vertrauliche Daten im Schulzimmer zu bearbeiten, ist eine höhere Sicherheit für LehrerInnen wünschenswert. Bereits das Abhören eines Lehrerpasswortes kann für SchülerInnen verlockend sein. Dies wird mit der Kabelvernetzung weitgehend verhindert.

Empfehlung 29 Verwenden Sie keine Zugangskontrolle, die auf MAC-Adressen beruht

Den Zugriff auf das WLAN mit Hilfe von MAC-Adressen einschränken zu wollen, lohnt sich nicht. Es ist aufwendig und unsicher.

Gewisse Access Points bieten die Möglichkeit, den Zugriff auf den AP (und somit auch das Netzwerk) durch eine Liste erlaubter MAC-Adressen zu definieren. Jede Netzwerkkarte besitzt eine weltweit eindeutige MAC-Adresse, die sie eindeutig identifiziert. Es ist nun möglich, bei den APs nur solchen Funk-Datenverkehr zuzulassen, der von genehmigten MAC-Adressen stammt.

Dieses Verfahren hat zwei Haken. Einerseits ist es bei vielen Benutzern sehr administrationsintensiv, da jeder CA erfasst werden muss. In den Spezifikationen fehlt zudem oft die Angabe, wie viele MAC-Adressen die entsprechende Access-Control-List speichern kann.

Entscheidender ist jedoch die vorhandene Sicherheitslücke. Wie bei den meisten traditionellen Netzwerkkarten lässt sich die MAC-Adresse bei verschiedenen WLAN-Karten ändern. Da MAC-Adressen selbst bei WEP unverschlüsselt übertragen werden, ist das Abhören fremder MAC-Adressen möglich. Wird nun ein fremder CA mit der abgehörten MAC-Adresse versehen, kann er nun auf das WLAN lesend und schreibend zugreifen.

Quellen und weiterführende Literatur:

W. A. Arbaugh et al. : **Your 802.11 Wireless Network has No Clothes**
http://www.cs.umd.edu/~waa/wireless.pdf

Glossar

Ad-hoc-Modus Betriebsart, bei der Rechner ein spontanes Netz ohne Access Point aufbauen können – etwa mehrere mit WLAN-CA ausgerüstete Notebooks in einer Konferenz.

ACL Access Control List, Liste der Hardware-Adressen (MAC-Adressen), von denen ein AP Daten für die Weiterleitung akzeptiert

AP Access Point: Relaisstation, welche die Daten der Client Adapter weiterleitet (ans angeschlossene LAN, Internet oder andere Client Adapter)

Burst kurzzeitige, extreme Anhäufung (z.B. von Datenpaketen)

CA Client Adapter: Hardwarekomponente mit integrierter Antenne, die beim Benutzergerät benötigt wird, um am WLAN teilzunehmen.

CSMA/CA Carrier Sense Multiple Access / Collision Avoidance. Protokoll, das den Zugriff auf ein Medium durch mehrere Teilnehmer regelt. Es soll die Kollision von Datenpaketen verhindern, führt jedoch zu relativ langen Wartezeiten vor dem Senden eines Paketes.

DHCP Dynamic Host Configuration Protocol, dient zur dynamischen Zuteilung von IP-Adressen in einem LAN. Die Rechner erhalten auf Anfrage von einem DHCP-Server IP-Adressen aus vordefinierten Bereichen

Gateway Rechner, der Netzwerke unterschiedlicher Struktur koppelt, etwa ein hausinternes LAN mit dem Internet.

Hub Verteilstation für drahtgebundene LAN. Leitet eingehende Signale an alle angeschlossenen Stationen weiter.

IEEE 802.11 Die Normenreihe IEEE 802.x des Institute of Electrical and Electronic Engineers (IEEE, www.ieee.org) spezifiziert unter anderem Verfahren für die Netzwerkkommunikation: mit CSMA/ CD (Carrier Sense Multiple Access/Collision Detection) funktionierende Ethernet-Netzwerke arbeiten nach 802.3, Token-Ring-Pendants orientieren sich an 802.5. 802.11 ist der Standard für drahtlose Infrarot- oder Funk-Netzwerke. Letztere verwenden als Übertragungsverfahren entweder DSSS (Direct Sequence Spread Spectrum) oder FHSS (Frequency Hopping Spread Spectrum).

Infrastruktur-Modus Betriebsart, bei der ein Access Point den Datenverkehr in einem WLAN regelt. PCs können dabei keine direkte WLAN-Verbindung miteinander aufnehmen. Ausserdem kann der AP als Übergang ins Unternehmensnetz oder Internet fungieren.

MAC Medium Access Control, Element des Data-Link Layer, der zweiten Schicht im OSI-Modell. MAC kontrolliert den Zugriff auf das physische Übertragungsmedium, etwa den Token-Ring-, Ethernet- oder FDDI-Anschluss. Auf dieser Schicht

	hat jede Netzwerkkarte eine individuelle 48-Bit-Adresse, die sie weltweit eindeutig kennzeichnet, daher die Bezeichnung MAC-Adresse.
NAT	Netzwerk Address Translation: besorgt in einem Gateway die Übersetzung interner IP-Adressen 1:1 in externe, so dass die Struktur eines LANs von aussen betrachtet verborgen bleibt.
NIC	Network Interface Card, die (W)LAN- oder ISDN-Karte in einem Rechner, auch Netzwerk-Adapter
RADIUS	Remote Authentication Dial-In User Service, Verfahren für die Authentifizierung von Remote Benutzern
Roaming	Zusammenarbeit zwischen verschiedenen AP's, so dass ein unterbruchsfreier Übergang von einem AP zum nächsten möglich wird. Benötigt eine Verkabelung der AP's über einen gemeinsamen Hub bzw. Switch, einen sich überdeckender Einsatzbereich mit unterschiedlichen Funkkanälen.
SSH	Secure Shell. Ersatz für Telnet, der mit Verschlüsselung arbeitet. Ermöglicht den verschlüsselten Zugriff auf entfernte Rechner.
SSID	Service Set Identifier, wird benutzt, um einen bzw. mehrere APs mit Namen auszustatten und damit logisch gegenüber anderen APs abzugrenzen.
SSL	Secure Socket Layer (Verschlüsselungsmechanismus)
Switch	Verteilstation, welche eingehende Signale nur genau an deren Empfängeradresse weiterleitet.
VPN	Virtual Private Network
WAN	Wide Area Network, Weitverkehrsnetzwerke, z.B. Telefonnetz Schweiz
WEP	Wired Equivalent Privacy, ein Verschlüsselungsverfahren, welches das Abhören von WLAN Funksignalen verhindern soll.
Wi-Fi	Wireless Fidelity, soll als Industriestandard das reibungslose Zusammenarbeiten von WLAN-Komponenten verschiedener Hersteller nach der 802.11-Norm garantieren; siehe www.wi-fi.org
(W)LAN	(Wireless) Local Area Network, (drahtloses) lokales Netzwerk.
Zelle	Abdeckungsgebiet eines Access Points. Manchmal wird eine Zelle auch durch mehrere parallele APs abgedeckt.

Dank

An dieser Stelle möchten wir uns recht herzlich bei folgenden Personen und Schulen für ihre Auskunftsbereitschaft und Zusammenarbeit bedanken:

Armin Brunner, Informatik-Dienste, ETH Zürich

Willy Meister, KV Business School, Zürich

Reinhard Dietrich, KPMG Information Risk Management

Ein herzliches Dankeschön geht auch an die zahlreichen Korrekturleserinnen und -leser!