Autoren: Prof. Herbert Wiese, Patrick Cervicek

Roaming für FHTE Angehörige

Was versteht man unter Roaming

Roaming ist bei Mobilfunk ein gängiges Verfahren, bei dem ein GSM- (**G**lobal **S**ystem for **M**obile Communication) oder UMTS-Mobil-Telefon-Benutzer (UMTS = Universal Mobile Telecommunications System) sich zwischen Netzen verschiedener Provider – sofern vertragliche Regelungen zwischen den Providern existieren – bewegen kann und überall unter seiner festen Telefonnummer Mobilfunkdienste wie z.B. Telefonieren mit der Telefonnummer, die er von seinem Netzbetreiber erhalten hat, in Anspruch nehmen kann.

Ein ähnliches Verfahren steht auch für Nutzer des FHTE-Datennetzes zur Verfügung. Ein mögliches Anwendungsszenario sei hier kurz beschrieben: Ein Nutzer des FHTE Datennetzes ist zu Gast bei einer anderen Hochschule oder ein Gast, der normalerweise an einer anderen Hochschule arbeitet, möchte während eines Meetings bei der Gasthochschule Zugang zum Datennetz seiner Heimathochschule haben und dort z.B. auf seine Emails und seine Dateien zugreifen sowie Intranetfunktionen seiner Heimathochschule nutzen können. Voraussetzung für die Realisierung eines solchen Dienstes ist, dass die Betreiber verschiedener Netze eine gegenseitige Regelung zur Nutzung und Durchleitung und die dafür notwendigen Installationen durchgeführt haben. Ein Nutzer dieses Dienstes erwartet, dass er vertraulich auf die Daten in seinem Heimatnetz zugreifen kann, dass niemand seine Daten sowie vertrauliche Informationen (wie z.B. sein Passwort) mitlesen kann. Andererseits muss die Gastgebereinrichtung Vorsorgemaßnahmen dagegen treffen, dass ein Gastbenutzer unbefugte Zugriffe zum Gastnetz vornehmen kann. Die Gasteinrichtung soll nur Durchleitungsfunktionen vornehmen.

DFN- und BelWue-Roaming

Ein solcher Dienst steht im DFN (Deutsches Forschungsnetz, Datennetz nahezu aller Hochschulen und Wissenschaftseinrichtungen in Deutschland) kostenfrei zur Verfügung. Allerdings müssen die einzelnen Hochschulen die entsprechenden Einrichtungen und Freischaltungen selbst vor Ort vornehmen. Eine Variante dieses Dienstes steht zusätzlich im BelWue (Landesnetz der Baden-Württembergischen Hochschulen) zur Verfügung. Bei allen Varianten ist ein sicherer Weg für den Zugang zum Heimatnetz vorgesehen. Dabei gibt es unterschiedliche Verfahren, wobei die FHTE alle Varianten anbietet. Das technisch beste, aber auch aufwändigste Zugangsverfahren ist ein gesicherter Zugang zum Datennetz über das IEEE 802.1x-Protokoll (IEEE = Institute of Electrical and Electronics Engineers, u.a. ein Normierungsgremium). Dieses Protokoll erlaubt u.a. einem Benutzer nur dann Zugang zu einem Datennetz, wenn er sich in einer festzulegenden Form ausweisen kann. Es werden von Anfang an bis zum erfolgreichen Login alle vertraulichen Daten verschlüsselt übertragen. Der Vorteil dieser Lösung liegt darin, dass sie im Prinzip nach gleichem Muster für weltweite Netze einsetzbar ist. Der Nachteil ist die kompliziertere Einrichtung sowie die notwendige Verfügbarkeit von IEEE 802.1x an allen beteiligten Netzkomponenten. Es gibt aber auch einfachere und leichter administrierbare Lösungen mit ausreichender Sicherheit, die ebenfalls einen Berechtigungsnachweis verlangen. Bei beiden Verfahren reicht als Ausweis ein erfolgreiches Login (mit Passwort) beim Heimatnetz aus, d.h. jeder Nutzer mit einer gültigen Benutzerkennung an einer teilnehmenden Hochschule kann ohne weitere Genehmigung direkt am Roaming (im Hochschulnetz der teilnehmenden Hochschulen) teilnehmen. Vertraulicher Zugriff mit Authentifizierung und Verschlüsselung wird über den VPN-Dienst (VPN = Virtual Private Network) gewährleistet. VPN steht an der FHTE bereits seit Einführung des mobilen Netzes „FHTE Mobile-Net“ zur Verfügung [4].

Die FHTE hat seit Einrichtung des Roaming-Dienstes seitens des DFN und des BelWue zunächst an den Testphasen teilgenommen und seit 01.03.2006 diesen Dienst Gästen anderer Hochschulen zur Verfügung gestellt. Dabei kooperiert unsere Hochschule mit BelWue sowie dem DFN [1] [2]. Dieser Dienst steht auch FHTE-Angehörigen an teilnehmenden Roaming-Partnerhochschulen zur Verfügung [1] [3]. Um Roaming nutzen zu können ist ein WLAN-fähiges Notebook (WLAN = Wireless Local Area Network) mit einem VPN-Client Vorraussetzung [4].

Roaming war vor dem 01.03.2006 nur in der aufwändigeren Variante möglich. Auch die Installation und Konfiguration des mobilen Notebooks für IEEE 802.1x ist wesentlich aufwändiger als bei der einfachen

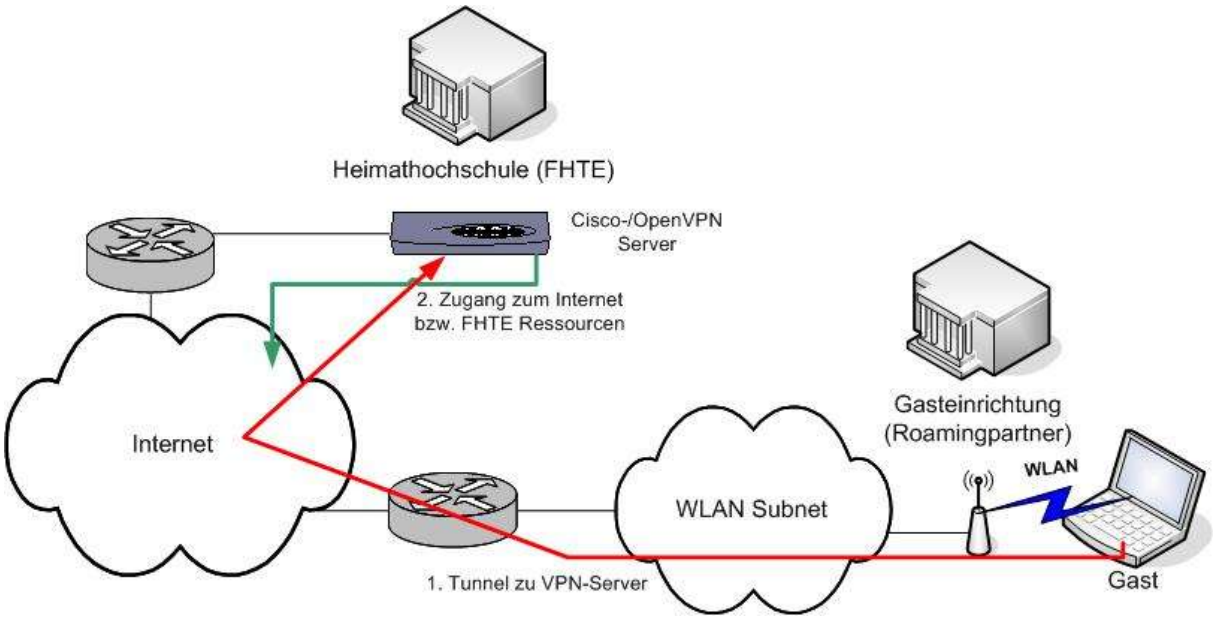
Variante über CASG (Controlled Address Space for Gateways), wie sie die FHTE seit dem 1.3. 2006 bereitstellt. Ein Benutzer muss bei dieser Variante speziell für Roaming an seinem Laptop nichts mehr neu machen, sofern der Laptop für Nutzung des Mobile-Net an der FHTE inklusive VPN eingerichtet ist. Damit der Benutzer immer die gleiche Netzumgebung vorfindet, ist die SSID (Service Set IDentifier, Name eines WLAN's) der Accesspoints bei allen Roaming-Partnern gleich. Der Aufwand für die Rechenzentren der Hochschulen ist bei der einfachen Variante sehr gering und besteht im Wesentlichen aus dem einmaligen Freischalten des CASG-Adressbereich an der WLAN-Firewall. Da der Dienst noch nicht flächendeckend an allen Hochschulen eingerichtet ist und die aktive Teilname einer Hochschule erforderlich ist, muss man sich (leider) immer zuerst noch erkundigen, ob Roaming nutzbar ist und in welcher Variante es zur Verfügung steht. Dafür stehen sowohl beim DFN als auch beim BelWue entsprechende Informationen im Internet zur Verfügung [1] [2].

Die beiden Roaming-Varianten, an denen die FHTE von Anfang an beteiligt war, werden im Weiteren etwas ausführlicher beschrieben.

Roaming mit CASG

Bei der einfachen Variante muss jede teilnehmende Hochschule einen Zugangs-Server in einem speziellen IP-Adressraum (IP = Internet Protocol) zur Verfügung stellen. Dieser CASG-Adressbereich (CASG = Controlled Address Space for Gateways) wird anschließend von allen teilnehmenden Roaming-Partnern an der WLAN-Firewall freigegegeben, damit sich ein Roaming-Benutzer zu Gast bei einem Roaming-Partner mit seinem Zugangs-Server an seiner Heimeinrichtung verbinden kann. In der Regel sind an der WLAN-Firewall nur die IP-Adressbereiche zu den eigenen Zugangs-Servern freigegeben, damit kein Netzmissbrauch zu anderen Internet-Teilnehmern möglich ist.

Bei den Zugangs-Servern handelt es sich meist um VPN-Server, die eine verschlüsselte und authentifizierte Verbindung zwischen Notebook und VPN-Server ermöglichen, d.h. es muss eine VPN-Verbindung zum VPN-Server der Heimateinrichtung aufgebaut werden. CASG-Roaming ist leicht umsetzbar, um das Roaming für seine Gäste zu ermöglichen. Allerdings kommt es an die Grenze, wenn auch zu anderen Nicht-Hochschuleinrichtungen Roaming möglich sein soll, da diese nicht im CASG-Adressbereich vertreten sind.

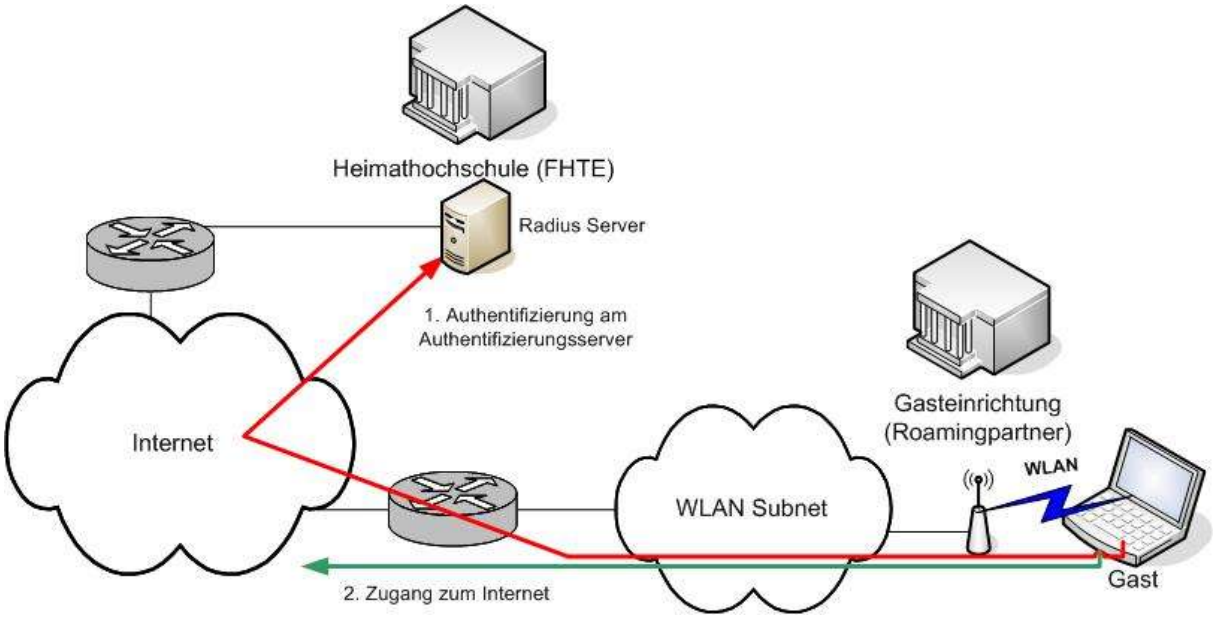


Roaming mit CASG

Roaming mit 802.1X

Die aufwändigere, jedoch komfortablere und besser skalierbare Variante ist IEEE 802.1x. Hierbei authentifiziert sich das Endgerät am Netzwerk (Switchport oder Accesspoint). Das Netz kontrolliert am Heimatnetz, ob es sich um einen gültigen Benutzer handelt, und schaltet den Zugang für den Gast erst nach erfolgreicher Authentifizierung frei. Der Benutzer kann nun mit einer IP-Adresse aus dem Gastnetz das Internet nutzen. Damit Benutzer nun die gewünschten Zugriffsmöglichkeiten zum Heimatnetz voll nutzen können, ist anschließend ebenso wie bei der einfachen Variante über CASG eine VPN-Verbindung mit „Tunnelung“ und Verschlüsselung zur Heimathochschule aufzubauen.

Bei 802.1x-Roaming ist eine höhere Investition in Hardware notwendig, da alle beteiligten Netzkomponenten im Gastnetz 802.1x-fähig sein müssen. Diese Voraussetzung ist nicht bei allen Roaming-Partnern erfüllt.



Roaming mit 802.1x

Roaming für FHTE Angehörige am Beispiel "Café.com"

Bei einem Kaffeebesuch im Café.com entstand die Idee, die Einfachheit, Nutzen und Umsetzung von CASG-Roaming gegenüber Hochschulangehörigen zu demonstrieren. Das Café.com ist ein Internetcafe am Esslinger Hafenmarkt, mit Sitzmöglichkeit im Innen- und Außenbereich. Ein Accesspoint war bereits vorhanden, stand aber den Gästen nicht zur Verfügung, da das WLAN mit WEP (Wired Equivalent Privacy) verschlüsselt war. Anfang Juli 2006 wurde beim Betreiber des Café.com (Herr Manfred Bruckner) angefragt, ob er denn Interesse hätte, seinen Accesspoint für Hochschulangehörige zu öffnen. Er war sofort damit einverstanden, da schon öfters andere Gäste danach gefragt hatten. Als ihm das Prinzip des CASG-Roaming erklärt wurde, hatte er auch keine Sicherheitsbedenken. Eine DSL-Flatrate-Leitung stand bereits zur Verfügung, so dass keine zusätzlichen laufenden Kosten zu erwarten waren. Um das LAN von WLAN zu trennen (Sicherheit!), war allerdings ein anderer Accesspoint notwendig. Ausgewählt wurde ein WRT54GL von Linksys, auf welchem sich DD-WRT [5], einem alternativen "Betriebssystem" für Accesspoints, installieren (Fachjargon: „flashen“) lässt. Herkömmliche Accesspoints kommen meist mit einem proprietären Betriebssystem einher, an dem viele Punkte nur beschränkt über die Weboberfläche konfigurierbar sind. Herr Bruckner erklärte sich bereit die Kosten zu für den Accesspoint zu übernehmen, während Herr Cervicek sich um die Implementierung kümmern sollte.

Das Café.com von innen (Quelle: Cafe.com)

DD-WRT auf WRT54GL

Linksys WRT54GL (Quelle: Linksys)

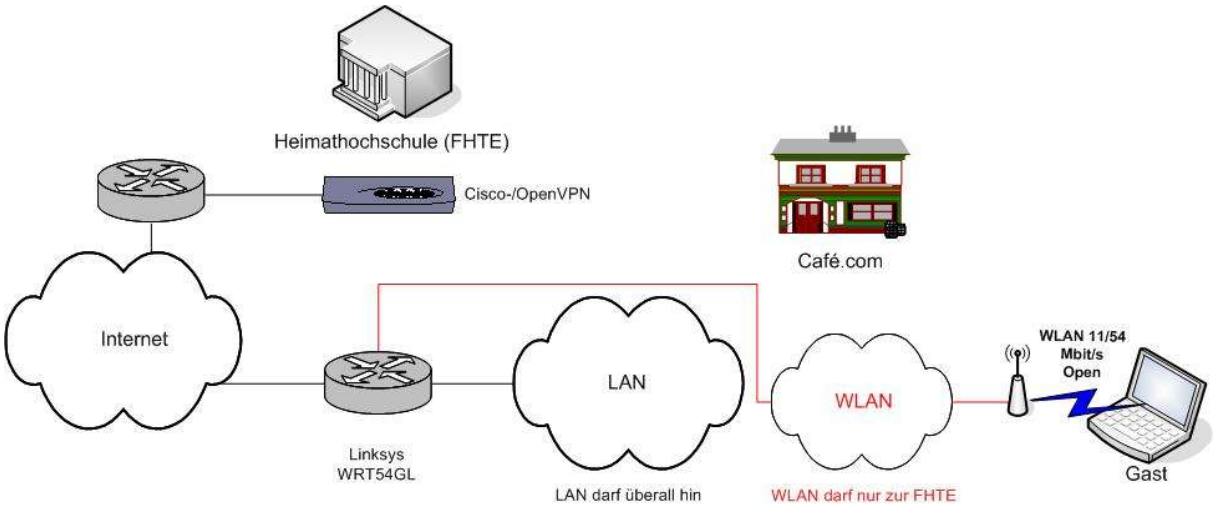
Da es sich bei DD-WRT um ein Linux-basierendes Betriebssystem handelt, lassen sich die im Linux-Kern implementierten Routing- und Firewall-Funktionalitäten einfach und effizient auf einem LinkSys Accesspoint nutzen. DD-WRT kompatible Accesspoints wie der Linksys haben einen Flash-/ sowie einen Arbeitsspeicher. Der Flash-Speicher lässt sich dauerhaft mit dem Bootloader, der Firmware sowie den Konfigurationsdaten beschreiben. Der Flash-Speicher lässt sich etwa 10.000 Mal beschreiben. Nach einem Reboot bleibt der Inhalt im Flash-Speicher erhalten während der Inhalt des Arbeitsspeichers verloren geht. DD-WRT erzeugt nach dem Booten eine für Linux übliche Verzeichnisstruktur im Arbeitsspeicher, wobei sich die Verzeichnisse sich wie folgt unterscheiden:

- /tmp ist ein Verzeichnis im Arbeitsspeicher
- /jffs ist ein beschreibbares Verzeichnis im Flashspeicher
- /etc ist ein read-only Bereich im Flashspeicher

Die Umsetzung

Am 10.07.2006 hat Herr Bruckner den Accesspoint gekauft (~69 Euro) und Herr Cervicek übergeben, so dass der Accesspoint konfiguriert werden konnte.

Im Café.com wurde ein LAN vorgefunden, in dem 5 Rechner für Gäste bereit standen sowie ein WLAN, das sich in dem gleichen Subnetz befindet. Aufgabe war nun, WLAN von LAN zu trennen, so dass sich jeder WLAN-Gast nur mit der FHTE verbinden kann und dabei keinen Zugriff auf das LAN hat. Dies ist in sofern wichtig, da sonst ungebetene Gäste anonym Missbrauch über die IP-Adressen des Café.com begehen könnten. Da die Authentifizierung & Verschlüsselung über VPN abgewickelt wird, konnte auf die WEP Verschlüsselung verzichtet werden.



Netzplan Café.Com (Erweiterung ist rot eingezeichnet)

Nachdem auf dem Accesspoint DD-WRT installiert wurde, mussten folgende Punkte konfiguriert werden:

- Automatische DSL Einwahl
- Wiedereinwahl um 6 Uhr morgens zur Verhinderung einer Zwangstrennung
- DHCP für die 5 Rechner im LAN
- DHCP für die Gäste im WLAN
- DNS Forwarding
- Firewall zwischen WAN (DSL), LAN und WLAN
- NAT
- SSH für Fernwartung, um ggf. Änderungen durchführen zu können
- Webserver, um unberechtigten Gästen einen kurzen Hinweis zu geben

Diese Punkte ließen sich über die CLI (Command Line Interface) leicht konfigurieren. Auf der DD-WRT Homepage wird ausreichend Hilfestellung geboten, so dass auf die Konfigurationsdetails hier nicht näher eingegangen wird. Bereits am Sonntag, den 16.07.2006 konnte der Accesspoint wieder an das Café.com übergeben werden. Angehörige der Hochschule können nun auch im Café.com ihre Arbeiten erledigen, indem sie sich über VPN am FHTE-Netz anmelden.

Literatur:

[1]: BelWue Info Seite über Roaming & teilnehmende Hochschulen
http://www.belwue.de/roaming

[2]: DFN Info Seite über Roaming
http://www.dfn.de/roaming

[3]: Liste von teilnehmenden Roamingpartnern im DFN
http://www.dfn.de/content/de/dienstleistungen/dfnroaming/roamingstandorte/

[4]: Mobile-Net Dokumentation des RZ der FHTE
http://www.fht-esslingen.de/mobile-net

[5]: Alternatives Betriebssystem für Accesspoints - DD-WRT
http://www.dd-wrt.org

Autoren Details:

Herbert Wiese: Professor am Fachbereich Informationstechnik, Leiter des Rechenzentrums der FHTE.
Patrick Cervicek: Student im 8. Semester Technische Informatik (FB IT), Studentische Hilfskraft im Rechenzentrum der FHTE, Vertreter der AstA im DV-Ausschuss