

Wireless LAN Konzept der ETHZ 2002

Version 1.0
4. April 2002

Zusammenfassung

Die Wireless LAN Installationen an der ETHZ unterliegen folgenden Richtlinien:

- Es gibt keine „ungeschützten“ Access-Points.
 - Installationen für eine grössere Benutzerschaft (public-WLAN) müssen mit einer Benutzer-Validierung auf Basis der N-ETHZ Accounts arbeiten. Wenn immer möglich soll dies über den VPN-Tunnel-Service mit IPSec Verschlüsselung geschehen.
 - Bei einer kleinen „closed user group“ (Arbeitsgruppe, Institut) muss mit WEP (Wired Equivalent Privacy) mit mindestens 40Bit gearbeitet werden, wobei der Schlüssel/Passwort nicht öffentlich publiziert werden darf.
- Alle Access-Points müssen mit einer korrekten SSID konfiguriert werden.
 - Bei Installationen die mit Benutzer-Validierung arbeiten, soll die SSID „public“ konfiguriert werden.
 - Bei Installationen mit WEP soll eine SSID auf der Basis des Subnetznamens gewählt werden.
- Die Standorte und die Konfiguration aller Access-Points werden von den Informatikdiensten koordiniert.

Die Ziele die mit diesem Konzept angestrebt werden:

- Stabiler und sicherer Betrieb der Wireless LANs und auch der herkömmlichen drahtbasierten Netzwerk-Installationen.
- Schutz der Netzwerk-Ressourcen, der -Infrastruktur und der verfügbaren Informationen.
- Vermeiden von Problemen durch sich gegenseitig überlappende Funkbereiche in verschiedenen Netzen.

Ausgangslage

Im Laufe der letzten Jahre wurde Wireless LAN Equipment gemäss Standard IEEE802.11b auf dem Markt allmählich verfü- und bezahlbar. Es entstand an der ETHZ, mitunter aufgrund der Publizität des ETHWorld Projektes WLAN, eine grosse Nachfrage verschiedenster Institute nach solchem Equipment. Übersteigerte Erwartungen, eine kinderleichte Installation (solange es sich nur um eine sehr kleine Installation handelt) und mangelndes Sicherheitsbewusstsein machen es notwendig, dass die Informatikdienste mit diesem Papier die Randbedingungen formulieren, denen Wireless LANs an der ETHZ unterliegen.

Motivation

Je länger je mehr stützt sich sowohl Lehre als auch Forschung auf Netzwerk-Dienste ab. Ein schnelles und stabiles Netzwerk ist inzwischen eine Selbstverständlichkeit und bei einem Netzwerk- oder Serviceunterbruch läuft so gut wie nichts mehr. Es ist darum im Interesse aller Beteiligten (Betreiber wie Benutzer) den Nutzen einer neuen Technologie zu maximieren und den möglichen Schaden derselben zu minimieren. Dabei gilt es drei Aspekte zu betrachten:

- Den Nutzen gilt es zu maximieren, indem die neue Technologie möglichst „artgerecht“ genutzt wird und durch sinnvolle Koordination Konflikte und Kollisionen vermieden werden.
- Schaden kann entstehen, wenn rechtliche Verpflichtungen nicht erfüllt werden. So werden einige der auf dem Netzwerk verfügbaren Dienste aus vertraglichen Bedingungen ausschliesslich für ETHZ Angehörige angeboten (z.B. Software-Verteilung, elektronische Publikationen der Bibliothek, u.s.w.). Die ETHZ muss mit geeigneten Massnahmen sicherstellen, dass diese Verträge erfüllt werden.
- Schaden kann durch absichtliche oder unabsichtliche Störung der Netzwerk-Infrastruktur entstehen. Da alle Netzwerk-Ressourcen in ihrer Stabilität gefährdet sind, muss einerseits die Gefährdung durch geeignete Massnahmen möglichst klein gehalten werden und andererseits muss im Notfall die Quelle der Störung möglichst schnell gefunden und isoliert werden können.

Alle drei Bereiche sind nicht neu, bilden jedoch durch die spezifischen Eigenschaften von Wireless LANs neue Herausforderungen die im Folgenden näher beleuchtet werden sollen.

Technische Grundlagen

Aufgrund der technischen Voraussetzungen weisen Wireless LANs die folgenden drei Problembereiche auf:

- Die nutzbare Bandbreite eines WLANs ist sehr begrenzt.
- Die Verbindung vom Client zum Funk-Netzwerk ist unsichtbar.
- Wireless LANs werden über ein shared Media betrieben.

Allen drei Problemkreisen kann mit geeigneten Massnahmen begegnet werden.

Die nutzbare Bandbreite ist sehr begrenzt.

Eine Wireless LAN Installation kann kein Ersatz für eine drahtbasierende Kommunikations-Infrastruktur sein, sondern sie soll diese wo nötig ergänzen und erweitern. Dies mit folgender Begründung:

Mit der heutigen Technik bieten Wireless LANs (IEEE 802.11b) bei einer rohen Bitrate von 11MBit/s eine nutzbare Bandbreite von etwa 5MBit/s pro Access-Point. D.h. alle Benutzer am selben Access-Point (theoretisch max. >250, praktisch ca. 10-20) teilen sich diese Bandbreite. Pro Benutzer bleiben somit 0.2 bis 0.5MBit/s an echter Bandbreite übrig.

Bei der heutigen Standardinstallation eines Arbeitsplatzes wird ein Netzwerkanschluss bereitgestellt der dedizierte 100MBit/s Bandbreite (FastEthernet) liefern kann. Damit ist ein kabelgebundenes LAN um einen Faktor 200 bis 500 schneller gegenüber einer Wireless LAN Lösung.

Ab ca. 2003 wird in Europa die nächste Generation von WLAN Produkten auf dem Markt erhältlich, resp. etabliert sein. Diese zukünftige Generation von Geräten (IEEE802.11a, Hyperlan2) wird momentan noch in Labors getestet und arbeitet mit 54 MBit/s roher Bitrate, d.h. voraussichtlich werden im alltäglichen Einsatz etwa 20Mbit/s brauchbar sein. Auch diese neue Technik verwendet noch immer ein shared media, d.h. auch diese zukünftig verfügbare Bandbreite muss weiterhin mit anderen Benutzern geteilt werden.

Dagegen sind bereits heute erste Produkte auf dem Markt erhältlich, mit denen ein kabelgebundenes LAN (sprich UKV) mit Geschwindigkeiten im Bereich von GBit/s betrieben werden kann. Bis zum Jahr 2004/2005 wird der Standardanschluss an der ETHZ wahrscheinlich 1000MBit/s dedizierte Bandbreite pro Arbeitsplatz anbieten. Während also auf dem WLAN Sektor eine Steigerung um den Faktor 4 zu erwarten ist, steigt die Bandbreite einer UKV um den Faktor 10. Damit wächst das Missverhältnis der nutzbaren Bandbreite pro Benutzer zwischen Wire-less und Wire-based LANs auf einen Faktor 500 - 1000 (20MBit geteilt durch 10-20 Benutzer = 1-2Mbit/Benutzer gegenüber 1000MBit/Benutzer).

Damit beschränkt sich der sinnvolle Einsatz einer WLAN Installation auf folgende Gebiete:

- Erschliessung von öffentlichen und halböffentlichen Bereichen wie Innenhöfe, Bibliotheks-Lesesälen, Cafeterias, Mensen, Sitzungszimmer u.s.w., damit diese als temporäre Arbeitsflächen z.B. für die Studierenden verwendet werden können.
- Erschliessung von Flächen, in denen mit beweglichen Computern gearbeitet werden soll.

Die Verbindung vom Client zum Funk-Netzwerk ist unsichtbar.

Dies hat mehrere Implikationen:

- Der Kreis der potenziellen Benutzerschaft (Clients) erstreckt sich nicht nur auf den Raum in dem sich der Access-Point (der fest installierte Teil einer WLAN-Installation) befindet. Die Zelle (der nutzbare Raum rund um den Access-Point) umfasst gewollt oder ungewollt auch die Nebenräume und unter Umständen auch Flächen ausserhalb des Gebäudes. Gute Antennen vorausgesetzt, kann ein Client bis zu mehreren hundert Metern vom Access-Point entfernt sein. Ein Access-Point kann nicht ohne weiteres zwischen berechtigten und nicht berechtigten Clients unterscheiden. Da es jedoch zum Schutz der Netzwerk-Ressourcen und der -Infrastruktur unerlässlich ist, ausschliesslich berechnete Benutzer zuzulassen, muss eine Validierung des Clients stattfinden.

Dies kann auf verschiedene Arten geschehen:

- Sämtliches Equipment ist kompatibel zu IEEE802.11b Standard und unterstützt das Wired Equivalent Privacy (WEP) Protokoll. Dabei werden die Daten auf der Luftstrecke mit 40 oder 128Bit verschlüsselt. Dazu muss in den Access-Points und in den Client-Karten ein Schlüssel oder ein Passwort konfiguriert werden. Alle berechtigten Benutzer müssen diesen Schlüssel kennen und ihre Client-Karten entsprechend konfigurieren. Es kann jeweils nur ein Schlüssel aktiv sein. WEP ist kein Sicherheits-Protokoll. Alle Clients die mit dem richtigen Schlüssel konfiguriert worden sind, können sämtlichen Datenverkehr an „ihrem“ Access-Point mithören. Diese Art der „Validierung“ kann nur funktionieren, wenn der Kreis der berechtigten Benutzer klein ist. Bei 20'000 potentiellen Benutzern kann WEP nicht mehr funktionieren, weil der WEP-Schlüssel sehr weit und offen publiziert werden müsste. WEP eignet sich jedoch für kleine „closed user groups“ wie Arbeitsgruppen oder Institute. Ebenso eignet sich WEP zur „Validierung“ von autonomen Computern (Computer, für die nach der Konfiguration keine Person mehr jederzeit zuständig ist und die keine eigentlichen Benutzer kennen, z.B. Drucker, autonome Roboter, intelligente Kühlschränke u.s.w.)
- Mit WEP findet keine Benutzer-Validierung statt, sondern es wird nur die Kenntnis, resp. Konfiguration des richtigen Schlüssels überprüft. Für grössere Benutzergruppen, z.B. alle Studierenden oder alle Mitarbeitenden, ist WEP ungeeignet und es muss eine echte Benutzer-Validierung eingeführt werden.

Dies wiederum ist auf zwei Arten möglich:

- Die Client-Karte erhält nach der Herstellung einer Verbindung zum WLAN, d.h. nach Eintritt in den Funkbereich eines Access-Points (Zelle) mittels DHCP (Dynamic Host Configuration Protocol) eine korrekte IP-Nummer mit allen dazu gehörenden Parametern (Netzmaske, Gateway, DNS-Server, u.s.w.). Mit dieser IP-Nummer kann jedoch, mit Ausnahme aller Rechner auf dem WLAN-Netz, nur eine sehr eng limitierte

Anzahl von Diensten erreicht werden. Ad-hoc Netzwerke (z.B. mehrere Rechner im selben Sitzungszimmer) sind somit ohne jede Validierung jederzeit möglich. Um mit dem gesamten Netzwerk verbunden zu werden, muss nun der Benutzer mittels eines SSH- (Secure Shell) Clients eine Verbindung zum Host VALID.ETHZ.CH aufbauen und sich mit seiner N-ETHZ Kennung bestehend aus Benutzername und Passwort ausweisen. Kann die Validierung erfolgreich durchgeführt werden, so wird die IP-Nummer, von der die SSH-Verbindung aufgebaut wurde, in eine dynamische Liste aufgenommen und die vorherigen Restriktionen sind aufgehoben. Der Client kann nun mit der ganzen ETHZ und der Welt transparent kommunizieren.

Der Eintrag in der dynamischen Liste wird nach einer Stunde ohne Aktivität oder nach insgesamt 12 Stunden wieder gelöscht.

Diese Validierungsmethode funktioniert im ETHWorld WLAN Projekt für alle Studierenden und Mitarbeitenden der ETHZ einwandfrei.

- Der Netzwerk-Client bezieht ebenfalls via DHCP eine korrekte IP-Konfiguration. Nun wird jedoch anstelle von SSH ein VPN-Tunnel (Virtual Private Networking) zum zentralen VPN-Server aufgebaut. Dazu muss ein entsprechender VPN-Client installiert sein, mit dem auch die Benutzer-Validierung durchgeführt werden kann.

Die Informatikdienste bieten einen solchen VPN-Service in zwei Varianten an:

- IPsec VPN-Tunnels mit Verschlüsselung (DES und 3DES). Dazu stehen VPN-Clients für alle Windows, Linux, Solaris und MacOS-X Betriebssysteme unter <https://n.ethz.ch/software/vpn> zur Verfügung. Kommerzielle Clients für MacOS 8 und 9, PalmOS und WinCE sind erhältlich. Mit diesen verschlüsselten VPN-Tunnels sind auch sämtliche Sicherheitsprobleme der Wireless LANs gelöst.
- PPTP VPN-Tunnels ohne Verschlüsselung. Die Microsoft Betriebssysteme bringen von Haus aus einen solchen VPN-Client mit, resp. dieser kann ab CD installiert werden. Bei diesen VPN-Tunnels ist nur die Login-Information verschlüsselt. Die eigentliche Datenübertragung ist im Klartext. Damit sind die Sicherheitsprobleme der WLANs teilweise gelöst.

Unter <http://www.id.ethz.ch/Dienste/VPN> ist eine allgemeine Beschreibung dieses Services zu finden.

Die VPN-Tunnel Variante (vor allem IPsec) ist von uns priorisierte Lösung zur Validierung der Benutzerschaft und zur Lösung der Sicherheitsproblematik. Als Nachteil ergibt sich daraus der möglicherweise nicht optimale Weg des Datenverkehrs (jedes Paket muss immer zuerst zum VPN-Server geschickt werden und gelangt erst von da aus zur eigentlichen Ziel-Destination). Ebenso können unter gewissen Umständen MTU- und Fragmentierungs-Probleme auftreten (das Tunnelprotokoll vergrössert ein Paket um ein paar wenige Bytes. Damit wird ein vom Client gesendetes Paket mit maximaler Grösse nun zu gross und muss fragmentiert werden. Dies ist suboptimal und kann unter gewissen Umständen zu Problemen führen).

- Da der Umfang einer Zelle nicht kontrollierbar ist, können sich Zellen ungewollt überlappen. Dies ist besonders dann der Fall, wenn am selben Ort mehrere Subnetze drahtlos übertragen werden. Ein Client kann jedoch zu jedem Zeitpunkt nur mit einem Access-Point in Verbindung stehen. Um die verschiedenen Zellen zu unterscheiden, ist eine „Radio Service Set Identification“ (SSID) vorgesehen. Jeder Access-Point muss mit einer SSID konfiguriert werden (alle Access-Points im ETHWorld Projekt WLAN haben die SSID „public“). Ein Client kann durch die Konfiguration der SSID bestimmen, mit welcher Zelle, resp. Subnetz, Verbindung aufgenommen werden soll. Ist die SSID nicht konfiguriert, so ist es Zufall, bei welchem Access-Point ein Client eingebucht wird. Die Überlappung der Zellen stellt auch noch aus einem anderen Gesichtspunkt ein Problem dar. Die Access-Points der überlappenden Zellen können sich auf der Funkebene stören. In Europa ist das ISM (Industrial, Science and Medical) Band (2.4-2.5 GHz), mit dem IEEE802.11b arbeitet, in 13 Kanäle aufgesplittet. Hierbei wird jedem Access-Point ein Kanal fest zugeordnet. Diese Kanäle überlappen sich jedoch mit den Nachbarkanälen und es muss darauf geachtet werden, dass benachbarte Access-Points mit einem genügend grossen Kanalabstand zueinander konfiguriert werden.

Glücklicherweise funktioniert ein WLAN auch noch einwandfrei, wenn dieser Umstand nicht beachtet wird. Allerdings wird dann die ohnehin schon sehr knappe Bandbreite noch zusätzlich dramatisch verschlechtert. Um dies zu vermeiden, müssen die Standorte aller Access-Points, die verwendeten Kanäle, die Sendeleistung und die Art der Antennen (Gewinn und Richtcharakteristik) koordiniert werden.

Wireless LANs werden über ein shared Media betrieben

Ein Problem welches beim Betrieb eines Wireless LANs auftritt, ist die Tatsache, dass diese Technik das Medium allen Clients gleichzeitig zur Verfügung stellt (shared media). Das bedeutet, dass sich alle angeschlossenen Clients, resp. alle bei einem Access-Point eingebuchten Client-Karten, die verfügbare Bandbreite teilen und alle Pakete von allen Clients empfangen werden (analog wie bei Netzwerken, die mit Coax-Kabeln betrieben wurden).

Dies birgt drei Probleme in sich:

- Erfahrungsgemäss sollten pro Access-Point höchstens 10-20 gleichzeitige Clients eingebucht sein, so dass pro Client noch eine „brauchbare“ Bandbreite zur Verfügung steht. Dies ist selbstverständlich stark von der Art der Benutzung abhängig. Wenn hauptsächlich Office-Applikationen verwendet werden, dürfen auch mehr Clients pro Access-Point eingebucht sein, arbeiten die Clients mit Bewegtgraphiken unter X-Windows, so ist die Bandbreite bereits für einen Client zu gering. Das IEEE802.11b Media Access Protokoll sorgt normalerweise dafür, dass die Bandbreite jederzeit „fair“ unter den Clients am Access-Point verteilt wird. Dies funktioniert jedoch nur gut, wenn alle Client-Netzwerk-Karten vom selben Hersteller stammen und mit den selben Low-Level Parametern arbeiten. Bei Karten von verschiedenen Herstellern kann es vorkommen, dass eine Karte den Medienzugriff monopolisiert und im Extremfall sogar über längere Zeit (mehrere Sekunden) die gesamte Bandbreite beansprucht.
- Sollen in einer Zelle mehr als 20 Clients bedient werden, so können weitere Access-Points installiert werden. Diese weiteren Access-Points müssen selbstverständlich auf unterschiedlichen Kanälen konfiguriert werden. Da maximal 13 Kanäle vorhanden sind, kann eine Zelle auch maximal mit 13 Access-Points ausgerüstet werden. Dies würde bedeuten, dass in einer Zelle bis zu 260 Clients bedient werden könnten. In Realität jedoch können innerhalb derselben Zelle, wegen der sich überlappenden Frequenzbänder benachbarter Kanäle, nur 3-4 Access-Points (mit gut gewählten Kanälen) verwendet werden. Dies bedeutet wiederum, dass pro Zelle nicht mehr als etwa 30-80 Clients „vernünftig“ arbeiten können.
- Durch den „shared Media“ Charakter bergen WLANs auch ein grosses Sicherheitsrisiko in sich. Client-Karten können ohne weiteres in den sog. „promiscuous Mode“ geschaltet werden und können dadurch den gesamten Datenverkehr der Zelle (resp. Access-Point), bei der dieser Client eingebucht ist, abhören. Dieser Umstand ist umso bemerkenswerter, da der Umfang einer Zelle, wie schon erwähnt, nicht wirklich kontrolliert werden kann. Die Access-Points der meisten Hersteller können eine Liste von MAC-Adressen der erlaubten Clients (=möglicher „Abhörer“) verwalten. Diese Technik kann bei 2 oder 3 Access-Points und einem Dutzend Clients noch mit einem vertretbaren Aufwand verwendet werden, bei Hunderten von Access-Points und mehreren Tausend Clients ist dieses Feature jedoch wenig hilfreich. Dies bedeutet, dass der Kreis der möglichen „Abhörer“ sehr gross ist. Die Tatsache, dass der Datenverkehr unbemerkt abgehört werden kann, muss vom Benutzer in seinem Verhalten in Betracht gezogen werden. Wenn immer möglich soll ein Verschlüsselungsmechanismus (SSL, SSH, IPSec, u.s.w.) verwendet werden und auf keinen Fall sollen Login-Informationen im Klartext übertragen werden. Wenn ein IPSec-VPN-Tunnel als Validierungsmethode gewählt wird ist die gesamte Strecke Client – VPN-Server verschlüsselt und damit auch die abhörbare Luftstrecke.

Schlussfolgerungen

Mit diesen Ausführungen sollen Wireless LANs an der ETHZ auf keinen Fall behindert werden. Die Komplexität von grösseren WLAN-Installationen macht es jedoch unabdingbar, dass der Aufbau einer solchen Infrastruktur auf koordinierte Weise geschehen muss. Als verantwortliche Betreiberin der drahtbasierenden Kommunikation sind die Informatikdienste prädestiniert, diese notwendige Koordinations-Funktion wahrzunehmen und damit auch die Rahmenbedingungen zu definieren.

Wireless LANs sind eine interessante und zukunftssträchtige Technologie. Wenn die Limitierungen und Schwächen der WLAN Technologie beachtet werden, so kann damit eine sinnvolle Ergänzung zur allgemeinen drahtbasierten Kommunikationsinfrastruktur aufgebaut werden.

Die Informatikdienste wollen nicht die alleinigen Installateure und Betreiber von WLANs sein. Instituts-interne Installationen können in Eigenregie beschafft, bezahlt und betrieben werden. Die Auflagen zur Koordination müssen jedoch beachtet und eingehalten werden.

WLANs, die von einer breiten Benutzerschaft verwendet werden können, (SSID=public), werden ausschliesslich von den Informatikdiensten beschafft, installiert und betrieben. Die Auswahl, die Anzahl und die Reihenfolge der Orte, die mit „public“ Access-Points ausgerüstet werden, liegt in der Entscheidung der Informatikdienste. Die Anzahl der neuen Standorte von Access-Points ist jedoch limitiert durch die vorhandenen Ressourcen (Geld sowie Planungs- und Installations-Arbeitszeit).

Bei der Auswahl der Standorte der Access-Points kommt folgendes Kriterium zur Anwendung: Je grösser der Nutzen ist, desto eher wird ein Access-Point installiert.

Dabei kann Nutzen verschiedene Aspekte aufweisen: (absteigende Relevanz)

- Anzahl möglicher Nutzer (Neue Flächen)
- Anzahl wirklicher Nutzer (Ausbau bestehender Flächen)
- Bedarf durch konkrete Lehrprojekte
- Als „Enabler“ von Lehrprojekten
- Bedarf durch konkrete Forschungsprojekte

Es besteht die Möglichkeit, dass durch Eigenleistung eines Departementes oder Institutes das „public“ WLAN an zusätzlichen Orten, als ursprünglich vorgesehen, erweitert wird. In Absprache mit dem WLAN-Verantwortlichen der Informatikdienste ist es möglich, konfigurierte „public“ WLAN-Access-Points zum Selbstkostenpreis (2kFr. Stand 1Q02) bei den Informatikdiensten zu beziehen. Die Installation obliegt dabei dem Departement oder Institut selbst (ebenfalls nach Absprache mit den Informatikdiensten). Die Informatikdienste sind anschliessend besorgt um die Wartung und den Betrieb dieser Access-Points.

Informationen über das Public Wireless LAN an der ETHZ sind erhältlich unter <http://www.wireless.ethz.ch/>

Der WLAN-Verantwortliche der Informatikdienste kann kontaktiert werden unter der E-Mail Adresse WLAN@id.ethz.ch