Es funkt auf dem Campus

Funk-LAN an der Universität Konstanz

Andreas Merkel[1]

Am Anfang stand eine Idee...

Zu Beginn des Jahres '98 sammelte das Rechenzentrum (RZ) im Rahmen eines Funk-LAN-Projektes erste Erfahrungen mit Funknetzen (Funk-LAN bzw. Wireless LAN, WLAN). Die mit dieser Technik damals erzielbare Datenübertragungsrate betrug gemäß dem Standard 802.11 [1] maximal 2 MBit/S. Anfang 2000 kamen die ersten WLAN-Komponenten gemäß dem neuen Standard 802.11b [2] auf den Markt; diese erlaubten Datenraten von bis zu 11 MBit/s. Das entspricht in etwa der Übertragungskapazität eines normalen (‚geshareten') 10 MBit/S Netzsegmentes (10 Base T). Damit waren aus der Sicht des RZ die Voraussetzungen geschaffen, WLANs auch an der Universität Konstanz einzusetzen.

Von der Vorstellung, ohne Kabel von (nahezu) jedem Arbeitsplatz ins INTERNET zu kommen, waren auch Vertreter der Bibliothek - hier sei stellvertretend und allen voran Herr Franken genannt - fasziniert. In einem ersten Treffen im Frühjahr 2000 wurde das Thema WLAN gemeinsam erörtert. Während seitens der Bibliothek anfangs nur ein WLAN zur mobilen Datenerfassung angedacht war, plädierte das RZ für den Aufbau eines dedizierten, gebäudeübergreifenden WLAN, welches das vorhandene Campusnetz an ausgesuchten Lokationen ergänzen sollte. Man verständigte sich schnell auf eine uniweite Einführung der WLAN-Technik; die Festlegung des Einführungszeitpunktes wurde hingegen kontrovers diskutiert: bestand das RZ auf einer mehrstufigen Einführung mit entsprechender Vorlaufzeit zur Implementierung der Sicherheitsfunktionen (s. u.), hätte das Management der Bibliothek das WLAN am liebsten gleich übermorgen in ihren Räumen auch ohne diese Funktionen in Betrieb genommen....

...dann kamen die Anforderungen

In mehreren ‚Brainstroming'-Sitzungen des RZ-WLAN-Projektteams (Barbara Löhle, Andreas Kalkbrenner, Andreas Merkel, Stephan Pietzko) wurden die Eckwerte für das Anforderungsprofil für den Betrieb von WLANs an der Universität Konstanz wie folgt festgelegt::

- **Funk-LAN als ideale Ergänzung zum vorhandenen Campusnetz**
  Das Funk-LAN sollte das drahtgebundene Campusnetz in den Lokationen ergänzen, die entweder nur sehr kostspielig (Buchbereiche in der Bibliothek), oder überhaupt nicht (Außenbereiche wie Innenhof, Meetingpoints im Eingangsbereich, etc.) mit einem Festnetz erschlossen werden konnten. Ein 100% flächendeckendes Funk-LAN war von Anfang an nicht vorgesehen. Die Funk-LAN-Ausstattung von Hörsälen wurde als optionale Forderung mit aufgenommen. Die temporäre Versorgung von Seminarräumen mit Funk-LANs sollte möglich sein; war aber nicht als stationäre Einrichtung gefordert.
- **Separates physikalische Funk-LAN-Netz (Virtuelles Privates Netz, VPN)**
  Aus Sicherheitsgründen sollte das Funk-LAN als physikalisch separate Netzinfrastruktur ausgelegt und über eine definierte Übergangsstelle an das Campusnetz angeschlossen werden. Als Übergabeschnitt-

1 Rechenzentrum der Universität Konstanz

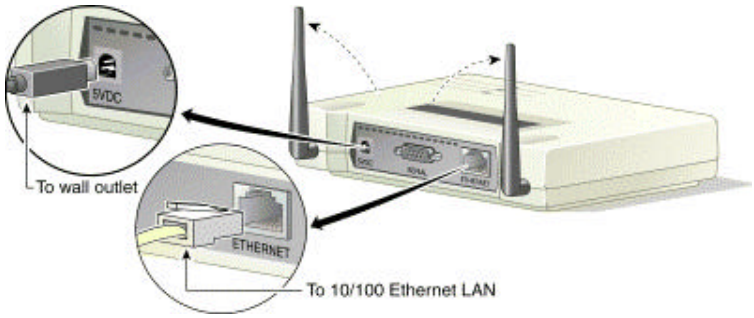
stelle sollte eine redundant ausgelegte dedizierte Netzwerkkomponente (VPN-Konzentrator) mit Datenfiltermöglichkeiten eingesetzt werden.

- **Benutzerbasierte Authentifizierung für Zugriff auf Funk-LAN**
  Funknetze, welche von jedem portablen Rechner mit entsprechender Funk-LAN-Karte genutzt werden können, erfordern im Hinblick auf Benutzungsberechtigung und Missbrauch vor der Nutzung eine Authentifizierung (Benutzerkennung und Passwort). Diese sollte aus betrieblichen Gründen automatisiert über einen Authentifizierungsserver (z.B. einen RADIUS-Server) erfolgen und mit der Benutzerdatenbank der Universität gekoppelt sein. Für schützenswerte Daten (z.B. Benutzerkennung und Passwort) sollte eine sessionbassierte Datenverschlüsselung zwischen portablen Rechnern und Authentifizierungsserver möglich sein.
- **Unterstützung einer dynamischen IP-Adressvergabe:**
  Nach Authentifizierung sollte dem Rechner des Benutzers aus einem IP-Adresspool eine Netzwerkadresse zusammen mit anderen für den INTERNET-Zugang benötigten Netzwerkparametern dynamisch (DHCP) zugewiesen werden.
- **Unterstützung heterogener Funk-LAN-Clients**
  Mobile Funk-LAN-Clients verwenden PCMCIA-Funk-LAN-Karten, welche mit entsprechenden Treibern in das Betriebssystem eingebunden werden. Funk-LAN-Karten und Software-Clients sollten nicht nur für das Windows- bzw. NT-Betriebssystem der Firma Mircosoft unterstützt werden, sondern auch für andere Betriebssysteme (z. B. Der Fa. Apple, Mac OS 9.x und X, oder für LINUX-OS).
- **Ausbau der Funk-LAN-Authentifizierung zu generischem Net-Login-Verfahren**
  Die rechnergestützten Zugangsregelungen (RADIUS-Client bzw. VPN-Client) sollten optional zu einem allgemeinen ‚Net-Login'-Verfahren (Einwählen Universitätsangehöriger ins Datennetz der Universität über externe Internet Provider) erweiterbar sein.
- **Realisierung unterschiedlicher Sicherheitszonen**
  Neben dem INTERNET-Zugang sollen Funk-LAN-Segmente für unterschiedliche Sicherheitsanforderungen eingerichtet und verwaltet werden können. Hierzu zählen zum Beispiel dedizierte Subnetze zur Informations-Recherche in der Bibliothek, oder zum Informationsaustausch einer geschlossenen Benutzergruppe in Instituts- und Bereichsnetzen.
- **Betriebliche und organisatorische Aspekte**
  Für die Initiierung des Funk-LAN-Projektes war ein Startkontingent von 50 Funk-LAN-Karten vorgesehen. Die Ausleihe von Laptops war von Anfang an nicht geplant; stattdessen sollten in Zusammenarbeit mit lokalen Händlern preislich attraktive Angebote zum Kauf von Laptops und Funk-LAN-Karten für die Nutzer ausgehandelt werden eine Förderinitiative zum Thema ‚Funknetze' an der sich auch das Rechenzentrum für die Universität Konstanz mit einem Projektantrag im August 2000 beteiligte. Im November 2000 kam die Zusage, dass die Universität Konstanz - zusammen mit drei weiteren Universitäten des Landes Baden-Württemberg - in den bundesweiten Förderkreis des BMBF-Projektes aufgenommen wurde (BMBF-Projekt mit der Fördernummer 08NM040). Damit war der Weg frei und der Aufbruch in das WLAN-Zeitalter konnte beginnen.

Drei Teile braucht ein WLAN

Im wesentlichen besteht ein WLAN aus drei Komponenten:

- Sende-/Empfangskomponente (Access Point, AP); sie stellt das Bindeglied zwischen drahtgebundenem Campusnetz und Funknetz dar.



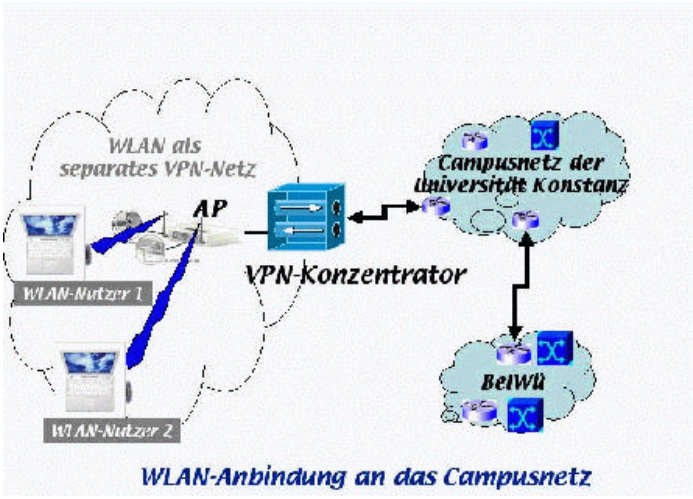
- WLAN-PC Card (PCMCIA-Karte) in einem Laptop,

- Software in Form eines PC-Card-Kartentreiber und Standard Anwendungssoftware wie zum Beispiel ein Web-Browser, E-Mail-Programme, etc.

Das nächste Bild zeigt den prinzipiellen Aufbau eines WLAN und dessen Anbindung an das universitäre Datennetz.

Festlegung der WLAN-Zellen

Wie bei jeder Einführung von neuen Netzwerktechnologien erfolgte auch hier die Implementierung in mehreren Schritten. Zuerst wurden die



WLAN-Architektur und die Anbindung an das Campusnetz

WLAN-Zellen, jene Bereiche auf dem Universitätsgelände, welche mit einem WLAN ausgestattet werden sollten, festgelegt. Schon bei den Vorüberlegungen zeichneten sich die nachfolgenden Areale als prädestinierte Bereiche für die Installation von WLANs ab:

- Eingangsbereiche und Treff- bzw. Aufenthaltsbereich außerhalb der Gebäude,
- Arbeitsplätze in den Buchbereichen der Bibliothek,
- Experimentieranlagen im Freien.

Hier waren nicht nur die Kriterien "hohe Personen-Belegungsdichte" und "minimale/keine Festnetzanschlussdichte" erfüllt. Auch die im Vorfeld mit der Bibliothek und einzelnen Nutzergruppen geführten Gespräche ließen in diesen Bereichen eine hohe Akzeptanz bzw. Nutzung des Funk-LAN erwarten[2].

Die ersten WLAN-Tests

Im September 2000 wurden dann als nächstes im Buchbereich S der Bibliothek erste WLAN-Tests durchgeführt. Dabei wurde die prinzipielle Machbarkeit eines Funk-LANs in dem geplanten Umfeld verifiziert; als Testgerät wurde ein Leihgerät der Firma Lucent (WavePoint II) eingesetzt. Danach wurden verschiedene Anbieter kontaktiert und um Teststellungen gebeten. In der anschließenden Evaluationsphase waren Geräte der Firmen Apple, Cisco, Enterasys, Lucent und Siemens vertreten. Bei den praktischen Versuchen vor Ort ergaben sich zum Teil überraschende Ergebnisse:

- Die Interoperabilität zwischen PC-Cards und AP der verschiedenen Hersteller war ausgezeichnet, alle Systeme waren in der Grundfunktionalität zueinander kompatibel.
- Nach einigen Versuchen konnten auch per WEP verschlüsselte Verbindungen mit unterschiedlichen Karten realisiert werden.
- WLAN-Zellen auf dem Universitätsgelände (ohne projektbezogene Funkzellen)
- Die erzielten Reichweiten waren - vor allem aufgrund der offenen Strukturen in den Bibliotheksbereichen - überraschend groß.
- Eine effektive Störung, die zur Unterbrechung einer 802.11b-basierten Funkverbindung führt, war nur durch Sender möglich, die ebenfalls mit dem Spreizbandmodulationsverfahren arbeiteten, also insbesondere durch andere APs, die auf benachbarten Kanäle betrieben wurden.

Während dieser Evaluierungsphase wurde dann damit begonnen, durch Funkfeldmessungen in den zu versorgenden Bereichen die Standorte der APs festzulegen. Bei diesen Vermessungen traten die ersten Probleme auf:

Bedingt durch die offenen Bereiche, Halbebenen, großen Glasflächen und einer ‚verschachtelten' Struktur kommt es zu großen Funkfeldausdehnungen; dies gestaltete die Frequenzeinteilung bzw. die Funkkanalverteilung schwierig: Durch das im Standard 802.11b verwendete Spreizband-Modulationsverfahren ist auf den 13 freigegebenen Kanälen nur der störungsfreie Betrieb von maximal 4 APs gleichzeitig möglich. Es zeigte sich, dass dies mit omnidirektional abstrahlenden Antennen nicht zu erfüllen war - die Funkzellen waren zu groß und störten die benachbarten Bereiche. Da der Standard 802.11b keine situationsbezogene Reduktion der Sendeleistung der Clients vorsieht, war die einzige Alternative eine Anpassung des auszuleuchtenden Volumens an die vorhandene Architektur. Dies erforderte den Einsatz

Hier sind die mit Funk versorgten Bereiche skizziert;

2 (detailliertere Informationen sind unter der Webseite des RZ zu finden: http://www.rz.uni-konstanz.de/wlan).

von Antennen mit Richtcharakteristik und eine möglichst fein skalierte Absenkung der Sendeleistung der APs. Damit wurde eine Unterstützung von externen Antennen seitens der APs zwingend erforderlich - die Systeme von Apple und Siemens schieden damit bereits aus.

Neben finanziellen Aspekten waren schließlich die nachfolgenden Eigenschaften für die Entscheidung zugunsten der AiroNet-Funk-LAN-Komponenten der Firma CISCO (340-er Komponentenfamilie) verantwortlich:

- Hohe Durchsatzwerte,
- Sehr gute Administrationstools für Konfiguration (Terminal, WWW, SNMP, Telnet), WEP-Verschlüsselung, Überwachung der Funk-Verbindungsqualität und sehr detailliertes Log.
- Funk-LAN-Karten mit Anschlussmöglichkeit für externe Antennen,
- Leistungsstarker 32 Bit Power-PC-Controller mit 16 MB DRAM,
- Einstellbare Sendeleistung sowohl auf Seite der APs also auch auf Seite der Clients.

Die erste WLAN-Testperson

Nach der Festlegung der Standpunkte der APs wurden zwischen Weihnachten und Neujahr die Verbindungspunkte (Daten- und Stromkabel) für den Anschluss ans Campusnetz installiert; am 30.12.2000 war die Installation des ersten AP im S-Buchbereich der Bibliothek abgeschlossen; damit konnte der Probebetrieb begonnen werden.

Mittels Verschlüsselung und ‚versteckter' SSID (service set identifier) wurde das Funknetz für eine Bibliotheksmitarbeiterin als geschlossene Benutzergruppe zugänglich gemacht. Dank ihrer Tätigkeit - Datenerfassung auf allen 6 Etagen des S-Buchbereiches - konnten somit wertvolle Erfahrungen im täglichen Einsatz hinsichtlich der Zuverlässigkeit, der Funkfeldausleuchtung und der Netzwerkqualität (Datenrate, Antwortverhalten, Verfügbarkeit, etc.) gesammelt werden.

Inbetriebnahme

Nachdem der erste Probebetrieb zur Zufriedenheit aller verlief, stand der offiziellen Inbetriebnahme des WLANs nichts mehr im Wege. In zwei Phasen sollte das WLAN in den normalen Betrieb überführt werden:

Die erste Betriebsphase (Pilotphase) sah eine benutzerbasierte Authentifizierung (mittels des VPN-Tunnelprotokolls PPTP1) über einen mit der Benutzer-Datenbank gekoppelten RADIUS-Server vor. Als VPN-Konzentrator wurde hierzu ein vorhandener Router eingesetzt.

In der zweiten Betriebsphase (Wirkbetriebsphase), welche zum WS 2001/2002 startet, wird das PPTP Tunnelprotokoll durch L2TP/IPSec2 ersetzt. Als VPN-Konzentrator kommt dann eine dedizierte, redundant ausgelegte Komponente zum Einsatz.

Mitte Mai diesen Jahres startete die erste Betriebsphase in den nachfolgend aufgelisteten Fachbereichen und Gebäuden:

- Eingangsbereich der Universität im Gebäude A vor dem Campuscafe und im Innenhof.

- Fachbereich Informatik in den Gebäudeetagen B2 und E2.
- Rechenzentrum im V-Gebäude und in den beiden Sitzungssälen auf der Etage V10
- Bibliothek in den Buchbereichen S2-S6 (Bild 5) im Gebäude G, im Gebäude N in den Buchetagen N4-N6, in der alten Ausleihe im Gebäude B4, in der Spange G2-S2

- Fachbereich Biologie im Außenbereich vor dem U-Gebäude, am Bodenseeufer vor dem Wasser-Pumpwerk der Universität und auf dem Bodensee (Überlinger See)

- Im Fachbereich Physik in den Laborhäusern des Sonnenbühl Haus 2 und 3.

Im Zuge der Unterstützung für die Studierenden wurden zwischenzeitlich weitere 75 Funk-LAN-Karten zu sehr günstigen Konditionen beschafft; diese können über das RZ[3] entweder für Testzwecke ausgeliehen, (50,- DM/Semester) oder zu einem Selbstkostenpreis von 299,- DM erworben werden.

3 E-Mail an die Liste support@uni-konstanz.de

Erste Betriebserfahrungen

Das Funknetz wurde von allen Benutzergruppen freudig begrüßt. Dank dieses Projektes konnte ein ‚WLAN-Wildwuchs' verhindert werden. Durch das einheitliche Funk-LAN-Konzept wurde der Betrieb entscheidend vereinfacht. Die Etablierung der Funkhoheit beim Netzbetreiber (Funkkanalverteilung aus einer Hand), sowie die Erweiterung des vorhandenen Authentifizierungsmodells für das Funk-LAN tragen wesentlich zum wirtschaftlichen und effizienten Funk-LAN-Betrieb auf dem Universitätsgelände bei.

Die Durchdringung in der Präsenzlehre steht noch am Anfang; bei der Fachbereichsbezogenen Forschung hingegen erfreut sich die Funk-LAN-Technologie infolge der reizvollen Möglichkeiten (mobile Online-Messdatenerfassung im Experimentierfeld vor Ort, Online-Visualisierung von Phänomen in der Natur und Technik, etc.) großer Akzeptanz.

Der Einsatz von Funk-LANs in den Hörsälen wird zur Zeit an der Universität noch diskutiert.

Neben dem allgemein sehr knapp bemessenen Projektzeitrahmen, sorgten vor allem die nachfolgenden Umstände für zeitliche Verzögerungen und erschwerten die Projektdurchführung:

- Aufgrund der ‚kompakten' Gebäudebauweise war die Identifikation und Festlegung von Funkzonen als Ergänzung zum drahtgebundenen Campusnetz sehr zeitintensiv.
- Die Abwicklung der Baumaßnahmen zur Anbindung der APs an das Festnetz - speziell im Außenbereich und in Bereichen mit viel Publikumsverkehr - zwangen immer wieder zu zeitintensiven Begehungen vor Ort; doch dank der sehr guten Kooperation aller Projektbeteiligten (Ansprechpartner und Testperson in der Bibliothek, Installationsfirma und Projektmitarbeiter) konnten alle Baumassnahmen zügig abgewickelt werden.

Der Betrieb des WLAN wurde vom RZ erst freigegeben, als eine Authentifizierung per UserID und Passwort über den zentralen Authentifizierungsserver des RZ zur Verfügung stand. Dadurch wurde so manch Ungeduldiger ‚auf die Folter gespannt'. Inzwischen bestätigt die aktuell entbrannte Sicherheitsdiskussion (s.a. Literaturhinweis [3]) jedoch dieses Vorgehen.

Ausblick

Sobald die ersten Geräte für den neuen IEEE Standard 802.11a-1999 [4], welcher eine Funkübertragung im 5 GHz Frequenzband definiert, verfügbar sind, wird das RZ deren Einsatz an der Universität Konstanz vorbereiten.

Literatur

[1] IEEE Standard 802.11; "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications", IEEE 1997.

[2] IEEE Standard 802.11b-1999 DRAFT Supplement to IEEE Stan-dard 802.11; "Higher Speed Physical Layer extension in the 2,4 GHz Band", IEEE 1999.

[3] heise online NEWS; "Schwachstellen im Sicherheitsprotokoll für Funk-LANs", 06.02.2001.

[4] IEEE Standard 802.11a-1999 DRAFT Supplement to IEEE Std 802.11-1999 "Higher Speed Physical Layer extension in the 5,4 GHz Band"; [Adopted by ISO/IEC and redesignated as ISO/IEC 8802-11:1999/Amd 1:2000(E)]; IEEE 1999