Aufbau und Betrieb des drahtlosen Netzes DUKATH an der Universität Karlsruhe

Willi Fries, Matthias Müller, Lars Wolf

Universität Karlsruhe (TH)
Zirkel 2
76128 Karlsruhe
{Willi.Fries, Matthias.Mueller, Lars.Wolf}@rz.uni-karlsruhe.de

Zusammenfassung Anfang 2000 begannen wir an der Universität Karlsruhe mit der Planung und dem Aufbau eines drahtlosen Netzes, um zusätzlich zum campusweiten, kabelgebundenen Kommunikationsnetz KLICK auch eine darüber hinaus gehende flexible Nutzung von Netzdiensten zu ermöglichen. In diesem Bericht wird der Aufbau und der Betrieb von DUKATH, dem **d**rahtlosen Kommunikationsnetz der **U**niversität **Ka**rlsruhe (**TH**), beschrieben.

1 Netzaufbau

DUKATH wird unter Einsatz von Funknetzkomponenten nach dem derzeit aktuellen IEEE 802.11b Standard aufgebaut. Bei dieser Technik wird das lizenzfreie 2,4 GHz ISM (Industrial, Scientific, Medical) Frequenzband verwendet, so dass keine nutzungsabhängigen Kommunikationsgebühren entstehen – nach der Anschaffung der Komponenten ist die Verwendung des Netzes für die Nutzer kostenlos. Vor allem die beiden folgenden Komponenten werden zur Funk-Versorgung eingesetzt:

Netzadapter (in PC-Card Bauform) zum Einschub in Laptops, etc. Es gibt auch die Möglichkeit diese über ein Trägermodul in anderen Rechnern einzusetzen.

Funknetz-Basisstationen, die die Infrastruktur des Funknetzes bilden und von denen ein Übergang in das Campusnetz erfolgt.

Die Basisstationen sind alle in ein spezielles, nur für dieses drahtlose Netz verwendete VLAN eingebunden, d.h., die Basisstationen sind alle Teil eines logischen LANs (auch wenn sie weit über den Campus verteilt sind). Dieses VLAN ist mit den regulären Komponenten unseres Campus-Netzes KLICK aufgebaut, also der auch ansonsten für Festnetzanschlüsse eingesetzten Switches, etc. Von diesem VLAN gibt es genau eine dedizierte Übergangsmöglichkeit über einen Router in das Campusnetz. Eine direkte Kommunikation mit einem Gerät im Festnetz über einen anderen Weg als diesen Router ist nicht möglich. Zwischen Geräten innerhalb des Funknetzes kann selbstverständlich eine direkte Kommunikation erfolgen.

2 Betriebs- und Sicherheitskonzept

Bei dem Aufbau und der Konzeption des Netzes war für uns die Verwendung von standardkonformen Komponenten wichtig, d.h., wir wollten keine proprietären Techniken einsetzen, auch wenn diese zu einem bestimmten Zeitpunkt evtl. Zusatzfunktionalität bieten

würden. Wir wollen uns nicht zwangsläufig an einen einzelnen Hersteller binden und rechnen damit, dass auf Dauer eine heterogene Umgebung mit Komponenten verschiedener Hersteller entstehen kann und haben hierzu auch Komponenten verschiedener Hersteller untersucht.

DUKATH soll vor allem IP Protokolle unterstützen, also dem ohnehin vorherrschenden Trend entsprechend, IP als dominantes Vermittlungsprotokoll zu verwenden. Wir beabsichtigen nicht andere Protokolle aus diesem Netz zu verbannen, sehen aber derzeit keine große Notwendigkeit für eine konkrete aktive Unterstützung. Die Vergabe der IP-Adressen für die Rechner in DUKATH erfolgt über DHCP.

Ein wesentlicher Punkt für das Netzkonzept ist die Frage des notwendigen administrativen Aufwands und der Sicherheit. Wir wollen sowohl einen Schutz gegenüber dem Missbrauch dieses Netzes erreichen, so dass auch nicht unbefugt von dem Funknetz der Internet-Anschluss der Universität genutzt werden kann, als auch den administrativen Aufwand möglichst gering halten.

Insgesamt muss also die Verwendung des drahtlosen Netzes auf Personen eingeschränkt werden, die dem RZ als Betreiber des Netzes bekannt sind, so dass nicht eine fremde Person mit einer Funknetzkarte einfach das Netz benutzen kann. Bei den 802.11b Funkkomponenten wird dies unterstützt, indem eine Überprüfung der MAC-Adressen der einzelnen Funknetzkarten stattfinden kann. Die Basisstationen können dann bei jedem Datenpaket überprüfen, ob die MAC-Adresse des Absenders in einer Zulassungsliste eingetragen ist. Dieses Verfahren ist bei einer kleinen Anzahl an Nutzern sicher gut geeignet, um einen Zugangsschutz zu erreichen. Bei einer großen Nutzerzahl, wie wir Sie letztendlich an der Universität anstreben, halten wir diesen Ansatz nur bedingt für geeignet. Ein weiteres vom Standard vorgesehenes Verfahren ist der Einsatz von Funknetznamen, nur wenn der richtige Name in dem Rechner eingetragen ist, kann er das Funknetz verwenden. Allerdings ist bei einer großen Anzahl an Nutzern, bei einer Universität wie in Karlsruhe kann dies mittel- bis langfristig sicher im Bereich von etlichen hundert bis einigen tausend liegen, der Wert solcher “Geheimnisse” recht gering.

Das für DUKATH erarbeitete Konzept sieht eine Authentisierung bei einer entsprechenden Server-Komponente im Netz zu Beginn einer Sitzung vor; dies entspricht dem Vorgehen, wie es auch bei der Telefoneinwahl üblich ist. Neben der Verhinderung der Nutzung unserer Ressourcen durch evtl. unbefugte Personen können wir mit diesem Verfahren auch sehr flexibel Sicherheits- und Vertraulichkeitsaspekte berücksichtigen und bspw. Verschlüsselungsverfahren einbinden. Wir wollen damit auch die Möglichkeit schaffen, dass sich Mitarbeiter direkt in ihr jeweiliges Institutssubnetz “einwählen” können, also die Ressourcen ihrer Einrichtung wie gewohnt verwenden können, so als wenn sie an ihrem Arbeitsplatz säßen.

Wenn keine solche Authentisierung durchgeführt wird, dann kann keine Kommunikation mit Rechnern im Campus-Netz oder im Internet erfolgen. Abbildung 1 zeigt exemplarisch die notwendige Anmeldung eines Nutzers bei einem der Gateways (die beim Übergangs-Router DUKATH / KLICK als zugelassen eingetragenen sind). Alle Kommunikation dieses Nutzers erfolgt in einem sogenannten Tunnel zu diesem Gateway, der auch mittels Verschlüsselung die Daten schützen kann, von dort aus werden die Daten dann an den eigentlichen Zielrechner weitergegeben. Ohne diese Authentisierung werden die Daten beim

Übergang in das Campus-Netz durch den Router verworfen wie es durch die untere Linie symbolisiert wird.

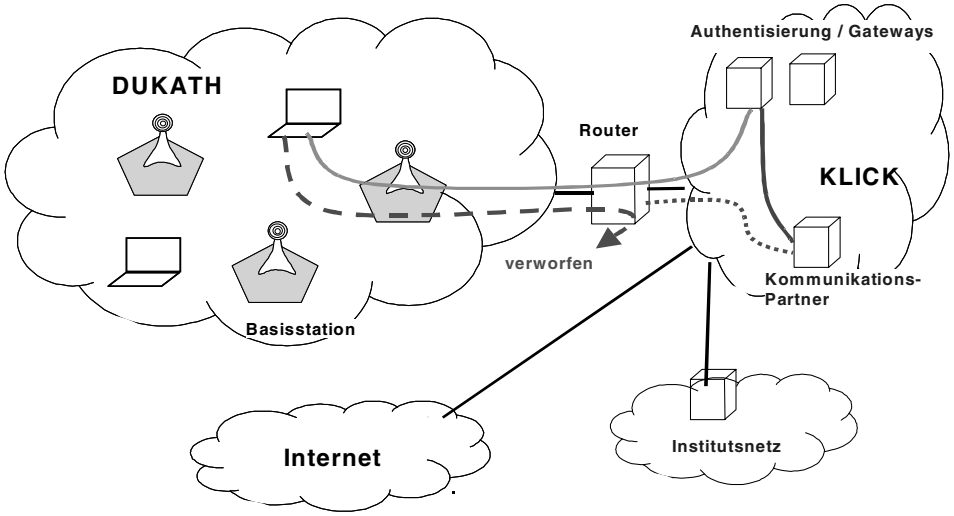

Abbildung 1. Erforderliche Anmeldung zur Nutzung von DUKATH

Bei der expliziten Zugangskontrolle in DUKATH mittels Benutzerkennung und Passwort werden Techniken zum Aufbau von VPNs (Virtuellen Privaten Netzen) eingesetzt, hiermit wird zwischen dem Endgerät und dem zuvor erwähnten Gateway ein Tunnel aufgebaut. Zunächst erhält ein Endgerät innerhalb von DUKATH mittels DHCP nur eine private IP Adresse zugewiesen. Nach der Anmeldung bei einem bekannten VPN-Gateway erhält das Endgerät eine IP-Adresse für den bei diesem Gateway endenden Tunnel zugewiesen. Durch die Einrichtung mehrerer solcher Gateways können dann zum einen verschiedene Protokolle unterstützt werden (so dass neueren Entwicklungen leicht gefolgt werden kann). Zum anderen kann somit auch die direkte ‚Einwahl' in ein Institutsnetz ermöglicht werden, so dass ein Mitarbeiter also alle Ressourcen seines Institutsnetzes so verwenden kann wie es mit einem drahtgebundenen Anschluss direkt im Institut der Fall wäre.

Unsere Ziele beim Einsatz von VPN-Verfahren waren neben dem Angebot der direkten Einbindung in ein Institutsnetz, der Sicherung des Netzzugangs, also das der Zugriff auf andere Netze nur über das Gateway erfolgen kann, auch das soweit möglich keine Änderungen bei den Client-Rechnern nötig wären und die Verwendung dieser Verfahren transparent für Nutzer ist. Daher ergibt sich die Notwendigkeit Verfahren der OSI Schichten 2 oder 3 einzusetzen. Auf der Schicht 2 gibt es derzeit die Möglichkeiten PPTP (Point to Point Tunneling Protocol) von Microsoft und L2TP (Layer 2 Tunneling Protocol), welches auf PPTP und L2F (von Cisco) basiert. Auf Schicht 3 ließe sich das IP Security Protocol IPSec einsetzen.

Aufgrund der direkten Verfügbarkeit von PPTP-Client-Software (bspw. für verschiedene Windows-Versionen und Linux) bieten wir nun ein PPTP-Gateway an und beabsichtigen ein zusätzliches L2TP-Gateway aufzubauen. Bei PPTP wird sozusagen die PPP (Point-to-Point Protocol) Übertragungsstrecke über das IP-Netz "verlängert". Eine Authentifizierung des Clients erfolgt innerhalb der Aufbauphase der PPP Verbindung und die transportierten Pakete innerhalb von PPP können verschlüsselt werden.

3 Betriebserfahrung

Vordergründig scheint eine 100% -tige Kompatibilität der Funknetzkomponenten gegeben zu sein. Dies stimmt nach unseren Erfahrungen auch, soweit es die Verbindungen zwischen Funknetz-Basisstationen und PC-Netzadaptern betrifft. Erfreulicherweise klappt auch die Übergabe (Roaming) der Netzadapter von einer Basisstation zur anderen problemlos, auch dann, wenn die Basisstationen nicht vom gleichen Hersteller sind. Es ist uns aber bis heute nicht gelungen eine Kommunikation zwischen zwei Basisstationen verschiedener Hersteller drahtlos herzustellen. (Offenkundig erlaubt der Standard an dieser Stelle wohl zu viele Freiheiten).

Problematischer ist die Vielfalt der Netzadapter und deren Treiberversionen. Die schnelle Entwicklung stellt uns vor die Wahl entweder laufend neue Installationsanleitungen zu schreiben oder laufend in Beratungsgesprächen verwickelt zu sein.

Positive Erfahrungen haben wir mit dem PPTP-Server gemacht. Dieser läuft unter Linux stabil und ein spürbaren Overhead ist lediglich beim ersten Verbindungsaufbau in Form einer etwas höheren Delay-Zeit festzustellen.

Die maximal beobachtete Anzahl gleichzeitig aktiver Benutzer lag bei knapp 40, wobei mehr als 100 Accesspoints installiert sind. So ist es nicht verwunderlich, daß bislang noch keine Klagen über Bandbreitenengpässe erfolgten. Auch bei Veranstaltungen, wie bspw. einer Tagung, mit vielen DUKATH-Nutzern an einem Accesspoint, wurde die verfügbare Bandbreite nicht bemängelt. Dementsprechend konnten wir auch den Erfolg unserer Funkkanal Optimierungsversuche für die Basisstationen noch nicht überprüfen.

Der verwendete VPN-Ansatz, also der Einsatz von PPTP, hat sich bislang bewährt und konnte in gleicher Form auch für weitere Zwecke genutzt werden. Die in unserem Netz eingesetzten Client-Rechner der Nutzer werden u.a. mit verschiedenen Windows-Varianten, Linux und MAC OS9 betrieben. Auch die zuvor erwähnten Besucher einer internationalen Tagung konnten mit ihren Geräten und hierfür ausgegebenen Nutzerkennungen DUKATH verwenden und waren damit sehr zufrieden. Des Weiteren sind wir durch den Einsatz dieses VPN kaum von den kürzlich aufgedeckten Problemen mit der WEP-Verschlüsselung betroffen. Um PPTP-Sicherheitsmängeln entgegenzutreten werden wir zukünftig auch weitere VPN-Verfahren wie IPSec einsetzen.

Problematisch gestalten sich die Verbindungen zwischen Accesspoints, weil da gegenseitig die jeweiligen Hardwareadressen eingetragen werden müssen. Wenn da nicht genau darauf geachtet wird, daß sich die Funkkanäle nicht überschneiden, kommt es zum zeitweiligen Ausfall der Verbindungen.

4 Zusammenfassung und Ausblick

Drahtlose Netze wie DUKATH werden in Zukunft an vielen Hochschulen eingesetzt und die Nutzung von Rechnern in Lehrveranstaltungen im speziellen und die Form der Lehre im allgemeinen verändern. DUKATH soll die bisher vorhandene sehr gute Infrastruktur weiter ausbauen und verbessern sowie neue und erweiterte Möglichkeiten zum Lehren und Lernen, zum Forschen und Arbeiten an der Universität Karlsruhe bieten. So verfolgen wir beim Aufbau von DUKATH das Ziel sowohl der Bereitstellung von Kommunikationsmöglichkeiten an möglichst jeder Stelle des Universitäts-Campus als auch des Einsatzes dieses drahtlosen Netzes in konkreten Nutzungsszenarien. Erste Erfahrungen mit DUKATH an sich und auch seinem Einsatz sind insgesamt positiv.

Bis zum Ende des Jahres 2001 sollen ca. 180 Zugangspunkte zum Funknetz installiert sein, wobei basierend auf den bisherigen Erfahrungen jeweils ein durchaus signifikanter Installationsaufwand zu leisten ist. In Zukunft soll diese Anzahl weiter ausgebaut werden, so dass letztendlich Flächendeckung erreicht wird. Zur Standardausstattung von Hörsälen, Seminarräumen, etc. wird mindestens ein solcher Zugangspunkt gehören.

Derzeit ist DUKATH ein rein flaches Netz der Schicht 2, d.h., es gibt nur beschränkte Möglichkeiten der Filterung von Broadcasts, etc. Durch die weitere Untergliederung in verschiedene Subnetze würde dies besser möglich sein. Dann wäre aber ein ‚Roaming', ein Wandern unter Beibehaltung einer Kommunikationsbeziehung mit einer gleichbleibenden IP-Adresse, nicht ohne weiteres mehr möglich. Dafür müsste ein Protokoll wie Mobile IP eingesetzt und in der Infrastruktur unterstützt werden. Wir werden das Verhalten und die Eigenschaften des jetzigen flachen Netzes und die sich daraus evtl. ergebende Notwendigkeit von Mobile IP beobachten und beabsichtigen, die dazu erforderlichen Komponenten wie Foreign und Home Agents später aufzubauen.

Weitere Informationen Auf der Homepage des DUKATH-Netzes sind weitere Informationen zu finden: http://www.uni-karlsruhe.de/~DUKATH