Dr. Suppan International Institute

Der Netzwerk Insider

Mai 2002

Technologie Information für die Ausbildung zum ComConsult Certified Network Engineer

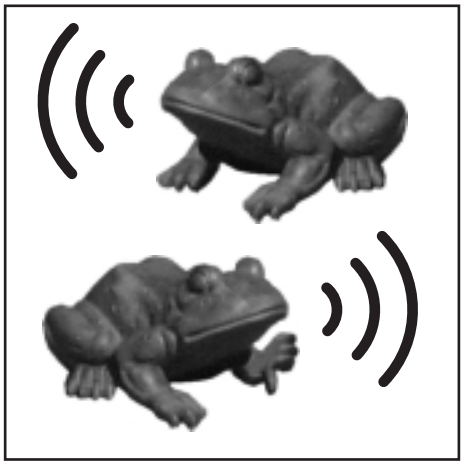
Schwerpunktthema

Konvergenz zu IP in mobilen Kommunikationssystemen – Weniger ist mehr

von Dr. Simon Hoff und Dr. Jochen Wetzlar

Es ist die Zeit der Unkenrufer – eine neue Technik steht an. Sie ist teuer, und den Technologiewerten an den Börsen geht es immer noch schlecht – also: Daumen runter. Jedoch, so ganz unberechtigt ist das nicht.

Mit der Überschrift "Horrorszenario für Deutschland" eröffnete Spiegel Online Ende März vergangenen Jahres einen Artikel über eine Studie von McKinsey, die den Telefonkonzernen Verluste in Milliardenhöhe im Geschäft mit dem Universal Mobile Telecommunications System (UMTS) prophezeit. Dies war nicht die erste (und ist auch nicht die letzte) Prognose dieser Art. Denn alleine das Summieren der Kosten, die bereits entstanden sind und von denen man ziemlich genau weiß, dass sie entstehen werden, genügt. Man denke nur an das Paket von etwa 50 Milliarden Euro an Herrn Eichel aus der Auktion der Funklizenzen für UMTS. Das muss sich erst einmal auszahlen.



UMTS:
Unken machen Technik schlecht

Es droht also heftige Konkurrenz speziell unter den UMTS-Lizenznehmern und generell zwischen allen Netzbetreibern im Mobilfunkbereich (auch wenn es bedingt durch die dramatischen Kosten für den Aufbau der Netze zu überraschenden Koalitionen zwischen den angehenden UMTS-Betreibern gekommen ist). Damit UMTS sich rechnet, muss nach Einführung schnell eine hohe Teilnehmerzahl erreicht werden (und nicht nur passive Teilnehmer, sondern solche, die auch tatsächlich heftig Dienste in Anspruch nehmen). Nur, nach den fetten Jahren des (exponentiellen) Anstiegs der Teilnehmerzahlen ist eine erste Stagnation deutlich spürbar. Wer wird tatsächlich zu UMTS wechseln?

weiter Seite 11

Sommerschule der ComConsult Akademie

Heftige Diskussion über neue LAN-Design-Verfahren

Auf dem diesjährigen Netzwerk-Redesign Forum der ComConsult Akademie, das Anfang April in Königswinter statt fand, wurden die Arbeitsergebnisse eines seit Ende 2001 laufenden Projekts präsentiert, das sich mit neuen Design-Ansätzen im LAN-Bereich befasste. An dem Projekt beteiligt waren Mitarbeiter der ComConsult Technologie Information GmbH und Petra Borowka von der Unternehmensberatung Netzwerke UBN. An einem typischen Projektbeispiel wurden unter Nutzung der neuen Design-Ansätze Einspar-Potenziale von bis zu 43 % der Beschaffungskosten ermittelt.

Dabei wurde bereits unterstellt, dass alle weiteren Ansätze der wirtschaftlichen Optimierung, die ebenfalls in einem Vortrag vorgestellt wurden, voll genutzt wurden. In der Folge entstand auf der Veranstaltung unter den über 200 Teilnehmern und den anwesenden Herstellern sowie auch in den Wochen danach eine heftige Diskussion, ob und für wen diese Ansätze eine Perspektive darstellen. Als Tendenz stellte sich heraus, dass für Unternehmen bis 5000 Mitarbeitern neue Möglichkeiten des LAN-Designs mit erheblichen Einsparpotenzialen bestehen, dass ein Einsatz in Großunternehmen bis zu 50.000 Mitarbeitern auf jeden Fall starke Einzelfall-Elemente haben wird.

Naturgemäß wurden seitens der Hersteller, speziell durch CISCO und Extreme, die Vorzüge der bisherigen traditionellen Design-Ansätze betont. Immerhin besteht auf der Herstellerseite die Befürchtung, dass eine Einsparung von 43 % mit einem ähnlich hohen Umsatzverlust einher geht. Dem wurde durch Dr. Suppan von der ComConsult Technologie Information widersprochen. Seiner Ansicht nach eröffnen die neuen Design-Ansätze speziell den mittelständischen Kunden die Nutzung von Technologien und Produkten, auf deren Einsatz sie bisher aus Kostengründen verzichtet haben. Für diese Kunden realisieren die neuen Ansätze eine höherwertige Netzwerk-Infrastruktur ohne die Kosten zu erhöhen.

weiter Seite 3

Zum Geleit

LAN-Analyse am Scheideweg

In einer der letzten Ausgaben der Network-World wurde eine stark kontroverse Auseinandersetzung zwischen Agilent und Synapse veröffentlicht. Gegenstand der Diskussion war die heiße Frage, ob der traditionelle LAN-Analysator ausgedient hat und durch eine neue Analyse-Technik ersetzt werden muss. Anlass waren entsprechende Aussagen von Synapse, die mit einem neuen Produktansatz die bisherigen Analyse-Technologien in Frage stellen. Dem stand eine vehemente Abwehrposition von Agilent gegenüber, die dieser Argumentation naturgemäß nicht zustimmen konnten.

Impressum

Verlag:
Dr. Suppan
International Institute b.v.
Ahornenlaan 12
4493 DG Kamperland
Niederlande

Telefon (0049)02408/955-400
Fax (0049)02408/955-399

Herausgeber
und verantwortlich
im Sinne des Presserechts:
Dr. Jürgen Suppan

Gestaltung:
Zweipfennig
(norbert@zweipfennig.de)

Erscheinungsweise:
Monatlich,
12 Ausgaben im Jahr

Bezug:
Kostenlos
als PDF-Datei
über den eMail-
VIP-Service
der ComConsult Akademie

Für unverlangt
eingesandte Manuskripte
wird keine Haftung übernommen

Was steckt dahinter?

Wir beobachten speziell im LAN-Bereich eine immer stärker zunehmende Lastsituation. Gigabit-Netzwerke erfordern bei höherer Auslastung schon für die direkte Analyse eine erhebliche Hardware-Leistung, um alle zu analysierenden Pakete erfassen zu können. Gehen in der Trace-Phase Pakete verloren, werden die aufsetzenden Experten-Module vor erhebliche Probleme gestellt, da sie nicht entscheiden können, ob die fehlenden Pakete ihre Ursache in einem Fehler oder in einem Versagen der Mitschneide-Schnittstelle hatten. Diese Situation wird sich noch weiter verschlimmern. Auf der einen Seite erhöhen Technologien wie 10 Gigabit-Ethernet in Kombination mit Server- und Speicher-Zentralisierung die Datenströme und sorgen damit für erhebliche Probleme, diese Datenmengen noch adäquat analysieren zu können. Auf der anderen Seite besteht die Gefahr, dass sich die Menge der Endgeräte massiv erhöht, insbesondere wenn die neuen PDA-Technologien mit sehr leistungsstarken CPUs und neuen Anwendungen zum Beispiel auf der Basis von .NET ins Netzwerk kommen. Beides in Kombination erhöht auf jeden Fall die Komplexität von LAN-Analyse. Gleichzeitig zeigt aber gerade der Trend zu vielen neuen Endgeräten mit vielen neuen Funktionen und auch neuen Applikations-Architekturen, dass auch ein zunehmender Bedarf an Analyse-Funktionalität entsteht.

Wie sehen nun die kontroversen Positionen aus?

Auf der einen Seite die Sichtweise von Synapse, dass nur noch eine Offline-Analyse mit sehr großen Datenmengen Sinn macht. Ziel ist, zum Beispiel einen kompletten Tag mitzuschneiden und danach eine Auswertung des sehr großen Traces mit neues Auswertungsfunktionen zu fahren. Ein entsprechendes Produkt wird von Synapse angeboten. Die Gegenposition kommt von Agilent, die nach wie vor die Kombination eines traditionellen LAN-Analysators mit Online- und Offline-Analyse als den sinnvollen Weg ansehen. Eine ähnliche Sichtweise würde voraussichtlich Sniffer vertreten, die ja speziell zur Handhabung großer Datenmengen den Umgang mit Filtern perfektioniert haben.

Parallel ändert sich die Produktsituation massiv. Agilent hat seine Produktpalette komplett erneuert, Fluke hat mit seinem Omniview den Markt schon gehörig aufgemischt und kommt jetzt auch mit weiteren neuen Geräten auf den Markt, Sniffer baut den Funktionsumfang seiner Geräte immer weiter aus.

Wer hat angesichts dieser Situation Recht? Was bedeutet das für den Anwender?

Ich kann diese Frage nicht beantworten, auf jeden Fall muss die Situation geklärt werden, da an der Problematik immer größerer Datenströme und immer mehr Teilnehmer nicht zu rütteln ist. Ein Ausfall der LAN-Analyse in dieser Situation wäre eine Katastrophe. Auf der einen Seite würden wir mit Server- und Speicher-Zentralisierung alles was im Untenehmen läuft vom Netzwerk abhängig machen, auf der anderen Seite würden wir die Fähigkeit zur Fehleranalyse verlieren.

Hier besteht ein absoluter Entscheidungs- und Handlungszwang. Wir haben deshalb unseren führenden Analyse-Experten, Dr. Jochen Wetzlar von der ComConsult Beratung und Planung GmbH gebeten, die aktuellen Anforderungen an LAN-Analyse aus seiner Sicht eines Profis, der jeden Tag große und komplexe Netzwerke mit schwierigen Fehlersituationen bearbeiten muss, vorzustellen. Dies wird auf der Sommerschule vom 1. bis 5.7. in Aachen erfolgen. Dies wird kombiniert mit der Vorstellung von Agilent, Fluke, Sniffer und Synapse, die jeweils ihre Sichtweise, ihre neuen Produkte und ihre Bewertung präsentieren. Abgerundet wird dies durch eine offene Podiumsdiskussion. Wir dürfen uns auf eine spannende Sommerschule und auf eine heiße Diskussion freuen.

Ihr
Dr. Jürgen Suppan
drsuppan@comconsult-akademie.de

Heftige Diskussionen

Fortsetzung von Seite 1

Worauf beruhen die ermittelten Einsparpotenziale und was ist die Basis des neuen Designs?

In dem genannten Projekt wurden alle Produkte aller namhaften und marktrelevanten Hersteller auf ihre Architektur, ihre Ausfallsicherheit und ihre Kostenstruktur untersucht. Dabei wurden gezielt die Stellen eines LAN-Designs ermittelt, die einen starken Einfluss auf die Gesamtkosten und die Gesamtleistung haben. Dem wurden die zur Zeit möglichen Design-Ansätze gegenüber gestellt. Dabei wurde insbesondere das Potenzial der neuen Technologien a la Rapid Spanning Tree untersucht und mit den Standard-Verfahren wie OSPF, VRRP und Link Aggregation kombiniert. Das Ergebnis ist ein Design, das als Kaskaden-Design bezeichnet wird und die Netzwerk-Struktur in den Gebäuden betrifft. Ziel ist die Reduzierung der Glasfaser-Ports der Switches in den Hauptverteilern. Das Ergebnis kann nur unter Nutzung des Rapid-Spanning Tree erzielt werden. Es muss noch einmal betont werden, dass die dargestellten Ergebnisse nicht auf den WAN-Bereich übertragen werden können.

Parallel wurden auf dem Netzwerk-Redesign-Forum 2002 neue LAN-Design-Ansätze für den Fertigungsbereich vorgestellt und diskutiert. Diese basieren auf Technologien, die von Hirschmann in die laufende IAONA-"Normung" eingebracht worden sind. Auch hier entstand eine erhebliche Diskussion auch hinter den Kulissen der Veranstaltung, da auf der einen Seite die besonderen Anforderungen der Fertigungsumgebung unstrittig sind auf der anderen Seite aber kaum ein Anbieter außer Hirschmann hier besondere Verfahren und Produkte anbietet. Insbesondere erschwert der isolierte Weg, den Siemens in der Automatisierungstechnik beschreitet, eine Bewertung.

Wir greifen diese Diskussion um die neuen Ansätze des LAN-Designs und auch die Hirschmann-Vorschläge für den Fertigungs-Bereich auf und machen sie zu einem der beiden Hauptschwerpunkte der diesjährigen Sommerschule. Auf der Sommerschule, der ComConsult Akademie 2002 werden die neuen Ansätze noch einmal durch Frau Borowka und Dr. Suppan präsentiert. Danach werden die Hersteller, voraussichtlich vertreten durch CISCO, Extreme und Hirschmann ihre Sicht präsentieren. Dr. Moayeri von der ComConsult Beratung und Planung wird diese Runde mit der Präsentation von Design-Ansätzen für sehr große Netzwerke abrunden. Anschließend werden die verschiedenen Sichtweisen in einer Podiumsdiskussion mit den Teilnehmern diskutiert.

Top Veranstaltung

Sommerschule 2002 mit vier absoluten Top-Knüllern

Die Sommerschule der ComConsult Akademie vom 1. bis 5. Juli 2002 kommt mit vier absoluten Top-Knüllern, die die heftige Diskussion der letzten Wochen zu diesen Themen aufgreifen. Traditionelle Netzwerk-Technologien werden durch neue Ansätze in Frage gestellt bzw. modifiziert. Was steckt dahinter? Top-Experten des Marktes stellen die verschiedenen Standpunkte vor, die beteiligten Kontrahenten vertreten ihre Sichtweise, in mehreren Podiumsdiskussionen treffen die verschiedenen Sichtweisen aufeinander.

Achtung: die Zahl der Teilnehmerplätze der Sommerschule ist stark beschränkt, da eine intensive Beteiligung der Teilnehmer an den Diskussionen ermöglicht werden soll. Zögern Sie deshalb nicht, sich rechtzeitig einen Platz zu sichern!

(Anmeldung auf Seite 4)

1. Neue LAN-Design- und Redundanz-Verfahren
mit Petra Borowka (UBN), Dr. Jürgen Suppan (ComConsult Akademie) und Dr. Behrooz Moayeri (ComConsult Beratung und Planung) und Kai Lorentz (IAONA)
- Vorstellung der aktuellen Design-Alternativen
- Kaskadendesign kontra traditionelle Verfahren
- Kostenreduzierung im LAN-Design
- Sichtweise der Hersteller: CISCO, Extreme und Hirschmann
- Sonderfall: Design von Fertigungsnetzen
- Sonderfall: Design sehr großer Lokaler Netzwerke
- Podiumsdiskussion aller Beteiligten

2. Netzwerk-Technologien neuester Stand: Trendanalyse
mit Dr. Jürgen Suppan (ComConsult Akademie)
- Entwicklungstrend IT-Technologien und die Konsequenzen für das Netzwerk
- Voice over IP: Aufstieg oder Fall einer Schlüsseltechnologie
- Wireless: Ausblick auf die nächsten Jahre
- Multimedia-Verkabelung
- Home-Networking
- Fertigungsnetze
- Ethernet-Positionierung im Gesamt-Netzwerk-Markt

3. Wireless-Technologien: die dominante Technik der nächsten Jahre
mit Dr. Jürgen Suppan (ComConsult Akademie), Dr. Franz-Joachim Kauffels, Dr. Jochen Wetzlar und Dr. Simon Hoff (ComConsult Beratung und Planung)
- Grundlagen der Wireless-Technologie
- Besonderheiten von Funknetzen
- Signalausbreitung, Störsituationen, Einfluss der Funktechnologie
- Netzwerkplanung: Antennenpositionierung und Feldabdeckung
- Leistungsvermögen von Wireless-Lösungen: Reichweiten Durchsatz, Fehlerraten, sinnvolle Teilnehmermengen
- Sicherheit und Wireless: Life-Vorführung eines Angriffs und Erklärung der Schwachstellen von Wireless
- Wireless-Analyse: was sollte ein Analysator können? Life-Vorführung eines typischen Produkts und Erläuterung der erforderlichen Funkitonalität
- Neue Standards: welcher Standard ist der richtige, Kompatibilitäts-Gesichtspunkte
- Gesundheitliche Risiken: Ergebnis einer Untersuchung

4. LAN-Analyse am Scheideweg
mit Dr. Jochen Wetzlar (ComConsult Beratung und Planung) und Agilent, Fluke Networks, Sniffer, Synapse
- Nutzbarkeit traditioneller Analysetechnik im Gigabit-Netzwerk
- Anforderungen an die moderne Analysetechnik
- Typische Störsituationen und ihre Analyse
- Produkte im Umbruch, Life-Vorführung der aktuellen und neuen Produkte von Agilent, Fluke, Sniffer und Synapse
- Podiumsdiskussion

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
Sommerschule der ComConsult Akademie 2002

☐ Ich melde mich an zur
Sommerschule der ComConsult Akademie 2002

vom 01.07. - 05.07.02 in Aachen

zum Preis von € 2.290,-- zzgl. MwSt.

☐ Bitte buchen Sie für mich ein Zimmer im Dorint Quellenhof in Aachen (€ 108,-- pro Übernachtung/Frühstück)

von _____ bis _____

Faxen Sie uns einfach diesen Abschnitt an **02408/955-399** oder schicken Sie eine eMail an **mail@comconsult-akademie.de** oder buchen Sie über unsere Web-Seite **http://www.comconsult-akademie.de** Ihren Platz auf unserer Veranstaltung.

Name	Vorname
Firma	Abteilung
Position	Funktion
Straße	PLZ, Ort
Telefon	Fax
eMail	Unterschrift

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
Netzwerk Sicherheits-Forum 2002

Ich melde mich an für das
Netzwerk Sicherheits-Forum 2002

☐ **vom 10.06. - 13.06.02 mit Tutorium**
zum Preis von € 1.790,-- zzgl. MwSt.

☐ **vom 11.06. - 13.06.02 ohne Tutorium**
zum Preis von € 1.590,-- zzgl. MwSt.*

☐ Bitte buchen Sie für mich ein Zimmer im Maritim Königswinter

von _____ bis _____
(€ 110,95 pro Übernachtung/Frühstück)

Faxen Sie uns einfach diesen Abschnitt an **02408/955-399** oder schicken Sie eine eMail an **mail@comconsult-akademie.de** oder buchen Sie über unsere Web-Seite **http://www.comconsult-akademie.de** Ihren Platz auf unserer Veranstaltung.

Vorname	Name
Firma	Abteilung
Position	Funktion
Straße	PLZ, Ort
Telefon	Fax
eMail	Unterschrift

Security

Sicherer Einsatz von TCP/IP auf IBM Hostsystemen

Die Implementierung des TCP/IP-Stacks auf IBM Host-Betriebssystemen und eng damit verbunden der Aufbau einer UNIX-Systemumgebung ist sicherlich ein entscheidender Grund dafür, dass der Mainframe nicht – wie oftmals vorhergesagt – nach und nach ausstirbt, sondern sich sogar noch einer Renaissance erfreut. Wie aber wirkt sich die Aktivierung von IP-basierender Kommunikation auf die (geradezu mythische) Sicherheit des Hosts und der auf ihm befindlichen Daten und Anwendungen aus?

Im folgenden werden kurz die wichtigsten Problemfelder aus Security-Sicht beim IP-Einsatz unter OS/390 (bzw. z/OS) umrissen und Lösungswege zur Absicherung des Hosts aufgezeigt.

Der Autor

Dipl. Phys. Frank Breitschaft war in verschiedenen öffentlichen Rechen-zentren für Konzeption und Betrieb größerer heterogener Netzwerke verantwortlich. Seit 1998 berät er bei der GAI NetConsult als Security Consultant größere und mittlere Unternehmen bei der umfassenden Sicherung ihrer IT-Umgebungen.

f.breitschaft@gai-netconsult.de

Problemfelder beim Einsatz von IP am Host

Worin liegen die Probleme, die sich aus der Aktivierung des IP-Stacks am Host ergeben?

Eigentlich sind die Themenfelder genau die selben, die man auch betrachten muss, wenn man IP-Anwendungen auf anderen Systemplattformen bereitstellt. In so fern ist es nichts Neues, neu sind die Punkte lediglich für die Hostumgebung und häufig auch für ihre Betreiber.

Die Problemfelder lassen sich mit folgenden Schlagworten umreißen:

- IP everywhere - starke Zunahme der mit dem Host über das bekanntermaßen sicherheitsanfällige IP-Protokoll konnektierten Systeme
- 08/15-Dienste - Nutzung von Netzwerkdiensten und -anwendungen, die im UNIX-Umfeld bereits seit langem als unsicher gelten
- Falsches Vertrauen in die RACF - ohne zuverlässige Authentisierung nützt die beste Autorisierungsdatenbank nichts

IP everywhere

Durch die Einbindung des Hosts in das IP-basierende Netzwerk eines Unternehmens ergeben sich eine Reihe von Vorteilen - zunächst einmal für die Netz- und Systembetreiber, die sich jetzt SNA sparen und sich stattdessen ganz auf IP als zentralem und einzigem Protokoll konzentrieren können. Das gilt von den Endgeräten über die Netzwerkkomponenten bis hin zu den UNIX- oder NT-Servern, die mit dem Host kommunizieren.

Daneben eröffnen sich mit IP aber auch eine ganze Reihe von Möglichkeiten zur Anbindung weiterer Netze und Systeme, z.B. im Remote Access oder VPN-Bereich. Aber genau da liegt auch das Problem: mit der zunehmenden (natürlich IP-basierenden) Vernetzung steigt die Anzahl der Systeme, die mit dem Host kommunizieren können, enorm an. Dabei handelt es sich nicht nur um Systeme, die direkte Anwendungen am Host nutzen und daher die IP-Konnektivität zum Host benötigen, sondern oft auch um Rechner, die nunmehr aufgrund bestehender oder neu geschaffener Netzverbindungen (zumindest theoretisch) den Host per IP erreichen, ohne dass dies eigentlich notwendig wäre. Fehlende Firewalls bzw. Filterregeln auf den Routern sind der Hauptgrund dafür, manchmal auch der Einsatz von Adressumsetzung (NAT) beim Anschluss von Netzen, so dass die Ausgangssysteme nicht mehr unterschieden werden können.

Häufig müssen wir feststellen, dass nicht nur von allen Rechnern eines Unternehmens IP-Konnektivität zum Host besteht, sondern dass auch noch ganze Netze von Dienstleistern, Partnern oder auch Kunden entsprechend angebunden sind (leider oft auch so, dass wiederum deren Dienstleister, Partner oder auch Kunden mehr oder weniger problemlos mit dem Host kommunizieren könnten).

Langer Rede kurzer Sinn: Ohne netzwerk- bzw. systemseitige Schutzmaßnahmen hat die Verwendung eines einheitlichen Netzwerkprotokolls fast zwangsläufig ein starkes Anwachsen der mit dem Host faktisch verbundenen Rechner und Netze zur Folge.

Für den nun über IP erreichbaren Host heißt dies aber, dass eine weitaus größere Zahl von Systemen für Angriffe gegen die auf ihm befindlichen Daten und Anwendungen genutzt werden können; zum einen durch den böswilligen Nutzer eines konnektierten Systems, aber auch in Folge der Kompromittierung eines der angeschlossenen Teilnetze. Wegen der Einheitlichkeit des Netzprotokolls sind auch Angriffe leichter denkbar, bei denen ein am Host zugriffsberechtigtes System als Relais missbraucht wird.

Hinzu kommt, dass das IP-Protokoll selbst bekanntermaßen so gut wie keine Sicherheitsfeatures bietet. So lassen sich durch das Setzen falscher Absende-IP-Adressen problemlos falsche Identitäten annehmen (IP-Spoofing). Aber auch andere häufig zu Prüfungen herangezogene Parameter wie Portnummer oder DNS-Name sind leicht fälschbar. Weitere sattsam bekannte Schwachpunkte liegen im mangelnden Schutz von Hilfsprotokollen gegen Manipulationen, wie z.B. Routingprotokollen. Zudem bietet IP selbst keine Mechanismen zum Schutz der Daten in punkto Vertraulichkeit und Integrität. Nicht zuletzt ist IP auch anfällig gegen so genannte Denial-of-Service (DOS)-Attacken, deren einziges Ziel es ist die Verfügbarkeit einer Ressource einzuschränken.

Fazit: Mit IP ergeben sich zum einen wesentlich mehr Ausgangsmöglichkeiten für Angriffe auf den Host, zum anderen bieten sich mit IP dem Angreifer viel "bessere" Möglichkeiten. Nicht zuletzt muss man auch berücksichtigen, dass Wissen über IP und seine Angreifbarkeit wesentlich verbreiteter ist als bei jedem anderen Netzwerkprotokoll.

08/15-Dienste

Wie ist aber die Angreifbarkeit eines Hosts über IP einzuschätzen?

Dabei sind (neben den Anwendungen selbst) zwei Bereiche relevant: der IP-Stack und die Kommunikationsdienste.

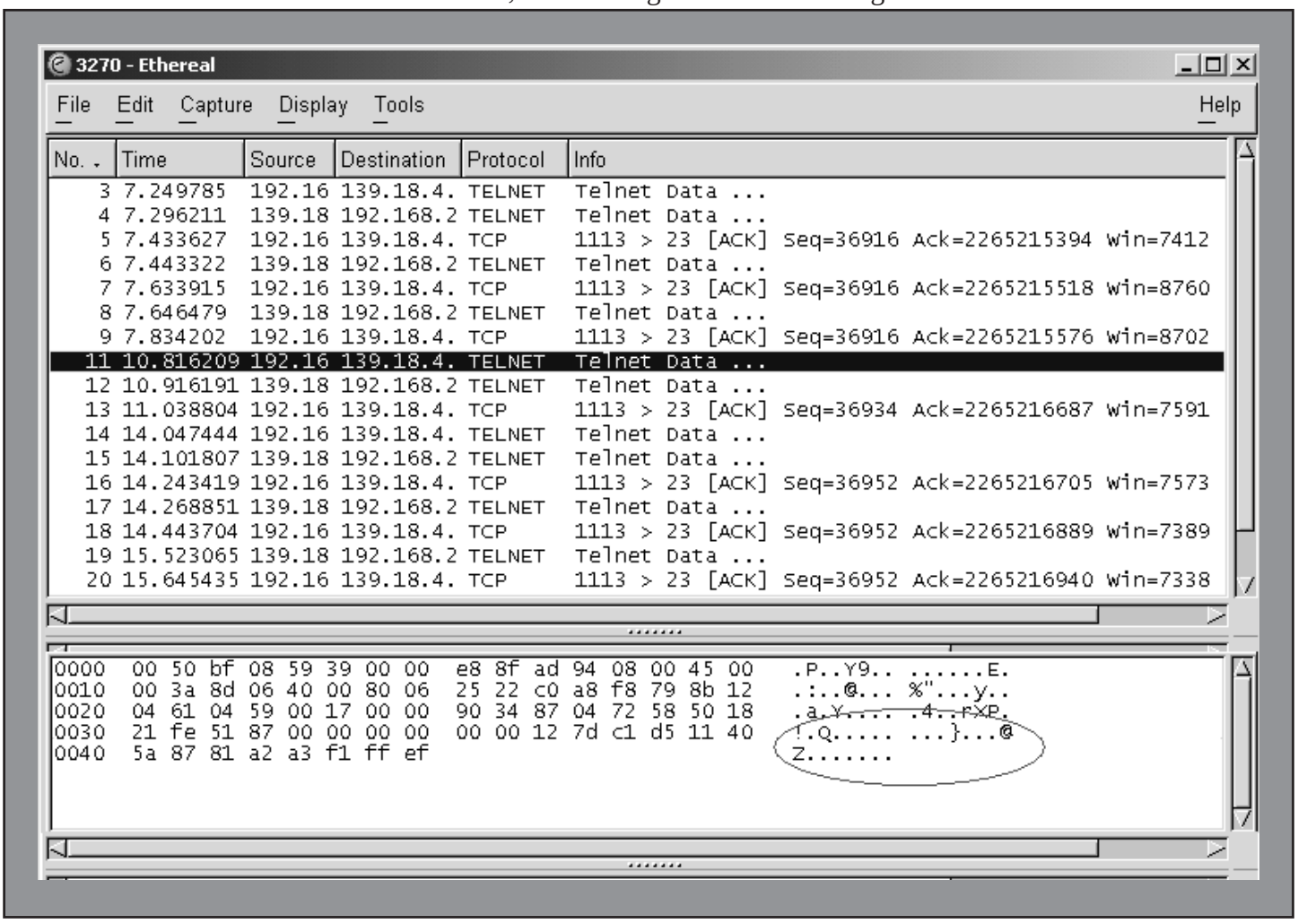
Wie bereits erwähnt war die Bereitstellung des IP-Stacks für das Host-Betriebssystem OS/390 eng mit dem Aufbau einer UNIX-Systemumgebung (auch als UNIX System Services bezeichnet) neben MVS verbunden. Der Grund ist ganz simpel: der IP-Stack selbst läuft innerhalb der UNIX-Umgebung von OS/390 ab - oder andersherum: der UNIX-Teil des Host-OS kommuniziert wie alle anderen UNIXe über IP. Da IBM bei der Entwicklung des IP-Stacks und der zugehörigen Dienste auf ihr UNIX-System AIX zurückgreifen konnte, wird vermutlich ein großer Teil des Codes identisch sein. Es liegen weder von IBM noch von dritter Seite Informationen vor, dass der Stack selbst besonderen Härtungsmaßnahmen oder Prüfungen unterzogen wurde. Da in der Vergangenheit immer wieder Implementierungsfehler in IP-Stacks gefunden wurden, die es erlaubten, Sicherheitsmaßnahmen zu umgehen oder die Verfügbarkeit des Zielsystems einzuschränken, muss auch für den Host-IP-Stack von potentiellen Sicherheitslücken ausgegangen werden. Aufgrund der Gesamtarchitektur des OS/390-Betriebssystems (insbesondere der Trennung von Code- und Datensegmenten im Speicher) haben diese aber vermutlich nicht so weitreichende Auswirkungen, wie in anderen Betriebssystemen.

Die größere Gefahr liegt aber eher in der weitgehenden Übernahme der Kommunikationsdienste aus dem UNIX-Umfeld, zum einen, was die Standards angeht, zum anderen (vermutlich) weitgehend auch, was den Code angeht.

In der Regel werden die meisten Unternehmen innerhalb der UNIX-Umgebung ihrer OS/390-Hosts Standard-UNIX-Dienste vorfinden, die in jedem Buch über Netzwerk oder UNIX-Sicherheit als problematisch eingestuft werden, beispielsweise:

- Telnet/TN3270, FTP: Klartextkommunikation (inkl. unverschlüsselte Übertragung der Passworte)
- Berkeley r-Dienste: basieren auf Vertrauensbeziehungen zwischen Systemen, die nur in geschlossenen Netzen sicher herzustellen sind
- TFTP: UDP-Variante von FTP ohne Authentisierung

Bild 1 Mitschnitt einer TN3270-Session; die übertragene Nutzerkennung ist zunächst nicht lesbar



Die genannten Sicherheitsprobleme gründen dabei weniger auf ggf. vorhandenen Bugs im Programmcode, sondern auf konzeptionellen Unzulänglichkeiten, die natürlich genau so auch im Hostumfeld weiter bestehen und gerade unter dem Aspekt der zunehmenden Vernetzung zu ernsthaften Problemen führen.

Aber so wie auch für den IP-Stack nicht von einer Fehlerfreiheit ausgegangen werden kann, gilt dies erst recht für die Zusatzdienste und natürlich auch für Applikationen. Dort wo der Code direkt aus anderen UNIX-Derivaten bzw. aus allgemein verbreiteten Bibliotheken übernommen wurde, werden die gleichen Bugs auftreten wie unter anderen UNIXen. Unter OS/390 werden die Auswirkungen auf die gesamte Systemumgebung oder andere Prozesse ggf. geringer sein, Fehler, die aber innerhalb der Applikation wirksam sind, beispielsweise Umgehung der Authentisierung oder Manipulation von Daten, werden am Host vermutlich genau zu den gleichen Konsequenzen führen. Fazit: Die Bewertung von Kommunikationsdiensten und Anwendungen muss am Host genauso erfolgen, wie beispielsweise im UNIX-Umfeld. Von einer höheren Sicherheit darf nicht per se ausgegangen werden.

Falsches Vertrauen in die RACF

Das Hauptargument für die Sicherheit von Hostanwendungen, das uns immer wieder vorgetragen wird, ist die RACF, welche ja die Zugriffe auf alle Ressourcen regele und sicher sei. Dabei sollte man sich aber vor Augen führen, dass die RACF zuvorderst eine Autorisierungsdatenbank ist. In ihr sind die Berechtigungen eines jeden Nutzers in einer im Vergleich mit anderen Systemen enorm feinen Abstufung verzeichnet. Voraussetzung für die Vergabe von Rechten an einen Nutzer ist aber zunächst dessen sichere Identifizierung, seine Authentisierung. Dazu werden in der Regel Nutzername und Passwort angefordert.

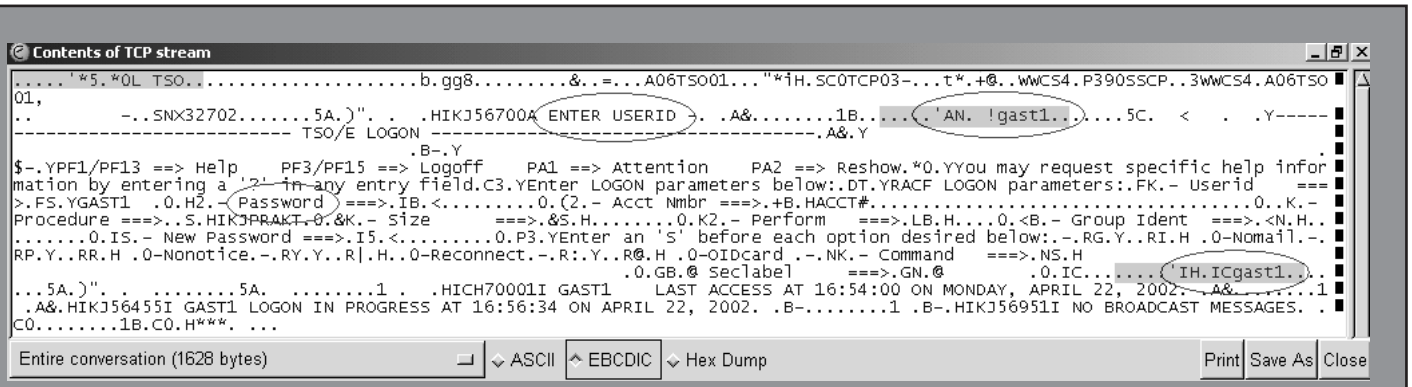
Und genau da liegt das Problem: ein mehrfach verwendbares Passwort bietet für die Vergabe von sensiblen Berechtigungen keinen ausreichenden Schutz - insbesondere dann, wenn es unverschlüsselt über das Netz übertragen wird. Genau das ist aber bei vielen Hostanwendungen der Fall, zum Beispiel bei TN3270-Kommunikation: Nutzername und Passwort gehen (wie bei Telnet) zu Beginn der Sitzung im Klartext über die Leitung und können mit herkömmlichen Mitteln abgehört werden; der einzige "Trick" dabei ist, den Netzwerksniffer von ASCII auf EBCDIC umzustellen (siehe Bilder 1 und 2).

Wird aber das Passwort von einem Angreifer, der ein System oder Teilnetz kompromittiert hat, mitgelesen, kann er sich anschließend unter der gewonnenen Kennung erfolgreich gegenüber der RACF authentisieren und wird dementsprechend autorisiert. Das einzige "Problem" des Angreifers ist es vermutlich, die "richtigen", hoch privilegierten Kennungen von den unwichtigen zu trennen. Aber auch hier gibt es Hoffnung für den Angreifer: bei eingehender Prüfung der in der RACF abgebildeten Berechtigungsstruktur stellen viele Unternehmen fest, dass die Rechte bei weitem nicht so granular vergeben wurden, wie es möglich wäre, und dass oftmals zu weit gehende Berechtigungen (beispielsweise für Operatoren) eingeräumt wurden.

Fazit: Ohne adäquate Authentisierungs- und Kommunikationsverfahren ist die Vergabe von sensiblen Rechten über die RACF angreifbar.

Das folgende Angriffsszenario soll noch einmal das Zusammenwirken der drei genannten Problemfelder in einem Beispiel verdeutlichen: Einem Angreifer ist es gelungen, den schlecht gesicherten Internetzugang einer Werbeagentur zu hacken. Zu seiner Freude stellt er fest, dass die Agentur regelmäßig größere Graphikdokumente per FTP über eine Wählleitung zu einem großen Unternehmen überträgt. Noch mehr freut ihn, dass offenbar keine Filterregeln eingerichtet sind, so dass er eine Vielzahl von Systemen im Unternehmensnetz anpingen kann. Schnell ist ein Linux-Rechner gefunden, der noch einen angreifbaren Telnet-Daemon besitzt (siehe z.B. http://www.kb.cert.org/vuls/id/745371). Ein paar herumliegenden Skripten lässt sich entnehmen, dass der Rechner wohl für die Auswertung von Routerprotokollen genutzt wird (sprich: in diesem Netzsegment ist mit Administratoren zu rechnen). Nach Installation eines ARP-Spoofing-Tools lässt sich der gesamte Verkehr am lokalen Switch mitlesen. Mit einem kleinen Programm, das gezielt nach Authentisierungsinformationen sucht, wird die Spreu vom Weizen getrennt – jetzt heißt es nur noch Warten. Beim nächsten Upload von Dokumenten durch die Werbeagentur (und der damit verbundenen Möglichkeit zum Zugriff auf den gehackten Linux-Rechner) finden sich tatsächlich eine Reihe von Telnet und FTP-Passworten, aber viel interessanter sind diese merkwürdigen EBCDIC-Zeichenketten im Verkehr mit dem Rechner lpar1.rz.xxx.de.

Bild 2 Auswertung der EBCDIC-Zeichen der TN3270-Session



vom Server (auf weißem Grund) bzw. Client (grau unterlegt) gesendete Daten; eingekreist sind die Anfrage nach Nutzername und Passwort sowie die jeweiligen Antworten des Nutzers (gast1/gast1) zu erkennen.

Sicherer Einsatz von TCP/IP auf IBM Hostsystemen

Jetzt kommt es nur noch darauf an, welche Berechtigungen mit den darin enthaltenen Kennungen verbunden sind - vielleicht war einer der Netzadministratoren in der Arbeitsvorbereitung oder Operator im Hostumfeld, aber auch ein "Sachbearbeiter"-Zugang zu den Daten ist sicherlich interessant.

Sicherung der Host-IP-Umgebung

Ich denke, es ist deutlich geworden, dass die Inbetriebnahme von IP am Host nicht als einfaches Umlegen eines Schalters verstanden werden darf, sondern dass die damit verbundenen Sicherheitsprobleme umfassend betrachtet werden müssen, um böse Überraschungen zu vermeiden. Ganz wichtig ist dabei, sich noch einmal darüber klar zu werden, wie hoch einerseits der Schutzbedarf der am Host gespeicherten Daten und Applikationen des jeweiligen Unternehmens ist. Im Vergleich dazu ist das Sicherheitsniveau des IP-Netzes, an das der Anschluss erfolgen soll, und seiner Außenzugänge (Internet, Remote Access, Partner etc.) zu sehen.

Unserer Erfahrung nach klafft hier oft eine Lücke: während die Hostressourcen meist (zu Recht) als hoch schutzbedürftig eingestuft werden, ist das Netz nur auf einen mittleren Schutzbedarf hin ausgelegt, also beispielsweise anhand der Vorgaben des BSI-Grundschutzhandbuchs gesichert.

Der daraus resultierende zusätzliche Sicherungsbedarf muss nun durch netzwerkseitige Schutzmaßnahmen, durch systemseitige Härtung am Host und/oder durch spezielle Sicherung auf Anwendungsebene befriedigt werden. Im folgenden werden wir die einzelnen Punkte kurz ausführen.

Perimeterschutz

Die einfachste Maßnahme zum besseren Schutz der Hostumgebung ist häufig der Aufbau eines netzwerkseitigen Perimeterschutzes, also die Entkopplung der jeweiligen IP-Netze und die Sicherung der Übergänge durch geeignete Firewall-/Filterlösungen. Der geschützte Bereich kann dabei je nach Anforderungen das gesamte Rechenzentrumsnetz oder Teile davon umfassen. Manchmal kann es aber auch sinnvoll sein, lediglich den Host selbst dort anzusiedeln, ihn also direkt hinter einer Firewall anzubinden. Ziel des Perimeterschutzes muss es sein, den IP-Verkehr mit dem Host auf das notwendige und zugelassene Maß (sprich: zugelassene Nutzer und Dienste) einzuschränken und unzulässigen Verkehr gar nicht erst bis zum Host gelangen zu lassen. Insbesondere ist dabei anzustreben, administrative Arbeiten oder andere hoch privilegierte Zugriffe wirksam zu kontrollieren. Das wird insbesondere dort gut gelingen, wo aus den Nutzernetzen heraus keine direkte Client-Server-Kommunikation mit dem Host stattfindet oder die zugänglichen Dienste per se gut zu sichern und zu kontrollieren sind.

Ist aber als Dienst beispielsweise TN3270 vorgesehen, über den Mitarbeitern sowohl "normale" Anwendungsprogramme am Host nutzen, aber über den auch administrative Tätigkeit möglich ist, kann ein Perimeterschutz alleine nicht ausreichen.

Systemseitige Schutzmaßnahmen

Für die Sicherung der IP-Kommunikation eines OS/390-Systems stehen systemseitig bereits eine Reihe von Komponenten zur Verfügung:

Zugriffskontrolle auf den IP-Stack

Zur Absicherung der IP-basierten Kommunikationsbeziehungen stehen eine Reihe von Zugriffseinschränkungen auf den Stack zur Verfügung: Network, Stack und Port Access Control.

Ihnen allen ist gemeinsam, dass sie im Wesentlichen erst ab der OS/390-Version 2.10 (und somit auch in z/OS) umfassend zur Verfügung stehen. Mittels Network Access Control lässt sich die vom Host ausgehende IP-Kommunikation bezüglich der Ziel-IP-Adressen einschränken, so dass der Datenexport an unberechtigte Clients bereits auf IP-Ebene unterbunden werden kann.

Allerdings lassen sich über diese Methode Angriffe gegen die Verfügbarkeit, die lediglich auf eingehenden Datenpaketen basieren, nicht zuverlässig ausschließen. Mit Stack und Port Access Control lässt sich darüber hinaus die Nutzung des bzw. der IP-Stacks durch Anwendungen und Nutzer wirksam einschränken.

Über diese Mechanismen lässt sich weitgehend die Schutzfunktion eines sonst typischerweise vorgeschalteten Paketfilters direkt am Host abbilden, mit dem zusätzlichen Vorteil, dass sowohl auf Nutzerberechtigungen (RACF) zurückgegriffen werden kann, als auch eine direkte Bindung zwischen Applikation und Filterregel (und nicht wie sonst zwischen Portnummer und Filterregel) hergestellt werden kann.

SecureWay Security Server unter OS/390

Die optionale Komponente Security Server bietet für OS/390 eine Reihe von zusätzlichen Firewallfunktionen, die über die o.g. Access Control Mechanismen hinausgehen. Die wichtigsten Features dabei sind:

- IP-Paketfilter: Anhand der in den Headern der Layer 3 und 4 enthaltenen Adressierungsinformationen lässt sich die Weiterleitung von IP-Paketen zwischen zwei Netzwerkinterfaces unterbinden bzw. zulassen. Eine Überprüfung des Sessionzusammenhangs bei TCP oder eine Filterung der Applikationsprotokolle ist hierbei nicht möglich. Lediglich für FTP steht ein Proxy-Server zur Verfügung.

- VPN-Server: Der SecureWay Security Server bietet umfangreiche Möglichkeiten zum Aufbau von verschlüsselten Verbindungen mit Hilfe des IPSEC-Protokolls. Dabei ist sowohl die statische Tunneldefinition als auch dynamische Aushandlung mit ISAK-MP (heute IKE) möglich.

Darüber hinaus bietet der Security Server die Möglichkeit, sowohl die RACF, als auch LDAP-Verzeichnisse für Authentisierungs- und Autorisierungszwecke einzubinden. Da keine Kontrolle des Verkehrs auf Verbindungs- und Applikationsebene möglich ist, kann der Security Server nicht das Schutzniveau eines typischen netzwerkbasierenden Firewalls im Perimeter erreichen. Insbesondere zur Absicherung von Zugriffen auf webbasierende Anwendungen bietet er keinen ausreichenden Schutz. Sinnvoll ist daher aus unserer Sicht vor allem ein Einsatz da, wo ein herkömmlicher Perimeterschutz nicht sinnvoll realisiert werden kann (z.B. zur Absicherung von Verkehr zwischen zwei Host-LPARs) oder wenn der Host dedizierter Endpunkt von VPN-gesicherten Verbindungen sein soll. Letzteres kann beispielsweise die Ende-zu-Ende-Absicherung der Kommunikation zwischen mehreren Host-Systemen sein, die auf verschiedene Rechenzentren verteilt sind und denen kein ausreichend vertrauenswürdiges Netz zur Verfügung steht.

OS/390 UNIX level security

OS/390 bietet neben der üblichen UNIX-Rechtevergabe auf Ressourcen (anhand von Eigentüme und Gruppennummer) ein erweitertes Rechtevergabeschema an. Insbesondere lassen sich die mit Superuser-Privilegien verbundenen Rechte (innerhalb der Prozessausführung und bei Zugriffen auf das Dateisystem) granularer aufteilen. Bei konsequenter Nutzung dieser Möglichkeiten können die

Auswirkungen von Schwachstellen in einzelnen IP-Diensten stärker eingeschränkt werden, auch wenn der Dienst über die eigentlichen Zugriffsrechte des Nutzers hinausgehende Funktionen benötigt. Auch wenn damit die bei UNIX häufig zu beobachtende Kompromittierung des Gesamtsystems aufgrund einer Schwachstelle in einem einzelnen IP-Dienst wirksam unterbunden werden kann, bleiben dennoch die Risiken innerhalb des IP-Dienstes selbst bestehen. Zudem bleibt offen, in wie weit alle IP-basierenden Anwendungen (insbesondere Kaufsoftware und/oder Software, die von herkömmlichen UNIXen portiert wurde) diese Möglichkeiten voll ausschöpfen.

TCP/IP application security

Unter diesem Stichwort bietet OS/390 für die meisten mitgelieferten Standard-Dienste Sicherungsmöglichkeiten. Dabei sollte aber berücksichtigt werden, dass die beste Sicherung (auch im Host-Umfeld) ein abgeschalteter Dienst ist. Ebenso wie bei allen anderen Systemwelten sollten zunächst alle Dienste deaktiviert und erst bei Bedarf und nach Prüfung freigegeben werden. Besteht aber Bedarf an einem der Standard-Dienste, kann er erfreulicherweise stärker abgesichert und feiner konfiguriert werden als im Gros der UNIX-Umgebungen. Beispiele dafür sind die Kerberos-Unterstützung für Telnet, RSH und FTP sowie die SSL-Verschlüsselung für Webserver und TN3270-Kommunikation (siehe auch weiter unten).

Schutz auf Anwendungsebene

Neben netzwerk- und systemseitigen Schutzmaßnahmen ist natürlich auch anwendungsseitig für eine Sicherung zu sorgen. Im einzelnen müssen diese natürlich vor dem Hintergrund der tatsächlichen Anwendung diskutiert werden. Erfahrungsgemäß sind dabei folgende zwei Bereiche immer wieder kritisch:

- Authentisierung und Autorisierung: Die zulässigen Nutzer einer Anwendung müssen zunächst zuverlässig authentisiert werden, bevor ihnen möglichst fein abgestufte Berechtigungen zugeordnet werden können. Mit den üblichen mehrfach verwendbaren Passworten lässt sich - insbesondere im Zusammenhang mit unverschlüsselter Übertragung über nur bedingt vertrauenswürdige Netzwerke - kein hoher Schutz erreichen. Hier sollten generell stärkere Verfahren eingesetzt werden, beispielsweise Token oder SmartCards.

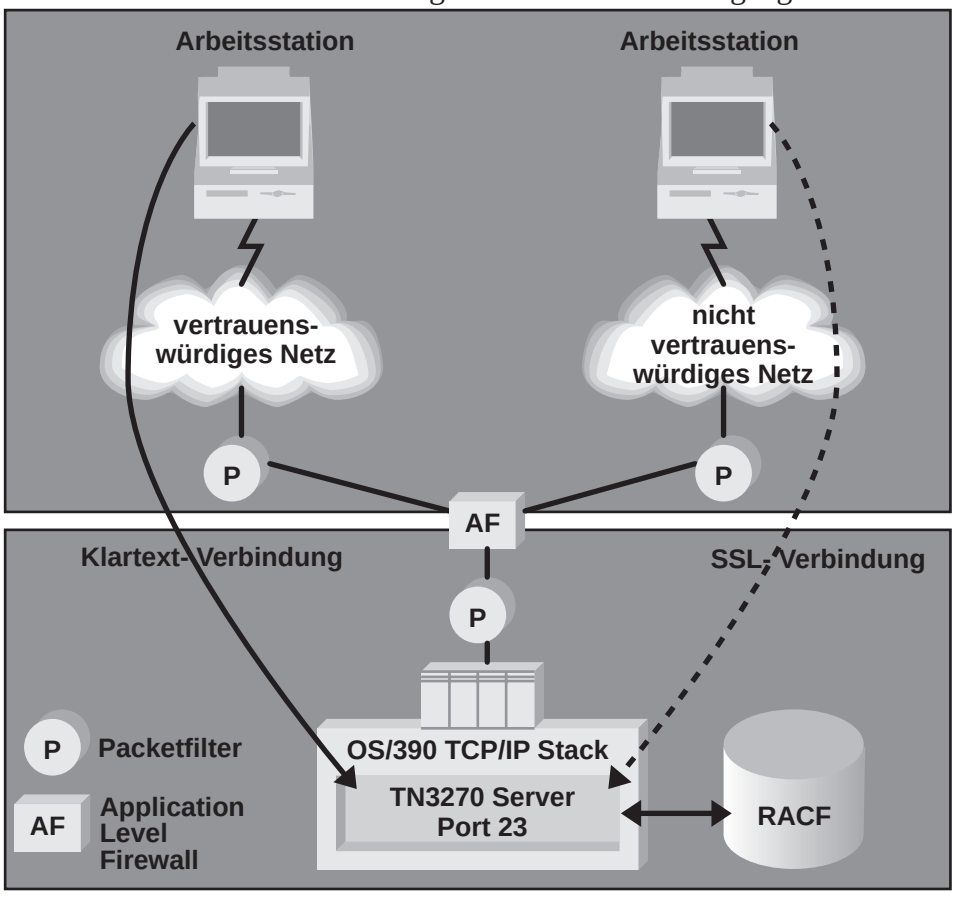
- Kommunikationsverfahren: Leider tauschen eine Vielzahl von Anwendungen ihre Daten immer noch unverschlüsselt und unsigniert aus. Da das IP-Protokoll hier direkt keine eigenen Schutzmaßnahmen mitbringt, kann ein Angreifer leicht vertrauliche Informationen mitlesen oder sogar Daten während der Übertragung verfälschen. Bei der Übermittlung über nicht (ausreichend) vertrauenswürdige Netze sollten daher zusätzliche Verschlüsselungsprotokolle eingesetzt werden, wie sie beispielsweise mit SSL und IPSEC für den Host zur Verfügung stehen.

Anhand von zwei Beispielen soll kurz illustriert werden, wie die Absicherung der Hostumgebung konkret aussehen kann:

Unterschiedlich stark abgesicherter TN3270-Zugang zu SNA-Anwendungen

TN3270-Zugänge zu Hostsystemen lassen sich relativ einfach absichern, da die üblicherweise eingesetzten Clientprogramme bereits die verschlüsselte Kommunikation über SSL unterstützen. Auch der TN3270-Server in OS/390 ist seit Version 2.6 SSL-fähig. Ab Version 2.10 kann auch unter einer Server-Portnummer (in der Regel 23) sowohl verschlüsselte, als auch unverschlüsselte Kommunikation parallel abgewickelt werden. Bild 3 zeigt ein Szenario, in dem über zwei unterschiedlich vertrauenswürdige Netze auf einen Host zugegriffen wird. Der Host selbst ist über eine Application-Level-Firewall von beiden Netzen abgetrennt, an der lediglich der Telnet-Proxy freigegeben ist. Der TN3270-Server ist nun so konfiguriert, dass anhand der Client-IP-Adresse bestimmt wird, ob der Nutzer sich im vertrauenswürdigen Netz befindet. Für diese Nutzer wird keine SSL-Verschlüsselung gefordert und es wird die normale Nutzername/Passwort-Authentisierung verwendet. Nutzer aus dem nicht vertrauenswürdigen Netz müssen hingegen eine verschlüsselte Verbindung über SSL aufbauen, die sicherstellt, dass nicht nur die Authentisierungsinformation, sondern auch der gesamte Datenstrom nicht mitgelesen werden kann. Optional lässt sich mit SSL Client-Zertifikaten auch noch eine weitere Verbesserung der Authentisierung erreichen. Nebenbemerkung: Da hier an der Client-IP-Adresse eine für den Sicherheitskontext wesentliche Entscheidung festgemacht wurde, muss ein ausreichender Schutz gegen Vorgabe einer falschen Identität (IP-Adresse) gegeben sein. Im abgebildeten Szenario wird dies durch die Firewall gewährleistet, die Adressen des vertrauenswürdigen Netzes nur am entsprechenden Interface zulässt.

Bild 3 Unterschiedlich stark gesicherter TN3270-Zugang



Absicherung einer Websphere-Anwendung

Webbasierte Anwendungen sind aus Sicherheitssicht äußerst kritisch zu betrachten, da eine Risikoanalyse den gesamten Kommunikationsweg vom Client bis zum Backendserver (Host) umfassen muss. Eine direkte Verbindung zwischen Client-Desktop und dem Web-Application-Server (2-tier-Modell) ist unbedingt zu vermeiden, da jede dort auftretende Schwachstelle eine hohe Gefährdung des gesamten Hostbereichs zur Folge hätte. Es sollte deshalb immer ein separierter Webserver als Kommunikations-Gateway zwischen Client und Web-Application-Server genutzt werden.

Auch der Webserver als erster Anlaufpunkt jeder Verbindung muss aber als besonders gefährdet eingestuft werden, wie die Erfahrungen von vielen erfolgreichen Attacken und bekannt gewordenen Schwachstellen aufzeigen. Neben einer Manipulation der Inhalte muss sogar die Übernahme des ganzen Servers einkalkuliert werden. Dies gilt praktisch für alle verfügbaren Webserver und damit auch für den HTTP-Server für OS/390 von IBM (Abkömmling des populären Webservers Apache), der häufig zusammen mit WebSphere eingesetzt wird.

Daher wird folgende Kommunikationsarchitektur eingesetzt (siehe Bild 4):

Der extern erreichbare Webserver soll aus Performance- und Skalierbarkeitsgründen ebenfalls unter OS/390 ablaufen und wird daher in einer vollständig getrennten logischen Hostpartition (LPAR) betrieben. Aus den Clientnetzen ist er nur über eine Application Level Firewall zu erreichen. [Nebenbemerkung: Da die Kommunikation zwischen Client und Webserver zum Schutz der Vertraulichkeit über SSL geführt wird, können die meisten Firewalls keine über den TCP-Session-Zusammenhang hinausgehende Kontrolle vornehmen. Löbliche Ausnahme: Symantec Enterprise Firewall (früher Axent Raptor), die zumindest den Ablauf des typischen SSL-Handshakes überprüft.] Von einem im Webserver integrierten HTTP-Plugin aus wird der Verkehr zum eigentlichen Application-Server in der zentralen Backend-LPAR weitergeleitet. Der Übergang zwischen den LPARs wird über die Secure Server Option am IP-Stack der Backend-LPAR geschützt.

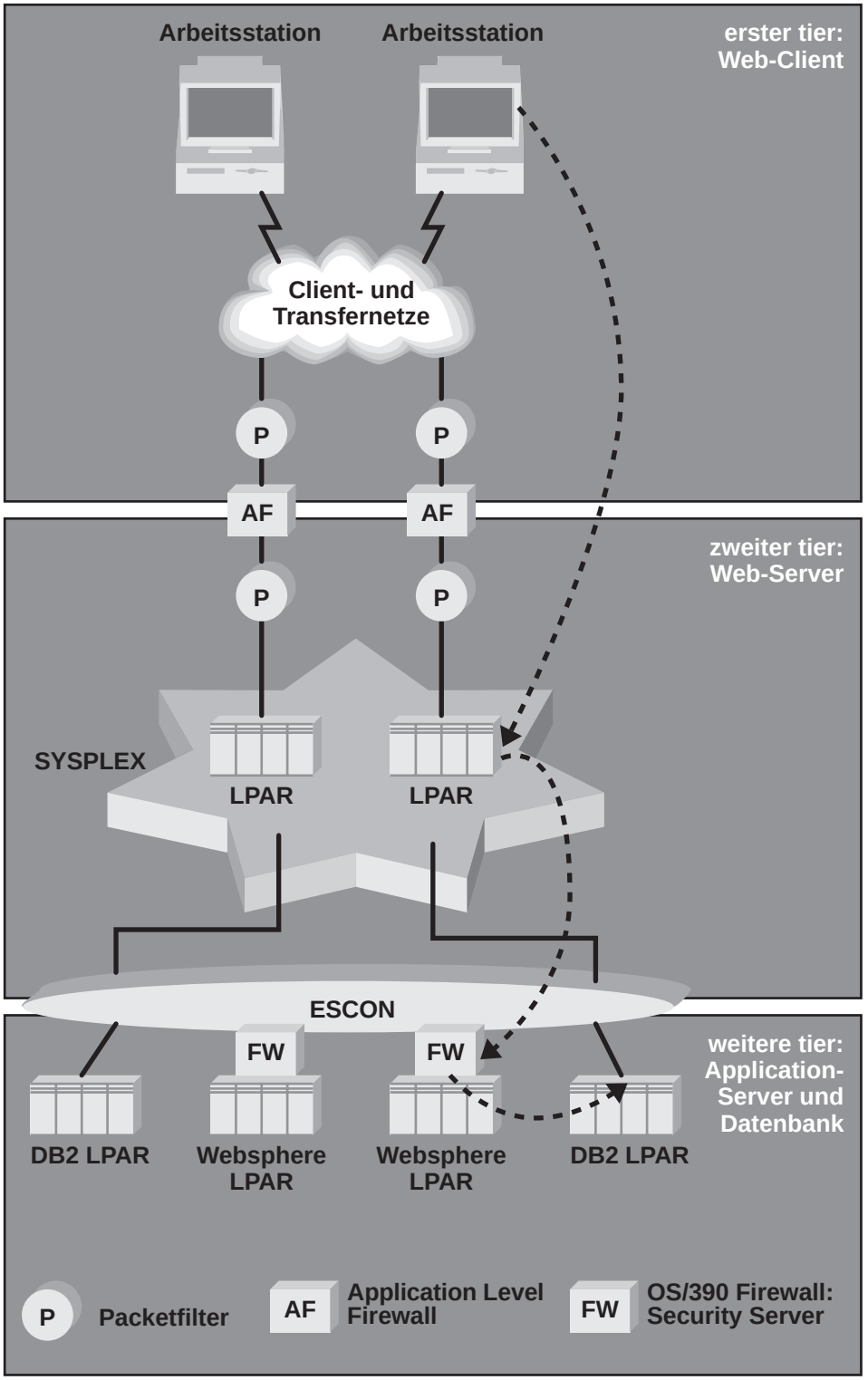


Bild 4 Mehrstufige Absicherung einer Websphere-basierenden Anwendung

Referenzen

Für die weitere Vertiefung sei auf den großen Fundus der IBM RedBooks verwiesen (http://www.redbooks.ibm.com):

- Secure e-business in TCP/IP Networks on OS/390 and z/OS, SG24-5383-01, IBM Redbook, published June-11-2001
- IBM WebSphere V4.0 Advanced Edition Security, SG24-6520-00, IBM Redbook, published March-19-2002

Konvergenz zu IP in mobilen Kommunikationssystemen - Weniger ist mehr

Dr. Simon Hoff ist technischer Direktor der ComConsult Beratung und Planung und blickt auf jahrelange Projekterfahrung im Bereich lokaler Netze und mobiler Kommunikationssysteme zurück.
hoff@comconsult.com

Dr. Joachim Wetzlar von der ComConsult Beratung und Planung bekam auf dem Netzwerk-Redesign Forum 2002 standing ovations für seinen Vortrag "Wireless LANs".
wetzlar@comconsult.com

Fortsetzung von Seite 1

Ist die Nachfrage nach neuen mobilen Diensten wirklich groß genug?

Die Frage nach den Diensten zieht automatisch die Frage nach den Endgeräten für UMTS nach sich.

Bislang gab es für Europa nur Designstudien und Prototypen zu sehen. Die rechtzeitige Verfügbarkeit von Endgeräten in genügend großer Stückzahl ist ein entscheidender Faktor. Es gibt bereits Stimmen, die nicht von einer ausreichenden Verfügbarkeit vor 2004 ausgehen. Marktreife Endgeräte vor Ende 2002 in Europa vorzufinden, gilt als unwahrscheinlich.

Ein beträchtliches Risiko, denn schon jetzt kostet jeder Tag mehr als eine Million Euro an Zinsen für Lizenzkosten und Investitionen in die Netztechnik.

Auf einen unmittelbaren Quantensprung sollte man sich also nicht in den ersten UMTS-Netzen einstellen. Die Erwartungshaltung ist jedoch sehr groß und wurde lange von Marketingstrategen auf Seite von Betreibern und Ausrüstern, aber auch von der Politik geschürt. Dass NTT Docomo, der japanische Vorreiter für den Einsatz von UMTS, vergangenen Jahres erst mit Verspätung in Betrieb gegangen ist, bis Anfang des Jahres noch mit technischen Problemen gekämpft hat und Ende Februar mit 55.000 Teilnehmern hinter den Erwartungen liegt, belastet das Klima zusätzlich.

Nur zum Vergleich: Die Anzahl der GSM-Teilnehmer lag Ende 2001 weltweit bei 640 Millionen.

Gerüchte über Probleme bei Ausrüstern und Betreibern verdichten sich und sind inzwischen zur gewohnten Presselektüre geworden. Was den deutschen Markt betrifft, blieb man - zumindest offiziell - bis vor kurzem noch bei einem Startschuss Ende diesen Jahres.

Erschwerend kommt hinzu, dass die Ausrüster von der allgemeinen Flaute zum Teil erheblich getroffen wurden. Nortel hat zigtausend Mitarbeiter entlassen, und bei Ericsson, Alcatel, Siemens usw. sieht es ähnlich aus. Ein Dominoeffekt droht, der zu einer internationalen Verzögerung (und mehr) führen kann.

Trotz aller Sparmaßnahmen: Der "point of no return" für UMTS ist überschritten. Dies ist nicht notwendig negativ zu sehen. Es wird unerwartete Kräfte freisetzen, denn UMTS darf nun einmal kein Misserfolg werden, und da werden alle letztendlich an einem Strang ziehen.

Obwohl das System kurz vor der Einführung steht und damit wesentliche technologische Weichen bereits gestellt sind, scheint uns die skizzierte Problemsituation Grund genug, diese Technik aus einem anderen Blickwinkel zu betrachten. Kann die gegebene Notlage die Evolution nicht beschleunigen oder sogar in eine andere Richtung lenken? All-IP ist in diesem Zusammenhang ein Begriff, dem man spätestens seit vergangenem Jahr vermehrt in der mobilen Kommunikation begegnet. All-IP bedeutet den konsequenten Einsatz von IP in der gesamten Netzinfrastruktur, Ende zu Ende, von Access zu Core, in Transport und in Signalisierung. Dies wäre ein fundamentaler Schritt in der Evolution mobiler Kommunikationssysteme.

Dieser Artikel wird dem Schlagwort All-IP auf den Grund gehen und Lösungsansätze, die zur Zeit von den verschiedenen Ausrüstern und Standardisierungsgremien erarbeitet werden, vorstellen. Insbesondere werden die Fragen analysiert, ob, wann und wie in UMTS mit einer Konvergenz zu IP Netzen zu rechnen ist und welche Konkurrenz von WLAN dem bisher wenig beachtetem Mitspieler ausgehen kann. Bild 1 (nächste Seite) zeigt zur Einstimmung eine typische Klassifizierung mobiler Kommunikationssysteme, wie wir sie seit Jahren in einschlägigen Veröffentlichungen gesehen haben. Zunächst wollen wir diese Klassifikation hinnehmen und das Thema quasi mit der Steigerung der Datenrate erschließen. Später werden wir sehen, dass die isolierte Betrachtung von Datenrate und Mobilität eigentlich keinen Sinn mehr macht. Andere Parameter wie Dienstflexibilität und Dienstgüte sind wesentlich bedeutsamer geworden.

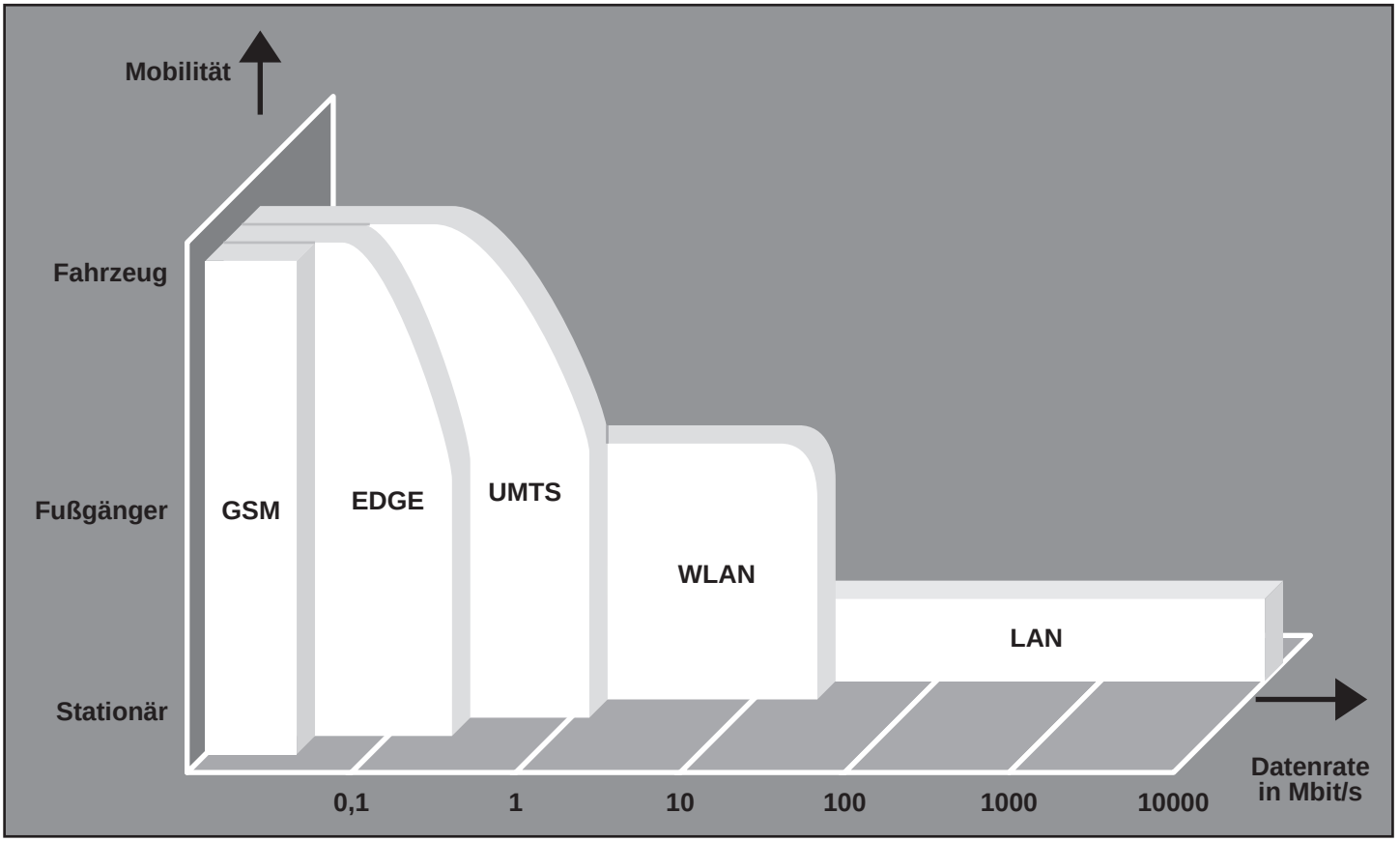


Bild 1 Datenraten im Vergleich zur Mobilität

2.
Die zweite Generation: Mobile Kommunikation für jedermann und überall

Mit der Phase 2 des Global System for Mobile Communications (GSM) ist die mobile Telekommunikation in ihrer zweiten (sprich: digitalen) Generation ein Massenmarkt geworden. Sprachdienste, Short Message Service (SMS), Wireless Application Protocol (WAP) etc. ermöglichen eine selbstverständlich gewordene Erreichbarkeit und Informationsversorgung für jedermann, jederzeit an (fast) jedem Ort.

GSM Phase 2 basiert auf einer leitungsvermittelnden Netzarchitektur mit einem kombinierten FDMA/TDMA-Verfahren auf der Luftschnittstelle und bietet Datenübertragung mit maximal 9.6 kb/s, was der Bandbreite möglicher Anwendungen natürlich erhebliche Grenzen setzt [1]. Die Einführung von High-Speed Circuit Switched Data (HSCSD) in GSM Phase 2+ hat am Prinzip der Leitungsvermittlung nichts geändert; die Kapazität wird jedoch durch Kanalbündelung auf maximal 57,6 kb/s gesteigert [2].

2.1
Mobil und "Always Online"

Für viele Anwendungen ist die permanente Reservierung einer kostbaren Ressource unökonomisch. Dem Wunsch, "always online" und nach Tarifen gemäß übertragenem Datenvolumen kann jedenfalls nur mit einer paketvermittelnden Netzstruktur gedient werden. Mit der Einführung des General Packet Radio Service (GPRS) in GSM Phase 2+ soll jetzt dieser Markt der mobilen Datenkommunikation erobert und der Teilnehmer mit einer Vielzahl mobiler Anwendungen versorgt werden. Nach E-Commerce macht nun das Schlagwort M-Commerce zusammen mit Mobile Internet die Runde [3].

GPRS bietet eine paketvermittelnde Netzarchitektur, d.h. die Einführung zusätzlicher Protokolle auf der Luftschnittstelle, zwischen Mobiltelefon und Base Station Controller sowie neue Knoten und Schnittstellen in der Netzinfrastruktur. Das Netz wird quasi zweigeteilt, in einen leitungsvermittelnden Teil und in einen paketvermittelnden Teil. Analog stehen auf der Luftschnittstelle Kanäle für klassisches GSM und für GPRS zur Verfügung (ohne die grundsätzliche physikalische Übertragungstechnik zu ändern). In diesem Sinne ist GPRS also in das bestehende GSM voll integriert. Ein "Nicht-GPRS-Endgerät" wird durch die Anwesenheit von GPRS nicht weiter gestört; es nutzt einfach die leitungsvermittelten Übertragungsressourcen. Umgekehrt vereint ein GPRS-Endgerät typischerweise beide Möglichkeiten, d.h. Sprachdienste gehen ihren gewohnten Weg gemäß GSM Phase 2.

Theoretisch kann GPRS zwar mit einer Datenrate von etwa 170 kb/s aufwarten (wenn alle 8 Slots genutzt werden können und ermöglicht durch exzellente Empfangsbedingungen auf Codes zur Fehlerkorrektur verzichtet werden kann). In der Praxis wird man diesen Wert nie finden, denn allein der erforderliche Energiebedarf ist für mobile Endgeräte im "Handy-Format" zu hoch. GPRS-Mobiltelefone bieten zur Zeit meist vier Downlink-Slots und einen Uplink-Slot (als "4+1" bezeichnet). Die Datenrate pro Slot hängt von der Kodierung ab, deren Auswahl den Empfangsbedingungen angepasst wird.

Bei schlechtem Empfang (niedriges Verhältnis von Signal- zu Störleistung) würde mit CS-1 (Coding Scheme) etwa 9 kb/s pro Slot erreicht, mit CS-2 13,4 kb/s, mit CS-3 15,6 kb/s und bei sehr guten Empfangsbedingungen erlaubt CS-4 schließlich 21,4 kb/s. Bei einer typischen Konfiguration mit 4+1 und CS-2 erhält man nach Abzug von weiterem Protokoll-Overhead (MAC und LLC) 12 kb/s pro Slot und damit dann eine (durchaus realistische) Datenrate von 48 kb/s, die mit Kompressionsmechanismen auch noch verbessert werden kann [4].

Leider ist das Spektrum für GSM knapp bemessen. Obwohl GPRS eine höhere Datenrate anbietet, mit paketvermittelnden Techniken die Ressourcenvergabe den Anwendungsanforderungen entsprechend optimiert, hohen Erwartungshaltungen an ein Mobile Internet wird GPRS nicht entsprechen können. Mobilität hat nun einmal seinen Preis. Nichtsdestotrotz, GPRS ist ein spannendes System: Ohne dramatische Änderungen ist es gelungen, auf eine sinnvolle, wenn auch einfache Weise, mobile Datendienste zu erbringen. Wir sind überzeugt, dass in GPRS ein erhebliches Marktpotential liegt. Man sollte sich nie durch plakatives Bitratenzählen blenden lassen.

2.2
Zwischen den Generationen: Mobile Multimedia ist machbar

Mit EDGE (Enhanced Data rates for Global Evolution) kann das dem GSM zugewiesene Spektrum effizienter genutzt werden. EDGE optimiert unter anderem die Modulation zur Funkübertragung durch den Einsatz von 8-PSK, was 3 Bit pro moduliertem Symbol kodiert, im Vergleich zu 1 Bit pro kodiertem Symbol in GMSK, dem für GSM verwendeten Modulationsverfahren. Durch den zusätzlichen Einsatz einer Kanalkodierung, die sich dynamisch an die Qualität des Funkkanals anpasst, können Datenraten von bis zu etwa 70 kbit/s pro TDMA-Slot erreicht werden, ohne dabei das GSM Frequenzspektrum zu verlassen. Das Resultat ist eigentlich ein neues Netz, zwar unter Wiederverwendung und Erweiterung bestehender Infrastruktur-Komponenten, jedoch um den Preis neuer Endgeräte und neuer Transceiver in den Basisstationen. EDGE-Endgeräte werden auch Dienste aus GSM und GPRS unterstützen. Dem mobilen Endgerät können mit EDGE durchaus Datenraten von etwa 140 kbit/s und mehr zur Verfügung stehen. Solche Datenraten werden natürlich nicht im gesamten EDGE-Netz zu erwarten sein, sondern werden typischerweise in Hot-Spot-Bereichen zur Verfügung gestellt. Einfach gesagt, was mit ISDN geht, das geht auch mit EDGE, und zusätzlich gibt es noch GPRS-Dienste mit höherer Datenrate. Grundsätzlich ist man mit EDGE in einem Bereich, in dem mobile Multimedia-Dienste machbar sind [5].

EDGE wurde schon Ende 2001 in den USA in Betrieb genommen und stößt dort auf sehr großes Interesse. Trotzdem ist die Frage, wie stark EDGE sich in Europa durchsetzen wird, berechtigt. Zunächst würde sich die Einführung von EDGE und der dritten Generation (3G) mobiler Kommunikationssysteme wahrscheinlich überschneiden. Auch wenn EDGE Schritt für Schritt aus einem bestehenden GSM-Netz aufgebaut werden kann, EDGE ist eine nicht unerhebliche Investition. Betreiber, die eine Lizenz für ein 3G-System erworben haben, werden sich außerdem nicht automatisch die eigene Konkurrenz ins Haus stellen wollen. EDGE wird also primär bei Betreibern zu finden sein, die keine Lizenz für ein 3G-System erworben haben. Das schafft im Prinzip eine interessante Konkurrenzsituation. In Deutschland haben allerdings alle GSM-Betreiber auch eine UMTS-Lizenz ersteigert, und demgemäß sind hier noch keine (offiziellen) Aktivitäten in Richtung EDGE sichtbar.

3.
Die dritte Generation: Schneller, weiter, höher

Nach dem Startschuss Anfang der 90er-Jahre steht nach langer Forschungs-, Standardisierungs- und Entwicklungsarbeit nun die dritte Generation mobiler Kommunikationssysteme ins Haus. Mit dem Universal Mobile Telecommunications System (UMTS) sollen persönliche multimediale Kommunikations- und Informationsdienste flächendeckend und im lokalen Bereich angeboten werden. In dem zugewiesenem Spektrum im 2000-MHz-Bereich werden Datenraten von bis zu 2 Mbit/s möglich sein, die jedoch nur in lokalen Bereichen tatsächlich angeboten werden können. In der ersten Zeit wird man, wie aktuell im japanischen UMTS-Netz, mit nur maximal 384 kbit/s rechen müssen.

Universell soll UMTS gleich in mehreren Beziehungen werden. Eine hierarchische Zellstruktur erlaubt verschachtelte Netze und eine flexible Funkversorgung, die an die Anforderungen der Umgebung angepasst ist. Innerhalb öffentlicher UMTS-Netze können so beispielsweise private Netze geschaffen werden, die etwa die Firmengebäude mit Kleinstzellen (Pikozellen) versorgen. UMTS soll die Übertragung unterschiedlichster Inhalte ermöglichen (Sprache, Video, Bilder, Texte, Daten), und eine Vielfalt von Diensten und Anwendungen sollen hierauf aufbauen. UMTS definiert hierzu eine Architektur und ein Framework, mit dem universell Dienste realisiert werden können. UMTS stellt dem Teilnehmer über die Grenzen von Netzwerken und Endgeräten hinweg eine persönliche Umgebung von Diensten und Anwendungen, das so genannte Virtual Home Environment (VHE) zur Verfügung. Dies ist durchaus vergleichbar mit einer persönlichen Desktop-Umgebung, die ein Computerbetriebssystem dem Benutzer nach einem Login präsentiert. Die Vorstellung, UMTS als Verteiltes System zu sehen, ist im Grunde nicht allzu abwegig.

3.1
Dienste in UMTS: Mehr als Mobile Internet?

War in GSM, GPRS und EDGE noch das Ziel die Bereitstellung von Kommunikationsmitteln, soll in UMTS der Schwerpunkt auf der Bereitstellung von Inhalten liegen. UMTS mit Mobile Internet gleichzusetzen wäre falsch; es ist allerdings ein wesentlicher Bestandteil. Das UMTS-Forum nimmt an, dass die Nachfrage nach 3G-Diensten in den nächsten 5 Jahren mehrheitlich durch folgende sechs Dienstkategorien gebildet wird [6]:

- Mobile Internet Access ermöglicht den Zugang zu ISP-Dienstleistungen, der hinsichtlich Dienstgüte und Funktionsumfang annähernd dem gewohnten Festnetzzugang entsprechen soll. Dies beinhaltet E-Mail, WWW-Zugriff ohne Kompromisse inklusive Video- und Audio-Streaming.

- Mobile Intranet/Extranet Access ermöglicht über UMTS den sicheren Zugang zu Corporate LAN und VPN.

- Customized Infotainment bietet über so genannte mobile Portale einen auf die Person maßgeschneiderten Informationszugang. Nachrichten und Spielen wird dabei ein durchaus erhebliches Marktpotential eingeräumt, man denke nur an ein UMTS-Endgerät mit Gameboy-Funktionalität und der Möglichkeit zu interaktiven graphischen Computer-Spielen.

- Multimedia Messaging Service soll anknüpfend an den Erfolg des SMS der zweiten Mobilfunkgeneration realzeitfähiges Messaging (also unidirektional) für multimediale Daten anbieten.

- Location-based Services fassen als Sammelbegriff Dienste zusammen, die mit dem Aufenthaltsort des mobilen Endgeräts korreliert sind. Hierzu gehören neben der Be-

stimmung des aktuellen Aufenthaltsorts und den entsprechenden Informationsdiensten ("Wo finde ich den nächsten Geldautomaten") die ganze Palette von Anwendungen der Verkehrstelematik, wie Zielführung, Verkehrsinformation und -warnung, Fracht- und Flottenmanagement und Zugangskontrolle.

- Rich Voice bezeichnet einen bidirektionalen Realzeitdienst, der neben den klassischen Sprachdiensten auch Voice over IP (VoIP), Videophonie und Multimediadienste unterstützen soll.

Entsprechend werden UMTS-Endgeräte nur noch partiell an klassische Telefone erinnern. Vielmehr werden wir in einem Gehäuse unterschiedlichste Kombinationen von Sub-Notebook, Web-Pad, Personal Digital Assistant (PDA), Mobiltelefon und Videokamera erleben.

Die eben diskutierten Dienstkategorien genügen zur Feststellung, dass ohne IP in UMTS (fast) nichts mehr gehen wird. Die Weichen sind gestellt. Allein die Vorstellung, dass in Zukunft weltweit jedes 3G-Endgerät eine eigene IP-Adresse haben wird, deutet den nächsten Schritt an. IPv6 ist der Schlüssel zu dem angestrebten Spektrum an Diensten.

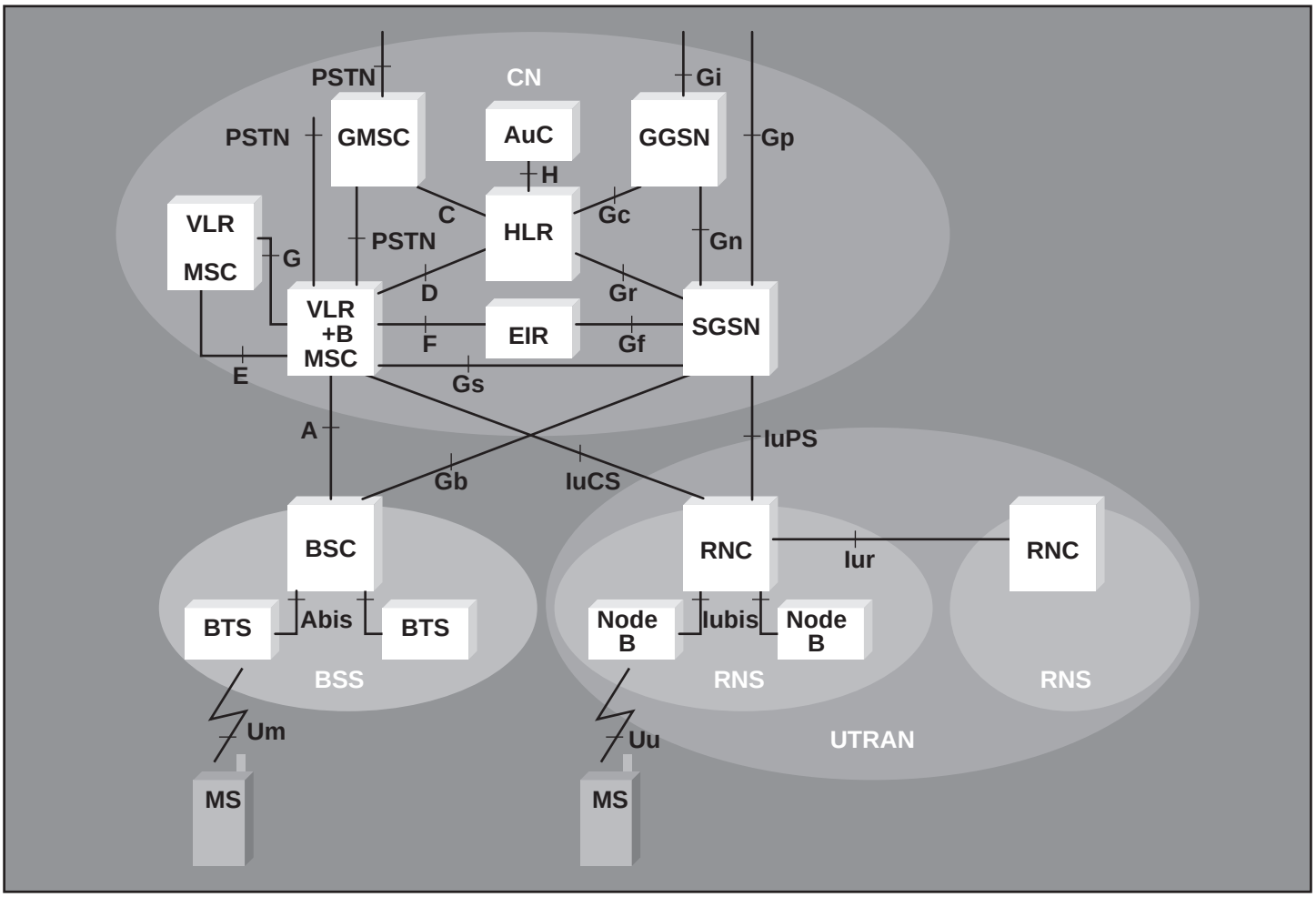
Damit dem Teilnehmer Dienste angeboten werden können, die – wie eben skizziert – weit genug über das Angebot in bestehenden GSM- und künftigen EDGE-Netzen hinausgehen, muss eine Teilnehmerversorgung mit Bitraten zumindest im ISDN-Bereich mit einer gewissen Wahrscheinlichkeit zugesichert sein. Wird ein Download einer Straßenkarte auch nach dem fünften Versuch nach mehreren Minuten abgebrochen, hat der Dienstanbieter hier sicher einen Kunden verloren. Es muss demnach ein sehr dichtes Netz mit entsprechend vielen Antennenstandorten geknüpft werden. Dies ist ein nicht unerhebliches Problem, denn Standorte werden rar, kosten Geld und der (zumindest potentielle) Beitrag zur elektromagnetischen Umweltbelastung erleichtert den Netzaufbau keineswegs.

3.2 UMTS-Netzarchitektur und Protokolle

UMTS wird vom 3rd Generation Partnership Project (3GPP) in mehreren Stufen standardisiert. Mit Release 1999 sollen wir nächstes Jahr in Deutschland die ersten UMTS-Netze im Betrieb sehen. Ursprünglich war geplant eine Release 2000 zu spezifizieren. September letzten Jahres wurde jedoch entschieden, stattdessen zwei Releases auszuliefern. Release 4 wurde im März inhaltlich eingefroren, und Release 5 soll Ende Dezember diesen Jahres folgen.

Die Netzarchitektur für Release 1999 ist eine unmittelbare Weiterentwicklung von GSM und GPRS (siehe Bild 2 und [7]). Grundsätzlich wird zwischen Radio Access Network (RAN) und Core Network (CN) getrennt. Grob gesagt ist das RAN für alle Funktionen der Funkübertragung verantwortlich, während das CN die Teilnehmer- und Dienstverwaltung sowie die Anbindung an andere Netze übernimmt.

Bild 2 Netzarchitektur für UMTS Release 1999 (vereinfacht)

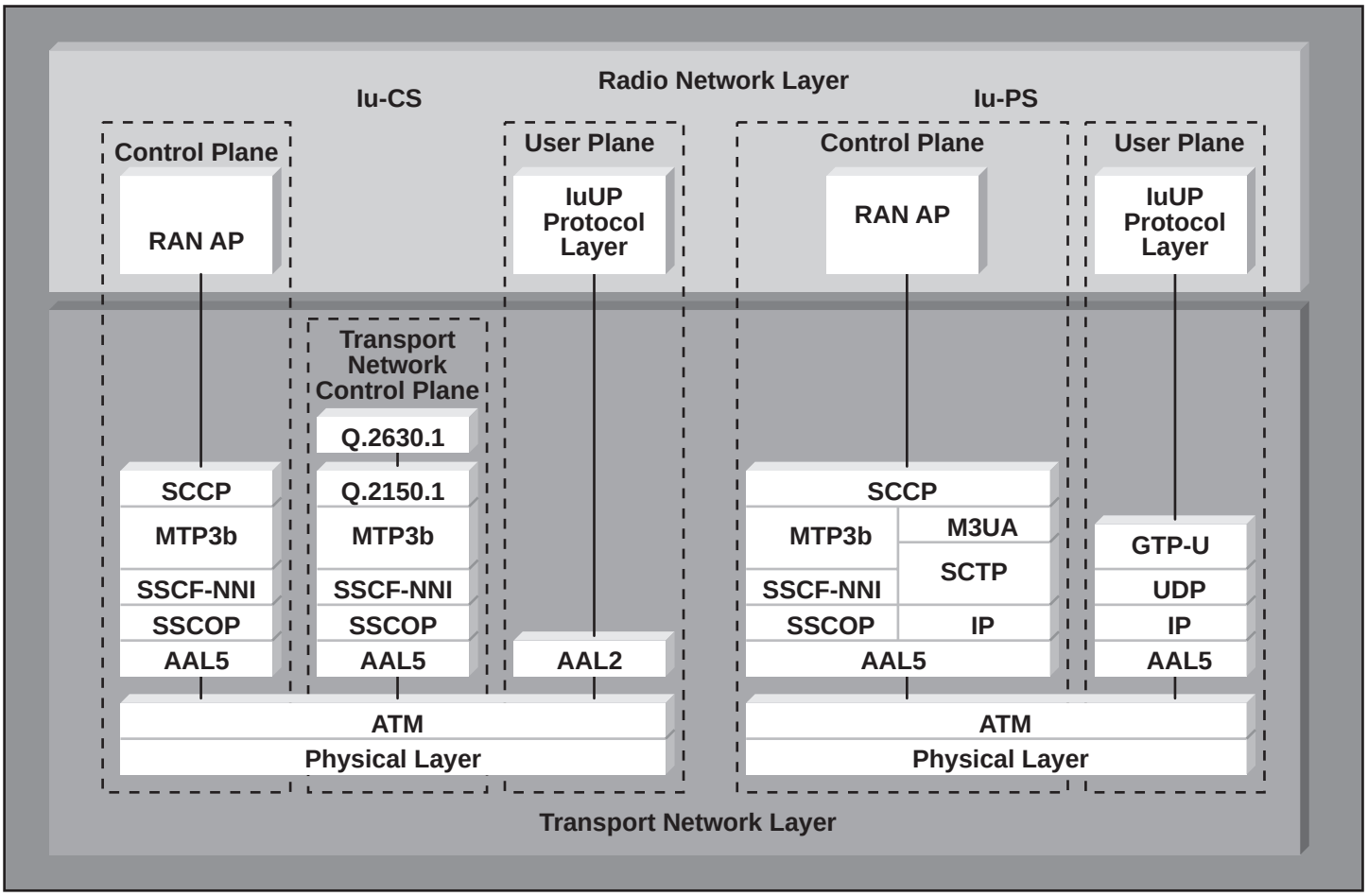


Die Funkübertragung in Release 1999 – spezifiziert im UMTS Terrestrial RAN (UTRAN) – geschieht mit Wideband Code Division Multiple Access (WCDMA). Das Signal wird hierbei mit einer Pseudozufallszahlenfolge kodiert und breitbandig gesendet. Der Empfänger kann mit Kenntnis von diesem Code das richtige Signal aus der Vielzahl überlagerter Signale wieder herausfiltern. Für die Übertragung zwischen UTRAN und CN wurde ATM festgelegt. Release 1999 wird Roaming und Handover zwischen UMTS und GSM unterstützen, d.h. ein UMTS-Endgerät (vorausgesetzt es unterstützt auch GSM-Frequenzbereiche) kann sich auch in einem GSM-Netz einbuchen. Selbst während eines Gesprächs kann sich ein UMTS-Endgerät aus dem UMTS Empfangsbereich herausbewegen und wird automatisch an ein GSM-Netz übergeben. Dabei wird ein Handover vom UMTS Radio Network Subsystem (RNS) in das Base Station Subsystem (BSS) von GSM durchgeführt. So ist es möglich ein UMTS-Netz schrittweise aufzubauen und beispielsweise erst einige Ballungsräume zu versorgen.

Wie bei GSM/GPRS besteht das CN aus einer leitungsvermittelnden und einer paketvermittelnden Komponente, was durchaus historisch bedingt ist, bewegen wir uns doch in einem Pfad der Evolution, der seine Wurzeln in der Telephonie hat. Für den leitungsvermittelten Verkehr ist das Mobile Switching Center (MSC) und das Gateway MSC (GMSC) verantwortlich. Für die Vermittlung von Paketdaten ist der Serving GPRS Support Node (SGSN) und der Gateway GPRS Support Node (GGSN) zuständig. Teilnehmerdaten, wie z.B. Dienstprofil und Routing-bezogene Informationen über den Aufenthaltsort, sind im Home Location Register (HLR) gespeichert und werden bei Bedarf in das Visitor Location Register (VLR) kopiert. Zugangskontrolle, Schlüsselverwaltung etc. obliegen dem Authentication Center (AuC). Das Equipment Identity Register (EIR) sorgt schließlich dafür, dass sich keine gestohlenen oder nichtzugelassenen Endgeräte ins Netz schmuggeln können. Die Koordination zwischen all diesen CN-Knoten, UTRAN und BSS geschieht mittels spezieller Signalisierungsprotokolle, mit dem Signalling System No. 7 (SS7) als Basis.

Bild 3 zeigt die Protokollstruktur für die Iu-Schnittstelle. ATM dient als gemeinsames Transportnetz für den leitungsvermittelten Verkehr (primär Sprache) über die Iu-CS Schnittstelle und für den paketvermittelten Verkehr über die Iu-PS Schnittstelle [8]. Alleine die Protokollstruktur macht deutlich, dass es zunächst vorgesehen ist diejenigen Dienste über die CS-Komponente mit AAL2 zu realisieren, deren Quality-of-Service-Anforderungen über einen Best-Effort-Trägerdienst hinaus gehen. Hierzu gehören insbesondere alle Sprach- und Multimediadienste. In diesem Sinne ist der Schwerpunkt in der Systemarchitektur noch klar auf der CS-Seite zu sehen; IP spielt "nur" in der PS-Komponente eine Rolle. Bis auf eine neue Luftschnittstelle mit erhöhter Kapazität und einem gemeinsamen Transportnetzwerk ist im Vergleich zu GSM/GPRS und EDGE nicht viel hinzugekommen.

Bild 3 Protokoll-Stack auf der Iu-Schnittstelle zwischen RAN und C



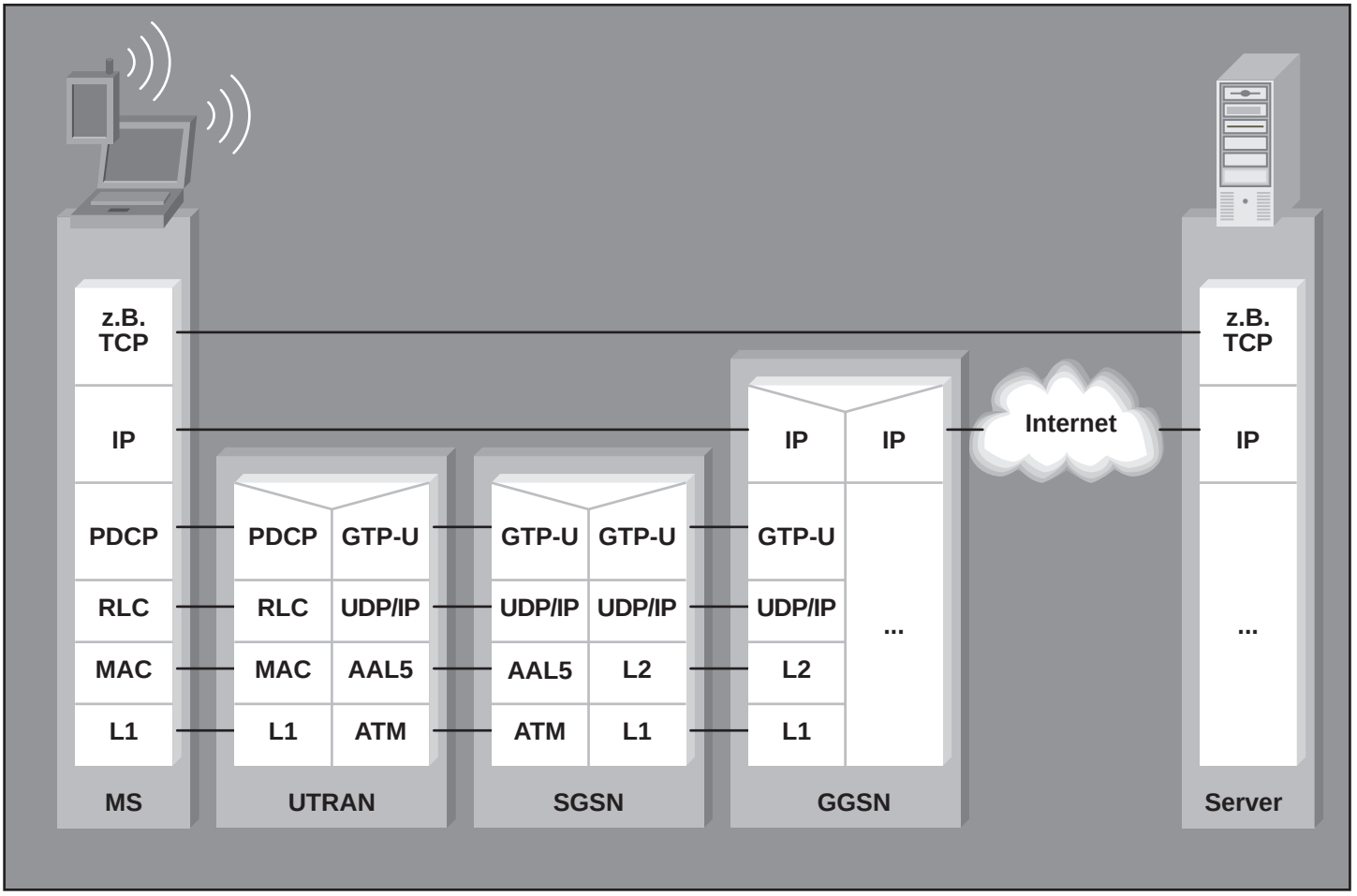


Bild 4 Grundsätzliches Prinzip des Internet-Zugriffs über UMTS

Bild 4 illustriert beispielhaft, wie sich eine Verbindung zu Internet-Diensten über die paketvermittelnde Komponente von UMTS realisieren lässt, die für GPRS in wesentlichen Bereichen analog verläuft [9]. Trotzdem müssen die Knoten im CN für den Schritt von GMS nach UMTS natürlich teilweise erheblich adaptiert werden.

Entscheidend ist in jedem Fall folgendes: Erstens ist eine strikte Trennung zwischen Access und Core vorgenommen worden mit dem klaren Ziel, zukünftig unterschiedlichste Zugangstechnologien zu erlauben. Zweitens ist es möglich, für die PS-Komponente eine komplett IP-basierte Infrastruktur von RNC bis GGSN aufzubauen.

4. Lizenzfrei, drahtlos und schnell

Systeme wie GSM und UMTS sind für den öffentlichen Weitverkehrssektor konzipiert und stellen allein mit ihrer komplexen Technik und ihrem Umfang Schwergewichte dar. Entsprechend langsam folgen ihre Bewegungen den Trends der richtungsbestimmenden Welt um das Internet herum. Die Entwicklung erfolgt quasi top-down mit der Spezifikation vollständiger Systeme und einer langsamen Konvergenz in Richtung IP als universelles Netzwerkprotokoll. Von einem anderen Ende betrachtet ist die Frage eher, wie mit Internet-Technik auf eine schnelle und unkomplizierte Weise neue Dienste realisiert werden können. Mit dieser pragmatischen Bottom-up-Strategie sind in den letzten Jahren Techniken entstanden, die den klassischen Konzepten der Telekommunikation mehr und mehr Konkurrenz machen. Voice over IP (VoIP) ist Realität, und bereits heute sind im privaten Sektor Systeme im Einsatz, die über IP alle Kommunikationsdienste und Anwendungen inklusive Sprache, Videokonferenz, Multimediaanwendungen auf einer einzigen Netzinfrastruktur anbieten. Wir erleben zum Beispiel aktuell, wie in Nordrhein-Westfalen aus der bisherigen Einbahnstrasse des TV-Kabelnetzes schrittweise ein interaktives System mit VoIP, High-Speed Internet Access (und natürlich TV) wird. VoIP ist also bereits auf dem besten Wege, in die Domäne öffentlicher Telekommunikationssysteme vorzudringen.

Analog sind Techniken entstanden, die lokale drahtlose Netze bilden (so genannte Wireless LAN, kurz WLAN), über IP eine Endgerätemobilität erlauben (Mobile IP, kurz MIP) und so den mobilen Zugang zu einer unternehmensweiten IP-basierten Infrastruktur ermöglichen. Diese Techniken sind standardisiert und preiswert, und der Markt liefert eine gesunde Konkurrenz und Verfügbarkeit.

Kombinieren wir in Gedanken diese Trends, ergibt sich ein Werkzeugkasten, aus dem ein im wesentlichen vollständiges mobiles Kommunikationssystem aufgebaut werden kann. Ein attraktiver Gedanke, der mehr und mehr Befürworter in der Mobilkommunikationsszene findet.

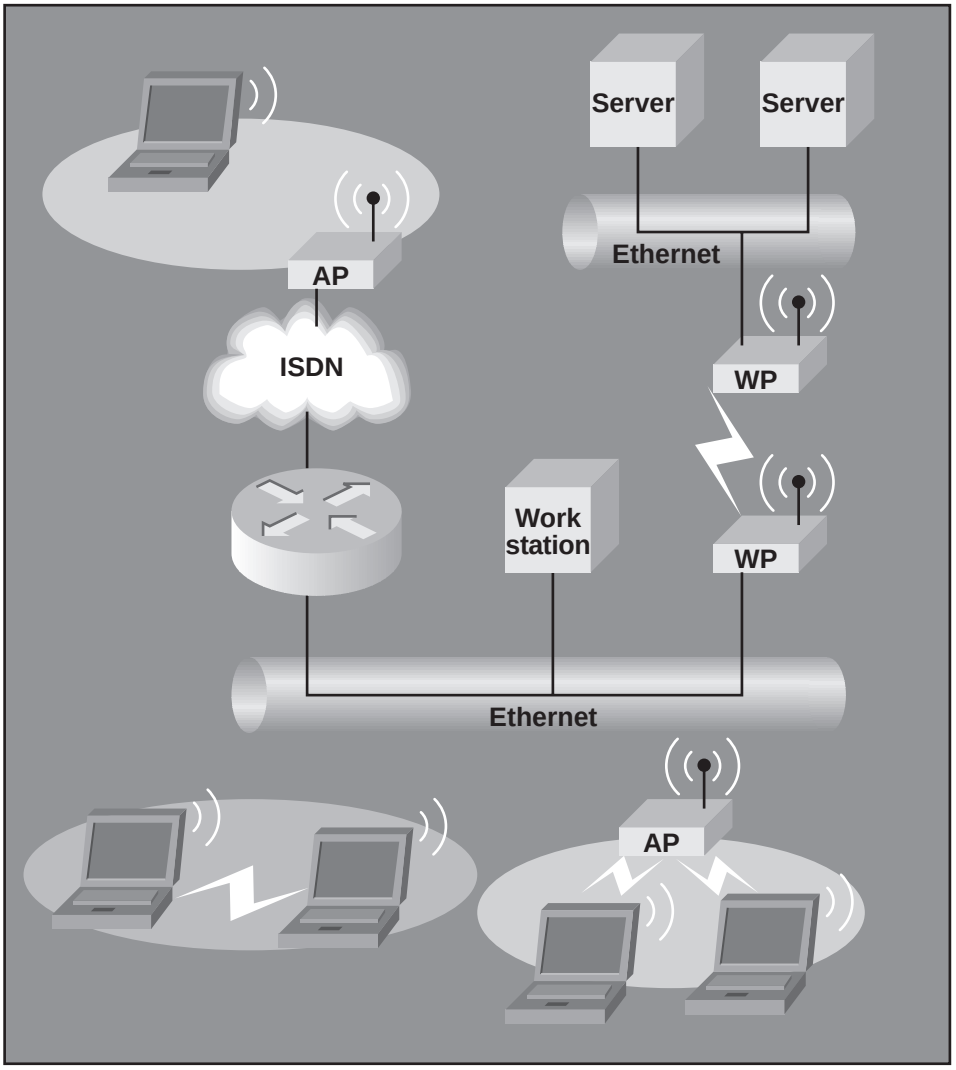


Bild 5 Typisches Wireless-LAN-Szenario

Ganz im Sinne kabelgebundener lokaler Netze werden WLAN auf Ebene 1 und 2 des OSI Referenzmodells definiert. Jedoch unterscheiden sich Konzepte und Protokolle erheblich von den Kollegen der Festnetzseite. Grundsätzlich hat ein WLAN zwei Komponenten, ein mobiles Endgerät und einen Access Point (AP), der als Basisstation die Kommunikation zwischen mobilen Endgeräten und der kabelgebundenen Infrastruktur herstellt.

Bild 5 zeigt ein exemplarisches WLAN-Szenario. Mobile Endgeräte kommunizieren entweder mit einem AP oder direkt miteinander. Im letzteren Fall spricht man auch von einem sogenannten Ad-hoc-Netzwerk, welches beispielsweise nur für die Dauer einer Besprechung aufgesetzt wird. Die Reichweite eines AP liegt typischerweise in Gebäuden im Bereich von 10 m bis 100 m (unter Idealbedingungen). Im Freien können durchaus 300 m erreicht werden. Der tatsächliche Empfangsbereich hängt von den konkreten baulichen Gegebenheiten ab. Verschiedene Materialien in Wänden dämpfen das Signal auch unterschiedlich. Es kann ebenso zu Reflexionen und Interferenzen mit anderen Sendern kommen, die das Signal stören können. WLAN sind hinsichtlich Abdeckung und Mobilität mit schnurlosen Telekommunikationssystemen wie DECT (Digital Enhanced Cordless Telecommunications) vergleichbar. Vom Blickwinkel zellularer Mobilfunknetze aus ist man mit WLAN im Bereich von Pikozellen. Mit speziellen Richtantennen können Punkt-zu-Punkt bei Sichtverbindung mit WLAN auch wesentlich höhere Distanzen (mehrere km) zwischen Gebäuden überbrückt und so zwei LAN-Segmente über Wireless Bridges (WB) gekoppelt werden. Dadurch stoßen WLAN auch in den Bereich Wireless Local Loop (WLL) vor.

WLAN ermöglichen eine Mobilität auf Layer 1 und 2. Das Endgerät kann sich innerhalb einer Funkzelle bewegen. Eine geeignete Kodierung auf Layer 1 und (falls vorhanden) Automatic Repeat-Request(ARQ)-Mechanismen auf Layer 2 können bis zu einem gewissen Umfang die Schwankungen in der Empfangsqualität ausgleichen. Besteht nun ein WLAN aus mehreren überlappenden Zellen, so kann sich ein Endgerät auch von einer Zelle in eine andere bewegen, ohne dass dabei eine Kommunikationsbeziehung auf höheren Protokollebenen abbricht. Ein Handover ermöglicht die Übergabe einer Kommunikationsbeziehung von einem AP zum anderen.

Generell ist ein Handover in einem mobilen Kommunikationssystem nichts anderes als der Abbruch einer (qualitativ schlechten) Funkverbindung und der Aufbau einer neuen (qualitativ besseren) Funkverbindung auf einem anderen Kanal, unter Aufrechterhaltung der Ende-zu-Ende-Kommunikationsbeziehung. Steuerung und Protokolle für ein Handover sind systemabhängig und unterscheiden sich erheblich z.B. zwischen GSM und einem einfachen WLAN.

WLAN sind immer dann attraktiv, wenn ein Netz schnell aufgebaut werden muss, wenn die Kosten oder der Denkmalschutz den Baumaßnahmen zu hohe Grenzen setzen oder wenn das Netz eine dynamische Anzahl in das Netz kommender und gehender Endgeräte unterstützen muss. Typische Szenarien sind die Vernetzung von Besprechungsräumen, Konferenzzentren, Hotels, Flughäfen, Krankenhäusern und Universitäten, also im Grunde überall dort, wo Menschen sich an einem Ort für eine vergleichsweise kurze Zeit aufhalten, oft "umziehen" und mit vertretbarem Aufwand kein (ausreichender) Festnetzanschluss zur Verfügung gestellt werden kann.

WLAN werden vom Institute of Electrical and Electronics Engineers (IEEE) und vom European Telecommunications Standards Institute (ETSI) standardisiert. Leider haben sich hier unterschiedliche Systeme etabliert. Zwei Standards sind zwar besser als keiner, aber immer noch einer zuviel. Wir werden im folgenden beide Familien kurz diskutieren. Neben WLAN ist mit Bluetooth ein weiterer interessanter drahtloser Kommunikationstyp auf der Bildfläche erschienen: Personal Area Networks (PAN) erlauben eine drahtlose Kommunikation im Nahbereich (wenige Meter) und sollen beispielsweise zur Anbindung von Peripheriegeräten dienen.

4.1
Die 802.11-Familie von IEEE

Für höhere Datenraten ist ISM bei 2,4 GHz nicht gut geeignet. Um Datenraten bis zu 54 Mbit/s anbieten zu können, weicht 802.11a auf den 5-GHz-Bereich aus. Leider liegen gerade hier einige Probleme: In Europa werden Teile des 5-GHz-Bandes bereits von militärischen und Regierungsanwendungen genutzt. HIPERLAN ist zwar auch in diesem Bereich zugelassen (genauer gesagt handelt es sich hier um zwei Frequenzbereiche: 5150 - 5350 MHz und 5470 - 5725 MHz), jedoch spezifiziert HIPERLAN Mittel auf physikalischer Ebene, um mit einer Parallelnutzung des Frequenzbands umzugehen. 802.11a ist von ETSI zwar noch nicht für Europa zugelassen, jedoch arbeitet IEEE unter 802.11 TGh an einem Vorschlag, der die spezifisch europäischen Probleme ausräumen soll. ETSI fordert dabei Nacharbeiten im Netzmanagement und fordert insbesondere bessere Kontrollmechanismen für die dynamische Kanalwahl und für die dynamische Anpassung der Sendeleistung.

Der Kanalzugriff (Medium Access Control, MAC) geschieht für alle spezifizierten Übertragungstechniken einheitlich über Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA).

Hierbei hört eine sendewillige Station zunächst den Kanal ab. Ist das Medium frei, so beobachtet die Station den Kanal zunächst noch für eine Sicherheitsspanne und beginnt, falls der Kanal dann immer noch frei ist, mit der Übertragung. Das vermeidet nicht, dass zwei sendewillige Stationen zur gleichen Zeit den Kanal abhören und zur gleichen Zeit mit einer Sendung beginnen. In diesem Fall kommt es zu einer Kollision, die in Funknetzen nicht wie in einem kabelbasierten Netz unmittelbar erkannt werden kann. Während in einem kabelbasierten System die Pakete mit einer Kollision in den allermeisten Fällen vernichtet werden, kann es in einem Funknetz durchaus noch passieren, dass trotz Kollisionen Pakete ihren Empfänger erreichen. In diesem Sinne trägt eine Kollision zwar zur Interferenz bei, jedoch besteht bei ausreichend großem Verhältnis von Signalleistung zu Interferenzleistung auch eine genügend große Wahrscheinlichkeit, das Signal erfolgreich zu dekodieren.

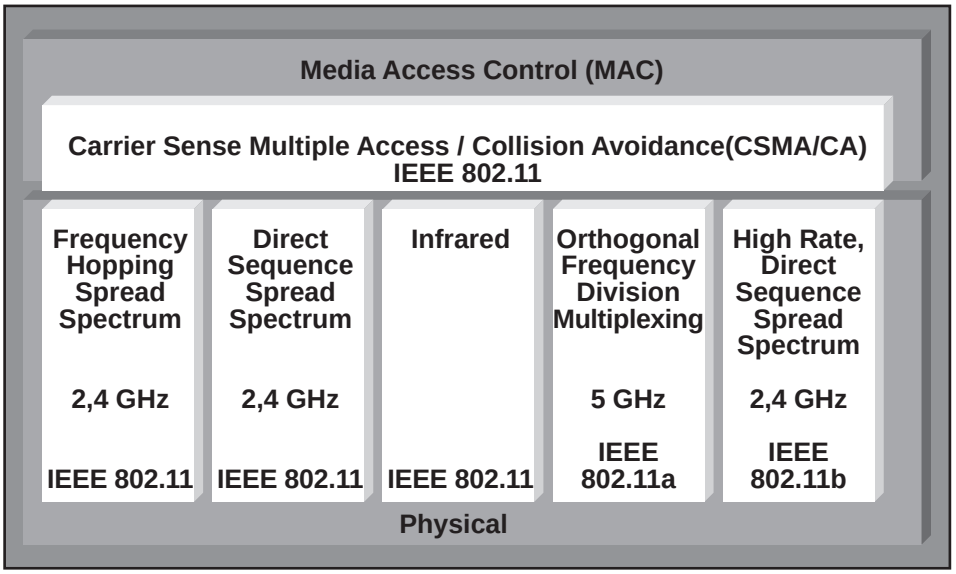
Eine Kollisionserkennung und -vermeidung kann in Funknetzen nur durch einen Rückkanal erfolgen. Auf Empfängerseite wird das Paket daher quittiert. Bleibt diese Quittung aus, geht der Sender von einer Kollision (oder einem sonstigen Fehler bei der Funkübertragung) aus und startet, sofern die maximale Anzahl von Übertragungsversuchen nicht überschritten wird, eine erneute Übertragung des Pakets. Andernfalls wird das Paket verworfen.

Ist der Kanal belegt, so wird der Übertragungswunsch zurückgestellt. Ist der Kanal wieder frei, so wartet die Station zunächst eine zufällige Zeitspanne ab, bevor ein erneuter Zugriff geschieht. Diese zufällige Zeitspanne wird so gewählt, dass das Zeitintervall, aus dem die Zufallszahl gewürfelt wird, mit der Anzahl der Zugriffsversuche exponentiell bis zu einer maximalen Größe wächst (Exponential Backoff). Analog zu CSMA/CD, dem Ethernet-Zugriffsverfah-ren, stellt sich ein sogenannter Last-In-First-Out-Effekt (LIFO-Effekt) ein, bei dem eine Station benachteiligt wird, je länger sie wartet.

Die Erkennung durch Carrier Sensing, ob der Kanal frei oder belegt ist, funktioniert in Funknetzen jedoch nicht immer. Nehmen wir beispielsweise zwei Clients, die in einer Distanz zueinander stehen, dass sie sich gegenseitig nicht mehr empfangen können. Nehmen wir jetzt noch an, dass in der Mitte der beiden Stationen ein Access Point steht, so dass beide Clients den Access Point empfangen können. Überträgt nun ein Client an den Access Point und führt der zweite Client ein Carrier Sensing durch, geht der zweite Client von einem vermeintlich freien Kanal aus und beginnt seinerseits mit der Übertragung. Am Access Point kommt es dann zu einer Kollision. Dieses Beispiel beschreibt das für Funknetze typische sogenannte Hidden-Station-Problem. IEEE 802.11 spezifiziert hierzu ein virtuelles Carrier Sensing, als RTS/CTS bezeichnet (Request To Send, Cleared to Send). Dabei wird zunächst ein sehr kurzes Kontrollpaket unter Angabe der Länge der eigentlichen Nutzdaten gesendet (RTS). Bei erfolgreicher Übertragung antwortet der Empfänger mit einer kurzen Bestätigung (CTS). Alle anderen Stationen warten die entsprechende Zeitspanne ab und vermeiden so eine mögliche Kollision. Bei Ausbleiben der Quittung geht der Sender von einer Kollision aus und wird wie oben beschrieben gegebenenfalls einen Neuzugriff nach einer zufälligen Verzögerung starten.

CSMA/CA arbeitet sehr effizient bei einer niedrigen bis mittleren Last. Bei einer größeren Zahl sendewilliger Stationen sorgt die maximale Wartezeit zwar für eine Stabilität des Verfahrens, jedoch ist das System im Vergleich zu den in HIPERLAN/2 spezifizierten Mechanismen nicht für hohe Auslastungen durch viele Stationen konzipiert. In 802.11 wird CSMA/CA im Rahmen der sogenannten Distributed Control Function (DCF) spezifiziert. Neben diesem "zufällig" gesteuerten Kanalzugriff spezifiziert 802.11 auch ein Polling-Verfahren, das jeder Station eine Sendemöglichkeit einräumt und bei dem es zu keinem Wettbewerb mit anderen Stationen (und daher auch zu keinen Kollisionen) kommt. Diese so genannte Point Coordination Function (PCF) ist jedoch in aktuell verfügbaren WLAN-Produkten nach 802.11b nicht implementiert.

Bild 6 Struktur des Standards gemäß IEEE 802.11



Kommen wir abschließend erneut auf die Bitrate zurück.

Netto bietet das MAC-Layer bei Verwendung von 802.11b eine effektive Datenrate von maximal etwa 6 MBit/s. Dies ist primär darin begründet, dass gewisse Teile eines MAC Pakets stets mit geringerer Datenrate (1 Mbit/s bzw. 2 Mbit/s) übertragen werden, Schutzabstände beim Kanalzugriff eingehalten werden müssen und schließlich MAC-Protokollinformationen in jedem Paket mit übertragen werden.

Bei 802.11a ist eine effektive Datenrate von ca. 36 Mbit/s möglich, immer noch genug, um das Medium effektiv mit anderen Teilnehmern zu teilen und trotzdem ein Gefühl wie im kabelgebundenen Netz zu genießen. Anwendungen, die nur eine beschränkte Varianz der Übertragungszeit erlauben, wie Sprache und Videophonie, können hier bei entsprechender Netzlast trotzdem Probleme bekommen, denn Ressourcengarantien gibt es nicht.

Andererseits ist die Robustheit von Sprache erstaunlich; man denke nur an die trickreichen Codierungen in GSM, die mit immer weniger Bandbreite auskommen. Grundsätzlich funktioniert VoIP sogar über 802.11b, und das drahtlose VoIP-Handy wird bereits von Herstellern angeboten. Es ist zwar "nur" Best-Effort, jedoch kann man einiges daraus machen, gerade wegen der simplen Technik!

Trotzdem: Ohne Quality of Service (QoS) geht es nicht, will man WLAN ernsthaft in einem größeren und professionellen Rahmen etablieren, der ein höheres Verkehrsvolumen mit sich bringt und die Unterstützung verschiedener Verkehrsklassen erfordert.

Die klassische Vorgehensweise aus Festnetzen, einfach eine genügend hohe Bandbreite durch entsprechende Kabelkapazität zu schaffen und damit das Risiko von Überlastspitzen abzufedern, funktioniert nämlich in Funknetzen nicht. Man hat nur ein Spektrum, und erst außerhalb eines durch Gesetze der Funkausbreitung gegebenen Abstands kann ein Kanal wiederverwendet werden, ohne signifikant zur Interferenz beizutragen. Die Kapazität lässt sich damit nur durch kleinere Zellen steigern, was der Skalierbarkeit schnell Grenzen setzt.

Gehen Festnetze verschwenderisch mit Bandbreite um, ist Bandbreitenökonomie eine Grundregel im Entwurf von Funknetzen.

In diesem Zusammenhang arbeitet die IEEE-Arbeitsgruppe für 802.11e an einer Erweiterung der MAC-Schicht von 802.11 zur Unterstützung von Anwendungen mit QoS-Anforderungen.

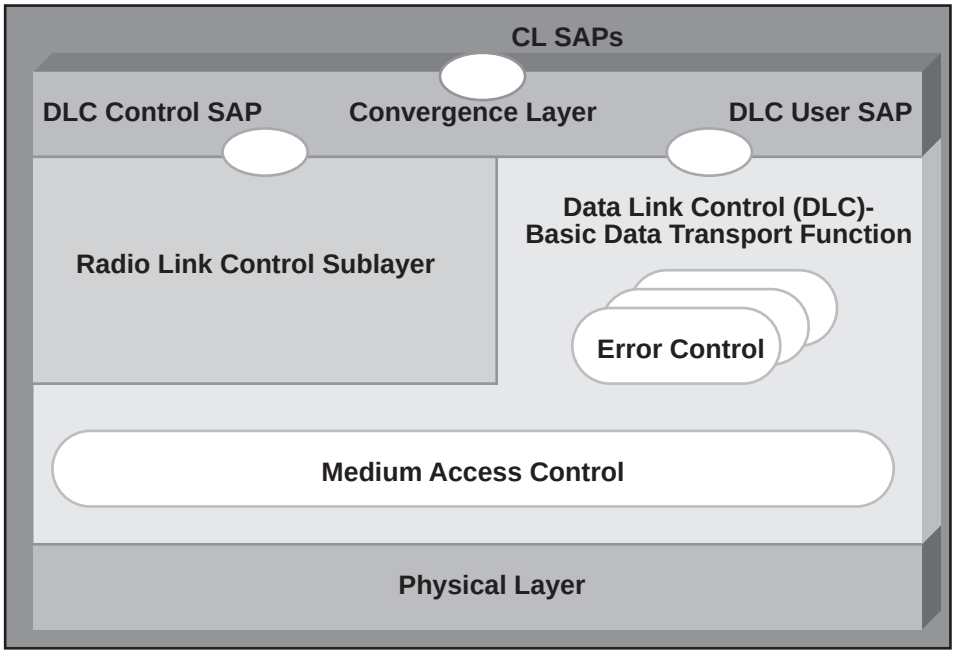
Die Produktsituation für WLAN-Komponenten nach IEEE 802.11b ist als sehr gut zu bewerten. WLAN nach IEEE 802.11b sind seit dem Jahr 2000 zu einem Massenmarkt geworden. Der Wettbewerb der verschiedenen Hersteller sorgt für qualitative hochwertige Produkte bei einem gleichzeitig gesunden Preisgefüge mit einem fallenden Trend. Auch große Netze im professionellen Umfeld sind seit wenigen Jahren erfolgreich in Betrieb. Die Technik kann als bewährt und stabil eingestuft werden. Der Interoperabilität von 802.11-Komponenten verschiedener Hersteller dient die Ausrüsterinitiative WECA (Wireless Ethernet Compatibility Alliance), die mit Wi-Fi (Wireless Fidelity) einen auf IEEE 802.11 DSSS basierten Industriestandard geschaffen hat, der auch entsprechende Tests vorschreibt und eine Liste der Wi-Fi-zertifizierten Produkte veröffentlicht. Der WECA gehören inzwischen alle namhaften Ausrüster (mehr als 140) der WLAN-Gemeinde an. Für IEEE 802.11a wird ein neues Zertifikat der WECA unter der Bezeichnung Wi-Fi5 eingeführt. In den USA sind inzwischen die ersten Produkte für 802.11a verfügbar. Zu nennen sind hier beispielsweise Proxim, Atheros und Intel. Andere Hersteller wie D-Link und Symbol haben Produkte für die erste Jahreshälfte 2002 angekündigt.

4.2 Die HIPERLAN-Familie von ETSI

Seit geraumer Zeit liegt von ETSI mit dem High-Performance Radio LAN (HIPERLAN) ein weiterer WLAN-Standard vor [5]. HIPERLAN gibt es in zwei Generationen: HIPERLAN/1 und HIPERLAN/2. Beide Typen operieren im 5-GHz-Band. HIPERLAN darf in Europa eingesetzt werden (der entsprechende Frequenzbereich ist sogar explizit für HIPERLAN ausgewiesen), was aktuell für 802.11a noch nicht gilt. Während in HIPERLAN/1 der Schwerpunkt auf der direkten Vernetzung mobiler Endgeräte liegt (sogenannte Ad-hoc-Netzwerke) und ein Best-Effort-Service mit einer Bruttorate von maximal 20 Mbit/s angeboten wird, zielt HIPERLAN/2 auf Breitbanddienste mit entsprechenden QoS-Anforderungen. Konzeptionell ist HIPERLAN/2 eher als drahtloser ATM-Zugang zu sehen und grenzt sich damit deutlich von IEEE 802.11a ab. Bild 7 zeigt vereinfacht die grundsätzliche Architektur von HIPERLAN/2 [13].

Die Trennung von Uplink und Downlink auf der Luftschnittstelle erfolgt in HIPERLAN/2 mit Time Division Duplex (TDD). Damit mehrere Teilnehmer gleichzeitig kommunizieren können, wird ein dynamisches Time Division Multiple Access (TDMA) eingesetzt. Wesentliches Feature der physikalischen Schicht ist die Möglichkeit der Nutzung unterschiedlicher Übertragungsmodi mit verschiedenen Code-Raten und Modulationstechniken. Dabei werden insgesamt 7 Übertragungsmodi mit Datenraten zwischen 6 und 36 Mb/s und optional auch 54 Mb/s angeboten.

Bild 7 HIPERLAN/2 Architektur (vereinfacht)



Die Übertragungsrahmen für den Kanalzugriff haben eine feste Dauer von 2 ms. Jeder Rahmen ist in mehrere Felder aufgeteilt, die Übertragungskanäle für unterschiedliche Zwecke definieren (Bild 8). Eine sendewillige Station hört zunächst den Broadcast Channel (BCH) ab. Auf diesem Kanal werden beispielsweise Parameter zur Funkübertragung gesendet. Der Frame Channel (FCH) gibt Aufschluss über die genaue Vergabe von Ressourcen in diesem Rahmen. Am Ende des Rahmens liegen dann die Random Access Channel (RCH). Auf einen dieser Slots greift die Station schließlich zu, um dem Access Point (AP) den Übertragungswunsch mitzuteilen. Dabei kann es natürlich auch zu einer Kollision kommen, wenn eine andere Station zur gleichen Zeit den gleichen Slot gewählt hat. Auf dem Access Feedback Channel (ACH) wird die Station anschließend im nächsten Rahmen über die Kollision informiert. Falls ein erfolgreicher Zugriff vorliegt, bestimmt der AP die Ressourcenvergabe. HIPERLAN/2 unterstützt auch die direkte Kommunikation zwischen Stationen zur Bildung von Ad-hoc-Netzen, Direct Mode genannt, im Gegensatz zum Centralized Mode bei der Kommunikation mit einem AP.

HIPERLAN/2 spezifiziert 3 Modi zur Fehlerkontrolle: Im Acknowledged Mode werden im Fehlerfall Neuübertragungen in einem ARQ-Schema mit Selective Repeat durchgeführt, wie man es ähnlich von klassischen Link-Layer-Protokollen oder auch von GPRS kennt. Im Repetition Mode werden PDUs ohne Quittungsmechanismus einfach mehrfach übertragen. Schließlich gibt es noch die einfache unquittierte Übertragung im Unacknowledged Mode. Mehrere Verbindungen können parallel von einem mobilen Endgerät über das Data Link Control Layer (DLC) geöffnet werden, und jede Verbindung kann mit einem unterschiedlichen QoS versorgt sein.

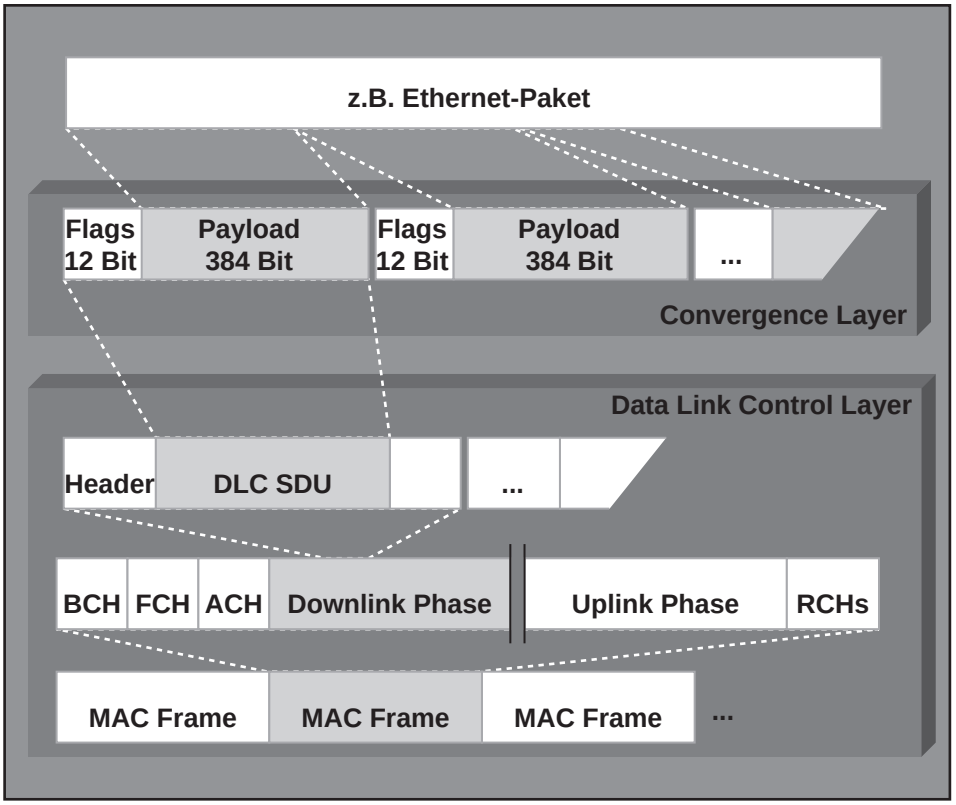
QoS bedeutet in Funkumgebungen mehr als in kabelgebundenen Netzen. Das Medium ist einfach instabiler. Es ist Störeinflüssen ausgesetzt, die sich während der Kommunikation ständig ändern können. Diese Störungen können durch ein weiteres, in der Nachbarschaft betriebenes Netz entstehen. Durch Reflexionen kann das eigene Signal mehrfach und zeitversetzt beim Empfänger ankommen. Bewegt sich das Endgerät während der Kommunikation, ändern sich die Bedingungen fortwährend. Frequenzen müssen dynamisch gewählt werden können, und ein Handover von einer Zelle zu einer anderen mit besseren Empfangsbedingungen muss möglich sein. Code-Raten und Modulationen müssen gewechselt werden können, um auf eine Verschlechterung (oder Verbesserung) der Übertragungsqualität zu reagieren. Dazu müssen AP und Endgerät kontinuierlich die Qualität der Funkverbindung messen. In Abhängigkeit von der gewünschten Dienstgüte und der Information über die Qualität der Funkübertragung kann der AP dann auch ein Error-Control-Schema und die entsprechenden Parameter setzen, wie ARQ-Fenstergröße und Anzahl der Retransmissions. Sind mehrere Verbindungen gleichzeitig vom AP zu unterhalten, muss ein Scheduler entscheiden, welches Endgerät und welche Warteschlange im nächsten MAC-Rahmen zu bedienen ist und wie viele Daten und Signalisierungsinformationen im nächsten MAC-Rahmen zu übertragen sind. Zur Vermeidung von Überlastsituationen dienen interne Funktionen wie Admission Control und Congestion Control.

Das Convergence Layer (CL) dient im Wesentlichen zur Konvertierung und Segmentierung von Daten der oberen Protokollebenen (bzw. der Protokolle des angebundenen Festnetzes) auf die HIPERLAN/2-Struktur, z.B. auf die an ATM orientierte feste SDU-Länge, die im DLC verwendet wird. Grundsätzlich wird zwischen einem paketbasierten CL zur Übertragung von Daten mit variablen Längen (z.B. Ethernet) und einem zellbasierten CL zur Übertragung von Daten mit einer festen Länge (z.B. ATM) unterschieden.

Nach Abzug von Protokoll-Overhead bleiben effektiv zwischen 30 und 40 Mbit/s übrig, vergleichbar mit 802.11a.

HIPERLAN/1 hat sich bis heute nicht am Markt gegen 802.11b behaupten können. Für HIPERLAN/2 sind zur Zeit noch keine Produkte verfügbar, und eine unmittelbare Konkurrenz zu IEEE 802.11a ist vorprogrammiert. Vorteilhaft für 802.11a ist die strukturelle Einfachheit. Für HIPERLAN/2 spricht das bereits vorliegende QoS-Konzept, das für 802.11 schließlich erst in Arbeit ist. Mit seinem drahtlosen ATM-Konzept hat HIPERLAN/2 eine natürliche Nähe zu UMTS und wird als eine weitere zukünftige Zugangstechnologie (RAN) zu UMTS-Netzen gesehen. Welcher Standard sich letztendlich durchsetzen oder ob es zu einer "Heirat" zwischen beiden Standards kommen wird, kann noch nicht endgültig gesagt werden. Manche Ausrüster stellen sich darauf ein, beide Standards unterstützen zu müssen. Mit der Entscheidung von Ericsson (einem der Ausrüster, welche die HIPERLAN-Technik lange vorangetrieben haben) die Entwicklung von HIPERLAN/2 zugunsten von 802.11a ruhen zu lassen und der Verfügbarkeit von ersten Produkten, ist das Pendel aktuell stark zu IEEE 802.11a ausgeschlagen.

Bild 8 Übertragungen von Daten in HIPERLAN/2



4.3 Kommunikation im Nahbereich mit Bluetooth

Bluetooth wurde entworfen, um im Nahbereich bei der Vernetzung eines Geräts (z.B. ein PC oder ein mobiles Telefon) mit Peripheriegeräten (z.B. Drucker oder ein Headset für das Telefon) auf die lästigen Kabel zu verzichten [4].

Eine erste verabschiedete Version der Bluetooth-Spezifikation liegt seit 1999 vor. Nach einer anfänglich eher schleppenden Einführung von Bluetooth-Produkten hat sich die Produktsituation im vergangenen halben Jahr deutlich gebessert. Access Points und Client-Adapter für PCs, PDAs und Drucker sind von verschiedenen Herstellern verfügbar. Einige Hersteller von GSM Mobiltelefonen statten ihre Geräte bereits mit Bluetooth aus.

Wie 802.11b operiert Bluetooth im ISM Band bei 2,4 GHz. Frequenzy Hopping wird zur physikalischen Übertragung eingesetzt, um das Risiko schmalbandiger Störungen zu minimieren. Dabei wird das Spektrum in 79 Kanäle mit einer Breite von 1 MHz aufgeteilt, und mit 1600 Hops pro Sekunde wechselt Bluetooth bei der Übertragung die Kanäle. Bluetooth-Geräte senden entweder mit einer Leistung von 1 mW oder mit 100 mW. Die meisten Bluetooth-Adapter unterstützen jedoch nur 1mW. Das entspricht einem Empfangsbereich von ca. 10 m bei 1 mW bzw. 100 m bei 100 mW. Wie immer in Funkumgebungen hängt dies natürlich stark von den räumlichen Gegebenheiten ab.

Bluetooth wurde von vorneherein zur Übertragung von Daten und Sprache ausgerichtet. Die Datenübertragung kann asymmetrisch mit unterschiedlichen Datenraten in beiden Richtungen geschehen. Sind z.B. Daten zu einem Drucker zu senden, benötigt man nur in Richtung des Druckers eine entsprechend hohe Kapazität. Maximal sind 723 kbit/s in die eine Richtung möglich; die Rückrichtung ist dann allerdings auf 57,6 kbit/s beschränkt. Ein ARQ-Mechanismus dient zur Fehlerkontrolle. Zur Sprachübertragung stehen 3 Kanäle mit 64 kbit/s zur Verfügung, bei denen eine entsprechende Codierung für eine genügend gute Qualität sorgt (ARQ scheidet bei Sprachübertragung ohnehin aus).

Tritt Bluetooth einen Siegeszug an, wird das Auswirkungen auf 802.11b haben. Man stelle sich nur eine Arbeitsumgebung vor, bei der permanent das WLAN gestört ist, weil Bluetooth überträgt.

5. IP und Mobilität

Betrachten wir nun die Mobilität aus der IP-Perspektive. Bewegt sich beispielsweise ein Endgerät innerhalb eines WLAN, so bleibt es in einem Layer-2-Segment und die Bewegung bleibt IP verborgen. Ähnlich ist die Situation in GSM. Dem Endgerät wird ein Kommunikationslink zur Verfügung gestellt, über den letztlich eine Verbindung zum ISP aufgebaut wird. Auch hier ist die Mobilität für IP unsichtbar, solange der Teilnehmer sich im GSM-Netz des Betreibers bewegt. Interessant ist dann jedoch die Frage, was passiert, wenn das Endgerät sich über (Sub-)Netzgrenzen hinweg bewegt. Das typische Beispiel sind Notebook-Nutzer, die oft zwischen Standorten in einer Firma wechseln, ohne auf eine Netzanbindung verzichten zu können.

Hierzu sei kurz daran erinnert, wie Routing in IP-Netzen funktioniert. Ein Router (bzw. Layer 3 Switch) trifft die Entscheidung, in welche Richtung ein IP-Paket weiterzuleiten ist, ausschließlich anhand eines Vergleichs der Zieladresse im IP-Header des IP-Pakets mit den Einträgen in der Router-internen Routing-Tabelle. Damit ein Router nicht für jedes Endgerät einen Eintrag in der Routing-Tabelle führen muss, speichert der Router sogenannte Network Prefixes, die unterschiedliche Längen haben können. Zu jedem Eintrag in der Routing-Tabelle gehört ein Link, auf den ein Paket weitergeleitet werden kann. Empfängt ein Router ein IP-Paket, so sucht er in seiner Tabelle nach dem längsten Eintrag, der mit einem Präfix der Zieladresse des eingegangenen IP-Pakets übereinstimmt (sprich: nach dem besten Match) und schickt das Paket auf den assoziierten Link. Dieses Routing-Prinzip, basierend auf einem Netzpräfix, erfordert insbesondere, dass alle Knoten an einem Link (bzw. Layer-2-Segment) den selben Netzpräfix haben. In diesem Sinne ist eine IP-Adresse mit seiner netztopologischen Information ortsgebunden.

Bewegt man ein Endgerät C (Client) von einem Netz H (Home) in ein Netz F (Foreign), werden Pakete an C also weiterhin an H geroutet statt an F. Grundsätzlich gibt es an dieser Stelle zwei Alternativen: Entweder das Endgerät C bekommt eine neue IP-Adresse passend zu Netz F zugewiesen oder IP wird um Funktionen erweitert, die es erlauben, dass C seine IP-Adresse behalten darf und die an C adressierten Pakete auf "magische Weise" an F geroutet werden. So einfach dieser Sachverhalt scheint, dies ist ein wichtiges Grundproblem des Mobile Computing.

5.1 Dynamische IP-Adressen

Die naheliegende Lösung ist, dem Endgerät bei einem Ortswechsel eine neue passende IP-Adresse zu geben.

Hierzu wird typischerweise ein IP-Adressbereich für mobile Nutzer festgelegt und die Vergabe einer entsprechenden IP-Adresse dem Dynamic Host Configuration Protocol (DHCP) überlassen. Bei der Initialisierung des Protokoll-Stacks erhält das Endgerät dann leihweise eine IP-Adresse von einem DHCP-Server.

Nutzer, die sich über eine Telefonleitung oder über GSM (via HSCSD oder GPRS) bei einem ISP über das Point to Point Protocol (PPP) einwählen, erhalten über das IP Control Protocol (IPCP) eine temporäre IP-Adresse.

Unabhängig davon, welche der beiden Mechanismen zur IP-Adressvergabe eingesetzt werden, es handelt sich immer um eine temporäre geliehene Adresse. Die IP-Adresse identifiziert hier also weniger das Endgerät als den aktuellen Aufenthaltsort im Netz.

Nimmt man in Kauf, dass bei jedem Ortswechsel der Protokollstack neu initialisiert werden muss, reicht das für konventionelle Client-Server-Anwendungen mit einem mobilen Client jedenfalls aus (solange die Client-Anwendungen nicht für einen speziellen IP-Bereich lizensiert werden müssen). Das Netz kann dabei so konfiguriert werden, dass der Nutzer von der dynamischen Vergabe der IP-Adressen im Regelfall nichts merkt.

Soll eine IP-Adresse jedoch zu Identifikationszwecken dienen oder sollen Anwendungen unterstützt werden, die es erfordern, dass ein mobiles Endgerät unabhängig von seinem Standort direkt "angefunkt" werden kann, kommt man mit den eben vorgestellten Ansätzen nicht weit.

Vergleichen wir eine IP-Adresse mit einer Telefonnummer, so haben wir zwar dafür gesorgt, dass ein Gerät eine Telefonnummer erhält, diese jedoch von Anmeldung zu Anmeldung wechselt und eigentlich niemand diese Nummer erfragen kann.

Um direkt erreichbar zu sein, müssten wir also eine Art Rufumleitung einrichten und die Zielnummer der Rufumleitung ständig ändern.

5.2 Mobile IP

Immer mehr Features werden von immer kleineren mobilen Endgeräten angeboten, die drahtlos auf die eine (GSM, UMTS) oder andere Weise (WLAN) mit einer Infrastruktur verbunden sind. Zudem werden immer mehr dieser Endgeräte eine eigene IP-Adresse haben. Dieser Massenmarkttrend ist nicht zu unterschätzen und hat direkte Konsequenzen auf die Verwaltung der Endgerätemobilität in IP-basierten Systemen, begleitet mit der Forderung, die Mobilität direkt auf Netzwerkebene zu unterstützen.

Mobile IP (MIP) ist eine Erweiterung von IP, die für IP Version 4 in RFC 2002 standardisiert ist. MIP ermöglicht die Bewegung (Roaming) eines mobilen Endgeräts über Netzgrenzen (speziell auch Netzbetreibergrenzen) hinweg unter Beibehaltung der Erreichbarkeit des Endgeräts unter einer einzigen IP-Adresse. Da MIP als echte Erweiterung von IP spezifiziert ist, gilt insbesondere, dass MIP vollständig unabhängig vom Übertragungsmedium ist.

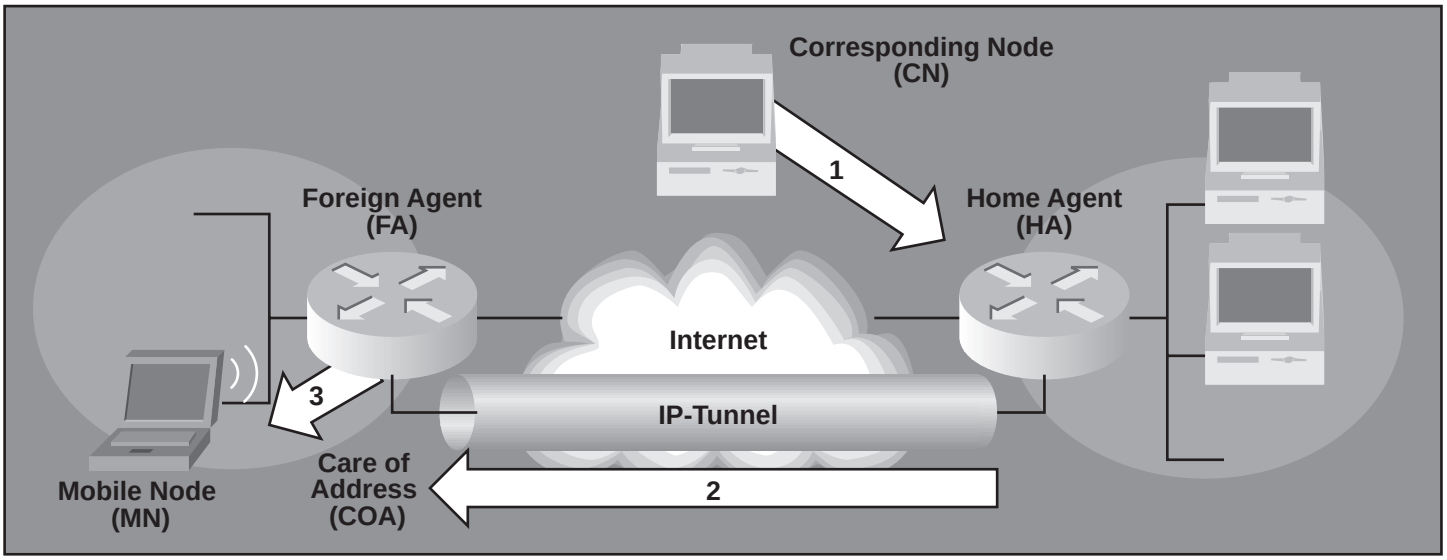
Die Verwaltung der Mobilität in Mobile IP funktioniert nach einem ähnlichen Schema, wie es auch in "klassischen" mobilen Kommunikationssystemen wie GSM realisiert ist. Kernelement ist die Bereitstellung und Verwaltung der Routing-Information zum aktuellen Aufenthaltsort eines mobilen Endgeräts. Hierzu führt MIP zwei neue Netzelemente ein, die typischerweise als Funktionen in einem handelsüblichen Router realisiert werden: Home Agent und Foreign Agent. Bild 9 zeigt die grundsätzliche Funktionsweise von MIP, die wir im folgenden kurz erläutern wollen (unter Verzicht auf Details und Spezialfälle, die durchaus ein komplettes Buch füllen können, siehe z.B. [14]).

Wird ein mobiles Endgerät (Mobile Node, MN) eingeschaltet, muss es sich zunächst einmal orientieren und die Frage klären, ob es sich im Heimatnetz befindet oder gerade ein anderes Netz besucht. Hierzu dienen Erweiterungen von IRDP, dem ICMP Router Discovery Protocol (RFC 1256). Nehmen wir an, das Gerät stellt fest, dass es sich in einem fremden Netz befindet und hat einen entsprechenden Foreign Agent (FA) kennengelernt. In diesem Fall registriert sich der MN beim FA unter Angabe seiner eigenen IP-Adresse und der IP-Adresse des Home Agents (HA). Der FA leitet die Registrierung an den HA weiter und liefert dabei die IP-Adresse, über die der MN nun erreichbar ist, die so genannte Care of Address (COA). Wird ein IP-Paket an MN geschickt, wird es zunächst zum Heimatnetz geroutet und dort vom HA an die COA getunnelt. Dies geschieht beispielsweise über IP in IP Encapsulation (RFC 2003). Am Tunnelendpunkt (hier der FA) wird das originale IP-Paket ausgepackt und an den MN weitergeleitet. Das "Dreiecks-Routing" über den HA kann natürlich ineffizient werden. Man stelle sich vor, dass zwei Computer wenige Meter (sprich: Hops) voneinander weg aufgestellt sind, jedoch der HA von einem der beiden Kommunikationspartner 5000 km und viele Hops entfernt ist. Damit geht der Weg eines Paketes über MIP dann zunächst zum HA und anschließend wieder zurück. Zu diesem Problem gibt es Erweiterungen von MIP, die ein effizienteres Routing ermöglichen, indem sie einen Umweg über den HA bei Bedarf vermeiden.

Die Bedeutung von MIP für aktuelle und zukünftige mobile und drahtlose Netze ist zur Zeit noch unklar, obwohl sich bereits deutliche Trends in Richtung MIP abzeichnen. MIP für IP Version 4 wird bereits von vielen Herstellern von Routern und Layer-3-Switchen unterstützt und in den UMTS Standards sind schon für Version 99 Szenarien für den Einsatz von MIP definiert [15]. Die praktische Anwendung hat jedoch zumindest in Europa noch Seltenheitswert. Ausrüster, die Lösungen für öffentlich betriebene WLAN anbieten (z.B. Nokia), die z.B. in Hot Spots wie Flughäfen installiert werden, verzichten zur Zeit noch auf den Einsatz von MIP, da VPN-Technologien und DHCP für die allermeisten Anwendungen genügen. Spannend wird es jedoch mit der Einführung von IP Version 6. Will man in einem mobilen Umfeld die Vorteile von IP Version 6 nutzen, wird man automatisch auf MIP zurückgreifen.

Für GPRS wird MIP interessant, wenn ein Roaming zwischen GSM-Netzen unter Beibehaltung der IP-Adresse realisiert werden soll. Da GPRS und damit UMTS Release 1999 und zumindest auch Release 4 eine Mobilität auf Layer 2 ermöglichen, würde man die Funktion von HA und FA im GGSN realisieren. In diesem Sinne würde MIP die Makromobilität für IP-basierte Dienste zwischen GPRS bzw. UMTS-Netzen realisieren. Je mehr IP auch innerhalb von UMTS zur Kernvermittlungstechnik wird, desto interessanter ist die Anwendung von MIP auch für das netzinterne Mobilitätsmanagement [16]. CDMA2000 von der Telecommunications Industry Association (TIA), das zur Zeit außerhalb von Europa etabliert wird, setzt für das Core Network schon jetzt konsequent auf den Einsatz von MIP.

Bild 9 Routing zu mobilen Endgeräten mit Mobile IP



6. All-IP: Konvergenz statt Konkurrenz

Der Begriff All-IP bezeichnet einen Trend, der sich bereits deutlich in der bestehenden UMTS-Standardisierung zeigt: In einem All-IP-Szenario ist IP der gemeinsame Träger für jegliche Kommunikation zwischen den Netzelementen. Beginnend mit dem IP-basierten Teil des Core Network in Release 1999 wird VoIP in Release 5 von UMTS im Rahmen eines allgemeinen Multimedia ein natürlicher Bestandteil von UMTS. Generell gilt, dass die angestrebte Dienstvielfalt in UMTS nicht mehr mit der bestehenden, von GSM geerbten monolithischen Netzarchitektur möglich ist [17].

Die Vorteile von All-IP liegen auf der Hand: Alle Kommunikationsdienste werden von einer einzigen Netzinfrastruktur erbracht, die Sprache, Daten und multimediale Dienste effektiv integriert. Die verschiedenen Transportmedien und Zugangstechniken, wie LANs, WANs, ISDN und Mobilfunktechniken werden durch IP transparent. Schließlich ermöglicht erst eine vereinheitlichte Netzwerkübertragung die gewünschte Dienstflexibilität und damit die zur Zeit noch visionäre Angebotspalette mobiler multimedialer Kommunikations- und Informationsdienste.

6.1 Die Rolle von IP für UMTS

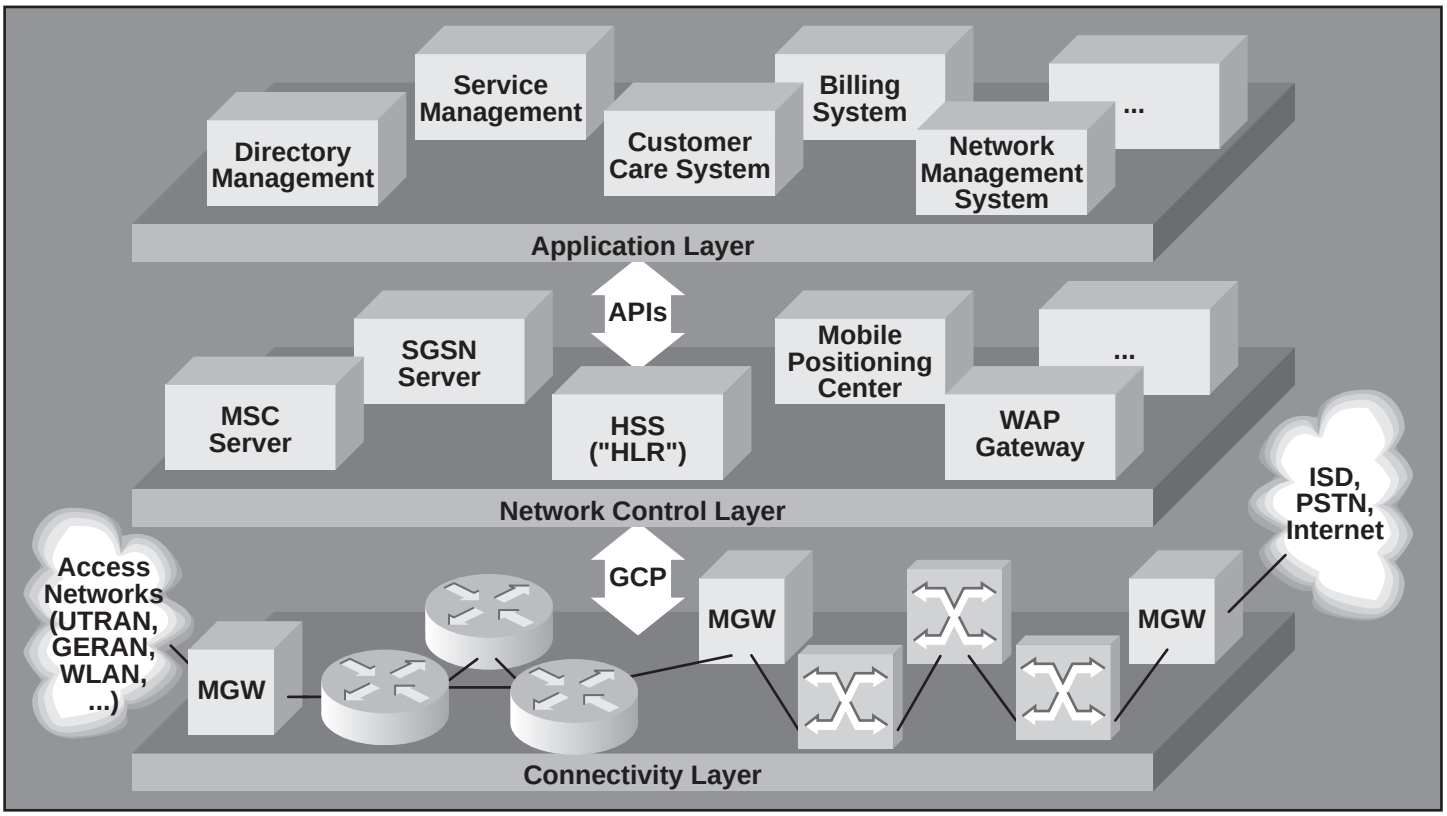
Die Netzarchitektur im Core Network wird sich zu einer dienstorientierten horizontalen Architektur entwickeln (Bild 10). Statt wie bisher Netzwerkknoten wie einen MSC mit immer mehr Funktionen zu überfrachten, werden zunächst Vermittlungsaufgaben, Netzkontrolle und Dienstbearbeitung bzw. Anwendung getrennt. Streng genommen ist das nichts anderes als die konsequente Fortführung des Konzepts Intelligenter Netze. Entscheidend ist dabei die Einführung der Media Gateways (MGW), die vom Transportnetz abstrahieren und so eine sanfte Migration zu einem IP-basierten Transportnetz ermöglichen. Dieses Prinzip ist nicht nur integraler Bestandteil der Standardisierung der 3GPP für UMTS [18], es wird letztendlich als Kooperation verschiedener Standardisierungsinitiativen realisiert werden, wie z.B. Megaco in IETF/ITU, Tiphon in ETSI sowie im Multiservice Switching Forum [19], [20].

All-IP geht über das Core Network hinaus. Die Szenarien, die von Ausrüstern und Betreibern diskutiert werden, beinhalten auch den Einsatz von IP als Träger von Signalisierungs- und Nutzerverkehr im UTRAN, also zwischen Basisstationen und RNC, zwischen RNC und RNC sowie zwischen UTRAN und Core Network [21].

Dies wird ähnliche Konsequenzen für die Architektur haben wie im Core Network. Ob diese Entwicklung langfristig das Ende von SS7 bedeutet, sei dahingestellt. Zunächst werden SS7-Protokolle von SCCP aufwärts über IP übertragen. Bis auf die Technik zur Vermittlung von Signalisierungsnachrichten ändert sich also nichts. Sieht man jedoch das Core Network von einer anwendungsorientierten Sicht als Verteiltes System interagierender Objekte, werden früher oder später entsprechende Middleware-Konzepte, wie CORBA, zur Unterstützung verteilter komponentenbasierter Anwendungen auch hier Fuß fassen. In diesem Sinne wird SS7 von zwei Seiten in die Zange genommen: von der Netzwerkseite durch IP und von der Anwendungsseite durch moderne Softwarearchitekturen.

Die Voraussetzung für den konsequenten Einsatz von IP sind die Unterstützung von QoS für verschiedene Verkehrsklassen, die Möglichkeit zur Etablierung sicherer Kommunikationsbeziehungen, welche Vertraulichkeit, Verfügbarkeit und Integrität garantieren, sowie die Unterstützung von Mobilität auf IP-Level. Prinzipiell sind diese Voraussetzungen mit IP Version 4 und seinen vielfältigen Erweiterungen bereits erfüllt, jedoch gleicht die IPv4-Protokollsuite einem unüberschaubaren Patchwork.

Bild 10 Netzwerkarchitektur für UMTS Release 5



Mechanismen wie DiffServ, MPLS und SIP erlauben die Übertragung und Verwaltung von multimedialen Verkehrsströmen mit garantierter Dienstgüte, von der Sprachübertragung über Video- und Audio-Streams bis hin zur Videokonferenz [22], [23]. Mit IPSec (RFC 2401 und folgende) können sichere Kommunikationswege etabliert werden und MIP ermöglicht Teilnehmermobilität unter Beibehaltung der IP-Adresse.

Erst IP Version 6 (RFC 2460 und folgende) integriert die eben skizzierten Anforderungen und Mechanismen auf eine Weise, die für ein All-IP-Szenario Sinn machen [24]. IPv6 unterstützt außerdem einen Adressraum, für den auch weltweit mobile Endgeräte mit einer eigenen IP-Adresse kein Problem darstellen. Insbesondere kann auf Network Address Translation (NAT) verzichtet werden, was bislang zu schwer beherrschbaren Problemen beim Einsatz von IPsec und Mobile IP führen kann.

6.2
WLAN als Radio Access Network

WLAN sind als mögliche RAN bereits in zukünftigen UMTS-Versionen ab Release 5 vorgesehen. Dabei stellt ein UMTS-Netz dem WLAN die notwendige Infrastruktur zur Authentifizierung des Teilnehmers sowie zur Dienst- und Mobilitätsverwaltung zur Verfügung. In diesem Sinne ergänzen sich drahtlose Technik und Mobilkommunikation perfekt. Schauen wir genauer hin, stellen wir fest, dass im Prinzip eigentlich nichts anderes passiert als die Ergänzung eines WLAN um sichere VPN-Technik, und das gibt es schon heute. Tatsächlich ist es sogar grundsätzlich empfehlenswert, den Aufbau eines WLAN mit VPN-Mitteln abzusichern, da insbesondere IEEE 802.11b nur mit einer ausgesprochen schwachen Verschlüsselung aufwartet, die mit geringem Aufwand gebrochen werden kann.

Um zu zeigen, dass dies mehr als realistisch ist, wollen wir kurz ein System vorstellen, das Nokia für die Implementierung öffentlicher WLAN anbietet. Dieses System nutzt 802.11b WLAN als Medium, um in Hot Spots (Flughäfen, Hotels, Besprechungsräume in Firmen, usw.) eine Internet-Verbindung für Notebooks und PDAs zu schaffen. Die Authentifizierung eines Nutzers gegenüber dem System geschieht durch eine gewöhnliche GSM-SIM-Karte. Dabei wird durch eine spezielle Komponente im öffentlichen WLAN über das Internet eine Verbindung zu dem entsprechenden GSM-Vermittlungsnetzwerk (sprich: HLR und AuC) aufgebaut, und über GSM-Protokolle geschieht dann die Authentifizierung. Genauso wie Mobiltelefone in einem fremden GSM-Netzwerk eingebucht werden können (sofern ein entsprechendes Roaming-Agreement zwischen den Betreibern vorliegt), wird Roaming auch für diese WLAN-Inseln unterstützt. Analog funktioniert die Abrechnung. Der Teilnehmer findet die Kosten für die Nutzung des WLAN einfach auf seiner GSM-Abrechnung. Das öffentliche WLAN nutzt also für spezielle Funktionen, die sonst neu zu implementieren wären, einfach eine bestehende GSM-Infrastruktur und ist so quasi zu einem vereinfachten Base Station Sub-System geworden.

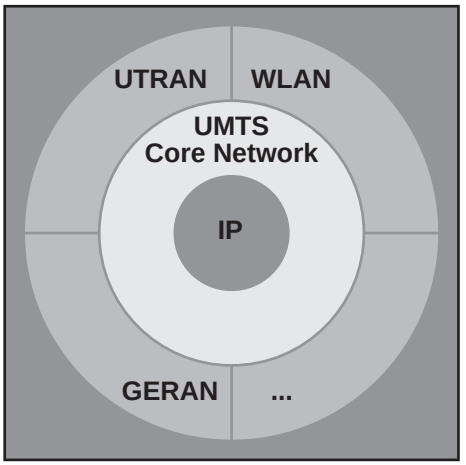
In diesem Sinne werden wir mit All-IP (unabhängig davon, welche Szenarien sich durchsetzen werden) eine Konvergenz zu einer gemeinsamen Netzwerkarchitektur für die Tele- und Datenkommunikation erleben, in der LAN, MAN und WAN eine natürliche mobile Fortsetzung finden. Wie weit diese Integration gehen wird, ist zur Zeit schwer zu sagen. Mit dem Angebot erster VoIP-Telefone für 802.11b WLAN hat zumindest DECT eine Konkurrenz bekommen. Erwähnenswert ist in diesem Zusammenhang, dass eine Erweiterung von DECT für das ISM-Band bei 2,4 GHz bereits spezifiziert ist [26]. Das Zusammenwachsen von schnurloser Telekommunikation und WLAN ist eigentlich nur noch eine Frage der Zeit. An Endgeräten, die GSM bzw. UMTS und WLAN integrieren und ein automatisches Umschalten zwischen beiden Systemen erlauben, wird zur Zeit gearbeitet bzw. geforscht. Schwerpunkt ist aktuell ein mobiler Internet-Zugang. Sprachdienste spielen im Umfeld von WLAN noch eine untergeordnete Rolle. Spannend wird es jedoch mit einer breiteren Einführung von VoIP in UMTS, denn dann werden WLAN RAN den "konventionellen" RAN direkte Konkurrenz machen können. Spätestens bis zu diesem Zeitpunkt ist die Regulierungsbehörde gefordert, zu einem Ungleichgewicht Stellung zu beziehen: Einerseits wurde das Spektrum für UMTS mit erheblichen Auflagen für die Netzbetreiber teuer versteigert, andererseits werden die kostenlosen Frequenzspektren für WLAN immer mehr kommerziell genutzt.

In einigen Veröffentlichungen werden WLAN-basierte öffentliche Systeme bereits als erster Schritt zur 4. Generation mobiler Kommunikationssysteme verkauft, mit der obligatorischen Warnung vor einer finanziellen Katastrophe für UMTS. Meist werden hier jedoch Äpfel mit Birnen verglichen. Klar ist, dass für mobile Breitband-Anwendungen auf Spektren in höheren Frequenzbereichen ausgewichen werden muss. Ob 802.11a genügt, ist mehr als fraglich. Was letztendlich jedoch passieren wird, ist eine Integration in UMTS mit IP als gemeinsamer Netzwerktechnik. Ob es dann noch die 3. Generation ist oder schon die 4., ist eigentlich egal.

7.
Das Funknetz der Zukunft: Weniger ist mehr

Im Outdoor-Bereich wird früher oder später UMTS dominieren, jedoch wird GSM und speziell GPRS eine überraschende Langlebigkeit beweisen (und das nicht nur durch EDGE). Ein interessanter Schachzug von 3GPP ist in diesem Zusammenhang, dass GSM und EDGE kurzerhand als weiteres mögliches Radio Access Network unter dem Kürzel GERAN mit an Bord genommen wurden [25].

Für den drahtlosen Indoor-Bereich lässt sich allerdings prognostizieren, dass WLAN sich durchsetzen werden und die gesamte Bandbreite an Kommunikationsdiensten unterstützen werden, privat, im Business-Bereich und öffentlich. Damit UMTS die Rolle einer globalen Infrastruktur für die mobile und drahtlose Kommunikation auch wirklich einnehmen kann, ist eine saubere Integration mit WLAN von strategischer Bedeutung. IP wird sich dabei auf breiter Front etablieren, und der Massenmarkt weltweiter mobiler und drahtloser Kommunikation wird zum eigentlichen Motor für eine konsequente Migration zu IPv6, und letztendlich gilt damit auch: Die Zukunft heißt VoIP!*



* Die ComConsult Akademie trägt dem Rechnung und bietet zwei neue VoIP-Seminare an, Seite 27 - 28

Konvergenz zu IP in mobilen Kommunikationssystemen - Abkürzungen

3G	3rd Generation
3GPP	3rd Generation Partnership Project
AAL	ATM Adaptation Layer
ACH	Access Feedback Channel
AP	Access Point
ARQ	Automatic Repeat Request
ATM	Asynchronous Transfer Mode
AuC	Authentication Center
BCH	Broadcast Channel
BSC	Base Station Controller
BSS	Base Station Subsystem
BTS	Base Transceiver Station
CDMA	Code Division Multiple Access
CL	Convergence Layer
CN	Core Network
COA	Care of Address
CORBA	Common Object Request Broker Architecture
CRC	Cyclic Redundancy Code
CS	Coding Scheme
CS	Circuit Switched
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
DLC	Data Link Control
DCF	Distributed Coordination Funktion
DHCP	Dynamic Host Configuration Protocol
DLC	Data Link Control
DSSS	Direct Sequence Spread Spectrum
EDGE	Enhanced Data Rates for Global Evolution
EIR	Equipment Identity Register
ETSI	European Telecommunications Standards Institute
FA	Foreign Agent
FDMA	Frequency Division Multiple Access
GERAN	GSM/EDGE Radio Access Network
GGSN	Gateway GPRS Support Node
GMSC	Gateway MSC
GMSK	Gaussian Minimum Shift Keying
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
GTP-U	GPRS Tunnelling Protocol
HA	Home Agent
HIPERLAN	High-Performance Radio LAN
HLR	Home Location Register
HSCSD	High-Speed Circuit-Switched Data
HSS	Home Subscriber Server
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPCP	IP Control Protocol
IPv4	IP Version 4
IPv6	IP Version 6
IRDP	ICMP Router Discovery Protocol
ISDN	Integrated Services Digital Network
ISM	Industrial Science Medical
ISP	Internet Service Provider
ITU	International Telecommunication Union

M3UA	SCCP adaptation layer "SS7 MTP3 - User Adaptation Layer"
MAC	Medium Access Control
MGW	Media Gateway
MIP	Mobile IP
MN	Mobile Node
MS	Mobile Station
MSC	Mobile Switching Center
MTP	Message Transfer Part
NAT	Network Address Translation
NNI	Network Node Interface
OSI	Open Systems Interconnection
PAN	Personal Area Network
PDA	Personal Digital Assistant
PDCP	Packet Data Convergence Protocol
PPP	Point to Point Protocol
PS	Packet Switched
PSK	Phase Shift Keying
PSTN	Public Switched Telecommunications Network
QoS	Quality of Service
RAN	Radio Access Network
RANAP	RAN Application Part
RCH	Random Access Channel
RLC	Radio Link Control
RNC	Radio Network Controller
RNS	Radio Network Subsystem
RTS/CTS	Request to Send/Clear to Send
SAP	Service Access Point
SCCP	Signalling Connection Control Part
SCTP	Stream Control Transmission Protocol
SDU	Service Data Unit
SGSN	Serving GPRS Support Node
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SMS	Short Message Service
SS7	Signalling System No. 7
SSCF	Service Specific Coordination Function
SSCOP	Service Specific Connection Oriented Protocol
TCP	Transmission Control Protocol
TDD	Time Division Duplex
TDMA	Time Division Multiple Access
TIA	Telecommunications Industry Association
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
UTRAN	UMTS Terrestrial RAN
VHE	Virtual Home Environment
VLR	Visitor Location Register
VoIP	Voice over IP
VPN	Virtual Private Network
WAN	Wide Area Network
WAP	Wireless Application Protocol
WB	Wireless Bridge
WCDMA	Wideband CDMA
WECA	Wireless Ethernet Compatibility Alliance
Wi-Fi	Wireless Fidelity
WLAN	Wireless LAN
WLL	Wireless Local Loop
WWW	World Wide Web

Literatur

[1] M. Mouly, M.B. Pautet, "The GSM System for Mobile Communications", publiziert durch die Autoren, 1992.

[2] ETSI TS 101 038, "Digital cellular telecommunications system (Phase 2+); High Speed Circuit Switched Data (HSCSD)", GSM 03.34, Version 7.0.0, Release 1998.

[3] J. Zobel, "Mobile Business und M-Commerce", Hanser, 2001.

[4] C. Andersson, "GPRS and 3G Wireless Applications", Wiley, 2001.

[5] B. Walke, "Mobilfunknetze und ihre Protokolle", Bd. 1+2, 2. Auflage, Teubner, 2000.

[6] UMTS Forum Report No. 9, "The UMTS Third Generation Market - Structuring the Service Revenues Opportunities", September 2000.

[7] 3GPP TS 23.002, "Network Architecture (Release 1999)".

[8] 3GPP TS 25.410, "UTRAN Iu Interface: General Aspects and Principles (Release 1999)".

[9] 3GPP TS 23.060, "General Packet Radio Service (GPRS); Service description; Stage 2 (Release 1999)".

[10] ANSI/IEEE Std 802.11, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", 1999.

[11] IEEE Std 802.11b, "Higher-Speed Physical Layer Extension in the 2.4 GHz Band", 1999.

[12] IEEE Std 802.11a, "High-speed Physical Layer in the 5 GHz Band", 1999.

[13] ETSI TS 101 761-1, "Broadband Radio Access Networks (BRAN); HIPERLAN Type 2; Data Link Control (DLC) Layer, Part 1: Basic Data Transport Functions", 2000.

[14] J. D. Solomon, "Mobile IP - The Internet Unplugged", Prentice Hall, 1998.

[15] 3GPP TS 29.061, "Interworking between the Public Land Mobile Network (PLMN) supporting Packet Based Services and Packet Data Networks (PDN), (Release 1999)".

[16] I. Guardini, P. D'Urso, P. Fasano, "The Role of Internet Technology in Future Mobile Data Systems", IEEE Communications Magazine, November 2000.

[17] S. Dixit, Y. Gou, Z. Antoniou, "Resource Management and Quality of Service in Third-Generation Wireless Networks", IEEE Communications Magazine, Februar 2001.

[18] 3GPP TS 23.002, "Network Architecture (Release 5)".

[19] N. Björkman, Y. Ziang, T. Lundberg, A. Latour-Henner, A. Doria, "The Movement from Monoliths to Component-Based Network Elements", IEEE Communications Magazine, Januar 2001.

[20] T. Tailor, "Megaco/H.248: A New Standard for Media Gateway Control", IEEE Communications Magazine, Oktober 2000.

[21] 3GPP TSG RAN TR 25.933, "IP Transport in UTRAN", März 2001.

[22] G. Armitage, "MPLS: The Magic Behind the Myths", IEEE Communications Magazine, Januar 2000.

[23] H. Schulzrinne, J. Rosenberg, "The Session Initiation Protocol: Internet-Centric Signaling", IEEE Communications Magazine, Okt. 2000.

[24] L. Ladid, "IPv6 - The new-generation Internet", Ericsson Review No. 1, 2000, verfügbar unter http://www.ericsson.com/review/2001-01/.

[25] 3GPP TS 43.051, "GSM/EDGE Radio Access Network (GERAN); Overall Description - Stage 2; (Release 4)".

[26] ETSI TS 101 948, "Digital Enhanced Cordless Telecommunications (DECT); DECT derivative for implementation in the 2,45 GHz ISM Band (DECT-ISM)", V1.1.1, April 2001.

Alle Standards und Arbeitspapiere des 3GPP sind frei verfügbar unter http://www.3gpp.org/.
Die Standards der IETF können unter http://www.ietf.org gefunden werden.
Berichte des UMTS Forum liegen unter http://www.umts-forum.org/.
Zumindest alle IEEE-Standards der Serie 802 sind unter http://www.ieee.org/ frei verfügbar.

Neue Seminare

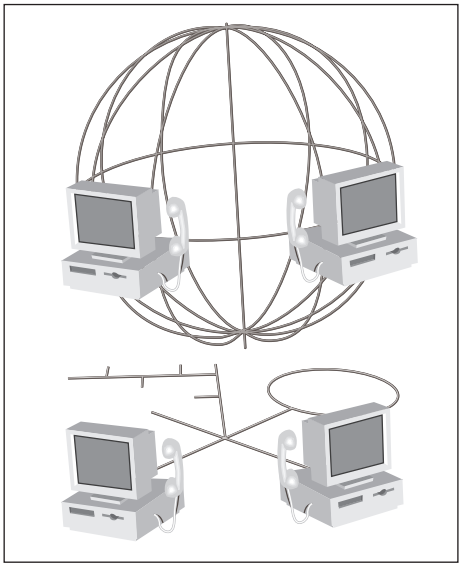
Voice over IP

Vom 3. bis 5. Juni 2002 veranstaltet die ComConsult Akademie im Park Plaza Köln zum ersten Mal ihr neues Seminar "Voice over IP erfolgreich und profitabel im Unternehmen einsetzen".

Das Seminar richtet sich an die Verantwortlichen, Entscheidungsträger, Planer und Betreiber von TK-Anlagen, Lokalen Netzwerken, Call Centern, die sich über die optimale und erfolgreiche Weiterentwicklung bestehender Telephonie-Lösungen in Richtung Voice-over-IP informieren wollen. Das Seminar konzentriert sich auf IP-Telefonie und ihre Funktion im strategischen Gesamtzusammenhang der Unternehmens-Kommunikation im Enterprise-Umfeld. Behandelt werden Anforderungen, Verfahren, Komponenten, Funktionen, Einsatz-Szenarien und etablierte Hersteller-Lösungen, mit denen über IP-Netzwerke wie Intranet und Internet Voice und multimediale Informationen übertragen werden können. Standards und Produkte für Voice Endgeräte, IP-TK-Anlagen und Gateways zur klassischen Telefonie werden vorgestellt.

Die Referentin Dipl.-Inform. Petra Borowka leitet das Planungsbüro UBN und gehört zu den führenden deutschen Beratern für Kommunikationstechnik. Sie ist langjährige Referentin der ComConsult Akademie, ihre Kenntnisse, internationale Veröffentlichungen, Arbeiten und Praxisorientierung sowie herstellerunabhängige Position sind international anerkannt. Sie verfügt über langjährige erfolgreiche Praxiserfahrung bei der Planung und Realisierung von Netzwerk-Lösungen. Das Seminar nimmt Stellung zu folgenden Themen:

- welche Leistungsmerkmale IP-Telefone und VoIP-Lösungen bieten, aus welchen Komponenten eine Lösung besteht, welche Standards relevant sind
- welche neuen Entwicklungen und Standards wann realistisch zu erwarten sind
- was VoIP nicht leistet, wann und wie die Defizite beseitigt werden können
- wie die entscheidenden Profit-Anwendungen realisiert werden
- wie die Integration aus VoIP mit bestehenden TK-Lösungen erfolgt
- welche Vorteile ein Call-Center oder eine Unified Messaging Lösung auf Basis Voice over IP bietet
- wie der typische Einsatz einer erfolgreichen Lösung aussieht
- wie die Haltung wichtiger Hersteller wie Siemens und CISCO zu diesem Thema ist, was ihre Produkte leisten, wohin der weitere Entwicklungstrend geht
- welche Investitionen und Änderungen zuvor im LAN-Bereich erfolgen müssen



Zum Thema

IP-Technologie ist die Basis für alle Kommunikations-Anwendungen der Zukunft. Naturgemäß werden damit nicht IP-basierte Technologien mehr und mehr verdrängt. Von daher ist auch die Verdrängung der traditionellen Telephonie nur eine reine Frage der Zeit. Speziell im Provider-Markt ist auch erheblicher Druck in dieser Richtung zu beobachten. Gerade die aktuellen Siemens-Ankündigungen im Bereich der Weiterentwicklung der bisherigen HICOM-Systeme belegen, dass aus der Voice-over-IP-Spielwiese der letzten Jahre nun Marktrealität wird. Für die Unternehmen stellt sich somit nicht die Frage, ob sondern mehr wann und wie der Wechsel Richtung Voice over IP erfolgt. Mit der neuen Marktrealität haben sich aber auch die Positionierung von IP-Telefonie und die sinnvollen Einsatzszenarien geändert. Für viele Anwender werden die nächsten Jahre aus einem genau ausgewogenen Mischbetrieb aus VoIP und traditioneller Telefonie bestehen. Aus beiden Welten das Optimum in einem kombinierten Betrieb nutzen, das ist die Basis für einen erfolgreichen und wirtschaftlich optimalen Einsatz von VoIP. Mit dem Umbau der Provider-Netzwerke hin zu mehr Bandbreite entstehen die technischen Voraussetzungen zur Übertragung von Voice over IP quasi als Abfallprodukt. Für die Provider wird dabei Voice over IP zu einer Schlüsseltechnologie im Leistungsangebot den Kunden gegenüber, da die Infrastrukturkosten vergleichsweise gering sind, die Kundenwirkung aber sehr hoch ist.

Vom 3. bis 4. Juni 2002 veranstaltet die ComConsult Akademie im Courtyard by Marriott in Düsseldorf zum ersten Mal ihr neues Seminar "Voice over IP in Providernetzen".

Das Seminar richtet sich an die Verantwortlichen, Entscheidungsträger, Planer und Betreiber von Provider-Netzen für Voice over IP und Multiservice over IP.

Naturgemäß unterscheidet sich die technische Realisierung für Voice over IP innerhalb einer Provider-Infrastruktur gegenüber den Realisierungen bei Endkunden. Für den Provider sind ernst zu nehmende Infrastruktur-Maßnahmen erforderlich, die weit über die reine Übertragung von digitaler Sprache hinaus gehen. Als Beispiele seien nur die Gateway und die Abrechnungs-Problematik genannt.

Behandelt werden Protokolle, Standards und Komponenten, mit denen sich über Provider-IP-Netze Voice, Video und multimediale Informationen übertragen lassen. Standards und Produkte für Video- und Multimedia-Conferecing werden vorgestellt, ebenso wie neue Ideen aus den Standard-Arbeitsgruppen der ITU (International Telecommunications Union), der IETF (Internet Engineering Task Force) sowie den Labors der Hersteller.

Der Referent Dr. Behrooz Moayeri blickt auf langjährige Erfahrungen bei der Beratung von großen Unternehmen und Service Providern zum Aufbau von Multiservice-Netzen zurück. Er gehört der Geschäftsleitung der ComConsult Beratung und Planung GmbH, Aachen, an.

Das Seminar beantwortet folgende Fragestellungen:

- Warum Provider auf Voice over IP setzen
- Warum Voice over IP eine Schlüsseltechnologie ist
- Welche Eigenschaften ein IP-Netzwerk für die Voice-over-IP-Nutzung aufweisen muss
- Welche Standards und Verfahren für die Umsetzung bei Providern relevant sind und welche Marktrelevanz die einzelnen Standards haben
- Aus welchen Komponenten die Providerlösung für Voice over IP bestehen muss
- Wie Quality of Service und Security zu bewerten und umzusetzen sind
- Worin die Unterschiede zwischen einer Provider- und einer Endkundenlösung liegen

Voice over IP

Voice over IP
erfolgreich und profitabel im Unternehmen einsetzen

Der Inhalt

- Basis IP: was bedeutet das?
- Kommunikationstechnische Anforderungen von Voice, Multimedia und Conferencing: Antwortzeit, Puffer und Jitter, Datenraten, Kompression, Netzdesign in LAN und WAN
- Arbeitsweise von Multicast-Anwendungen: wie werden LANs und WANs Multicast-fähig gemacht?
- Protokolle und Standards für Voice over IP, Ansätze der ITU und IETF und ihre Marktrelevanz: UDP, RTP / RTCP / RTSP, H.323, H.450, H.248 / MeGaCo, SIP, MGCP, GLP, User Location Services
- Welche Funktionen braucht eine IP-Telefonie Lösung? Welche werden heute unterstützt? Basis-Funktionen, Erweiterte Leistungsmerkmale, Call-Center und Kunden-kontakt, Skalierbarkeit, Redundanz, unterstützte Endgeräte (analog, digital, DECT, 10 Mbit, 100 Mbit, remote ...)
- Komponenten einer IP-Telefonie Lösung und wie sie funktionieren: PC mit Softphone, IP-Telefon, TK-Anlage mit IP-Anschluss, LAN-PBX, Telefonie-Server, weitere VoIP Applikations-Server, VoIP-Gateways: H.323 - PSTN; H.323 - Herstellerwelt , LAN und WAN Einsatz-Szenarien für IP-Telefonie in Corporate Netzwerken , IP-Telefonie und VPN-Einsatz
- Überblick über Herstellerlösungen: Siemens, Cisco, Alcatel, Avaya, Nortel
- Priorisierung / Quality of Service in LANs und WANs – notwendig oder Spielerei? DiffServ, 802.1p/Q, RSVP, MPLS, OSPF-TE, Policy Server

Voice over IP
in Providernetzen

Der Inhalt

- Kommunikationstechnische Anforderungen von Echtzeit-Informationsströmen
- Kommunikationsprotokolle und Protokollstacks für Voice-Kommunikation
- IP und ATM für Voice und Video: Miteinander oder Gegeneinander?
- Bereitstellung von mehr und mehr Kapazität vs. aufwendige Verfahren für Quality of Service
- Priorisierung in IP-Netzen
- Multicast-Problematik: Wie lassen sich IP-Netze auf Multicasts vorbereiten?
- Conferencing für Voice, Video und Daten
- Probleme bei Voice over IP: Netto-Datenraten, Kompression, Signalverzögerung, Buffering und Jitter
- IP-Netze und IP-Routing
- IP-VPN Netze
- Die Standards für Voice over IP: H.323 / H.450, SIP, MGCP, H.248 / MeGaCo,
- VoIP-Nebenstellentechnik, VoIP in Kundennetzen
- Komponenten von VoIP in Providernetzen
- Funktion der Komponenten: Media Gateway, Signaling Gateway, Media Gateway Controller, Applikationsserver
- Sicherheitsbewertung von Voice oder IP

Der Veranstalter behält sich Änderungen in den Programmen vor.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
Voice over IP

Ich melde mich an für das Seminar

Voice over IP erfolgreich und profitabel im Unternehmen einsetzen
☐ 03. bis 05.06.02 Park Plaza Köln
☐ 08. bis 10.10.02 Hilton Bonn
zum Preis von € 1.590,-- zzgl. MwSt. an

Voice over IP in Providernetzen
☐ 03. bis 04.06.02 Courtyard Düsseldorf
☐ 08. bis 09.10.02 Exelsior Berlin
zum Preis von € 1.290,-- zzgl. MwSt. an

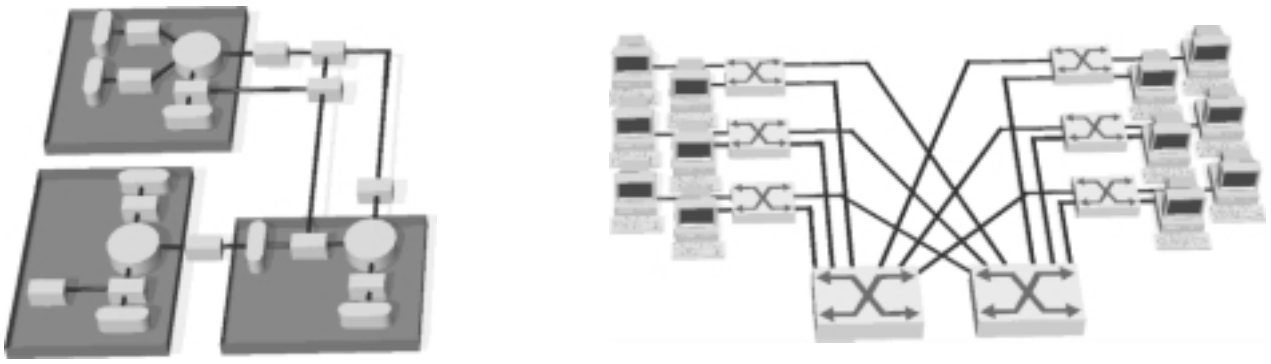
☐ Bitte buchen Sie für mich ein Hotelzimmer

Faxen Sie uns einfach diesen Abschnitt an **02408/955-399** oder schicken Sie eine eMail an **mail@comconsult-akademie.de** oder buchen Sie über unsere Web-Seite **http://www.comconsult-akademie.de**

Name	Vorname
Firma	Abteilung
Position	Funktion
Straße	PLZ, Ort
Telefon	Fax
eMail	Unterschrift

Neues Seminar

OSPF und VRRP optimal konfigurieren



Zum Thema

Durch den Preisverfall von Layer 3 Switches halten Routingtechnologien auch in Lokalen Netzen zunehmend Einzug. Diese Verfahren bieten weitere Vorteile zu den klassischen Layer 2 Mechanismen.

OSPF hat sich in den vergangenen Jahren zu dem Standard-Routingprotokoll für Unternehmen entwickelt. Mittlerweile wird es nicht nur von allen führenden Herstellern unterstützt sondern die Interoperabilität zwischen den verschiedenen Produkten ist hergestellt. So sind nicht nur Lastverteilung über kostengleiche Wege und schnelle Umschaltzeiten sondern auch die Möglichkeit der Fehlertrennung gute Gründe Routing einzusetzen. Viele schrecken heute vor dem Einsatz von OSPF noch zurück und arbeiten entweder ohne dynamisches Routing oder setzten veraltete bzw. herstellerproprietäre Protokolle ein.

VRRP bietet die Möglichkeit eine geräteübergreifende Redundanz für Default-Gateways zu realisieren, ohne an den einzelnen Clients Änderungen vornehmen zu müssen. Aktuell ist die Tendenz festzustellen, dass der Standard VRRP sich immer mehr gegenüber den herstellereigenen Lösungen durchsetzt. Für die Realisierung eines vollständigen Redundanzkonzeptes ist eine solche Routerdedundanz unverzichtbar.

Vom 9. bis 11. Juli 2002 veranstaltet die ComConsult Akademie in Aachen zum ersten Mal ihr neues Seminar "OSPF und VRRP optimal konfigurieren".

Diese Veranstaltung vermittelt umfassende Kenntnisse zu den Layer 3 Standards OSPF und VRRP.

Das Seminar vermittelt die notwendigen Kenntnisse für die Migration und den erfolgreichen Betrieb von OSPF Netzen. Grundlegende Theorien werden eingehend erläutert und somit die notwendigen Grundlagen für ein erfolgreiches Troubleshooting gelegt.

Besonderer Wert wird dabei auf die direkte Anwendbarkeit durch Live-Vorführungen unter Einsatz von Produkten führender Hersteller gelegt.

Für ein umfassendes, Layer 3 basiertes Redundanzkonzept ist Router-Redundanz ein unverzichtbares Element. Aus diesem Grund wird VRRP eingehend behandelt und typische Fehlkonfigurationen werden anhand von Fallbeispielen dargestellt.

Abgerundet wird die Veranstaltung durch die Besprechung von LAN und WAN Installationsbeispielen.

Die Teilnehmer lernen:

- Wie die Verfahren VRRP und OSPF funktionieren
- Wann der Einsatz im LAN oder WAN Betrieb sinnvoll ist
- Wie man die Migration vorbereitet
- Worauf man bei der Implementierung achten muss
- Wie man typische Fehler vermeidet

Markus Schaub ist seit vielen Jahren für die ComConsult Technologie Information GmbH tätig. Seine Aufgabenbreiche umfassen die Evaluierung, Konfiguration und Inbetriebnahme neuster Hard- und Software aus dem Netzwerkumfeld. Insbesondere verfügt er über langjährige Betriebs- und Praxiserfahrung mit CISCO-Routern und CISCO-Switch-Systemen. Er ist ComConsult Certified Network Engineer und von Cisco CCNP™ zertifiziert. Darüber hinaus ist er für den Betrieb des CISCO-Router-Netzes der ComConsult Akademie verantwortlich.

OSPF und VRRP optimal konfigurieren

OSPF und VRRP optimal konfigurieren – Der Inhalt

Einleitung

- Routing
  - Wann Switching
  - Wann Routing
- Routingtabelle
  - Best Match Prinzip
  - Abgrenzung First Match
- Routing Konzepte
  - Statisch
  - Dynamisch
  - Distant Vecor
  - Link State
  - Vor- und Nachteile der Verfahren
  - Anwendungsbeispiele

Einleitende Theorie

- VLSM / CLNS
- Aufbau von IP Adressen
- Aufbau von Subnetzmasken
- Route Aggregation
- Strukturiertes IP Design
- Beispiele

OSPF Grundlagen

- Topologie-Tabelle
  - Funktion
  - Aufbau
  - Algorithmus
- Routing-Tabelle
  - Funktion
  - Aufbau
- Equal Cost Routing
  - Funktionsweise
  - Effizientes Pfadkostendesign
- Nachbarn
  - Poin-to-Point
  - Point-to-Multipoing
- Authentifizierung
- Routerstati
- Rerouting
- Sonderfälle
  - Externe Routen
  - TOS based Routing

OSPF Areas

- Konzept
  - Normal Area
  - Backbone Area
  - NSSA
  - Totaly Subby
- Router Typen
  - Internal Router
  - Backbone Router
  - ABR
  - ASBR
- LSA Typen
- Virtual Link
- Einsatzbeispiele
  - LAN
  - FrameRelay

VRRP

- Problembeschreibung
- Alternative Lösungen
- Virtual Router Konzept
  - Arbeitsweise
  - Master/Slave
  - Wahlverfahren
  - Fehlerbehandlung
- Lastverteilung
  - Funktionsprinzip
  - Einschränkung
  - Probleme
- Problemfälle
- Anwendungsszenarien
- Herstellerverfahren
  - HSRP
  - ESRP
  - FSRP

Der Veranstalter behält sich Änderungen im Programm vor.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
OSPF und VRRP optimal konfigurieren

Ich melde mich an für das Seminar
OSPF und VRRP optimal konfigurieren

☐ vom 09. - 11.07.02 Aachen
zum Preis von € 1.590,-- zzgl. MwSt. an

☐ Bitte buchen Sie für mich ein Zimmer im Hotel

Faxen Sie uns einfach diesen Abschnitt an **02408/955-399** oder schicken Sie eine eMail an **mail@comconsult-akademie.de** oder buchen Sie über unsere Web-Seite **http://www.comconsult-akademie.de** Ihren Platz auf unserer Veranstaltung.

Name _____ Vorname _____

Firma _____ Abteilung _____

Position _____ Funktion _____

Straße _____ PLZ, Ort _____

Telefon _____ Fax _____

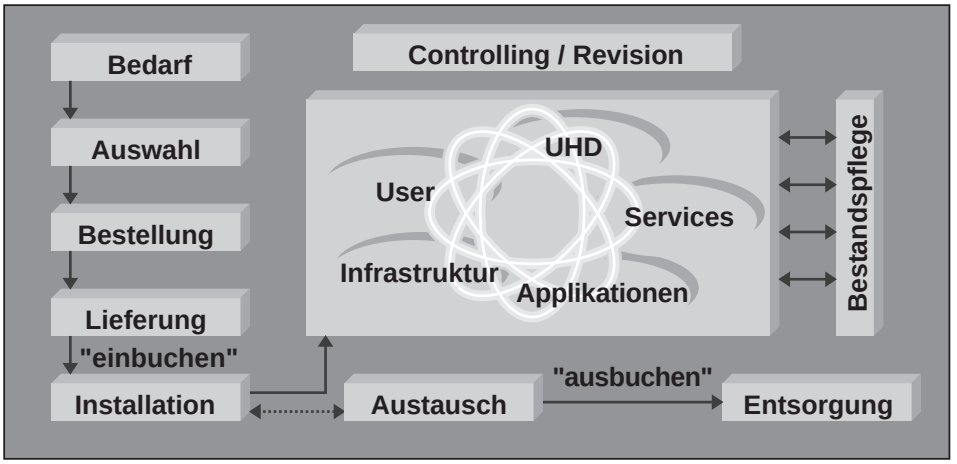
eMail _____ Unterschrift _____

Neues Seminar

IT-Asset Management wertschaffend einsetzen

Am 9. und 10. Juli 2002 veranstaltet die ComConsult Akademie in Hilton Bonn zum ersten Mal ihr neues Seminar "IT-Asset Management wertschaffend einsetzen".

Die Veranstaltung richtet sich an Geschäftsführer, IT-Manager, IT-Controller, IT-Revisoren, Mitarbeiter im IT-Einkauf, IT-Organisation, Inventarisierungsmanager, Leiter Rechenzentren und allgemein allen Asset-Management Verantwortlichen.



Zum Thema

Der Ruf nach effektiven IT-Asset Management – Lösungen ist in den letzten Jahren immer lauter geworden. Die wachsenden Komplexität der IT-Kostenstrukturen (TCO) und die Beherrschung der IT-Lebenszyklen bei anhaltend steigendem Kostendruck bindet zunehmend Personalressourcen.

Kosten-Transparenz fehlt, da Daten von verschiedenen Bereichen mehrfach und zum Teil manuell erhoben, gepflegt und aktualisiert werden. Eine Übersicht von Betriebs-, Prozess- und Verwaltungskosten und der Einfluss von Prozessänderungen auf diese Kostenstrukturen kann nicht erstellt werden. Anforderungen wie Revisionssicherheit und ein effektives Kosten-Controlling sind damit kaum zu erfüllen. Abhilfe schafft hier ein bereichs- und technologieübergreifendes IT-Asset Management. Durch Zusammenführung der verschiedenen Informationskanäle können nun aussagekräftige Angaben über die wahren Kosten der IT-Assets gemacht werden. Hierbei werden diejenigen Ansatzpunkte deutlich, bei deren Optimierung sich die größten Kosteneinsparungen ergeben. Ebenso kann auf Grundlage der gewonnenen Daten eine Leistungsverrechnung erfolgen. Der Mehrwert beschränkt sich nicht nur auf die Betriebsunterstützung, sondern gibt den strategischen Überlegungen der Unternehmensführung einen entscheidenden Vorsprung um flexibel und planend agieren zu können.

Jedes Unternehmensumfeld ist einzigartig. Daher müssen die Best-Practice-Lösungen für jede Umgebung neu bewertet und angepasst werden.

Das Seminar gibt anhand von Analystenaussagen und Studien einen Überblick der zukünftigen Herausforderungen an ganzheitliches IT-Asset Management und die hieraus entstehenden Kosteneinsparpotentiale. Das Seminar berücksichtigt auch Best-Practice Vorgehensweisen in Anlehnung an ITIL-Prozesse und eine Übersicht der im Markt führenden Werkzeuge. Die Teilnehmer erhalten Antworten auf die Fragen:

- Wie kann Transparenz in der Verteilung der IT-Vermögensgüter Ihres Unternehmens geschaffen werden?
- Wie funktioniert ein automatisches IT-Inventory?
- Wie kann Ihr Unternehmen IST- und SOLL-Daten vergleichen und welchen Nutzen erlangen Sie hierdurch?
- Wie beantworten Sie leicht folgende Fragen: Wo steht das Gerät "XY"? Wann läuft der Leasing-Vertrag aus? Welche Kostenstelle ist hiervon betroffen?
- Für welche Leitungen oder Dienste entstehen jeden Monat welche Kosten und wie werden diese genutzt?
- Welche Geräte sollen in den nächsten 4 Monaten planmäßig ausgetauscht werden?
- Welche Vorteile bietet eine zentrale IT-Inventory-Datenbank?
- Welche Vorteile gewinnt Ihr Unternehmen durch Verknüpfung der kaufmännischen, der technischen und der Dienst-orientierten Asset-Daten?
- Wie und wo ist Kosteneinsparung möglich und sinnvoll?
- Welche Angaben benötigt das IT-Controlling zur effektiven Kostenkontrolle?
- Was sind die Unterschiede und Überschneidungen zwischen IT-Asset Management und Themen wie: Config. Management, Facility-Management, Service-Management, Leistungsverrechnung, LifeCycle-Management, Vertrags- und Lizenz-Management etc.?
- Wie kann man strukturelle und technische Informationen sinnvoll miteinander verknüpfen?
- Welche Prozesse pflegen unsere Daten? Was sind bewährte Inventarisierungs-Methoden?
- Welchen Nutzen kann Ihr Unternehmen aus einem aussagekräftigen Reporting ziehen und welche Maßnahmen leiten sich hieraus ab?
- Was sind die zukünftigen Herausforderungen an ein ganzheitliches Asset-Management?
- Wie ist eine strategische Planungsgrundlage zu schaffen?

Der Referent Dr.-Ing. Roger H. Jakobs sammelte nach Studium und Promotion an der Fakultät für Maschinenwesen der RWTH Aachen bei einem IT-Systemintegrator Erfahrung als Ausbilder, Systemberater und Manager von Roll-outs bei Großunternehmen. Nach einer mehrjähriger Tätigkeit als IT-Leiter und im höheren Management unterstützt er nun als Senior-Berater den Ausbau des Wachstumsbereichs IT Asset Management bei der ComConsult Kommunikationstechnik GmbH.

IT-Asset Management wertschaffend einsetzen

IT-Asset Management wertschaffend einsetzen – Der Inhalt

1. Tag

Allgemeine Einführung in die Thematik des IT-Asset Managements

LifeCycle-Betrachtung
- Beschaffung
- Installation / Austausch
- Bestandspflege

Entwicklungsstufen des IT-Asset Managements
- Beherrschung des Chaos
- Reaktives Feuerlöschen
- Transparenz über IST- und Soll-Daten
- Beitrag zur Verwirklichung der Unternehmensziele
- Vollständige Integration der Geschäftsprozesse

Bereichsübergreifendes Reporting
- Strategische Planung: die gesammelten Informationen verwerten

Diskussion
ggf. Fallbeispiele der Teilnehmer

2. Tag

Projektvorgehen für erfolgreiches IT-Asset Management
- Zuständigkeiten klären
- Projektteam gründen
- Ziele definieren
- Projekt-Reportingstrukturen definieren
- KickOff
- IST-Situation klären
- Datenerhebung / -Aktualisierung
- Prozesse erheben, optimieren und festlegen
- Effektives Reporting und strategische Planung koppeln

Werkzeuge für IT-Asset Management Projekte
- Marktübersicht
- Maßgeschneiderte Lösung oder "Out-of-the-Box"/Best Practice?
- Für wen lohnt sich ein IT-Asset Management-Projekt (ROI)?
- Inventory-Tools (z.B. Tivoli Inventory, Peregrine Infratools etc.)
- Tools mit kaufmännischem Schwerpunkt (z.B. Peregrine Asset Center, USU ValueWise, SAP etc.)
- Tools mit technischem Schwerpunkt (z.B. ComConsult CCM, MainControl MC/EM Power etc.)

Diskussion, Klärung offener Punkte der Merker-Liste

Der Veranstalter behält sich Änderungen im Programm vor.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
IT-Asset Management wertschaffend einsetzen

☐ Ich melde mich an für das Seminar **IT-Asset Management wertschaffend einsetzen** vom 09.07.-10.07.02 im Hilton Bonn zum Preis von € 1.290,-- zzgl. MwSt.

☐ Bitte buchen Sie für mich ein Zimmer im Veranstaltungshotel

Faxen Sie uns einfach diesen Abschnitt an **02408/955-399** oder schicken Sie eine eMail an **mail@comconsult-akademie.de** oder buchen Sie über unsere Web-Seite **http://www.comconsult-akademie.de** Ihren Platz auf unserer Veranstaltung.

Name	Vorname
Firma	Abteilung
Position	Funktion
Straße	PLZ, Ort
Telefon	Fax
eMail	Unterschrift

ComConsult Certified Network Engineer

"Ich war schon immer auf der Suche so etwas zu machen."

Klaus Künstle (37) arbeitet bei der Alno AG in Pfullendorf in der Nähe vom Bodensee. Er ist zuständig für Netzwerkinfrastruktur, Verkabelung, aktive und passive Komponenten, Switches, Router – alles was zum Netzwerk gehört. Der Netzwerk Insider sprach mit ihm unmittelbar nach seiner bestandenen Prüfung zum ComConsult Certified Network Engineer.

Insider: Sind Sie dort in einer größeren Gruppe?

Klaus Künstle: Nein, ich bin dort mehr oder weniger alleine. Ich führe dort die Planung und führe auch die Installation durch.

Insider: Wie lange machen Sie das schon?

Klaus Künstle: So drei bis vier Jahre. Bei Alno bin ich schon seit 10 Jahren, war aber zuerst im Bereich Telekommunikation tätig. Dann ging es los mit Netzen, die Netze wurden entsprechend aufgebaut und da wurde jemand dafür gebraucht, der das macht. Und das hab ich dann übernommen.

Insider: Was haben Sie gelernt?

ComConsult Certified Network Engineer Klaus Künstle

Klaus Künstle: Ich habe Elektroinstallateur gelernt und habe mich dann entsprechend weitergebildet in Richtung Informations- und Kommunikationstechnik.

Insider: Wie kamen Sie zur Ausbildung zum ComConsult Certified Network Engineer?

Klaus Künstle: Ich bin eigentlich schon seit einigen Jahren in Kontakt mit der Firma ComConsult und hab da schon mehrere Seminare gemacht. Ich war schon immer auf der Suche so etwas zu machen, wo es nachher ein Zertifikat oder eine Anerkennung gibt. Gerade im Netzwerkbereich gibt es ja eigentlich nichts, es gibt ja bis jetzt noch keinen entsprechenden Ausbildungsberuf. Dass man das Wissen nachweisen kann, ist natürlich auch für die Zukunft wichtig, um in der Firma oder sonst irgendwo weiterzukommen und um die Qualifikation beim Geld oder bei Verhandlungen ums Geld mit einbringen zu können.

Insider: Hat das, was Sie in der Ausbildung gelernt haben, einen Einfluss auf Ihre Berufspraxis?

Klaus Künstle: Auf jeden Fall. Grade die letzten beiden Kurse, die ich gemacht habe, Internetworking und Ethernet-Technologien hatten eine große Auswirkung, da ich momentan dabei bin, ein Netz neu zu planen, vom Token Ring in Richtung Ethernet zu migrieren. Da hat mir das sehr sehr viel gebracht. Jetzt kann ich auf die entsprechenden Firmen zu gehen und kann sagen, okay, das und das möchte ich, welcher Hersteller kann das realisieren?

ComConsult Veranstaltungskalender

Aktuelle Veranstaltungen

Verkabelungssysteme für Lokale Netze, 03. - 04.06.02 in Bonn

Das Seminar basiert auf der Erfahrung einer Vielzahl aktueller Verkabelungsprojekte und deren Betrieb. Es führt methodisch vom aktuellen Stand der Technik bis zu den Leistungsmerkmalen zukünftiger Lösungen.
Referent: Dipl.-Ing. Hartmut Kell, ComConsult Beratung und Planung — Preis: € 1.290,-- zzgl. MwSt.

Betrieb von TCP/IP-Netzen, 03. - 05.06.02 in Bonn

Das Seminar vermittelt praxisnah die für den erfolgreichen Betrieb von IP-Netzen notwendigen Basis-Kenntnisse der TCP/IP-Technologie und geht insbesondere wird auf die für den professionellen Betrieb unverzichtbaren Hilfsmittel ein.
Referenten: Dipl.-Inform. Oliver Flüs, Dipl.-Inform. Andreas Meder — Preis: € 1.590,-- zzgl. MwSt.

Voice over IP in Providernetzen, 03. - 04.06.02 in Düsseldorf

Das Seminar behandelt Protokolle, Standards und Komponenten, mit denen sich über Providernetze Voice, Video und multimediale Informationen übertragen lassen und stellt Standards und Produkte für Multimedia Conferencing vor
Referent: Dr. Behrooz Moayeri — Preis: € 1.290,-- zzgl. MwSt.

Voice over IP erfolgreich und profitabel im Unternehmen einsetzen, 03. - 05.06.02 Köln

Das Seminar informiert über neue Möglichkeiten und Entwicklungen durch Integration von Sprache in Datennetzen, welchen Mehrwert und welche Lösungen in Unternehmen gewinnbringend eingesetzt werden können.
Referent: Dipl.-Inform. Petra Borowka — Preis: € 1.590,-- zzgl. MwSt.

Migration zu Windows 2000 Active Directory, 10. - 11.06.02 in Bonn

Das Seminar vermittelt die grundsätzlichen Migrationsansätze und welche Tools in welcher Form dabei eingesetzt werden können.
Referenten: Markus Holländer, Dipl.-Ing. Michael van Laak — Preis: € 1.290,-- zzgl. MwSt.

MOM 2000 – Microsoft Operation Manager, 17. - 18.06.02 in Bonn

Das Seminar hinterfragt den Operation Manager, der die gesamte Bandbreite BackOffice, Server- und Net-Produktfamilie "out of the box" managen soll, demonstriert live die Funktionsweise und stellt die Extended Management Packs vor.
Referent: Dipl.-Ing./MCSE Martin Barbian, ITC GmbH — Preis: € 1.290,-- zzgl. MwSt.

Schirmung, Erdung, Potentialausgleich..., 24. - 25.06.02 in Bonn

Das Seminar behandelt die scheinbar unerklärbaren Störerscheinungen in Netzwerken und im Betrieb elektronischer Geräte, die durch Wechselwirkungen mit der Elektroinstallation entstehen.
Referenten: Dipl.-Ing. Karl-Heinz Otto und Hans-Günter Hergesell — Preis: € 990,-- zzgl. MwSt.

DNS-/IP-Design für Windows 2000 Active Directory, 24. - 26.06.02 in Bonn

Dieses Seminar behandelt in konzentrierter Form die Implementierungsgrundlagen aus dem IP-Bereich für Windows 2000 bzw. für das Active Directory. Dabei spielt DNS die Hauptrolle, wobei auch insbesondere die dynamische Verbindung zum DHCP betrachtet wird.
Referenten: Markus Holländer, Lars Kuhl, Michael van Laak, Frank Neunzig — Preis: € 1.590,-- zzgl. MwSt.

ComConsult Akademie – Telefax: 02408/955-399

Anmeldung

Titel des Seminars _____ Name _____ Vorname _____

Termin _____ Firma, Abteilung _____ Position, Funktion _____

☐ Bitte buchen Sie für mich ein Zimmer im Veranstaltungshotel

Straße _____ PLZ, Ort _____

Faxen Sie uns einfach diesen Abschnitt an **02408/955-399** oder schicken Sie eine eMail an **mail@comconsult-akademie.de** oder buchen Sie über unsere Web-Seite **http://www.comconsult-akademie.de**

Telefon _____ Fax _____

eMail _____ Unterschrift _____

Handelsplattform für gebrauchte Netzwerkkomponenten

Gebrauchte Netzwerkkomponenten

Die Spielregeln

Gebrauchte Netzwerk-Komponenten, die im Rahmen eines Redesigns ausgemustert werden, könnten einige Betriebe sehr gut gebrauchen. Hier wollen wir helfen.

Die Spielregeln: Sie melden uns ihr Angebot oder Gesuch per Mail, mit dem Fax-Formular (unten) oder über den Web-Server. Wir veröffentlichen es unter einer Anzeigen-Nr. im Insider und auf dem Webserver der ComConsult Akademie unter www.comconsult-akademie.de. Wir stellen den Kontakt zwischen Anbieter und Nachfrager her. Wir erhalten vom Verkäufer für diese Leistung 10% Provision auf den erzielten Kaufpreis. Davon stellen wir die Hälfte ausgewählten Schulen als Spende zum Aufbau ihres Internet-Zugangs oder ihres internen Netzwerks zur Verfügung. Der Kaufvertrag entsteht direkt zwischen Käufer und Verkäufer. Wir selber haften in keiner Form für die Qualität oder Nutzbarkeit der Komponenten.

Gebote

Adapter

3Com 3C905CX-TX-M, Anzahl 2000, Preis Stck./ 31,75 Euro, 4x 25-pack pro 100-pack, 1 x Treiber-CD pro 25-pack, 1 x Kabel pro Karte. Alle Karten sind neu, in Originalverpackung, "Made in Ireland", Preis zzgl. Fracht, Anzeigen-Nr. B20403

3Com 3C905C-TX-M, Anzahl 400, Preis Stck./31,75 Euro, 4x 100-pack je mit 4 x 25-pack, 1 x Treiber-CD pro 25-pack, 1 x Kabel pro Karte, Original 3Com, "Made in Ireland", Preis zzgl. Fracht Anzeigen-Nr. B20402

IBM 8228 MAU, Anzahl 10, Preis VB, Anzeigen-Nr. B20413

Madge Presto PCI und PCI mk2, Anzahl 140, Preis 20 Fr. pro Stck., Anzeigen -Nr. 20117

Ringleitungsverteiler

Madge Smart LAM, Anzahl 1, Preis VB, Anzeigen-Nr. B20408

Madge LANstack TR20UE 20 Port RJ45, Anzahl 2, Preis VB, Anzeigen-Nr. B20409

Madge Smart CAU plus, Anzahl 5, Preis VB, Anzeigen-Nr. B20410

IBM 8230 Lobe Attachement Modul, Anzahl 4, Preis VB, Anzeigen-Nr. B20411

IBM 8230 Controlled Access Unit, Anzeigen-Nr. B20412

Gebote

Router

Cisco Cisco1750-V2, Anzahl 550, Preis 1200 Euro/Stck., 10/100 Modular Router mit 2 Voice Channels, IOS IP/VOICE und Software. Neu in Originalverpackung, Sigel intakt. Anzeigen-Nr. B20405

Sonstige

ACO-Einsätze 2xRJ45, Cat. 5, geschirmt, Anzahl 88, Preis VB, 4-polig, Belegung 3456 (für TR) Anzeigen-Nr. B20416

IBM 3174-13R mit TR-Adapter, Anzahl 1, Preis VB, Anzeigen-Nr. B20415

IBM 8220-3 Optical Fiber Converter, Anzahl 4, Preis VB, 2 Einbau-Rack mit Netzteil 220V,Anzeigen-Nr. B20414

TR Balun Typ I/RJ45, Anzahl 23, Preis VB, Anzeigen-Nr. B20417

RAD MF 3 TR Media Filter DB-9/RJ45, Anzahl 4, Preis VB,Anzeigen-Nr. B20418

TR Fiber Transceiver Black Box ST-DB9, Anzahl 2, Preis VB, Anzeigen-Nr. B20419

Maxell DataCartridges 8mm, 160ft/7 GB, Anzahl 80, Preis ca. 3 Euro/Stk., gebraucht, Anzeigen-Nr. B20420

Switch/Brücke

Nortel Networks C100, Anzahl 10, Preis gesamt 34.000 Euro, 8 vollausgestattete C100 mit 4 MMF-ATM-ports und MCP, jeweils ein 20-Port-Modul, geswitcht 10/100 und 2 Netzteilen; 1 C100 mit 4 MMF-ATM-Ports und MCP, 5x 4-Port-Module, geswitcht 100 MBit und 2 Netzteile; 1 C100 mit 4 SMF-ATM-Ports und MCP, 5x10-port-Module, shared media 10 oder 100 MBit Zugabe: 1x 2-Port-ATM-Speed (MMF); 1x 4-Port-Etherrspeed(100); 2x 16-Port TOKENSpeed(!! ideal für Migration von Token Ring auf Ethernet); 1x 4-Port-TOKENSpeed; alle C100 haben die SW-Version 4.2.1.0, Anzeigen-Nr. B20404

Cisco WS X5506, Anzahl 2, Preis VB, Cisco Supervisor Engine II MMF für Catalyst 5500. Unbenutzte Teile aus Reservebestand. Anzeigen-Nr. B20401

RAD TRE 8, Anzahl 2, Preis VB, Anzeigen-Nr. B20406

RAD Trim Bridge-16, Anzahl 2, Preis VB, Anzeigen-Nr. B20407

DEC FDDI GIGA Switch, Anzahl 2, Preis 9500 Euro/Stk., je Switch folgende IF: 3x DEFGL-AA (Rev. F) FDDI Linecard, dual, 4x DEFGL-AB (Rev. A, F) FDDI Linecard, single. Auch als Reservematerial einsetzbar, anstelle teurer Wartung! Anzeigen-Nr. B20301

Gesuche

Adapter

Olicom UTP MAU OC 3626, Anzahl 1, Preis VB, erbitte Preisvorstellung, Anzeigen-Nr. S20302

Ringleitungsverteiler

Olicom UTP LAM OC 3612, Anzahl 1, Preis VB, erbitte Preisvorstellung, Anzeigen-Nr. S20303

Sonstige

Wir suchen für den Aufbau eines Intranetzes in einem Studentenwohnheim 5 Switche/ Brücken, 1 TP Ethernet Cat 5 Kabel über 400 Meter und 1 Netzwerk-Server gegen Spendenquittung. Als Gegenleistung können wir nur Spendenquittungen und wenn gewünscht Berichte in div. lokalen Zeitungen (Baden Württemberg) anbieten. Anzeigen-Nr. S20122

Fax an ComConsult 02408/955-399

☐ **Ich suche**
☐ **Ich biete**
☐ **Antwort auf Anzeigen-Nr.** ☐ ☐

Produkt/Komponente/Release/Software

Preisvorstellung

Ansprechpartner

Firma

Ort

Straße

Telefon

Fax

eMail