

Hauptseminar überfachlich Sommersemester 2004
Trends der Mobilkommunikation im internationalen
Umfeld und ihre wirtschaftlichen Auswirkungen

Thema: Roaming und Handover zwischen verschiedenen
Netzen und Netztechnologien

Betreut von: Marco Chiesa

Bearbeitet von Yan Lin

Inhaltverzeichnis

1. Begriffsdefinitionen.....	3
1.1. Was ist Roaming?.....	3
1.2. Was ist Handover?.....	3
1.2.1 Verschiedene Klassifikationen von Handovers	3
1.2.1.1. Klassifikationen von Handovers (Wo).....	3
1.2.1.2. Klassifikationen von Handovers (Wie).....	4
1.2.1.2. Klassifikationen von Handovers (DIR).....	4
1.3. Roaming HLR/VLR.....	4
2. Realisierung vom Roaming in verschiedenen Technologien.....	4
2.1. GSM/UMTS.....	4
2.1.1. Handover/Roaming.....	4
2.1.1.1. Handover/Roaming in GSM.....	4
2.1.1.2. Handover/Roaming in UMTS.....	6
2.1.1.3. Warum gibt es Handover/Roaming zwischen GSM und UMTS?.....	7
2.1.1.3.1. Roaming von UMTS Nutzer in GSM.....	7
2.1.1.3.2. Roaming von GSM Nutzer in UMTS.....	7
2.1.2. Abrechnung und Clearinghouse.....	7
2.1.2.1. Clearinghouse.....	8
2.1.2.2. Abrechnung.....	8
2.2. WLAN Roaming.....	8
2.2.1. Pre-access Authentikation.....	9
2.2.2. Die Methoden der Authentifizierung.....	10
2.3. Dial-In (Internet).....	11
2.3.1. Warum Dial-IN ?.....	11
2.3.2. Authentisierung	12
2.3.3. Autorisierung	12
2.3.4. Abrechnung/Accounting.....	12
2.3.5. Einwahltechnik ins Internet.....	13
2.3.5.1. Technik der Authentifizierung mit RADIUS-Protokoll.....	13
2.3.5.2. Das RADIUS-Zonen-Konzept.....	14
2.3.5.3. Technik der Authentifizierung mit TACACS-Protokoll.....	14
2.3.6.1. iPass.....	15
2.3.6.2. GRIC.....	15
3. Zusammenfassung.....	16

1. Begriffsdefinitionen

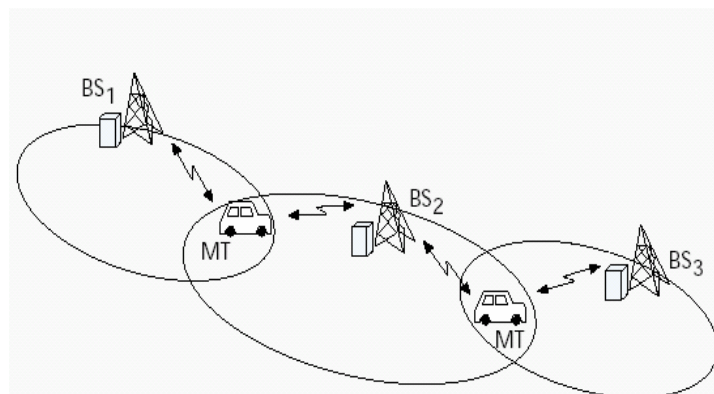
1.1. Was ist Roaming?

Der Begriff Roaming bezeichnet zwar nur die Möglichkeit, die Funkzelle zwischen Netzen zu wechseln. Meist wird er aber nur dann verwendet, wenn Nutzer zwischen Ländern und verschiedenen Technologien wechselt. Innerhalb von Deutschland bietet nur O₂ dieses National Roaming an. In Gebieten, in denen das O₂-Netz noch nicht ausgebaut ist, kann der Nutzer das T-Mobile-Netz mitnutzen. International Roaming bezeichnet dementsprechend die Mitnutzung von ausländischen Mobilfunknetzen.

1.2. Was ist Handover?

Mobilfunknetze sind zelluläre Netze. In jeder Zelle befindet sich eine Sendestation, die Kontakt mit den Handys hält. Wenn Nutzer nun die Zelle wechselt, weil er zum Beispiel im Zug sitzt und telefoniert, dann übernimmt die Basisstation der Nachbarzelle das Gespräch in dem Moment, in dem sie dauerhaft ein stärkeres Signal erhält als die ursprüngliche Zelle. Diese automatische und unterbrechungsfreie Übergabe nennt man Handover.

Bei jedem Handover bucht sich das Handy neu ins Netz ein. Schließlich ist jetzt eine andere Basisstation für Nutzer zuständig, und das Netz muss einen neuen Weg finden, dem Nutzer ein Gespräch zuzustellen.



1.2.1 Verschiedene Klassifikationen von Handovers

1.2.1.1. Klassifikationen von Handovers (Wo)

- Intra-Cell:
 - Lediglich Wechsel auf anderen Kanal
- Inter-Cell:
 - Wechsel in eine andere Zelle

1.2.1.2. Klassifikationen von Handovers (Wie)

- Hard Handover:
 - MT schaltet vom alten auf den neuen Link
 - Nur eine aktive Verbindung
 - Kurze Unterbrechung
- Soft Handover:
 - MT unterhält zwei Kanäle zugleich
 - Beim Wechsel schaltet es „weich“ von einer BS zur anderen

1.2.1.2. Klassifikationen von Handovers (DIR)

- Forward Handover:
 - MT entscheidet sich für die „nächste Zelle“
 - Kontaktiert die BS der neuen Zelle
 - Neue BS initiiert das Trennen der alten Verbindung
- Backward Handover:
 - MT entscheidet sich für die „nächste Zelle“
 - Kontaktiert aktuelle BS
 - Alte BS signalisiert der neuen BS das Handover

1.3. Roaming HLR/VLR

Das Home Location Register. Eine der Datenbanken von entscheidender Wichtigkeit im GSM/UMTS. Das HLR enthält neben einem Verweis auf das VLR, in dessen Bereich sich der Kunde aufhält und Informationen, die für verschiedene Authentifizierungsprozesse notwendig sind, alle kundenrelevanten Daten wie etwa Rufnummern, erlaubte Dienste etc. HLR kennt immer letztgültige fremdes VLR und sendet an fremdes VLR eine Authorisierung für Roaming-Nutzer. Dadurch kann der Roaming-Nutzer die Services vom fremden Netzanbieter weiter benutzen.

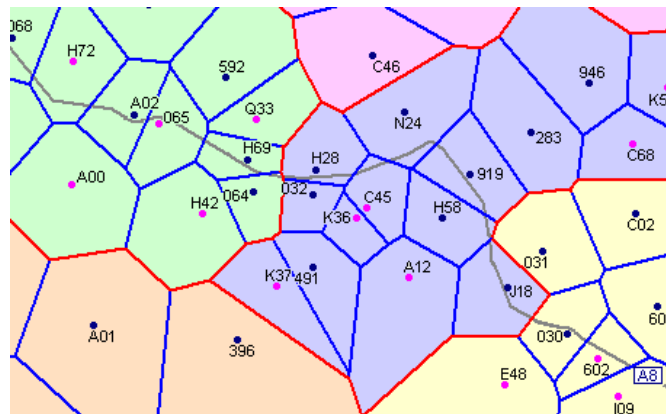
Das Visitor Location Register. Eine der Datenbanken im GSM/UMTS. In dieser Datenbank werden Besucher gespeichert - also Teilnehmer anderer Netze, die sich gerade per "Roaming" im betreffenden Netz eingebucht sind. Das VLR enthält Informationen zum genauen Aufenthalt des betreffenden Kunden und eine Kopie der Daten des HLR des Teilnehmers.

2. Realisierung vom Roaming in verschiedenen Technologien

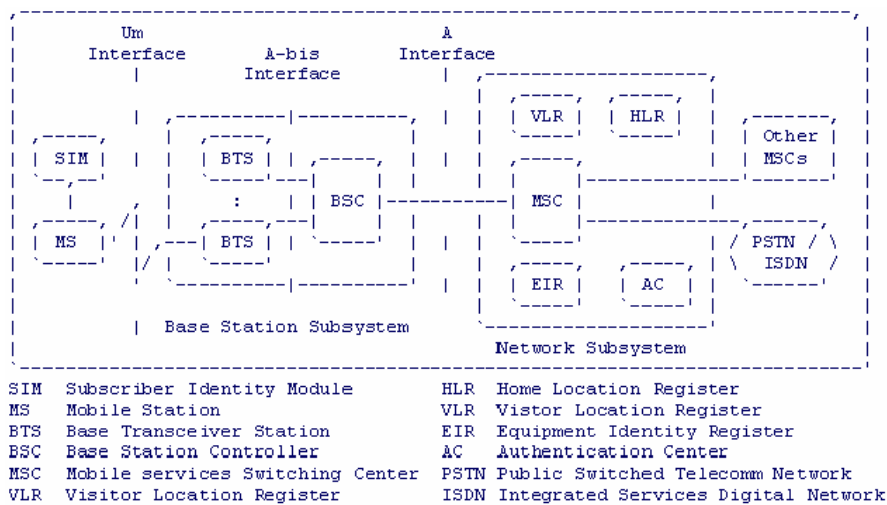
2.1. GSM/UMTS

2.1.1. Handover/Roaming

2.1.1.1. Handover/Roaming in GSM



GSM Netzplan



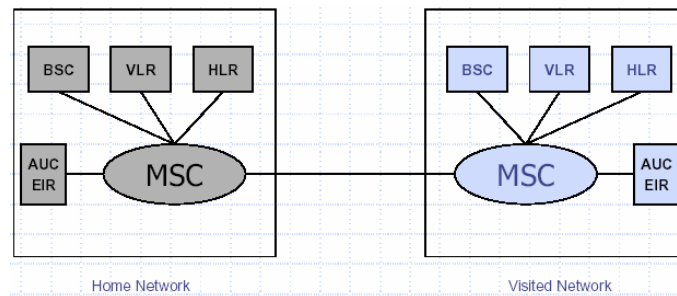
GSM Architektur

- Internal Handover:
 - Intra-BTS: Kanalwechsel innerhalb der Zelle
 - Intra-BSC: Wechsel von einer Zelle in eine andere. Beide sind jedoch dem selben BSC zugeordnet.

- External Handover:
 - Intra-MSC: Wechsel zu einem anderen BSC, allerdings dem gleichen MSC.
 - Inter-MSC: Wechsel zu einem anderen MSC.

GSM Roaming kann mit Hilfe von HLR und VLR realisiert werden. Nutzer bleibt irgendwo im In- oder Ausland. Sein Handy meldet sich bei dem BSC mit eigenen Kundendaten in SIM-Karte. Solche Daten werden an seine MSC weiter übermittelt. MSC kontaktiert die Heimat-MSC des Nutzers und aktualisiert die VLR-Datenbank mit den HLR-Daten des Heimat-MSC's. Danach wird mit Hilfe der AUC- und EIR-Datenbanken die Erlaubnis einer Netzbenutzung überprüft und die aktuelle Position des Nutzers im HLR bzw. VLR

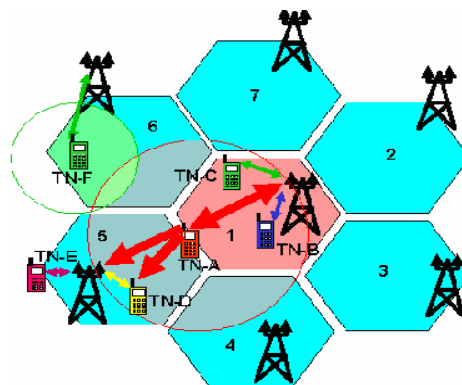
aktualisiert.



2.1.1.2. Handover/Roaming in UMTS

Anders als bei GSM haben die Funkzellen der UMTS-Netze jedoch keine feststehende räumliche Ausdehnung. Vielmehr verändern sich die Zellgrößen in Abhängigkeit von der Zahl der Nutzer: Sie „atmen“ gewissermaßen. Jede UMTS-Funkzelle hat eine mögliche maximale Sendeleistung. Je mehr Menschen in der Zelle mobil telefonieren, desto weniger Leistung kann auf den einzelnen entfallen. Dadurch verringert sich die Bandbreite beziehungsweise die mögliche Entfernung zur Sendestation: Die Zelle wird kleiner. Bei sehr hohem Sendeaufkommen kann es sein, dass weiter entfernte Teilnehmer von einer anderen, daneben liegenden Zelle versorgt werden müssen.

Auch der Übergang von einer Funkzelle zur nächsten – der so genannte Handover – erfolgt bei UMTS fließend. Das Netz bestimmt jeweils das stärkste Funksignal eines Handys, das sich in Bewegung befindet, und ordnet es einer Zelle zu. In dicht besiedelten Gebieten haben die Nutzer sogar überwiegend gleichzeitig Kontakt zu mehreren Basisstationen. Dies verringert die Gefahr von Abbrüchen des Funksignals. Zudem ist ein unbemerkter Übergang in die GSM-Netze möglich, wenn der Nutzer ein Gebiet mit UMTS-Versorgung verlässt.



Dass man mit einem GSM-Handy überall weltweit telefonieren kann, ist inzwischen selbstverständlich. Das bedeutet aber auch, dass mit der Einführung vom UMTS diese Technologie zeitgleich in allen anderen Ländern eingeführt werden muss, in denen durch Roaming-Verträge die Mitnutzung von UMTS-Ressourcen ermöglicht werden soll.

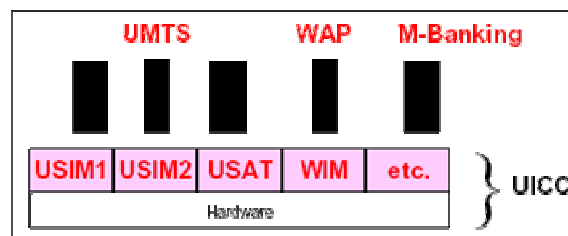
2.1.1.3. Warum gibt es Handover/Roaming zwischen GSM und UMTS?

Nach Einführung von UMTS wird es die alte GSM-Technik noch für eine unbestimmte Zeit weiterhin geben. Die GSM-Netzbetreiber werden nicht schlagartig ihr gesamtes Netz durch UMTS-Technik ersetzen können. Vielmehr wird eine weiche, schrittweise Migration zu UMTS angestrebt. Dies betrifft auch die Kundenseite. Neben der Masse von Bestandskunden, die ein GSM-Telefon und eine GSM-SIM besitzen und weiterhin benutzen wollen. UMTS-Neukunden wollen sofort mit einer USIM ausstatten. Also müssen beide Kartentypen nebeneinander bereitgehalten werden.

2.1.1.3.1. Roaming von UMTS Nutzer in GSM

In diesem Fall benutzt ein UMTS Nutzer ein Dual Modus GSM/UMTS Gerät. Er muss eine USIM Chipkarte ins Gerät einsetzen. Die UMTS Chipkarte ist multi-applikationsfähig. D.h neben einer USIM sind weitere Applikationen unterstützbar.

Wenn Nutzer eigene UMTS Versorgung verliert und unbemerkt in GSM Netze eintretet, wird UICC als eine SIM-Karte das GSM-Netz kontaktieren (z.B. für Sicherheit und Authentikation). UICC(Universal IC Card) ist eine Multi-Applikationsplattform. Sie geht über die logische Funktionalität einer reinen USIM hinaus. Und vielmehr ist die UICC eine Basis für beliebige Applikationen, von denen die UMTS-USIM nur eine darstellt. Die UICC inkludiert die verschiedene Funktionalitäten von SIM und USIM.



Das GSM-VLR wird gleichzeitig das UMTS-HLR von diesem Fremdkunden abfragen. Das UMTS-HLR wird die Benutzeridentität authentisieren. Und Das UMTS-HLR kann GSM Provider die Authentikation senden.

2.1.1.3.2. Roaming von GSM Nutzer in UMTS.

Ein GSM Nutzer benutzt ein UMTS Mobilfunkgerät oder ein Dual Modus GSM/UMTS Gerät mit einer GSM SIM Chipkarte. Die SIM Chipkarte muss von UMTS Mobilfunkgerät oder ein Dual Modus GSM/UMTS Gerät akzeptiert werden. Das VLR von UMTS macht einen Kontakt mit GSM HLR, um eine GSM-Authentikation bekommen zu können. Wenn die Identität von GSM-Nutzer von HLR erfolgreich authentisiert wird, darf der GSM Nutzer Service von UMTS Operator benutzen.

2.1.2. Abrechnung und Clearinghouse

2.1.2.1. Clearinghouse

Clearinghouse ist ein Anbieter von "Roaming Billing Data Service". Ein Clearinghouse bietet einpaar Post-Connection Services bei der Behandlung der Billingsdata, Bestätigungs- und Bewertungsservice sowie finanzieller Abrechnung.

Die Mobiloperatoren haben heute grossen Einfluss in WISP Industrie, insbesondere in Europa. Sie möchten WLAN Roaming Tarif mit existierenden Clearinghouse Kanälen verbinden. Bis heute haben einpaar Clearinghouses WLAN Clearing auf Markt als ein Service eingesetzt.

2.1.2.2. Abrechnung

Die Abrechnung oder Billing vom Roaming basiert auf Call Detail Record (CDR), der von visited Operator bestimmt ist. Der CDR wird nach Clearinghouse übertragen und weiter nach Home Operator, wo die Rechnung sich für Nutzer erstellen lässt.

Clearing und finanzielle Settlement werden einpaar speziellen Clearinghouses weitergegeben und werden nach einem abgeschlossenen Abkommen behandelt. Solche Clearinghouses behandeln die CDR Informationen von Visited Operator, aber nehmen nicht an real-time Authentifikationsaustausch mit Home Operator teil. Wenn die Operatoren einen gemeinsamen Roamingsaustausch haben und mit verschiedenen Clearinghouses verbinden, werden solche Clearinghouse zusammenarbeiten, um eine genaue Clearing und Settlement zu erstellen.

Die TAP (Transferred Account Procedure) ist ein Set von Formaten und Prozeduren, die von GSM Assoziation definiert werden. Die TAP dienen zum Austausch von Roaming Billing Informationen. Tatsächlich bestimmt TAP Formaten von CDR Speicherungen und Dateien, dadurch dass die Operatoren mit Clearinghouse austauschen können.

Jeder Operator verwendet einen pre-agreed Tarif/inter-operator Tarif (IOT). Der IOT bestimmt eine Rate. Der WISP kann erstattet werden, falls ein Nutzer von anderen Netzwerken in seine Hotspot roamt. Die CDRs in TAP Files werden aufgrund IOT von Visited Operator bewertet. Der Home Operator muss diesen Preis erstatten und Nutzer Rechnung schicken.

2.2. WLAN Roaming

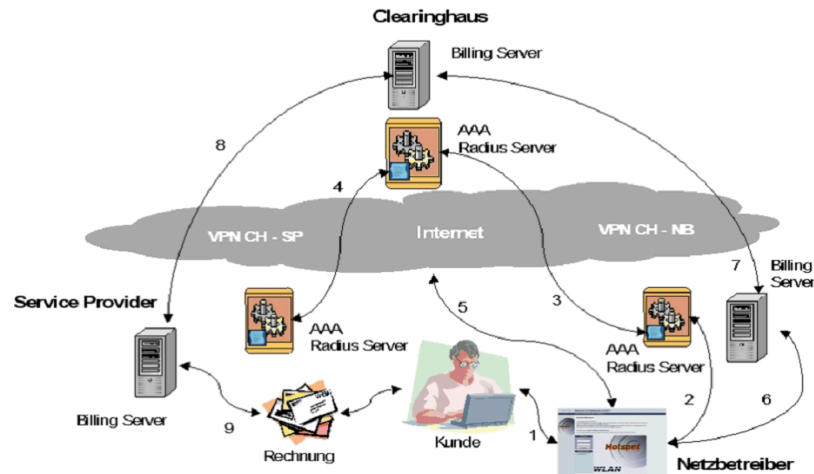
Bezeichnung für die Nutzung eines fremden Wireless-LAN-Netzes mit dem eigenen Rechner (z.B. Notebook, PDA). Ähnlich wie beim Mobiltelefon-Roaming werden die Verrechnungs- und Authentifizierungsdaten zwischen den betroffenen Netzbetreibern ausgetauscht. Voraussetzung für WLAN-Roaming ist, dass der eigene Netzbetreiber mit anderen WLAN-Netzbetreibern ein Roaming-Abkommen geschlossen hat.

Roaming bedeutet die anonyme, autorisierte Nutzung fremder WLAN Netzwerke als Gast (Visiting User/VU). Der Zugang zum Netz, die Authentifizierung, erfolgt unter Verwendung der persönlichen Zugangsdaten des Nutzers, die von seinem Service Provider (SP) vorgehalten und geprüft werden. Das Netz, in dem der Nutzer roamt, ist das Visited Netzwerk (VN) des Netzbetreibers (NB). Es geht bei Roaming primär um Prozesse und Verfahren zur Authentifizierung und Authorisierung „fremder“ Nutzer.

Sekundär ist die Frage nach der Abrechnung (Accounting) der Dienste. Diese erfolgt bilateral, zwischen Netzbetreiber und Service Provider des Kunden. Der Netzbetreiber stellt der Service Provider die Nutzung in Rechnung. Da nur der Service Provider die Identität des Nutzers kennt und nur er mit ihm ein Vertragsverhältnis hat, ist er in der Lage dem Nutzer eine Rechnung zu erstellen.

WLAN Hotspot Roaming muss technisch und organisatorisch in der Lage sein, die folgenden, netzwerk- und organisationsübergreifenden Aufgaben und Prozesse effizient zu erfüllen: Authentifizierung, Authorisierung sowie Accounting

Hier muss man nochmal die Rolle des Clearinghouses (CH) beachten. Das Clearinghouse nimmt die Nutzungsdaten der Roamer vom Netzbetreiber entgegen. Diese Daten werden verarbeitet und den jeweiligen Service Providern zugestellt. Monatlich erfolgt die Abrechnung des Service Providers im Namen und auf Rechnung des Netzbetreibers.



2.2.1. Pre-access Authentikation

Dieser Prozess fängt mit einer Einlogung des Endnutzer an. Die folgenden Schritte sind Authentifizierungsverfahren für WLAN Roaming.

- Identifizierung des Nutzers
- Kontakt mit Home WISP
- Die Anforderung an Authorisierung wird an Home WISP gesendet.
- Übertragung von Kundendaten

- Billing Counter wird aktiviert.

2.2.2. Die Methoden der Authentifizierung

Die Authentifizierung von einem Endnutzer kann entweder ein Gerät oder browser-based sein. Es gibt folgende 2 Fälle:

- Im ersten Fall wird ein Laptop sich mit Netzwerk und Home Provider (z.B. durch SIM Karte) authentifizieren (Siehe unten links)



Am Beispiel des „Pay-by-Mobil“ Roamingservice von EXCILAN (oben rechts) sei ein Variante vorgestellt. Die Authentifizierung erfolgt mit der Handy-Rufnummer. Nach Eingabe im Hotspot Portal wird sie vom Netzbetreiber an EXCILAN übermittelt. EXCILAN initiiert einen Anruf auf dem Handy des Nutzers. Bestätigt der Nutzer die per IVR System (Interactive Voice Response) angesagten Konditionen mit Druck auf „1“, erfolgt die Authorisierung und Freigabe an den Netzbetreiber. Am Ende der Nutzung sendet der Netzbetreiber die Aountingsdaten an EXCILAN. EXCILAN wir solche Daten an der Service Provider des Nutzers weiterleiten.

- Im zweiten Fall kann der Nutzer sich manuell durch eine Log-In Page authentifizieren. Z.B durch Benutzername und Kennwort mit dem RADIUS-Standard.

Im Rahmen von „Greenspot“ gestaltet der Roamingsablauf sich wie folgt:

Der Nutzer von einem Service Provider möchte Hotspot eines Netzbetreibers nutzen. Beide Service Provider und Netzbetreiber sind über das Greenspot Clearinghouse

technisch und vertragsrechtlich verbunden. Zur Authentifizierung gibt der Nutzer seine persönliche Zugangskennung und das Passwort an. Der verschlüsselte Datenaustausch zwischen Netzbetreiber, Clearinghouse und Service Provider erfolgt auf Basis des RADIUS-Protokoll. Der RADIUS-Client auf Netzbetreiber Seite übermittelt die Daten an RADIUS-Server des Clearinghouses. Der Service Provider entscheidet über die Authorisierung, also die Freigabe. Die Entscheidung wird wieder über das Clearinghouse dem Netzbetreiber-Hotspot mitgeteilt. Bei positiver Authorisierung erhält der Nutzer den Zugang zum Internet. Ist die Nutzung beendet, was durch Logout oder durch Timeout erfolgt, sendet der Netzbetreiber die Accountingsdaten an das Clearinghouse, welches sie an den Service Provider weiterleitet.

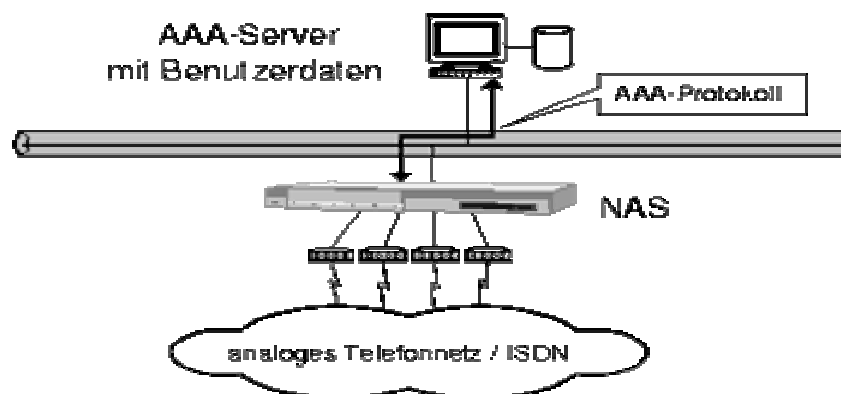
Neben Greenspot gibt es zahlreiche, weitere Anbieter von Roaming Service. Details der AAA Verfahren, ebenso wie RADIUS Attribute und Formate. So finden zur Authentifizierung Software-Client Programme (z.B. GRIC, iPass).

2.3. Dial-In (Internet).

2.3.1. Warum Dial-IN ?

Dial-IN stellt Mitarbeitern zu Hause, unterwegs oder beim Kunden vor Ort Firmeninformationen zur Verfügung und bietet eine Komplettunterstützung von Sprache, Daten, Fax und Internet, ermöglicht sichere, hochleistungsfähige Zugänge und eignet sich für kritische Firmenanwendungen, die auf hohe Leistung angewiesen sind.

Durch die Remote Node Technologie stehen den entfernten Benutzern sämtliche Ressourcen des Netzwerks transparent zur Verfügung. Die Absicherung des Netzzugangs kommt dadurch eine große Bedeutung zu. Verstärkte Sicherheitsanstrengungen auf einzelnen exponierten Rechnern mögen bei Remote Control Lösungen oder Anwendungsservern noch ausreichend sein, die Sicherheitsrisiken müssen jedoch mit einer umfassenden Netzwerksicherheit gelöst werden. Beispielsweise durch einen „AAA“ Server (Authentisierung, Authorisierung, Abrechnung/Accounting).



2.3.2. Authentisierung (Wer ist der Nutzer?)

Eine grundlegende Rolle in der Netzwerksicherheit kommt der Authentizität des Benutzers zu. Nur wenn diese sichergestellt ist, können die folgenden Maßnahmen wie Autorisierung und Accounting wirkungsvoll sein. Als unterstützende Maßnahme der üblichen Authentisierungsverfahren können auch Eigenschaften des Telefonnetzes ausgenutzt werden, z.B. der automatische Rückruf oder als spezieller Dienst im ISDN die Rufnummernübermittlung. Da auch das Telefonnetz nicht als absolut sicher gelten kann und Dienste wie Anrufweitschaltung den Ort des Endgeräts eventuell verschleiern können, sollten diese Authentisierungsmethoden mit Hilfe des Telefonnetzes immer nur zusätzlich zu anderen Verfahren angewendet werden.

2.3.3. Autorisierung (Was darf der Nutzer?)

Unter Autorisierung versteht man in diesem Zusammenhang die vom jeweiligen Benutzer abhängige dynamische Einschränkung des Netzwerkzugriffs. Dies wird durch ein benutzerspezifisches Profil erreicht, welches in einer allgemeinen Benutzerdatenbank gespeichert wird. Mit der Autorisierung werden im wesentlichen zwei Ziele verfolgt: zum einen kann der Zugriff auf Ressourcen im Netzwerk eingeschränkt werden, und zum anderen kann die Komplexität für bestimmte Benutzergruppen hinter speziell angepaßten Menüs verborgen werden. Gruppenprofile erlauben die Zusammenfassung ganzer Benutzerklassen und verringern so den Konfigurationsaufwand. Wichtig ist hierbei, daß Profile auch auf einzelne Benutzer angewendet werden können, gleichgültig auf welchem Port am Wählzugangsserver sie sich einwählen. Dies hört sich trivial an, ist aber bei manchen Wählzugangsserver in der aktuellen Softwareversion nicht konfigurierbar. In einem solchen Fall müßte ein spezielles Benutzerprofil für eine Einwählleitung konfiguriert werden, was die Gesamtzahl der allgemeinen Zugänge pro Spezialfall verringert. Dies ist dann kein Problem, wenn insgesamt mehr Einwählleitungen als Benutzer zur Verfügung stehen, aber bei einem Service Provider oder einer Universität ist dieser Fall wenig realistisch.

2.3.4. Abrechnung/Accounting (Welche Ressourcen hat der Nutzer verwendet?)

Komfortables und umfassendes Accounting ist nicht nur für kommerzielle Anbieter von Online Diensten für die Rechnungserstellung notwendig. Auch für die Absicherung der Fernzugänge gegenüber Mißbrauch und zur Trendanalyse der Auslastung wird ein gutes Abrechnungssystem benötigt. ISP's benötigen eine verlässliche Aufstellung der Anschaltzeit, der Menge der übertragenen Daten und der Nutzung spezieller Dienste. Diese Aufzeichnungen müssen auch dann fehlerfrei funktionieren, wenn Verbindungen nicht korrekt beendet wurden. Wenn die Kunden das Vertrauen in die Rechnungsstellung des Anbieters erst einmal verloren haben, ist sehr viel Mühe notwendig, dieses Vertrauen zurückzugewinnen. Für Firmen, die nur den eigenen Mitarbeitern den Zugang ermöglichen, und für Universitäten, die meist allen Studenten und Mitarbeitern den Zugang kostenlos zur Verfügung stellen, ist das Accounting dennoch ein wichtiges Hilfsmittel, um die

Auslastung der Zugangsleitungen zu überwachen und notfalls bereits im Vorfeld geeignete Maßnahmen zu ergreifen. Es hat sich dabei als nützlich erwiesen, die Auslastung auf die Wochentage und Tageszeiten bezogen graphisch aufzuarbeiten und den Benutzern zur Verfügung zu stellen. Damit werden diese in die Lage versetzt, Nutzungslücken selbständig zu erkennen und auszunützen. Das wichtigste Hilfsmittel, um die Fernzugänge hinsichtlich Mißbrauchs zu überwachen, sind die Zugriffsstatistiken. Benutzer, die gleichzeitig mehrfach angemeldet sind, müssen von der Software erkannt und gegebenenfalls automatisch gesperrt werden. Zumindest muß der Administrator in geeigneter Weise alarmiert werden. Eine noch bessere Lösung bestände darin, daß bereits der Authentisierungsserver die gleichzeitige Nutzung durch ein und dieselbe Person unterbinden könnte. Dies ist momentan bei den meisten Lösungen für LAN-Erweiterungen nicht implementiert. Eine Erstellung der Top Ten kann außerdem Hinweise auf die mißbräuchliche Mitbenutzung eines Accounts geben, ebenso wie ungewöhnliche Anschaltzeiten am Wochenende oder in der Nacht. Letzteres gilt natürlich nicht für Universitäten, sondern in erster Linie für Firmen, wobei in diesem Fall definierte Zeitfenster für die Einwahl eine bessere Lösung darstellen

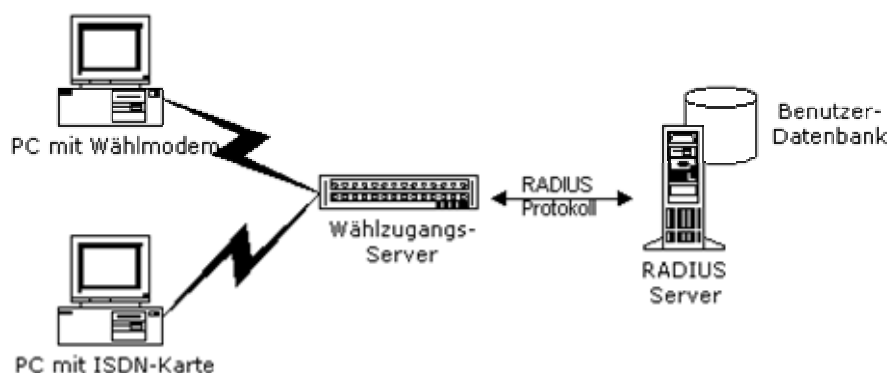
2.3.5. Einwahltechnik ins Internet

Abhilfe: RADIUS(Remote Dial-In User Service)-Protokoll oder TACACS(Access Controller Access Control System)-Protokoll bietet Verbindung zwischen Authentifizierungsserver und Einwahlauthentifizierung.

2.3.5.1. Technik der Authentifizierung mit RADIUS-Protokoll

RADIUS ist ein Authentikationes- und Accountingssystem, das von vielen WISPs verwendet wird. Bei Einloggen in einen LAN oder WLAN Service muss man eingenen Benutzername und Kennwort eingeben. Diese Information lässt sich einem RADIUS Server abgeben, um die Korrektheit zu kontrollieren. Danach ist es zulässig, dass der Nutzer die Services von WISP zugreifen darf.

Die Anmeldung an einem Wählzugangsserver findet über das RADIUS-Protokoll statt. RADIUS ist ein Protokoll zur Validierung der Benutzer von Wählzugängen. Ein typisches Wählzugangssystem ist in dieser Abbildung dargestellt. Hier wird der AAA Server durch einen RADIUS Server ersetzt.

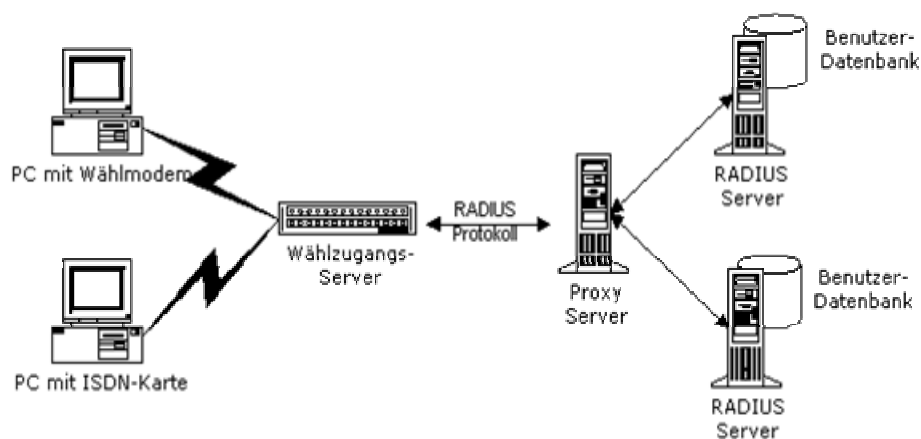


Bei einem Verbindungsaufbau werden in einem solchen System folgende Schritte durchlaufen:

- Der Benutzer baut mit Hilfe eines Modems oder einer ISDN-Karte eine Verbindung zum Wählzugangsserver auf.
- Nach dem erfolgreichen Verbindungsaufbau übergibt er seinen Benutzernamen und das dazugehörige Paßwort.
- Der Wählzugangsserver sendet diese Daten mit Hilfe des RADIUS-Protokolls an den RADIUS-Server. Dieser überprüft die Gültigkeit des Benutzernamen und des Paßworts anhand seiner Benutzerdatenbank, und sendet das Ergebnis zurück an den Wählzugangsserver

2.3.5.2. Das RADIUS-Zonen-Konzept

Der Proxy-Mechanismus erlaubt es mehrere RADIUS-Server für die Validierung der Benutzer einzusetzen. Dies hat den Vorteil, dass die Verwaltung von Benutzerkennzeichen und Paßwörter dezentral erfolgen kann. Der schematische Aufbau eines Wählzugangs mit einem Proxy-Server ist in der Abbildung dargestellt.



RADIUS-Zonen dienen zur Authentifikation von Benutzern und deren Kennungen von RADIUS-Servern verwaltet werden. Wer also eine Kennung an einem der aufgeführten RADIUS-Rechnern besitzt, kann sich mit seinem Anmeldennamen anmelden.

Wenn viele Einwählleitungen betrieben werden, sollte die Authentisierung, Autorisierung und Abrechnung zentral auf einem Rechner erfolgen um die Komplexität und Fehleranfälligkeit so gering wie möglich zu halten. Mit Hilfe von RADIUS Server können die Authentisierungs- Autorisierungs- und Accountingdaten zentral verwaltet und ausgewertet werden. Der Wählzugangsserver sendet die Daten an den RADIUS Server, der die Authentisierung durchführt und Accountingdaten aufzeichnet.

2.3.5.3. Technik der Authentifizierung mit TACACS-Protokoll

Authentifikationsprotokoll, das insbesondere für Remote-Access-Anwendungen ("Einwahlzugänge") spezifiziert wurde. TACACS erlaubt die zentrale Verwaltung der

Accounts von Benutzern und ihrer Passwörter in einem System, das aus mehreren dezentralen Servern (TACACS-Servern) besteht. Weiterentwicklungen sind XTACACS und TACACS+, die ähnliche Features wie das Sicherheitskonzept RADIUS (Remote Authentication Dial-in User Service) anbieten. Größtes Problem der ersten beiden TACACS-Versionen war die unverschlüsselte Datenübertragung, was bei der Passwortübermittlung als unsicher angesehen werden muss. Während das originale TACACS-Protokoll ein offener Internet-Standard war, entwickelte sich TACACS+ durch Erweiterungen seitens der Firma Cisco immer mehr zu einem proprietären Protokoll. Dies ist auch ein Grund für die weite Verbreitung von RADIUS.

2.3.6.1. iPass

Aggregator/Broker iPass bietet der mobilen Geschäftswelt eine optimale und sichere Lösung für den Zugang zu Firmennetzen, E-Mail und Internet von fast jedem Punkt der Welt aus. Mit der Flexibilität des IP-Protokolls ist iPass in der Lage, einen sicheren Zugang über Wireless und Wired Broadband, ISDN und analogen Anschluss zu lokalen Einwahlgebühren herzustellen. Das global verfügbare WLAN-Netz ist marktführend, die weltweite Gewährleistung von Sicherheitsstandards in den WLAN-Zellen einzigartig. Zusätzlich ist der preisgekrönte Client „iPassConnect“ in der Lage, bestehende Sicherheitskomponenten eines Unternehmens wie Personal Firewalls und VPN Clients aller führenden Hersteller in die Remote Lösung zu integrieren. Zusammen mit der iPass eigenen Authentifizierung wird dadurch der Remote-Zugang vollständig abgesichert. 1996 gegründet mit Firmensitz in Redwood Shores, California ist iPass heute in den USA, Europa und im asiatisch-pazifischen Raum international vertreten.

2.3.6.2. GRIC

Aggregator/Broker GRIC hat einen Roaming Einwahlzugang durch ein Abkommen mit ca. 300 ISPs in der Welt zur Verfügung. In vergangenen Jahren hat GRIC mit WISPs geschlossen, und begann wireless Services anzubieten. (Als „GRIC Mobile Office“ bezeichnet)

GRIC bietet drei Services an:

- Es bietet eine Client Software an. Sie zeigt, welche WISPs für Netzverbindung zur Verfügung stehen.
- Es behandelt die Authentifizierung und Authorisierung. Die Nutzer kontaktieren zuerst einen GRIC Server, wenn sie irgendwo bei einem Public W-LAN einloggen. Der GRIC Server baut eine Verbindung mit dem local Alliance Member auf. Als Vorteil brauchen die Nutzer nur einen Benutzernamen und ein Kennwort und bekommen nur eine Rechnung für alle Benutzungen von WISP Services.
- GRIC macht alle finanziellen Abrechnungen für Mitglieder und überwacht, wer wem was schuldet.

3. Zusammenfassung

Das Roaming zwischen verschiedenen Netzen und Netztechnologien realisiert ein globales Mobilkommunikationssystem. In diesem Kommunikationssystem können die Nutzer mit eigenem Endgerät (z.B. Mobil Phone, Laptop etc) überall in der Welt die Services von verschiedenen Service Providern mitnutzen. Der Netzzugang muss durch verschiedene Sicherheitsmassnahmen abgesichert. Z.B bei Handy roaming wird die Kundenidentität durch HLR und VLR überprüft. Bei WLAN und EINWAHL gibt es RADIUS und TACACS für die Authentifizierung zur Verfügung zu stehen.