Stefanus Römer

Leitfaden
zur mobilen Applikationsentwicklung
Grundlagen, Konzepte, Empfehlungen

Herausgegeben von
Concept Factory Mathias Reinis
bei Books on Demand GmbH, Norderstedt

Bibliographische Information der Deutschen Bibliothek:
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind im Internet über http://dnb.ddb.de abrufbar.

Impressum

Autor:
Stefanus Römer

Herausgeber:
Concept Factory Mathias Reinis
„Ihre professionelle Projekt-Begleitung"
Bonner Logsweg 46
53123 Bonn

http://www.concept-factory.de
http://www.privacy-audit.de

Das Cover wurde gestaltet von Klaus-D. Honemann
Konzeption & Grafik Design, St.Augustin

Herstellung und Verlag:
Books on Demand GmbH, Norderstedt

ISBN 10: 3-8334-6405-4
ISBN 13: 978-3-8334-6405-8

Inhaltsverzeichnis

Inhaltsverzeichnis Seite

Vorwort

Grusswort

Technik bestimmt unser aller Leben. Täglich sind wir von einer immensen Vielzahl technischer Geräte umgeben. Wir sind Zeugen und Nutzer einer rasanten Entwicklung in der Informations- und Telekommunikationstechnik, insbesondere in der Mobilfunkkommunikation. Das Mobiltelefon ist aus dem Alltags- und Geschäftsleben nicht mehr wegzudenken, ist gar Kulturgut für jedermann geworden und dient längst nicht mehr nur zur Sprachübertragung. Mobile Datendienste wie GPRS, UMTS oder HSDPA setzen die Maßstäbe für derzeitige und künftige Anwendungen über alle Bereiche der Telekommunikation. Für den Entwickler ergeben sich dadurch anspruchsvolle Herausforderungen an die Konfiguration und für das Design sowie die Implementierung.

Die Redaktion der Fachzeitschrift WissenHeute der Telekom Training empfiehlt den Leserinnen und Lesern dieses Nachschlagewerk, das eine praxisorientierte Unterstützung bei der Entwicklung hochwertiger und professioneller Anwendungen im Mobilfunk gibt.

Detlef Hechtel

Chefredakteur

WissenHeute

Danksagungen

Ein besonderer Dank gilt der Fachredaktion WissenHeute der Deutschen Telekom, die mich stets tatkräftig unterstützt hat und mir mit Rat und Tat zur Seite stand, sowie meinem Arbeitgeber, der T-Mobile International, die mit vielen fachlichen Informationen die Entstehung dieses Werkes überhaupt ermöglichte.

Erwähnen möchte ich zudem die inhaltlichen Beiträge von Marcus Freitag, Holger Zwingmann und Harald Schmitt sowie das Engagement meines Herausgebers Mathias Reinis.

Vorwort

Das vorliegende Praxisfachbuch gibt eine Einführung in die Grundlagen der mobilen Anwendungsentwicklung. Es orientiert sich an dem allgemeinen Phasenmodell des Software-Development-Prozesses und hilft dem Entwickler, seine Anwendung für den mobilen Einsatz anzupassen.

Nach einer allgemeinen Einleitung über die Bedeutung der mobilen Datenkommunikation, deren Vorteile und typischen Anwendungsszenarien gliedert sich das Fachbuch in zwei Hauptteile (Abbildung 1).

Teil 1 befasst sich mit den Grundlagen der mobilen Datenkommunikation.

Zunächst werden die speziellen Fragestellungen der mobilen Anwendungsentwicklung aufgezeigt. Der Leser erhält einen Überblick über den gesamten Entwicklungsprozess und erkennt, welche Aspekte in den einzelnen Phasen wichtig sind.

Das darauf folgende Kapitel beschreibt die Eigenschaften der mobilen Datendienste General Packet Radio Service (GPRS), Universal Mobile Telecommunications System (UMTS) sowie High Speed Data Packet Access (HSDPA) und deren Auswirkungen auf die Anwendungsentwicklung.

Das letzte Grundlagenkapitel widmet sich dem Querschnittsthema der Sicherheit im Mobilfunk und gibt wichtige Hinweise, die sowohl bei der Software-Entwicklung selbst als auch beim späteren Einsatz der fertigen Anwendung zu berücksichtigen sind.

Abbildung 1: Gliederung des Lehrstoffs

Der zweite Teil dieses Leitfadens behandelt die einzelnen Phasen des allgemeinen Phasenmodells - Analyse, Design, Implementierung und Test – und geht jeweils im Detail auf die speziellen Fragestellungen der mobilen Datenkommunikation ein.

Anhand von konkreten Empfehlungen für die Analyse-, Design-, Implementierungs- und Testphase erfährt der Leser Schritt für Schritt, welche Aspekte in den einzelnen Phasen eine wesentliche Rolle spielen, und wie diese bei der Software-Erstellung konzeptionell zu berücksichtigen sind. Ergänzend hierzu sind viele

nützliche Code-Beispiele im Application Configuration & Developer Guide der T-Mobile [1] zu finden.

Bei der Stoffauswahl wurde grundsätzlich der **praktische Nutzen für Programmierer und Projektleiter** in den Vordergrund gestellt. Auf eine detaillierte technische Beschreibung der Abläufe im Mobilfunknetz wurde weitestgehend verzichtet, sofern diese nicht für das grundlegende Verständnis notwendig sind. Wichtig waren stets die besonderen Eigenschaften von GPRS, UMTS und HSDPA im Vergleich zu drahtgebundenen Datennetzen und deren Folgen für den Prozess der Anwendungsentwicklung.

Dieser Leitfaden richtet sich an Studenten der Informatik oder Elektrotechnik/Informationstechnik sowie an Berufsanfänger und erfahrene Programmierer, Projektleiter und IT-Verantwortliche, die sich in dieses Themengebiet einarbeiten wollen oder ein praxisorientiertes Nachschlagewerk suchen.

Er ist eine Hilfestellung für alle Beteiligten des Software-Entwicklungsprozesses und trägt dazu bei, mobile Datenkommunikation zu verstehen und sinnvoll in Projekte einzuplanen. Dem Projektleiter bietet er die Möglichkeit, Aufwände genauer abzuschätzen und das Budget realistisch zu planen. Der Analyst bekommt viele Informationen, die für ein schnelles Verständnis der Technologie sorgen. Der Designer kann die besonderen Anforderungen an die Architektur mobiler Anwendung erkennen. Algorithmen und Beispielcode geben dem Entwickler Anregungen für die Umsetzung der Architektur. Den Testern zeigt der Leitfaden, wie eine mobile Anwendung auch im Labor auf ihre Eignung im mobilen Einsatz getestet werden kann.

Die Leser sollten die grundlegenden Konzepte der Software-Erstellung beherrschen und Kenntnisse in Windows, TCP/IP, Modemkommunikation, den Programmiersprachen C und C++ sowie den Bibliotheken WIN32 API und MFC (Microsoft Foundation Classes) besitzen.

Kommentare und Verbesserungsvorschläge sind jederzeit willkommen und können unter www.stefanus-roemer.de eingestellt werden.

Einführung

1 Einführung

1.1 Die Bedeutung der mobilen Datenkommunikation

Die mobile Datenkommunikation hat für viele Unternehmen inzwischen grundlegende Bedeutung erlangt. Die ständige Erreichbarkeit sowie die Möglichkeit zum Zugriff auf geschäftskritische Daten an jedem Ort und zu jeder Zeit werden in einem sich verschärfenden Wettbewerb immer wichtiger. Kundennähe und Service sind die entscheidenden Wettbewerbsfaktoren. Der direkte Zugriff auf aktuelle und konsistente Informationen wird somit unverzichtbar.

Für die Unternehmen ist es heute wichtig, gezielte Informationen zur richtigen Zeit am richtigen Ort und in der richtigen Form zur Verfügung zu stellen. Die wachsende Bedeutung des Produktionsfaktors Information in allen Bereichen der Wirtschaft zwingt sie zu einer umfassenden Vernetzung entlang ihrer gesamten Wertschöpfungskette, und zwar angefangen mit den Lieferanten, über die internen Unternehmensbereiche bis hin zu den Kunden. Wer in den dynamischen Märkten von heute bestehen möchte, muss schnell und flexibel auf veränderte Bedingungen reagieren können. Der verschärfte Wettbewerb erfordert insbesondere eine größere Kundennähe mit deutlich verkürzten Reaktionszeiten bei Akquisition und Service. Die Qualität der Kundenbetreuung wird somit zum entscheidenden Wettbewerbsfaktor und bedingt den verstärkten Einsatz mobiler Außendienstmitarbeiter und deren flexible Anbindung an das vorhandene Kommunikationsnetz. Remote Access zum lokalen Unternehmensnetz ist daher eines der am stärksten wachsenden Marktsegmente der Telekommunikation. Der zunehmende Wettbewerb und der Zwang zu mehr Kundennähe in allen Bereichen der Wirtschaft führt dazu, dass immer mehr Unternehmen dezentrale Strukturen

ausbilden und die Zahl ihrer Außendienststellen sowie ihrer Außendienstmitarbeiter erhöhen. Gleichzeitig führt die Flexibilisierung der Arbeitsformen zu einer Zunahme der Heimarbeitsplätze. Grundsätzlich können zwei Nutzergruppen unterschieden werden:

- Mobile Workers sind Mitarbeiter, die regelmäßig außerhalb ihres Büros arbeiten bzw. keinen festen Arbeitsort haben. Für den Zugriff auf das Firmennetzwerk wird meist ein Laptop und Mobilfunk eingesetzt. Bei dieser Nutzergruppe liegt der Schwerpunkt auf der Mobilität.
- Teleworkers arbeiten regelmäßig, aber nicht ständig, außerhalb ihres Büros. Der alternative Arbeitsplatz ist dabei nicht mobil. Normalerweise ist ein so genanntes Home Office (Heimarbeitsplatz) dann der Arbeitsplatz. Der Zugriff auf das Firmennetzwerk geschieht in der Regel mittels eines Standard-PC und einer Modem-/ISDN- oder DSL-Einrichtung. Bei dieser Nutzergruppe liegt der Schwerpunkt auf den kostengünstigen und einfachen Anschlussmöglichkeiten.

1.2 Generelle Vorteile mobiler Datenlösungen

1.2.1 Höhere Produktivität

Unproduktive Arbeitszeiten sind für viele Unternehmen ein Problem. Viele Mitarbeiter verbringen einen großen Teil ihrer Arbeitszeit auf Dienstreisen. Dabei kommt es stets zu Wartezeiten z.B. auf Bahnhöfen oder Flugplätzen. Auch während der eigentlichen Fahrt oder bei Kunden kann häufig die Arbeitszeit nicht produktiv genutzt werden, da sich der Mitarbeiter nicht mit dem Unternehmensnetz verbinden und auf interne Ressourcen wie z. B. den Email-Server oder das interne Dateisystem zugreifen kann.

Wenn durch den Einsatz einer mobilen Zugangslösung nur zwei Stunden pro Mitarbeiter und Woche gewonnen werden, so ergibt sich bei einem angenommenen Stundensatz von zwischen 50,-€ und 75,- € konservativ geschätzt eine Ersparnis pro Mitarbeiter und Jahr von ca. 2300,- € bis 3450,- €.

1.2.2 Steigerung der Wettbewerbsfähigkeit durch verbesserten Kundenservice

Der verschärfte Wettbewerb bietet den Kunden eine Vielfalt von Wahl- und Vergleichsmöglichkeiten. Kundennähe und ein verbesserter Kundenservice gehören für die meisten Unternehmen daher bereits zu den kritischen Erfolgsfaktoren.

Ein guter Kundenservice zeichnet sich insbesondere durch kurze Reaktionszeiten aus. Die Möglichkeit, jederzeit sowie ortsunabhängig auf zentral gespeicherte Daten (z.B. Kundendaten, Warenwirtschaftssysteme, technische Daten oder Service-Aufträge) zugreifen zu können, ist unverzichtbar.

Für den Vertrieb bedeutet dies beispielsweise, sich während eines Kundengespräches im Bedarfsfall direkt in das eigene Unternehmensnetz einwählen zu können, um sofort auskunftsfähig über Produktverfügbarkeit, Lieferzeiten und Preise zu sein oder ohne Verzug Bestellvorgänge anstoßen zu können.

1.2.3 Kosteneinsparung

Durch den Einsatz moderner Datenkommunikationslösungen lassen sich in manchen Fällen erhebliche Kommunikationskosten sparen, da sich

Kommunikationsvorgänge schneller und effektiver abwickeln lassen und teurere Kommunikationsdienste vermieden werden. Anstatt Service-Aufträge über lang andauernde Telefongespräche mit vielen Rückfragen von der Einsatzzentrale zu erhalten, lassen sich die nötigen Informationen viel schneller und viel effizienter beispielsweise per Email übermitteln. Traditionelle Arbeitsformen, bei denen sich der Service-Techniker morgens oder zwischendurch seine Service-Aufträge persönlich in der Zentrale abholen muss, können vollständig ersetzt werden. Reisekosten und unproduktive Arbeitszeiten lassen sich vermeiden.

1.2.4 Schnellere Entscheidungsprozesse

Häufig kommt es vor, dass kritische Entscheidungen verschoben werden müssen, weil wichtige Entscheidungsträger nicht zur Verfügung stehen und keinen Zugang zu den relevanten Informationen haben. Mit Hilfe mobiler Einwahllösungen können sich die Entscheidungsträger jederzeit ein Bild von der aktuellen Lage machen und aktiv am Entscheidungsprozess teilnehmen.

1.3 Anwendungsgebiete und Zielgruppen

Mobile Datenkommunikationslösungen kommen in den verschiedensten Bereichen zum Einsatz. Neben speziellen Lösungen für bestimmte Wirtschaftszweige wie z.B. Transport und Logistik oder die Energiewirtschaft findet man auch branchenübergreifende Lösungen. Häufig werden durch den Einsatz mobiler Datenkommunikation nicht nur die Kosten gesenkt und die Effizienz gesteigert, sondern auch neue Einsatzmöglichkeiten erschlossen, die mit bisheriger Technik und Arbeitsweise nicht denkbar waren.

Nachfolgend werden beispielhaft einige typische Anwendungsszenarien beschrieben, bei denen die Vorteile von mobilen Datenlösungen leicht nachvollziehbar sind. Wie mit jeder neuen Technik sind die Einsatzmöglichkeiten vielfältig und beschränken sich nicht auf einige wenige Fälle.

1.3.1 Vertrieb (Mobile Sales Force)

Vertriebsmitarbeiter müssen kurzfristig und kompetent auf Kundenanfragen reagieren können und im Kundengespräch stets auskunftsfähig sein. Mobile Einwahllösungen ermöglichen es, jederzeit und unabhängig vom Ort auf zentrale Daten zuzugreifen. Hierzu gehören beispielsweise:

- Kundendaten (Verträge, Historie, Rechnungsdaten, etc.)
- Produktdaten (Beschreibungen, Präsentationen, Preis, Lieferzeiten, Verfügbarkeiten, etc.)
- Bestellvorgänge

Der Vorteil liegt in einer unmittelbaren Steigerung des Vertriebserfolgs. Der Vertriebsmitarbeiter ist jederzeit kompetent und kann dem Kunden sofort alle nötigen Informationen beschaffen, um einen Auftrag abzuschließen.

1.3.2 Technischer Kundendienst (Mobile Service Force)

Der technische Kundendienst muss schnell auf Service-Aufträge reagieren können und Störungen umgehend beseitigen.

Insbesondere im Investitionsgüterbereich wird eine schnelle Verfügbarkeit von Service-Technikern und eine professionelle Instandsetzung in kurzer Zeit vorausgesetzt.

Durch den Einsatz mobiler Einwahllösungen lassen sich gegenüber der herkömmlichen Arbeitsweise erheblich Effizienzgewinne realisieren.

Ohne den Einsatz von mobilen Dispositionslösungen fahren Service Techniker im Außendienst gewöhnlich zu Beginn ihres Arbeitstages in die Unternehmenszentrale, um sich ihre Arbeitsaufträge für den Tag abzuholen. Es folgt die Anreise zum Kunden, dann die Service-Leistung selbst. Arbeitszeiten, gefahrene Kilometer, durchgeführte Wartungsarbeiten, Ergebnisse und Ersatzteilbestellungen werden handschriftlich festgehalten. Zwischendurch melden sich die Techniker allenfalls per Mobiltelefon, um nach weiteren Aufträgen zu fragen. Informationen über Ersatzteilverfügbarkeit, Lieferzeiten und Preise sind jedoch in der Regel vor Ort nicht verfügbar und können dem Kunden erst am nächsten Tag mitgeteilt werden. Am Ende des Arbeitstages geht es wieder zurück in die Zentrale, um die Daten manuell in das Warenwirtschaftssystem einzugeben.

Lösungen zur Optimierung und Beschleunigung des technischen Service ermöglichen demgegenüber:

- eine strukturierte Disposition der Service-Techniker (sofortige Auftragsweiterleitung, Routenplanung, sofortige Leistungsverrechnung -> optimierte Zahlungseingänge)
- einen Zugriff auf Lagerbestände, Preisauskunft und sofortige Bestellung

Die Vorteile sind eine deutliche Verkürzung von Reaktions- und Entstörzeiten, eine signifikante Kostenreduktion sowie insbesondere eine erhöhte Kundenzufriedenheit.

1.3.3 Mobile Office Solutions

Viele Angestellte im Dienstleistungsunternehmen verbringen einen großen Teil ihrer Arbeitszeit mit der täglichen Bearbeitung ihrer Emails oder ihrer Kalendereinträge.

Durch den Einsatz mobiler Office-Lösungen für E-Mail und Kalender können unproduktive Arbeitszeiten z.B. während einer Dienstreise genutzt werden. Zudem können die Mitarbeiten im Bedarfsfall auch zwischendurch flexibel auf ihre Emails zugreifen und somit ihre Arbeitslast während der Bürozeiten von Routinearbeiten befreien.

Die Vorteile sind je nach Anwendungsszenario erhebliche Kostenersparnisse sowie Produktivitätssteigerungen.

1.3.4 Maschine-zu-Maschine

Die Vernetzung von technischen Anlagen wie Maschinen, Zähler, Automaten oder Fahrzeuge mit einer zentrale Steuerungs- und Überwachungsstelle wird im industriellen Bereich zunehmend erfolgskritisch.

Beispiel Energieversorger:

Energieversorger unterhalten eine Vielzahl geographisch verteilter Zähler und Stellwerke (Utilities), die nötig sind, um das Energieversorgungssystem zu überwachen und zu steuern.

Für diese Utilities gibt es eine Reihe von Anwendungsfelder:

- Zählerfernabfrage, die heute zunehmend auf GPRS-Lösungen umgestellt wird, um aktuelle und genaue Verbrauchsdaten für die Kunden zu bekommen.
- Service & Maintenance
- Remote Management der Messgeräte
- Echtzeitabfrage aller Zähler (quasi-gleichzeitig) anstatt zeitaufwendige und teure Abfrage über leitungsvermittelte Modemverbindungen.

Die Vorteile sind Kostenersparnisse und Produktivitätssteigerungen der jeweiligen Anlagen sowie Qualitätssteigerungen und die Erschließung neuer Nutzungsmöglichkeiten (z.B. die Teilnahme am Stromhandeln auf der Basis zeitgenauer Zustandsdaten).

1.3.5 Transport & Logistik

Lösungen für Auftragsmanagement, Sendungsverfolgung, Fahrzeugdaten- und Statusübermittlung sowie für die Ortsinformation von Fahrzeugen oder Containern auf Basis von SMS (Short Message Service) stehen seit vielen Jahren zur Verfügung. Die deutlichen Kostenvorteile durch Einsatz dieser Lösungen lassen sich mit der GPRS-Technologie noch weiter steigern.

1.3.6 Gesundheitswesen / Mobile Health Care[1]

Mit Lösungen, die auf mobiler Datenkommunikation basieren, lassen sich die medizinische Einsätze deutlich effizienter gestalten und die Abrechnung zeitnah abwickeln. Beispiele sind:

- Herbeiruf von Bereitschaftsärzten und Pfleger. Mobiler Abruf von Patientendaten.
- Reduzierung von internen Rückfragen (Arzt –> Pflegepersonal, Stationsarzt –> Chefarzt)
- Schneller Zugriff aller Mitarbeiter auf zentrale Daten (z.B.: Pflegestatus oder Medikamenten-Datenbank)
- Verringerung von Medienbrüchen bei der Eingabe patientenbezogener Daten (z.B.: Ergebnisse der Visite werden direkt im Laptop erfasst)
- Gute Akzeptanz durch einfache Bedienung

Die Vorteile sind Kostenersparnisse und Produktivitätssteigerungen sowie letztlich eine Verbesserung der medizinischen Leistungen.

[1] Siehe hierzu auch die aktuelle Studie „conceptory® Klinik IT Report 2006“ von Mathias Reinis, ISBN 978-3-8334-5250-5

Grundlagen

2 Grundlagen

2.1 Besonderheiten mobiler Anwendungsentwicklung

Die Datenkommunikation spielt bei der Software-Entwicklung eine wesentliche Rolle, denn nur in den seltensten Fällen werden noch isoliert auf einem Rechner Anwendungen (Applikationen) entwickelt. Ob über das lokale Netzwerk (Local Area Network = LAN), Weitverkehrsnetze, Digital Subscriber Line (DSL) oder über die klassischen Einwahlverbindungen: Anwendungen haben Zugriff auf zentrale Unternehmensdaten und können diese direkt abrufen und/oder manipulieren. Zunehmend kommen dabei auch mobile Übertragungstechniken, wie beispielsweise General Packet Radio Service (GPRS) oder das Universal Mobile Telecommunication System (UMTS) zum Einsatz. Bei der mobilen Datenübertragung ist eine effiziente Ausnutzung der verfügbaren Bandbreite und ein möglichst schneller Datentransfer besonders wichtig, um den Anwender nicht durch zeitraubende Verzögerungen zu verärgern. Dieses Kapitel bietet zunächst einen Überblick über die Besonderheiten bei der Entwicklung und orientiert sich an dem allgemeinen Phasenmodell der Anwendungsentwicklung (Abbildung 2). In den nachfolgenden Kapiteln werden aufeinander aufbauend die wesentlichen Aspekte der mobilen Anwendungsentwicklung erläutert.

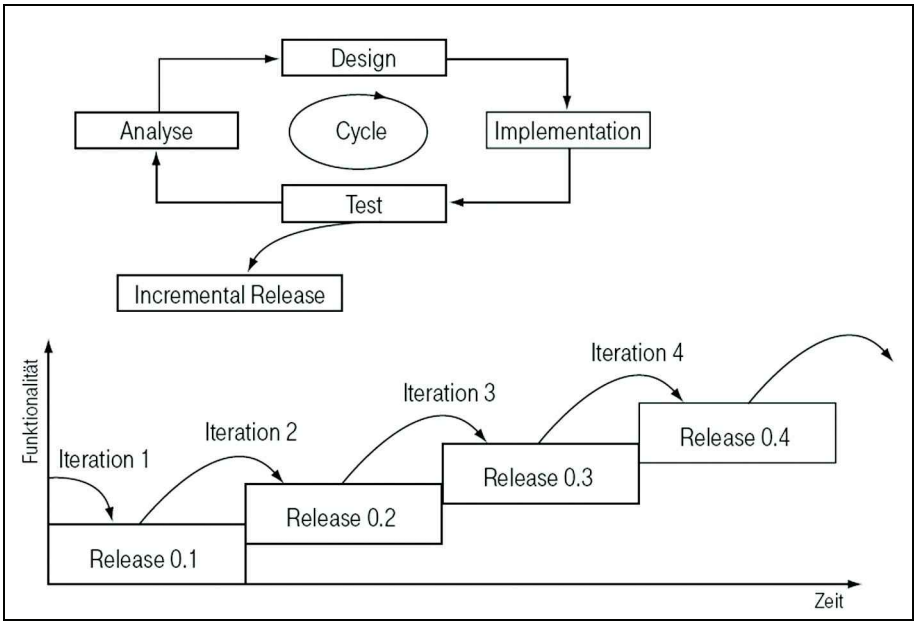


Abbildung 2: Inkrementelles Phasenmodell der Software-Entwicklung

2.1.1 Einführung

Komfortable Entwicklungsumgebungen und mächtige Klassenbibliotheken für nahezu alle Einsatzbereiche vereinfachen die Software-Entwicklung heutzutage deutlich. Komplexe Plattformen wie zum Beispiel Microsoft .NET oder auch J2EE (Java Platform Enterprise Edition) bieten dem Entwickler eine gute Basis für die schnelle Entwicklung von Anwendungen jeglicher Art. Auch für den Bereich der Datenkommunikation unterstützen zuverlässige Standardbibliotheken die schnelle Implementierung von Kommunikationsabläufen.

Als Beispiele seien hier SOAP (Simple Object Access Protocol[2], RFC 3288) oder IIORB (Internet-Inter Object Request Broker) von SUN genannt.

Anwendungsfälle und Geschäftsprozesse spielen beim Entwurf einer neuen Anwendung die entscheidende Rolle, die technischen Aspekte wie etwa die zu verwendenden Protokolle treten dagegen in den Hintergrund. Basierend auf den Anforderungen wird eine Architektur entworfen, das Datenmodell definiert und die Interaktion zwischen den Komponenten festgelegt. Bei der Implementierung schließlich kann sich das Entwicklungsteam auf eine Vielzahl von existierenden und wieder verwendbaren Bibliotheken und Programmierschnittstellen (APIs) stützen.

Die Zuverlässigkeit und damit auch die Akzeptanz von Kommunikationsanwendungen hängt dabei von der Verfügbarkeit und Qualität aller beteiligten Komponenten ab. Eine verständliche, intuitiv bedienbare Benutzerschnittstelle, schnelle Datenbankabfragen und eine robuste Fehlerbehandlung zeichnen unter anderem eine gute Anwendung aus. Im Bereich der Datenübertragung ist die effiziente Ausnutzung der verfügbaren Bandbreite und damit ein möglichst rascher Datentransfer notwendig, um den Anwender nicht durch zeitraubende Verzögerungen zu verärgern. Viele Kommunikations-Anwendungen wurden dementsprechend entwickelt und laufen hervorragend, selbst über klassische Einwahlverbindungen mit 56 – 64 KBit/sec.

Mobile Übertragungstechniken, wie z.B. GPRS, UMTS, HSDPA, oder Wireless LAN (WLAN) eröffnen neue Möglichkeiten beim Einsatz von Kommunikationsanwendungen. Weder ein Netzwerkkabel noch eine Telekommunikationsanschlusseinheit (TAE) sind notwendig, um die Anwendung

[2] SOAP: Standardisiertes Protokoll zum Austausch von Daten zwischen unterschiedlichen Anwendungen. SAOP ist von grundlegender Bedeutung bei der Erstellung von so genannten Webservices.

mit einem Unternehmensnetzwerk zu verbinden - ein Funkmodem oder ein Handy reichen für den Zugriff aus.

Die Konzeption und Umsetzung eines mobilen Anwendungsszenarios ist jedoch eine sehr vielschichtige Aufgabe. Es gibt eine fast unüberschaubare Vielfalt an Lösungen und Bausteinen, die jeweils für verschiedene Anforderungen oder Einsatzmöglichkeiten geeignet sind. Zu Beginn eines jeden Entwicklungsprojektes sind daher zunächst sehr viele grundlegende Fragen zu klären.

Zahlreiche Unternehmen nutzen Applikationen, die für eine reine LAN-Umgebung oder für das Internet entwickelt wurden und setzen somit leistungsstarke Rechner, Netze mit hohen Übertragungsbandbreiten und geringen Laufzeiten (Delay) sowie komplexe Benutzerschnittstellen voraus. Mobile Systeme können diese Anforderungen jedoch nicht erfüllen. Möchte man die vorhanden Applikationen ohne spezielle Anpassungen in einer mobilen Umgebung einsetzen, so kann dies zu erheblichen Einschränkungen führen, die die Akzeptanz der Nutzer grundlegend in Frage stellen. Die Leistungsdaten mobiler Übertragungsmedien, wie beispielsweise GPRS, ähneln zwar auf den ersten Blick sehr denen einer ISDN-Verbindung, denn die Datenrate ist durchaus vergleichbar. Ein näherer Vergleich zeigt jedoch schnell, dass es gegenüber drahtgebundenen Übertragungsverfahren wesentliche Unterschiede gibt, die erhebliche Einflüsse auf die Anwendungsentwicklung haben.

Entscheiden sich Unternehmen für den Einsatz mobiler Datenkommunikation, testen sie ihre Anwendungen meist zunächst beispielsweise in der Entwicklungsabteilung mit dem neuen Medium. Oft sind die ersten Ergebnisse sehr vielversprechend, die Übertragungsgeschwindigkeit ausreichend, das Ansteuerung der neuen Endgeräte zwar etwas gewöhnungsbedürftig, aber beherrschbar.

Verhältnismäßig schnell wird dann mit einem Feldtest oder gar einer vorzeitigen Einführung (Rollout) begonnen.

Hier treten dann häufig erhebliche Probleme auf: Die Software läuft nicht stabil, verhält sich unberechenbar, wird plötzlich langsamer bis zum Stillstand oder die Verbindung bricht ständig mit unerklärlichen Fehlermeldungen ab. Die Anwender sind deshalb unzufrieden mit der Performance[3] und der Handhabung und reagieren zunehmend verärgert. Die Entwickler beginnen dann oft eine intensive Fehlersuche (Debugging) ihrer Anwendung, bauen punktuelle Änderungen ein, die oftmals die Anwendungslogik negativ beeinflussen und versuchen das eigentliche Problem an der falschen Stelle zu lösen. Nicht wenige Projekte sind durch eine solche Vorgehensweise gescheitert und haben hohe Kosten verursacht.

Doch es gibt auch Anwendungen, die stabil über mobile Kommunikationswege laufen. Es gibt Lösungen, bei denen Unternehmen mobilen Zugriff ortsunabhängig und zu jeder Zeit für ihre Kunden einsetzen. Diese Unternehmen haben sich bereits in einer frühen Projektphase intensiv mit den Eigenschaften des neuen Kommunikationsmediums auseinander gesetzt und ihre Anwendungen an diese Eigenschaften angepasst.

2.1.2 Schwerpunkte in der Analysephase

2.1.2.1 Anforderungen an mobile Anwendungen

Bevor die ersten Zeilen eines Programmcode geschrieben werden können, sind in einem Software-Projekt viele vorbereitende Schritte notwendig. Ausgehend von den wesentlichen Anforderungen an die zukünftige Anwendung, beginnt der

[3] Performance: Leistungsstärke.

Projektleiter zunächst mit der Informationsbeschaffung. Danach erstellt er im Rahmen der Analyse auf Grund der erhalten Informationen die Anforderungs-Spezifikation und das so genannte Pflichtenheft für das Projekt.

Ist im Vorfeld eines Projektes GPRS als Übertragungsmedium festgelegt worden, so steht eventuell nur dieser Begriff auf der Liste für die Informationsbeschaffung. Was sich tatsächlich dahinter verbirgt, ist für den Projektleiter in dieser Phase schwer abzuschätzen. Folgende sieben Fragen sind zu stellen:

- Was sind die grundlegenden Eigenschaften der mobilen Datenkommunikation mit GPRS und UMTS?
- Welche Client-Plattform eignet sich für das Projekt?
- Welche Anschlüsse an das Unternehmensnetz sind nötig?
- Welche Tarife bieten sich für das Projekt an?
- Welcher Netzbetreiber eignet sich für das Projekt?
- Welche Auswirkungen hat GPRS auf die Software-Entwicklung?
- Wie kann man den Entwicklungsaufwand reduzieren?

Diese sieben Kernfragen sind typisch für Projekte im Bereich mobiler Datenkommunikation. Bei der intensiven Beschäftigung mit dem Thema treten häufig weitere Fragen auf, zusätzliche Entscheidungen sind zu treffen und weitere Anforderungen zu definieren. Mit einem breitem Wissensfundament sinkt jedoch das Risiko, eine falsche Entscheidung zu treffen.

2.1.2.2 Client-Plattform

Eine Client-Plattform besteht aus einem

- Rechner,
- Betriebssystem und
- Endgerät für die Datenkommunikation.

Die Client-Plattform wird vom Anwender benutzt, um mobil mit der Software-Lösung zu arbeiten. Die Entscheidung für eine bestimmte Client-Plattform muss in einem Projekt so früh wie möglich getroffen werden. Wichtig ist es, dass die Anwender die gewählte Client-Plattform akzeptieren und dass sie in das Projektbudget passt. Weil es die "ideale" Plattform für alle Projekte jedoch nicht gibt, muss man diese sorgfältig anhand des jeweiligen Anforderungsprofils auswählen. Spontane Entscheidungen, die beispielsweise durch ein günstiges Angebot getroffen werden, können sich später ungünstig auswirken.

Anmerkung: Auf Grund der zentralen Bedeutung der gewählten Client-Plattform bietet der zweite Teil in Abschnitt 3.1 eine systematische Gegenüberstellung der unterschiedlichen Geräteklassen und/oder Gerätekonfigurationen (Abbildung 3) sowie praktische Entscheidungshilfen für die Wahl der richtigen Plattform.

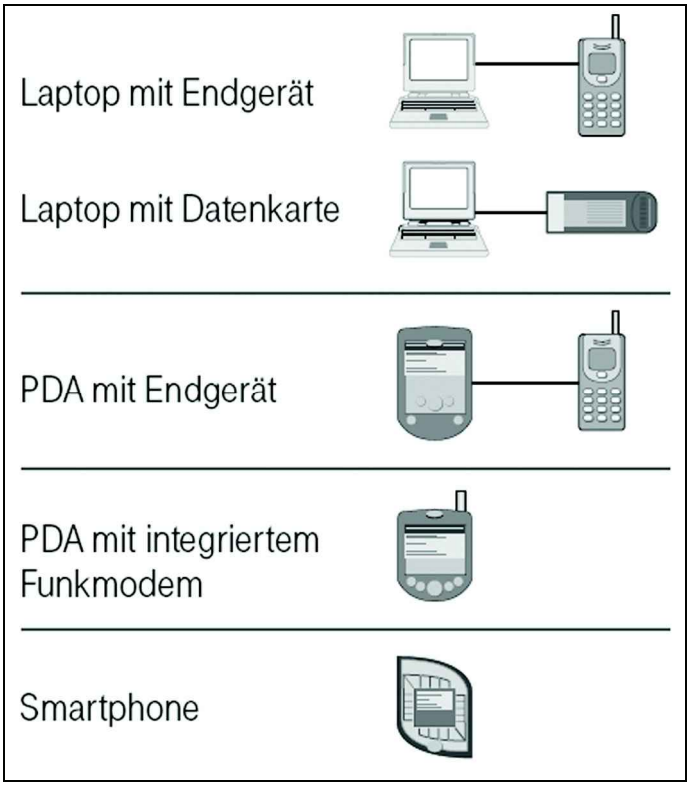


Abbildung 3: Gerätekonfigurationen

2.1.2.3 Anschluss an das Unternehmensnetz

Die Daten können auf verschiedene Wege vom Netzbetreiber in das Unternehmensnetz gelangen. Unterschiedliche Anschlusskonzepte ermöglichen die direkte Verbindung von GPRS- und Unternehmensnetz. Die Auswahl eines Anschlusskonzeptes beeinflusst die Netzwerkarchitektur im Unternehmen sowie die Sicherheitsanforderungen und damit auch die Projektkosten.

- Auswahlkriterien für die Wahl des richtigen Anschaltekonzeptes:
    - Kosten: Investitionen, Lizenzen, Schulungsaufwand, Support- und Betriebskosten
    - Sicherheitsvorgaben für die Wahl der Übertragungsplattform: Soll das Internet oder ein spezielle Datenplattform (z.B. ATM) genutzt werden?
    - Art der Teilnehmerauthentisierung: Soll nur die Mobilfunk-Rufnummer geprüft werden oder sollen sich die Benutzer mit Benutzername und Kennwort anmelden? Ist vielleicht sogar eine starke Authentisierung mit Hilfe eines Einmalpassworts gefordert? Soll die Zugangskontrolle (Authentisierung) vom Mobilfunk-Netzbetreiber im Mobilfunknetz oder vom Kunden selbst im Kundennetz vorgenommen werden.
    - Art der IP-Adressvergabe: Sollen die Mobilfunkgeräte bei jeder Einwahl stets die gleiches IP-Adresse (statische Vergabe) oder ihre IP-Adresse zufällig aus einem Adress-Pool (dynamische Vergabe) erhalten?
    - Art der Zugangsverwaltung: Wer soll die einzelnen Geräte bzw. Benutzer für den Netzzugang verwalten? Ist eine spezielle Web-basierte Administrationsschnittstelle erforderlich?
    - Redundanzkonzept: Soll die Unternehmensnetzanschaltung an das Mobilfunknetz redundant ausgelegt sein?
    - SLA/Support: Gibt es eine spezielle Hotline für die Zugangslösung? Wie sind die Erreichbarkeiten? Gibt es kompetente Ansprechpartner? Wie sind die Reaktionszeiten?
    - Reports: Gibt es spezielle Reports zur jeweiligen Zugangslösung.

Grundsätzlich kann der allgemeine Internet-Zugang aus dem Mobilfunknetz für die Einwahl genutzt werden. Hierzu ist lediglich eine Festverbindung (Standleitung) zwischen Zielnetzwerk und Internet erforderlich. Darüber hinaus wird auf der Client-Plattform ein VPN[4]-Client (z.B. für IPSec) benötigt.

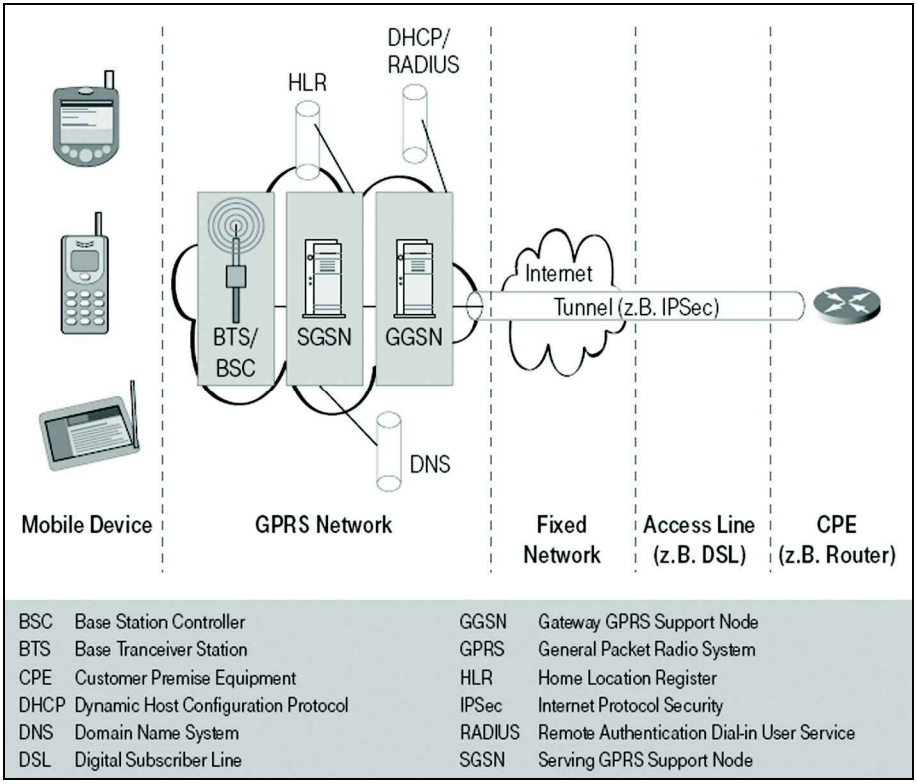


Abbildung 4: Anschaltekonzept über das Internet

[4] VPN: Virtual Private Network – Geschütztes Kommunikationsnetz, dass Ressourcen einer öffentlichen Transportplattform (z. B. das Internet) nutzt.

T-Mobile bietet darüber hinaus mit dem Produkt „Mobile IP VPN" individuelle VPN-Lösungen an, die einen geschützten Zugang zum Unternehmensnetz z.B. über einen IPSec-Tunnel (Abbildung 4) oder eine sichere ATM-Verbindungen über eine spezielle VPN-Plattform[5] (Abbildung 5) ermöglichen[6].

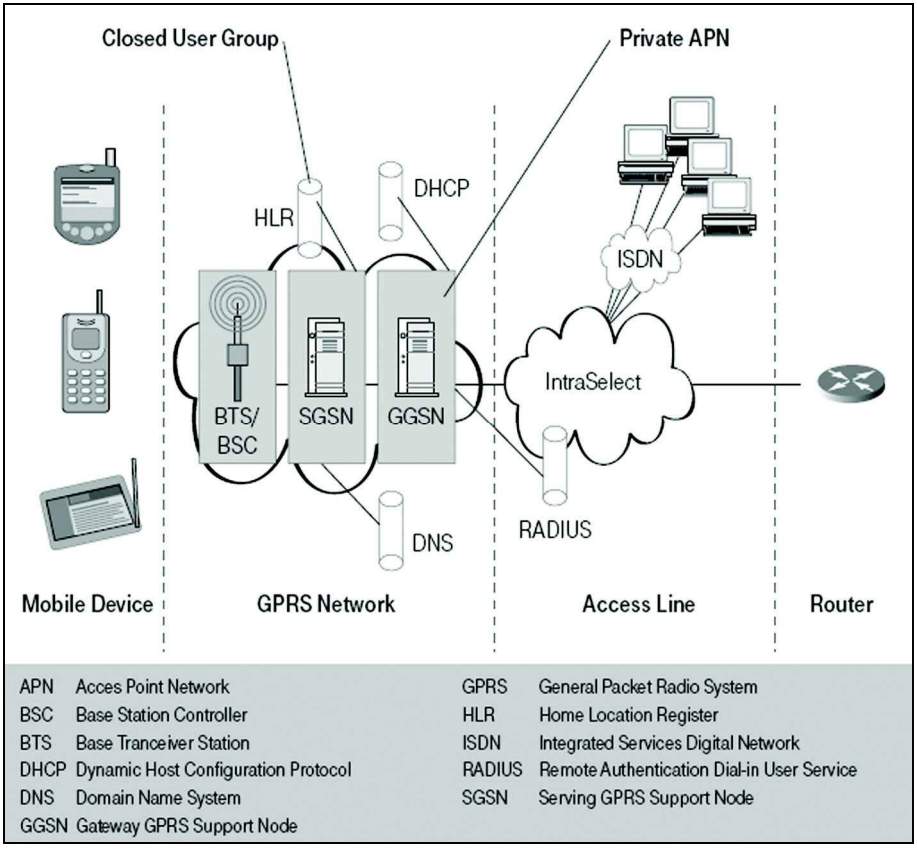


Abbildung 5: Anschaltekonzept über Mobile IP VPN von T-Mobile

[5] z.B. IntraSelect der T-Systems

[6] Siehe hierzu den Beitrag, „Mit GPRS ins Intranet – Das Produkt LAN to LAN GPRS Access", Unterrichtsblätter 3/2001, S. 168 ff.

Hierbei wird das Kundennetz direkt an den Gateway Knoten (Gateway GPRS Support Node = GGSN) der GPRS-Plattform angeschaltet. Der Zugang zum Unternehmensnetz wird mit Hilfe einer geschlossenen Benutzergruppe (GBG) im Mobilfunknetz kontrolliert. Gleichzeitig wird die Übertragungssicherheit durch die vorhandenen Verschlüsselungs- sowie Tunnel-Verfahren von GPRS und UMTS gewährleistet.

Die Vor- und Nachteile dieser beiden Anschlussarten sind in Tabelle 1 zusammengestellt.

Hinweis: Auf Grund der zentralen Bedeutung der gewählten Zugangslösung werden die verschiedenen Konzepte in Abschnitt 2.4 im Einzelnen vorgestellt.

Tabelle 1	Vor- und Nachteile der Anschlussarten	
	Allgemeiner Zugang über Internet (Ende zu Ende)	Direkter Zugang über Mobile IP VPN
Vorteile	■ Kostengünstigste Lösung ■ Internetzugang bei den meisten Unternehmen vorhanden	■ Exklusive Anschaltung des Kundennetzes über VPN-Lösungen der Deutschen Telekom (Intra-Select) für den Datentransfer, unabhängig vom Internet oder über einen IPSec durch das Internet ■ Statische oder dynamische Vergabe privater IP-Adressen für die Clients ■ Hohe Sicherheit ■ Geschlossene Benutzergruppen (Closed User Groups = CUG) möglich, nur spezielle Teilnehmer haben Zugriff ■ Integration mit vorhandenen RADIUS- und Sicherheits-lösungen möglich ■ Einfache Fehlersuche und Support durch einen Ansprech-partner ■ Kombinier- und erweiterbar mit anderen Zugangsmedien
Nachteile	■ Zusätzliche Sicherung bei kritischen Daten notwendig (Einsatz von VPN-Software) ■ Keine exklusive Leitung vom GGSN zum Zielnetz, deshalb eingeschränkte Qualität ■ Keine eindeutigen IP-Adressen der Clients ■ Lizenzkosten je Ein-wahl- Client	■ Je nach Variante zusätzliche Standleitung notwendig ■ Kosten

2.1.2.4 Tarifwahl

Die Ermittlung der entstehenden Kommunikationskosten sind in jedem Projekt ein wichtiger Bestandteil. Anders als beim leitungsvermittelten ISDN, verwendet man beim GPRS nicht die Verbindungsdauer, sondern das übertragene Datenvolumen als Grundlage für die Kostenermittlung. Man spricht daher von einer volumenorientierten Tarifierung, die für den Datentransport über die Strecke vom mobilen Endgerät bis zum Anschaltepunkt des Unternehmensnetzes an das GPRS-Netz aufkommt.

Für die Gebührenberechnung über die Funkstrecke bieten die Netzbetreiber unterschiedliche Tarife mit verschiedenen monatlichen Grundgebühren und Volumenentgelten an. Oft ist in der Grundgebühr schon ein bestimmtes Kontingent an Datenvolumen enthalten (Freivolumen). Die innerhalb des Freivolumens aufkommenden Einheiten sind - je Einheit -günstiger als die darüber hinaus gehenden. Nicht genutztes Freivolumen verfällt am Monatsende. Deshalb ist es sinnvoll, einen Tarif zu wählen, bei dem das Freivolumen möglichst gut mit dem tatsächlichen Volumen übereinstimmt. Die Wahl eines angemessenen Tarifes beeinflusst die Gesamtkosten der Lösung erheblich. Tabelle 2 zeigt eine beispielhafte Tarifberechnung mit fiktiven Tarifen.

2.1.2.5 Beispiel

- Tarif A: Normaltarif: kein Freivolumen, je Megabyte (MB) Datenvolumen werden 8 EUR berechnet, die Abrechnung geschieht je 10 Kilobyte (KByte) à 0,08 EUR, für die Datennutzung werden keine zusätzlichen Grundgebühren berechnet, so dass die Vertragsgrundgebühr nicht in die Kalkulation mit einfließt.

- Tarif B: spezieller Datentarif: 5 MB Freivolumen, die in der Grundgebühr von 13 EUR enthalten ist, je weiteres MB Datenvolumen werden 1,60 EUR berechnet, die Abrechnung erfolgt je angefangenes MB.
- Tarif C: spezieller Datentarif für Vielnutzer: 50 MB Freivolumen ist in der Grundgebühr von 35 EUR enthalten, je weiteres MB Datenvolumen werden 1,50 EUR berechnet, die Abrechnung erfolgt je angefangenes MB.

Hinweis: In der Regel wird die übertragene Datenmenge nach Verbindungsende auf feste Blocklängen (z.B. 1 KByte oder 10 KByte) aufgerundet. Häufige Verbindungsabbrüche können daher zu erhöhten Kommunikationskosten führen.

Tabelle 2	Beispielhafte Tarifberechnungen		
monatliches GPRS-Daten-volumen	Tarif A	Tarif B	Tarif C
51 MB	= 51 x 8 = 408 EUR	= 13 + 46 x 1,60 = 73,60 EUR	= 36,50 EUR
8,8 MB	= 8 x 8 + 82 x 0,08 = 70,56 EUR	= 13 + 4 x 1,60 = 19,40 EUR	= 35 EUR
1,1 MB	= 1 x 8 + 10 x 0,08 = 8,80 EUR	= 13 EUR	= 35 EUR

2.1.2.6 Wahl eines geeigneten Netzbetreibers

Mit der Entscheidung für einen Netzbetreiber legt sich das Unternehmen für einen längeren Zeitraum auf einen Partner fest. Die gesamte Kommunikation und die Funktionsfähigkeit der Gesamtlösung hängen unmittelbar von der Qualität und der

Unterstützung des Netzbetreibers ab. Der kostengünstigste Anbieter muss damit nicht zwangsweise der wirtschaftlichste für ein Projekt sein.

Verschiedene Kriterien beeinflussen die Wahl des geeigneten Partners:

Ein offensichtlicher, zum Teil jedoch überbewerteter Maßstab sind die angebotenen Tarifkonditionen. Diese betreffen sowohl die Kosten für die Kartenverträge als auch für den erforderlichen Anschluss an das Mobilfunknetz. Da die laufenden Gebühren die Gesamtkosten einer mobilen Lösung sehr beeinflussen, widmet man diesem Aspekt viel Aufmerksamkeit.

Neben diesen recht einfach quantifizierbaren Kriterien, bestehen weitere, etwas schwieriger zu bewertende Maßstäbe zur Beurteilung. Dazu zählen die so genannte

- Flächenversorgung und die Netzqualität,
- die Anzahl der verfügbaren Anschlussalternativen,
- Support und Quality of Service (QoS), sowie
- die Verfügbarkeit der Ansprechpartner im Bedarfsfall.

Hier ist es weitaus schwieriger, verlässliche Aussagen zu erhalten.

Persönliche Kontakte und eine über Jahre aufgebaute Vertrauensbasis sind mindestens ebenso gute Gründe für eine Entscheidung, wie geringfügig günstigere Tarife. Eine langjährige Erfahrung mit der Projektabwicklung im Geschäftskunden-Segment ist deshalb besonders wichtig.

2.1.3 Auswirkungen von GPRS und UMTS auf die Software-Entwicklung

Schon bei der Planung eines Projektes sollten die Auswirkungen der mobilen Datenkommunikation eingeschätzt werden können und das notwendige Wissen erworben werden.

2.1.3.1 Vergleich ISDN und GPRS

Ein Vergleich der Eigenschaften zweier häufig genutzter Kommunikationsmedien zeigt die Auswirkungen mobiler Datenkommunikation auf die Anwendungen. Stellvertretend wurden für das Festnetz ISDN und für den mobilen Einsatz GPRS gewählt, weil sie nicht nur jeweils für ihr Segment typische Eigenschaften aufweisen, sondern in heutigen Netzinfrastrukturen weit verbreitet sind. Tabelle 3 verdeutlicht die Unterschiede.

Tabelle 3	Vergleich zwischen ISDN und GPRS	
	ISDN	GPRS
Bandbreite	64 KBit/s, symmetrisch	Bis zu 28,8 KBit/s im Uplink, bis zu 57,6 KBit/s im Downlink
Netzwerkverzögerung	20 ms bis 50 ms	500 ms bis 1 500 ms
Übertragungsqualität	Exklusive Bandbreite	Abhängig von der Zellauslastung
Stabilität	Hoch	Variabel
Verbindungsaufbau	3 bis 5 Sekunden	5 bis 30 Sekunden

Tabelle 3 Fortsetzung	Vergleich zwischen ISDN und GPRS	
	ISDN	GPRS
Typische Fehler	Falsche Nummer, Leitung besetzt	Viele unterschiedliche Fehlermöglichkeiten
Sicherheit	Ende-zu-Ende-Verbindung	Funkverbindung und oft Übertragung durch das Internet

2.1.3.2 Asymmetrie und eingeschränkter Datendurchsatz

GPRS ist ein asymmetrischer Datendienst. Die Übertragungsrate in Senderichtung entspricht nicht der Übertragungsrate in Empfangsrichtung.

ISDN stellt den Anwendungen eine symmetrische Bandbreite von 64 KBit/s zur Verfügung. Beim GPRS werden zwar im Downlink (Übertragung vom Server zum Client) maximal 57,6 KBit/s erreicht, im Uplink (Übertragung vom Client zum Server) jedoch nur maximal 28,8 KBit/s (abhängig vom verwendeten Endgerät). Eine Anwendung benötigt damit doppelt solange für das Senden wie für das Empfangen derselben Datenmenge. Dadurch arbeiten Programme, die vornehmlich Daten vom Client zum Server senden, langsamer als gewohnt.

Da bei typischen Client-Server-Anwendungen im Allgemeinen mehr Daten empfangen als gesendet werden, ist die Bandbreite der Funkzellen zu Gunsten der Empfangsrichtung aufgeteilt worden. Die tatsächliche Übertragungsrate hängt von der Leistungsfähigkeit und Kanalaufteilung des Endgerätes sowie von der Qualität der Funkversorgung ab. Das Verhältnis zwischen Sende- und Empfangsrichtung wird häufig in den Datenblättern der Endgeräte angegeben (z.B. 1:4, 2:3). Ein

Kanal hat eine theoretische Bandbreite von 14,4 KBit/s (siehe 0). Die Übertragungsgeschwindigkeiten betragen in der

- Senderichtung: bis zu 28,8 KBit/s (2 Kanäle) und in der
- Empfangsrichtung: bis zu 57,6 KBit/s (4 Kanäle).

Diese Asymmetrie und die geringe Datenübertragungsrate erfordern sorgfältige Überlegungen, welche Daten tatsächlich übertragen werden sollen und welche möglicherweise lokal zwischengespeichert werden können. Ein unnötiger so genannter Protokoll-Overhead[7] macht sich besonders störend bemerkbar.

2.1.3.3 Netzwerkverzögerung

Unter einer Netzwerkverzögerung versteht man die Laufzeit eines Datenpaketes vom Client zum Server und wieder zurück. Sie wird auch als Round Trip Time (RTT) bezeichnet. Die Verzögerung beträgt bei GPRS zwischen 600 ms und 2 000 ms, im Durchschnitt etwa 700 ms. Damit liegen die Laufzeiten der Datenpakete bei einer mobilen Datenübertragung mit GPRS deutlich höher als im lokalen Netzwerk oder bei einem Zugriff über das Festnetz. Dies kann - je nach Anwendung und benutztem Transportprotokoll - einen deutlichen Einfluss auf den Datendurchsatz haben[8]. Ein Datenpaket benötigt über GPRS im Durchschnitt 700 ms, um vom Client zum Server und wieder zurück zu gelangen. Werden viele kleine Datenpakete übertragen, wie zum Beispiel in Emulationen[9], so sind die

---

7 Protokoll-Overhead: Prozesse, die der Verarbeitung von Daten dienen, aber nicht Bestandteile des Anwendungsprogramms oder der Daten selber sind.

8 Siehe hierzu den Beitrag „Mit GPRS ins Intranet – Optimierungsmaßnahmen für den praktischen Einsatz in Unternehmensnetzen“, Unterrichtsblätter, Nr. 11/2001,S. 626 ff.

9 Emulation: Nachahmung der Funktionen eines anderen Computers.

Verzögerungen spürbar. Auch Anmeldeprozeduren können sich schnell in die Länge ziehen, wenn viele Informationen in kleinen Datenpaketen miteinander ausgetauscht werden. Besonders negativ werden Anwendungen beeinflusst, die auf einem in dieser Weise „gesprächigen", d.h. interaktionsreichen, und ineffizienten Kommunikationsprotokoll basieren. Diese Anwendungen wurden meistens für den Einsatz im lokalen Netzwerk entwickelt und arbeiten im mobilen Umfeld unakzeptabel langsam. Als Beispiel sei hier das auf dem User Datagram Protocol (UDP) basierte NetBIOS- Protokoll genannt.

Die Übertragungsprotokolle sollten deshalb mit möglichst wenigen Einzelschritten auskommen und Daten möglichst kompakt versenden.

2.1.3.4 Schwankende Verbindungsqualität

Die Verbindungsqualität einer ISDN-Leitung ist normalerweise stabil und verschlechtert sich selten durch äußere Einflüsse. Bei einer mobilen Übertragung sieht die Situation aber anders aus: Eine überlastete Funkzelle, eine schlechte Funkversorgung, der so genannte Handover beim Wechsel des Endgerätes zwischen zwei Funkzellen, elektromagnetische Störungen und vieles mehr können die Übertragungsgeschwindigkeit bis zum Stillstand beeinflussen. Diese Situationen treten zwar nicht ständig auf, doch wenn sie auftreten, arbeitet die Anwendung oft nicht mehr oder die Session (Sitzung) bricht mit einer Fehlermeldung ab.

Anwendungen können auf solche Situationen reagieren, wenn sie speziell dafür entwickelt worden sind. Doch oft wird bei der Entwicklung das Kommunikationsmedium als vorhanden und stabil vorausgesetzt. Ein Fehler in einer LAN-Umgebung ist selten und auch ein Abbruch einer Einwahlverbindung tritt nicht häufig auf. Zudem liefern die Verbindungen eine gleich bleibende

Übertragungsqualität. Zeigen nun aber diese Verbindungen „Schwächen", so hat dies schwer wiegende Auswirkungen auf die Handhabung und die Geschwindigkeit der Anwendungen.

2.1.3.5 Verbindungsaufbauzeiten

Während beim ISDN der Verbindungsaufbau schnell vonstatten geht und meist innerhalb weniger Sekunden abgeschlossen ist, dauert dieser Vorgang bei GPRS meist deutlich länger. Dies liegt in der Komplexität des Systems begründet. Statt eines einfachen Aufbaus einer Einwahlverbindung sind beim Einbuchen eines GPRS-Endgeräts deutlich mehr Schritte notwendig.

Beim Aufbau einer Verbindung über GPRS werden verschiedene Stufen durchlaufen (Abbildung 6):

1. Verbindungsaufbau vom Betriebssystem zum Endgerät
2. Einbuchung ins GPRS-Netz (GPRS Attach)
3. Aufbau des PDP-Kontextes
4. Eventuelle Authentifizierung gegen RADIUS-Server[10]
5. Aufbau der Transmission Control Protocol (TCP-) Verbindung

Die dadurch entstehenden Verzögerungen können 2 bis 20 Sekunden betragen. Der Verbindungsaufbau kann den Ablauf einer Anwendung unterbrechen, falls sie von einer funktionierenden Verbindung abhängig ist. Lange Aufbauzeiten können

[10] RADIUS: Abk. Remote Authentication Dial-in User Service, ein entwickeltes Sicherheitsprotokoll, um unerlaubte externe Zugriffe auf Daten und Systeme zu verhindern.

den Anwender verunsichern, es sollte daher unbedingt ein Fortschrittsbalken angezeigt werden.

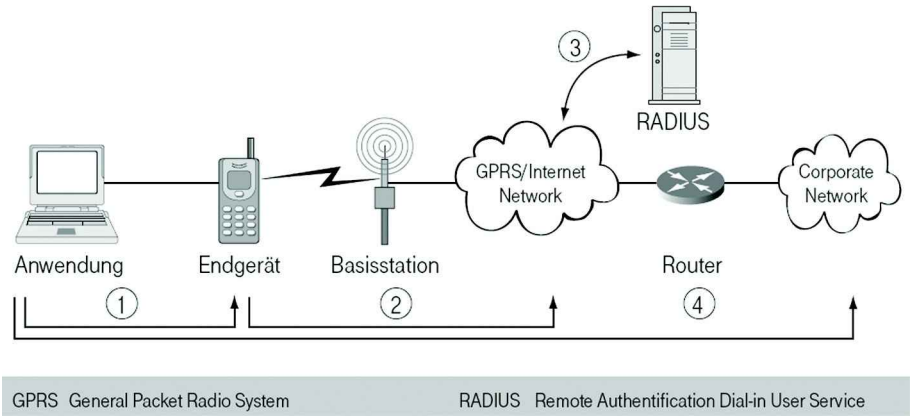


Abbildung 6: Aufbau einer TCP-Verbindung über GPRS

2.1.3.6 Handover

Ein Handover findet beim Wechsel des Mobilfunkteilnehmers zwischen zwei Funkzellen statt. Bei einem Handover bleibt der PDP-Kontext der aktuellen Sitzung erhalten. Es kann zu Verzögerungen beim Handover kommen (siehe Abschnitt 2.2.7.1). Das Endgerät bucht sich dabei nicht aus, stattdessen ist für eventuell mehrere Minuten keine Datenübertragung möglich. Dieses Phänomen tritt beim schnellen Wechsel zwischen mehreren Funkzellen auf (z.B. während einer Zugfahrt) und muss von der Anwendung berücksichtigt werden.

2.1.3.7 Fehlerszenarien

Beim Einsatz von GPRS sind - im Gegensatz zu ISDN - zahlreiche Fehlerquellen möglich:

- Vom Client zum Server und zum Funkmodem.
- Vom Funkmodem werden die Daten über die Luftschnittstelle an die nächste Funkzelle übertragen.
- Von der Funkzelle geht es durch das interne Netz des Mobilfunkanbieters und dann oft durch das Internet zu einem Router des Unternehmens.
- Von dort durch Firewalls und eventuell Virtual Private Network (VPN-) Konzentratoren zum Anwendungsserver.

Häufig wird zusätzlich ein Authentisierungs-Server eingesetzt, der bei jeder Einwahl Benutzernamen, Kennwort oder die Rufnummer überprüft, wodurch weitere Fehlerquellen hinzukommen.

In jeder der beschriebenen Übertragungsphasen (Abbildung 6) können Fehler auftreten, die erkannt und behandelt werden müssen. Reagierte die Anwendung bisher nur auf eine falsche Konfiguration oder einen Abbruch der Verbindung, so muss sie nun zum Beispiel

- die Verbindung zum Endgerät (z.B. mit Bluetooth-Übertragungstechnik),
- den Zustand des Endgerätes (z.B. eingebucht oder nicht),
- den Zustand des Netzwerkinterfaces (z.B. IP-Adresse zugewiesen oder nicht),
- die Erreichbarkeit des Zielnetzwerkes oder
- Unterbrechungen der Datenübertragung

kontrollieren und eventuelle Fehler selbstständig beheben, um dem Benutzer ein effektives Arbeiten zu ermöglichen.

2.1.3.8 Sicherheitsaspekte

2.1.3.8.1 Problemstellung

Mobile Endgeräte wie SmartPhones und PDAs haben sich inzwischen zu leistungsstarken Computern entwickelt, deren Rechenleistung und Speicherkapazität von mehreren hundert Megabyte mit dem PC-Standards vor fünf Jahren durchaus vergleichbar sind. Über immer breitbandigere mobile Datendienste können diese Endgeräte nahezu überall mit dem Internet oder einem Unternehmensnetz verbunden werden. Dadurch entstehen neue Gefahren für die einzelnen Unternehmensnetze. Da immer mehr sensible Daten auf diesen Endgeräten gespeichert werden, ergibt sich ein zusätzliches Risiko beispielsweise durch deren Verlust oder eventuellen Diebstahl.

Aufgrund des leistungsstarken und reichhaltigen Funktionsumfangs, der offenen Betriebssysteme sowie der zunehmenden Vernetzung über nahezu alle Kommunikationsmöglichkeiten sind SmartPhones und PDAs potenzielle Ziele für Angriffe jedweder Art.

Auf den Übertragungswegen durch die verschiedenen Netze werden die Daten häufig durch kaum geschützte Bereiche geführt. Insbesondere bei einem Zugang über das Internet ist die Datensicherheit ein wichtiger Aspekt. Doch nicht nur Daten müssen vor unbefugtem Zugriff geschützt werden, sondern auch die Clients und Server müssen vor Angriffen aus dem Internet gesichert werden. Die

Sicherheit einer „exklusiven" Einwahlverbindung, wie sie beispielsweise beim ISDN vorhanden ist, besteht nicht.

2.1.3.8.2 Schutzmaßnahmen

Praktisch alle Varianten von PDAs und Organizern lassen sich durch PINs oder Passwörter gegen unbefugten Zugriff absichern. Leider sind nicht alle vom Hersteller angebotenen Sicherheitsmechanismen so sicher, wie es wünschenswert wäre. Daher bietet sich je nach Schutzbedarf der zusätzliche Einsatz spezialisierter Sicherheitssoftware an, die eine leistungsstarke Pre-Boot-Authentisierung[11] und eine Verschlüsselung aller gespeicherter Daten in Echtzeit ermöglichen. Da alle Entschlüsselungsprozesse zum Booten des Betriebssystems von der gültigen Benutzerkennung sowie dem Passwort abgeleitet werden, können solche Lösungen bei Geräteverlust oder Diebstahl den Zugriff von Unbefugten auf Daten und Unternehmensnetze wirksam unterbinden.

Darüber hinaus empfiehlt sich wie im PC-Bereich der Einsatz einer Antiviren-Software, die das Gerät vor dem Eindringen schadhafter Programme wie Viren, Würmer und Trojaner wirkungsvoll schützt.

Solange keine speziellen Sicherheitstools installiert sind, sollten aber auf jeden Fall die vorhandenen Sicherheitsmechanismen genutzt werden. Alle Benutzer sollten sich aber über deren Wirkung und insbesondere deren Grenzen im Klaren sein.

2.1.3.8.3 Sensibilisierung der Benutzer

Die Nutzer von PDA oder SmartPhones sollten nicht nur über die Vorteile ihrer Geräte aufgeklärt sein, sondern auch über potenzielle Risiken und Probleme bei der

[11] Bei einer Pre-Boot-Authentisierung (PBA) erfolgt die Benutzerauthentisierung vor dem eigentlichen Start des Rechners und damit noch vor dem Laden des Betriebssystems in den Arbeitsspeicher.

Nutzung sowie über den Nutzen, aber auch die Grenzen der eingesetzten Sicherheitsmaßnahmen.

Ohne ein allgemeines Problembewusstsein der Benutzer, wie es im PC-Bereich bereits vorhanden ist, wird einer Gefährdung sensibler Daten und Systeme sowie einer ungehinderte Verbreitung von Handy-Viren nur schwer zu begegnen sein.

2.1.4 Einsatz spezieller Anpassungssoftware („Middleware")

Die Wiederverwendung von bewährten Komponenten kann die zeitnahe Fertigstellung von Software-Projekten unterstützen. Für die Entwicklung mobiler Anwendungen bieten Softwarehäuser verschiedene Lösungen an, die allgemein als „Middlewares" bezeichnet werden.

Nicht alle auf dem Markt erhältlichen Software-Produkte lassen sich für den mobilen Einsatz anpassen. Viele Lösungen bestehen bereits seit vielen Jahren oder Jahrzehnten in den Unternehmen und können nicht mehr geändert werden. Darüber hinaus gibt es viele Standardprodukte, die von den Herstellern nur zögerlich oder gar nicht für die mobile Übertragung optimiert werden. Schließlich steht auch bei der Entwicklung einer neuen Lösung nicht die Kommunikation im Mittelpunkt, sondern sie ist nur einer von vielen Bestandteilen.

Damit auch in diesen Fällen erfolgreiche mobile Projekte realisiert werden können, haben verschiedene Firmen Optimierungslösungen oder Middlewares für die mobile Datenkommunikation entwickelt. Diese Lösungen eignen sich, - je nach Produkt - auch als Kommunikationsplattform für die Entwicklung einer neuen Lösung. Was sich hinter dem Begriff Middleware verbirgt und welche Eigenschaften für den Software-Entwickler wichtig sind, wird nachfolgend erläutert.

2.1.4.1 Funktionsweise

Eine Middleware ist eine Software, die sich „nahtlos" in die Kommunikationsschichten des OSI-Referenzmodells[12] einfügt. Sie erweitert die Kommunikation um eine zusätzliche Ebene. Diese - für die Anwendungsschicht transparenten - Ebene adaptiert[13] Daten und Protokollabläufe für die mobile Datenübermittlung.

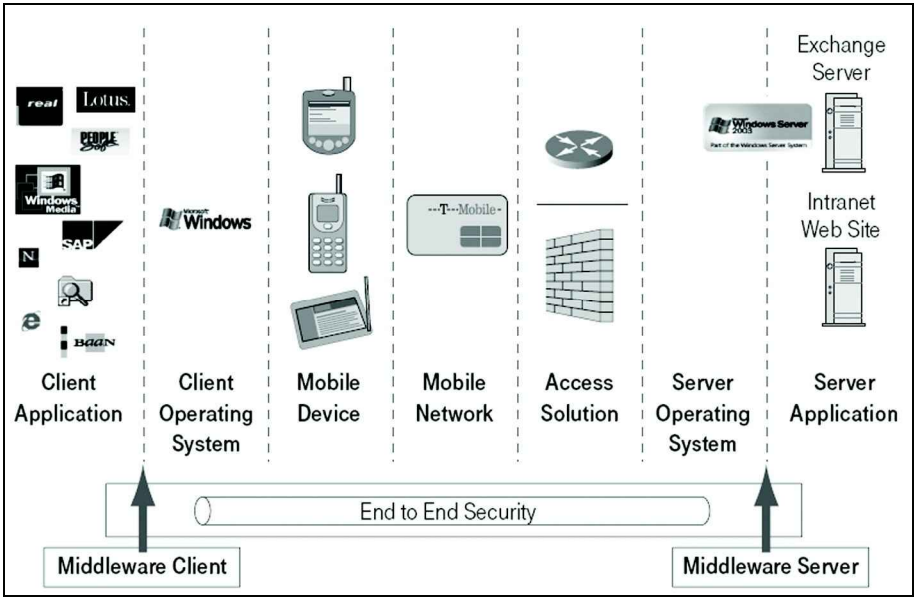


Abbildung 7: Architektur einer Middleware-Lösung

Die Systemarchitektur erweitert sich beim Einsatz einer Middleware um zwei zusätzliche Komponenten:

---

[12] OSI: Abk.: Open System for Interconnection; ein Gedankenmodell, das als Architekturmodell für die Zusammenarbeit von Endgeräten verschiedener Hersteller über beliebige Netze im Rechnerverbund bereitsteht.

[13] adaptieren: anpassen, für einen bestimmten Zweck herrichten.

- dem Middleware-Client, der in die Datenkommunikation auf dem Endgerät eingreift und
- dem Middleware-Server, der den Datenstrom im Zielnetzwerk bearbeitet (Abbildung 7).

2.1.4.2 Anforderungen und Leistungsmerkmale

Aus Sicht des Software-Entwicklers ergeben sich andere Anforderungen an eine Middleware-Lösung als aus der Sicht eines Netzwerk-Administrators. Folgende Leistungsmerkmale sind für die Verwendung einer solchen Lösung als Entwicklungsplattform von besonderer Bedeutung:

- Die Middleware muss zur leichten Einbindung in die Entwicklung ein geeignetes Software Development Kit (SDK)[14] und eine einfache Programmierschnittstelle (Application Programming Interface = API) besitzen. Unter anderem müssen verschiedene Bestandteile mit Hilfe der Software gesteuert werden können, dazu gehören die Konfiguration und die Steuerung sowie Überwachung des Verbindungsstatus.
- Beim Einsatz verschiedener Kommunikationsmedien und zur Stabilisierung der Funkverbindung sollte eine Middleware einen automatisierten Verbindungsaufbau ermöglichen (Verbindungsmanagement). Sie sollte darüber hinaus neben dem GPRS auch Zugänge über WLAN, Einwahlverbindungen oder LAN unterstützen und selbstständig das geeignete Verbindungsmedium wählen können.

[14] Software Development Kit: dt. "Werkzeug für die Software-Entwicklung", allgemein Bezeichnung für die Gesamtheit der Informationen, Dokumentationen, Beispiele und Werkzeuge, die in der Software-Entwicklung eingesetzt werden.

- Die Daten sollten von dem Produkt für den mobilen Transfer aufbereitet werden (Protokoll-Optimierung). Auch sind ein spezielles mobiles Übertragungsprotokoll und eine Kompression der Daten erforderlich. Abbrüche einer Verbindung oder Verzögerungen sind von der Middleware zu regeln. Die Middleware sollte sich transparent in die Datenübertragung einbinden lassen und zum Beispiel TCP-Verbindungen ohne Anpassungen der Anwendung optimieren. Bietet die Middleware spezielle Übertragungsmechanismen für Daten (z.B. Dateien) an, so kann bei der Software-Entwicklung eventuell auf die Implementation einer eigenen TCP-Kommunikation verzichtet werden.
- Zur Sicherung der Übermittlung sollten bekannte Verschlüsselungsverfahren (z.B. RSA[15]) unterstützt werden (Sicherheitsfunktionen). Beim Einsatz von IPSec-Tunneln sollte die Middleware eine Integration mit VPN-Clients ermöglichen.

2.1.5 Besonderheiten mobiler Browser

Viele Web-Applikationen nutzen Informationen über den genutzten Browser, um die Informationsinhalte jeweils optimal aufzubereiten. Dies ist ganz besonders wichtig, wenn die Applikation mit unterschiedliche Gerätetypen genutzt werden sollen. So müssen Inhalte für einen PDA aufgrund der geringen Display-Grösse beispielsweise anders dargestellt werden als auf einem Notebook.

Der wichtigste Aspekt ist die Benutzerfreundlichkeit oder Usibility. Die Auflösung des Pocket Internet Explorer auf einem PDA beträgt beispielsweise 240 x 320 Bildpunkte. Die tatsächlich nutzbare Auflösung ist jedoch geringer, da bestimmte Bereiche auf der Anzeige

[15] RSA: Abk.: Rivest Shamir, Adlemann; ein asymmetrisches Verschlüsselungsverfahren, das nach seinen Erfindern benannt wurde (siehe hierzu auch den Beitrag „Grundlagen der Kryptographie“ in dieser Ausgabe).

für die Applikation nicht nutzbar sind und z.B. für die Menüleiste am unteren Rand reserviert sind.

Sobald die Inhalte mehr als 240 Bildpunkte in der Vertikalen oder mehr als 320 Bildpunkte in der Horizontalen belegen, erscheinen automatisch entsprechende Scroll-Bars und die Benutzerfreundlichkeit wird eingeschränkt ([4]).

Aufgrund der Vielzahl unterschiedlicher Geräte- und Browser-Typen mit jeweils sehr unterschiedlichen Eigenschaften ist es sehr schwierig, die jeweils benötigten Informationen zu finden bzw. aktuell zu halten. Konkrete Beispiele und aktuelle Informationen sind unter www.webcab.de zu finden.

2.2 Grundlagen GPRS, UMTS und HSDA

2.2.1 Allgemeine Eigenschaften von GPRS

Der GPRS-Dienst ist ein paketvermittelter mobiler GSM-Datendienst, der für einen Anschluss an IP-basierende Festnetze mit burstartigem LAN-Verkehr optimiert ist.

GPRS basiert durchgängig auf IP und stellt demnach ein mobiles IP-Netz dar. Als paketorientierter Datendienst erlaubt er eine volumenabhängige Tarifierung. Der Kunde kann somit ständig online sein, bezahlt aber nur für die übertragenen Datenmengen. Im Vergleich zu den bisherigen GSM-Datendiensten, dem Short Message Service (SMS) und dem leitungsvermittelten Dienst BS26 (Bearer Service), bietet GPRS wesentlich höhere Bandbreiten. Eine der wichtigsten Neuerungen bei GPRS stellt die Luftschnittstelle dar. Sie kann im Gegensatz zur klassischen Luftschnittstelle bei GSM einer Mobilstation sehr schnell Kanalressourcen zur Verfügung stellen oder sie ihr wieder entziehen. Es wird nur dann eine Luftschnittstellenkapazität blockiert, wenn auch wirklich Datenpakete zur Übertragung anstehen.

GPRS zeichnet sich insbesondere durch folgende Eigenschaften aus:

- Übertragungsbandbreite zwischen 25 kbit/s und 50 kbit/s
- paketorientierte Datenübertragung und damit effiziente Nutzung der knappen Übertragungskapazitäten insbesondere an der Luftschnittstelle;
- Multislotzugriff: Eine Mobilstation kann gleichzeitig auf mehrere Kanäle zugreifen (maximal acht Kanäle);
- asymmetrische Übertragung
- volumenabhängige Tarifierung;

- parallele Nutzung von Sprache und Datenübertragung in Abhängigkeit von zukünftigen Endgeräteklassen;
- Interworking zu IP-Netzen;
- Nutzung von PPP[16]-Standardeinwahlsoftware (z. B.: DFÜ-Netzwerk) auf der Client-Seite.

Der GSM-Standard definiert für GPRS drei verschiedene Endgeräteklassen, die sich im Wesentlichen darin unterscheiden, inwiefern der Sprachdienst und der Datendienst GPRS gleichzeitig genutzt werden können.

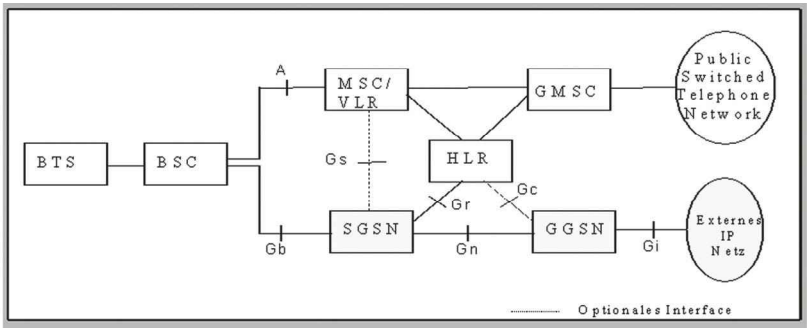
- Klasse A: Sprache und GPRS-Datentransfer ist gleichzeitig möglich.
- Klasse B: Es ist nur Sprache oder GPRS-Datentransfer möglich, aber Erreichbarkeit des nicht aktiven Dienstes.
- Klasse C: Es ist nur Sprache oder GPRS-Datentransfer und keine Erreichbarkeit des nicht aktiven Dienstes möglich.

2.2.2 Netzarchitektur GPRS

Mit der Einführung von GPRS[17] wurde die bestehende GSM-Netzarchitektur um zwei neue logische Paketvermittlungsknoten, dem Serving GPRS Support Node (SGSN) sowie dem Gateway GPRS Support Node (GGSN), erweitert (Abbildung 8).

16 PPP: Point To Point Protocol, RFC 1661

17 Siehe hierzu den Beitrag „Mit GPRS ins Intranet – Das Produkt LAN to LAN GPRS Access“, Unterrichtsblätter Nr. 3/2001, S. 168-174.



A	Schnittstellenbezeichnung	Gr	Schnittstellenbezeichnung
BSC	Base Station Controller	Gs	Schnittstellenbezeichnung
BTS	Base Tranceiver Station	HLR	Home Location Register
Gb	Schnittstellenbezeichnung	IP	Internet Protocol
Gc	Schnittstellenbezeichnung	MSC	Mobile Switching Center
GGSN	Gateway GPRS Support Node	PSTN	Public Switched Telephone Network
Gi	Schnittstellenbezeichnung	SGSN	Serving GPRS Support Node
Gn	Schnittstellenbezeichnung	VLR	Visitor Location Register
GMSC	Gateway Mobile Switching Center		

Abbildung 8: Erweiterte Netzarchitektur von GSM durch GPRS

Der funktechnische Teil der GSM-Architektur, bestehend aus den Basisstationen (Base Transceiver Station = BTS) und den Steuereinheiten (Base Station Controller = BSC), bleibt erhalten. Der SGSN ist über das so genannte Gb-Interface über eine oder mehrere BSC mit dem funktechnischen Teil des GSM-Netzes verbunden. Er besitzt eine SS7-Anbindung für die Kommunikation mit der zentralen Teilnehmerdatenbank des GSM-Netzes, dem Home Location Register (HLR), bzw. mit der mobilen Vermittlungsstelle für die leitungsvermittelten Dienste, der Mobile Switching Center (MSC), sowie eine IP-Anbindung für die Kommunikation mit den anderen GPRS Support Nodes.

Die Aufgaben dieses Knotens entsprechen größtenteils den Aufgaben der MSC, wie z.B. Authentifizieren der Mobilstationen und Durchführen des Mobility Management. Er besitzt eine integrierte Datenbasis, in der die GPRS Subscription

und Mobility-Management-Informationen über die eingebuchten Mobilstationen temporär gespeichert werden.

Eine weitere Aufgabe dieses Knotens besteht in der Verschlüsselung der übertragenen Daten und der Erfassung von Abrechnungsdaten. Der GGSN bildet die interne GSM-Adresse (International Mobile Subscriber Identitiy = IMSI[18]) auf eine IP-Adresse ab. Diese IP-Adresse kann fest oder temporär einer IMSI zugeordnet werden, und zwar entweder durch den internen DHCP-(Dynamic Host Configuration Protocol-)Server im GGSN selber oder durch einen externen RADIUS[19]- bzw. DHCP-Server. Meldet sich eine Mobilstation für den GPRS-Dienst an, wird dementsprechend eine temporäre oder fest der IMSI zugeordnete IP-Adresse aktiviert. Nach der Aktivierung können ankommende Pakete der Mobilstation über SGSN – BSC-BTS zugestellt und empfangen werden.

Von zentraler Bedeutung für die Funktionsweise eines GPRS-Netzes ist der Domain Name Service (DNS). Die Aufgabe eines DNS ist es allgemein, einen Domain

[18] IMSI: Abk. International Mobile Subscriber Identity, dt. Internationale Mobilfunk-Teilnehmerkennung. Im terrestrischen Mobilfunksystem GSM die internationale, höchstens fünfzehnstellige Kennung des GSM-Teilnehmers, die auf der Chipkarte (Subscriber Identity Module = SIM) des Mobilfunkgeräts gespeichert ist und dem Teilnehmer nicht bekannt ist. Der Zusammenhang zwischen der Kennung IMSI und der GSM-Rufnummer (Mobile Station ISDN Number = MSISDN) ist nur dem Netz (Home Location Register = HLR) bekannt. Hat der Teilnehmer mehrere GSM-Dienste (z.B. Telefon-, Telefax- und Datendienst) über eine Chipkarte (SIM) abonniert, so erhält er für jeden Dienst eine eigene MSISDN.

[19] RADIUS: Abk. Remote Authentication Dial-in User Service. Für Remote-Access-Anwendungen entwickeltes Sicherheitsprotokoll (RFC 2138, 2139), um unerlaubte externe Zugriffe auf Daten und Systeme zu verhindern. RADIUS funktioniert nach dem Client-Server-Konzept und legt die Kooperation zwischen einem AAA-Server (Authentification, Authorization and Accounting Server) und einem Network Access Server (NAS) fest. In diesem Konzept kann der AAA-Server als RADIUS-Server angesehen werden, in dem sämtliche Informationen über Remote-Benutzer zur Verfügung stehen. Der RADIUS-Client stellt ein Funktionsmodul dar, das auf dem NAS installiert wird.

Namen in eine IP-Adresse zu übersetzen. Zur Adressierung externer IP-Netze (z.B. Internet oder Unternehmensnetze) wird innerhalb des GPRS-Netzes jeweils ein Access Point Name (APN) verwendet.

Der APN ist – vereinfacht ausgedrückt – ein Domain-Name des externen Netzes nach RFC 1035 (Request For Comments[20]). Er hat eine Länge von bis zu 63 alphanumerischen Zeichen und wird nur innerhalb des GPRS-Backbones benutzt. Er dient zum einen dem SGSN zur Auswahl des richtigen GGSN und zum anderen dem GGSN zur Auswahl des richtigen externen Zielnetzes. Die Auflösung des APN in die IP-Adresse des GGSN wird durch eine Anfrage des SGSN am Domain Name Server (DNS) vorgenommen.

Vor dem Senden von IP-Paketen muss die Mobilstation (MS) eine GPRS-Einbuchung (GPRS Attach) und eine PDP[21]-Kontextaktivierung (PDP Context Activation) durchführen.

Die GPRS-Einbuchung setzt das Netz darüber in Kenntnis, dass die MS im Netz vorhanden ist. Die Einbuchung wird durch die MS beim SGSN vorgenommen. Bei der GPRS-Einbuchung gibt die MS ihre Identität bekannt (IMSI oder Packet TMSI[22]) und gibt an, ob die Einbuchung für Paketvermittlung (PS Attach) oder die

---

20 Request for Comments: Sammlung von Empfehlungen, Artikeln und Standards (RFC-Standards), in denen netzrelevante Konventionen und allgemeine Informationen zum Internet festgehalten sind. Als RFC sind auch die Anregungen und Verbesserungsvorschläge bezeichnet, die die Teilnehmer des Internets beim so genannten RFC-Editor einreichen.

21 PDP: Abk. Packet Data Protocol. Allgemeiner Begriff für ein Protokoll, das Daten in diskreten Einheiten bzw. Paketen überträgt. Beispiele sind IPv4 oder X.25. GPRS von T-Mobile unterstützt derzeit den PDP-Typ IPv4.

22 TMSI: Abk. Temporary Mobile Subscriber Identity, dt. Temporäre Teilnehmerkennung. Im GSM die von der Besucherdatei (Visitor Location Register VLR) für die einzelne Mobilfunkverbindung vergebene Kennung mit Funktionen im Rahmen der GSM-Sicherheitsmechanismen.

kombinierte Einbuchung für Paketvermittlung und Leitungsvermittlung / IMSI (PS und CS/IMSI Attach) angefordert wird.

Zum Senden und Empfangen von GPRS-Daten führt die MS nach der GPRS-Einbuchung eine PDP- Kontext Aktivierung aus. Die PDP- Kontext Aktivierung macht die MS dem betreffenden GGSN bekannt, woraufhin Datenübertragungen über den GGSN in externe Netze möglich sind. Die Adressierung des externen Zielnetzes wird von der MS im Rahmen der Kontextaktivierung unter Angabe des APN vorgenommen. Sofern die MS keinen APN angibt, wird die Verbindung mit Hilfe eines „Default-APN" aufgebaut, der im SGSN fest hinterlegt ist. In der Regel verbirgt sich hinter diesem „Default-APN" das Internet.

2.2.3 Luftschnittstelle GPRS

Der GPRS zeichnet sich insbesondere durch ein neues Multiplexverfahren an der GSM-Luftschnittstelle aus. Während die bisherigen GSM-Dienste (Sprache, Daten, Fax) nach dem Prinzip der Leitungsvermittlung arbeiten, wobei sich jeder Verkehrskanal aus fest zugewiesenen, periodischen Zeitschlitzen (Time-Slots) zusammensetzt, arbeitet GPRS nach dem Prinzip der Paketvermittlung.

Hierbei erhält ein GPRS-Kanal nur dann Übertragungsressourcen zugewiesen, wenn auch tatsächlich Daten zur Übertragung anstehen. Die knappen Frequenzressourcen an der Luftschnittstelle werden dadurch effizienter genutzt.

Die Ausführung der Luftschnittstelle von GPRS basiert auf der Idee, kleine Einheiten eines Verkehrskanals bei Bedarf einer Mobilstation zuzuweisen. Die Zuweisung von Uplink und Downlink kann unabhängig durchgeführt werden, um

eine hohe Effizienz oder Auslastung der vorhandenen Ressourcen zu gewährleisten.

Als Basis dienen Paketkanäle, so genannte Packet Data Traffic Channels (PDTCH), die aus Sicht der Kanalstruktur klassischen Traffic-Channels (TCH) entsprechen, die für die Realisierung eines Sprachkanals benutzt werden. Das Netz kann beliebig viele solcher Paketkanäle dynamisch auf allen verfügbaren Frequenzen anbieten. Einer Mobilstation können allerdings nur Paketkanäle innerhalb eines Trägers bzw. Frequenz zugewiesen werden.

Die Multislotfähigkeit der Mobilstation bestimmt die maximale Anzahl von Paketkanälen, auf die gleichzeitig zugegriffen werden kann (maximal acht Kanäle). Die kleinste zu vergebende Einheit auf dem Paketkanal ist ein Block, der sich aus vier Bursts zusammensetzt. Diese Blockstruktur besteht aus dem Uplink und dem Downlink und entspricht der Struktur, wie sie bisher für die Signalisierungskanäle in GSM definiert ist.

Der Zugriff auf den Uplink-Kanal wird mit Hilfe eines Packet Random Access Channel (PRACH) eingeleitet. Mit dem Senden eines Random Access Bursts fordert die Mobilstation das Netz auf, Kanalressourcen zur Verfügung zu stellen.

Das Netz antwortet mit der Zuweisung von einem Paketkanal, einem Uplink State Flag (USF) sowie einer temporären Adresse, der so genannten Temporary Flow Identity (TFI). Das Uplink State Flag ist eine Kennung für die Mobilstation, die vom Netz als Steuerung für den Uplinkzugriff benutzt wird; die TFI wird zur Identifizierung auf dem Downlink benötigt. Mehrere solcher Paketkanäle mit jeweils unterschiedlichen USF+TFI können zugewiesen werden.

Sobald die Mobilstation ein USF+ TFI zugewiesen bekommt, verfolgt sie jeden Block auf dem Downlink. In jedem Downlinkblock ist ein Uplink State Flag

enthalten. Findet eine Mobilstation ihr USF vor, bedeutet dies, dass der darauf folgende Uplink-Block von ihr genutzt werden darf. Das Netz könnte nun auf dem Downlink immer das gleiche USF setzen und somit einer Mobilstation ununterbrochen Kanalkapazität zuweisen. Im anderen Extremfall kann das Netz der Reihe nach alle verfügbaren USF durchgehen, d. h. alle aktiven Mobilstationen bekommen jeweils immer nur einen Block zugeteilt und müssen danach wieder warten, bis sie an der Reihe sind.

Wenn der Uplink von keiner Mobilstation als Datenkanal genutzt wird, setzt das Netz das Uplink State Flag auf FREI. Mobilstationen dürfen dann einen Random Access Burst im nächsten Block schicken, falls sie Daten übertragen wollen.

Im Downlink kann das Netz beliebig die Blöcke mit den anstehenden Daten senden, da alle Mobilstationen, die USF+TFI zugewiesen bekommen haben, jeden Block auswerten müssen. Aus Sicht der Mobilstation kann die Auswertung im Downlink in drei Stufen aufgeteilt werden. Die Mobilstation wertet zunächst das USF aus, das im Datenblock enthalten ist, um zu klären, ob es den nächsten Uplink- Block nutzen darf.

In einem zweiten Schritt wird die Temporary Flow Identity ausgewertet, um zu entscheiden, ob der Block für die eigene Adresse (TFI) bestimmt war. Ist dies der Fall, wird im letzten Schritt der Block zur Weiterverarbeitung weitergereicht. Entdeckt die Mobilstation nicht die eigene TFI, verwirft sie das Paket.

Jeder Paketkanal arbeitet völlig unabhängig voneinander. Eine Mobilstation kann demnach auf Paketkanal A das USF X und auf Paketkanal B das USF Y zugewiesen bekommen. Der beschriebene Kanalzugangsmechanismus ist in Abbildung 9 verdeutlicht.

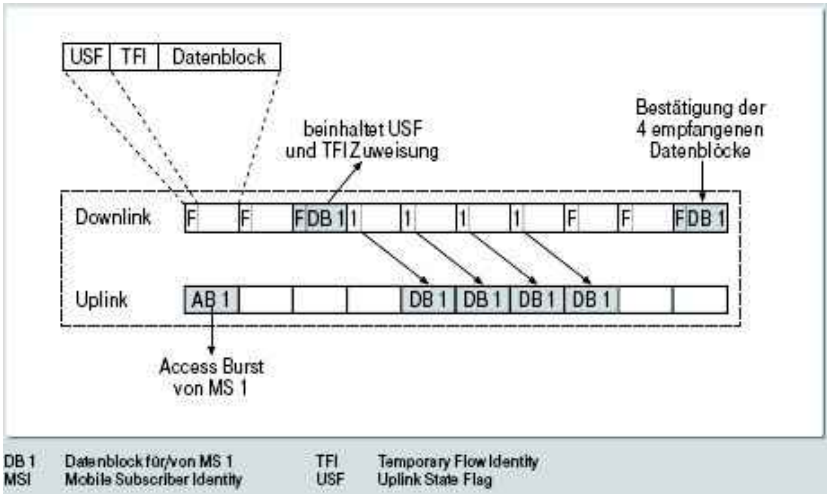


Abbildung 9: Beispiel einer Kanalvergabe mit einer aktiven Mobilstation

Sie beschreibt ein Szenario mit einer aktiven Mobilstation, die vier Datenblöcke überträgt.

Das Beispiel in Abbildung 10 zeigt drei aktive Mobilstationen mit sehr unterschiedlichem Datenverkehr: Mobilstationen 1 und 2 senden hauptsächlich Daten, während Mobilstation 3 nur Daten empfängt.

Der Uplink-Kanal wird Mobilstationen 1 und 2 jeweils in Zweierblöcken zugeteilt. Mobilstation 3 bekommt insgesamt nur einen Block, um Bestätigungen oder Wiederholungsaufforderungen für nicht korrekt empfangene Blöcke senden zu können. Auf Blockbasis existiert ein Quittierungsmechanismus, mit dem die Empfängerseite die korrekt empfangenen bzw. fehlerhaft empfangenen Blöcke der Gegenseite anzeigen kann (siehe RLC-Protokoll GSM03.64, GSM04.08).

Der GSM-Standard GPRS beschreibt nur die Multiplexing-Technik, die für GPRS entwickelt wurde. Die Strategie, mit der das Netz die vorhandenen Blöcke auf die

interessierten Mobilstationen verteilt, ist nicht spezifiziert. Sie wird herstellerspezifisch implementiert. Basis für die Strategie bilden die Quality of Service-(QoS-) Werte der aktiven Mobilstationen und deren Multislotfähigkeit.

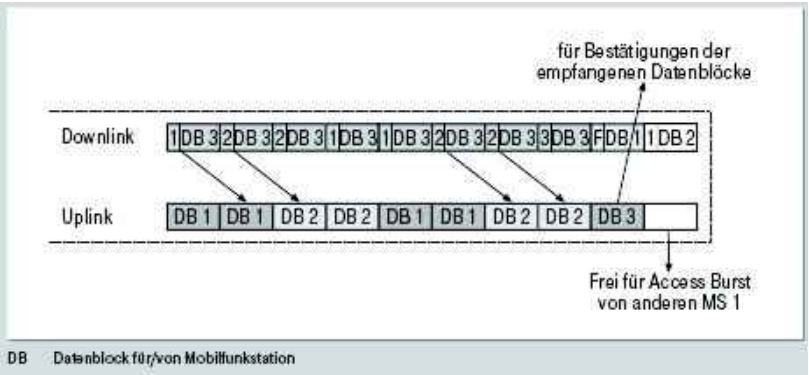


Abbildung 10: Beispiel einer Kanalvergabe mit drei aktiven Mobilstationen

2.2.4 Grundlagen UMTS

UMTS (Universal Mobile Telecommunication System) ist ein internationaler Standard der dritten Mobilfunkgeneration, der vom internationalen Standardisierungsgremium 3GPP (Third Generation Partnership Project) verabschiedet wurde.

UMTS ist dabei eine Weiterentwicklung des so genannten 2,5G Datendienstes GPRS mit einer Bandbreite, die je nach Funkfeldbedingungen um den Faktor 4 bis 12 höher liegt als bei GPRS und einer deutlich kürzen Übertragungsverzögerung von ca. 300 Millisekunden.

Auf Grund dieser Eigenschaften eignet sich UMTS nicht nur zum Herunterladen großer Datenmengen (z.B. über FTP, http oder Email), sondern erlaubt auch die

Nutzung multimedialer Anwendungen wie beispielsweise Streaming oder Online-Spiele.

Wie GPRS bietet UMTS ebenfalls einen asymmetrischen Datendienst mit unterschiedlichen Übertragungsraten für die beiden Übertragungsrichtungen Uplink und Downlink. Zu Beginn liegt die Datenrate bei 128/384 KBits (Uplink/Downlink). Wie bei GPRS gibt es jedoch keinen garantierten Datendurchsatz.

Die tatsächliche Bandbreite hängt auch bei diesem Dienst von der aktuellen Anzahl gleichzeitiger Nutzer in der gleichen Zelle sowie vom Abstand des Nutzers zur jeweiligen Basisstation (Node B) ab.

Im Gegensatz zu GPRS ist die Flächenversorgung auf städtische Bereiche begrenzt. Um dennoch eine großflächige Versorgung zu erzielen, ist eine enge Kopplung zwischen UMTS und GPRS nötig. Innerhalb eines mit UMTS versorgten Gebietes bucht sich die Mobilstation bevorzugt in UMTS ein.

Sobald sie das UMTS versorgte Gebiet verlässt, wechselt die Mobilstation automatisch nach GPRS, ohne dass die Verbindung neu aufgesetzt werden muss. Diese Grundeinstellung lässt sich jedoch auf den Geräten ändern.

Ein UMTS-Netz besteht aus zwei Hauptkomponenten:

- das paketvermittelte Kernnetz sowie
- der Funktechnische Teil, das UMTS Terrestrial Radio Access Network (UTRAN)

Das Kernnetz ist identisch mit dem in Abschnitt 2.2.2 beschriebenen Netzarchitektur von GPRS und besteht aus den beiden Komponenten SGSN und GGSN. Durch die Mitbenutzung der vorhandenen Kernnetzkomponenten von GPRS

ist eine enge technische Kopplung zwischen GPRS und UMTS gewährleistet. Diese Kopplung umfasst insbesondere:

- Die gleiche SIM-Karte kann zur Authentisierung und Netzeinbuchung genutzt werden.
- Die Einwahlprozedur ist identisch (siehe Abschnitt 2.2.6)
- Der Nutzer kann auf die gleichen Zielnetze und Dienste zugreifen.
- Dual-Mode-Geräte können genutzt werden und 2G/3G Interworking wird unterstützt.

Die neue Funkschnittstelle UTRAN (UMTS Terrestrial Radio Access Network) nutzt als Modulationsverfahren die "Spread Spectrum"-Technologie, die zuvor im militärischen Bereich seit vielen Jahren zum Einsatz kam. Sie zeichnet sich daher durch eine hohe Unempfindlichkeit gegen Störsignale sowie eine hohe Abhörsicherheit aus.

Weitere technische Informationen sind u.a. in [27] zu finden.

2.2.5 Grundlagen HSDPA

High Speed Data Packet Access (HSDPA) ist die erste Weiterentwicklung von UMTS. Hauptziel von HSDPA ist die Erhöhung der Spektraleffizienz für die Downlink-Richtung. Darunter versteht man eine Erhöhung des Datendurchsatzes bei gleich bleibender Frequenzbelegung. Diese Verbesserung wird durch den Einsatz neuer Modulationsverfahren auf der Luftschnittstelle erzielt.

Für den Nutzer bedeutet dies neben einer signifikanten Erhöhung des Durchsatzes zudem eine deutliche Verringerung der Übertragungsverzögerung (Delay).

Während die maximale Datenrate bei UMTS auf 384 KBit/s begrenzt ist, erzielt man mit HSDPA Download-Raten von bis zu 1,8 MBit/s. Damit kommt man in den Bereich von DSL-Geschwindigkeiten im Festnetz. In einer weiteren Ausbaustufe sind sogar Übertragungsraten von bis zu 3,6 MBit/s und mehr geplant.

In der Uplink-Richtung wird weiterhin das Übertragungsverfahren von UMTS genutzt, so dass in dieser Richtung die Bandbreite nach wie vor auf maximal 384 KBit/s begrenzt ist.

Da HSDPA nur lediglich eine Weiterentwicklung von UMTS ist, kommen im Kernnetz die gleichen Techniken und Einwahlprozeduren wie bei UMTS und GPRS zum Einsatz. HSDPA ist somit vollständig rückwärtskompatibel.

Ein HSDPA-Kanal ist eine Ressource, die von mehreren Nutzern geteilt wird, und hat folgende Eigenschaften:

- Adaptive Modulation und Kodierung:

Herkömmliche UMTS-Netzen passen die Übertragungsleistung an die jeweiligen Funkfeldbedingungen einer Mobilstation an, um die Übertragungs- sowie die Fehlerrate möglichst konstant zu halten. Bei HSDPA bleibt hingegen die Übertragungsleistung konstant und das Modulationsverfahren wird auf die jeweiligen Funkfeldbedingungen angepasst, um jeweils eine maximale Datenrate zu erzielen. Somit ergibt sich, dass Nutzer, die sich in der Nähe der Basisstation (Node B) befinden, eine sehr hohe Datenrate erzielen können, und das die Datenrate mit zunehmender Entfernung abnimmt (Abbildung 11).

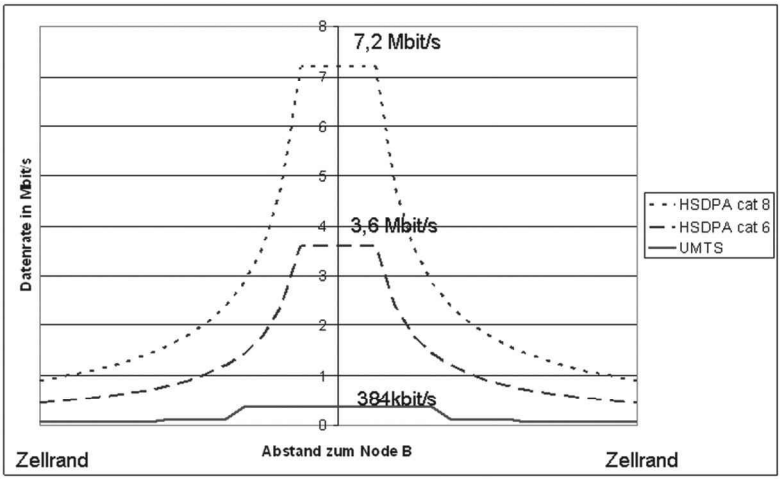


Abbildung 11: HSDPA Durchsatzraten in Abhängigkeit von der Entfernung zur Basisstation

- Ressourcenzuteilung durch die Basisstation (Fair and fast NodeB scheduling):

Der HSDPA-Kanal ist eine Ressource, die auf mehrere Nutzer verteilt werden muss. Die Zuteilungsinstanz, der HSDPA scheduler, ist Teil der Basisstation (Node B). Diese Instanz entscheidet über das Zuteilungsverfahren, wenn mehrere Mobilstationen gleichzeitig eingebucht sind. Gewöhnlich wird ein Verfahren genutzt, das darauf abzielt, den Summendatendurchsatz am Node B unter Berücksichtigung eines „Fairness-Faktors" zu maximieren. Für den einzelnen Nutzer kann dies bedeuten, dass seine Datenrate variiert, auch wenn er den Abstand zur Basisstation beibehält.

2.2.6 Protokoll-Architektur und Verbindungsaufbau

Die nachfolgend beschriebene Protokollarchitektur und Dial-In Prozedur gilt gleichermaßen für GPRS, UMTS und HSDPA. Weitere Einzelheiten sind in [1] zu finden.

2.2.6.1 Dial-IN Prozedur bei leitungsvermittelten Zugangsdiensten

Die wichtigsten Protokolle bei der Einwahl über GPRS, UMTS oder HSDPA in externe IP-Netze (z.B. IP VPNs) sind PPP (Point To Point Protocol, RFC 1661) und RADIUS (Remote Access Dial In User Service, RFC 2138, RCF 2868).

PPP wird gewöhnlich über leitungsvermittelte Zugangsnetze wie z.B. ISDN oder das analoge Modemverbindungen genutzt, um eine Einwahl in IP-Netze zu realisieren. Das Protokoll gehört zur Protokollschicht 2 des OSI (Open Systems Interconnection) Referenzmodells (Abbildung 38) und beinhaltet u.a. die Funktionen Authentisierung, Verbindungssteuerung und IP-Adressmanagement.

Der Verbindungsaufbau wird von einem PPP-Client initiiert, der üblicherweise Bestandteil des Betriebssystems (z.B. Windows) auf der Client-Plattform (z.B. Laptop) ist. Zur Authentisierung beim Einwahlserver (RAS: Remote Access Server) können wahlweise die Verfahren PAP (Password Authentication Protocol, RFC 1334) oder CHAP (Challenge Handshake Authentication Protocol, RFC 1994) genutzt werden. Hierzu übermittel der PPP-Client im Falle von PAP jeweils ein Benutzername sowie ein Kennwort an den RAS. CHAP nutzt zusätzlich ein Challenge-Response-Verfahren. Ein Kennwort wird nicht übertragen. Stattdessen übermittelt der RAS eine Zufallsnummer, die Challenge, an den PPP-Client, der

hieraus mit Hilfe eines vereinbarten Algorithmus eine Antwortzahl berechnet und an den RAS zurückschickt.

Die endgültige Authentisierung wird in der Regel von einem RADIUS-System vorgenommen. Hierzu benutzt der RAS das RADIUS-Protokoll und sendet einen RADIUS-Authentication-Request an den RADIUS Server, der hierauf mit einer positiven oder negativen RADIUS-Authentication-Response antwortet.

Nach erfolgreicher Authentisierung erhält der PPP-Client vom RAS eine IP-Adresse. Danach steht die IP-Verbindung bis zum Zielnetz in beider Übertragungsrichtungen zur Verfügung und die Session wechselt in die Phase der Datenübertragung. In dieser Phase beschränkt sich die Funktion des RAS auf reines IP-Routing.

2.2.6.2 Dial In Prozedur bei GPRS

Die im vorangegangen Protokolle und Abläufe finden sich auch bei der Einwahl über GPRS. Allerdings sind die Funktionen anders aufgeteilt. Die PPP-Verbindung wird nicht bis zum GGSN (vergleichbar mit dem RAS) geführt, sondern wird bereits vom Mobilfunkgerät terminiert. Die RADIUS-Schnittstelle ist jedoch weiterhin Funktionsumfang des GGSN (Abbildung 12, Abbildung 13).

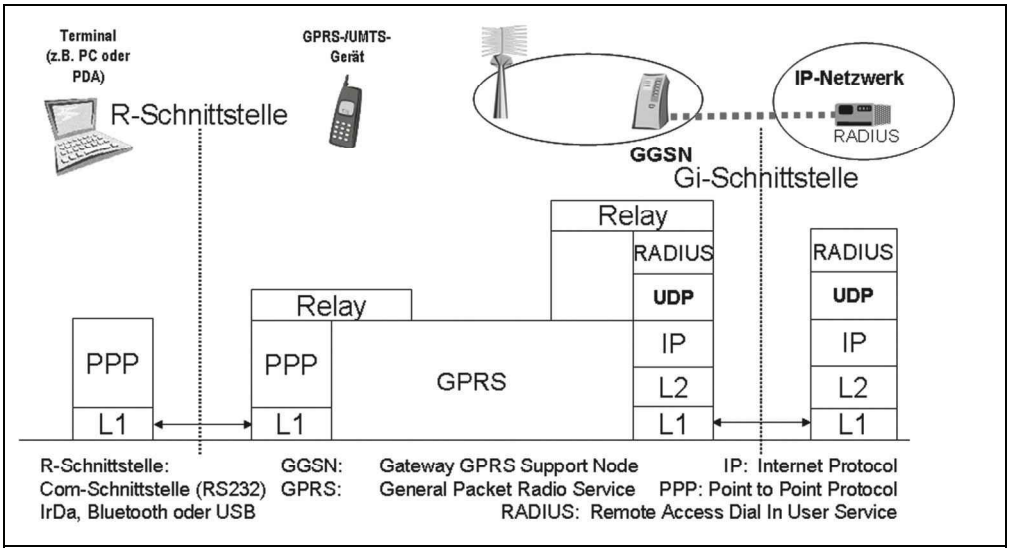


Abbildung 12: Protokollarchitektur für den Verbindungsaufbau über GPRS und UMTS

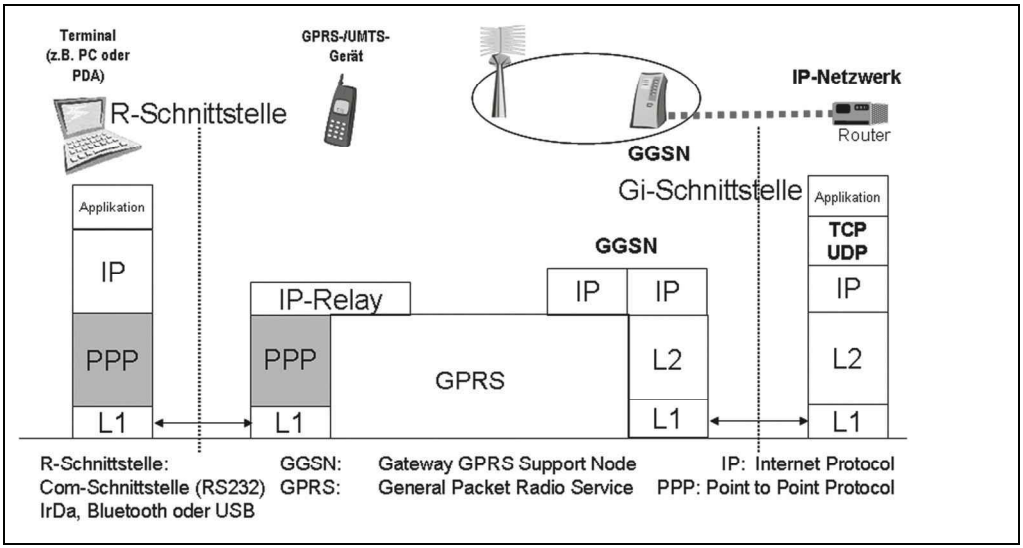


Abbildung 13: Protokollarchitektur für die Datenübertragung über GPRS und UMTS

2.2.6.3 Aufbau einer GPRS-Verbindung

Dieser Abschnitt beschreibt die Ansteuerung des mobilen Endgerätes zum Aufbau einer GPRS-Verbindung (GPRS context).

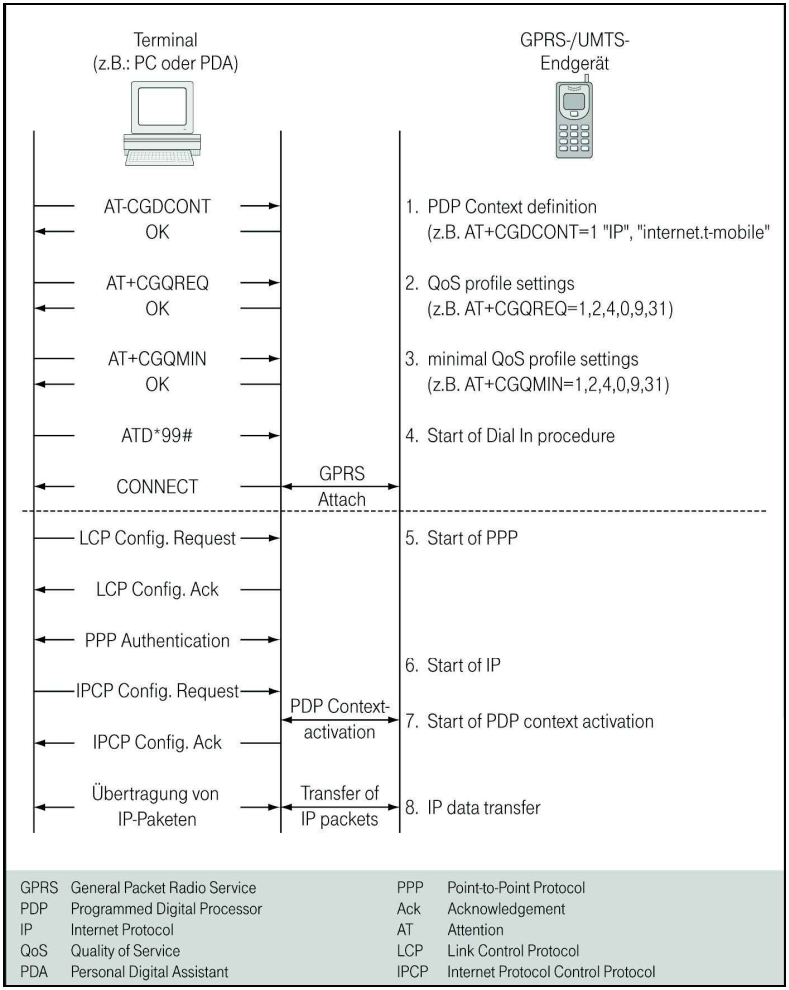


Abbildung 14: Verbindungsaufbau mit AT-Befehlen

Bevor die Einwahlprozedur gestartet werden kann, muss das Endgerät zuvor initialisiert werden. Dies geschieht mit folgendem AT-Befehl:

Beispiel: AT+CGDCONT=1,"IP","internet.t-mobile"

Mit diesem AT-Befehl wird der so genannte PDP-Kontext definiert.

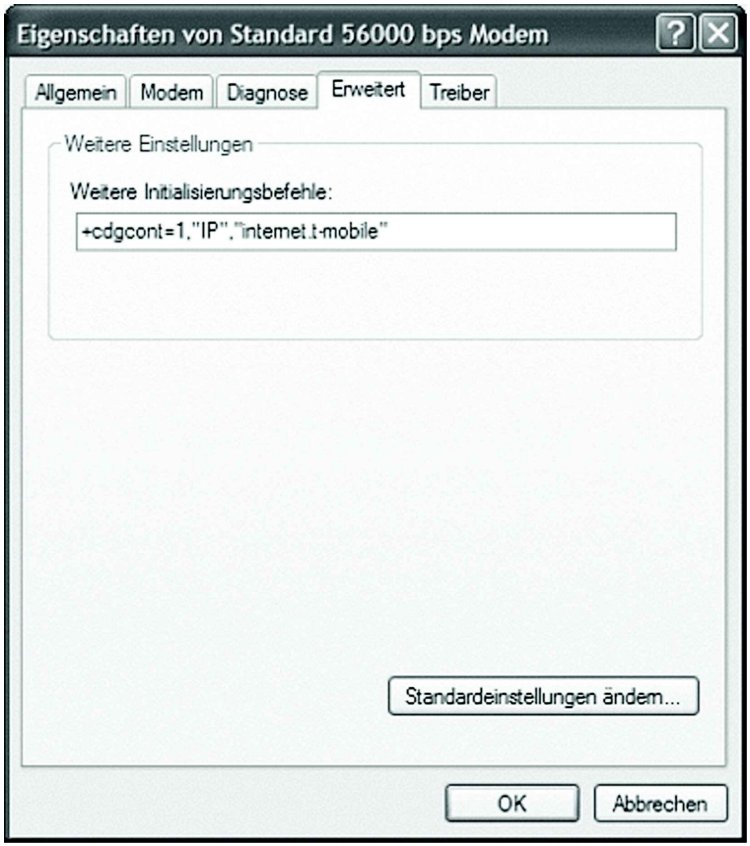


Abbildung 15: Modeminitialisierung unter Windows in der erweiterten Modemeinstellung

CGDCONT steht für "Control GPRS Data Configuration within Telephone". Die Zahl 1 ist die Identifikationsnummer (CID: Context ID) des so definierten PDP-Kontextes. Über diese Nummer ist es möglich, verschiedene Einstellung vorzunehmen, bevor der Verbindungsaufbau gestartet wird.

Der Parameter "IP", der unbedingt in Anführungszeichen anzugeben ist, definiert, dass eine IP-Verbindung aufgebaut werden soll. Anschließend folgt der Access Point Name (APN, siehe Abschnitt 2.2.2), der ebenfalls in Anführungszeichen anzugeben ist. Im gewählten Beispiel handelt es sich um den öffentlichen APN der T-Mobile für den Internet-Zugang.

Der angegebene Initialisierungsbefehl kann unter Windows in den erweiterten Modemeinstellungen eingegeben werden (Abbildung 15). Dies hat zur Folge, dass er jedes Mal vor dem Aufbau einer GPRS-Verbindung an das Mobilfunkgerät geschickt wird.

Optional kann mit folgendem AT-Befehl anschließend das QoS- (Quality of Service) Profil verändert werden:

Beispiel: AT+CGQMIN=1,2,4,0,9,31

CGQMIN steht für "Control GPRS Quality of Service Profile (Minimum acceptable)". Die Zahl 1 ist erneut die Kontextidentifikation ("CID"). Die nachfolgenden Zahlen legen die verschiedenen QoS-Klassen (Proirity, Delay, Reliability, Throughput) fest.

Der GPRS-Einwahlvorgang startet, sobald der Client die PPP Session aktiviert, indem er folgenden AT-Befehl sendet:

ATD*99***CID#

Die Zeichenfolge *99*** zeigt der Mobilstation an, dass kein leitungsvermittelter Dienst, sondern GPRS bzw. UMTS oder HSDPA[23] genutzt werden soll. Es folgt die Kontextidentifikationszahl, die zuvor initialisiert wurde. Daraufhin startet die Mobilstation die Attach- sowie anschließend die Kontext-Aktivierungs-Prozedur automatisch.

Mit der Attach-Prozedur registriert sich die Mobilstation am SGSN. Dabei wird bereits eine Authentisierung gegenüber dem GPRS-Netz durchgeführt. Nach der Registrierung startet das Mobility-Management im SGSN. Die jeweilige Zelle der Mobilstation bleibt fortan im SGSN bekannt.

Die Kontext-Aktivierungs Prozedur aktiviert die Ende-zu-Ende Verbindung zum Ziel IP- Netz. Hierzu wird vom GGSN der APN ausgewertet, mit dem am GGSN eine IP- Verbindung zum jeweiligen Zielnetz logisch verknüpft ist (siehe Abschnitt 2.2.2).

Bevor die IP-Verbindung zum Zielnetz jedoch zustande kommt, kann optional noch eine Authentisierung anhand von Benutzername und Kennwort vorgenommen werden. Hierzu übergibt der GGSN die nötigen Parameter per RADIUS-Protokoll an einen externen RADIUS-Server (Abbildung 16).

Sofern der Nutzer bekannt und berechtigt ist, antwortet der RADIUS-Server mit einem Authentication Accept und gibt darin u.a. die IP-Adresse für die Mobilstation zurück.

Nach Ende der Kontext-Aktivierungs-Prozedur ist die Mobilstation logisch mit dem Ziel-IP-Netz verbunden und kann beliebige Applikationen nutzen, die ihr das Zielnetz zur Verfügung stellt.

[23] Je nach Voreinstellung der Mobilstation wird bevorzugt ein Datendienst gewählt, sofern neben GPRS auch UMTS oder HSDPA zur Verfügung steht.

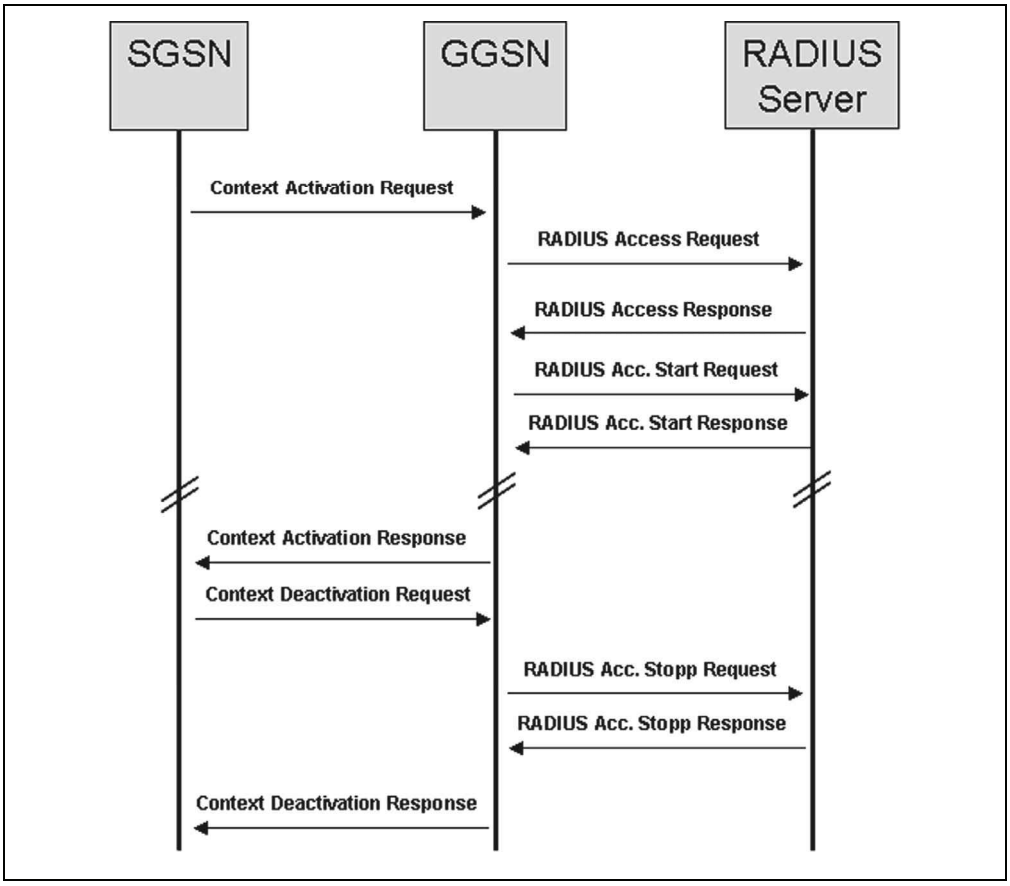


Abbildung 16: RADIUS-Authentisierung beim Aufbau einer GPRS-Verbindung

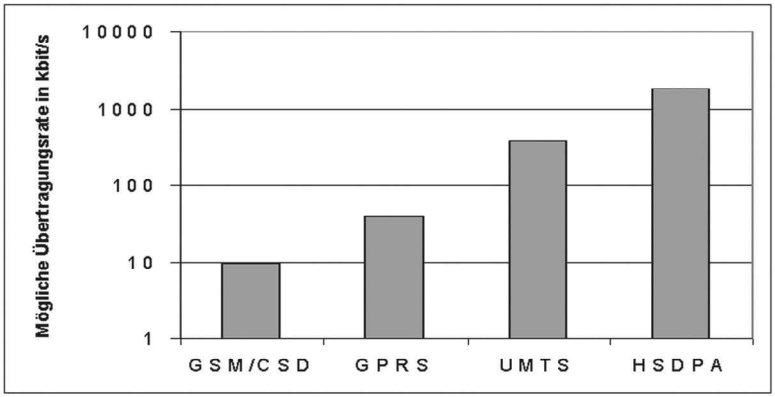
2.2.7 Eigenschaften der mobilen Datenübertragung mit GPRS, UMTS und HSDPA

2.2.7.1 Typische Leistungswerte von GPRS, UMTS und HSDPA

Die wesentlichen Leistungsparameter von GPRS, UMTS und HSDPA sind in Tabelle 4 zusammengefasst.

Tabelle 4	Übertragungseigenschaften von GPRS, UMTS und HSDPA		
Leistungs-Parameter	GPRS	UMTS	HSDPA
Attach Zeit	2 bis 12 Sekunden	2 bis 12 Sekunden	2 bis 12 Sekunden
Verbindungs-aufbauzeit Kontext-aktivierung	0,5 bis 5 Sekunden	0,5 bis 5 Sekunden	0,5 bis 5 Sekunden
Übertragungs-verzögerung (Round Trip Delay)	700 Millisekunden (Schwankung zwischen 0,4 und 2 Sekunden)	300 Millisekunden	150 Millisekunden
Übertragungsrate Downlink	40 kbit/s	384 kbit/s	1,8 Mbit/s
Flächen-versorgung	städtisch und ländlich	städtisch	städtisch (identisch mit UMTS)
Handover-Unterbrechungen	1 bis 17 Sekunden	Keine Unterbrechung (Soft Handover)	< 3 Sekunden

Während GPRS sich besonders durch eine große Flächenabdeckung auszeichnet, findet man UMTS und HSDPA vornehmlich im städtischen Gebieten. UMTS und HSDPA bieten jedoch gegenüber GPRS wesentlich höher Übertragungsbandbreiten bei deutlich geringerem Delay (Abbildung 17).



CSD: Circuit Switched Data
GPRS: General Packet Radio Service
UMTS: Universal Mobile Telecommunications System
HSDPA: High Speed Downlink Packet Access

Abbildung 17: Übertragungsraten im Vergleich

2.2.7.2 Besondere Übertragungseigenschaften von GPRS

Durchsatz

GPRS ist ein asymmetrischer Datendienst. Abhängig vom genutzten Mobilfunkgerät unterscheidet sich der Datendurchsatz in Uplink und Downlink. Die meisten Geräte unterstützen im Uplink maximal 2 Zeitschlitze (Slots) und im Downlink maximal 4 Zeitschlitze auf der Luftschnittstelle. GPRS unterstützt für die einzelnen Zeitschlitze vier verschiedene Kodierverfahren (CS-1 , CS-2, CS-3 oder CS4) mit unterschiedlichen Übertragungsraten (Abbildung 18), die abhängig von den jeweiligen Funkfeldbedingungen und dem jeweiligen Funktionsumfang des Endgeräts vom GPRS-Netz gewählt werden.

Der theoretisch maximal erzielbare Durchsatz ergibt sich somit für jede Übertragungsrichtung als Produkt aus der maximalen Anzahl der Slots und der

maximalen Übertragungsrate des jeweils genutzten Kodierverfahrens pro Zeitschlitz.

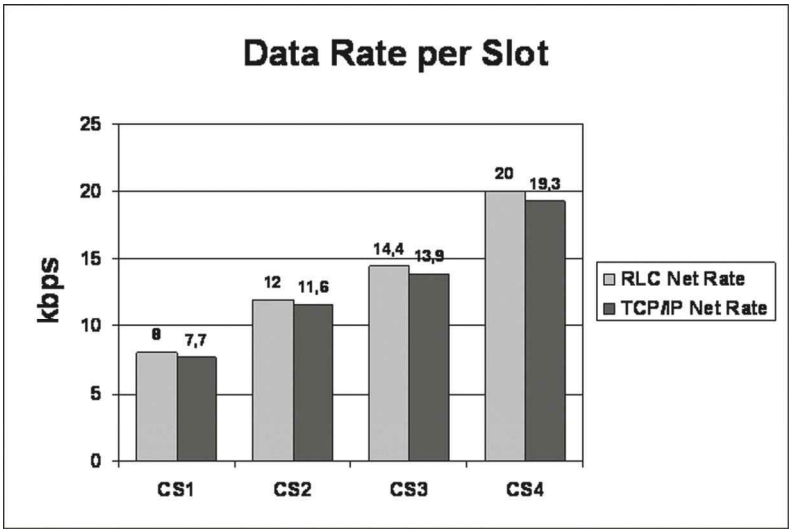


Abbildung 18: Theoretischer GPRS-Durchsatz nach Coding Scheme auf unterschiedlichen Protokollebenen

Eine Weiterentwicklung von GPRS ist E-GPRS, das im Netz von T-Mobile inzwischen zur Verfügung steht. E-GPRS basiert auf der EDGE (Enhanced Data Rates for GSM Evolution) Technologie und verwendet eine effizientere Kanalkodierung. Somit sind im Gegensatz zu GPRS Datenraten bis 55 KBit/s pro Kanal möglich. Bei einem Endgerät, dass z.B. vier Kanäle unterstützt, ergibt sich somit theoretisch eine maximale Bruttodatenrate von 220 KBit/s im Downlink.

Der tatsächliche Durchsatz hängt darüber hinaus von folgenden Faktoren ab:

- der augenblicklichen lokalen Netzlast und der Anzahl der aktiven Endgeräte,

- den aktuellen Funkfeldbedingungen,
- der augenblicklichen Mobilität des Nutzers
- der Flussteuerung von TCP (siehe Abschnitt 2.2.8.3) sowie
- vom genutzten Endgerät

Im stationären Fall lässt sich mit CS-2 und einer Kanalbündelung von 3 Zeit-Schlitzen ein FTP-Durchsatz von 25 – 32 KBit/s erzielen. Abbildung 18 zeigt jeweils theoretische Durchsatzwerte pro Zeitschlitz unter idealen Bedingungen.

Flächenversorgung

GPRS mit CS-1 benötigt einen geringfügig besseren Signal-Rausch-Abstand als der GSM-Sprachdienst. Demzufolge ist die Flächenversorgung von GPRS etwas kleiner als beim GSM-Basisdienst. Der Unterschied in der Flächenversorgung ist kleiner als 1%. Dies bedeutet, dass in Randgebieten ein Telefongespräch weiterhin möglich sein könnte, obwohl eine GPRS-Verbindung nicht mehr zustande kommt.

In Gebäuden oder in Fahrzeugen ist es ratsam, eine Außenantenne einzusetzen, um eine bessere Qualität zu erzielen.

Unterbrechungen

Unterbrechungen haben einen großen Einfluss auf den Datendurchsatz auf TCP-Ebene (siehe Abschnitt 2.2.8.3).

Aufgrund der Mobilität des Nutzers kann es vorkommen, dass eine aktive GPRS-Verbindung über längere Zeit unterbrochen wird. Dies geschieht beispielsweise,

- wenn der Nutzer das mit GPRS versorgte Gebiet (z.B. bei Einfahrt in eine Tiefgarage) verlässt,

- wenn der Nutzer sich von einer Zelle in eine andere Zelle bewegt, wodurch eine Unterbrechung von 1 bis 17 Sekunden entstehen kann,
- wenn der Nutzer ein ankommendes Telefongespräch annimmt oder eine Kurznachricht erhält,
- wenn die lokale Verbindung (z.B. Bluetooth) zwischen Mobilstation und Laptop verloren geht. In diesem Fall wird die GPRS-Verbindung beendet.

Wechselt ein Nutzer in schneller Abfolge mehrere Zellen hintereinander, so kann es zu Unterbrechungen im Minutenbereich kommen. Dauert eine Unterbrechung länger als 54 Minuten, so wird der PDP-Kontext vom GPRS-Netz automatisch beendet.

Befindet sich eine Mobilstation am Rande einer Zelle, kann es zu wiederholten Zellwechsel mit Unterbrechungen und erhöhter Paketverlustrate kommen.

2.2.7.3 Besondere Übertragungseigenschaften von UMTS

Aufgrund der neuen Modulationstechnik verfügt UMTS über Eigenschaften, die es in GSM/GPRS-Netzen nicht gibt. Die wichtigsten Eigenschaften sind:

- Zellatmung (Cell breathing)

Dieses Phänomen ist typisch für Systeme mit Spread-Spectrum-Modulation und äußert sich darin, dass der Zellradius immer kleiner wird, je mehr Nutzer in dieser Zelle aktiv sind. Dieses Verhalten liegt in der Eigenschaft begründet, dass Systeme mit Spread-Spectrum-Modulation für jeden aktiven Nutzer ungefähr den gleichen Signal-Rausch-Abstand benötigen. Diese Situation lässt sich sehr gut mit einem Raum voller Menschen vergleichen, die miteinander sprechen. Solange alle mit

ungefähr der gleichen Lautstärke sprechen, ist eine verständliche Unterhaltung möglich. Je mehr Menschen in den Raum hinzukommen, desto enger müssen nun die Menschen zusammenrücken, um auch weiterhin eine Verständlichkeit zu gewährleisten.

- Soft Handover

Soft/softer Handover bezeichnet eine Situation, in der eine Mobilstation simultan mit verschiedenen Basisstationen (Node B) in Kontakt steht. Im Falle eines Zellwechsels hält die Mobilstation weiterhin den Kontakt zur „alten" Zelle und überträgt bzw. empfängt hierüber weiterhin Daten, während der Signalisierungsverkehr bereits über die „neue" Zelle läuft. Der Nutzdatenverkehr wird erst dann umgeschaltet, wenn die neue Verbindung in der neuen Zelle etabliert ist. Dadurch werden Unterbrechungen vermieden.

- UMTS Zustandsmodell (State Model)

Bei UMTS kann eine Mobilstation mit aktiven PDP-Kontext verschiedene Zustände einnehmen, und zwar abhängig davon, wie lange sie schon keine Daten mehr gesendet oder erhalten hat. Dabei gilt: Je länger die Mobilstation bereits inaktiv war, desto länger dauert es, bis sie erneut Übertragungsressourcen zugeteilt bekommt. Hierdurch wird die knappe Ressource der Luftschnittstelle effektiver genutzt. Für die einzelne Mobilstation bedeutet dies nach einer längeren Inaktivität eine Verzögerung (Delay) von ca. 2-3 Sekunden, bevor erneut Daten übertragen werden.

2.2.7.4 Besondere Übertragungseigenschaften von HSDPA

Auch HSDPA verfügt aufgrund der neuen Übertragungstechnik ebenfalls über spezielle Eigenschaften:

- Schwankende Übertragungsraten

HSDPA ist eine Ressource, die unter mehreren aktiven Mobilstationen aufgeteilt wird. Dabei können Änderungen in der Zahl der Nutzer zu einer Verringerung des Durchsatzes für die anderen Nutzer führen. Zudem hängt der Datendurchsatz von den aktuellen Funkfeldbedingungen ab, die sich ebenfalls abhängig von der Mobilität der Mobilstation oder externen Störeinflüssen ständig ändern.

- Unterbrechungen bei Zellwechsel

Da HSDPA keinen Soft-Handover wie UMTS kennt, entstehen bei einem Zellwechsel wie bei GPRS Unterbrechungen von bis zu drei Sekunden.

2.2.8 Auswirkungen der Übertragungseigenschaften von GPRS auf TCP und Optimierungsmaßnahmen

2.2.8.1 Problemstellung

Die Akzeptanz von GPRS und UMTS im geschäftlichen Umfeld hängt wesentlich von der Performance TCP-basierter Anwendungen ab. Aufgrund der spezifischen Eigenschaften der mobilen Datenübertragung wird die theoretisch maximal zu Verfügung stehende Kanalbandbreite von TCP jedoch nur sehr schlecht genutzt. Mit Hilfe von Optimierungs-Software lassen sich hier jedoch signifikante Verbesserungen erzielen.

Die spezifischen Übertragungseigenschaften von Mobilfunknetzen beeinflussen auf vielfältige Weise die Arbeitsweise bzw. die Lauffähigkeit von IP-(Internet Protocol) basierten Protokollen und Anwendungen. Die verbreiteten Datenkommunikations-Protokolle wie beispielsweise die Protokollfamilie TCP/IP (Transmission Control Protocol) wurden in erster Linie für LAN- bzw. Festnetzumgebungen entwickelt und setzen im allgemeinen eine vergleichsweise hohe Bandbreite, eine hohe Stabilität sowie ein geringes Delay[24] voraus. Daher sind fallweise besondere Maßnahmen erforderlich, um die Lauffähigkeit der eingesetzten Protokolle und Anwendungen über eine mobile Netzanbindung zu gewährleisten.

Von entscheidender Bedeutung ist dabei die Performance von TCP. Da die Mehrzahl der Anwendungen dieses Protokoll einsetzt, ist die Lauffähigkeit von TCP kritisch für die Akzeptanz und den Erfolg des genutzten mobilen Datendienstes. Als gesichertes, verbindungsorientiertes Protokoll auf der Basis von IP ist TCP besonders sensitiv gegenüber "großen und variablen" Übertragungsverzögerungen (Delay bzw. Latenz) sowie "häufigen und gebündelten (bursty)" Paketfehlern bzw. Unterbrechungen. Gerade dies entspricht jedoch den typischen Eigenschaften eines mobilen Datendienstes.

Die IETF (Internet Engineering Task Force) hat daher eine eigene Arbeitsgruppe (WG = work group) mit der Bezeichnung "Performance Implications of Link Characteristics (PILC)" eingerichtet, um Empfehlungen zur Optimierung bzw. Modifikation von IETF-Protokollen (z.B. TCP) in Netzwerkumgebungen mit problematischen Übertragungseigenschaften zu erarbeiten. Einige dieser Empfehlungen werden in diesem Abschnitt vorgestellt.

---

[24] Delay: Verzögerungs- oder Wartezeit. Zeitspanne, um die ein Ereignis verzerrt oder verzögert wird. Beispielsweise die Zeit, die vergeht, bis eine abgesandte Information vom Zielsystem empfangen wird.

Auf Grund besonderer Störeinflüsse (Mehrwegeausbreitung[25], Abschattungen, Rauschen, Doppler-Effekt, Interferenzen, Wettereinflüsse, Mobilität) ist die Datenübertragung in Mobilfunknetzen grundsätzlich sehr fehleranfällig. Hieraus ergibt sich im Allgemeinen eine höhere Bitfehlerrate (BER = Bit Error Rate) als in terrestrischen Netzen mit häufigen und abrupten Schwankungen der Übertragungsqualität. Daher kommen auf der Funkverbindung (Radio Link Layer, Schicht 2) in der Regel zusätzliche Fehlerkorrekturverfahren wie FEC[26] (Forward Error Correction) und ARQ[27] (Automatic Repeat Request) zur Anwendung. Diese Aufgabe wird bei leitungsvermittelten Diensten in GSM-Netzen (Global System for Mobile Communications) vom Radio Link Protocol (RLP) wahrgenommen.

Bei GPRS kann ARQ auf zwei Protokollebenen aktiviert werden, einerseits auf LLC[28]-Ebene (Logical Link Control) zwischen Mobilstation und SGSN (Serving GPRS Support Node) und andererseits auf der Ebene der Luftschnittstelle zwischen Mobilstation und BSC in der RLC[29]-Schicht (Radio Link Control). In beiden Fällen spricht man jeweils von "Acknowledged Mode". Da ARQ auf LLC-Ebene ähnlich wie die Fehlersicherung im TCP bei Übertragungsfehlern in der Regel ganze IP-Pakete

---

25 Siehe hierzu auch den Beitrag ”Funkdienste und Frequenzmanagement der Deutschen Telekom”, Unterrichtsblätter Nr. 7/98, S.308-327.

26 Dt. Vorwärts-Fehlerkorrektur; Durch Hinzufügen von Redundanz wird ein Datenpaket mit einer Frame Check Sequence (FCS) geschützt, die sich aus den zu schützenden Datenbits ergibt.

27 Normalform eines Sicherungsprotokolls, bei der die gesicherte Datenübertragung auf der blockweisen Fehlerüberwachung beruht.

28 Dt. Logische Verbindungskontrolle. Kommunikationsprotokoll der Sicherungsschicht (LLC-Teilschicht) für IEEE-802-LAN, das der nachfolgenden Vermittlungsschicht Übertragungsdienste für den Austausch von Dateneinheiten zur Verfügung stellt.

29 In der Protokollarchitektur des Mobilfunksystems der dritten Generation UMTS (Universal Mobile Telecommunications System) eine Protokollschicht, die – aufsetzend auf die MAC-Schicht (Media Access Control) – für die Übertragungssteuerung und -sicherung auf den logischen Kanälen zuständig ist.

wiederholt, vorausgesetzt die IP-Paketgrösse passt in das Informationsfeld eines LLC-Frame, und damit eine Funktion erfüllt, die TCP ohnehin Ende-zu-Ende wahrnimmt, sollte ARQ in diesem Falle lediglich auf RLC-Ebene aktiviert werden.

Das RLC zerlegt (Segmentation) zu sendende LLC-Frames in einzelne Radio-Blocks und setzt die LLC-Frames auf der Empfangsseite wieder korrekt zusammen (Desegmentation). Verloren gegangene Blöcke werden durch ARQ von der Gegenstelle erneut angefordert. Dieses Verfahren wird durch einen Zähler für die maximale Anzahl von Wiederholungsanfragen bzw. durch einen Timer gesteuert, der angibt, wie lange auf die Quittierung eines übertragenen Radio-Blocks maximal gewartet wird, bevor der betreffende Block erneut übertragen wird.

Durch den Einsatz von FEC und ARQ kann somit zwar die Wahrscheinlichkeit unentdeckter Paketfehler reduziert werden, andererseits verursachen diese Verfahren jedoch in einem verrauschten Kanal auf Kosten der knappen Übertragungskapazität zusätzlichen Datenverkehr. Außerdem steigt auf Grund der mehrfachen Übertragung gestörter Radio-Blocks bzw. LLC-Frames die Übertragungsverzögerung (Delay, Latenz) sowie deren Varianz (Jitter[30]) im gleichen Maße an.

Typisch für die mobile Datenübertragung sind auf Grund der besonderen Störeinflüsse zudem häufige Schwankungen der Funkversorgung. Der Träger kann dabei auf Grund der Mobilität des Nutzers bzw. plötzlicher Störeinflüsse kurzzeitig für wenige Sekunden verloren gehen. Dies ist besonders für einen File-Transfer kritisch, weil ohne besondere Maßnahmen nach einem Verbindungsabbruch die gesamte Datei neu übertragen werden muss. Eine kurzfristige Verschlechterung

[30] Jitter: Weitgehend zufallsbestimmte Schwankungen der Flanken eines realen Datensignals um die Sollzeit des Nulldurchganges.

der Übertragungseigenschaften des Funkkanals verursacht die für die Funkübertragung typischen Bündelfehler (bursty errors). Diese Bündelfehler können mit Hilfe von ARQ auf RLC-Ebene korrigiert werden. Dabei kommt es jedoch für die Dauer der jeweiligen Störung zu einem ebenso sprunghaften Anstieg des Delay. Das Block-Interleaving wie bei leitungsvermittelten GSM-Datendiensten kommt bei GPRS nicht zur Anwendung.

Die besondere Eigenschaft von GPRS, nämlich die dynamische, bedarfsorientierte Kanalzuweisung, die eine effizientere Nutzung der knappen Frequenzressourcen ermöglicht, führt bei "burstartigem" Verkehr auf Grund des Zuteilungsverfahrens zu einem weiteren Delay-Anteil. Zeitschlitze, die eine Mobilstation zum Senden nutzen möchte, müssen zuvor vom GPRS-Netz bzw. BSC (Base Station Controller) durch die Mobilstation explizit angefordert und der Mobilstation zugeteilt werden. Dabei kann die Mobilstation bei der Anmeldung gleich mehrere Zeitschlitze reservieren (Dynamic Allocation) und damit diesen Delay-Anteil reduzieren.

Ein weiteres Merkmal mobiler Datenübertragung sind neben dem vergleichsweise hohen Delay die geringen Übertragungsbandbreiten. Nach RFC 2757 (Request for Comments) werden solche Übertragungsnetze daher als "Long Thin Networks" bezeichnet: "Long" wegen des hohen Delay und "Thin" wegen der Schmalbandigkeit. Obwohl mit der Einführung von GPRS deutliche Verbesserungen erzielt werden konnten, wobei Bandbreiten im Bereich der Übertragungsgeschwindigkeit von ISDN erzielbar sind, bleiben die Übertragungsraten im Vergleich zu einer reinen LAN-Umgebung oder zu einem festnetz-basierten Weitverkehrsnetz (z.B. ATM = Asynchronous Transfer Mode,

Frame Relay[31]) auch weiterhin deutlich zurück. Dies hat Auswirkungen auf die Lauffähigkeit von Anwendungen, die für reine LAN-Umgebungen bzw. Weitverkehrsnetze mit geringem Delay und höherer Bandbreite erstellt wurden und unverändert über einen mobilen Datendienst wie GPRS genutzt werden sollen.

Als Besonderheit kommen bei GPRS spezielle Kanalkodierungen (CS = Coding Schemes) zum Einsatz, die abhängig von der jeweiligen Übertragungsgüte unterschiedliche Datenraten erlauben. Man unterscheidet vier verschiedene Codierverfahren, zwischen denen je nach Feldstärke dynamisch gewechselt werden kann (Abbildung 18). Die auf Anwendungsebene effektiv nutzbare Bandbreite hängt bei idealen Bedingungen lediglich von der jeweiligen Kanalkodierung, der IP-Paketgröße sowie der Kanalbündelung des genutzten Endgerätes ab. Der GPRS-Standard definiert eine Kanalbündelung von maximal acht Time-Slots je Endgerät. Derzeit verfügbare Endgeräte erlauben im Downlink eine Kanalbündelung von zwei bis vier Time-Slots.

Bei einer Kanalbündelung von zwei Time-Slots ergibt sich beispielsweise für CS-2 (Coding Sequence) auf Anwendungsebene eine maximale theoretische Bandbreite von etwa 20 kbit/s. Die Übertragung eines IP-Pakets mit einer für LAN-Umgebungen typischen Paketlänge von 1 500 Byte verursacht bei der Übertragung über GPRS (2 Slot, CS 2) alleine auf Grund der Bandbreite ein Queueing-Delay von etwa 500 bis 600 Millisekunden (ms). Dieser Wert ist für Echtzeit- oder bestimmte Dialog-Anwendungen bereits zu hoch.

[31] Frame Relay: von engl. frame = Rahmen und to relay = weiterleiten; Bezeichnung für ein paketorientiertes Übertragungsprotokoll für Punkt-zu-Punkt-Verbindungen. Frame Relay arbeitet auf Schicht 1 und 2 des OSI-(Open Systems Interconnection) Referenzmodells und ist auch für Breitbandanwendungen geeignet.

2.2.8.2 Anforderungen an ein Übertragungsnetz aus Anwendungssicht

Nicht alle Anwendungen stellen die gleichen Anforderungen an die Qualität eines Übertragungsnetzes. Unternehmenskritische Anwendungen wie beispielsweise Supply Chain Management[32] oder Anwendungen im Finanzbereich erfordern eine hohe Verfügbarkeit sowie ein hohes Maß an Sicherheit in Bezug auf Authentizität, Vertraulichkeit und Manipulationsschutz. Demgegenüber ist für eine E-Mail-Anwendung eine "Best-Effort Performance[33]" wie im Internet bereits zu tolerieren. Abbildung 19 zeigt qualitative Anforderungen beispielhafter Anwendungen.

	Anforderungen					
	Bandbreite			Delay-Sensitiv		
	hoch	mittel	gering	hoch	mittel	gering
SAP R/3			■	■		
E-Mail		■				■
WWW-Zugang		■			■	
File Transfer	■					■
Voice over IP			■	■		

Abbildung 19: Qualitative Anforderungen beispielhafter Anwendungen

[32] Supply Chain Management: In den Unternehmen der Wirtschaft das Management der Liefer- und Logistikkette (Supply Chain).

[33] Best-Effort Performance: Dt. "Leistungsfähigkeit nach bestem Bemühen". Bezeichnung für Datenübertragungsverfahren, bei denen im Netz mit Hilfe von sporadischen oder periodischen Messungen Leistungs-Reports erstellt werden, wodurch die aktuelle Nutzung und Auslastung des Netzes sich darstellen lässt und zyklisch in der Datenbank abgespeichert werden kann.

Um bei der Vielzahl unterschiedlichster Anwendungen dennoch einheitliche Anforderungen herausarbeiten zu können, ist es zunächst erforderlich, weitestgehend homogene Anwendungsklassen zu definieren und dann für diese Klassen die jeweiligen Anforderungen zusammenzustellen.

Netz-Services

Netz-Services sind Dienste, die zur Organisation des Netzes benötigt werden. Diese Dienste werden typischerweise bei der Netzanmeldung bzw. zu Beginn einer Session einmalig in Anspruch genommen (z.B. IP-Adresszuweisung, Netzanmeldung oder Namensauflösung).

Dialog-Anwendungen

Diese Anwendungen sind durch die Interaktion Mensch-Maschine mit häufigen, kleineren Transaktionen charakterisiert. Beispiele sind typischerweise Datenbankabfragen, SAP- oder Terminal-Emulationen im Großrechnerumfeld, aber auch teilweise Web-Browsing (HTTP = Hypertext Transport Protocol), das von seiner Übertragungscharakteristik her zwischen Dialog-Anwendung und File-Transfer einzuordnen ist. Kritisch ist bei dieser Anwendungsklasse insbesondere das Antwortzeitverhalten sowie die Netzstabilität. Größere Datenmengen werden seltener übertragen.

Groupware/Messaging/Workflow

Typisch für diese Anwendungsklasse ist das asynchrone Kommunikationsmuster. Die Nachrichten werden auf dem Weg vom Sender zum Empfänger zwischengespeichert. Die zeitliche Verfügbarkeit der Netzverbindung sowie das Delay sind aus Anwendungssicht in der Regel eher unkritisch. Der typische

Vertreter dieser Klasse sind Groupware[34]-Anwendungen, z.B. E-Mail (ohne Anhänge).

File-Transfer

Beim File-Transfer werden Dateien zwischen Server und Client übertragen. Er stellt hohe Anforderungen in Bezug auf Bandbreite und Netzstabilität. Die Übertragungsverzögerung ist eher unkritisch.

Steuerung (Logistik/ Telemetrie)

Diese Anwendungsklasse ist durch ein sehr geringes, sporadisches Verkehrsaufkommen gekennzeichnet. Beispiele sind bestimmte Telemetrie-Anwendungen oder Alarmüberwachung. Die Anforderungen an Bandbreite und Delay sind gering. Mobilität, Zuverlässigkeit und Verfügbarkeit stehen im Vordergrund.

Echtzeitanwendungen

Diese Anwendungsklasse erfordert ein sehr geringes Delay sowie eine sehr geringe Delay-Varianz (Jitter). Für Video-Anwendungen werden zudem höhere Bandbreiten benötigt. Echtzeitanwendungen sind in der Regel tolerant gegenüber Paketverlust. Netzservices sowie Steuerungsanwendungen stellen die geringsten Anforderungen an die Übertragungsbandbreite sowie das Delay, sind jedoch sehr sensibel gegenüber einer schlechten Dienstverfügbarkeit.

Die höchsten Anforderungen in Bezug auf Übertragungsverzögerung und Paketverlust stellen Echtzeitanwendungen wie Video-Conferencing oder Voice over

[34] Groupware: Relativ unspezifische Bezeichnung für Software, die von Arbeitsgruppen (Teamworking) eingesetzt wird und oft mehrere Programme und Kommunikationsdienste umfasst. Sie unterstützt den standortunabhängigen mehrfachen Zugriff auf Objekte und fördert so die innerbetriebliche Kooperation.

IP (VoIP). Nach ITU-T G.144 (International Telecommunications Union) muss die Mund-zu-Ohr-Verzögerung bei VoIP im Bereich von 150 ms bis 400 ms liegen, um die Qualität des (digitalisierten) Telefonnetzes zu erzielen. Der Anhang zu ITU-T G.113 gibt je nach eingesetzten Sprachcodec[35] gemessen an der Qualität des Telekommunikationsnetzes Grenzwerte für die Paketverlustrate an:

- 10 Prozent (G.711 mit PLC[36]),
- 3,4 Prozent (G.729 (A) + VAD[37]),
- 2,1 Prozent (G.723.1 6,3 KBit/s + VAD).

Allgemein wird eine Verlustrate von 3 Prozent als Obergrenze akzeptiert.

Ähnlich hohe Anforderungen an das Übertragungs-Delay stellen Dialoganwendungen. Der RFC 1144 definiert als kleinste durch den Menschen wahrnehmbare Reaktionszeit einen Wert von 200 ms. Die Obergrenze ergibt sich für diesen Wert individuell als die Reaktionszeit, die der jeweilige Nutzer bzw. die jeweilige Nutzergruppe maximal bereit ist zu akzeptieren. Delay-Werte von mehreren Sekunden sind bei diesen Anwendungen sicherlich problematisch.

Die Anwendungsklasse des File-Transfer erfordert in erster Linie eine hohe, weitgehend konstante Übertragungsrate sowie eine stabile Verbindung, sie ist jedoch andererseits sehr unempfindlich gegenüber Delay und Jitter.

---

35 Codec: Abk. Coder/Decoder; Komponente zur Komprimierung und Dekomprimierung von Daten als Hardware oder Software.

36 PLC: Packet Loss Concealment ist ein Verfahren, mit dem kurzeitige Unterbrechungen im Datenstrom überbrückt werden können.

37 VAD: Abk. Voice Activity Detection. Oberbegriff für Verfahren zur Erkennung und effizienten Ausnutzung von Sprachpausen bei der Übertragung von Sprachsignalen. Mit dem Verfahren können die ”ungenutzten” Übertragungsleistungen während der Sprachpausen anderen Kommunikationsbeziehungen oder anderen Anwendungen zugewiesen werden.

2.2.8.3 Grundlagen und Eigenschaften von TCP/IP

Die Protokollfamilie TCP/IP wurde ursprünglich für reine LAN-Umgebungen bzw. terrestrische Weitverkehrsnetze mit vergleichsweise hoher Übertragungsbandbreite und geringem Delay entwickelt. Leitungsgebundene Netze zeichnen sich im Gegensatz zu Mobilfunknetzen zudem durch eine hohe Zuverlässigkeit und Stabilität in Bezug auf Paketverlust und Delay aus. Gerade diese Eigenschaft war eine grundlegende Design-Voraussetzung für den Fluss-Steuerungsmechanismus von TCP.

Die Annahme einer stabilen Netzverbindung führt in einer Mobilfunkumgebung dazu, dass die Übertragungsbandbreite auf Grund der Fluss-Steuerung bisweilen nur sehr schlecht genutzt wird. Gerade in einem Szenario, in dem es auf Grund der Mobilität des Nutzers zu häufigen Störeinflüssen kommt, ist dieser Effekt spürbar. In einem rein stationären Umfeld ohne Mobilität des Nutzers arbeitet TCP in der Regel zufrieden stellend.

Das TCP ist ein verbindungsorientiertes Ende-zu-Ende Übertragungsprotokoll, das einen gesicherten Übertragungsdienst (reliable stream delivery[38]) über verschiedene Übertragungsnetze zur Verfügung stellt. Verbindungen über TCP werden mit Hilfe des "Three-Way-Handshake"-Algorithmus zwischen zwei als Port bezeichneten Endpunkten initiiert. Ein TCP-Port ist dabei eine Nummer auf dem initiierenden Rechner bzw. dem Zielrechner und bezeichnet dort jeweils eindeutig eine Anwendung.

Der "Three-Way-Handshake"-Algorithmus umfasst drei Nachrichten, mit denen Sender und Empfänger die Startparameter einer Verbindung wie

[38] reliable stream delivery: dt. zuverlässige Strom Lieferung...

- Port Number und
- Initial Sequence Number

vereinbaren. Daher dauert ein TCP Verbindungsaufbau ungefähr dreimal solange wie das augenblickliche Delay. Dies kann z.B. bei Dialog-Anwendungen in einer Mobilfunkumgebung ebenfalls bereits kritisch sein.

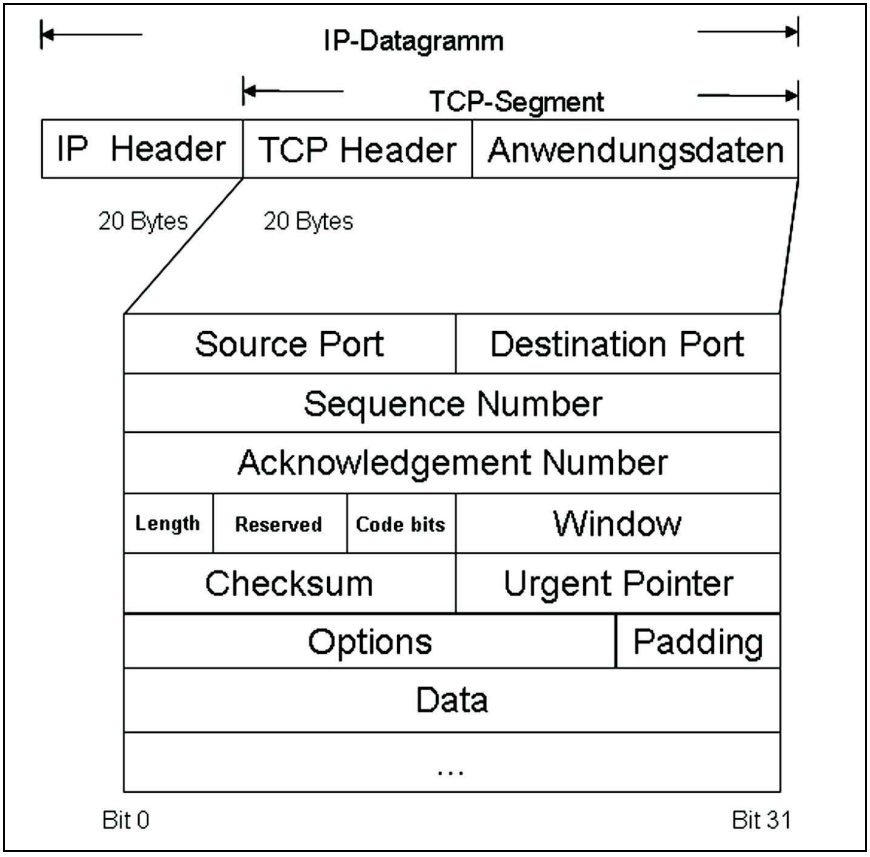


Abbildung 20: TCP-Segment im IP-Datagramm

Zur Übertragungssicherung sind in TCP im Wesentlichen folgende Mechanismen definiert:

- Paketfehlererkennung anhand einer Checksum (16 bit),
- Positive Quittierung empfangener Pakete (Positive Acknowledgement),
- Erkennen von Duplikaten anhand der Sequence-Number,
- Wiederholungen (Retransmission) bei Zeitüberschreitung (Timeout) der jeweiligen Quittung (ACK = Acknowledgement) oder beim Erkennen von Duplicate Acknowlegments,
- Sliding Window Technique,
- Congestion Avoidance and Slow Start und
- Selective Acknowledgement (SACK) Option.

Die Quittierung empfangener Segmente (Abbildung 20) wird von TCP implizit dadurch realisiert, dass der Empfänger in seinem Acknowledgement mit Hilfe der Acknowledgement-Number stets anzeigt, welches Segment er als nächstes erwartet. Hierdurch werden implizit alle vorangegangenen Segmente quittiert. Gleichzeitig kann der Sender anhand von duplizierten Acknowledgements mit identischer ACK-Number erkennen, ob Übertragungsfehler aufgetreten sind.

Da ein einfacher Quittierungsmechanismus in den meisten Fällen dazu führt, dass die zur Verfügung stehende Übertragungsbandbreite nur sehr schlecht genutzt würde, arbeitet TCP mit der so genannten "Sliding Window Technique" (Abbildung 21). Dabei werden hintereinander gleich mehrere Segmente übertragen, ohne dass eine Quittung empfangen werden muss. Die Größe des Senderfensters gibt dabei

an, wie viele dieser Segmente maximal übertragen werden, bevor die nächste Quittung durch den Empfänger vorliegt.

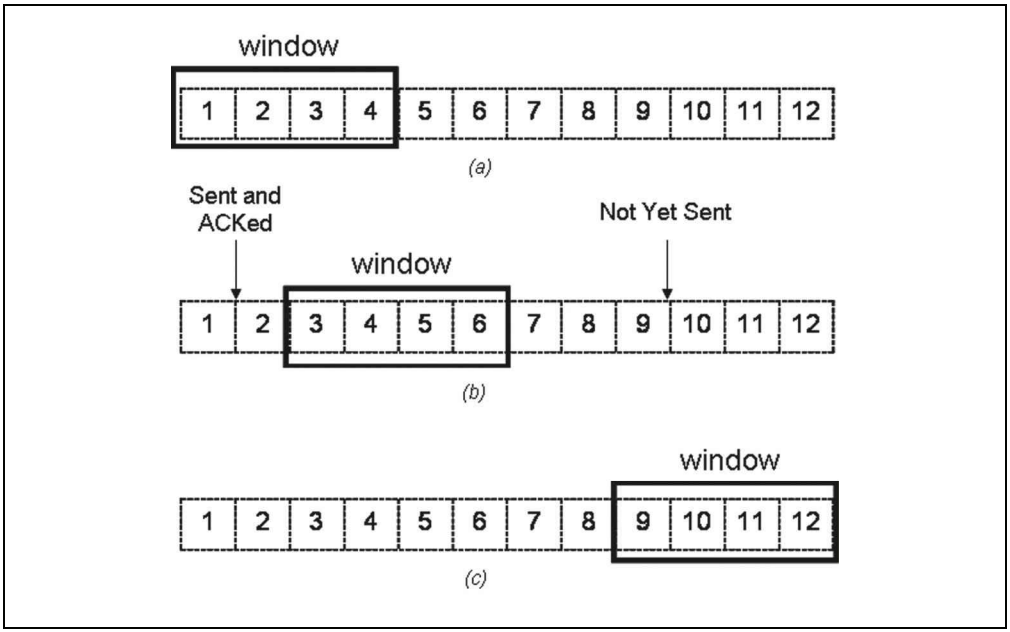


Abbildung 21: Sliding Window Algorithmus von TCP

Da TCP als Ende-zu-Ende-Protokoll über viele verschiedene Übertragungsnetzwerke definiert ist, wird die Fenstergröße des Senders von TCP dynamisch an die augenblickliche Übertragungsqualität angepasst. Dieser Mechanismus dient dazu, schnell Überlast-Situationen zu erkennen und entsprechend zu reagieren und wird daher als "Congestion Avoidance and Slow Start" bezeichnet. Das TCP verwaltet hierzu zwei Fenster, das

- Congestion Window, das vom Sender zur Fluss-Steuerung genutzt wird, sowie

- Advertised Receiving Window, mit dessen Hilfe der Empfänger angibt, wie viele Segmente er maximal hintereinander verarbeiten kann, bevor der Sender warten muss, bis er das nächste ACK empfängt.

Zu Beginn einer Verbindung sowie nach einer Überlast-Situation beträgt die Größe des Congestion Windows des Senders (Initial Window Size) in der Regel ein Segment. Danach befindet sich TCP zunächst in der Phase des Slow Start. In diesem Modus wird das Congestion Window für jedes implizit quittierte Segment um ein Segment erhöht und wächst somit exponentiell an. Sobald die Größe des Congestion Window einen bestimmten Schwellwert, den so genannten "Slow Start Threshold", erreicht hat, wechselt TCP in den Modus des Congestion Avoidance. In dieser Phase wird das Congestion Window mit jedem ACK nur noch um eins erhöht. Das Congestion Window kann jedoch niemals über das vom Empfänger vorgeschlagene (Advertised Receiving Window) hinaus anwachsen.

Überlast (Congestion) wird auf zwei Arten detektiert: Durch

- den Empfang von drei Duplicate Acknowledgements,
- das Retransmission Timeout (RTO-Timer).

In beiden Fällen wird der Slow Start Threshold auf die Hälfte seines aktuellen Werts eingestellt. Im zweiten Fall wird zusätzlich das Congestion Window auf den Wert 1 Segment zurückgesetzt. Mit diesem Verfahren kann sehr schnell auf eine Überlast reagiert werden. Dies ist entscheidend, um einen Kollaps des gesamten Netzes zu vermeiden.

Im ersten Fall, d.h. in der Regel nach dem Empfang von drei Duplicate Acknowledgements, wird nicht in den Slow-Start-Modus sondern in den Congestion-Avoidance-Modus umgeschaltet. Dieses Verfahren nennt man "Fast

Retransmit with Fast Recovery". Das Congestion Window wird dann also auch nicht auf den Wert von einem Segment sondern auf den Wert des Slow Start Threshold + 3 Segmentgrößen eingestellt. Das verlorene Segment wird anschließend erneut übertragen.

Für jedes weitere empfangene Duplicate ACK wird das Congestion Window um die Größe eines weiteren Segments erhöht. Trifft nun wieder ein reguläres ACK ein, wird das Congestion Window genau auf den Wert des Slow Start Thresholds eingestellt. Dieses empfangene ACK sollte nun die Quittung des erneut übertragenen Segments sein. Dieses ACK wird auch zusätzlich alle zwischenzeitlich empfangenen Datenpakete (die zwischen dem verlorenen Datenpaket und dem Empfang der drei Duplicate ACK empfangenen Pakete) quittieren.

Die Zeit zur Ermittlung eines Timeout wird anhand der fortlaufend gemessenen Retransmission Time (RTT) über eine gewichtete Mittelwertbildung bestimmt. Dabei wird jeweils die Zeit zwischen dem Versenden eines Segments und dem Empfang der zugehörigen Empfangsbestätigung gemessen und zur Anpassung des Retransmission Timer herangezogen.

In einer Mobilfunkumgebung, bei der es häufig zu längeren Unterbrechungen kommen kann und sich die Übertragungsgüte sowie das Delay auf Grund kurzfristiger Störeinflüsse auch mehrmals während einer TCP-Verbindung schlagartig ändern kann, führen diese adaptiven[39] Mechanismen zur Fluss-Steuerung bzw. zur Steuerung von Wiederholungen (Retransmission) häufig zu einer sehr schlechten Ausnutzung der zu Verfügung stehenden Bandbreite. Paketverluste werden im Mobilfunk hauptsächlich durch Bitfehler verursacht. Das TCP kann jedoch nicht die Ursache des Paketverlusts, Übertragungsfehler oder

[39] adaptiv: angepasst.

Netzwerküberlastung, unterscheiden. Es reagiert immer mit Überlastabwehr und reduziert sein Sendefenster. Große Laufzeitvariationen auf Grund von Paketwiederholungen auf LLC- bzw. RLC-Protokollebene (ARQ-Mechanismen) verursachen bei der Timeout-basierten TCP-Fluss-Steuerung (der Timeout-Wert wird geschätzt) große Leerlaufzeiten beim Sender (Abbildung 22).

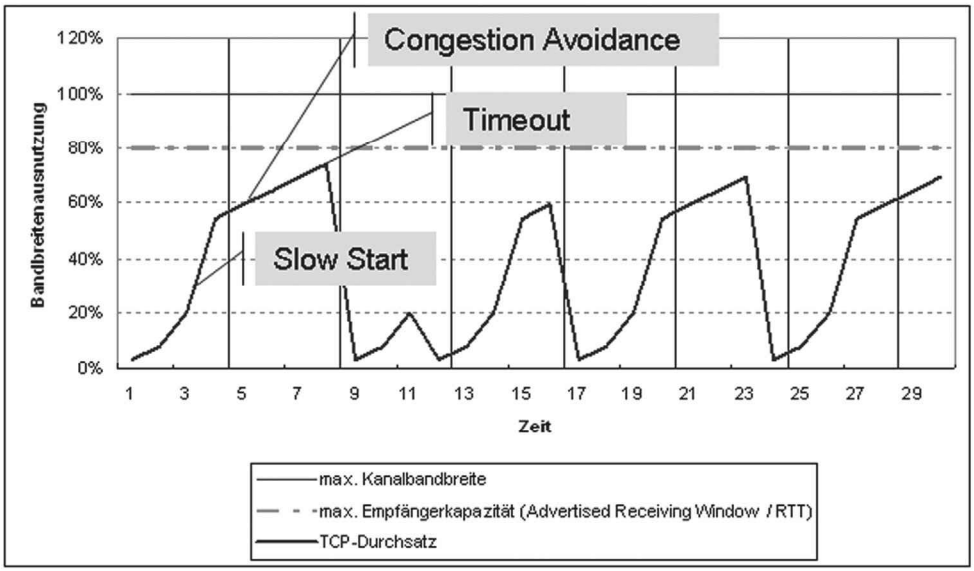


Abbildung 22: Ausnutzung der Bandbreite auf Grund der Fluss-Steuerung von TCP

Zu einer weiteren Verschlechterung des TCP-Durchsatzes kann die Strategie der exponentiellen Vergrößerung des RTO (exponentieller Backoff) führen. Wenn eine Paketwiederholung auf Grund eines abgelaufenen Timeout durchgeführt wird, wird der RTO bei TCP jeweils auf das Doppelte des bisherigen Timeout gesetzt. Gehen während einer temporären Störung auf der Funkstrecke mehrere aufeinander folgende Wiederholungen verloren, so wächst der Timeout schnell an. Wenn dann

die Störung beendet ist, vergeht so viel Zeit, bis die Übertragung wieder aufgenommen wird.

Der RTO Wert wird bei vielen Implementierungen mit einem Wert von drei Sekunden initialisiert. Treten auf dem Übertragungsweg regelmäßig längere RTT-Zeiten als drei Sekunden auf, empfiehlt es sich, den Initial-RTO-Wert entsprechend größer zu initialisieren.

Durch den Einsatz entsprechend proprietärer[40] Middleware lassen sich bereits heute einige dieser Probleme entschärfen.

2.2.8.4 Optimierungsmaßnahmen und Empfehlungen

Um den Anforderungen an ein Übertragungsnetz weitestgehend gerecht zu werden und die Performance von TCP in mobilen Datennetzen - wie beispielsweise GPRS - zu verbessern, gibt es eine Reihe von Empfehlungen und Optimierungsmöglichkeiten.

Auf Grund der vergleichsweise geringen Bandbreite eines mobilen Übertragungsdienstes besteht der einfachste Ansatz zur Performance-Steigerung darin, die zu übertragene Datenmenge zu komprimieren. Hier unterscheidet man Verfahren zur Komprimierung der Anwendungsdaten (z.B. HTML-[Hypertext Markup Language-]Seiten) sowie Header[41]-Komprimierungsverfahren, die den TCP- bzw. den IP-Header von insgesamt 40 Byte auf 3 Byte bis 5 Byte verringern und somit den Overhead reduzieren. Die IETF empfiehlt hierzu folgende Verfahren:

---

[40] proprietär: Engl. proprietary. Als Adjektiv verwendet, bezeichnet ”proprietär” in der Informations- und Telekommunikationstechnik in der Regel herstellergeprägte Entwicklungen, die keine Rücksicht auf Standardisierungen nehmen.

[41] Header: Kopfteil vorzugsweise asynchroner Übertragungsformate (Blöcke, Zellen, Pakete) mit administrativen Einträgen, wie Adressen, Prioritäten, Nachrichtentyp.

- Header Compression nach van Jacobsen RFC 1144,
- Payload[42] Compression entsprechend RFC 2393 (Framework).

Eine Header-Kompression nach RFC 1144 kann beispielsweise optional im Windows DFÜ-Netzwerk aktiviert werden. Da die PPP-Verbindung (Point-to-Point Protocol) bei GPRS bereits vom GSM-Endgerät terminiert wird, muss Header-Compression beim PDP[43]-Kontext-Aufbau durch das GSM-Endgerät explizit vom GPRS-Netz angefordert werden. Dabei kommt ebenfalls das Verfahren nach RFC 1144 zur Anwendung.

Als Payload-Komprimierungsverfahren lassen sich bewährte verlustlose Datenkompressionsalgorithmen verwenden wie z.B. PKZip oder GNUZip. Hier ist stets abzuwägen zwischen Kompressionsgüte und Kompressions-Geschwindigkeit, weil es sich bei diesem Einsatzbereich um eine Echtzeitumgebung handelt. Der Algorithmus GNUZip wird beispielsweise von allen Internet-Browsern ab HTTP Version 1.1 unterstützt, wobei die Steuerung durch einen Eintrag im HTTP Entity-Header (Content-Encoding) vorgenommen wird. Darüber hinaus gibt es die Möglichkeit, verlustbehaftete Algorithmen oder Filter einzusetzen. Beispielsweise kann man die Farbauflösung von Bildern in HTML-Seiten herabsetzen oder unnötige Banner-Werbung bzw. Kommentare herausfiltern.

Um den Protokoll-Overhead weiter zu reduzieren, sollte die maximale Segmentgröße (MTU = Maximum Transfer Unit) möglichst groß gewählt werden. Hier ist jedoch andererseits zu beachten, dass die Paketfehler-Wahrscheinlichkeit

---

42 Payload: In Kommunikationsprotokollen allgemein für den Inhalt (z.B. Nutz-/ Anwenderdaten) von Übertragungsrahmen (Block, Zelle, Paket).

43 PDP: Abk. für Packet Data Protocol.

sowie das Queueing[44]-Delay mit der Segmentgröße steigt. Durch den Einsatz von ARQ auf RLC-Ebene lässt sich die Paketfehlerwahrscheinlichkeit zwar reduzieren. Hierdurch verschlechtern sich jedoch die Delay- bzw. die Jitter-Werte ebenfalls proportional zur Segmentgröße. Gerade in Mobilfunknetzen mit kurzfristig hohen Bitfehler-Wahrscheinlichkeiten sowie geringen Bandbreiten ergibt sich hieraus eine Begrenzung für den Wert der MTU. Die IETF WG (work group) PILC empfiehlt, für die MTU einen Wert zu wählen, der einem Übertragungs-Delay von maximal 200 ms entspricht.

Beispiel:

GPRS, 2 Slot, CS-2: 20 kbit/s•200 ms = 512 Byte

Für die Wahl der MTU gilt andererseits jedoch:

Je kleiner die IP-Segmentgröße gewählt wird, desto größer fällt der durch die IP- und TCP-Header verursachte Protokoll-Overhead aus.

Je kleiner die IP-Segmentgröße gewählt wird, desto mehr RTT-Zeiten vergehen nach der Auslösung des TCP-Slow-Start-Algorithmus, bis die volle Kanalkapazität auf dem Übertragungsweg wieder erreicht werden kann.

Daher empfiehlt T-Mobile für die MTU allgemein für GPRS, UMTS und HSDPA einen Wert von 1500 Byte und damit einen höheren Wert als die WG PILC. Da Paketverluste auf Funkstrecken überwiegend durch Bitfehler verursacht werden, wächst die Wahrscheinlichkeit eines Paketverlustes proportional zu der Länge der Pakete. Im Falle eines Verlustes muss das gesamte Paket über den langsamen

[44] Queueing: Allgemein für zeitliche Verzögerung in Wartespeichern. In ATM-Systemen beispielsweise ist damit die Verzögerung gemeint, die entsteht, wenn eine Zelle im System zwischengespeichert werden muss, weil die Ressourcen für den Weitertransport der Zelle nicht vorhanden sind. Die Ursachen dafür können Überlastung des Links oder Zellen einer Verbindung höherer Priorität sein.

Funkkanal wiederholt werden. Mit Hilfe des RLC acknowledged mode kann dieser Effekt jedoch weitestgehend kompensiert werden, so dass sich hieraus für die Wahl einer höheren MTU tatsächlich keine Begrenzung ergibt.

Die adaptive Anpassung der Größe des Congestion Window sowie die Reaktion auf Paketverlust sind von großer Bedeutung für die Performance von TCP. Hier sind modifizierte Retransmission- und Congestion-Avoidance-Mechanismen erforderlich, um eine spürbare Verbesserung zu erzielen. Hieran wird derzeit im Rahmen der IETF gearbeitet. Proprietäre Middleware-Lösungen sind bereits verfügbar. Die IEFT WG pilc empfiehlt hierzu u.a., den Startwert für die Fenstergröße (Initial Congestion Window Size) auf zwei Segmente statt auf eins einzustellen.

Von entscheidender Bedeutung für die Performance von TCP ist zudem die Größe des TCP Receiving Windows, das bei Microsoft Windows standardmäßig auf 16 kByte eingestellt ist. Um über TCP jeweils die maximalen Übertragungs-geschwindigkeiten zu erzielen, empfiehlt T-Mobile in Abhängigkeit vom jeweils genutzten Übertragungsdienst folgende Einstellungen für das TCP Receiving Window:

Tabelle 5	Empfohlene TCP Fenstergrößen
Übertragungsdienst	TCP Receiving window size
GPRS	17520 Byte
EDGE	49640 Byte
UMTS	33580 Byte
HSDPA	64240 Byte

Sollte die Applikation verschiedene Übertragungsdienste nutzen so empfiehlt sich ein Wert von 32 kByte.

Es gibt zwei Möglichkeiten, den Wert für das TCP Receiving Window unter Microsoft Windows Betriebssystem zu verändern (Quelle: MSDN library):

- Entweder durch direktes Editieren des Parameters TcpWindowSize in der Registry, z.B. mit Regedit32.exe, als globale Änderung oder
- durch Aufruf der Windows Sockets Funktion setsockopt() als Änderung für die betreffende Socket bzw. TCP-Verbindung.

Die Funktion setsockopt() ist Bestandteil der Socket[45] API des Betriebssystems und wird dazu benutzt, die Werte für verschiedene Socket-Optionen für eine bestimmte Socket zu verändern.

Hinweis: Eine fehlerhafte Änderung von Registry-Parametern kann im schlimmsten Fall zu einem Systemabsturz führen. Es wird daher dringend empfohlen, vor jeder Änderung eine Sicherheitskopie der Registry zu erstellen. Änderungen an den TCP/IP Einstellungen können die Performance von TCP stark beeinflussen.

Sollte die Applikation verschiedene Übertragungsdienste nutzen so empfiehlt sich ein Wert von 32 kByte.

Weitere Maßnahmen sind:

- Vermeidung von Retransmission auf Anwendungsebene (z.B. FTP) auf Grund von plötzlichen Unterbrechungen durch Einsatz einer Middleware,
- Vermeidung von unnötigem Verkehr (z.B. "Keep-Alive-Meldungen" zwischen Client und Server) durch "Spoofing" und „Caching" in der Middleware. Viele Standardanwendungen wurden für eine LAN- bzw.

[45] Socket, englisch für Fassung, Steckdose, ist eine Bezeichnung für eine Programmierschnittstelle (API) des Betriebsystems zur Nutzung von TCP/IP.

Festnetzumgebung entwickelt, in der es keine Bandbreitenbegrenzung gibt, und zeichnen sich daher durch ein extensives Kommunikationsverhalten (z.B.: Polling, Übertragung redundanter Daten, ineffiziente Dialoge) aus, das in einer Mobilfunkumgebung sehr ineffizient ist und zu einer schlechten Performance führt.

- Vermeidung von TCP-Aufbauzeiten durch Einsatz von "Persistenten TCP-Verbindungen" (ab HTTP Version 1.1),
- Vermeidung von Wartezeiten beim HTML-Seitenaufbau durch "Request-Pipelining" (ab HTTP Version 1.1)

2.3 Sicherheit

Computerviren und –Würmer tauchen zunehmend auch in Mobilfunkdiensten und –Netzen auf und werden zu einer nicht zu unterschätzenden Bedrohung. Ein Beispiel dafür ist der Computerwurm CommWarrior, der sich seit März 2005 über einen Mobilfunkdienst verbreiten kann. Neben Antivirenprogrammen ist insbesondere ein ausgeprägtes Sicherheitsbewusstsein bei den Anwendern notwendig, um ein hohes Sicherheitsniveau zu erreichen. Deshalb sollten Schutzmaßnahmen beispielsweise im Umgang mit Bluetooth, unbekannter Software, zweifelhaften Internetseiten oder E-Mails sowie WLAN- und Infrarot-Schnittstellen getroffen und beachtet werden.

Mobile Endgeräte sind heute für die unterschiedlichsten Anwendungen erhältlich. Beispielsweise besitzt ein Notebook eine Vielzahl von Schnittstellen, die neben der Tastatur und dem Display auch Anschlüsse zu den verschiedenen Mobilfunknetzen, dem Festnetz aber auch insbesondere in Firmennetze zulassen. Deshalb kommt der Sicherheit, der mobile Security, eine herausragende Bedeutung zu. Die Bedrohung durch Computerviren und Spams hat in den letzten Jahren deutlich zugenommen. Seit Ende 2004 sind in der Fachwelt auch die ersten Viren und/oder Würmer für Mobilfunkendgeräte bekannt. Bisher sind die einzelnen Handy-Viren jedoch noch sehr einfach und können sich nur im begrenzten Umfang verbreiten. Ein wirkungsvoller Schutz kann nur unter Mitwirkung aller Beteiligten erzielt werden.

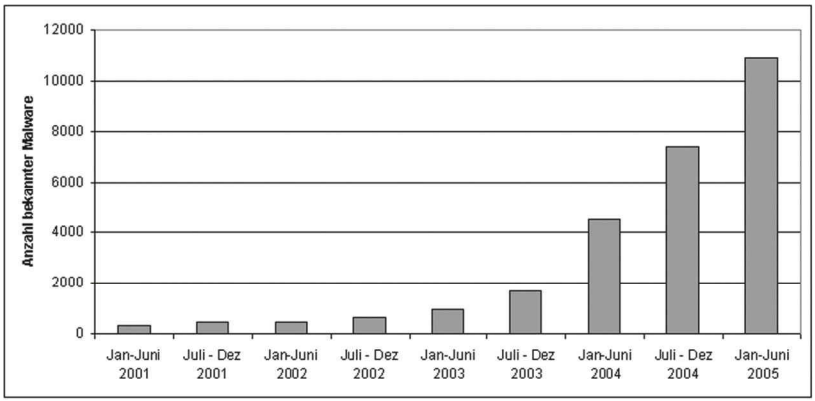
2.3.1 Ausgangslage

Tabelle 6	Auswahl bekannter Viren und Würmer für Mobilfunkendgeräte		
Datum	Virus	Plattform	Aktivität
15.06.04	Cabir	Symbian Series 60	Proof of Concept, Weiterverbreitung nur über Bluetooth, fester Dateiname caribe.sis
17.07.04	Duts	Windows Pocket PC	Proof of Concept, infizierte Dateien auf Device, keine automatische Weiterleitung
06.08.04	Brador	Windows Pocket PC, Mobile 2003 (Windows CE 4.2)	Proof of Concept; manuelle Verbreitung über E-Mails, Backdoor-Trojaner ermöglicht dem Hacker volle Kontrolle über das infizierte Endgerät
19.11.04	Skulls	Symbian Series 60, Series 80	Trojaner; ersetzt alle Applikations-Icons durch Totenköpfe und deaktiviert die Verknüpfung zu den ursprünglichen Anwendungen, so dass nur Telefonieren möglich ist; keine selbst-ständige Verbreitung
01.02.05	Gavno Locknut.A)	Symbian Series 60	Trojaner, der vorgibt, ein Patch für das Betriebssystem zu sein und der Teile des Betriebssystems überschreibt und somit das Gerät unbrauchbar macht
07.03.05	Comm-Warrior	Symbian Series 60	Trojaner, Phone Reset (auf spezielles Datum hin), versendet sich über MMS und Bluetooth; dabei benutzt die Variante C zufällige Dateinamen

Die ersten Computerviren für Mobilfunkendgeräte sind in der Fachwelt seit Ende 2004 bekannt (Tabelle 6). Davon sind aber nur wenige im Umlauf. Bei den meisten handelt es sich lediglich um Fallstudien (Proof of Concept). Im März 2005 tauchte jedoch unter der Bezeichnung CommWarrior zum ersten Mal ein Computerwurm auf, der Mobilfunkendgeräte mit offenen Betriebssystemen[46] wie SmartPhones oder Personal Digital Assistants (PDAs) befällt und sich mittels

[46] Offenes Betriebssystem: engl. Open Source, eine Software, deren Quellcode frei zugänglich ist.

Multimedia Messaging Service (MMS) sowie über Bluetooth[47] selbstständig verbreitet.



Quelle: Symantec Internet Security Report, September 2005

Abbildung 23: Bedrohung durch Viren, Würmer und Trojaner in der PC-Welt

Während schadhafte Computerprogramme (Malware) wie Viren, Würmer oder Trojaner[48] aus der PC-Welt schon seit vielen Jahren bekannt sind und sich der Anwender der damit verbundenen Gefahren bewusst ist, sind Computerviren im Mobilfunk in der Öffentlichkeit noch weitgehend unbekannt. Mit der zunehmenden Verbreitung von SmartPhones und PDAs sowie der steigenden Nutzung leistungsstarker mobiler Datendienste wie MMS, General Packet Radio Service (GPRS), Universal Mobile Telecommunications System (UMTS) oder High Speed Data Packet Access (HSDPA) wird sich die Bedrohungslage und damit auch das Problembewusstsein nachhaltig verändern.

---

47 Nahbereichsfunkstandard, IEEE 802.15.1; Siehe hierzu den Beitrag "Bluetooth - ein neuer Funkstandard", Unterrichtsblätter, Nr. 6/2000, s. 276 ff.

48 Siehe hierzu den Beitrag „Computerviren – Vom Ärgernis zur ernsten Bedrohung“, WissenHeute,Nr. 8/2004, S. 420 ff.

Nach der Untersuchung eines Herstellers von Antiviren-Software[49] wurden bereits im ersten Halbjahr 2005 knapp 11 000 verschiedene Viren, Würmer oder Trojaner registriert (Abbildung 23). Dies ist eine Zunahme von ungefähr 175 Prozent innerhalb eines Jahres. Gleichzeitig ist zu erkennen, dass sich der Schwerpunkt der Hacker mehr und mehr in den kriminellen Bereich verlagert. Ging es in der Vergangenheit überwiegend um Motive wie Selbstbestätigung oder Experimentierfreude, so stehen heute eindeutig finanzielle Absichten im Vordergrund. Es geht beispielsweise um Ausspähen sensibler Daten, Erschleichung von Diensten oder um die Nutzung von Bezahldiensten (z.B. 0190-Nummern) ohne Einwilligung des Geschädigten. Betrachtet man die Faktoren, die diese Entwicklung ermöglicht haben, so stößt man auf drei Grundvoraussetzungen:

- Vormachtstellung eines einzigen offenen Betriebssystems im PC-Umfeld
- hohe Verbreitung von PCs
- starke Nutzung von Breitband-Internet

Im Mobilfunkbereich sind diese Voraussetzungen für eine große Verbreitung von Malware zur Zeit noch nicht erfüllt. Eine klare Dominanz eines Betriebssystems ist nicht erkennbar; PDAs mit Microsoft Windows Mobile und SmartPhones mit Symbian-Betriebssystem sind ungefähr in gleichen Anteilen verbreitet. Zusammen machen PDAs und SmartPhones noch immer den kleineren Teil aller in Einsatz befindlichen Mobilfunkendgeräte aus. Dabei steht die Entwicklung mobiler Datenkommunikation erst am Anfang. Vergleicht man die aktuelle Zahl der bekannten Malware-Varianten für Mobilfunkendgeräte (Abbildung 24) mit den Zahlen aus der PC-Welt, so kann vermutet werden, dass die Entwicklung im

[49] Symantec Internet Security Report, September 2005.

Mobilfunkbereich auch hier ungefähr fünf Jahre hinter der Entwicklung im PC-Bereich zurückliegt. Die Zahl der bekannten Viren, Würmer und Trojaner in allen Varianten für Mobilfunkgerät lag nach einer Erhebung von F-Secure im Juli 2006 bei ungefähr 320.

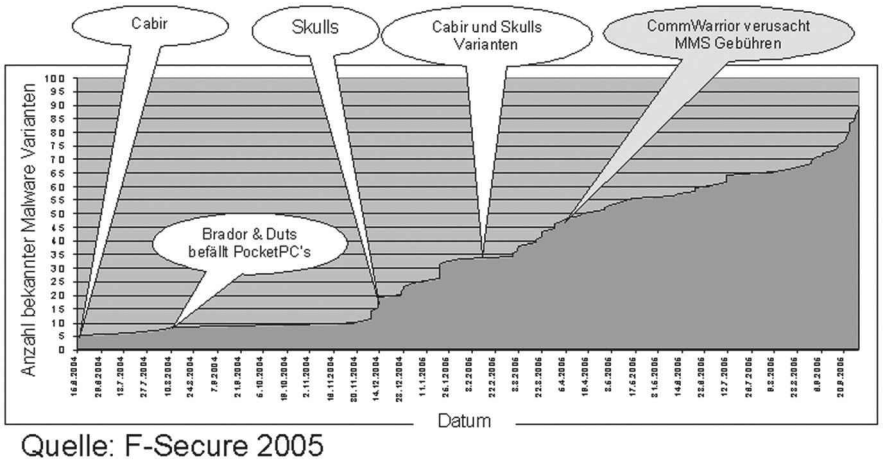


Abbildung 24: Bedrohung durch Viren, Würmer und Trojaner für Mobilfunkgeräte

2.3.2 Leistungsumfang heutiger PDAs und SmartPhones

Aufgrund des leistungsstarken und reichhaltigen Funktionsumfangs, der offenen Betriebssysteme sowie der zunehmenden Vernetzung über nahezu alle Kommunikationsmöglichkeiten sind SmartPhones und PDAs potenzielle Ziele für Angriffe jedweder Art. Zum Standardfunktionsumfang heutige SmartPhones und PDAs gehören unter anderem Dienste und Anwendungen wie:

- Short Message Service (SMS),
- MMS,

- E-Mail,
- Web-Browsing und
- GPRS, UMTS, HSDPA.

Hinzu kommen Schnittstellen für Nahbereichstechniken wie:

- Wireless Local Area Network (WLAN),
- Bluetooth,
- IrDa[50]
- Universal Serial Bus (USB).

Zudem können große Datenmengen und Anwendungen leicht über externe Speicherkarten ein- und ausgelesen werden.

Handy-Viren können sich über alle genannten Dienste und Schnittstellen verbreiten und in das Endgerät eindringen. Ohne ein allgemeines Problembewusstsein der Benutzer, wie es im PC-Bereich bereits vorhanden ist, wird einer ungehinderten Verbreitung von Handy-Viren nur schwer zu begegnen sein.

[50] IrDa: Abk. Infrared Data Association; Protokollarchitektur für die optische Infrarot-Datenübertragung im Kurzstreckenbereich (z.B. bei Notebooks).

2.3.3 Bedrohungsanalyse

Die Bedrohung durch schadhafte Programme betrifft sämtliche Beteiligte der Wertschöpfungskette (Abbildung 25):

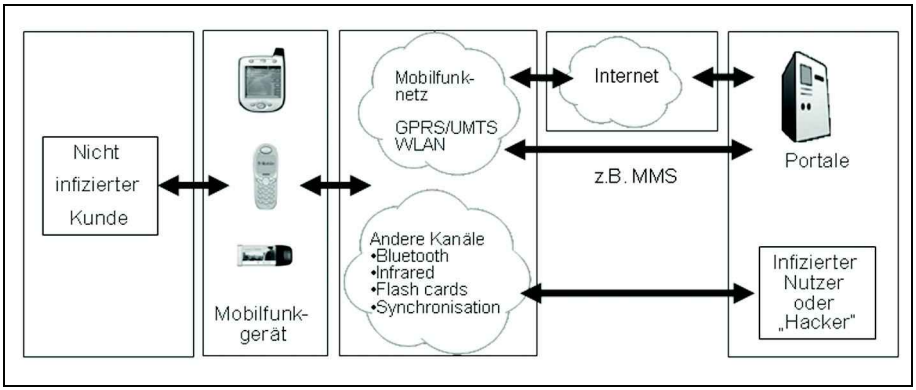


Abbildung 25: Akteure und Verbreitungswege für Handy-Viren

- Bedrohung für den Kunden: Unerwartete Kosten; Belästigung; Ausspähen, Verändern oder Löschen sensibler Daten; eingeschränkte Nutzbarkeit des Endgerätes oder des Mobilfunkdienstes; Beschädigung der persönlichen Reputation bei Weitergabe von Malware.
- Bedrohung für den Mobilfunkbetreiber: Image-Schaden; Umsatzeinbuße; Verschlechterung der Dienstqualität und erhöhte Kosten im Service.
- Bedrohung für den Endgerätehersteller: Image-Schaden; Umsatzverlust.
- Bedrohung für den Software-Entwickler bzw. Anwendungs-Provider: Misstrauen gegenüber neuen Anwendungen.

Die Hauptmissbrauchsfälle sind:

- Unberechtigte Nutzung von Telefondiensten, Nachrichtenversand (SMS, MMS) und Datenverbindungen (GPRS, UMTS; HSDPA);
- Verletzung von Datenintegrität bzw. Ausspähen sensibler Daten;
- Zugriff auf kritische Ressourcen der SIM-Karte[51] (z.B. Deaktivierung durch mehrfache Falscheingabe von PIN/PUK)[52];
- Missbrauch von Zugriffsrechten und Erschleichung von kostenpflichtigen Diensten;
- Mithören von empfangenen oder gesendeten Daten;
- Weitergabe von Malware;
- Einschränkung der Nutzung.

Die bis heute bekannten Malware-Varianten beschränken sich überwiegend auf das Betriebssystem Symbian Series 60; Microsoft-Betriebssysteme sind jedoch grundsätzlich mindestens ebenso gefährdet. Die sehr kurzen Produktlebenszyklen verschärfen die Situation zusätzlich, weil hierdurch Sicherheitslücken im Betriebssystem wahrscheinlicher werden, die von Malware gezielt ausgenutzt werden können. Handy-Viren können grundsätzlich über alle Medien verbreitet werden. Hierzu zählen unter anderem:

- Nahbereichstechniken wie Bluetooth, IrDA oder WLAN,
- Nachrichtendienste wie MMS, Instant Messaging oder E-Mail,

[51] SIM-Karte: Abk. Subscriber Identity Module; Chipkarte, die in Mobilfunktelefonen benutzt wird und für deren Betrieb zwingend erforderlich ist. Sie ordnet dem Mobiltelefon eine Rufnummer und einen Mobilfunkbetreiber zu.

[52] PUK: Abk. Personal Unblocking Key, dt. Persönlicher Entsperrcode; im Mobilfunksystem ein achtstelliger Sicherheitsschlüssel zum Entsperren einer durch Falscheingabe der Personal Identification Number (PIN) gesperrten SIM-Karte.

- Internetverbindungen (z.B. Web Download) oder
- externe Speicherkarten.

Da die derzeit bekannten Handy-Viren wie z.B. Cabir oder CommWarrior zur Verbreitung meist die Bluetooth-Schnittstelle nutzen, wird im Folgenden hierauf besonders eingegangen.

Die Bluetooth-Übertragungstechnik ist inzwischen sehr verbreitet, ohne dass den meisten Nutzern das damit verbundene Sicherheitsrisiko[53] bewusst ist. Bluetooth ist eine Technik zur kabellosen Vernetzung mehrerer Consumer-Endgeräte im Nahbereich bis etwa 10 m Abstand an einen Master ([21]). Überall, wo bisher im unmittelbaren Nahbereich Kabel notwendig war, kann heute Bluetooth zum Einsatz kommen, beispielsweise für Verbindungen wie:

- Handy-zu-PC,
- Freisprecheinrichtung/Headset-zu-Handy,
- PDA/Notebook-zu-PC,
- Handy-zu-Handy,
- PC-zu-Drucker,
- Digitalkamera-zu-PC,
- Handy im Auto oder
- HiFi-zu-Multimedia-PC.

[53] Siehe hierzu den Beitrag „Sicherheitsaspekte beim Bluetooth-Standard“, WissenHeute, Nr. 8/2006, S. 425 ff.

Ein sehr häufiger Anwendungsfall ist der Einsatz von Bluetooth für Freisprecheinrichtung (Headset). Auch für Spiele und Musik wird Bluetooth immer beliebter.

Vielen Anwendern ist jedoch nicht immer bewusst, dass eine dauerhaft aktive Bluetooth-Schnittstelle die Gefahr eines Viren-Befalls oder des Auslesens persönlicher Daten mit sich bringt. Die Sorglosigkeit der Anwender wird bereits von Werbeagenturen ausgenutzt, die an stark frequentierten zentralen Plätzen Bluetooth-Sender für Werbeeinspielungen aufstellen. Erste Erfahrungen mit dieser „neuen" Werbemethode haben gezeigt, dass sehr viele Handy-Besitzer ständig ihre Bluetooth-Schnittstelle aktiviert halten und ein erschreckend hoher Anteil die unbekannten Werbeeinspielungen akzeptieren und auf ihr Endgerät laden. Bei ersten Feldversuchen im September letzten Jahres wurden innerhalb von 18 Tagen insgesamt 26 205 Passanten mit einer offenen Bluetooth-Schnittstelle gezählt; davon akzeptierten fast fünf Prozent die Werbeeinspielung.

2.3.4 Beispiel CommWarrior

Der MMS-Wurm CommWarrior tauchte zum ersten Mal im März 2005 auf und ist der erste Wurm, der sich über einen Mobilfunkdienst verbreiten kann. Von dem MMS-Wurm CommWarrior sind verschiedene Varianten bekannt. Allen Varianten ist gemeinsam, dass sie sich per Bluetooth oder MMS verbreiten und vor der Installation ausdrücklich vom Benutzer bestätigt werden müssen. Eine Schadfunktion enthält CommWarrior nicht, er versucht lediglich weitere Handys zu infizieren. Dazu versendet er zeitlichen Abstand von etwa 31 Minuten eine Nachricht mit Anhang an sämtliche Kontakte, die er im Adressbuch findet. Nach der Installation laufen alle Varianten vom Nutzer unbemerkt im Hintergrund. Dabei wählen sie in den Kontakten zufällige Mobilfunkrufnummern aus und verschicken sich selbst als Anhang von MMS-Mitteilungen an die entsprechenden Empfänger. Um eine weite Verbreitung des CommWarriors zu verhindern, werden derart infizierte MMS-Nachrichten jedoch von den meisten Mobilfunknetzen abgewiesen und der Kunde erhält eine Fehlermeldung „"Message sending failed!".

Wenn andere Handys in der näheren Umgebung mittels Bluetooth erreichbar sind, versucht der CommWarrior, eine Verbindung zu diesen herzustellen und sich selber an diese Endgeräte zu übertragen. Für die Herstellung einer Bluetooth-Verbindung muss üblicherweise beim empfangenden Handy der Aufbau der Verbindung vom Nutzer akzeptiert werden. Daher sollte der Benutzer darauf achten, dass er keine Bluetooth-Verbindung von unbekannten Nutzern akzeptiert. Problematisch wird es, wenn sich der Wurm permanent mittels Bluetooth verschickt, weil das „Opfer" in diesem Falle so lange mit Anfragen „bombardiert" wird, bis es entweder die Installation akzeptiert oder die Bluetooth-Verbindung deaktiviert.

Infizierte MMS-Nachrichten enthalten Texte wie sie im Kasten beispielhaft aufgeführt sind.

Tabelle 7: CommWarrior Nachtichtentexte[54]

- Norton AntiVirus Released now for mobile, install it!
- Dr.Web New Dr.Web antivirus for Symbian OS. Try it!
- MatrixRemover Matrix has you. Remove matrix!
- 3DGame 3DGame from me. It is FREE !
- MS-DOS MS-DOS emulator for SymbvianOS. Nokia series 60 only. Try it!
- PocketPCemu PocketPC *REAL* emulator for Symbvian OS! Nokia only.
- Nokia ringtoner Nokia Ringtone Manager for all models.
- Security update #12 Significant security update. See www.symbian.com
- Display driver Real True Color mobile display driver!
- Audio driver Live3D driver with polyphonic virtual speakers!
- Symbian security update See security news at www.symbian.com
- SymbianOS update OS service pack #1 from Symbian inc.
- Happy Birthday! Happy Birthday! It is present for you!
- Free SEX! Free *SEX* software for you!
- Virtual SEX Virtual SEX mobile engine from Russian hackers!
- Porno images Porno images collection with nice viewer!
- Internet Accelerator Internet accelerator, SSL security update #7.
- WWW Cracker Helps to *CRACK* WWW sites like hotmail.com
- Internet Cracker It is *EASY* to *CRACK* provider accounts!
- PowerSave Inspector Save you battery and *MONEY*!
- 3DNow! 3DNow!(tm) mobile emulator for *GAMES*.
- Desktop manager Official Symbian desktop manager.
- CheckDisk *FREE* CheckDisk for SymbianOS released!MobiComm

[54] Quelle F-Secure. Die Schreibfehler entstammen den Original-Nachrichten

2.3.5 Schutzmaßnahmen

Unstrittig ist, dass sich die Bedrohungslage im Mobilfunkbereich weiter verschärfen wird. Unklar ist jedoch, ab wann die Bedrohung zu einem ernsten Problem werden kann. Zwar ist bis heute mit dem MMS-Wurm CommWarrior nur ein einziger Malware-Typ bekannt geworden, der sich in begrenzten Rahmen selbstständig verbreitet. Die Bedrohungen durch Viren und Spams werden in der Fachwelt dennoch Ernst genommen. Bereits heute haben beispielsweise Kunden von T-Mobile die Möglichkeit, über T-Zones einen Antiviren-Client für SmartPhones oder ihren PDA zu beziehen.

Um allerdings ein möglichst hohes Sicherheitsniveau zu erzielen, reichen isolierte Einzelmaßnahmen auf Dauer nicht aus. Vielmehr ist ein Maßnahmenbündel unter Einbeziehung sämtlicher Beteiligten einschließlich des Kunden, Hersteller, Mobilfunkbetreiber und Softwareentwickler notwendig.

An vorderster Stelle steht der Anwender: Beim Empfang einer Nachricht z.B. über Bluetooth und vor jeder Software-Installation wird er um Zustimmung gefragt. Wie im PC-Bereich, muss er sich der zunehmenden Bedrohung bewusst sein und folgende Grundregel beachten:

- Niemals neue Software unbekannter Herkunft installieren. Selbst wenn, wie im Falle des CommWarriors, die Absenderadresse bekannt ist, sagt dies nichts über die tatsächliche Herkunft der Software aus. Im Zweifel sollte beim vermeintlichen Absender nachgefragt werden, ob die Software tatsächlich unbedenklich ist.
- Niemals Software von einer zweifelhaften Internetseite herunterladen.

- Bluetooth-, WLAN- oder IrDa-Schnittstelle nur dann aktivieren, wenn sie auch tatsächlich benötigt wird und deaktivieren, wenn sie nicht mehr benötigt wird.
- Bluetooth-, WLAN- oder IrDa-Schnittstelle so konfigurieren, dass diese für andere Personen unsichtbar ist.
- Keine Bluetooth-, WLAN- oder IrDa-Verbindungen von unbekannten Gegen-Stellen akzeptieren.
- Nutzung von WLAN-Verschlüsselung (z.B. WEP[55] oder WPA[56]).
- Den Zugang zum Endgerät mittels Kennwort schützen.
- Sicherheitsregeln bei der Wahl der Kennwörter beachten.
- Kennwörter niemals zusammen mit dem Gerät ablegen.
- Nutzung von Verschlüsselungssoftware zum Speichern sensibler Daten auf dem Endgerät.

Darüber hinaus sind die Hersteller in der Pflicht, Mobilfunkendgeräte mit einer Sicherheitsarchitektur (Security Framework) auszustatten, die unter anderem folgende Grundanforderungen erfüllt:

- Installation von Software nur mit Zustimmung des Benutzers.
- Unterstützung von Zertifikaten, die den Ursprung einer neuen Software eindeutig authentisiert.

---

55 WEP: Abk. Wired Equivalent Privacy; im Standard IEEE 802.11 spezifizierter Verschlüssungsdienst, der die Vertraulichkeit der übertragenen Daten gewährleisten soll.

56 WAP: Abk. Wi-Fi Protected Access; Vorgriff auf den offiziellen Sicherheitsstandard IEEE 802.11i; entwickelt von der Industrievereinigung WiFi Alliance.

- Schutz kritischer Systemressourcen (z.B. SIM-Karte, Adressbuch oder Nachrichtenversand) vor Zugriff durch nicht zertifizierte Anwendungen.
- Unterstützung von Möglichkeiten zur nachträglichen Aktualisierung des Betriebssystems.

Der Softwareentwickler steht in der Verantwortung, seine Software zertifizieren zu lassen, um es dem Anwender zu ermöglichen, den Ursprung der Software vor einer Installation zweifelsfrei erkennen zu können.

Der Mobilfunkbetreiber ist gefordert, eine grundlegende Sicherheitsarchitektur bei seinen Lieferanten einzufordern und seinen Kunden Endgeräte mit einem hohen Sicherheitsniveau bereitzustellen. Als kundenorientierter Dienstleister wird der Mobilfunkbetreiber darüber hinaus bestrebt sein, seine Kunden maximal zu unterstützen und einer massiven Verbreitung von Malware über sein Mobilfunknetz entgegenzutreten. Hierzu zählt die Bereitstellung von leistungsstarker Antiviren-Software sowie kompetente Hilfestellung über Customer Care sowie Internet. Schon jetzt stellt T-Mobile über T-Zones (**http://pfw.t-zones.de/**) unter dem Menüpunkt „Downloads" eine Antiviren-Software für verschiedene SmartPhones zum direkten download bereit (SmartPhone-Typ auswählen und Suchbegriff „Antivirus" eingeben).

2.3.6 Zusammenfassung

Die Bedrohung durch schadhafte Computerprogramme (Malware) für Mobilfunkgeräte wird in den kommenden Jahren weiter zu nehmen. Das Bedrohungspotenzial ist jedoch heute noch sehr gering, weil die Voraussetzungen für eine massenhafte Verbreitung von Malware noch nicht erfüllt sind. Mobilfunkbetreiber und Endgerätehersteller arbeiten bereits gemeinsam an Maßnahmen, um dieser Entwicklung entgegenzuwirken. Um ein hohes Sicherheitsniveau zu erzielen, sind die Mitwirkung der Kunden und deren Problembewusstsein von entscheidender Bedeutung.

2.4 Zugangslösungen auf Basis verschiedener VPN-Konzepte

2.4.1 Einführung

Virtuelle Private Netze (VPN) werden eingesetzt, um entweder geographisch verteilte Standorte eines Unternehmens bzw. einer Organisation mit einander zu verbinden oder den Mitarbeitern eines Unternehmens eine kontrollierte Einwahl ins interne Unternehmensnetz zu ermöglichen. Im ersten Anwendungsfall spricht man von „Branch-Office VPN". Einwahllösungen werden dagegen mit „Dial-In VPN" bezeichnet. Ein Spezialfall sind so genannte Extranet-VPNs, die im Gegensatz zu Branch-Office VPNs dazu genutzt werden, Standorte unterschiedlicher Organisationen miteinander zu vernetzen.

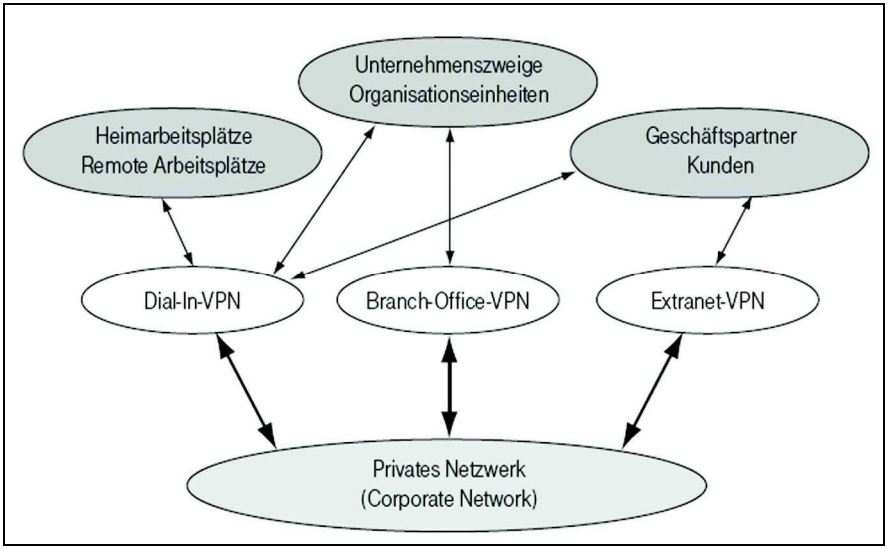


Abbildung 26: VPN Einsatzfelder

Solche Netze sind "privat", da sie nur von dem jeweiligen Unternehmen oder der jeweiligen Organisation selber genutzt werden können bzw. sollen. Sie bieten somit einen Schutz vor unbefugten Zugriff, wodurch ein Mitlesen, Manipulieren, Einschleusen von fremden Daten oder Attacken verhindert werden soll. VPNs sind daher durch eine Sicherheitsregelwerk (Policy) definiert, das genau festlegt, wer in welcher Form und unter welchen Bedingungen Zugang zu den Ressourcen im jeweiligen Unternehmensnetz haben soll.

Der praktische Nutzen eines VPN liegt darin, dass die genannten Sicherheitsanforderungen bereits auf unterer Netzebene umgesetzt werden und sich die Anwendungen bzw. die einzelnen Nutzer um derartige Sicherheitsfragen nicht sorgen müssen. Ein praktisches Beispiel ist der Versand vertraulicher Informationen per Email zwischen zwei Unternehmensstandorten. Sofern die Verbindung zwischen diesen Standorten über ein VPN realisiert ist, muss der jeweilige Anwender keine besonderen Verfahrensweisen beachten. Er verschickt die Email, als befände sich der Empfänger im gleichen lokalen Netz. Sind die beiden Standorte jedoch ohne VPN nur über das öffentliche Internet mit einander verbunden, so müssen die Information vor dem Versand durch eine aktive Handlung des Benutzers z.B. mit Pretty Good Privacy (PGP)[57] verschlüsselt und signiert werden, um den nötigen Schutz zu gewährleisten.

Ursprünglich wurden standortübergreifende Unternehmensnetze (CN: corporate networks) mit Hilfe von Mietleitungen realisiert. Dies hatte zur Folge, dass teure Übertragungskapazitäten exklusiv für das jeweilige CN vorgehalten wurden, ohne dass sie auch zu jeder Zeit maximal ausgelastet werden konnten. Daher kamen in

[57] Pretty Good Privacy: PGP ist ein frei verfügbares Verfahren (Anwendungsprogramm) zur Verschlüsselung von Daten, das insbesondere beim Datenaustausch über E-Mail weit verbreitet ist. Es handelt sich um ein Public-Private-Key-Verfahren, das mit einem Schlüsselpaar aus einem öffentlichen und einem privaten Schlüssel arbeitet.

der Folge vermittelte Datennetze zunächst auf der Basis von X.25, später dann basierend auf Frame Relay oder ATM, zum Einsatz, bei denen anstelle von physikalischen Mietleitungen zwischen den einzelnen Standorten virtuelle Kanäle auf der Datenvermittlungsplattform eines Dienstleisters (VPN Service Provider) konfiguriert werden.

Derartige vermittelte Unternehmensnetze sind somit "virtuell", da Einrichtungen und Übertragungskapazitäten, die zum Aufbau und zum Betrieb dieser Netze notwendig sind, für mehrere VPNs gleichzeitig genutzt werden, ohne die Trennung bzw. ihre grundlegende Sicherheit dieser Netze aufzuheben.

Mit der Verbreitung der Internet-Technologie kamen in der Folge zunehmend IP basierte VPNs (IP-VPNs) zum Einsatz, bei denen anstelle virtueller Verbindungen auf Schicht 2 des OSI Modells so genannte Tunnel-Verbindungen eingerichtet werden.

Häufig werden hierfür die Tunnel-Protokolle GRE[58] oder IPSec (Schicht 3) bzw. L2TP oder PPTP (Schicht 2) eingesetzt. PPTP sowie L2TP werden in der Regel für Dial-In VPNs genutzt (siehe unten). Als Transportplattform wird das weltweite Internet oder eine spezielle IP-Plattform eines VPN-Providers genutzt. Darüber hinaus haben sich z.B. mit SSL (Secure Sockets Layer) auf Schicht 4 des OSI-Modells im Internet noch weitere Technologien etabliert, mit denen sich ein gesicherter Datenaustausch realisieren lässt. Diese Lösungen können jedoch nur für bestimmte Anwendungen (z.B. Browsing) genutzt werden. Abbildung 27 zeigt eine Übersicht verschiedener VPN-Technologien und deren Einordnung im OSI-Modell.

[58] GRE: Generic Route Encapsulation – Ein von Cisco entwickeltes, weit verbreitetes Tunnel-Verfahren.

OSI-Schicht	VPN-Protokoll
Transport (Schicht 4)	■ Secure Socket Layer (SSL)
Netzwerk (Schicht 3)	■ IP Security (IPSec) ■ Generic Route Encapsulation (GRE) ■ Multi Protocol Label Switching (MPLS)
Verbindung (Schicht 2)	■ Frame Relay (FR) ■ Asynchronous Transfer Mode (ATM) ■ Layer 2 Tunnelling Protocol (L2TP) ■ Point-to-Point Tunnelling Protocol (PPTP)
Physik (Schicht 1)	■ Mietleitungen

Abbildung 27: VPN Protokolle im OSI Modell

Während die verschiedenen Standorte eines Unternehmens bzw. einer Organisation mit Hilfe von Branch-Office VPNs miteinander verbunden werden, können mit Hilfe von Dial-In VPNs für die einzelnen Mitarbeiter eines Unternehmens gesicherte Einwahlmöglichkeiten über verschiedene Zugangswege (z.B. Modem, ISDN, DSL, GPRS, WLAN, UMTS) realisiert werden. Auch hier wird eine gemeinsame Einwahlplattform eines Providers (z.B. die eines Internet Service Providers) anstelle einer eigenen Ende zu Ende Einwahllösung über das Telefonnetz genutzt, um Kosten zu sparen.

Die Einwahl wird ebenfalls unter Beachtung eines Sicherheitsregelwerks (Policy) überwacht, das festlegt, wie sich die Nutzer authentisieren müssen und welche Maßnahmen zum Schutz der Authentizität und der Vertraulichkeit der übertragenen Daten zu beachten sind. Häufig kommen hierzu die Übertragungsprotokolle PPP, PPTP, L2TP und/oder IPSec zum Einsatz. Der Zugang zum Unternehmensnetz wird in der Regel durch die Abfrage von Benutzername und Passwort von einem RADIUS System oder einem VPN-Gateway kontrolliert. Zunehmend kommen jedoch

auch „starke" Authentisierungsverfahren wie z.B. Einmalpasswort oder Zertifikate zum Einsatz.

Allgemein lässt sich somit festhalten, dass VPNs durch zwei wesentliche Merkmale gekennzeichnet sind:

1. VPNs sind durch eine Regelwerk (Policy) definiert, das genau festlegt, wer in welcher Form Zugang und unter welchen Bedingungen zu dem jeweiligen Unternehmensnetz haben soll.
2. VPNs werden auf einer öffentlichen Datenvermittlungsplattform realisiert und teilen sich gemeinsame Einrichtungen und Übertragungswege eines Providers untereinander.

2.4.2 VPN-Klassen

Aufgrund der kaum zu überblickenden Vielzahl an unterschiedlichen VPN-Lösungen ist es hilfreich zunächst verschiedene Klassifizierungen vorzunehmen, die helfen, einen ersten Überblick zu gewinnen, ohne zu sehr ins Detail zu gehen.

Neben der grundlegenden Einteilung nach Branch-Office VPN und Dial-In VPN (Abbildung 26) lassen sich weitere Einteilungen treffen:

- „Layer-2-VPN" versus „Layer-3-VPN" (gemäß OSI-Modell)
- „Secure VPN" versus „Trusted VPNs"
- „CPE[59] basierte VPN" versus „Netzwerk basierte VPN"
- „Best effort VPN" versus QoS[60]-VPNs

[59] CPE steht für Customer Premise Equipment und bezeichnet in der Regel einen Router oder ein VPN-Gateway, der sich in einem Standort des Kunden am Übergang zwischen dem internen Netz des Kunden und dem Weitverkehrsnetz des Providers befindet.

Die Unterscheidung in „Layer-2-VPNs (L2VPN)" bzw. „Layer-3-VPNs (L3VPN)" hängt davon ab, in welcher Schicht des OSI-Referenzmodell das VPN realisiert wird. Eine Einteilung wichtiger VPN-Technologien ist bereits weiter oben vorgenommen (siehe Abbildung 27). L2VPNs auf der Basis von Frame Relay oder ATM sind noch immer am weitesten verbreitet. Da jedoch viele Diensteanbieter neben den klassischen Frame Relay bzw. ATM-Plattformen inzwischen auch IP-basierte Plattformen betreiben, gibt es Bestrebungen, L2VPN Dienste zukünftig auf einer gemeinsamen Layer-3-Plattform zu realisieren. Bei den L3VPNs unterscheidet man im wesentlichen drei Basistechnologien, die weiter unten näher eingeführt werden:

- Tunneling (z.B. IPSec, GRE)
- Virtuelle Router
- MPLS

Die Klassifizierung nach „Secure VPN" versus „Trusted VPN" ist eine Einteilung, die vom VPN-Consortium eingeführt wurde (http://www.vpnc.org/). Demnach bezeichnet ein „Secure VPN" eine VPN-Lösung, die zwischen den jeweiligen Endstellen eine starke Verschlüsselung eingesetzt wird, die es einem Angreifer, der an irgendeiner Stelle des Übertragungsweges den Datenverkehr aufzeichnet, praktisch unmöglich macht, die Daten zu entschlüsseln und im Klartext zu lesen. Die Sicherheit von „secure VPN" stützt sich demnach einzig auf die eingesetzte Ende-zu-Ende Verschlüsselung, die von den Endstellen vorgenommen wird, und ist im Gegensatz zu der Klasse der „trusted VPNs" unabhängig von der

[60] QoS steht für Quality of Service und bezeichnet die Eigenschaft bestimmter Übertragungsverfahren wie zum ATM, zwischen zwei Endstellen Verbindungen mit einer fest definierten bzw. garantierten Übertragungsqualität (z.B. Mindestbandbreite, maximale Übertragungsverzögerung) bereitzustellen.

Vertrauenswürdigkeit der genutzten Übertragungsplattform. Beispiele für „secure VPNs" sind VPN-Lösungen auf der Basis von IPSec über das Internet. Demgegenüber hängt bei der Klasse der „Trusted VPNs" die Sicherheit von der Vertrauenswürdigkeit der Übertragungsplattform des jeweiligen Service Providers ab. Der Kunde verlässt sich hierbei darauf, dass niemand anderes als der Service Provider selbst die Übertragungspfade konfigurieren oder ändern kann und dass niemand anderes auf dem Übertragungsweg Zugang zu den übertragenen Daten hat und Daten verändern, löschen oder manipulieren kann.

Bei der Differenzierung nach „CPE basierte VPN" versus „Netzwerk basierte VPN" geht es um die Frage, in welcher Komponente die VPN-Policy hinterlegt und umgesetzt wird (Abbildung 28).

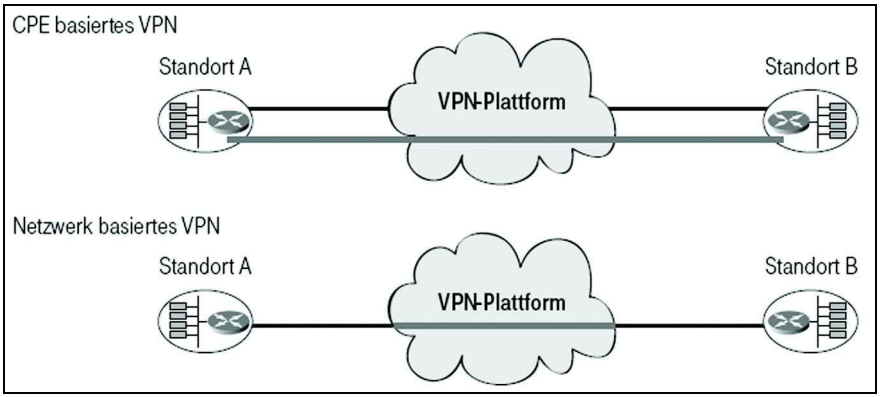


Abbildung 28: CPE versus Netzwerk basiertes VPN

Die Fachwelt spricht in diesem Zusammenhang vom Service Creation Point. Grundsätzlich gibt es hier genau zwei Möglichkeiten. Entweder ist die Konfiguration der VPN-Zugehörigkeit in der CPE, z.B. einem Anschluss-Router in den Räumen des

Kunden zu finden, oder sie wird am Provider Edge, dem jeweiligen Zugangs-Router zur VPN-Plattform des Providers, vorgenommen. Im ersten Fall spricht man von CPE basierte VPN, in zweiten Fall wird die Lösung Netzwerk basiertes VPN genannt. CPE basierte VPNs können ohne spezielle Mitwirkung des Service Providers vom Kunden selbst realisiert werden. Hierzu sind jedoch Spezialkenntnisse erforderlich. Bei Netzwerk basierten VPNs hingegen muss die CPE nur gewöhnliche IP Routing-Funktionen unterstützen.

Die Klassifizierung nach „Best-Effort VPN" versus „QoS VPN" betrifft die Übertragungsqualität zwischen den einzelnen Standorten eines VPN. Unterschiedliche Anwendungen haben unterschiedliche Anforderungen an ein Übertragungsnetz. So stellt z.B. ein File Transfer hohe Anforderungen in Bezug auf Bandbreite und Netzstabilität. Die Übertragungsverzögerung ist eher unkritisch. Echtzeitanwendungen wie Video-Conferencing oder Voice over IP (VoIP) erfordern demgegenüber ein geringes und stabiles Delay. Um diesen unterschiedlichen Anforderungen Rechnung zu tragen, kommen bei der Realisierung von VPNs Übertragungstechniken wie z.B. ATM, Frame Relay oder MPLS eingesetzt, die die geforderten Qualitäten z.B. Mindestbandbreite, konstantes Delay[61] oder Jitter[62] zwischen zwei Standort Ende zu Ende einhalten können. Zudem müssen die jeweiligen Endstellen bzw. Abschluss-Router so konfiguriert werden, dass diese unterschiedlichen Übertragungsklassen abhängig von der jeweils genutzten Anwendung bereitgestellt werden und somit jede Anwendung die Behandlung

[61] Delay: Verzögerungs- oder Wartezeit. Zeitspanne, um die ein Ereignis verzerrt oder verzögert wird. Beispielsweise die Zeit, die vergeht, bis eine abgesandte Information vom Zielsystem empfangen wird.

[62] Jitter: Weitgehend zufallsbestimmte Schwankungen der Flanken eines realen Datensignals um die Sollzeit des Nulldurchganges.

erfährt, die sie für eine einwandfreie Funktionsweise benötigt. Ein Beispiel für ein QoS-VPN ist wiederum die Produktfamilie IntraSelect der Deutschen Telekom.

Von einem Best-Effort VPN ist hingegen dann die Rede, wenn sich aufgrund der gewählten Übertragungstechnik oder der genutzten Datenplattform wie z.B. dem Internet keine Ende zu Ende Qualitätszusagen geben lassen und die Übertragungsressourcen nicht fest für eine Verbindung reserviert werden können.

2.4.3 VPN-Basistechnologien

Neben der Kenntnis der unterschiedlichen VPN-Klassen und Konzepte gehört ein grundlegendes Verständnis der wichtigsten VPN-Technologie zum Basiswissen über Virtuelle Private Netze.

Dieser Abschnitt bietet jeweils einen kurzen Überblick über wichtige Basistechnologien, die am häufigsten zum Aufbau von VPNs genutzt werden. Dabei werden lediglich die grundlegenden Eigenschaften vermittelt. Weitergehende Aspekte würden den Rahmen dieses Beitrags sprengen und werden bewusst ausgeklammert.

Von besonderer Bedeutung sind hierbei die Übertragungstechnologien MPLS (Multi Protocol Label Switching) und IPSec (Internet Protocol Security). Diese Technologien werden zukünftig eine immer wichtigere Rolle im Bereich der Branch-Office VPNs einnehmen, wobei MPLS die etablierten Übertragungstechniken wie Frame Relay oder ATM im Bereich der VPN-Lösungen sukzessive ablösen wird. Bereits heute ist IPSec im Bereich der Internet-VPNs bzw. „secure VPNs" die am häufigsten genutzte Technologie.

Frame Relay

Frame Relay (ITU-T Q.022) ist ein paket- und verbindungsorientiertes Datenübertragungsverfahren und gilt als Weiterentwicklung von X.25. Durch den Verzicht auf Übertragungssicherungsverfahren auf Schicht 3 des OSI-Modells können deutlich höhere Durchsatzraten bzw. Bandbreiten realisiert werden als mit der Vorgängertechnik.

Genauso wie X.25 arbeitet Frame Relay ebenfalls verbindungsorientiert. D.h. zwischen den einzelnen Anschlüssen werden feste virtuelle Verbindungen eingerichtet, die festlegen, über welchen Weg die einzelnen Datenpakete durch die Plattform zum jeweiligen Ziel gelangen.

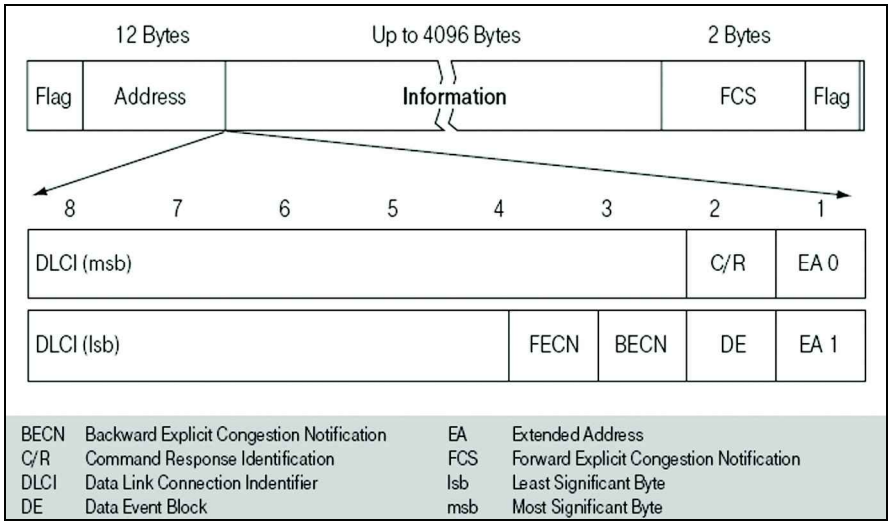


Abbildung 29: Frame Relay Rahmenformat

Die Nutzdaten (z.B. einzelne IP-Pakete) werden dabei jeweils in einem Rahmen (Frame) verpackt. Ein Frame hat eine variable Länge und besteht aus

vorangestellten Informationselementen zur Verbindungssteuerung (Header) sowie aus angehängten Informationselementen (Trailer), die das jeweilige Rahmenende markieren. Abbildung 29 zeigt den Rahmen des Frame Relay Protokolls. Jeder einzelnen Frame enthält im Header eine Kanalnummer (DLCI[63]), anhand derer er entlang eines „virtuellen Pfads" durch die Datenplattform vermittelt wird. Die einzelnen Rahmen einer virtuellen Verbindungen nehmen dabei stets den gleichen Übertragungsweg durch die Datenplattform. Die Verbindung ist insofern wie bei einer Mietleitung durch den Provider fest vorgegeben, wenngleich sie nur aufgrund der Kanalnummer virtuell existiert.

Eine wesentliche Eigenschaft von Frame Relay ist, dass sich mit dieser Technik für jede Verbindung eine garantierte Übertragungsbandbreite (CIR: Commited Information Rate) fest vergeben lässt. Diese Eigenschaft macht Frame Relay zu einer QoS-Technologie, mit deren Hilfe sich QoS-VPNs realisieren lassen.

ATM

ATM (Asynchronous Transfer Mode, ITU-T I.361- ITU-T I.366)[64] ist wie Frame Relay ein paket- und verbindungsorientiertes Übertragungsverfahren.

Die einzelnen Pakete werden ATM-Zellen genannt. Im Gegensatz zu Frame Relay haben sie eine feste Größe von nur 53 Byte und bestehen aus einem Header von insgesamt 5 Byte und einem Nutzdatenfeld von 48 Byte (Abbildung 30). Ein Trailer wie bei Frame Relay ist aufgrund der festen Größe nicht notwendig. Genauso wie bei Frame Relay werden die Daten verbindungsorientiert übertragen. Dies bedeutet, dass zwischen zwei Endstellen jeweils eine feste virtuelle Verbindung bzw. eine virtuelle Wählverbindung eingerichtet wird. ATM zeichnet sich gegenüber

[63] DLCI: Data Link Connection Identifier
[64] siehe Unterrichtsblätter 10/98 bzw. http://www.atmforum.com

Frame Relay im wesentlich durch höhere Übertragungsraten sowie weiter differenzierte Übertragungsqualitäten in Bezug auf Bandbreite, Übertragungsverzögerung und Zellverlust aus.

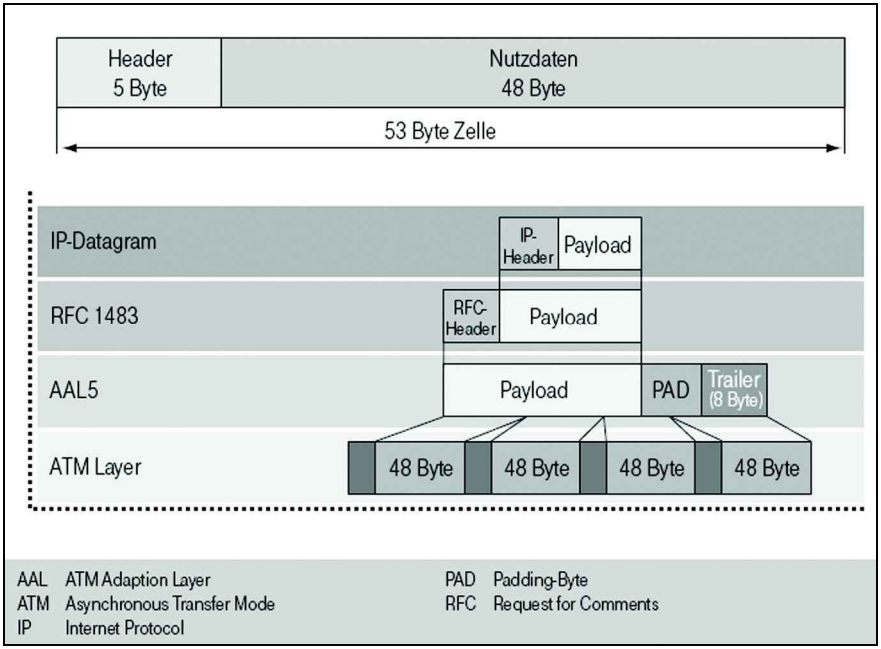


Abbildung 30: ATM Layer

Aufgrund der zur Verfügung stehenden Übertragungsqualitäten bzw. Verkehrskategorien ist ATM universell sowohl für isochronen[65] Verkehr (wie z.B. Sprache) als auch bursthaften Verkehr (wie z.B. LAN-Kopplung) einsetzbar. Folgende Verkehrskategorien stehen zur Wahl:

[65] Isochrone Anwendungen: Diese Anwendungsklasse erfordert ein sehr geringes Delay sowie eine sehr geringe Delay-Varianz (Jitter).

Tabelle 8	ATM Verkehrskategorien
Verkehrskategorie	Beschreibung
CBR (Constant Bit Rate)	Die Verkehrskategorie CBR wird im allgemeinen zur Übertragung von isochronem, zeitsensitivem Verkehr, wie von Sprache und Video, genutzt. Bei CBR werden die einzelnen Zellen mit höchster Priorität und minimaler Übertragungsverzögerung übertragen.
nrt-VBR (non-real-time Variable Bit Rate)	Die Verkehrskategorie nrt-VBR ist definiert durch eine Spitzenzellrate (PCR: Peak Cell Rate; MBS: Maximum Burst Size) sowie einer garantierten durchschnittlichen Zellrate (SCR: Sustainable Cell Rate) für nicht-synchronen Verkehr, wie z.B. für Anwendungen mit variablem oder burstartigem Verkehrsverhalten, konzipiert. Sie eignet sich daher für die Übertragung von paketorientierten Daten, d.h. für Anwendungen, für die keine Bitsynchronität erforderlich ist. In der Regel wird der nrt-VBR Service genutzt, um Informationen zwischen LANs über ATM zu transportieren.
UBR (Unspecified Bitrate)	Die Verkehrskategorie UBR ist definiert durch eine Spitzenzellrate (PCR: Peak Cell Rate) in Sende- und Empfangsrichtung und speziell für Anwendungen mit stark burstartigem, nicht-synchronem Verhalten geeignet, bei denen keine oder nur geringe Anforderungen hinsichtlich Zellenverzögerung und Zellverzögerungsschwankungen bestehen. Diese Verkehrskategorie ist auch besonders geeignet für Anwendungen, deren Verkehrsverhalten nicht oder nur sehr ungenau vorhersagbar ist (z.B. Internet-Anwendungen). Für die UBR Verkehrskategorie werden dem Anwender keine Güteparameter garantiert.

Um die Nutzdaten an die Größe der ATM-Zellen anzupassen, ist innerhalb des OSI Layers 2 eine zusätzliche Umsetzungsfunktion erforderlich, die als ATM Adaption

Layer (AAL) bezeichnet wird. Je nach gewählter Verkehrskategorie bzw. je nach Anwendung stehen hier fünf verschiedene AALs zur Wahl, die an dieser Stelle jedoch nicht im Einzelnen eingeführt werden.

Wichtigster Apaption Layer ist AAL5 (siehe Abbildung 30), der für typischen LAN-Verkehr eingesetzt wird und somit im Bereich der Branch-Office VPN am häufigsten genutzt wird.

MPLS

Im Gegensatz zu ATM und FR ist MPLS eine „Peer-Technologie", mit deren Hilfe VPNs nach dem bekannten Peer-Modell realisiert werden.

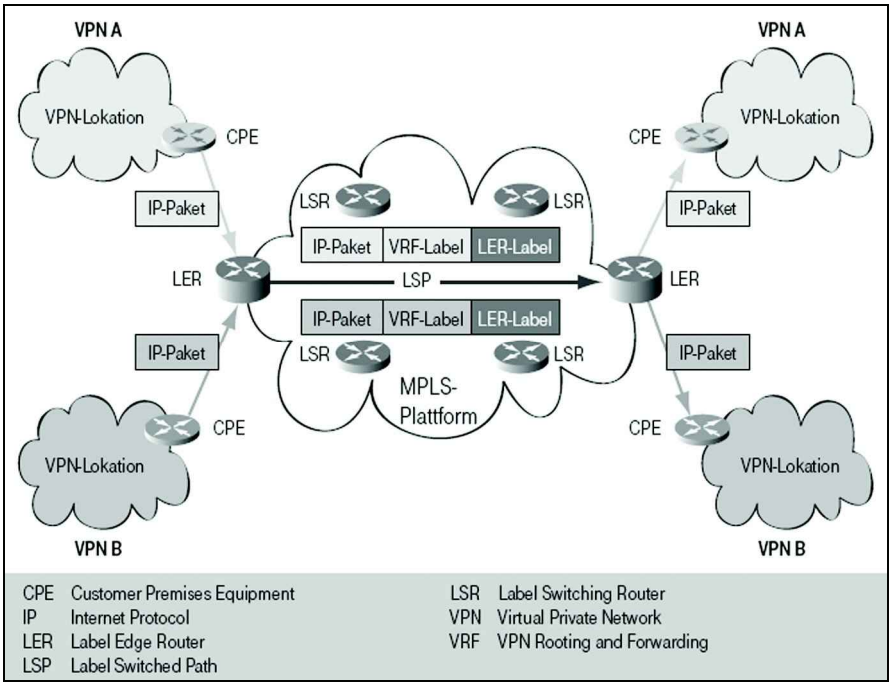


Abbildung 31: Multi Protocol Label Switching (MPLS)

MPLS steht für Multi Protocol Label Switching (RFC 2547) und vereint die Vorteile der schnellen ATM-Vermittlungstechnik mit den Felexibilität von IP-Routing. MPLS bietet die Möglichkeit viele VPNs mit identischen privaten IP-Adressbereichen ohne Adressvermischung transparent über eine MPLS-Plattform zu transportieren. Die Einrichtung eines VPNs wird vollständig im Zugangs-Router zur MPLS-Plattform, den so genanten „Label Edge Router" (LER), und nicht wie bei ATM- oder Frame Relay basierten VPNs im Kunden-Router (CPE) vorgenommen. Das Innere einer MPLS-Plattform wird von ‚Label Switch Router' (LSR) gebildet, die für den VPN-Verkehr völlig transparent sind. Dies bedeutet, dass die einzelnen LSR keine Unterscheidung der einzelnen VPNs treffen und jeglichen Verkehr in gleicher Weise bearbeiten.

Dadurch ist eine gute Skalierbarkeit zur Unterstützung vieler VPNs auf der MPLS-Plattform gewährleistet. Grob gesagt, ist MPLS eine Technik, die die Vorzüge von IP-Routing sowie Layer2-Switching wie beispielsweise bei Frame Relay oder ATM vereint. Routing-Funktionalitäten sind lediglich in den Zugangsknoten der MPLS-Plattform, den LER, zu finden. Im Inneren wird der Verkehr ähnlich wie bei Frame Relay anhand einer Pfadkennung, dem so genanten Label, vermittelt bzw. „geswitcht". Das Label ist daher vergleichbar mit der Kanalkennung DLCI im Falle von Frame Relay mit dem einzigen Unterschied, dass dieses Label nicht fest vorkonfiguriert ist, sondern sich dynamisch mit Hilfe der Routing-Funktionalität der LER ergibt. Somit lässt sich die Flexibilität des IP-Routings mit der Übertragungseffizienz des Layer-2-Switchings kombinieren (siehe Abbildung 31).

Getunnelte Übertragungsverfahren (Tunneling):

Tunneling-Verfahren werden eingesetzt, um VPNs über IP-Netze zu realisieren. In diesem Falle spricht man von einem IP-Tunnel. Ein IP-Tunnel wird allgemein

dadurch realisiert, dass die Protokolldaten von Layer-2- (z.B. PPP) bzw. Layer-3-Protokollen (z.B. IP) in IP-Pakete eingepackt, an eine feste Zieladresse bzw. den Tunnelendpunkt übertragen und dort entsprechend wieder ausgepackt werden (siehe Abbildung 32). Mit diesem Verfahren können beispielsweise lokale Netze mit privaten IP-Adressräumen über das öffentliche Internet miteinander vernetzt werden, ohne dass es zu Adresskonflikten kommt. Da die ursprünglichen IP-Pakete mit privaten IP-Adressen aus den lokalen Netzen jeweils in ein neues äußeres IP-Paket mit offiziellen IP-Adressen eingepackt und am Zielpunkt jeweils wieder ausgepackt werden, sind im Internet nur die offiziellen IP-Adressen sichtbar. Ein häufig genutztes Verfahren, das im Bereich der Branch-Office VPNs Anwendung findet, ist das von CISCO entwickelte und im RFC 2784 spezifizierte Tunnelprotokoll GRE (Generic Route Encapsulation). GRE ist ein sehr einfaches Tunnelverfahren, bei dem die ursprünglichen IP-Paket aus dem internen Unternehmensnetz ein GRE-Header von 8 Byte und eine neuer IP-Header mit einer externen IP-Adresse vorangestellt wird. Mit Hilfe von GRE werden die inneren IP-Pakete lediglich „getunnelt". Eine Verschlüsselung wird nicht durchgeführt.

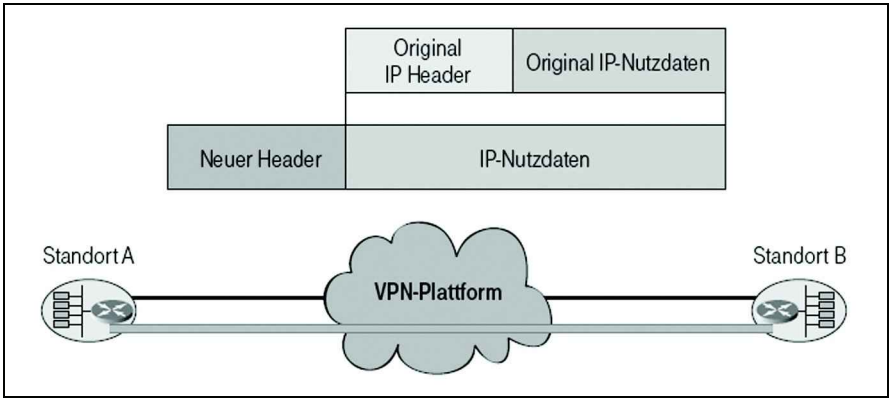


Abbildung 32: IP-Tunnelverfahren

Ebenfalls weit verbreitet sind die Layer-2-Tunneling Verfahren PPTP und L2TP, mit deren Hilfe sich Dial-In VPN realisieren lassen. Im Gegensatz zu dem Layer-3-Tunneling Verfahren IPSec (Internet Protocol Security, RFC 2401) werden die Nutzdaten bei der Übertragung mit PPTP bzw. L2TP ebenfalls unverschlüsselt und ohne Manipulationsschutz übertragen. PPTP ist eine Erweiterung von PPP und wird häufig verwendet, da es fester Bestandteil von Windows ist. L2TP erlaubt gegenüber PPTP zudem den Aufbau sowie den gleichzeitigen Betrieb paralleler Tunnel-Sitzungen (Sessions) zu unterschiedlichen Gegenstellen.

Aufgrund des unzureichenden Schutz bei PPTP sowie L2TP wurden mit IPSec verschiedene Verfahren entwickelt, um die Unversehrtheit (Integrität), die Vertraulichkeit (Privacy) der Nutzdaten sowie die Echtheit (Authentizität) von Absender und Empfänger zu gewährleisten. Hierzu können wahlweise verschiedene Sicherheitsverfahren wie die Hash-Algorithmen MD-5 oder SHA-1 zur Gewährleistung der Datenintegrität sowie bewährte Verschlüsselungsverfahren wie DES (Data Encryption Standard), 3DES (Triple DES) oder AES. IPSec besteht somit nicht aus einem einzigen Protokoll, sondern stellt vielmehr eine Sammlung unterschiedlicher Protokolle und Verfahren bereit, die in unterschiedlichster Kombination eingesetzt werden können. Trotz dieser Vielfalt haben sich dennoch bestimmte Standardkonfiguration bewährt, die in den meisten Fällen zur Anwendung kommen.

IPSec ist inzwischen neben MPLS die wichtigste VPN-Technologie und hat sich im Bereich der Internet-VPNs zum beherrschenden Standard entwickelt.

2.4.4 Zugangslösungen für die mobile Einwahl in Unternehmensnetze

Zugangslösungen für die mobile Einwahl über GPRS und UMTS oder HSDPA lassen sich entsprechend der weiter oben eingeführten Klassifizierung in zwei Kategorien unterteilen:

1. Ende-zu-Ende Lösungen (secure VPN)
2. Netzbasierte Lösungen (trusted VPN)

Unter Ende-zu-Ende Lösungen versteht man Zugriffsverfahren, bei denen die Authentisierung und die Übertragungssicherheit ausschließlich durch einen VPN-Client auf der mobilen Client-Plattform am einen Ende und einem VPN-Gateway am anderen Ende der Zugangslösung gewährleistet werden. Für die dazwischen liegende Mobilfunkstrecke ist dieses Verfahren völlig transparent (siehe Abbildung 28). Beispiele für diese Lösungskategorie sind Verfahren, die IPSec oder SSL Ende-zu-Ende einsetzen. Der Vorteil dieser Lösungen sind insbesondere die Unabhängigkeit von des jeweils genutzten Mobilfunknetzes. Nachteilig sind die zusätzlichen Lizenz- und Wartungskosten, die sich im allgemeinen nach der Anzahl der mobilen Einwahl-Clients bemessen. Zudem ist zu bedenken, dass es nicht für alle Endgeräte einen geeigneten VPN-Client gibt. Daher ist für spezielle Anwendungsbereiche (z.B. Telemetrie, Transport & Logistik) häufig die zweite Kategorie geeigneter.

Netzbasierte Lösungen fallen in die allgemeine Kategorie der „trusted VPN" und basieren auf Sicherheitsverfahren im Mobilfunknetz sowie von dort aus einen gesichertem Übertragungsweg zum Unternehmensnetz. Ein spezieller VPN-Client wird bei diesen Verfahren nicht benötigt. Daher sind Kosten von der Anzahl der

mobilen Endgeräte weitgehend unabhängig. Ein Beispiel für netzbasierte Lösungen ist das Zugangsprodukt „Mobile IP VPN" von T-Mobile.

2.4.5 Beispiel „Mobile IP VPN" von T-Mobile

Mobile IP VPN ist eine netzbasiertes Zugangsprodukt für die gesicherte Einwahl in private Netze. Lösungsbestandteile sind in der Basisvariante (Abbildung 33):

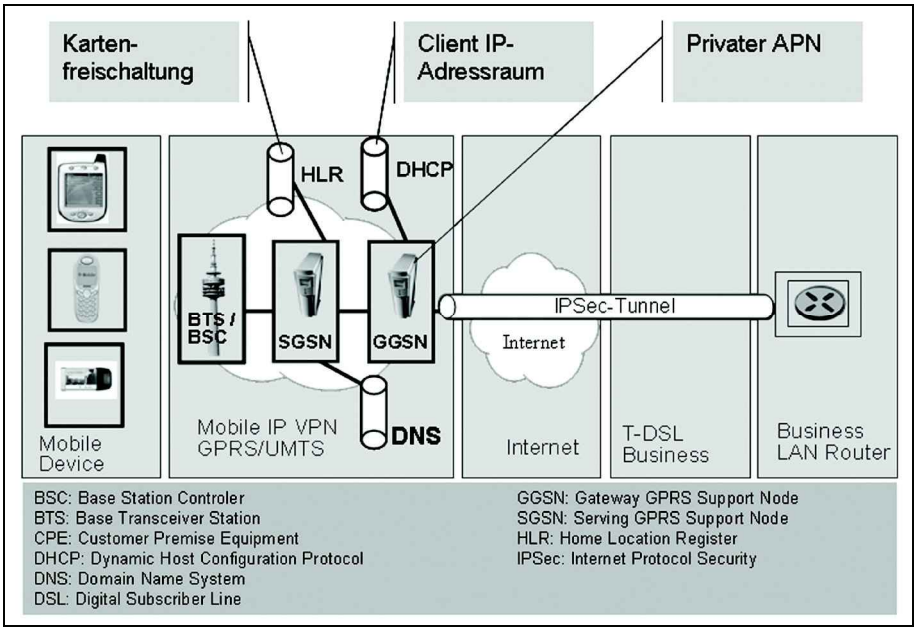


Abbildung 33: Mobile IP-VPN von T-Mobile

- ein privater APN für jedes private Netze

- eine Kartenfreischaltung sowie Zugangsprüfung der berechtigten Mobilfunkkarten in zentralen Teilnehmerdatenbank des Mobilfunknetzes (HLR: Home Location Register
- IP-Adressvergabe durch das Mobilfunknetz
- eine spezielle Anschaltung des privaten Netzes über eine gesicherte Festnetzverbindung, z.B. über IPSec oder ATM.

Darüber hinaus bietet T-Mobile verschiedene Optionen und Varianten, u. a.:

- Integration eines Kunden-RADIUS im Kundennetz zur Benutzerauthentisierung sowie zur IP-Adressvergabe.
- RADIUS im Mobilfunknetz mit web-basierte Benutzerverwaltung durch den Kunden zur Benutzerauthentisierung sowie zur IP-Adressvergabe
- Redundante Anschaltung des privaten Zielnetzes des Kunden
- Sperrung des direkten Internet-Zugangs für die einzelnen Benutzer
- Integration mit vorhandenen VPN-Lösungen im Festnetz (z.B. gemeinsam mit T-Systems).

Stichwortverzeichnis

4 Stichwortverzeichnis

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z

Anhang

5 Abbildungsverzeichnis

6 Abkürzungsverzeichnis

3DES	Triple DES
3GPP	Third Generation Partnership Project
ACK	Acknowledgement
AES	Advanced Electronic Signature
API	Application Programming Interface
APN	Access Point Name
ARM	Advanced RISC Machines
ARQ	Automatic Repeat Request
AT	Advanced Technology
ATM	Asynchronous Transfer Mode
ATMP	Ascend Tunnel Management Protocol
BMP	Bitmap Format
BS	Bearer Service
BSC	Base Station Controller
BTS	Base Transceiver
CE	Customer Edge
CHAP	Challenge Handshake Authentication Protocol
CID	Context Identifier
CLI	Calling Line Identity
CLID	Calling Line Identification
CN	Corporate Network
COM	Communications Port
CPE	Customer Premise Equipment
CRC	Cycling Redundancy Check
CS	Coding Schemes

CUG	Closed User Group
DES	Data Encryption Standard
DFÜ	Datenfern-Übertragung
Dial In	Einwahl
DLCI	Data Link Connection Identifier
DNS	Domain Name Server
DSL	Digital Subscriber Line
FEC	Forward Error Correction
FR	Frame Relay
Gb	(Schnittstellenbezeichnung)
GBG	Geschlossene Benutzergruppe
GGSN	Gateway GPRS Support Node
GIF	Graphics Interchange Format
GNUZip	Datenkompressionsprogramm
GPRS	General Packet Radio Service
GRE	Generic Route Encapsulation
GSM	Global System for Mobile Communications
HLR	Home Location Register
HSDPA	High Speed Data Packet Access
HTML	Hypertext Markup Language
HTTP	Hypertext Transport Protocol
IETF	Internet Engineering Task Force
IIORB	Internet-Inter Object Request Broker
IMSI	International Mobile Subscriber Identity
IN	Intelligent Network
IP	Internet Protocol
IPCP	Internet Protocol Control Protocol
IPSec	IP Security

IrDA	Infrared Data Association
ISDN	Integrated Services Digital Network
IT	Information Technology
ITU	International Telecommunications Union
ITU-T	International Telecommunications Union/ Telecommunication Sector
J2EE	Java Platform Enterprise Edition
J2ME	Java 2 Mobile Edition
JPG	JPEG-(Joint Photographics Expert Group-)Format
L2TP	Layer 2 Tunneling Protocol
L2VPN	Layer 2 VPN
L3VPN	Layer 3 VPN
LAN	Local Area Network
LER	Label Edge Router
LLC	Logical Link Control
LSR	Label Switch Router
LZH	Lempel, Ziv und Haruyasu
MBS	Maximum Burst Size
MD5	Message Digest Algorithm 5
MDA	Mobile Digital Assistant
MMS	Multimedia Messaging Service
MP3	MPEG 1-2 (Moving Picture Experts Group) Audio Layer 3
MPEG	Moving Picture Experts Group
MPLS	Multiprotocol Label Switching
MSC	Mobile Switching Center
MTU	Maximum Transfer Unit
NetBios	Network Basic Input/Output System
OSI	Open System for Interconnection
PAP	Password Authentication Protocol

PC	Personalcomputer
PCI	Protocol Control Information
PCMCIA	Personal Computer Memory Card International Association
PCR	Peak Cell Rate
PDA	Personal Digital Assistano
PDP	Packet Data Protocol
PDTCH	Packet Data Traffic Channel
PE	Provider Edge
PGP	Pretty Good Privacy
PILC	Performance Implications of Link Characteristics
PIM	Personal Information Management
PIN	Personal Identification Number
PKZip	Datenkompressionsprogramm
PLC	Packet Loss Concealment
PPP	Point-to-Point Protocol
PPTP	Point to Point Tunnelling Protocol
PRACH	Packet Random Access Channel
PUK	Personal Unblocking Key
PVC	Permanent Virtual Circuit
QoS	Quality of Service
RADIUS	Remote Access Dial-in User Service
RAS	Remote Access Service
RFC	Request for Comments
RIM	Research in Motion
RLC	Radio Link Control
RLP	Radio Link Protocol
ROM	Read Only Memory
RSA	Rivest Shamir Adleman

RTO	Retransmission Timeout
RTT	Retransmission Time
SACK	Selective Acknowledgement
SAP	Session Announcement Protocol
SCR	Sustainable Cell Rate
SDK	Software Development Kit
SGSN	Serving GPRS Support Node
SHA-1	Secure Hash Algorithm
SIM	Subscriber Identity Module
SMS	Short Message Service
SOAP	Simple Object Access Protocol
SSL	Secure Sockets Layer
TAE	Telekommunikationsanschlusseinheit
TCH	Traffic Channel
TCP	Transmission Control Protocol
TFI	Temporary Flow Identity
TXT	Text Format
UMTS	Universal Telecommunications System
USB	Universal Serial Bus
USF	Uplink State Flag
UTRAN	UMTS Terrestrial Radio Access Network
VAD	Voice Activity Detection
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAP	Wireless Application Protocol
WEP	Wired Equivalent Privacy
WG	Workgroup
WinSock	Windows Socket

WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

7 Literatur

[1] Application Configuration & Developer Guide (ACDG), T-Mobile International, 2005-2006, www.t-mobile.de/entwickler

[2] Cobb, S., "PPP Internet Protocol Control Protocol Extensions for Name Server Addresses", RFC1877, 1995

[3] Comer, D. E, Internetworking with TCP/IP, Vol I, II, III, Prentice-Hall International

[4] Hillebrand, Rainer und Wierlemann Thomas, Guidelines for the Mobile Internet, 2001 – 2003, www.mobileinternetguide.org

[5] McGregor, G., "The PPP Internet Protocol Control Protocol", RFC1332, 1992

[6] Postel, J., "Internet Protocol", RFC791, 1981.

[7] Postel, J., "Transmission Control Protocol", RFC793, 1981.

[8] Postel, J., "User Datagram Protocol", RFC768, 1980.

[9] Römer, Stefanus, „Fernzugriff auf Computernetze mit DSL-Anschluss", WissenHeute, 5/2004

[10] Römer, Stefanus, „GPRS-Roaming in GSM-Netzen", Unterrichtsblätter der Deutschen Telekom,8/2003

[11] Römer, Stefanus, „Mit GPRS ins Intranet – Optimierungsmaßnahmen für den praktischen Einsatz in Unternehmensnetze", Unterrichtsblätter der Deutschen Telekom, 11/2001

[12] Römer, Stefanus, „Mit GPRS ins Intranet – Outlook Optimierung", Unterrichtsblätter der Deutschen Telekom

[13] Römer, Stefanus, Besonderheiten der Anwendungsentwicklung für die mobile Nutzung - ein Leitfaden – Teil 1, WissenHeute 11/2004

[14] Römer, Stefanus, Besonderheiten der Anwendungsentwicklung für die mobile Nutzung - ein Leitfaden – Teil 2, WissenHeute 12/2004

[15] Römer, Stefanus, Besonderheiten der Anwendungsentwicklung für die mobile Nutzung - ein Leitfaden – Teil 3, WissenHeute 3/2005

[16] Römer, Stefanus, Besonderheiten der Anwendungsentwicklung für die mobile Nutzung - ein Leitfaden – Teil 4, WissenHeute 4/2005

[17] Römer, Stefanus, Besonderheiten der Anwendungsentwicklung für die mobile Nutzung - ein Leitfaden – Teil 5, WissenHeute 5/2005

[18] Römer, Stefanus, Integration von WLAN mit GPRS und UMTS, WissenHeute 7/2004

[19] Römer, Stefanus, Mit GPRS ins Intranet – Das Produkt LAN to LAN GPRS Access", Unterrichtsblätter der Deutschen Telekom, 3/2001

[20] Römer, Stefanus, Verbindungen nutzen – Virtuelle private Netze heute, NET 1-2/05

[21] Schulte, Heinz, Telekommunikation von A-Z, Interest Verlag

[22] Simpson, W., "PPP Challenge Handshake Authentication Protocol", RFC1994, 1996

[23] Simpson, W., "PPP in HDLC-like Framing", RFC1662, 1994

[24] Simpson, W., "PPP LCP Extensions", RFC1570, 1994

[25] Simpson, W., "PPP Vendor Extensions", RFC2153, 1997

[26] Simpson, W., "The Point-to-Point Protocol", RFC1661, 1994

[27] Walke, Bernhard H., Seidenberg, Peter, Althoff, Marc P., UMTS – The fundamentals, Wiley, 2003

[28] Witt, Martin (Hrsg.), GPRS-Start in die mobile Zukunft, MITP-Verlag, Bonn, 2000, ISBN 3-8266-0696-5.

[29] Balachander Krishnamurthy, Jennifer Rexford, Web Protocols and Practice: HTTP/1.1, Networking Protocols, Caching, and Traffic Measurement, ISBN: 0-201-71088-9, Addison Wesley Professional, 2001

[30] Jim Beveridge, Robert Wiener, Multithreading Applications in Win32,ISBN: 0201442345, Addison Wesley, 1996

[31] Erich Gamma, Richard Helm, Ralph E. Johnson, Design Patterns, ISBN: 0201633612, Addison Wesley, 1997

[32] Stephen D. Huston, James CE Johnson, Umar Syyid, ACE Programmer's Guide, Practical Design Patterns for Network and Systems Programming, ISBN: 0-201-69971-0, Addison Wesley, 2004

[33] Charlie Kaufman, Radia Perlman, Mike Speciner, Network Security, Second Edition, ISBN 0-13-046019-2, Prentice Hall, 2002

[34] Cem Kaner, Jack Falk, Hung Q. Nguyen, Testing Computer Software, Second Edition, ISBN: 0471358460, John Wiley & Sons Inc., 1999

[35] Jeffrey Richter, Advanced Windows, ISBN:1572315482, Microsoft Press, 1997

[36] James Rumbaugh, Ivar Jacobson, Grady Booch, The Unified Modeling Language Reference Manual, ISBN: 020130998X, Addison Wesley Professional, 1998

[37] Bruce Schneier, Applied Cryptography, Second Edition, ISBN 0471117099, John Wiley & Sons Inc.

[38] Bob Quinn, Dave Shute, Windows Sockets Network Programming, ISBN: 0201633728, Addison Wesley Professional, 1995

In eigener Sache