Vermaschter Datenfunk

Maschennetze stellen eine interessante Netzwerktopologie dar. Wird diese Topologie bei Funknetzen verwendet, bilden sich flächendecke, ausfallsichere und sich selbstorganisierende Funknetze. In diesem Artikel wird beschrieben, welche Schritte die weit verbreitete WLAN-Technik bis heute gemacht hat. Weiter werden die grundsätzlichen Probleme, welche beim nächsten Entwicklungsschritt der WLAN-Technik hin zu Mesh-WLANs auftreten, mit ähnlichen Problemen bei den uns vertrauten Kabelnetzen verglichen. Es wird gezeigt, wie die Probleme bei den Kabelnetzen erfolgreich gelöst wurden und welche Ideen existieren, dieselben Probleme für Funknetze zu lösen. Die Erfahrungen beim Aufbau eines Mesh-WLANs werden beschrieben und ein Ausblick auf mögliche und geeignete Anwendeungen für Mesh-WLANs gemacht.

Andreas Hofmann, Claude Rubattel | andreas.hofmann1@fhnw.ch

Immer mehr Stadtgebiete werden heute flächendeckend mit drahtlosem Internet-Zugang (WLAN) versorgt. Dabei kommt vermehrt die Maschen-Technik zum Einsatz, weil dadurch im grossen Stil auf Kabelanschlüsse ans Internet verzichtet werden kann. So rüstet zum Beispiel Nortel den Campus eines nationalen Kunstzentrums in Taiwan mit einem Maschennetz aus [NOR07], oder Packethop erstellt im Bundesstaat New Jersey ein Maschennetz für die Polizei von Lakewood [PAC07]. Die Polizei soll auf diese Weise ein erweitertes Kommunikationsmittel erhalten. In der Stadt Cambridge baut das Massachusetts Institute of Technology (MIT) zusammen mit der Stadt ein Maschennetz nach einem System, welches am MIT selbst entwickelt worden ist [ROO07].

Auch in Europa ist man auf diesen anfahrenden Zug aufgesprungen. In Berlin entsteht seit einiger Zeit ein freies Funknetz, das sogenannte Freifunk-Netz [FRE07a]. Es macht sich die beiden Umstände zu Nutzen, dass einerseits die von 802.11x benutzten Frequenzbänder konzessionslos von allen benutzt werden dürfen und anderseits dass die Firma Linksys die Firmware eines ihrer Access-Points (AP) im Quellcode offen legen musste, nachdem bekannt wurde, dass für diese Firmware Opensource-Software eingesetzt wurde. Mittels ausgetauschter Firmware werden die normalen APs in Maschenknoten verwandelt, die sich selbständig zu einem Maschennetz vermaschen. Viele Privatpersonen installieren solche modifizierten APs auf den Dächern ihrer Häuser und so breitet sich das Netz ständig weiter über Berlin aus. Es spannt sich ein eigentliches Bürgernetz, das von keiner zentralen Infrastruktur abhängig ist. Ein Internet Service Provider (ISP) sorgt schliesslich dafür, dass einzelne der APs über einen Gateway mit dem Internet verbunden sind. Somit dienen die APs auf den Dächern den Benutzern als indirekten Zugang ins Internet.

Einfache Funknetze

Momentan bestehen hauptsächlich zwei Möglichkeiten, um Geräte mittels WLAN miteinander kommunizieren zu lassen [IEE03]. Zum einen ist dies der so genannte Ad-Hoc-Modus (auch Peer-To-Peer-Modus genannt), in dem meist zwei Geräte spontan ohne weitere Konfiguration eine gleichberechtigte Ende-zu-Ende Verbindung errichten. Dadurch können genau die beiden partizipierenden Geräte miteinander kommunizieren. Man nennt diesen Modus auch Independent Basic Service Set (IBSS).

Die zweite Möglichkeit besteht darin, dass ein spezielles Basisgerät – der Access-Point (AP) – eine Funkzelle mit einem bestimmten Radius spannt und mehrere Geräte mit WLAN-Anschluss (WLAN-Clients) diese Funkzelle nutzen, um untereinander in Kontakt zu treten (siehe Abb. 1). Dabei können zwei kommunizierende Clients weiter auseinander liegen als im Ad-Hoc-Modus, da der AP als Zwischenstation und Vermittler fungiert. Dieser Modus wird Infrastrukturmodus, manchmal auch Basic Service Set (BSS), genannt. Clients melden sich beim AP an, der diese verwaltet und koordiniert. Häufig sind APs gleichzeitig auch Router und können so Verbindungen in andere Netze, zum Beispiel ins Internet, herstellen.

Erweiterte Funknetze

Die Reichweite von WLAN-Funkzellen ist stark von der räumlichen Umgebung abhängig und beträgt zwischen 30 und 100 Metern. Das ist für viele Wohnungen ausreichend. Soll ein grösseres Firmengebäude oder gar ein ganzes Gelände damit abgedeckt werden, so ist diese Reichweite aber meistens zu gering. Es bestehen mehrere Möglichkeiten, eine grössere Abdeckung durch das WLAN zu erreichen. Allen Lösungen ist jedoch gemein, dass sie nicht mehr nur aus einem einzigen AP und einigen WLAN-Clients bestehen, sondern immer mehrere APs umfassen.

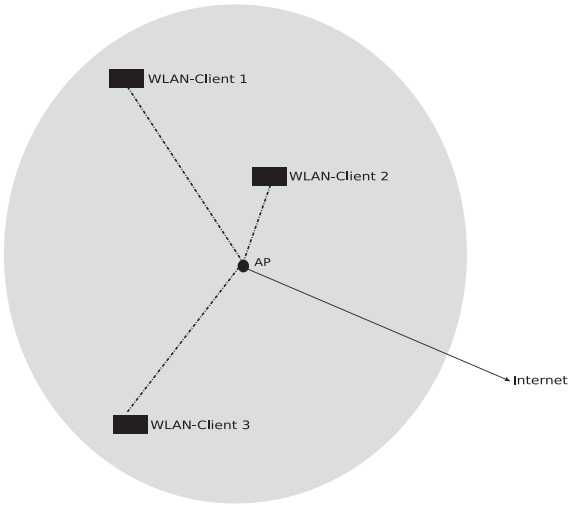

Abb. 1: Der Access Point (AP) spannt eine Funkzelle auf an der mehrere WLAN-Clients teilnehmen

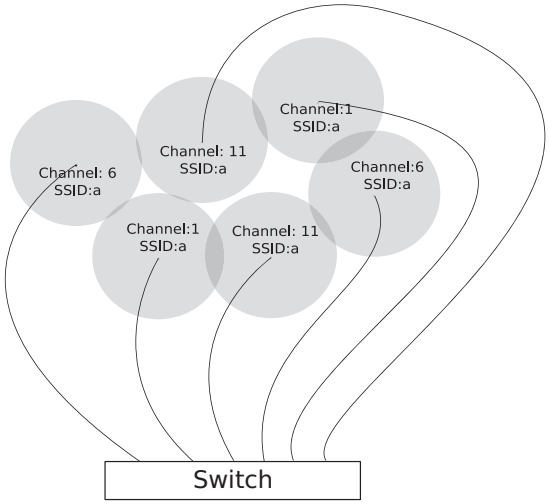

Abb. 3: Flächendeckendes WLAN mit kabelgebundenem Distribution System

Geht es lediglich darum, an jedem Ort via WLAN Zugriff auf das Internet zu realisieren, können mehrere APs mit Routing-Funktion und Internetanbindung so aufgestellt werden, dass alle relevanten Bereiche des Geländes mindestens durch eine Funkzelle abgedeckt sind. Der Nachteil dieser Lösung ist, dass zu jedem AP eine Internetanbindung geführt werden muss und dass die Gesamtheit aller WLAN-Zellen kein zusammenhängendes Netz bildet, in welchem alle eingebuchten WLAN-Clients untereinander erreichbar sind (siehe Abb. 2). Dieser Nachteil kann unter Verwendung eines gemeinsamen, kabelbasierten Backbones (Distribution Systems) wettgemacht werden (siehe Abb. 3). Bei einer solch modifiziernten Konfiguration spricht man nicht mehr vom Basic Service Set, sondern vom Extended Service Set (ESS). Es handelt sich beim ESS um eine Kopplung zweier oder mehrerer BSS. Das Distribution System wird meist über ein lokal vorhandenes Netzwerk, z.B. ein Ethernet, kabelgebunden realisiert. In einem derartigen ESS ist sogar ein ziemlich nahtloses Handover möglich, was bedeutet, dass sich WLAN-Clients im ganzen WLAN-Netz frei bewegen können, ohne dass die Verbindung beim Einbuchen an den nächsten AP unterbrochen wird. Ein weiterer Vorteil ist, dass infolge des Backbones alle WLAN-Clients untereinander erreichbar sind.

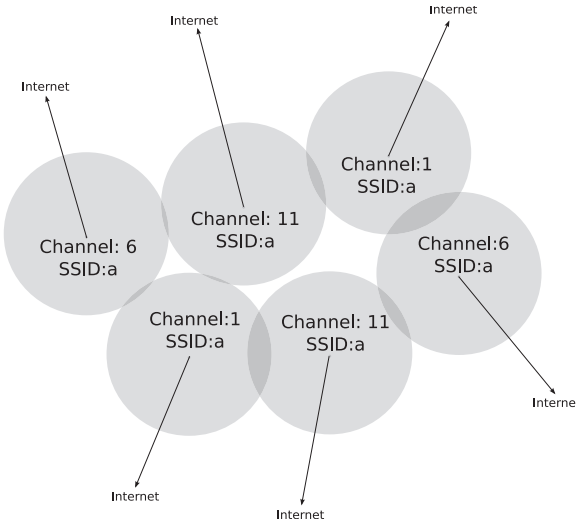

Abb. 2: Grossflächige WLAN-Abdeckung mit separatem Internet-Anschluss pro Funkzelle

Kabelloses Backbone

Ausgehend von der zuletzt beschriebenen Netzwerktopologie liegt es auf der Hand, das kabelgebundene durch ein kabelloses Backbone (Wireless Distribution System, WDS) zu ersetzen. APs, die heute schon ein solches WDS unterstützen, können meist entweder im Bridge-Modus oder im Repeater-Modus operieren. In beiden Fällen ist jedoch mit einem nicht unwesentlichen Konfigurationsaufwand zu rechnen.

Der Bridge-Modus dient dazu, z.B. zwei Ethernet-Switches kabellos miteinander zu verbinden (Point-to-Point); an jedem Switch ist ein AP angeschlossen, der via Funk die Verbindung zwischen den Switches herstellt (siehe Abb. 4). In diesem Betriebsmodus kann sich kein WLAN-Client bei den zwei ausgezeichneten APs einbuchen; die APs dienen exklusiv als Bridge.

Im Repeater-Modus kommunizieren alle APs und Clients auf dem gleichen Kanal. Jeder AP sendet alles was er empfängt an seinen benachbarten AP weiter (siehe Abb. 5). So kann die Reichweite des Funknetzes zwar vergrössert werden, doch reduziert sich die Übertragungsrate pro eingesetztem Repeater, da der gemeinsame Funkkanal infolge der Weiterleitung länger belegt bleibt.

Maschennetze

Ein Maschennetz ist grundsätzlich eine Netzwerktopologie, bei welcher jeder Knoten mit einem

Abb. 4: Zwei Access-Points im Bridge-Modus verbinden zwei Ethernet Switches

oder mehreren anderen Knoten verbunden ist. Bei einer vollständig vermaschten Topologie ist jeder Knoten mit jedem anderen verbunden. Das Ziel der Maschen-Funknetze ist es, Datennetze zu bilden, die sich durch einfaches Hinzufügen eines sogenannten Maschenknotens (eines speziellen AP) von alleine bilden und ohne Kabelverbindungen auskommen. Man spricht von mobilen Ad-Hoc-Netzwerken (MANET), wenn die Knoten auch noch mobil sein können. MANETs sind eine Unterkategorie von Maschennetzen. Maschennetze gelten als die ausfallsicherste Netzwerktopologie, die allerdings komplexe Routing-Algorithmen notwendig macht. Der Übergang in andere Netze, z.B. das Internet, soll nur an wenigen Maschenknoten realisiert werden müssen (theoretisch an genau einem) und von allen Teilnehmern als Gateway benutzt werden können. Es wird somit eine logische Kombination der beiden in Abb. 2 und Abb. 3 gezeigten Topologien angestrebt. Die APs sollen sich selbständig via Funk verbinden, damit ein durchgehendes Funknetz existiert, in welchem alle WLAN-Clients untereinander erreichbar sind.

Das Problem der Schleifen

Auf den ersten Blick scheint die funkbasierte Vermaschung der APs ein kleiner Schritt zu sein. Doch bereits bei genauerer Betrachtung erkennt man Probleme, wie sie bei kabelgebundenen LANs ebenfalls auftreten, wenn redundante Wegstrecken zur Erhöhung der Ausfallsicherheit geführt werden. Es geht bei den Problemen unter anderem um die Mehrfachübermittlung von Paketen, die ein Netz mit unnötigem Datenverkehr fluten und so das Funktionieren des Netzes gefährden.

Ein Ethernet-Netzwerk, wie in Abb. 6 dargestellt, würde sehr rasch mit Datenverkehr geflutet, da Pakete, die von LAN-Client 1 nach LAN-Client 2 gesendet werden, auf mehreren Pfaden ans Ziel gelangen können und bald im Kreis rotieren wür-

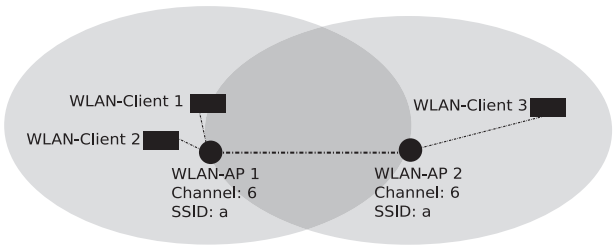

Abb. 5: WLAN-Zelle mit einem AP als Repeater, der die Reichweite erweitert

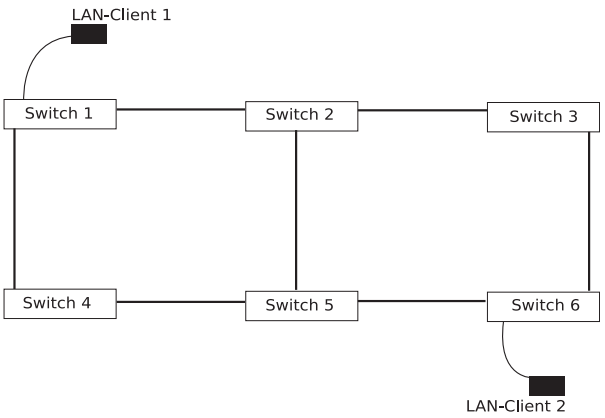

Abb. 6: Schleifen lassen ein Kabelnetz aus dem Tritt kommen

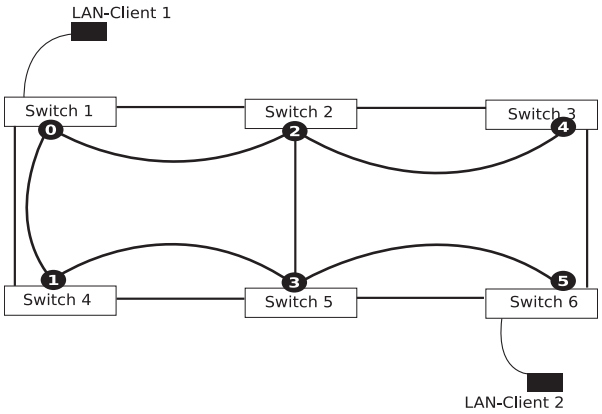

Abb. 7: Logische Topologie ohne Schleifen durch den Spannbaum

den. Die physikalische Topologie ermöglicht diese Situation und ohne getroffene Gegenmassnahmen wäre das Netz auch tatsächlich sofort überlastet. In kabelgebundenen LANs, in welchen aber genau solch redundante Verbindungen wie z.B. zwischen Switch 2 und Switch 5 oder zwischen Switch 3 und Switch 6 erwünscht sind, kommt ein Netzwerkprotokoll zum Einsatz, welches von allen Switches beherrscht werden muss. Es legt eine logische Netztopologie über die physikalische Topologie, so dass zu jedem Ziel genau ein Pfad führt. Das hierfür verwendete Protokoll bedient sich dem Spannbaum aus der Graphentheorie (siehe Abb. 7) und nennt sich denn auch Spanning Tree Protocol (STP). Es ist in der IEEE-Norm 802.1D standardisiert [IEE04]. Datenpakete werden dann nur noch auf den Pfaden des Spannbaumes transportiert. Fällt eine Verbindung in diesem Baum aus, so spannt das Protokoll automatisch einen neuen Spannbaum.

Falls keine geeigneten Protokolle verwendet werden, tritt das gleiche Überflutungsproblem auch in einem vermaschten WLAN-Netz auf, welches über ein kabelloses Backbone verfügt. Bei Funknetzen, zumal sie sich erst noch spontan bilden können und die Knoten mobil sind, eignen sich aber nicht dieselben Protokolle. Für vermaschte Funknetze eignet sich vor allem das Optimized Link State Routing.

Optimized Link State Routing

Beim Optimized Link State Routing Protokoll (OLSR) handelt es sich um eine optimierte Variante des bekannten Link State Routing Protokolls, welches die kürzesten Wege in einem kantengewichteten Graphen bestimmt [CLA03]. Die Gewichtung der Kanten wird als Distanz bezeichnet und wird mittels der Antwortzeit eines Nachbarknotens auf eine Kontrollmeldung berechnet. OLSR benötigt keine zentrale Verwaltungsstelle. Die Topologie bildet sich, indem die Knoten periodisch Kontrollmeldungen senden, um gegenseitig Nachbarschaftsinformationen auszutauschen. Jeder Nachbar muss umgehend auf diese Meldungen antworten. Mit diesen Nachbarschaftsinformationen erstellt sich jeder Knoten seine eigene Routing-Tabelle und kann mit einem geeigneten Algorithmus den kürzesten Weg zu jedem Knoten berechnen.

Die Optimierung von OLSR gegenüber dem Link State Routing liegt darin, dass jeder Knoten aus den direkten Nachbarn nur eine beliebige Untermenge auswählt, und diese in sein sogenanntes Multi Point Relay Set (MPR) stellt (siehe Abb. 8). Wenn ein Knoten eine Meldung versendet, so wird diese nur von jenen Nachbarknoten weitergeleitet, die sich im MPR-Set des sendenden Knoten befinden. Die Idee der MPRs ist also, die Broadcast-Meldungen beim Fluten des Netzes zu reduzieren.

802.11s der neue Standard für Maschen-WLANs

Bis zum heutigen Zeitpunkt ist noch kein Standard verabschiedet worden, der die Funktionsweise von Maschen-Funknetzen beschreibt. Doch mit IEEE 802.11s ist eine Teilspezifikation des Industriestandards 802.11 am Entstehen, der es gestatten soll, dass Geräte unterschiedlicher Hersteller Maschennetze mittels WLAN spannen können [IEE07]. Im Juni 2005 sind 15 Vorschläge für diesen Standard eingereicht worden, von denen zwei den grössten Zuspruch hatten. Zum einen handelt es sich um die SSEMesh-Gruppe, in der hauptsächlich die Firmen Cisco und Intel dabei sind. Zum anderen gibt es die Wi-Mesh-Allianz mit den Firmen Philips, Swisscom Innovation und Nortel. Die Vorschläge dieser beiden Gruppen sind im Januar 2006 vereint worden und das Resultat dieser Verschmelzung dient momentan als Ausgangslage zur Erarbeitung des 802.11s Standards. Es wird erwartet, dass dieser im Jahr 2009 verabschiedet wird.

Heute gibt es erste Hersteller, die Maschen-Access-Points mit einem Pre-Standard 802.11s anbieten und deren Geräte noch als proprietär zu bezeichnen sind. Zu nennen sind unter anderem die Hersteller Motorola, Cisco, Firetide, Nortel, Packethop, Belair und auch Meraki. Viele der erhältlichen Mesh-WLAN-APs können auch als herkömmliche WLAN-Clients eingesetzt werden. Selbst das Handover wischen den verschiedenen Zellen beherrschen einige Geräte.

Eigene Erfahrungen mit Mesh-WLAN

Wir haben an zwei verschiedenen Standorten separate Mesh-WLANs auf der Basis des Berliner Freifunkprojektes aufgebaut [FRE07b]. Als geeigneter AP wird in diesem Projekt der WRT54G-Router der Firma Linksys empfohlen, unter an-

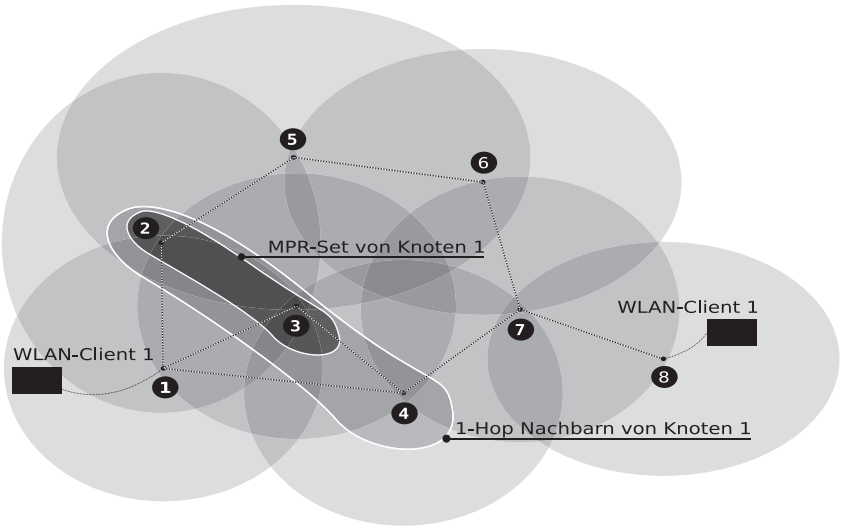

Abb. 8: OLSR hat eine logische Netztopologie gespannt

derem weil er die Anpassung der Sendeleistung zulässt und weil der Quellcode für die Original-Firmware von Linksys veröffentlicht worden ist. Dadurch sind eine Vielzahl von erweiterten Firmwares entstanden (BatBox [WRT07b], Wifibox [SFN07a], Sveasoft [SVE07] und OpenWRT [WRT07a]), die der WRT54G-Familie zusätzliche Funktionen bescheren, welche sonst nur bei viel teureren Routern vorhanden sind [FRE07a]. Die Routers dieser Familie unterstützen Internetverbindungen mit mehreren Clients über Ethernet 802.3, WLAN 802.11b sowie WLAN 802.11g

In unseren beiden Netzwerken verwenden wir APs vom Typ WRT54GL (L steht für Linux, Version 4 mit BCM5352E Chipset und 200-MHz-CPU). Dies weil die Weiterentwicklung vom WRT54G keine erweiterte Firmware mehr zulässt. Diese Weiterentwicklung hat dazu geführt hat, dass ab Version 5.0 der Router anstelle von Linux nur noch mit dem weniger ressourcenintensiven Betriebssystem VxWorks der Firma Wind River Systems läuft. Sie lässt momentan nur die originale Firmware von Linksys zu.

Ein Ziel von Maschen-Funknetzen kann es sein, Datennetze auf Bedarf hin zu bilden oder anzupassen. Soll sich also das Maschennetz durch einfaches Hinzufügen eines APs von alleine neu organisieren, so müssen drei Voraussetzungen erfüllt sein. Erstens müssen die APs im Ad-Hoc-Modus betrieben werden, so dass jeder AP direkt mit jedem anderen AP kommunizieren kann. Zweitens müssen alle APs dieselbe ESSID verwenden. Die ESSID (Extended Service Set Identifier) erlaubt die eindeutige Identifikation des WLANs und wird benötigt, damit die Clients in einem erweiterten Funknetz den richtigen AP finden. Drittens müssen die APs die erweiterten Routing-Funktionen anbieten. Üblicherweise bauen die Hersteller diese aber nicht in ihre Geräte ein, so dass man mit einem Austausch der Firmware selber dafür sorgen muss.

In unseren beiden Netzwerken haben wir uns für die Firmware OpenWRT entschieden. Diese wird bei Lösungen empfohlen, die auf Optimized Link State Routing Protokoll (OLSR) basieren. OpenWRT ist eine Art Mini-Linux, das die Möglichkeit bietet, neue Pakete zu installieren [FRE07a].

Firmware-Upgrade und Betrieb

Bevor wir unsere APs (alle vom Typ WRT54GL) konfigurieren und in Betrieb nehmen können, tauschen wir bei jedem einzelnen AP die Firmware aus. Die Firmware wird unter [FRE07b] angeboten und kann ganz einfach auf den APs installiert werden. Alles was man tun muss ist, die Firmwaredatei bei sich lokal auf dem Computer bereit zu haben und die IP-Adresse des AP zu kennen, um so via Webbrowser auf die AP-Konfigurationswebseite zu gelangen. Beim WRT54GL findet man den Menupunkt „Administration“ und weiter den Punkt „Firmware Upgrade“. Wir mussten dann die sich auf unserem lokalen Computer befindende Firmware Binärdatei auswählen und den Upgrade Prozess starten. Alles was man jetzt noch tun muss, ist acht zu geben, dass der Vorgang nicht durch einen Stromausfall unterbrochen wird. Eine genaue Anleitung befindet sich in [FRE07d].

Die anschliessende Konfiguration der APs verläuft standardmässig: Kanäle, Netzwerkmodi, Gerätenamen und Service Set Identifier (SSID) wählen. Für die Beschränkung des Zugriffs kann zudem der übliche Sicherheitsmechanismus aktiviert werden. Danach sind die APs betriebsbereit und es reicht, einen von ihnen über ein Kabel ans Internet anzuschliessen. Die andern müssen nur noch strategisch platziert werden, wobei darauf geachtet werden muss, dass sie in Verbindung

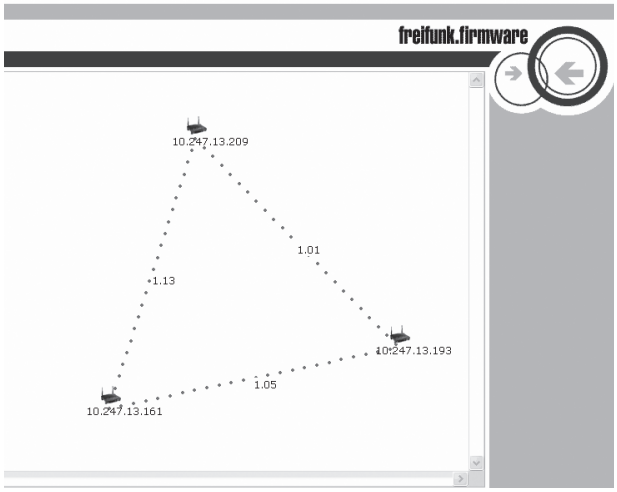

Abb. 9: Vermaschung von 3 APs

mit ihren Nachbarn bleiben. Ab diesem Zeitpunkt können mobile WLAN-fähige Geräte (Laptop, Pocket PC, usw.) eine drahtlose Netzwerkverbindung mit einem der verfügbaren AP aufbauen und eine Netzwerkadresse beziehen.

Das vermaschte Netzwerk lässt sich nun im Browser eines Rechners mit Internet-Zugang visualisieren. Dazu gibt man als Web-Adresse die IP-Nummer des zuvor ans Internet angeschlossenen APs ein. Daraufhin öffnet sich eine Webseite „freifunk.firmware“ und mit der Auswahl „OLSR-Viz“ erscheint eine Graphik des vermaschten WLAN-Netzwerks (siehe Abb. 9).

Ausblick auf mögliche Anwendungen

Mobile drahtlose Maschennetze ermöglichen interessante Anwendungen. So ist es zum Beispiel möglich, gerade an dem Ort, wo die nötige Infrastruktur fehlt, ein spontanes Funknetz zu errichten. Denkbare Szenarien sind Katastrophenfälle, wo in einem entlegenen Gebiet viele Hilfskräfte auf einem eng begrenzten Gebiet erscheinen und ein spontan gebildetes Datennetz von Nutzen ist, um die notwendigen Handlungen untereinander abzusprechen und Informationen auszutauschen.

Ein anderes schönes Beispiel, in welchem der einfache und kostengünstige Aufbau der Kommunikationsinfrastruktur im Vordergrund steht, zeigt das 100-Dollar-Laptop-Projekt, welches von der gemeinnützigen Organisation „One Laptop Per Child“ unter Vorsitz des MIT Professors Nicholas Negroponte gegründet wurde. Der dabei entwickelte Laptop verfügt ebenfalls über Maschen-WLAN. Er soll vor allem in Entwicklungsländern zum Einsatz kommen, wo keine vorhandenen Netzinfrastrukturen vorliegen, ein Austausch unter den Benutzern aber genauso gefragt ist und der Anschluss eines einzigen Laptops ans Internet allen den Zugang zum World Wide Web erlaubt.

Alleine durch die Tatsache, dass in einem Maschennetz die Abstände zwischen den Maschenknoten klein sind und sich mehrere Funkzellen überlappen müssen, wird unter der Voraussetzung der bekannten Position der festen APs eine recht genaue Lokalisierung der Teilnehmer auch ohne Zugriff auf Satelliten möglich. Genau diese Lokalisierung gestattet den mobilen Nutzern neuartige, ortsbezogene Anwendungen einzusetzen. Eine Fahrplananfrage für die nächstgelegene Haltestelle des öffentlichen Verkehrs könnte dann wesentlich komfortabler als heute geschehen, indem zum Beispiel nur noch der Zielort eingegeben werden muss. Das zu verwendende Transportmittel, allfällige Umsteigestationen und die Dauer bis zur nächstmöglichen Abfahrt können sofort angezeigt werden.

Ganz allgemein gilt: Die Ortsbezogenheit kombiniert mit anderen innovativen Ideen wird eine Vielzahl von innovativen Anwendungen ermöglichen.

Referenzen

[CLA03] T. Clausen, P. Jacquet, Optimized Link State Routing Protocol (OLSR), 2003

[FRE07a] J. Neumann, M. Behling, Was ist freifunk?, 2007

[FRE07b] Freifunk, http://freifunk.net, 2007-03-14

[FRE07c] Freifunk, http://freifunk.net/wiki/WikiStartSeite, 2007-03-14

[FRE07d] Freifunk, Linksys WRT54G Installation besserer Firmware, http://wiki.freifunk.net/Linksys_WRT54G_Installation_besserer_Firmware, 2007-03-14

[IEE03] IEEE 802.11 working group, ANSI/IEEE Std 802.11, 1999 Edition (R2003), 2003

[IEE04] IEEE 802.1 working group, IEEE Standard for Local and metropolitan area networks Media Access Control, 2004

[IEE07] IEEE 802.11s working group, Status of Project IEEE 802.11s, 2007-03-14

[NOR07] J. Lu, Taiwan‘s national center for traditional arts deploys nortel wireless mesh, 2006

[PAC07] PacketHop, Lakewood Police deploys New Jersey‘s First 4.9 GHz Broadband Mo-bile-mesh, 2007

[ROO07] D. Aguayo, J. Bicket, S. Biswas, D. S. J. De Couto, R. Morris, MIT Roofnet Imple-mentation, 2003

[SFN07a] WIFI-BOX - WRT54G(s) GPL Firmware, http://sourceforge.net/projects/wifi-box, 2007-03-14

[SVE07] http://www.sveasoft.com, 2007-03-19

[WRT07a] What is OpenWRT?, http://openwrt.org, 2007-03-14

[WRT07b] Linux on the WRT54G, http://www.batbox.org/wrt54g-linux.html, 2007-03-14