ComConsult Research

Der Netzwerk Insider

Mai 2005

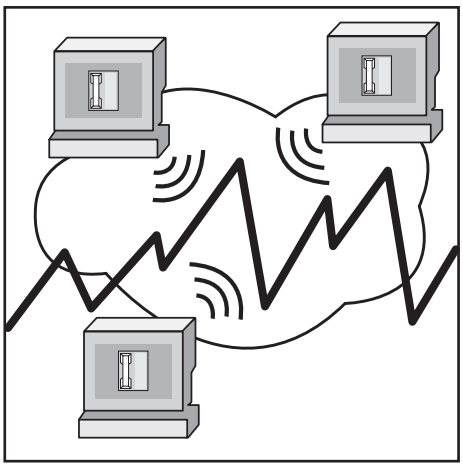
Technologie Information für die Ausbildung zum ComConsult Certified Network Engineer

Schwerpunktthema

Messung der VoIP-Tauglichkeit von Netzwerken

von Dipl.-Ing. Hartmut Kell

Im Bereich der Netzplanung können derzeit zwei sehr starke Trends festgestellt werden, die Einführung von Wireless LAN und die Einführung von VoIP. Bezüglich der WLAN-Technik herrscht die landläufige Meinung, dass eine Einführung bei entsprechend hoher Anzahl von geplanten Access Points grundsätzlich kein Problem ist, auch bei vorhandenen „älteren" Netzen nicht. Anders wird jedoch die Einführung von VoIP bewertet. Die Vorbereitung von neuen, noch zu realisierenden Netzen auf diese zukünftig extrem wichtige Applikation stellt eine „Muss" jeder Planung dar und es darf davon ausgegangen werden, dass eine gute Planung hier entsprechende Designregeln vorsehen wird. Doch wie sieht es bei vorhandenen Lokalen Netzen aus? Wer kennt sein Netz so gut, dass er hier eine zuverlässige Aussage machen kann? Bei wem besteht nicht ein Rest an „Unsicherheit"? Wer kann auf Basis der Topologiekenntnis, Kenntnis der Netzauslastung oder sonstigen möglichen Daten mit gutem Gewissen die Einführung von VoIP für sein Netz in Angriff nehmen? Zur Beseitigung derartiger Unsicherheiten wäre eine für VoIP spezialisierte Netz-Messung in entsprechend qualifizierter Art sehr nützlich, doch welche bringt hier die meisten Sicherheiten?



weiter Seite 27

Zweitthema

IEEE 802.11n: der große MIMO-Bluff und ernst zu nehmende Alternativen

von Dr. Franz-Joachim Kauffels

Selbst ansonsten ausgesprochen ernst zu nehmende Kollegen glauben z.Zt., die MIMO-Technologie, wie sie aktuell in IEEE 802.11n diskutiert wird, als mögliche Nachfolgetechnologie zu IEEE 802.11a/h WLANs aufgreifen zu müssen. Dabei handelt es sich hier nur um eine Art Werbegag, der allenfalls im Consumerbereich eine gewisse Daseinsberechtigung hat. Der einzige gangbare Weg zu Zellen mit mehr Nominalleistung, die gleichzeitig zu bisherigen Planungen im professionellen Umfeld verträglich sind, führt aber über eine Informationsverdichtung in der Modulation/Codierung. Dieser Artikel schafft Klarheit.

Seite 10

Sonderveranstaltung

IP-Telefonie: Markt und Produkte in der Analyse

auf Seite 6

Zum Geleit

Netzwerk-Design im Brennpunkt: neue Verfahren und Strukturen in der Diskussion

auf Seite 2

Report des Monats inkl. Seminar

Planung Elektrosmog-reduzierter WLANs - Das TERW-Konzept

auf Seite 25

Zum Geleit

Netzwerk-Design im Brennpunkt: neue Verfahren und Strukturen in der Diskussion

Der ComConsult Research-Design-Wettbewerb, der anlässlich des Redesign-Forums 2005 stattfand, hat zu einer hohen Resonanz geführt. Nahezu alle führenden Hersteller reichten ein Design basierend auf dem vorgegebenen Szenario ein. Die unterschiedlichen Lösungsansätze spiegeln dabei perfekt sowohl den gegebenen Handlungsdruck als auch das breite und umfangreiche Lösungsspektrum der Hersteller wieder. Auch die in den letzten Monaten zu beobachtenden Verschiebungen zwischen den Marktanteilen der Hersteller waren in den Entwürfen gut wieder zu finden.

Parallel führten auch die Vorträge einzelner Redner zu starken Diskussionen zwischen den Teilnehmern. Zusammengefasst kann man feststellen, dass das Design von Netzwerken sich noch einmal stark ändern wird. Neue Anforderungen wie die Senkung von Konvergenzzeiten im Fehlerfall und eine Benutzergruppenbasierte Segmentierung des Campus erfordern ein Redesign. Gleichzeitig werfen sie erhebliche Fragen auf, bringen sie doch neue und zum Teil herstellerspezifische Verfahren ins Spiel.

Die auf dem Redesign-Forum vorgestellten Design-Ansätze, Technologien und Marktentwicklungen werden wir angesichts der Tragweite dieser Entwicklung in der Sommerschule 2005 wieder aufgreifen.

So können Sie auf der Sommerschule 2005 erwarten:

- Übersicht über die Ergebnisse des ComConsult Research-Design-Wettbewerbs und Diskussion der Unterschiede zwischen den Herstellern
- Vorstellung der neuesten Design-Trends, Aufgreifen der Diskussionen des Redesign-Forums und Erarbeitung von Empfehlungen

Um Ihnen einen Vorgeschmack auf diese Inhalte zu geben, greife ich nachfolgend einige der Diskussionen des Netzwerk-Redesign-Forums 2005 auf. Dies soll die Notwendigkeit der Auseinandersetzung mit diesen Themen und auch die Tragweite möglicher Entscheidungen unterstreichen.

- Quality of Service und die Rolle im modernen Netzwerk-Design war zwischen mehreren Vortragenden umstritten: auf der einen Seite wird QoS als Basis der Trennung von Verkehrsströmen gesehen, also nicht reduziert auf den Schutz von Voice sondern als generelles gestalterisches Element. Auf der anderen Seite wird wie bisher ein unnötiger Einsatz von QoS-Verfahren wegen der hohen Konfigurations-Komplexität und der möglichen Herstellerbindung auf Bereiche reduziert, wo QoS unvermeidbar ist. In der Tat gibt es hier einen erheblichen neuen Diskussionsbedarf gerade auch im Zusammenhang mit Campus-Segmentation (neues Schlagwort im Campus-Design: Protect the good, punish the bad)

- Direkt daran ansetzend war Campus-Design eines der heißen Themen des Forums. Alle Redner waren sich darüber einig, dass nur noch ein reiner Layer-3-Campus zeitgemäß ist. Die alten Design-Ansätze mit Layer-2-Kernen in einem Layer-3-Campus sind definitiv tot. Skalierbarkeit und Konvergenz-Optimierung sind hier die tragenden Elemente. Erhebliche Uneinigkeit bestand in der Frage, ob das Layer-3-Design in Zukunft bis auf die Etage (den Tertiärbereich) ausgedehnt werden soll. Hintergrund dieser Diskussion sind neue Konzepte der Camus-Segmentierung, in denen Layer-3-Segmente die Verkehrsströme lokaler VLANs aufnehmen. Campus-übergreifende VLANs sind endgültig tot, allerdings ist dies kein neuer Trend, wir raten seit Jahren von gebäudeübergreifenden VLANs ab

- Daran schloss sich in den Diskussionen sofort das Thema Autorisierung auf der Basis von IEEE 802.1x an. Alle vertretenen Hersteller und auch alle anderen Vortragenden sehen in der Gestaltung des Anmeldeprozesses am Netzwerk den Schlüssel und die Basis für alle aufsetzenden Konzepte der Netzwerk-Sicherheit und der Benutzertrennung. Auch in diesem Forum wurde deutlich, wie komplex das Thema ist. Die Spannbreite reicht von der Diskussion des Anschlusses von PCs an Telefone mit eingebauten Miniswitches bis hin zur generellen Frage einer zentralen Benutzer- und Geräteverwaltung als Basis einer ACL-basierten Teilnehmer-Zuordnung. Eines wurde in allen Diskussionen und Vorträgen aber klar. 802.1X ist einer der am schnellsten wachsenden Bereiche und wird definitiv im Mittelpunkt aller zukünftigen Netzwerk-Designs stehen (bitte beachten sie unser Spezialseminar zu diesem Thema, 802.1X ist komplex)

- Naturgemäß stand die Frage eines Voice-ready-Design im Mittelpunkt mehrerer Design-Vorträge. Dr. Moayeri brachte die Problematik auf den Punkt. Bisher waren hohe Führungskräfte nur auf der Basis der Beschwerden von Mitarbeitern mit dem Thema Netzwerk-Ausfall befasst. Sobald sie mit IP-Telefonie telefonieren, dürfen sie sich direkt an der Frage der Diskussion von Netzwerk-Verfügbarkeit beteiligen. Der Druck auf die Netzwerk-Betreiber wird immens werden. Mehrere Vortragende griffen dann auch das Thema Verfügbarkeit in Netzwerken auf und es wurde schnell klar in der Diskussion, dass hier erheblicher Handlungsbedarf besteht. Man kann pauschal sagen, dass viele der etablierten Netzwerk-Verfahren nicht wirklich Voice-ready sind. Ein generelles Grundübel ist dabei, dass viele Redundanz-Verfahren auf Timern aufset-

zen, die als kleinste Einheit Sekunden haben. Entsprechend kann die Konvergenzzeit bei Ausfällen nur im Bereich eines Vielfachen von Sekunden liegen. Nur der Rapid-Spanning-Tree ist hier besser. Entsprechend war das Thema Konvergenzzeiten eines der wirklich wichtigen Themen des Forums. So wurden mehrere neue Verfahren vorgestellt, die speziell unter dem Blickwinkel von Konvergenzzeiten von weniger als 1 Sekunde entwickelt worden sind. Speziell Cisco prescht hier doch massiv vor. Für den Anwender ist dies ein unglückliches Thema, da diese neuen Verfahren überwiegend herstellerspezifisch sind. Wie weit soll Konvergenz denn betrieben werden, welchen Grad an Verfügbarkeit wollen wir in Netzen als Basis für Voice denn wirklich erreichen? Diese Frage muss diskutiert werden, zu häufig wird sie mit einem Schulterzucken als akademisch abgetan. Aber wie viele Unternehmen betreiben eine OSPF-Backbone-Struktur mit Konvergenzzeiten bis in den Minuten-Bereich? Ist das Thema in diesen Unternehmen wirklich ausdiskutiert worden? Kann ein Unternehmen damit leben, dass alle Telefonate mit Kunden abbrechen? Ein breites Diskussionsfeld für die Sommerschule

- Auch das Thema Wireless-Integration nimmt an Brisanz zu. Getragen wird dies auch von einer starken Konsolidierung auf der Anbieterseite. Die Übernahme von Airespace durch Cisco scheint der Startschuss für eine reihenweise Übernahme von Startups oder mindestens der starken Anbindung an die Großen der Szene zu sein. Im Mittelpunkt steht die Erkenntnis, dass professionelle Wireless-Netzwerke auf Enterprise-Ebene nur in Controller-/Switch-gesteuerten Architekturen überleben können. Nur auf der Basis einer zentralen Steuerung können eine ausreichende Skalierbarkeit, sinnvoll nutzbare Frequenz- und Zelleneinteilungen und eine optimale Aussteuerung der Sendeleistung umgesetzt werden. Auch das Thema Roaming wird nur auf dieser Basis gelöst werden können. Hier hat die Offenlegung des Codes durch Trapeze sicher den Druck auf den Markt erhöht. Auch andere Ansätze sind denkbar, wenn bisher mit einer traditionellen Access-Point-Architektur gearbeitet wurde. So erzeugt der Ansatz von Airwave mit einer zentralen Management-Station für Access Points beliebiger Hersteller seit der starken Nutzung durch HP immer mehr Aufmerksamkeit (Vertrieb in Deutschland durch Netcor). WLAN-Architekturen und ihre Integration in ein übergreifendes Netzwerk-Design werden ein Kernthema der Sommerschule sein

- Auch Power-over-Ethernet war ein heißes Diskussionsthema. Hintergrund ist die Bestrebung, die Norm auf eine Leistung von 70 Watt auszudehnen. Dazu passt die Ankündigung von Cisco, dass die Backplanes der neuen Switches jetzt 30 KW-fähig sind und die neuen Netzteile 9 KW leisten. Offensichtlich muss die Frage, wozu ein Switch wirklich gebraucht wird, neu diskutiert werden (neben der Frage der Klimatisierung der Verteilerräume und der Erhitzung bestehender Verkabelungs-Infrastrukturen und Steckersysteme). Wie auch immer, die daran ansetzende Frage, ob Midspan oder nicht, bedarf einer Klärung. Für jeden, der Gigabit zum Arbeitsplatz als Ziel hat, ist Midspan keine Lösung, da die Einbringung der Phantomspannung für Gigabit in jedem Fall wieder einen Switch erfordert, vielleicht würde der Name Power-Panel bleiben, aber es wäre de facto ein Switch. Damit scheint der Weg für eine Stromversorgung aus dem Standardswitch geebnet zu sein. Auch der starke Preisverfall in diesem Bereich spricht dafür (im Endeffekt haben es die Hersteller in der Hand, immerhin ist der Mehraufwand überschaubar, Formfaktor, Leitfähigkeit der Backplane, Wärmeabfuhr und Lautstärke werden zentrale Themen sein).

Dies war nur ein kleiner Ausschnitt aus den umfangreichen und vielfältigen Diskussionen, die im Forum, in den Pausen und in der Happy Hour das Redesign Forum 2005 geprägt haben. Wie schon gesagt, wir halten diese Themen für so wichtig, dass wir sie in der Sommerschule erneut aufgreifen.

Da die Zahl der Teilnehmer an der Sommerschule stark begrenzt ist und wir in den letzten Jahren häufig Wartelisten hatten, sollten Sie hier nicht zögern, sich rechtzeitig einen Platz zu sichern.

Ihr
Dr. Jürgen Suppan

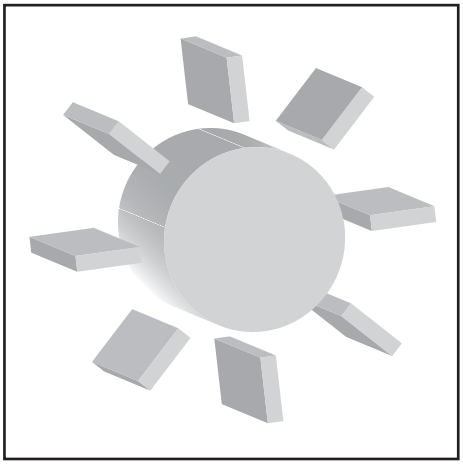
Top-Sommer-Veranstaltung

Sommerschule 2005 - Intensiv-Update auf den letzten Stand der Netzwerk-Technik Netzwerk-Design im Brennpunkt

Vom 04.-08. Juli veranstaltet die ComConsult Akademie ihre diesjährige Sommerschule in Aachen.

Netzwerke unterliegen einer permanenten Weiterentwicklung. Der aktuelle Design-Wettbewerb von ComConsult-Research, an dem sich nahezu alle führenden Hersteller beteiligten, unterstreicht dies sehr stark. Vor allem der Wunsch nach Benutzertrennung und nach kürzeren Konvergenzzeiten hat zu starken Änderungen im Backbonedesign, aber auch in den eingesetzten Verfahren geführt. Produkte haben sich entsprechend geändert. Moderne Switch-Systeme bieten einen deutlichen Zugewinn an Gestaltungsfunktionalität für leistungsstarke und sichere Netzwerke.

Die Sommerschule 2005 greift die aktuellsten Entwicklungen auf, stellt die wichtigsten Trends zur Diskussion und gibt Empfehlungen zur Weiterentwicklung und Verbesserung bestehender Netzwerke. Einige wichtige Themen in der Übersicht:



- Verändertes Campus-Design und Segmentierung
- Konvergente Netzwerke und ihre Konsequenzen
- Quality of Service als Basis einer Verkehrstrennungs-Strategie
- Ausdehnung Layer-3 bis in den Edge-Bereich
- Voice-Ready Netzwerke: was heißt das
- Sicherheit im Netzwerk und seine praktische Umsetzung: 802.1x und aufsetzende Gestaltungen
- Wireless-LAN-Architekturen und Integration
- Rechenzentren im Web und Änderungen im WAN-Design

Die Sommerschule 2005 bietet den 5-Tages-Intensiv-Update auf den letzten Stand der Netzwerk-Technik. Wir haben für Sie die aktuellen Entwicklungen analysiert, Erfahrungen aus Labor und gerade abgeschlossenen Projekten eingearbeitet und daraus eine Auswahl aus den zur Zeit anliegenden Top-Themen getroffen.

Zur Sicherstellung der Diskussionsfähigkeit und einer interaktiven Kommunikation haben wir die Teilnehmerzahl begrenzt. Zögern Sie deshalb nicht, sich schnell einen Platz in dieser herausragenden Veranstaltung zu sichern.

Montag, der 4.7.2005

Neue Netzwerk-Technologien und ihr zukünftiger Einfluss auf das Design und die Nutzung von Netzwerken
- Was sich im Bedarf ändert
- Mehr Bandbreite und ihre Verwendung
- Hierchische Architekturen
- Zonen und Sicherheits-Konzepte
- Neue Wireless-Technologien: WiMAX

Dipl.-Inform. Petra Borowka, UBN

Netzwerk-Konvergenz und seine Handhabung in der Praxis
- Herausforderung: Integration Sprache, Daten, Produktion, Logistik, Meldetechnik
- Unterschiede in den Anforderungen
- Power over LAN
- VLAN-Technologie 2005: wann und wie einsetzen
- Quality of Service
- IP-Adressierung unter Druck
- Anschluss von PC und Telefon am Arbeitsplatz
- Herausforderung Sicherheit
- Kosten

Dr.-Ing. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

Dienstag, der 5.7.2005

Netzwerk-Design im Umbruch
- LAN-Redesign
  - Neues Campus-Design
  - Senkung der Konvergenzzeiten: neue Verfahren in der Übersicht
  - Quality of Service als Basis einer Verkehrstrennung?
  - Service-Level-Betrieb
- Integration-Aufgaben und ihre strukturelle Lösung
  - WLAN-Integration
  - Voice-Integration
- Struktur und Empfehlungen für ein Redesign
  - Strukturbausteine
  - Wesentliche Design-Regeln

Dipl.-Inform. Petra Borowka, UBN

Der ComConsult Research-Design-Wettbewerb
- Vorgegebenes Szenario
- Design-Alternativen der Hersteller
- Analyse: welche Verfahren liegen im Trend
- Analyse: wie ändern sich Switch-Produkte
- Vorstellung der besten Designs und herausragender Design-Elemente
- Zusammenfassung und Bewertung
- Empfehlungen für die Teilnehmer

Dipl.-Inform. Petra Borowka, UBN

Sommerschule 2005

Mittwoch, der 6.7.2005

Rechenzentrum im Web: Funktionselemente und Umsetzung globaler Datacenter als Basis des Redesigns von Wide Area Networks

- Globale Strukturen, Daten und Dienste als zentrales Datacenter-Angebot
- Trends für die zukünftige WAN-Nutzung und ihre Auswirkungen auf das Design
- Messungen aus aktuellen Projekten
- Eigenrealisierung: wann sinnvoll, wann nicht
- Internet-VPN als Alternative zu MPLS, ATM und Frame Relay
- QoS-Angebote der Carrier
- Tipps für Ausschreibungen

Andreas Meder, ComConsult Beratung und Planung GmbH

Sicherheit im Netzwerk: Verfahren, Strategien und Konzepte

- Zugangssteuerung und Rechtezuweisung durch Einsatz von 802.1x
- Weitergehende Konzepte: Bildung virtueller Benutzergruppen
- Typische Problembeispiele und ihre Handhabung: Trennung von PC und Telefon
- Varianten der Trennung von Vertrauensbereichen: VLAN, MPLS, Virteulle Router und ACL in der vergleichenden Analyse
- Verschlüsselung Ende-zu-Ende: ist das machbar und für welche Anwendungen gilt das
- Intrusion Detection und Prevention
- Anomalie-Erkennung
- Sicherheit im WLAN und seine praxisgerechte Umsetzung

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

Donnerstag, der 7.7.2005

IP-Telefonie in der Praxis

- Migration: von alt nach neu, aber wie
- Erfahrungen aus Ausschreibungen und Migrationsprojekten
- Wie Voice-tauglich sind bestehende Netzwerke: Ergebnisse aus Einmessungen und laufenden Projekten
- Mehrpunkt-Konferenztechnik und ihre Umsetzung
- Planungsansätze
- Projekterfahrungen
- Wirtschaftlichkeit
- Voice im WAN versus Voice über öffentliche Provider-Netzwerke: welcher Weg ist sinnvoller?

Dr.-Ing. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

Produkte, Hersteller, Trends

- Alcatel, Cisco und Siemens im Vergleich
- Wohin geht der Trend
- Wo werden wir in 1 bis 3 Jahren stehen
- Wo liegen Grenzen der Entwicklung

Dipl.-Inform. Petra Borowka, UBN

Der zukünftige Mega-Standard SIP

- Struktur und Arbeitsweise von SIP
- Testbericht und Erfahrungen mit SIP-Clients und SIP-Servern
- SIP als Basis für Multimedia-Lösungen: Vision oder Realität?
- Problembereich NAT-Traversal
- Empfehlungen und Diskussion

Markus Schaub, ComConsult-Research, German-SIP-Center

Freitag, der 8.7.2005

Wireless-Networks

- Varianten
- Nutzbarkeit neuer Technologien
- Controller-based Architekturen und ihre Vorteile
- Dynamische Frequenz- und Kanalwahl
- Dynamische Steuerung der Sendeleistung
- Roaming: Stand der Technik
- Voice im WLAN: Stand der Technik und Ausblick
- Architekturen
- Produkte
- Planung und Design
- Betrieb
- Sicherheit in Netzwerken

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
Sommerschule 2005

Frühbucherrabatt bis 31.05.05

☐ Ich buche das Seminar
Sommerschule 2005
vom 04.07. - 08.07.05 in Aachen
zum Preis von € 2.015,-* zzgl. MwSt.
*gültig bis 31.05.05

(statt regulär € 2.290,- zzgl. MwSt.)

☐ Bitte reservieren Sie für mich
ein Hotelzimmer
vom_____bis_____05

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.com

Vorname	Nachname
Firma	Telefon/Fax
Straße	PLZ,Ort
eMail	Unterschrift

Sonderveranstaltung

IP-Telefonie: Markt und Produkte in der Analyse

Die Auswahl eines geeigneten Produkts für IP-Telefonie ist für jedes Unternehmen nicht leicht:

- Hersteller haben ihre Strategien, Produkte und Ankündigungen mehrfach geändert
- Produkt-Architekturen sind komplex, insbesondere in redundanten Standort-übergreifenden Situationen
- Die gleiche Komplexität betrifft die Umsetzung von Sicherheits-Konzepten, die gerade bei IP-Telefonie elementar sind
- Neue Standards wie SIP verändern Produkte und Architekturen
- Neue Funktionsbereiche wie Multipunkt-Audio und Video-Konferenzen, Kollaboration oder Präsenzbasierte Team-Funktionen erfordern die Kenntnis der zukünftigen Weiterentwicklung der Produkte

An dieser Stelle setzt diese hochaktuelle Sonderveranstaltung an, die Sie umfassend in Markt und Produkte einführt.

Sie erfahren in diesem Seminar:

- Was IP-Telefonie-Produkte leisten
- Worauf Sie bei der Auswahl achten müssen
- Wo typische Schwachstellen und Probleme liegen
- Welche Strategien ausgewählte Hersteller verfolgen

- Welche Erfahrungen ausgewählte Anwender gemacht haben

Die Veranstaltung besteht aus folgenden Teilen:

- Einführung in das Thema
- Anlagen-Architekturen, Funktionsmerkmale, Leistungsprofile
- Ergebnisse unserer großen Marktstudie
  - Alcatel
  - CISCO
  - Siemens

  In der Analyse und Bewertung, wer hat die beste Lösung für IP-Telefonie
- Vorstellung unseres Request for Information
- Stellungnahme und Präsentation der Hersteller
- Ausgewählte Anwender stellen ihre Erfahrungen mit IP-Telefonie-Installationen vor
  - Wie erfolgte die Auswahl
  - Wie hoch war der Konfigurationsaufwand
  - Wie aufwendig ist der Betrieb
  - Sind Erwartungen an Kostensenkung erfüllt worden
  - Wie zufrieden sind die Anwender
- Ergänzt wird das Programm durch Detailanalysen:
  - Die Zukunft der Siemens-Telefonie: was leistet die HiPath 8000
  - IP-Telefonie und Sicherheit: Lösungsansätze und Alternativen

Wie Sie sehen, eine herausragende Veranstaltung, die Sie auf keinen Fall versäumen sollten, wenn Sie sich für IP-Telefonie interessieren. Die Veranstaltung steht unter der Leitung von Dipl.-Inform. Petra Borowka, Unternehmensberatung Netzwerke, unter deren Leitung auch die großen Marktanalysen über Alcatel, CISCO und Siemens entstanden sind. Als Teilnehmer an der Veranstaltung können Sie diese Markt-Analysen zu einem sehr attraktiven Sonderpreis erwerben.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

IP-Telefonie: Markt und Produkte in der Analyse

☐ Ich buche das Seminar **IP-Telefonie: Markt und Produkte in der Analyse**
vom 20.06. - 22.06.05 in Bonn
zum Preis von € 1.990,- zzgl. MwSt.

☐ Bitte reservieren Sie für mich
ein Hotelzimmer
vom_____bis_____05

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.com

_____ Vorname	_____ Nachname
_____ Firma	_____ Telefon/Fax
_____ Straße	_____ PLZ,Ort
_____ eMail	_____ Unterschrift

Aktueller Kongress

ComConsult IT-Sicherheits-Forum 2005

Organisation und Technik der IT-Sicherheit mit Fachanalysen und Praxis-Workshops

Vom 06. - 09. Juni 2005 veranstaltet die ComConsult Akademie ihren Sicherheits-Kongress "ComConsult IT-Sicherheits-Forum 2005" in Königswinter.

Das Programm besteht aus Fachvorträgen unabhängiger Referenten und einer Vielzahl von Workshops mit live vorgeführten Produktvergleichen und Angriffssimulationen. Das Forum verbindet die Vermittlung aktuellen Know-hows mit der für den Tagesbetrieb benötigten Praxisrelevanz.

Der diesjährige Secuity-Kongress der ComConsult Akademie legt großen Wert auf Praxisnähe und bietet deshalb neben der notwendigen Behandlung ganz neuer Themen auch vielfältige Empfehlungen und direkt umsetzbare „Tipps und Tricks" für den Tagesbetrieb. Sie hat sich deshalb in den letzten Jahren zu einem stark besuchten Treffpunkt für alle Sicherheitsinteressierten entwickelt.

An insgesamt vier Tagen werden angeboten:

- Aktuelle Übersicht zum Stand der Sicherheitsbedrohungen
- Trends und Marktentwicklungen bei Sicherheitstechnologien
- Behandlung wichtiger Bereiche der Sicherheitsorganisation
- Moderierte Produktvergleiche mit Live-Demos
- Vertiefende Tutorien und Workshops

Der (optionale) 1. Tag hat einführenden Charakter mit insgesamt drei parallelen Seminaren, mit folgenden Themen:

- IT-Sicherheit im Überblick
  Stand und Ausblick bei wichtigen Sicherheitsthemen (Organisation und Technik)
- Sicherheit von Web-Applikationen
  Live-Hacks und Konzeption von Schutzmaßnahmen
- Information Security Management
  BS7799-1 und -2, Aufbau eines ISMS

Am 2. und 4. Tag werden durch erfahrene Referenten aktuelle fachliche Entwicklungen und Praxisbeispiele vorgestellt.

Als inhaltliche Schwerpunkte des IT-Sicherheits-Forums 2005 sind vorgesehen:

- Endpoint Security - Dezentralisierung der Schutzmaßnahmen
- Identity Management
- Security Management
- Sichere Nutzung von Webapplikationen
- Was bringt die virtuelle Poststelle?
- Sicherheitsaspekte bei Voice-over-IP
- Schutz kritischer Datenbestände
- Aufbau eines ISMS nach BS 7799
- Linux und Windows
- Security Awareness und Governance

Das IT Sicherheits-Forum zählt seit Jahren zu den herausragenden Events im diesem Bereich. Das Programm aus Fachvorträgen hersteller-unabhängiger Referenten und Workshops mit live durchgeführten Produktvergleichen hat einen hohen praktischen Wert für die Teilnehmer. Daneben werden aber auch neue Entwicklungen aufgezeigt, die sowohl Bedrohungen als auch Schutzmaßnahmen umfassen. Diese eher technischen Informationen werden ergänzt durch Empfehlungen zur Sicherheitsorganisation und zu ihrer Einbettung in interne Geschäftsabläufe, da hier nach aller Erfahrung immer noch die größten Defizite anzutreffen sind. Damit spricht das IT Sicherheits-Forum sowohl Techniker als auch Manager an.

Am 3. Tag werden in parallelen Sessions stark praxisorientierte Workshops durchgeführt. Dazu gehören moderierte Produktvergleiche (u.a. zu Application Security Gateways, Verschlüsselungslösungen, Secure Mail-Gateways, SIM-Tools, Endpoint Security) ebenso wie die gemeinsame Erarbeitung von Lösungsszenarien (u.a. für Sicherheitsorganisation, Firewallbetrieb, ISMS-Einführung).

Themen der Workshops werden sein:

- Sind SSL-VPNs aus Sicherheitssicht akzeptabel?
- Mobile Security
- Techniken der IT-Forensik
- Baukasten Identitiy Management-Schrittweise zum
- ISA Server 2004 - Ein vollwertiges Security-Gateway?
- Biometrie - Grundlagen und Praxis
- Rechtliche Aspekte der IT-Sicherheit

Moderation
Dipl.-Inform. Detlef Weidenhammer ist seit 1994 Geschäftsführer der GAI Net-Consult GmbH und hat seitdem in einer Vielzahl von Projekten national und international agierende Unternehmen bei der Konzeption von Netzwerk- und Sicherheitslösungen unterstützt. Seine fachlichen Schwerpunkte liegen in den Bereichen IT Risk Management, Security-Auditing und Security Management. Basierend auf langjähriger praktischer Tätigkeit bringt er seine Erfahrungen auch als Verfasser von Publikationen und als Referent bei Seminaren und Kongressen ein. Er leitet das jährlich stattfindende „IT-Sicherheits-Forum" und ist Herausgeber der Fachpublikation „Security Journal".

Programmübersicht - IT-Sicherheitsforum 2005

Montag, 06.06.05 Tutorien

☐ **Tutorium 1: Stand der IT-Sicherheit im Überblick (mit Live-Demos)**

- **Reale Angriffsszenarien** - Praktische Demonstration
- **Grundlagen der IT-Sicherheit** - Umgang mit Risiken, Schutzziele, Elementare Maßnahmen, Security Policy, Grundschutz, BS 7799
- **Kryptografie** - Begriffsklärung, aktuelle Sicherheitsdiskussionen
- **Von Firewall bis VPN** - Konzepte, DMZ, Betrieb, Praxis
- **Netzwerksicherheit** - W-Lans, Scans, IDS/IPS
- **Content Security** - Viren, aktive Inhalte, Spam
- **Sicherheitslösungen praktisch angewendet** - Hochverfügbarkeit, Integration

Natalie Mareth, Stefan Gora, Secorvo

☐ **Tutorium 2: Sicherheit von Webapplikationen (mit Live-Demos)**

- **Grundlagen zur Sicherheit von Webapplikationen** - Architektur, Komponenten, Protokoll
- **Live-Hacking: Angriffe auf Webapplikationen** - Techniken zur Informationsbeschaffung, Ausnutzen von Schwachstellen auf dem Webserver, Ausnutzen von Schwachstellen bei Nutzereingaben, Typische Fehler bei der Verwaltung von HTTP-Sessions, Zusammenfassung: Schwachstellen in Webapplikationen/OWASP Top 10
- **Sichere Architektur, Entwicklung und Betrieb von Webapplikationen** - Sichere Grundarchitektur, Konfigurationshinweise zu Web-, Applikations- und Datenbank-Servern, Programmierrichtlinien für Webanwendungen / Checkliste für Kaufsoftware, Sichere Authentisierung und Verschlüsselung
- **Produkte zur Sicherung von Webapplikationen** - Web Application Security Gateways, Intrusion Prevention Systeme, Live-Demo an Produktbeispielen

Frank Breitschaft, Björn Fröbe, GAI NetConsult

☐ **Tutorium 3: Praktische Einführung eines ISMS nach BS 7799**

- **Einführung** - Erfordernis eines Sicherheitsmanagements, Gesetzliche und andere externe Anforderungen (SOX, KonTraG, ISO 9001, Rating)
- **Vorstellung des BS 7799** - Historische Entwicklung, Vorstellung der Teile ISO/IEC 17799:2000 und BS 7799-2:2002
- **Abgrenzung zu anderen Standards** - Vergleich mit dem GSHB und anderen Standards, Möglichkeiten einer kombinierten Nutzung
- **Phasen des ISMS Prozesses** - Detaillierte Vorstellung der 4 Phasen
- **Schrittweise Einführung in der Praxis** - Typische Erfolgshemmnisse, Projektvorbereitung und Zeitplanung, Phasen der Einführung, Zusatznutzen durch Schnittstellen mit SOX und ISO 9001
- **Aufrechterhaltung und Erfolgskontrolle** - Reporting und Re-Audit Prozesse, Erfolgskontrolle in großen Unternehmen durch Scoring- Verfahren
- **Zertifizierung** - Nutzen einer Zertifizierung, Checkliste für ein Readiness Assessment, Ablauf der Zertifizierung

Holm Diening, GAI NetConsult

Der (optionale) 1. Tag hat einführenden Charakter mit insgesamt drei parallel stattfindenden Tutorien. Alle Tutorien starten um 10:00 Uhr und enden gegen 17:30 Uhr.
Bitte kreuzen Sie Ihr bevorzugtes Tutorium an.

11:30 - 12:00 Uhr Kaffeepause
13:00 - 14:30 Uhr Mittagspause
16:00 - 16:30 Uhr Kaffeepause

Dienstag, 07.06.05

10:00 Uhr – 10:15 Uhr
Begrüßung/Übersicht *Detlef Weidenhammer, GAI NetConsult*

10:15 Uhr – 11:00 Uhr
Sicherheit durch Kryptographie
- Darstellung wichtiger kryptographischer Mechanismen / Algorithmen
- Probleme durch kurze Schlüssellängen und schwache Algorithmen
- Angriffsziele: schwache Zufallszahlengeneratoren und Implementierungsschwächen
- Resümee und Ausblicke

Dr. Werner Schindler, BSI

11:00 Uhr – 11:45 Uhr
Enterprise Security Management - gibt es das schon?
- Bestandteile eines ESM - Theorie und Wirklichkeit
- Point-Solutions vs integrierte Lösungen
- Funktionen des Security Information Managements (SIM)
- Übersicht zu SIM-Tools

Detlef Weidenhammer, GAI NetConsult

12:15 Uhr – 13:00 Uhr
Identity Management - Informationssicherheit als Wertschöpfer?
- Informationssicherheit im Wandel
- Bausteine einer Identity Management Lösung
- Federated Identity Management
- Wertschöpfung und Umsetzung

Derk Fischer, PricewaterhouseCoopers

14:30 Uhr – 15:15 Uhr
Aktueller Stand der Biometrie
- Vorstellung der heute relevanten Verfahren
- Sicherheitsgewinn durch Biometrie?
- Bewertung der eingesetzten Techniken
- Absehbare Entwicklungen im öffentlichen und industriellen Bereich

Henning Daum, Fraunhofer IGD

15:15 Uhr – 16:00 Uhr
Aufbau einer sicherern Lösung für Telearbeit / Small Offices
- Motivation und Anforderungen
- Lösungskonzept mit VPN, SSO und Citrix MetaFrame
- Erfahrungen bei der Realisierung
- Fazit zu Sicherheitsgewinn und Kostenoptimierung

Alfred Dauven, BEV

16:30 Uhr – 17:15 Uhr
Durchführung forensischer Untersuchungen
- Definitionen und Einsatzgebiete
- Was ist unbedingt zu beachten?
- Herangehensweise und unterstützende Tools
- Zusatznutzen durch digitale Forensik

Manfred Hatzesberger, Security Consultant

17:15 - 18:00 Uhr
BSI-Grundschutz und ITIL - (k)ein Widerspruch in der Praxis?!
- ITIL und BSI-Grundschutz - zwei wichtige de facto-Standards für die IT-Praxis
- Projektbeispiel: eine BSI-Grundschutz-Forderung nach ITIL lösen
- Projektbeispiel: in ITIL-Prozessen BSI-Grundschutz berücksichtigen
- Resümee: ITIL und BSI-Grundschutz ohne Mehrfachaufwand-Stratgeie

Dipl.-Infom. Oliver Flüs, ComConsult Beratung und Planung

11:45 - 12:15 Uhr Kaffeepause
13:00 - 14:30 Uhr Mittagspause
16:00 - 16:30 Uhr Kaffeepause
ab 18:30 Uhr Happy Hour

Mittwoch, 08.06.05 Praxis-Workshops - Die Durchführung der Workshops wird am Teilnehmerinteresse ausgerichtet.

9:00 Uhr – 12:30 Uhr

Workshop 1:
Sind SSL-VPNs aus Sicherheitssicht akzeptabel?

Workshop 2:
Mobile Security

Workshop 3:
Techniken der IT-Forensik

Workshop 4:
Baukasten Identitiy Management - Schrittweise zum Erfolg

14:00 Uhr - 17:30 Uhr

Workshop 1:
Sind SSL-VPNs aus Sicherheitssicht akzeptabel?

Workshop 5:
ISA Server 2004 - Ein vollwertiges Security-Gateway?

Workshop 6:
Biometrie - Grundlagen und Praxis

Workshop 7:
Rechtliche Aspekte der IT-Sicherheit

Bitte wählen Sie zwei der aufgeführten Workshops auf der Folgeseite aus.

11:00 - 11:30 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause
16:00 - 16:30 Uhr Kaffeepause

Donnerstag, 09.06.05

9:00 Uhr – 10:00 Uhr
BS7799 - Auf dem Weg zum Zertifikat - Ein Praxisbericht
- Das Zertifikat: Der Weg das Ziel !?“
- Risiko Management: Wieviel darf oder muss es sein?
- Tools: ja oder nein?
- Lessons learned

Jörg Völker, Secorvo

10:00 Uhr – 11:00 Uhr
VoIP-Security in der Praxis
- Stand der Verschlüsselung von Sprachverkehr: Standards und Produkte
- Firewall-Regeln und Firewall-Konfiguration für Voice
- Argumente für und gegen VLAN-Trennung bei VoIP
- Quality of Service für Voice und Theft of Service aus Security-Sicht

Dr. Behrooz Moayeri, ComConsult Beratung und Planung

11:30 Uhr – 12:30 Uhr
Datenbank-Sicherheit
- Schwachstellen und Angriffsmöglichkeiten bei Datenbanken
- Auditierung von Datenbanken
- Sicherheitsmechanismen für Datenbanken

Stefan Middendorf, Cirosec

13:45 Uhr – 14:30 Uhr
Sichere E-Mail-Kommunikation in Unternehmen
- Bedrohungen und Gegenmaßnahmen bei Nutzung von E-Mail
- Probleme und Gefahren bei Verschlüsselung mit Outlook & Co.
- Vor- und Nachteile zentraler Lösungen in typischen Einsatzszenarien
- Überblick zu verfügbaren Lösungen

Dr. Torsten Johr, GAI NetConsult

14:30 Uhr – 15:15 Uhr
Rechtliche Aspekte der E-Mail-Sicherheit
- Virenhaftung / Spamhaftung
- Aufbewahrungspflichten und Überwachung
- Beweisrecht
- Signaturen und Verschlüsselung

Ulrich Emmert, esb Rechtsanwälte

15:15 Uhr – 16:00 Uhr
Neue Technische Richtlinie des BSI: Sicheres WLAN
- Darstellung und Bewertung der Sicherheitsmechanismen
- Vorgaben eines WLAN-Sicherheitskonzeptes
- Auswahlkriterien für WLAN-Systeme
- Prüfkriterien für WLAN-Systeme

Dr. Simon Hoff, ComConsult Beratung und Planung

11:00 - 11:30 Uhr Kaffeepause
12:30 - 13:45 Uhr Mittagspause
16:00 Uhr Ende der Veranstaltung

ComConsult IT-Sicherheitsforum 2005

Praxis-Workshops

9:00 - 12:30 Uhr

Workshop 1: Sind SSL-VPNs aus Sicherheitssicht akzeptabel?
Live-Demo von Angriffsszenarien und Schutzmöglichkeiten
- SSL-VPNs als Zugang zu Webanwendungen, als Remote GUI und IPsec-Ersatz
- Funktionsweise und Sicherheitsbetrachtung der verschiedenen Zugangslevel
- Wie kann die Nutzung von fremden Clients (Internetcafé) aus gesichert werden?

Frank Breitschaft, Björn Fröbe, GAI NetConsult

Workshop 2: Mobile Security
Live-Demo
- Einsatz-Szenarien und mögliche Sicherheitsprobleme
- Typische Sicherheitsmängel
- Rechtliche Aspekte (e.g. Haftungsfragen)
- Technische und organisatorische Maßnahmen
- Überblick zu Sicherheits-Tools
- Bestandteile und Beispiel einer PDA-Policy

Enno Rey, ERNW

Workshop 3: Techniken der IT-Forensik
Live-Demo mit Forensik-Tools
- Produktübersicht zu Analyse-Tools
- Betriebssysteme und Forensik
- Hashes MD5 vs. SHA-1
- Live-Forensik mit EnCase
- Weitergabe nützlicher Adressen

Manfred Hatzesberger, Security Consultant

Workshop 4: Baukasten Identitiy Management - Schrittweise zum Erfolg
Live-Demons auf Basis einer Laborimplementierung
- Grundlagen schaffen: Verzeichnisdienste als Basis einer offenen Lösung
- Wer bin ich und was darf ich: Authentisierung und Zugriffskontrolle
- Auf dem Weg zur Selbstverwaltung: Anforderungen an die Benutzerverwaltung
- Demonstration einzelner Funktionen
- Roadmap-Prototyp für ein IdM-Projekt

Derk Fischer. PricewaterhouseCoopers

Änderung im Programm und Schreib-/Druckfehler behält sich der Veranstalter vor!

14:00 - 17:30 Uhr

Workshop 1: Sind SSL-VPNs aus Sicherheitssicht akzeptabel?
Live-Demo von Angriffsszenarien und Schutzmöglichkeiten
- SSL-VPNs als Zugang zu Webanwendungen, als Remote GUI und IPsec-Ersatz
- Funktionsweise und Sicherheitsbetrachtung der verschiedenen Zugangslevel
- Wie kann die Nutzung von fremden Clients (Internetcafé) aus gesichert werden?

Frank Breitschaft, Björn Fröbe, GAI NetConsult

Workshop 5: ISA Server 2004 - Ein vollwertiges Security-Gateway?
Referenzumgebung zur Veranschaulichung
- Kurzüberblick über die MS Sicherheitsprodukte und Strategien
- ISA Server 2004 - Funktionen und Einsatzgebiete
- VPN Netze mit ISA Server 2004
- DMZ Konfigurationen mit ISA Server 2004
- Integration in Verzeichnissysteme
- Authentisierung und EAP Möglichkeiten
- Beispiele für sinnvolle Einsatzgebiete und Netzwerkintegration
- Vergleich mit „etablierten" Security-Lösungen

Jens Lorenz, Guido Alexius, Döres AG

Workshop 6: Biometrie - Grundlagen und Praxis
Live-Demo
- Vorstellung von Fingerbild, Gesichts- und Iriserkennung
- Live-Demos ausgewählter Verfahren
- Algorithmen und ihre Stärken/Schwächen
- Ergebnisse von Tests zur Überwindungssicherheit
- Anwendungsszenarien und bisherige praktische Erfahrungen

Henning Daum, Fraunhofer IGD

Workshop 7: Rechtliche Aspekte der IT-Sicherheit
Erarbeitung von Betriebsvereinbarungen zu Datenschutz und Datensicherheit
- Sicherheit und Recht
- Datenschutzrechtliche Organisationspflichten
- Rechtliche Grenzen der Mitarbeiterüberwachung
- Rechtssicherer Einsatz der Technik
- Umsetzung von Organisationsrichtlinien
- Haftungsfragen bei illegalen Inhalten, Links oder Hackerangriffen

Ulrich Emmert, esb Rechtsanwälte

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
IT-Sicherheits-Forum 2005

Ich buche den Kongress
ComConsult IT-Sicherheits-Forum 2005
vom 06.06. - 09.06.05 in Königswinter
Preis: € 1.990,- zzgl. MwSt. mit Tutorium -
€ 1.690,- zzgl. MwSt. ohne Tutorium

☐ **mit Tutorium € 1.990,- zzgl. MwSt.**

☐ Thema 1: Stand der IT-Sicherheit im Überblick

☐ Thema 2: Sicherheit von Webapplikationen

☐ Thema 3: Praktische Einführung eines ISMS nach BS 7799

☐ **ohne Tutorium € 1.690,- zzgl. MwSt.**

☐ Bitte reservieren Sie für mich ein Hotelzimmer
vom_____bis_____05

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.com

Bitte wählen Sie auch vorab zwei Workshopthemen aus:

vormittag

☐ Workshop 1: Sind SSL-VPNs aus Sicherheitssicht akzeptabel?

☐ Workshop 2: Mobile Security

☐ Workshop 3: Techniken der IT-Forensik

☐ Workshop 4: Baukasten Identitiy Management - Schrittweise zum Erfolg

nachmittag

☐ Workshop 1: Sind SSL-VPNs aus Sicherheitssicht akzeptabel?

☐ Workshop 5: ISA Server 2004 - Ein vollwertiges Security-Gateway?

☐ Workshop 6: Biometrie - Grundlagen und Praxis

☐ Workshop 7: Rechtliche Aspekte der IT-Sicherheit

_____ Vorname

_____ Nachname

_____ Firma

_____ Telefon/Fax

_____ Straße

_____ PLZ,Ort

_____ eMail

_____ Unterschrift

Zweitthema

IEEE 802.11n : der große MIMO-Bluff und ernst zu nehmende Alternativen

Fortsetzung von Seite 1

Dr. Franz-Joachim Kauffels ist einer der erfahrensten und bekanntesten Referenten der gesamten Netzwerkszene (über 20 Fachbücher und unzählige Artikel) und bekannt für lebendige und mitreißende Seminare.

Dauerhaft werden WLANs mit einer nominalen Zellen-Datenrate von 54 Mbit/s. nicht das Ende der Entwicklung darstellen. Die Standardisierungsgruppe IEEE 802.11n ist aus der früheren High Speed Study Group hervorgegangen und kümmert sich um die Definition von Standards für WLANs mit einer nominalen Zellen-Datenrate von mindestens 100 Mbit/s. Dies ist jedoch kein besonders großer Schritt. Ein angemessener Fortschritt würde m. E. erst erzielt, wenn die nominale Zellen-Datenrate auf mindestens 500 Mbit/s erhöht würde. In der Vergangenheit hat sich ja bei Ethernet eine Vorgehensweise in Zehnerpotenzen auch bestens bewährt.

Eine nachrichtentechnisch sinnvolle Lösung ist durchaus möglich und wir werden weiter unten im Artikel darstellen, wie so etwas aussehen kann. Allerdings ist die Entwicklung auch etwas aufwändig und die ursprüngliche Timeline von IEEE 802.11n wird sicherlich nicht eingehalten werden können. IEEE 802.11n ist aber offensichtlich in einer Art Zugzwang, vor allem weil zwei Herstellergruppierungen das Standardisierungsgremium als Werbeplattform benutzen.

In Ermangelung einer stabilen Technologie, die einen wirklichen Durchbruch im Sinne der Erzielung einer echten Steigerung der nominalen Zellen-Datenrate unterstützen könnte, bewegt man sich mit dem Stichwort „MIMO“ im Bereich von ca. 100 - 130 Mbit/s und liefert sich Marketingschlachten, die, wenn es für uns alle gut ausgeht, zur Paralysierung der Arbeitsgruppe führen könnten. Im Rahmen der Paralysierung der Arbeitsgruppe hätten diejenigen eine Chance, die einen wirklichen Schritt vollziehen möchten. Würden sich die aktuellen Herstellergruppierungen zusammentun oder sich eine von ihnen durchsetzen, bekämen wir unter dem Namen IEEE 802.11n einen echten Schrottstandard, der in Folge zu Verwirrung und ernsthaften Problemen in der Planung professioneller Campus-WLANs führen könnte.

Wir befassen uns in diesem Artikel zunächst mit dem generellen Entwicklungshintergrund. Danach kommen wir zu den ominösen MIMO-Geschichten. Allerdings ist dieser Autor nicht zufrieden damit, lediglich einen schwachen Zwischenstand einer an und für sich faszinierenden Entwicklung aufzuzeigen. Deshalb werden nach einer didaktisch völlig neuen Aufarbeitung der notwendigen nachrichtentechnischen Grundlagen Wege aufgezeigt, die zu wirklich professionellen und stabilen Lösungen für schnelle WLAN-Zellen führen können.

1. Entwicklungshintergrund

Bei der Planung von benachbarten Funkzellen für eine professionelle Flächendeckung mit vielen Teilnehmern wird man feststellen, dass es erhebliche Unterschiede zwischen dem 2,4 und 5 GHz Band gibt, die einfach in der physikalischen Wellenausbreitung begründet sind. Ein Zellendesign, welches bei IEEE 802.11b gut funktioniert, kann man deshalb nicht ohne weiteres für die schnellere Version IEEE 802.11a bzw. die „EU-Variante“ IEEE 802.11h verwenden, weshalb viele zunächst auf IEEE 802.11g ausweichen werden, was aber kurzsichtig ist, weil IEEE 802.11g mehr Porbleme schafft als löst. Insbesondere der Mischbetrieb von 11b und 11g bringt, wie Messungen gezeigt haben, erhebliche Nachteile mit sich. Es gibt Hersteller, die momentan Access Points anpreisen, deren Radioteile auswechselbar sind, aber wir werden ja sehen, wie weit man damit kommt, ganz abgesehen davon, dass jede physische Auswechslung von Radioteilen Kosten nach sich zieht, die das Konzept m.E. ad absurdum führen.

Die Frage, die sich natürlich brennend stellt, ist, ob eine Erhöhung der Übertragungsleistung in einer Zelle zwangsläufig wiederum mit einem neuen Zellendesign zwingend einher geht. Die Antwort der HTSG ist eindeutig: NEIN. Das Zellendesign nach IEEE 802.11a kann weiter benutzt werden.

Der Standard IEEE 802.11h erweitert IEEE 802.11a lediglich um Zusatzfunktionen, die die Kompatibilität zu in Europa bestehenden Funksystemen sichern. Nachrichtentechnisch gesehen gibt es aber aus der Perspektive des eigentlichen Übertragungsverfahrens keine Unterschiede zwischen diesen beiden Varianten. Die HTSG nimmt daher keine weiteren Differenzierungen vor und bezieht sich immer auf IEEE 802.11a. Das wollen wir hier auch so halten. Es wird sicherlich auch für die HTSG-Verfahren, wenn sie einmal standardisiert sind, einen europäischen Ableger geben, der dann wieder diese Zusatzfunktionen aufweist. Welche Buchstaben hierfür vergeben werden, kann man zu diesem frühen Zeitpunkt noch nicht absehen.

Momentan sind Systeme nach IEEE 802.11 b dominierend. Große Vermarktungskampagnen, z.B. Intel Centrino, haben dazu beigetragen. IEEE 802.11b hat deutliche Designlücken, am bekanntesten sind die auf dem Bereich der Sicherheit. Viel schlimmer ist jedoch, dass besonders interessante Anwendungen wie WLAN-VoIP nur schlecht oder gar nicht machbar sind, weil die geringe Nutzdatenrate dauerhaft nicht tragbar ist.

Systeme nach IEEE 802.11a mit 54 Mbit/s waren in Europa problematisch wegen Interferenzen im 5 GHz-Band. Dieser Konf-

likt konnte durch IEEE 802.11h durch folgende Maßnahmen gelöst werden:

- Interferenzvermeidung durch dynamische Kanalwahl und/oder Reduktion der Sendeleistung gemäß den
- ITU „Radio Regulations“ auf World Radiocommunications Conference 2003

Dies schafft

- Konformität zu Earth Exploration Satellite Service EESS
- Konformität zu Space Research Service SRS
- Konformität zu anderen, z.B. militärischen Radarsystemen

IEEE 802.11 b arbeitet mit „normaler“ Funktechnik. Diese setzt ein Signal mittels übersichtlicher Modulation auf eine Trägerschwingung. Die Datenrate lässt sich so aber nicht mehr wesentlich steigern, wenn man die Randbedingungen, z.B. FCC-Regulierungen, nicht ändert. IEEE 802.11 a arbeitet mit OFDM, Orthogonal Frequency Division Multiplex. Dieses wird zwar als Modulationsverfahren ein bezeichnet, ist aber streng genommen ein Verfahren zur Erzeugung synthetischer Signale. Die HTSG von IEEE 802.11 (Higher Througput Study Group) untersuchte Möglichkeiten für WLANs mit mehr als 100 Mbps in der Funkzelle. Die HTSG hat mittlerweile den Gruppennamen IEEE 802.11n und hat sich schon sehr früh auf Konformität zu IEEE 802.11a und auf den 5 GHz-Bereich festgelegt.

Diese Festlegungen bedeuten, dass man versuchen möchte, mehr Netto-Übertragungsleistung aus dem bestehenden OFDM-Funksystem herauszuholen. Wie man das machen kann, sehen wir noch.

Diese Festlegungen bedeuten aber vor allem:

- 802.11n-Systeme sind nach außen hin völlig konform zu allen Bestimmungen nach IEEE 802.11a und IEEE 802.11h
- 802.11n-Funkzellen können genauso designt werden wie IEEE 802.11a Funkzellen
- 802.11n-Funkzellen arbeiten im Rahmen der IEEE 802.11a Spektralmaske

Das kann für die Planung gar nicht hoch genug bewertet werden, denn

- IEEE 802.11a-Funkzellen können zu jedem späteren Zeitpunkt zu 802.11n-Funkzellen aufgerüstet werden
- Funktionen wie die automatische Kanalwahl und die automatische Leistungsanpassung werden in beiden Sorten Zellen arbeiten
- IEEE 802.11a-Funkzellen und 802.11n-Funkzellen können in einem Umfeld, z.B. Bürohaus, zusammen betrieben werden und stören sich nicht
- Wie man IEEE 802.11 einschätzen kann, wird es noch ein System zur automatischen Ratenanpassung geben. Dann können IEEE 802.11a Endgeräte in 802.11n-Zellen betrieben werden, allerdings mit max. 54 Mbps
- IEEE 802.11a und 802.11n bilden dann ein harmonisches zweistufiges Werk, wie wir es schon von 100 Mbps Ethernet und Gigabit Ethernet kennen

IEEE 802.11b Systeme haben in diesem Umfeld allerdings nicht direkt etwas verloren, aber: IEEE 802.11b-Systeme arbeiten im 2,4 GHz-Band, IEEE 802.11a und 802.11n-Systeme arbeiten im 5 GHz-Band. Die Systeme stören sich technisch nicht. Durch ein entsprechendes Distribution System könnten sie miteinander verbunden werden, wenn man das möchte. Dadurch entsteht eine dreistufige Hierarchie:

- IEEE 802.11b mit 11 Mbps pro Zelle
- IEEE 802.11a/h mit 54 Mbps pro Zelle
- IEEE 802.11n mit bis zu 320 Mbps pro Zelle und mehr

Intelligent installiert, kann man alle drei Systemarten gleichzeitig nutzen.

Problematisch ist zur Zeit aber besonders, dass voreilige Marketingstrategen dabei sind, die wichtigen und gut durchdachten Ziele, die insbesondere der Konformität der Systeme untereinander dienen und wesentlicher Bestandteil eines jeden Investitionsschutzes sind, ganz oder teilweise zu kippen oder mit Füßen zu treten !

Und das geschieht unter dem Stichwort „MIMO“!!

2. MIMO - der große Bluff

An und für sich kommt die MIMO-Antennentechnologie aus dem Umfeld der Systeme im Millimeterwellenbereich. Dort ist sie auch notwendig und sinnvoll. Verschiedene Protagonisten versuchen allerdings z. Zt., den Ansatz für die Zwecke eines 100+ Mbit/s. Schnellschusses zu verbiegen, schaffen dabei nachrichtentechnisch verwerfliche Lösungen, die im Heimbereich vielleicht noch erträglich sind, in einer professionellen Umgebung aber keinesfalls.

2.1 Der Ursprung von MIMO

Die Bezeichnung MIMO steht für Multiple Input Multiple Output und stammt aus der Entwicklung integrierter Schaltkreise, besonders hybrider Schaltkreise. Dort bedeutet sie, dass ein Schaltkreis Signale von mehreren Eingängen entgegennimmt, im Gegensatz zum Schaltnetz oder Schaltwerk boolescher Prägung korreliert verarbeitet und das Ergebnis schließlich auf mehreren Ausgängen bereitstellt. MIMO-Schaltungen sind besonders in der komplexen Codierung vorteilhaft und bezogen auf die Netzwerke z.B. die Grundlage für die Entwicklung von komplexen Schaltkreisen wie man sie für die Signalaufbereitung bei 10 GBASE-T benötigt.

Im Zusammenhang mit Funktechnologie wird der Begriff MIMO eigentlich erst im Millimeterwellenbereich, also ab ca. 50 GHz, verwendet. Hier gibt es sog. Beam Shaped MIMO-Antennen. Im Millimeterwellenbereich besteht wegen der kürzeren

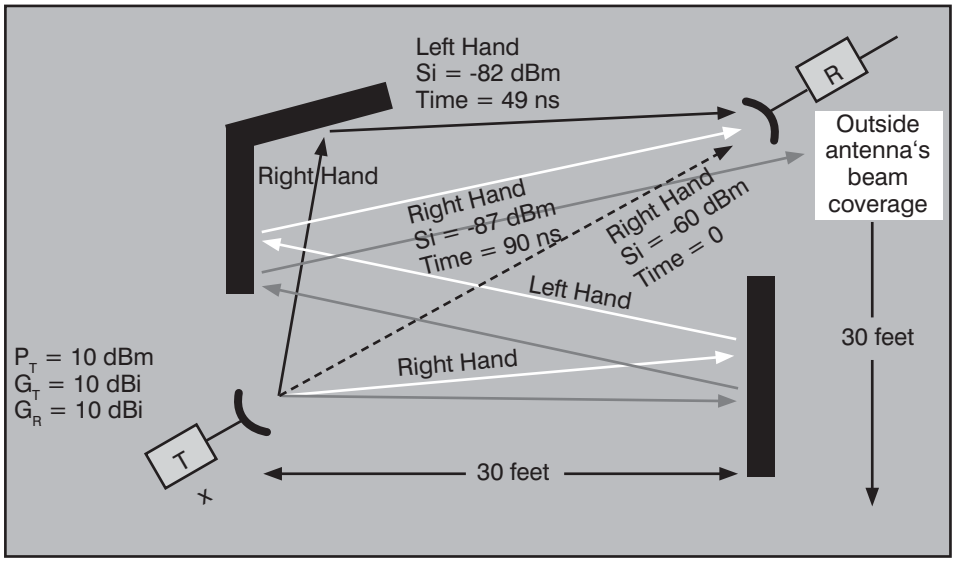


Abb. 2.1: Multipath Effekte bei ca. 50 GHz

Wellenlängen das Problem des Multipath Fadings in völlig anderer Größenordnung als bei den heute bekannten WLANs. Um überhaupt eine sinnvolle Übertragung aufsetzen zu können, benötigt man Antennen mit einer recht starken Richtwirkung. Auch diese erzeugen noch Multipath Fading, aber durch die Richtwirkung wenigstens mit einer begrenzten Anzahl primärer Signalwege recht hoher Intensität und einer hohen Anzahl sekundärer Signalwege mit geringer Intensität, die man dann wegfiltern kann. Je nach Anspruch reicht dies aber immer noch nicht aus, sondern muss mit Antennen Diversity kombiniert werden. Das kennen wir ja schon von den „normalen“ WLANs. Es werden mehrere (meist zwei) Antennen verwendet, die gleichartig ein Signal abstrahlen. Dabei wird es durch die Umgebungsbedingungen zu Signalen kommen, die relativ direkt mit relativ hoher Intensität auf dem Empfänger einstrahlen und solche, deren Intensität geringer ist oder die durch längere Wege und Reflexionen verzögert sind. Der Empfänger „nimmt“ sich dann einfach das stärkste und beste Signal heraus.

Antennen Diversity funktioniert gut und problemlos, generell ist es bei WLANs aber völlig ausreichend, wenn ein Access Point mehrere Antennen hat. Man kann auch einem Empfänger mehrere Antennen und einen entsprechenden nachgelagerten Schaltkreis geben. Die Leistungssteigerung ist aber in diesem Fall so gering, dass sich der Aufwand nicht lohnt und auch dem allgemein gewünschten mobilen Umgang mit den Endgeräten widerspricht. Bei WLANs kann das Antennen Diversity über das Management des Funkteils beeinflusst werden. Davon macht man allerdings so gut wie keinen Gebrauch, sondern läßt es automatisch laufen.

Zurück zu den Millimeterwellen. Hier muss man die MIMO-Richtantennen und dynamisches Antennen Diversity kombinieren, vor allem wenn man eine flächige Ausleuchtung erreichen möchte. Das scheint zunächst ein Widerspruch zu sein, aber man muß mehrere Richtantennen mit nicht allzu hoher Richtwirkung so kombinieren, dass sie eine zusammenhängende Fläche ausleuchten. Durch die Richtantennen wird wie zuvor beschrieben das Multipath Fading eingedämmt und durch das Antennen Diversity letztlich mittelbar die Fläche abgedeckt.

Sinnvollerweise beschickt man alle Antennen mit dem gleichen Sendesignal. Auf der Empfängerseite kann man dann auch mehrere Antennen anbringen, muss aber nicht. Im Gegensatz zu normalen WLANs steigert man aber damit die mögliche Leistung

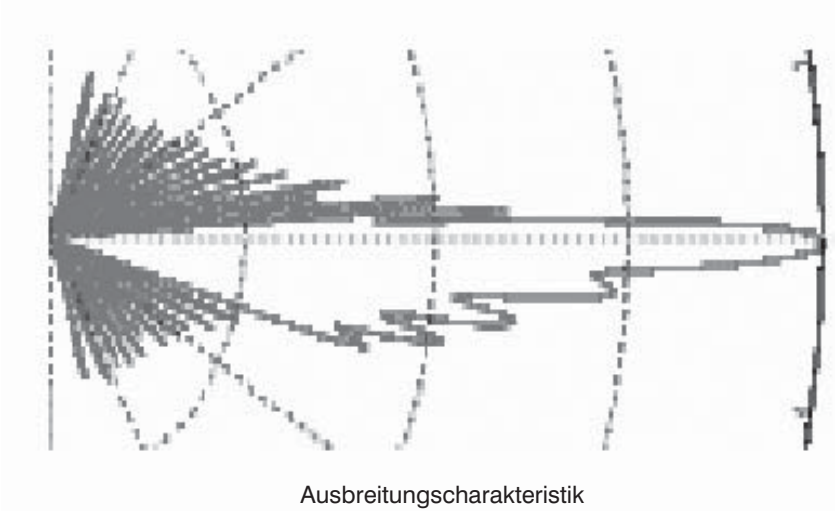


Abb. 2.2: 50 GHz Beam Shaped MIMO Antenne

deutlich. Die Ansammlung aus mehreren Sende- und Empfangsantennen hat dem ganzen den Namen MIMO eingebracht.

„Was für 50 GHz gilt, kann ja für 5 GHz nicht völlig falsch sein“ haben sich offensichtlich die IEEE 802.11n MIMO-Protagonisten gedacht und eine zunächst einmal ähnliche Grundstruktur vorgeschlagen.

Zweifellos hat eine solche Anordnung bei ansonsten nicht geänderten Radiochips genau einen Vorteil und genau einen Nachteil. Der Nachteil ist, dass man mehr Antennen und ein ganz kleines bisschen zusätzliche Elektronik benötigt, der Vorteil ist eine gegenüber einer einfachen Lösung gesteigerte Reichweite.

Das kann man sofort einfach bewerten. Alle heutigen seriösen Planungen für flächendeckende Campus WLANs gehen von kleinen WLAN-Zellen aus, weil die Zelle ein Shared Medium ist und niemand etwas davon hat, wenn im Rahmen einer großen Reichweite möglichst viele Stationen in Wettbewerb um das gemeinsam wechselseitig ausgeschlossen nutzba-

re Medium streiten. Eine größere Reichweite ist allenfalls in Sonderfällen und im Heimbereich nutzbar, allerdings auch nur für diejenigen, die ein hinreichend ausgedehntes Heim haben.

Aber damit nicht genug, man möchte ja eine Steigerung der nominalen Zellen-Datenrate erreichen. Und da beginnt das Problem.

2.2 Die Protagonisten

Es gibt zwei klingende Namen von Konsortien, die IEEE 802.11n vereinnahmen wollen, das sog. World Wide Spectrum Efficiency Konsortium WWiSE und die sog. Task Group N Synch TGNSync. Wow, das sind Hammer-Namen. Der erste hört sich so an, als würde sie die weltweite Spektraleffizienz erhöhen, womit natürlich der durchschnittliche Media-Markt Kunde viel anzufangen weiß, die zweite Gruppe richtet sich offensichtlich an eine jüngere Kundschaft und ist eine Kampftruppe zur Wiederbelebung einer Boy Group. Kommt sicher ganz toll an. Außer bei mir.

Hinter den Spektralverbesserern stecken Motorola, Broadcom und Texas Instruments, während die Boy Group von Intel und Nokia unterstützt wird, allesamt Firmen, die abgesehen vom Chipgeschäft hauptsächlich auf den Comsumer Markt zielen, weil der so schön riesig ist.

Sie liefern sich momentan schwere Grabenkämpfe innerhalb von IEEE 802.11n. Damit sich ein Vorschlag durchsetzen kann, sind 75% der Stimmen nötig. In der Abstimmung vom 14.3.2005 haben es die Boygroup-Wiedererwecker auf 54%, die anderen nur auf 46% der Stimmen gebracht, beides hat glücklicherweise nicht gereicht.

Beide setzen auf das MIMO-Verfahren, welches „dank mehrerer Antennen einen parallelen mehrfachen Datenstrom zwischen WLAN-Access Point und Client ermöglicht“. Und da ist der Hund begraben, so wie das in der Pressearbeit dargestellt wird, kann es nämlich nicht funktionieren, wie wir weiter unten darstellen werden. Ein ominöses Verfahren namens Path Diversity soll dafür sorgen, dass es trotzdem klappt.

Ganz klein wird dann noch erwähnt, dass man mit 20 bzw. 40 MHz breiten Bändern arbeiten möchte. Aha, wir verabschieden uns also von einem der wichtigsten Ziele die es bisher bei IEEE 802.11n gab, der Konformität zur IEEE 802.11a/h Spektralmaske. Dann kann man natürlich schnell und leicht mehr übertragen, z.B. 135 Mbit/s. Aber gleichzeitig zerstört man jede Art von Konformität und Interoperabilität zu bestehenden Funknetzen im 5 GHz Band komplett, und zwar nicht ein wenig, sondern man haut direkt mit dem Hammer drauf.

Der Kampf zwischen den beiden Gruppen ist deshalb so ausgeprägt, weil sie beide die gleiche zu nichts Sinnvollem passende technische Basis verwenden wollen, und sich lediglich im Grad der Ominösität des Path Diversity Verfahrens unterscheiden. Um den Blick davon abzulenken, dass das Ganze an und für sich unbrauchbar und eine echte Vergackeierung der potenziellen Kunden ist, bezichtigt jeder den anderen, ein unpraktikables Verfahren anzuwenden. Ich könnte diese Differenzen hier noch ausführlicher darstellen, aber das führt an dieser Stelle nicht weiter, weil es mein Ziel ist, die Unbrauchbarkeit beider Alternativen zusammen darzustellen.

2.3 Bandbreite und Nachrichtenwürfelchen

Bevor wir weiter diskutieren, möchte ich den Blick des interessierten Lesers auf eines meiner ältesten Bilder lenken. Das schleppe ich schon über 25 Jahre durch Seminare und Vorträge: das Bild mit dem Übertragungsfenster. Offensichtlich ist es immer noch nicht überall angekommen, so habe ich mir als didaktisches Hilfsmittel die Nachrichtenwürfelchen ausgedacht.

Die Informationsmenge kann man sich als Quader vorstellen, dessen Kantenlängen durch die Grundfrequenz, die Übertragungsdauer als Reziprok der Übertragungsgeschwindigkeit und den Logarithmus Dezimalis des Quadrats der Mächtigkeit der Menge des Symbolvorrats bestimmt sind. Baut man ein Übertragungssystem auf, besteht die Hauptaufgabe darin, den Quader solange umzuformen, dass er durch das Übertragungsfenster passt. Das Übertragungsfenster ist durch seine Bandbreite und den Logarithmus Dezimalis von 1 + Signal-zu-Rausch-Verhältnis bestimmt. Wird die zur Verfügung stehende Bandbreite größer, wird es breiter, bei gleichem Signal-zu-Rausch-Verhältnis passt dann auch mehr durch. Wird das Signal-zu-Rausch-Verhältnis bei bestehender Bandbreite kleiner, so geht das Fenster immer weiter zu.

Das Übertragungsfenster ist immer vorgegeben. Bei Verkabelungssystemen ist es durch die maximale Bandbreite des Kabels und der Stecker, Patchfelder usf. definiert, was ja letztlich zu den bekannten genormten Verkabelungsklassen geführt hat, während der Einfluss des Signal-zu-Rausch-Verhältnisses über weite Bereiche völlig unbedeutend ist.

Bei drahtlosen Übertragungssystemen ist das anders. Hier gibt normalerweise die Regulierung oder eine Standardisierungsorganisation die innerhalb eines Frequenzbereiches für einen Kanal zur Verfügung stehende Nutz-Bandbreite vor. Bei jeder Übertragung entstehen durch Unschärfen in den Senderschaltkreisen auch Signale neben dem eigentlichen Nutzsignal. Deren maximale relative Ausprägung wird relativ zur Stärke des Nutzsignals in Dezibel ausgedrückt und ebenfalls durch Vorgaben beschränkt. So entsteht eine Spektralmaske.

Man sieht in der Abbildung 2.5, dass für Systeme nach IEEE 802.11a/h eine Spektralmaske vorgesehen ist, die ein 20 MHz breites nutzbares Übertragungsband links und rechts einer Mittenfrequenz fc definiert, und zwar mit einer möglichen Abweichung von 2 MHz oder 10%. Diese Abweichung kann durch thermische Effekte auftreten und muss berücksichtigt werden. Links und rechts davon muss das Signal stark abfallen, und zwar um mindestens 28 dB relativ bei 9 MHz mehr oder weniger und um mindestens 40 dB relativ bei 19 MHz mehr oder weniger.

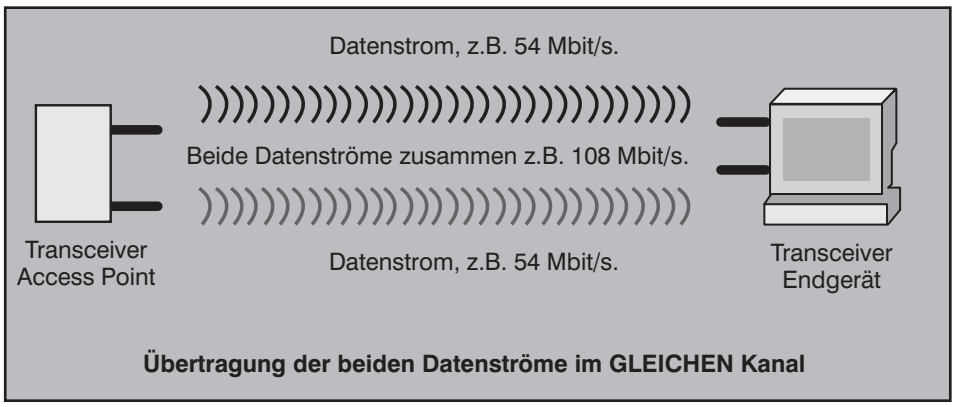


Abb. 2.3: WLAN-MIMO-Grundidee

IEEE 802.11n : der große MIMO-Bluff und ernst zu nehmende Alternativen

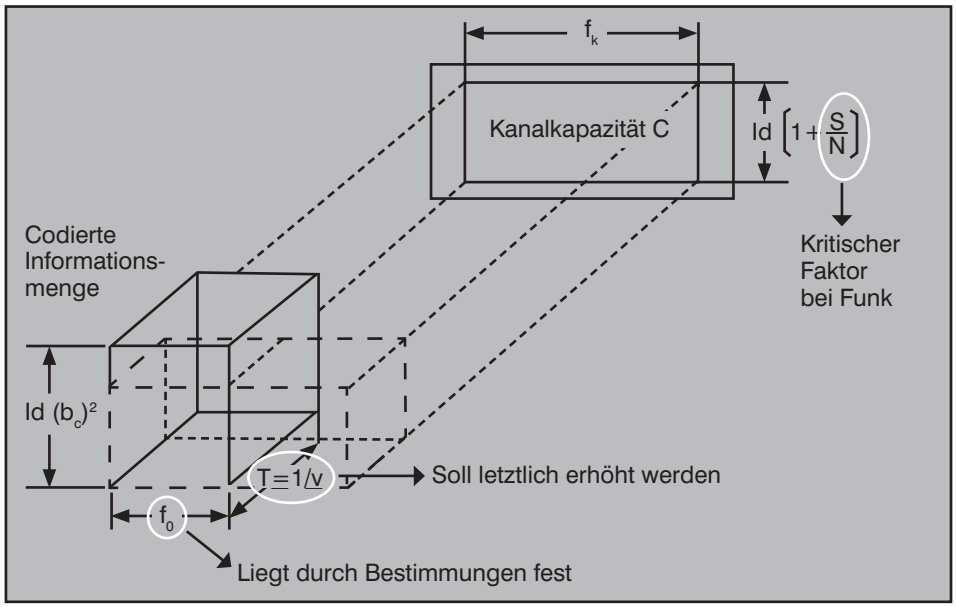


Abb. 2.4: Übertragungskanal und Informationsmenge

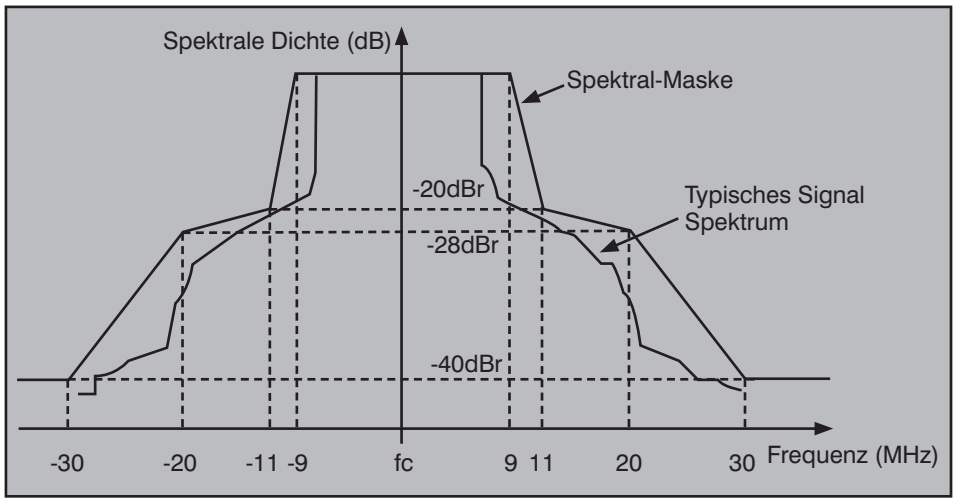


Abb. 2.5: IEEE 802.11a/h Spektralmaske

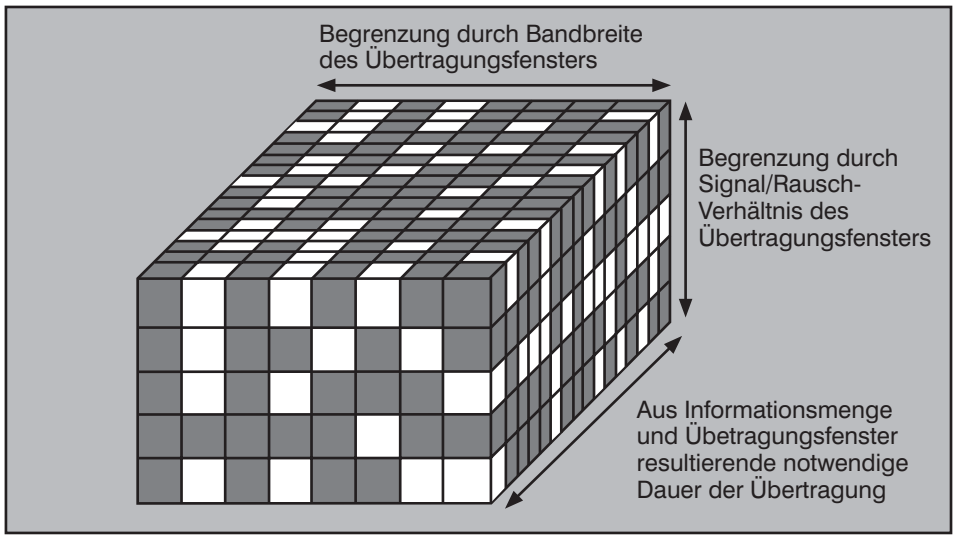


Abb. 2.6: Binär codierte Informationsmenge

Nur so kann man ein breiteres Frequenzband für die Übertragung auf mehreren Kanälen ordentlich und für planerische Zwecke sinnvoll organisieren.

Der Einfluss des Signal-zu-Rausch-Verhältnisses ist bei drahtlosen Übertragungssystemen allerdings gravierend. So ist auch zu erklären, dass das Übertragungsfenster bei zu großen Distanzen zwischen Sender und Empfänger ganz zugeht und keine Übertragung mehr möglich ist.

Wollen wir nun eine zu übertragende Nachrichtenmenge durch ein Übertragungsfenster schieben, müssen wir sie so anpassen, dass sie durch passt. Man kann sich den Nachrichtenquader am einfachsten vorstellen als eine Menge von kleinen Nachrichtenwürfelchen. Jedes Würfelchen entspricht einem zu übertragenden Symbol.

An der Grundfrequenz können wir nicht manipulieren, weil wir als Grundfrequenz diejenige verwenden müssen, die sich aus der durch gesetzliche oder normative Vorgaben bestimmten grundsätzlichen Lage des Übertragungsfensters ergibt. Wenn das Übertragungsfenster bei einer Mittenfrequenz 5125 MHz liegt und 20 MHz breit ist, müssen wir als Grundfrequenz eben 5115 MHz verwenden. Daran führt kein Weg vorbei, es lässt sich auch nicht wild herum manipulieren und der Schwingkreis für die Erzeugung der Trägerfrequenz hilft uns dabei.

Also müssen wir die Würfelchen der Nachrichtenmenge so anordnen, dass sie genau durch das Fenster passen. Bei vorgegebener Bandbreite z.B. 20 MHz und binären Nachrichtenwürfelchen können so z.B. max. 40 Millionen Nachrichtenwürfelchen pro Sekunde durch das Übertragungsfenster laufen. Das gilt wie gesagt nur bei binärer Übertragung, weil man hier aufgrund anderer bekannter Grundgesetze der Nachrichtenübertragung maximal 2 Bits pro Sekunde in ein Hz Bandbreite packen kann. Ob man wie bei IEEE 802.11 a/h die Nachrichtenwürfelchen dabei noch in Untergruppen packt, diese Untergruppen einzeln auf orthogonale Unterträger abbildet und diese dann zu einem OFDM-Signal synthetisiert, ist aus anderen Gründen interessant, spielt bei dieser Betrachtung aber keine Rolle.

Der einzige Schlüssel zu einer höheren nominalen Bitübertragungsleistung liegt also darin, mehr Information in ein Würfelchen zu packen. Alles andere sind Tricks, die nicht funktionieren. Das ist nichts Neues. So wird z.B. bei Fast Ethernet eine ternäre Übertragung verwendet, bei der ein Nachrichtenwürfelchen drei Informations-

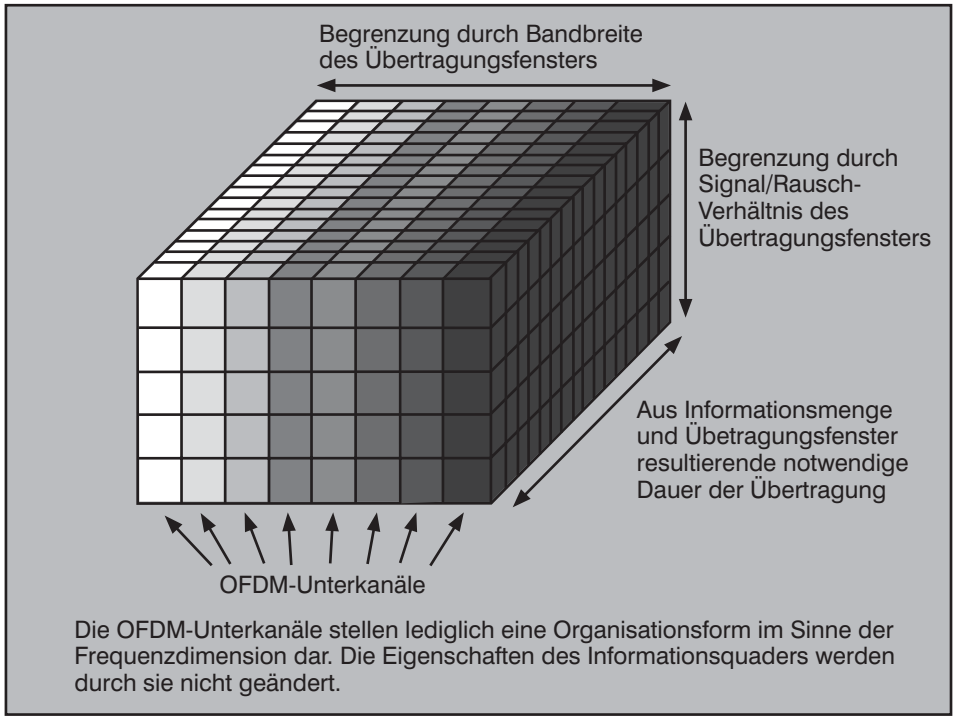


Abb. 2.7: Einfluss von OFDM

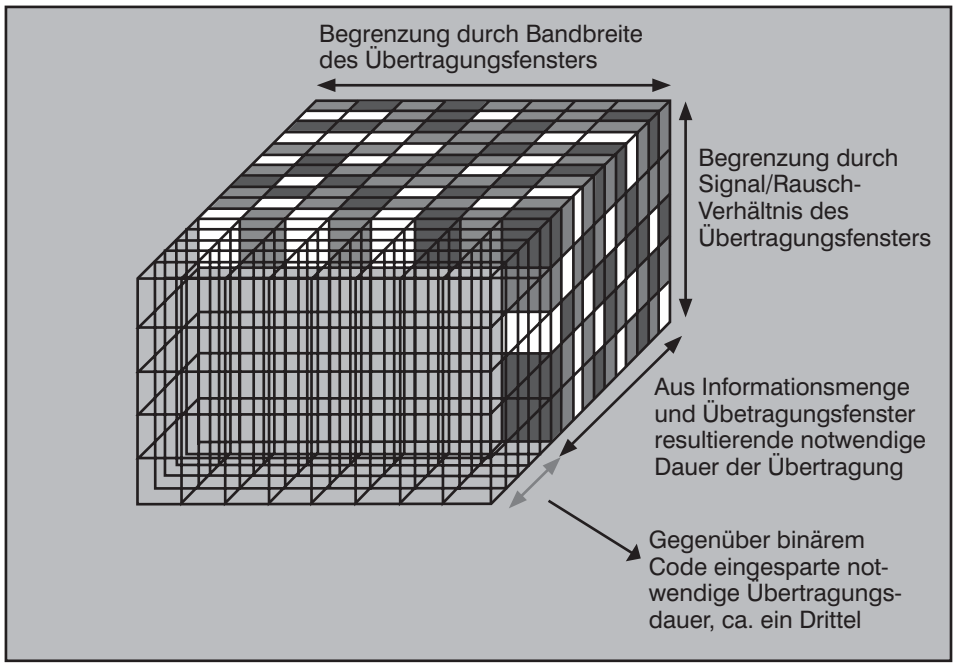


Abb. 2.8: Ternär codierte Informationsmenge

zustände hat. So senkt man die benötigte Bandbreite für die Überragung von 100 Mbit/s. auf 33 MHz. Bei Gigabit Ethernet verwendet man fünfwertige Nachrichtenwürfelchen und Vollduplex und senkt so die benötigte Bandbreite für die Übertragung von 1 Gbit/s. auf ca. 125 MHz.

Nachrichtentechnisch ist das darin begründet, dass die zu übertragende Informationsdichte maximal 2 Baud pro Hz Bandbreite ist. Das Baud ist das Maß für einen so genannten Übertragungsschritt. Wieviel Information in einem Baud enthalten ist, ist dabei zunächst egal und wird durch die Codierung bestimmt. Wenn man jetzt die Information nur binär codiert, schafft man eben maximal nur 2 Bit/s pro Hz, meist viel weniger. Das kann der Interessent in jedem Buch über Nachrichtentechnik ganz weit vorne nachlesen. Die Profis mögen mir dieser Darstellung verzeihen, aber ich habe es in den letzten Jahren immer vergeblich anders probiert und es geht mir darum, dass möglichst viele Betroffene verstehen, wo der Hund begraben ist. Ein Nachrichtenwürfelchen entspricht in unserem Modell also einem Schritt oder Baud. Also ist es entscheidend, wieviel Information man in ein Nachrichtenwürfelchen packen kann.

Nimmt man statt binärer zweiwertiger ternäre dreiwertige Nachrichtenwürfelchen, benötigt die zu übertragende Informationsmenge vergleichsweise deutlich weniger Übertragungszeit, siehe Abb. 2.8

Nimmt man jetzt statt binärer zweiwertiger quartäre vierwertige Nachrichtenwürfelchen, passen in ein Nachrichtenwürfelchen doppelt so viele Informationen hinein, so dass man bezogen auf eine festgelegte Nachrichtenmenge und ein vorgegebenes Übertragungsfenster mit der Hälfte der Übertragungszeit auskommt, oder anders ausgedrückt, doppelt so schnell übertragen kann.

Bei Gigabit Ethernet über Twisted Pair verwendet man quinäre fünfwertige Codierung für die Nachrichtenwürfelchen. Drum funktioniert das überhaupt auf Twisted Pair. Aber das kann sich jetzt jeder vorstellen und ich habe keine Lust mehr für noch ein Bild mit den vielen Kästchen.

Nur mehrwertige Codierungen für die Nachrichtenwürfelchen können also dabei helfen, trotz begrenztem Nachrichtenfenster bei ansonsten gleichen Randbedingungen systematisch mehr Bits pro Sekunde zu übertragen !

2.4 Ominöse Verfahren

Statt nun ordentlich und systematisch an der Einarbeitung dichterer Codierungsverfahren zu arbeiten, experimentieren die o.g. Protagonisten wild mit MIMO-Antennen herum und schaffen damit mehr Probleme als sie lösen.

Man sagt, dass man den binären Signalstrom auf mehrere, mindestens zwei unterschiedliche Funkwege, die durch MIMO-Antennen gebildet werden, aufteilt, auf jedem dieser Funkwege genau so viel überträgt wie bisher und dadurch bei z.B. zwei Wegen doppelt so viel. Und das Ganze natürlich im gleichen Kanal, bewerkstelligt durch ein Wunderwerk namens Path Diversity.

Welche Möglichkeiten stehen uns zur Verfügung, um innerhalb eines einzigen Kanals unterschiedliche Informationen zu übertragen? Generell ist dazu ein Multi-

plexverfahren nötig, und es gibt Raum-, Zeit-, Code- und Frequenzmultiplex sowie Mischungen davon.

Die Abbildung 2.10 zeigt wichtige Multiplexverfahren wiederum in der Dimensionierung der Informationsmenge.

Verwendet man aber ein Multiplexverfahren, kann man damit die Gesamtbandbreite nicht steigern, sondern man organisiert sie nur. So organisieren die OFDM-Unterkanäle die Bandbreite bei IEEE 802.11a/h und z.B. das Codemultiplexverfahren CDMA die Bandbreite bei GSM-Handys.

Alle diese Multiplexverfahren haben jedoch gemein, dass man zwischen einem Sender und einem individuellen Empfänger lediglich einen einzigen Weg benötigt, der durch je eine Antenne bei Sender und Empfänger gebildet wird.

Die MIMO-Protagonisten setzen also tatsächlich darauf, dass sie es schaffen, zwischen einem Access Point und einem Empfänger mindestens zwei unterschiedliche Wege aufbauen können, die sich trotz der Lage im gleichen Kanal gegenseitig nicht stören.

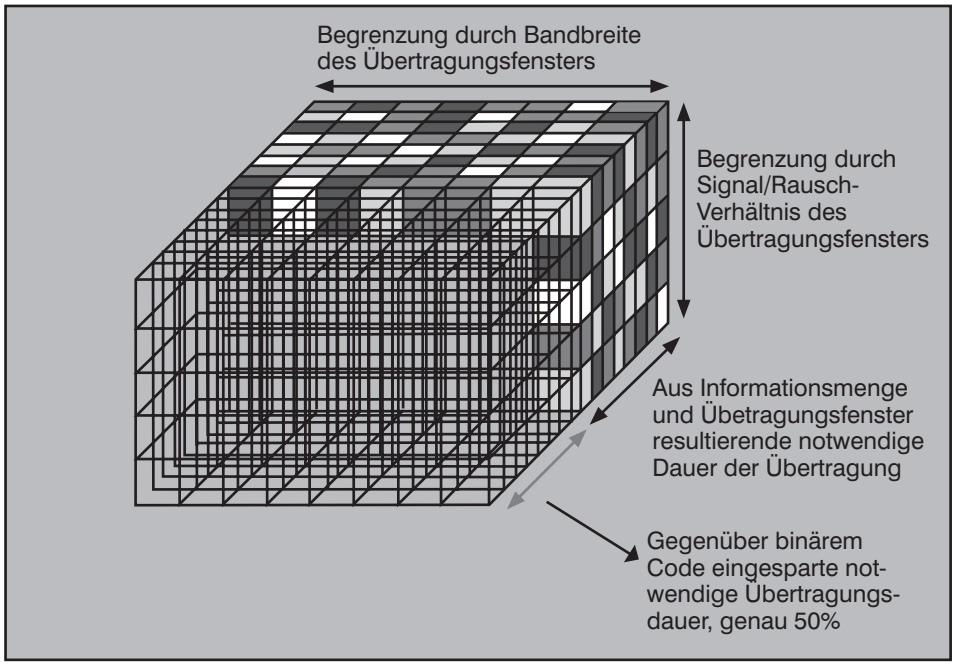


Abb. 2.9: Quartär codierte Informationsmenge

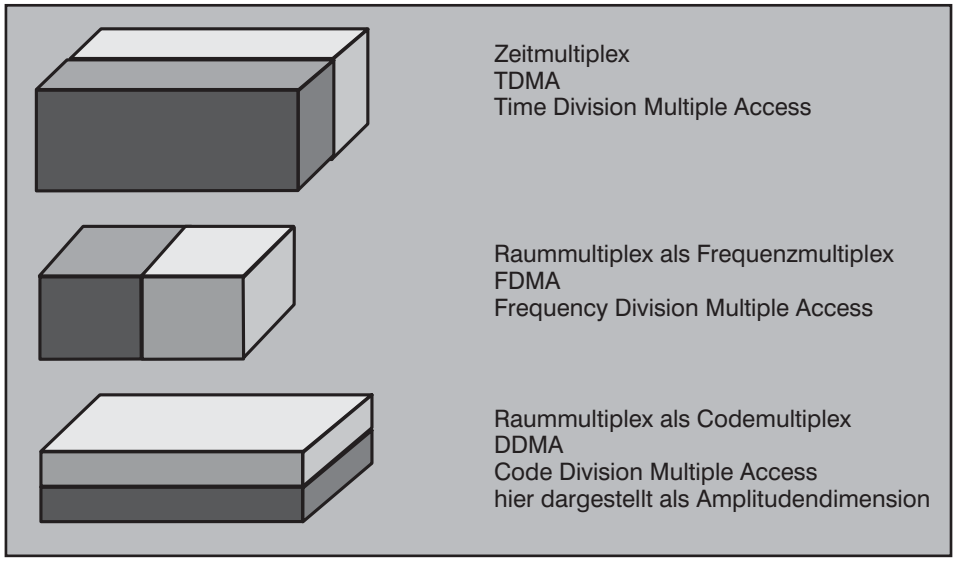


Abb. 2.10: Multiplexverfahren

Dies könnten sie dadurch erreichen, dass sie z.B. für jeden Weg nur eine Teilmenge der orthogonalen Unterträger verwenden. Dann wäre das als CDMA-Verfahren einzuklassifizieren. Hinsichtlich der nominalen Datenrate erreiche sie so aber gar nichts, es sei denn, sie verwenden vor der OFDM-Stufe ein Codierungsverfahren höherer Dichte. Davon ist aber nirgendwo die Rede. Im Gegenteil. Man spricht sogar davon, dass ein besonderer Vorteil der Verfahren die unveränderte Verwendungsmöglichkeit bisheriger Transceiverchips ist.

Eine andere Möglichkeit wäre die Verwendung unterschiedlicher Polarisationsebenen des Funksignals. Das kann man im Freiraum machen, wenn man bereit ist, beliebig viel Geld für entsprechende Antennen auszugeben, aber nicht in einem Zimmer, denn bei jeder Reflexion verändert sich die Polarisation und man kann nicht darauf bauen, dass die beiden Kanäle mit ihren unterschiedlichen Laufwegen gleichartig reflektiert werden.

Also liegt der Grundsatz der Konstruktion tatsächlich in der Annahme, dass man im gleichen Kanal zwei unterschiedliche Signale mehr oder minder störungsfrei nebeneinander übertragen kann. Natürlich wissen auch die Protagonisten, dass das eigentlich nicht geht. Mittels des Path Diversity möchte man aber erreichen, dass es trotzdem klappt. Man fügt dem Signal auf einem Weg eine Kennung hinzu, die den Empfänger in die Lage versetzen soll, dieses Signal auch dann zu erkennen, wenn es durch das andere Signal auf dem anderen Weg gestört ist. Nun ist das OFDM-Signal an und für sich derart stabil, dass man es, wie ich ja schon in früheren Artikeln nachgewiesen habe, praktisch zur Hälfte zerstören und dennoch den Informationsgehalt sauber rekonstruieren kann. Fügt man bei der Synthetisierung im Rahmen der inversen Fast Fourier Transformation eine Kennung hinzu, ist ein Empfänger tatsächlich in der Lage, mehrere zerstörte Signale eindeutig auseinanderzuhalten und die Information unfallfrei jeweils auszulesen und dann aus den unterschiedlichen Informationen die zu übertragende Information zusammenzusetzen. Dazu kommt er im Extremfall sogar mit einer einzigen Antenne aus, allerdings klappt es umso besser, je mehr Antennen er hat, weil er dann via Antennen Diversity die Wege mit den geringsten Störungen besser differenzieren kann.

Selbst wenn man Antennen verwenden würde, die in ihrer Bauart den aus dem Millimeterwellenbereich bekannten Beam Shaped MIMOs entsprechen, was ich auch aus Kostengründen überhaupt nicht sehe, würde man das Problem nur zum Teil lö-

sen, weil man dann zwar die Interferenzen zum guten Teil in den Griff bekäme, die Flächendeckung aber problematisch würde.

Es sind natürlich auch Antennenbauarten denkbar, die eine gewisse, aber nicht so scharfe Richtwirkung haben. Dann wäre die Signalüberlagerung geringer als bei Rundstrahlern, die Flächendeckung aber besser. Bisher wurden derartige Antennen von den MIMO-Protagonisten aber nicht erwähnt.

Wir fassen zusammen: die Protagonisten legen uns tatsächlich ein Verfahren nahe, bei dem absichtlich und bewusst mit Störungen gearbeitet wird und das überhaupt nur deswegen funktionieren kann, weil das standardmäßige OFDM vermöge der hohen Wirksamkeit der vor der eigentlichen Sendestufe eingesetzten redundanten Codierung sehr viele Störungen vertragen kann.

Auf diese Weise die spektrale Effizienz zu erhöhen, verdient wenigstens das Prädikat ominös, ich würde mich ja gerne noch deutlicher ausdrücken.

Stellen Sie sich vor, ein Zweiradhändler würde Ihnen ein normales für 25 km/h zugelassenes Moped verkaufen und dann in der Werkstatt auf ca. 55 km/h tunen. Abgesehen davon, dass ihre Versicherung begeistert wäre, würden im Falle eines Unfalles die Bremsen überhaupt nicht ausreichen und die „spektrale Effizienz“ Ihres Aufpralls deutlich gesteigert.

2.5 Weitere Gefahren durch ominöse Verfahren

Inwieweit jemand die genannte Technik im Heimbereich einsetzt, sei jedem selbst überlassen.

Abb. 2.11: WLAN-MIMO Verwendung von Rundstrahlern

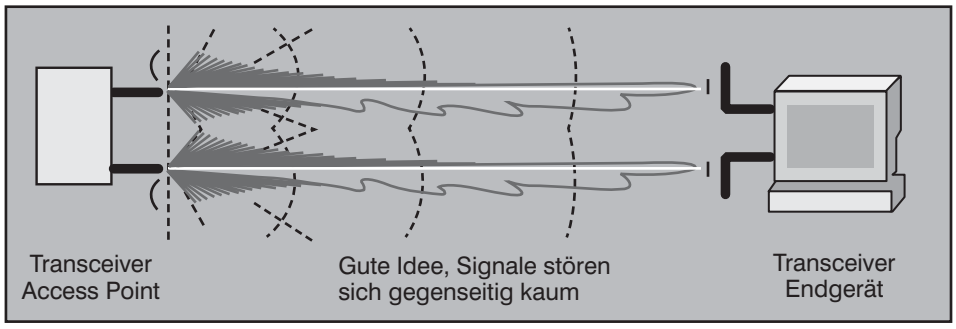


Abb. 2.12: WLAN-MIMO mit Richtantennen

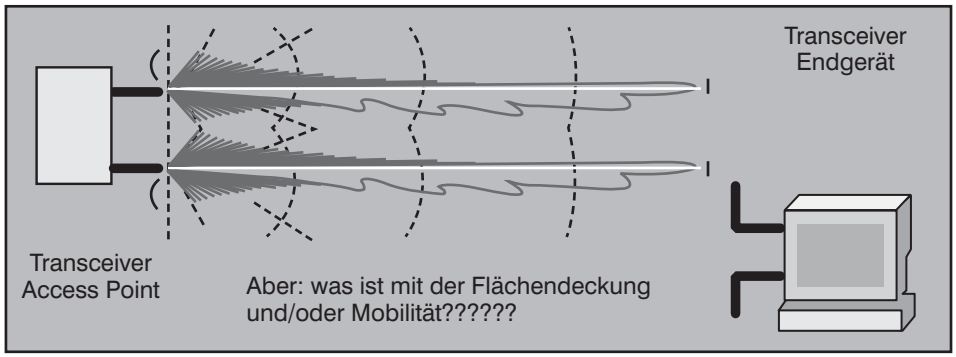


Abb. 2.13: Problem bei WLAN-MIMO mit Richtantennen

Für eine professionelle Umgebung ist das Ganze jedoch absolut abzulehnen. Dafür gibt es direkt eine ganze Reihe von Gründen.

Im Rahmen des Designs der Sender hat man keinen Einfluss darauf, ob sich nicht durch die mehr oder minder absichtliche Mischung der Signale auf den zwei Wegen Interferenzen ergeben, die in Frequenz und Intensität die vorgegebene Spektralmaske verletzen. Ich denke da z.B. an einen Effekt, der bei optischen DWDM-Systemen beschrieben wird, das sog. Four Wave Mixing. Innerhalb eines DWDM-Systems gibt es viele einzelne eng zusammenliegende Kanäle, z.B. 256 oder 1000. Diese werden durch die optischen Multiplexer und Demultiplexer zusammengemischt bzw. auseinandergezogen, um auf einer Glasfaser übertragen werden zu können. Unter Randbedingungen, deren Erklärung diesen Artikel sprengt, ist es möglich, dass die Signale auf drei Kanälen einfach ein viertes Signal auf einem weiteren Kanal „zusammenmischen“, in etwa in Art einer Schwebung. Dieses vierte Signal ist so stark, dass man diesen Kanal nicht mehr für die Datenübertragung verwenden kann. Elektromagnetische Wellen sind elektromagnetische Wellen, egal ob Funk oder Licht. Es gelten immer die gleichen mathematischen Grundsätze. Also kann es auch Four Wave Mixing bei Funksystemen geben. Prima, wenn dann ein Kanal gestört wird, den man eigentlich für etwas anderes benötigt.

Aber es reicht ja auch schon, wenn die Vorgaben der Spektralmaske einfach verletzt werden. Dann gibt es nämlich Probleme mit der Koexistenz eines MIMO-Systems auf einem und einem konventionellen System auf einem anderen Kanal.

Eingangs haben wir erwähnt, dass ein einfaches MIMO-System unter bestimmten Umständen auch ohne Erhöhung der Datenrate zu einer gesteigerten Reichweite führen kann. Ein im gleichen Kanal aktives Signal eines „normalen“ WLANs würde dadurch empfindlich gestört bzw. ganz platt gemacht.

Für die Verwendung von WLANs im 5 GHz-Bereich in Europa sind DFS und TPC Vorschrift. Wenn ein MIMO-System das auch können soll, müssen alle „Wege“ gleichzeitig den Kanal wechseln. Die Entscheidungsgrundlage für DFS ist eine Störung. Ab und an misst der Access Point nach, welche Kanäle ggf. von anderen Funkdiensten genutzt werden. Es gibt aber auch Systeme, die dynamisch auf Störungen reagieren. Das kann man bei MIMO-Systemen nicht implementieren, weil sich die unterschiedlichen Signalwege ja schon selbst erheblich stören. Zur Realisierung von DFS braucht ein

MIMO-System hineichend häufige Denkpausen.

Keiner der Protagonisten verliert z. Zt. auch nur ein Wort zu DFS oder TPC. Man beurteilt den Europäischen Teilmarkt offensichtlich als nicht lohnend. Ein Glück für uns.

Aus den bisherigen Ausführungen dürfte klar geworden sein, dass sich ein MIMO-System keinesfalls problemlos in eine systematische seriöse Planung für ein flächendeckendes Campusnetz eingliedern lässt.

Völlig erschütternd ist schließlich der Vorschlag, doch einfach 40 MHz breite Kanäle zu benutzen. Das tritt nicht nur das ursprüngliche Ziel von IEEE 802.11n der Beibehaltung der IEEE 802.11 a/h Spektralmaske mit Füßen, sondern zerstört auch sämtliche Ansätze zu ordentlichen flächendeckenden Zellenplanungen.

3. Sinnvolle Verfahren

Unter den eingangs genannten Voraussetzungen sind uns die Hände hinsichtlich einer möglichen Leistungssteigerung gebunden.

Wir haben folgende Randbedingungen zu beachten:

- Das Übertragungsfenster liegt fest
- Das S/N liegt fest
- Die Basisfrequenz liegt fest

Eine Erhöhung der Datenrate bei festliegender Basisfrequenz geht zwingend mit einer Verdichtung der Datendarstellung einher. Eine Verdichtung der Datendarstellung ist nur via „Codierung/Modulation“ möglich. Es gibt aber schon eine Reihe von Beispielen aus der verdrahteten Welt:

- dreiwertige Codierung bei 100 Mbps führt zu 33 MHz Bandbreite bei 100 BASE-T
- fünfwertige Trellis-Codierung bei 1 Gbps führt zu 125 MHz Bandbreite bei Gigabit Ethernet
- 5PAM (Puls Amplitudenmodulation mit fünfwertigen Signalen) schafft es, dass 1 - 2 Mbps mit DSL über eine einfache Telefonleitung wandern
- 10PAM (Puls Amplitudenmodulation mit zehnwertigen Signalen und Trellis-Codierung) ist Grundlage für 10 Gigabit mit 400-800 MHz Bandbreite bei 10 GBASE-T

Es gibt insgesamt folgende bei einer Funkübertragung beeinflussbare Parameter:

- Frequenzbereich
- Signalform
- Sendeleistung
- Empfängerempfindlichkeit
- Antennengewinn
- Modulation
- Vorwärts-Fehlerkorrektur

Durch die Vorgaben der Regulierungsbehörden (FCC, ...) sind Frequenzbereich, Signalform, maximale Sendeleistung und Antennengewinn unabänderbar vorgegeben. Durch den Kostenrahmen ist die Empfängerstruktur vorgegeben. Flexibilität besteht lediglich hinsichtlich der Vorwärts-Fehlerkorrektur und der Modulation.

Die aktuellen, ernsthaften Diskussionen innerhalb von IEEE 802.11n drehen sich vor allem um komplizierte Varianten der Trellis- und Viterbi-Codierung. Es macht aktuell keinen besonderen Sinn, diese im Einzelnen vorzustellen. Stattdessen möchte ich die generelle Richtung der möglichen Entwicklung unter Rückgriff auf konkrete bekannte und realisierte Technologien erklären.

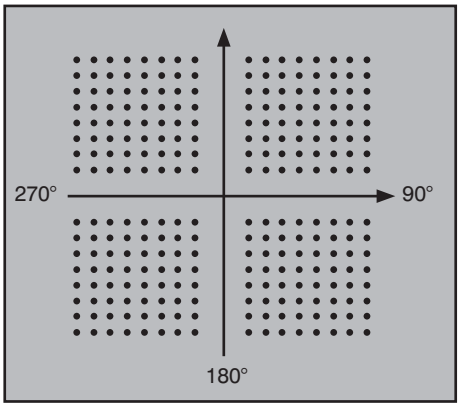


Abb. 3.1: 256 QAM Quadratur Amplituden Modulation

Innerhalb des OFDM-Verfahrens bestehen noch folgende Möglichkeiten:

- Änderung der Codierrate
- Mehr codierte Bits pro Unterträger
- Mehr codierte Bits pro OFDM-Symbol
- Verbesserung des Verhältnisses von codierten Bits zu tatsächlichen Nutzdatenbits

Jede Leistungssteigerung hat bestimmte Tradeoffs. Steigerung der Anzahl der Unterträger scheidet wegen der allgemeinen Kompatibilität zu IEEE 802.11a aus.

3.1 Verwendung von 256 QAM

Die nächstliegende Möglichkeit ist die Verwendung von 256QAM. Die Kulminationspunkte von 256 QAM sehen wir in Abb. 3.1.

Wir erhalten eine höhere Dichte von Kulminationspunkten und die Information von maximal 10 Bits in einem Kulminationspunkt. Dadurch ergibt sich eine Erweiterung der bekannten OFDM-Parametertabelle wie in Abb. 3.2 dargestellt.

Die Tradeoffs liegen auf der Hand:

+ einfach zu implementieren
+ keine Änderung an Rahmenformaten
+ kann bei Problemen oder schlechtem S/N

Daten-Rate in Mbit/s	Modulation	Codier-Rate	Codierte Bits pro Unterträger	Codierte Bits pro OFDM Symbol	Daten-Bits pro OFDM Symbol
6	BPSK	1/2	1	48	24
9	BPSK	3/4	1	48	36
12	QPSK	1/2	2	96	48
18	QPSK	3/4	2	96	72
24	16-QAM	1/2	4	192	96
36	16-QAM	3/4	4	192	144
48	64-QAM	2/3	6	288	192
54	64-QAM	3/4	6	288	216

Abb. 3.2: IEEE 802.11a Parameterliste

Leistungsparamter von 256 QAM bei Weiterführung der sonstigen Verfahren			
Codierdichte	2/3	3/4	1/1
Codierte Bits pro Unterträger	8	8	10
Codierte Bits pro OFDM-Symbol	384	384	480
Datenbits pro OFDM-Symbol	256	288	384
nutzbare Datenrate in Mbps	72	90	**120**

Abb. 3.3: OFDM-Parametertabelle mit 256 QAM

IEEE 802.11n : der große MIMO-Bluff und ernst zu nehmende Alternativen

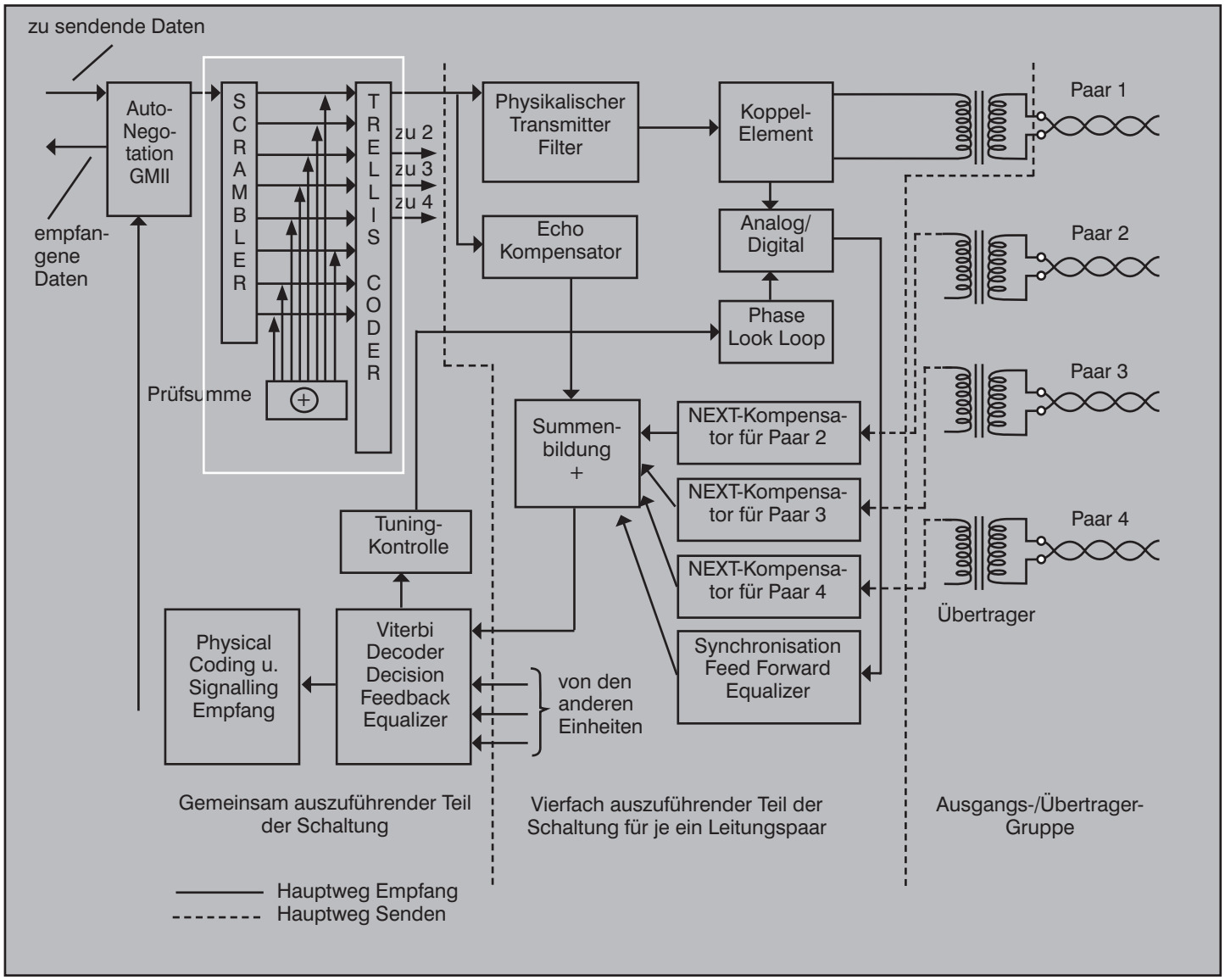
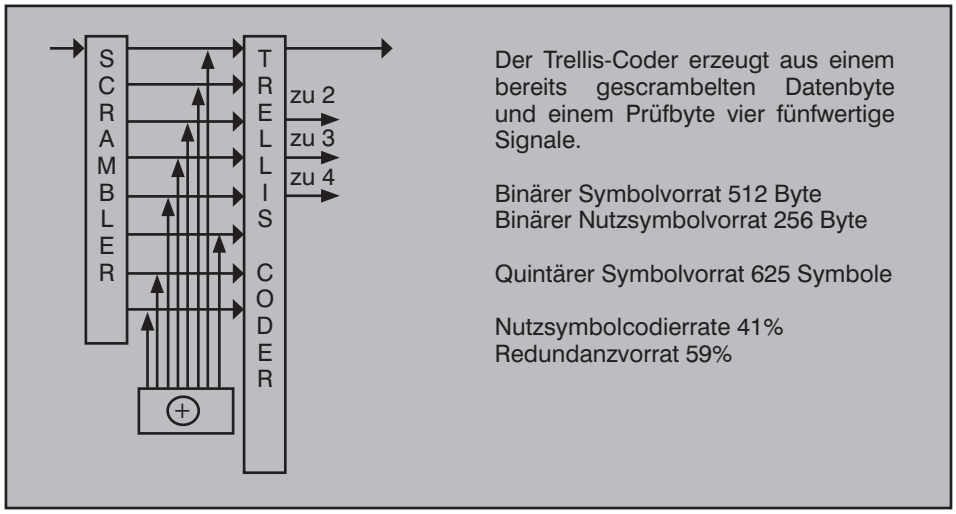


Abb. 3.4: 1000 BASE T Gesamtschaltung



Der Trellis-Coder erzeugt aus einem bereits gescrambelten Datenbyte und einem Prüfbyte vier fünfwertige Signale.

Binärer Symbolvorrat 512 Byte
Binärer Nutzsymbolvorrat 256 Byte

Quintärer Symbolvorrat 625 Symbole

Nutzsymbolcodierrate 41%
Redundanzvorrat 59%

Abb. 3.5: Trellis Codierer mit Scrambler

einfach zurückschalten
+ erreicht hohe Zuverlässigkeit mit FEC und Faltungscodierer
+ erreicht die Ziele und über 100 Mbit/s

- bei 120 Mbit/s ist Schluss
- könnte Decodierungsprobleme verursachen
- kein wirklicher Fortschritt

Immerhin ist 256 QAM eine ernst zu nehmende Alternative zu dem von einigen Herstellern angebotenen proprietären Bündelungsmodus, der zwar 108 Mbit/s bringen soll, dafür aber zwei Kanäle benötigt und somit die gegenüber IEEE 802.11b mühevoll gewonnene Freiheit beim Zellendesign unnötig beschneidet.

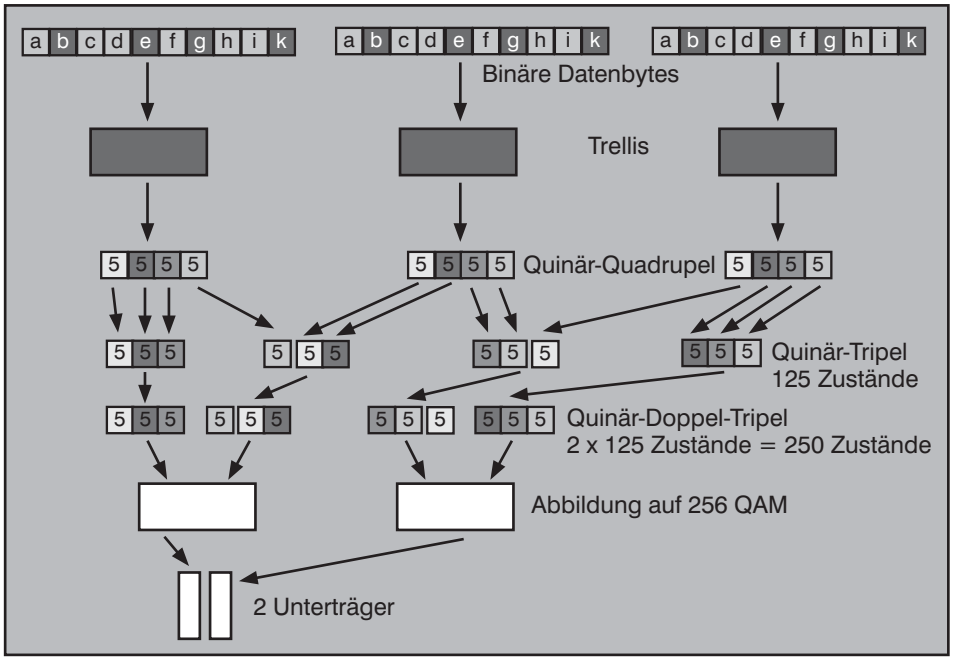


Abb. 3.6: Neue Codierung der Unterträger

Insbesondere ist 256 QAM aber eine Alternative zu den ominösen MIMO-Verfahren.

3.2 Abwandlung des Codierprozesses

Eine Stärke und die Basis für die relative Unempfindlichkeit gegenüber Störungen des IEEE 802.11a OFDMs ist der aufwändige Faltungscodierungs- und Scramblingprozess. Andererseits ist dies auch ein Problem, denn es wird gehörig Bandbreite durch Redundanzen verschwendet. Immerhin werden bis in die Stufe der Abbildung auf die xQAM rein binäre Signale verwendet. Das ist eigentlich nicht nötig und ich möchte zeigen, was passiert, wenn man einen alten bekannten und guten Kumpel verwendet, nämlich den Trellis-Codierer aus Gigabit Ethernet über Twisted Pair. Dieser Codierer ist millionenfach als Bestandteil von Gigabit Ethernet Adapter-Chips verbaut und alles andere als eine exotische Baugruppe. Abb. 3.4 zeigt uns nochmal das Schaltbild eines Gigabit Ethernet Adapters und Abb. 3.5 den Trellis-Codierer mit seinen Eigenschaften. Der Trellis Codierer erzeugt aus acht binären Datenbits und einem Kontrollbit vier quinäre (fünfwertige) Signale.

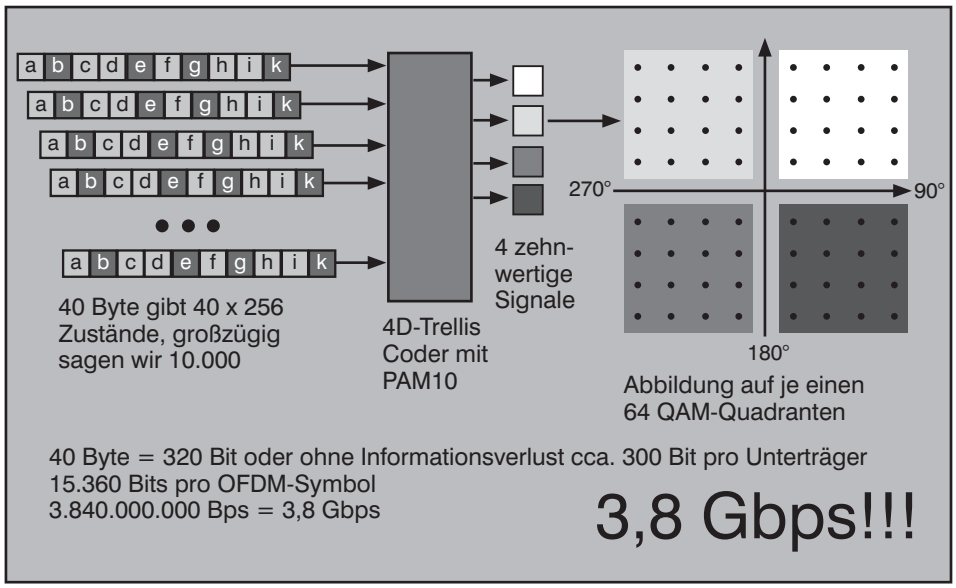


Abb. 3.7: 4D-Trellis mit PAM10 aus 10 GBASE-T

Daraus ergibt sich:

- Binärer Symbolvorrat 512 Byte
- Binärer Nutzsymbolvorrat 256 Byte
- Quinärer Symbolvorrat 625 Symbole
- Nutzsymbolcodierrate 41 %
- Redundanzvorrat 59 %

Die Abb. 3.6 zeigt die mögliche neue Codierung der Unterträger. Drei binäre Datenbytes werden zunächst in drei Trellis-Coder geschickt. Daraus entstehen drei Quinär-Quadrupel mit je vier fünfwertigen Signalen. Diese können anders gruppiert werden, nämlich in vier Quinär-Tripel. Jedes dieser Quinär-Tripel hat 125 unterschiedliche mögliche Zustände.

Zwei dieser Quinär-Tripel haben also nur 250 verschiedene Zustände, weil sie unabhängig voneinander sind. Darin unterscheidet sich ein Quinär-Doppel-Tripel von einem Quinär-Sechstupel, welches immerhin 31250 verschiedene Zustände annehmen können. Ein Quinär Doppel-Tripel kann also bequem auf die 256 Kulminationspunkte der 256QAM abgebildet werden. So schaffen wir es, die Information der drei Datenbytes in nur zwei Unterträger zu packen. Wir kommen zu folgendem Ergebnis:

3 Bytes ergeben 2 Unterträger. 48 Unterträger können somit 72 Bytes übertragen. Das sind 12 Bits pro Unterträger oder 576 Bits pro OFDM-Symbol. Das bedeutet bei 250.000 Symbolen/s. eine Datenrate von 144 Mbit/s unter Beibehaltung einer Sicherheitsreserve von ca. 60% im Symbolvorrat.

Das ist immer noch nicht besonders revolutionär, zeigt aber die Richtung, in die man gehen sollte. Der springende Punkt ist, dass die fünfwertige Codierung nicht in irgendeiner Weise in das eigentliche Funksignal eingeht, sondern letztlich innerhalb der Schaltkreise der Adapterkarte verbleibt, also von daher keinerlei Schwierigkeiten durch die Eigenheiten des Funkkanals zu erwarten sind.

Zur Zeit diskutiert IEEE 802.11n unterschiedliche Kombinationen aus Codierungen und QAM-Varianten mit bis zu 320 Mbps. Stand Dezember 2005 hat man ca. 4-5 Varianten in die engere Wahl gezogen. Es ist aber nicht sicher, ob daraus irgend etwas wird, weil diese Varianten zum Zeitpunkt der Fertigstellung der Standards nicht mehr den aktuellen Stand der Signalverarbeitungstechnik repräsentieren, sondern lediglich zart evolutionäre Weiterentwicklungen sind. Außerdem wurde die Arbeitsgruppe ja von den MIMO-Protagonisten lahmgelegt.

3.3 MIMO - aber richtig!

Innerhalb der Nachrichtentechnik besteht seit längerem ein Trend zur Abwendung von SISO (Single Input Single Output) hin zu MIMO (Multiple Input Multiple Output)-Schaltungen für die Signalverarbeitung. 10 GBASE-T ist undenkbar ohne derartige neue Chips. Teilweise arbeiten die gleichen Spezialfirmen für die Herstellung höchstintegrierter MIMO-Schaltkreise in den Arbeitskreisen für 10 GBASE-T und IEEE 802.11n. Vielleicht haben die Vielfachantennenprotagonisten den Ausdruck auch hier aufgeschnappt!

Es geht also jetzt um Schaltkreise, nicht um Antennenfelder.

Sehen wir uns an, was Schaltkreise, wie sie für 10 GBASE-T diskutiert und entwickelt werden, für OFDM-WLANs tun könnten. Zentrales Element bei 10 GBASE-T ist PAM10, die Pulsamplitudenmodulation mit 10-wertigen Ausgangssignalen. Vierdimensionaler Trellis-Code 4D mit acht Zuständen. Bei 10 GBASE-T bedeutet das bei vier Kabelpaaren eine Trellis-Dimension pro Kabelpaar, 12 Bits pro 4D-Symbol, 10 Level PAM (PAM-10) auf jedem Paar und somit eine benötigte Bandbreite von nur 833 Mbaud/s. Ein MIMO-Schaltkreis nutzt die zwischen den Eingangssignalen insgesamt bestehenden Abhängigkeiten systematisch aus und kann daher mit einer bezogen auf das Ergebnis wesentlich geringeren Komplexität aufgebaut werden als eine Ansammlung von SISO-Schaltungen für vergleichbare Funktionalität. Wir setzen jetzt die Existenz eines 4D Trellis-Coders mit PAM10 voraus. In Abbildung 3.6 zeigen wir dann einen möglichen Codierungsprozess.

Das Eingangssignal des Trellis-Coders bilden 40 Bytes, die parallel auf 40 Eingangsleitungen ankommen. Diese 40 Bytes haben pro Byte 256 unterschiedliche Zustände, also ergeben sich, großzügig gerechnet, ca. 10.000 Zustände. Die 240 Zustände, die wir hier gepflegt auslassen, können wir ausblenden, indem wir beim Scrambling und der Vorcodierung auf 6 Symbole pro Byte verzichten, was kein Problem sein sollte. Der 4D Trellis-Coder bildet diese zehntausend Zustände auf vier zehnwertige Ausgangssignale ab, das passt ja genau. Jedes dieser zehnwertigen Signale bilden wir dann auf einen Quadranten der 64 QAM ab. Jeder Quadrant hat 16 Kulminationspunkte, es bleiben also pro Quadrant sogar 6 Kulminationspunkte übrig, die von den Werten der zehnwertigen Variablen nicht benötigt werden und somit eine erhebliche Sicherheitsreserve darstellen.

Damit kommen wir in eine ganz neue Leistungsdimension. 40 Byte = 320 Bit oder ohne Informationsverlust ca. 300 Bit pro Unterträger ergeben unter Beibehaltung der bisherigen Parameter 15.360 Bits pro OFDM-Symbol also eine Gesamt-Datenrate von 3.840.000.000 Bit/s = 3,8 Gbit/s.

Und dies auch noch unter Verwendung des relativ unempfindlichen 64QAM auf der Luftschnittstelle. Der Trick hierbei ist wieder, dass die eigentlich komplexe Informationsverarbeitung und die empfindlichen zehnwertigen Signale vollständig innerhalb der Schaltkreise verbleiben, die sie erzeugen und verbrauchen. Die Verwendung für WLANs ist damit sogar noch einfacher und günstiger als für 10 GBASE-T, wo die zehnwertigen Signale ja über eine Datenleitung laufen und am Ende in nicht unerheblicher Weise wieder aufgepäppelt werden müssen.
Das OFDM-Verfahren nach IEEE 802.11a funktioniert funktechnisch immer gleich, unabhängig davon, wie viele Bit/s man auf die Unterträger abbildet. Das liegt an der Synthetisierung des Signals. Wenn man die Anordnung der vorigen Folie vierfach ausführt, und statt der 64-QAM eine 256-QAM verwendet, kommt man auf stattliche 15,2 Gbit/s.

Es sei an dieser Stelle nochmals ausdrücklich darauf hingewiesen, dass wir einen Diskussionsstand betrachten, nicht aber tatsächliche Standardisierungsvorschläge.

Diese werden erst in 2006 kommen. Es ging mir lediglich um die Frage, wie weit man das OFDM-Verfahren ausreizen kann, wenn man auf Komponenten zurückgreift, die sich momentan in der Fertigungsvorstufe befinden.

3.4 Verbesserungen von DCF

Es gibt ein sehr schönes Steuerungsverfahren, welches im Rahmen des ETSI Hiperlan/2 definiert wurde. IEEE 802.11 muss dieses Verfahren gekannt haben. Obwohl das Verfahren deterministisch ist und sogar verschiedene Dienstklassen zulässt, wurde es nicht berücksichtigt. Es ist auch in der Zukunft davon auszugehen, dass IEEE lieber eigene Verfahren definiert, anstatt in gutes, aus Europa kommendes Verfahren anzunehmen. Verschiedene Hersteller haben dies schon bedauert, aber das nützt momentan nichts. Es bringt deshalb auch nichts, dieses Verfahren hier zu beschreiben.

Sehen wir uns also lieber kurz an, worüber IEEE 802.11n diskutiert.

Aus Kompatibilitätsgründen möchte man DCF nicht völlig abschaffen, was im Grunde genommen die einzig wirkliche Lösung wäre, sondern ergänzen.

Im 5 GHz Band stehen bis zu 19 überlappungsarme Kanäle zur Verfügung. Selbst unter Berücksichtigung von Kanälen, die man wegen Interferenzen zu anderen Funksystemen nicht benutzen kann oder abschalten muss, bleiben auch bei einem dreidimensionalen Zellendesign genügend Kanäle übrig, um in einer Zelle zwei Kanäle gleichzeitig zu benutzen. In einem Kanal kann man das DCF-Verfahren fast wie gewohnt verwenden, in einem anderen Kanal kann man ein anderes Protokoll benutzen, z.B. das Direct Link

Control Protocol DLC. Günstig ist es, wenn man einen Mechanismus definiert, der es entsprechend ausgestatteten Stationen erlaubt, zwischen den Kanälen und somit den Zugriffsverfahren umzuschalten. Dann kann ein Kanal wie üblich mit DCF betrieben werden und auch die Stationen, die ein anderes Protokoll nicht unterstützen, können weiterhin kommunizieren.

Eine wichtige Anforderung an ein Ergänzungsprotokoll ist sicherlich die Determiniertheit. Diese ist Grundvoraussetzung für eine geringe Delayvarianz, wie man sie bei VoIP über Wireless dringend benötigt. Der Gedanke, zwei unterschiedliche Kanäle zu benutzen ist nahe liegend, weil es in einer Zelle immer Geräte bzw. Anwendungen geben wird, die zusätzlichen Determinismus nicht benötigen und andere, für die das sozusagen lebenswichtig ist. So könnte

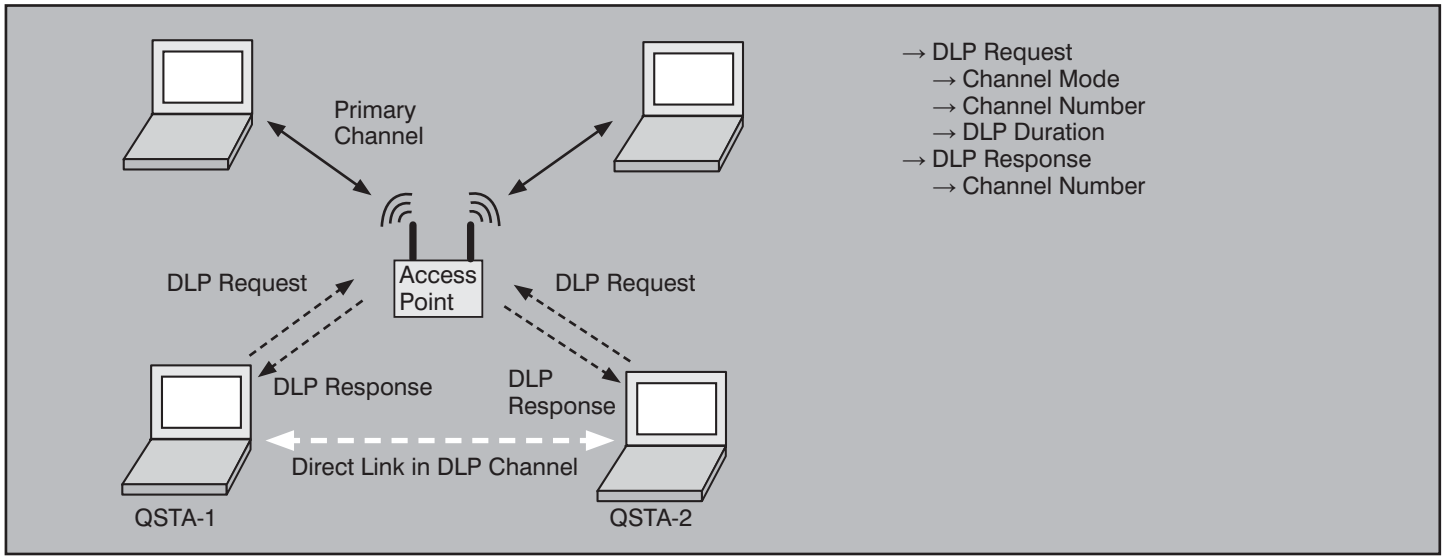


Abb.3.8: 4-Way Handshake

man sich in einer Zelle konventionelle PCs, Notebooks oder Handhelds vorstellen, die mehr oder minder gelegentlich Daten übertragen und somit mit DCF auskommen und Geräte, mit denen man telefonieren kann und die ein anderes Verfahren benötigen.

Das DLC setzt voraus, dass es einen Access Point und eine oder mehrere DLC-fähige Stationen gibt. Der Access Point hat eine zentrale Steuerungsfunktion.

DLP erlaubt den Austausch von Frames direkt zwischen nicht-AP Stationen im gleichen BSS.
Der AP kontrolliert die limitierte Ressource (d.h. den Kanal), um DLP- Kanäle von der Liste verfügbarer Kanäle zuzuordnen. Dazu macht er grundsätzlich einen Background SCAN, das ist ein periodischer Update der Liste verfügbarer Kanäle durch Prüfung der RSSI der Mittenfrequenz eines jeden Kanals, Zuteilung des DLP Kanals zu DLP Stationen erfolgt mit DLP Request oder DLP Response Frame.

DLP Stationen ändern den Kanal zwischen DLP and nicht-DLP. Dabei gibt es verschiedene Betriebsmodi:

- DLP Mode 1: DLP Stationen teilen sich den Primärkanal
- DLP Mode 2: DLP Stationen benutzen entweder den Primärkanal oder den DLP-Kanal in PCF or DCF nach 4-way handshake Transaktion
- DLP Mode 3: DLP Stationen benutzen nur den DLP-Kanal nach 4-way handshake Transaktion

Damit alles funktionieren kann, muss das Frameformat geändert werden, aber nur wenig. Man braucht drei neue Primitive (DLP Reques, DLP Response und DLP Start/End) sowie neue Action Codes auf Grundlage des üblichen IEEE 802.11 Management Frames.

Grob funktioniert der Beginn der DLP-Kommunikation wie folgt:

Wenn eine Station QSTA-1 mit einer anderen Station QSTA-2 in DLP kommunizieren möchte, schickt sie einen DLP Request mit Kanal-Modus, einem Vorschlag für eine Kanalnummer, dem gewünschten Adressaten, also der Station, mit der direkt kommuniziert werden soll und der gewünschten Dauer der DLP-Verbindung an den Access Point. Der Access Point schickt dann diese Anfrage an die für die DLP-Kommunikation adressierte Partnerstation QSTA-2 und schlägt eine Kanalnummer aus der Liste der freien Kanäle vor. Die Partnerstation QSTA-2 antwortet dann mit einem DLP-Response, in dem die Kanalnummer bestätigt wird. Der Access Point schickt dann einen DLP-Response an die anfragende Station QSTA-1 weiter und die direkte Kommunikation zwischen den beiden DLP-Stationen kann beginnen. Wenn die andere Station nicht kommunizieren möchte oder kann, gibt es keinen DLP-Response und die Kommunikation findet nicht statt. Die ursprünglich anfragende Station versucht es dann nach einer gewissen Zeit noch einmal oder gibt es auf. Das kommt jetzt ganz darauf an, wie man das letztlich implementieren möchte.

In Wahrheit wird es durch die verschiedenen möglichen Betriebsmodi doch noch komplizierter:

1. DLP Requestor Station sendet DLP Request Frame mit geeignetem Channel Mode, Channel Number und DLP Duration

   Wenn Channel Mode 1 ist, kein extra Kanal....
   Wenn Channel Mode 2 ist, Channel Number := 0 und DLP Duration = „Time value“
   Wenn Channel Mode 3 ist, Channel Number := 0 und DLP Duration = NULL

2. AP empfängt den DLP Request Frame
   Wenn Channel Mode 1 ist, leitet der AP ihn an den Empfänger weiter.

   Wenn Channel Mode 2 oder 3 ist, setzt AP die DLP Channel Number im DLP Request Frame wenn es einen verfügbaren Kanal in der Kanal-Liste gibt und leitet sie an den Empfänger weiter.

3. DLP Responder Station sendet DLP Response Frame

   Wenn Channel Mode 1 ist, sendet die DLP Responder Station den DLP Response Frame an den DLP Requestor. Wenn Channel Mode 2 oder 3 ist, setzt die DLP Responder Station die DLP Channel Number im DLP Response Frame wenn die DLP Channel Number ungleich 0 ist im DLP Request Frame (der vom AP empfangen wurde) und die DLP Responder Station tritt in den DLP-Modus. Die DLP Responder Station sendet einen DLP Response Frame an den AP.

4. AP empfängt den DLP Response Frame

   Wenn der Channel Mode 1,2, oder 3 ist, leitet der AP ihm zum DLP Requestor weiter.

Durch die Einführung des DLP-Modus wird auch ein neues Association Request Frame Format notwendig, welches eine Station mit DLP-Fähigkeiten entsprechend kenntlich macht.

Ein weiteres Element ist der Polling Mechanismus. Stationen müssen aus betrieblichen Gründen vom Access Point angepollt werden können, um festzustellen, ob sie pollbar und damit DLC-fähig sind. Eine untätige DLP Station sollte nicht im DLP- Channel sondern im Primärkanal sein. Der AP prüft eine Polling Tafel basierend auf empfangenem Association Request und Liste verfügbarer Kanäle basierend auf DLP Request/Response Frame. Der AP sollte im PCF-Modus pollen.

Für die Funktionalität einer DLP-Station nach Betreten des DLP-Modus muss wiederum entlang der drei möglichen DLP-Modi differenziert werden.

DLP Mode 1 folgt dem DLP Mechanismus (802.11e) in dem der Primärkanal im BSS aufgeteilt wird.

DLP Mode 2. Es gibt zwei Fälle: erstens Umschalten des Kanals im PCF-Modus. Nach Empfang eines Beacons schaltet die DLP Station zum DLP- Kanal für die Dauer des DLP NAV. Nach Rückkehr zum Primärkanal im CFP wartet die DLP Station auf einen Poll vom AP. Zweitens: Umschalten des Kanals im DCF-Modus. Wenn die DLP Station den Wettbewerb um den Kanal gewinnt und einen Frame für die Übertragung zu einer DLP Station hat, broadcastet die DLP Station den DLP Start Frame um darüber zu informieren, dass DLP Stationen für die Dauer des DLP NAV auf den DLP-Kanal umschalten. Wenn die DLP Station den Wettbewerb um den Kanal verliert und der empfangene Frame nicht an die DLP Station gerichtet ist, schaltet die DLP Station für die Dauer eines DLP NAV auf den DLP-Kanal.

DLP Mode 3. Wenn die DLP Station den Wettbewerb um den Kanal gewinnt, broadcastet sie den DLP Start Frame, um darüber zu informieren, dass DLP Stationen auf den DLP Kanal switchen und nach der Übertragung des DLP End Frames wieder zurückswitchen.

Es wird auch sofort klar, was dem Autor an diesem Verfahren nicht gefällt: Voraussetzung für das Betreten des DLC-Modus ist der Gewinn des Wettbewerbs im DCF-Modus. Dies fügt dem an und für sich deterministischen Verfahren einen Nicht-Determinismus zu, der für die eingangs angesprochenen Anwendungen sicherlich nicht wünschenswert ist. Der Vorschlag bleibt sozusagen auf halber Strecke zwischen den Alternativen reines Wettbewerbsverfahren und reines deterministisches Verfahren stecken.

Das Problem der VoWLAN-Übertragung löst der DLC-Modus auch nicht elegant.

4. Konsequenzen für die Unternehmensnetze

Die momentane Situation bei IEEE 802.11n ist alles andere als befriedigend. Der MIMO-Werbegag eignet sich in keinster Weise für die Eingliederung in ein seriöses Planungskonzept.

Die Diskussion über mögliche andere Verfahren, die eine sinnvolle nachrichtentechnische Grundlage haben, wird durch die aktuellen Vorgänge behindert. Ich bin nicht optimistisch, dass wir vor Mitte 2006 irgendetwas Brauchbares aus dieser Arbeitsgruppe zu erwarten haben.

Bis dahin sollte die Planung ausschließlich auf IEEE 802.11h basieren und ggf. noch das Problem der Einbeziehung bestehender 802.11b-Lösungen betrachten.

Ärgerlich ist vor allem, dass sich IEEE 802.11n offensichtlich nicht zuständig für die Entwicklung von Kanalsteuerungsverfahren hält, die VoWLAN unterstützen. Es gibt zwar stark geheim gehaltene Herstellerkonzepte dafür, aber eine standardisierte Lösung steht penetrant aus.

Der Lösungsansatz, auch dieses Problem einfach mit Bandbreite zu erschlagen oder eine Priorisierung nach IEEE 802.1p vorzuschalten, wird fehlschlagen.

Ohne VoWLAN bleiben flächendeckende WLAN-Konzepte jedoch nur eine halbe Sache. Befaßt man sich aber mit dem Problem der VoWLAN-Realisierung näher, erlebt man eine Reihe von Überraschungen. Das werden Sie in meinem nächsten Artikel sehen.

Sonderveranstaltung

Business Service Management ExpertDays 2005

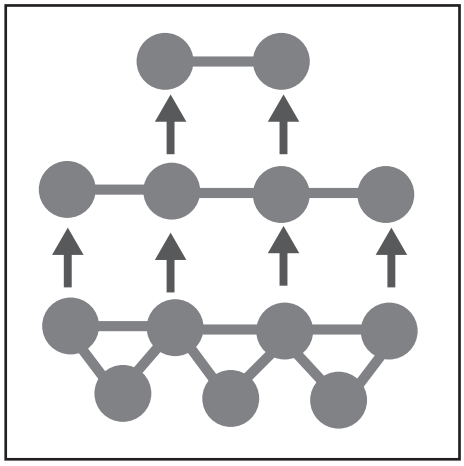
Die ComConsult Akademie veranstaltet vom 27.06. - 28.06.05 erstmalig die „Business Service Management ExpertDays 2005“ in Köln.

Mit den Business Service Management (BSM) ExpertDays 2005 wollen wir Ihnen erstmalig die Gelegenheit geben, das marktbestimmende Thema Business Service Management neutral und kompetent aufbereitet in komprimierter Form zu durchleuchten.

Die BSM ExpertDays 2005 analysieren die aktuellsten Entwicklungen im Business Service Management und bewerten Markttrends und Produktentwicklungen.

Im Mittelpunkt der BSM ExpertDays 2005 stehen u.a. die folgenden Fragen

- Was ist Business Service Management? Für wen lohnt sich Business Service Management?
- Ist Business Service Management wirklich etwas Neues oder nur ein neuer Begriff für alte Ideen?
- Wie unterscheidet sich Business Service Management von früheren System- und Service-Management-Ansätzen?
- Was sind die Kernmerkmale einer Business Service Management Architektur?
- Wie setzt man ein Business Service Management Projekt auf? Worauf muss man hier besonders achten?
- Welche Produktstrategien verfolgen die Key Player auf dem Business Service Management Markt? Gibt es hier Unterschiede?



Die BSM ExpertDays 2005 bieten Ihnen hochaktuelle Aussagen in Form von

- Neutrale Meinungen zum BSM-Markt hochkarätiger Analysten, seiner aktuellen Stellung und zukünftigen Entwicklung,
- Erfahrungsberichte von Kunden, die sich mit BSM bereits beschäftigt haben oder aktuell in der Einführungsphase sind,
- Hersteller-Statements zu zukünftigen Produkt- und Marktstrategien,
- Projektberichte aktueller Implementierungen

Aufgrund der Aktualität und Internationalität werden einzelne Vorträge in englischer Sprache gehalten!

Mit dieser 2-Tages-Veranstaltung kommen Sie schnell auf den aktuellen Diskussionsstand, die vermittelten Inhalte ermöglichen Ihnen den schnellen Einstieg in ein toprelevantes Thema. Die Veranstaltung wendet sich nicht nur an IT-Manager, sondern auch an alle Service-Verantwortlichen (Service Manager, Prozess-Verantwortliche, Service Sales Einrichtungen...) von Unternehmen und Service Providern sowie deren Kunden.

Zögern Sie nicht und sichern Sie sich einen Platz auf unserer Top-Veranstaltung des Jahres 2005.

Moderatoren
Ralf Horstmann, Dipl.-Kfm. Martin Woyke

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Business Service Management ExpertDays 2005

☐ Ich buche das Seminar **Business Service Management ExpertDays 2005**
vom 27.06. - 28.06.05 in Köln
zum Preis von € 1.490,- zzgl. MwSt.

☐ Bitte reservieren Sie für mich
ein Hotelzimmer
vom_____bis_____05

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.com

_____ Vorname	_____ Nachname
_____ Firma	_____ Telefon/Fax
_____ Straße	_____ PLZ,Ort
_____ eMail	_____ Unterschrift

Report des Monats inklusive Seminar

Planung Elektrosmog-reduzierter WLANs Das TERW-Konzept

Neue europäische Studien belegen, dass es ein generelles gesundheitliches Risiko durch Einwirkung von Elektrosmog gibt. Die Ergebnisse dieser Studien gehen weit über die bisherigen Annahmen hinaus, so dass in den nächsten Monaten auch seitens der Betriebsräte und der Benutzer mit einer verstärkten Diskussion zu rechnen ist. Wir haben diese Studien analysiert und geben konkrete Empfehlungen für deren Handhabung.

Wireless LANs sind von dieser Diskussion stark betroffen, führen sie doch stufenweise zu einer flächendeckenden Belastung. Auch unter Berücksichtigung der Ergebnisse der neuen Studien ist ein Einsatz von WLANs generell möglich und sinnvoll. Allerdings sollten angemessene technische Grenzwerte berücksichtigt werden.

Angesichts der Dringlichkeit des Themas hat sich die ComConsult Research in Zusammenarbeit mit der ComConsult Akademie dazu entschlossen, Ihnen eine Sonderveranstaltung anzubieten. Diese ist mit dem Preis der Studie identisch, so dass Sie hier zum Preis der Studien quasi kostenfrei die Möglichkeit erhalten, sich vom Autor die Ergebnisse erläutern zu lassen und entsprechend zu diskutieren.

In einer topaktuellen Exklusivstudie haben wir für Sie untersucht:
- Welche Erkenntnisse lassen sich aus den neuen Studien ableiten
- Welche Grenzwerte sollten Sie in ihrer Planung von WLAN-Infrastrukturen berücksichtigen
- Was bedeutet das konkret für die Auslegung von Wireless-Funkzellen

Im Ergebnis kommt die Studie zu einem völlig neuen Planungsansatz für Wireless-Netzwerke, den wir als “Three Zone Electrosmog Reduced Wireless Networks, das TERW Zonen-Konzept” bezeichnet haben. Der Autor der Studie ist Dr. F.-J. Kauffels, der generell nicht im Verdacht steht, Gefahren durch Esmog über zu bewerten.

Interessant sind die Ergebnisse naturgemäß auch für den Bereich der Handy-Nutzung. Hier wird immer deutlicher, dass eine intensive Nutzung des Handys mit hohen gesundheitlichen Risiken verbunden ist. Unabhängig von der persönlichen Risiko-

Bewertung des Einzelnen stellen die Ergebnisse der neuen Studien Unternehmen vor ein immer größeres Problem. Gestatten sie ihren Mitarbeitern eine intensive Handy-Nutzung oder ist diese sogar untrennbar mit dem Job verbunden, besteht durchaus das Risiko einer zukünftigen Haftungssituation.

Auch hier setzt die neue Studie von ComConsult-Research mit dem neuen Planungsansatz an. Ein konsequenter Ersatz der GSM-Technik durch Voice-over-Wireless führt auch nach traditionellen Planungsansätzen zu einer massiven Senkung der Belastung. Wird dann auch noch der neue in der Studie ausgearbeitete TERW-Ansatz berücksichtigt, entsteht eine signifikante Reduktion der Belastung. Entsprechende Dual-Mode-Geräte, die sowohl GSM als auch VoWLAN unterstützen, kommen zur Zeit vermehrt auf den Markt. Sie haben allerdings den Nachteil, dass sie eine IP-Telefonie-Installation voraussetzen.

Inhaltsschwerpunkte sind:
Wireless World: Technologien und Potenziale
- Wireless World - Übersicht, Anwendungen
- WLANs: aktueller Stand
- IEEE 802.16 WiMAX
- IEEE 802.20

Neue Wireless-Technologien und Elektrosmog
- Wichtige aktuelle Studien und Empfehlungen
- Die NRBP-Empfehlungen, UK 2005
- EU-Aktivitäten
- Die REFLEX-Studie
- Zur Problematik von Grenzwerten

Planungsaspekte
- Einflussfaktoren
- Entwicklung der Campus-Netze
- Planungshilfen
- Ergebnisse der ComConsult Metastudie 2002
- RF-EMF-Belastung durch andere Kommunikationsdienste
- Weitere Verbesserungsmöglichkeiten durch neue WLAN-Konzepte
- Der Einfluss von WiMAX
- Zusammenfassende Planungsaspekte

Three Zone Electrosmog Reduced Wireless Networks: das TERW-Konzept
- Die TERW-Zonendefinition
- „Traditioneller“ Wireless Ansatz
- Drahtlose Voice Kommunikation heute
- TERW-Zonenplanung
- Infrastrukturfähige belastungsminimierte WLAN-Zellen
- Voice und WiMAX
- Kostenvergleich

Fazit

Motivation
Die neuen Kommunikationsmöglichkeiten durch WLANs und WiMAX sind wirtschaftlich und operationell ausgesprochen attraktiv und werden sich noch schneller als bisher ausbreiten. Weltweit rechnet man mit einem Wachstum von ca. 20% pro Jahr. Der eigentliche Durchbruch gegenüber bisherigen WLAN-Systemen geschieht durch die Möglichkeit der Bildung geschlossener Wireless Infrastrukturen im Rahmen einer Wireless Hierarchie. Die für ein individuelles Endgerät erzielbaren Datenraten liegen bei derartigen Lösungen weit höher als bei den bekannten Systemen, die auf GPRS oder UMTS basieren. Wegen der vergleichsweise geringen Reichweiten ist allerdings der Aufbau einer flächendeckenden Wireless Infrastruktur erforderlich. Diese wird innerhalb von Unternehmen und Organisationen die bisher kabelbasierten Lösungen mittelfristig verdrängen. Alle neuen Endgeräte werden in Weiterführung des mit der Centrino-Technologie entwickelten Grundgedankens standardmäßig mit Schaltkreisen ausgerüstet sein, die eine Einbindung in die Wireless-Infrastrukturen ermöglichen. Es

gibt eine Reihe von kommerziell ausgesprochen interessanten Kernanwendungen, die ausschließlich durch die neue Wireless Infrastruktur unterstützt werden können, wie z.B. die „funkenden Etiketten“ RFID, die die Logistik revolutionieren werden. Die allgemeingültigste Killer-Applikation ist „Voice over Wireless“ in Weiterführung der bisherigen VoIP-Entwicklungen. VoWLAN kann in Unternehmen und Organisationen GSM-Handys substituieren und insgesamt erhebliche Kostenvorteile mit sich bringen. Entsprechende Endgeräte werden schon Anfang 2005 vorgestellt.

Die Ausbreitung von Wireless-Infrastrukturen wirft die Frage nach der Belastung von Menschen durch die entstehenden elektromagnetischen radiofrequenten Felder (RF-EMF) auf.

Generell ist ein sensibler, vorsorgeorientierter Umgang mit diesen Fragestellungen nützlich und entspricht den Empfehlungen von WHO, EU-Kommission und anderen Institutionen. Es gibt nur wenige Aussagen zur Belastung durch WLAN-RF-EMF. Erschwerend bei der Erschließung der Thematik sind unterschiedliche Quantifizierungen in Radiotechnik und Dosimetrie. Neue Studien zeigen, dass die z.B. im Rahmen der CE-Zertifizierung vorgeschriebenen Grenzwerte für RF-EMF unter Umständen nicht ausreichend sind, um Wirkungen innerhalb menschlicher Körper mit Sicherheit völlig auszuschließen. Innerhalb der Studien ergeben sich jedoch auch Werte, bei denen keine Belastung mehr festzustellen ist. Dies ist jedoch kein endgültiges Kriterium, weil ein Negativbeweis aus theoretischen Gründen nicht möglich ist.

Die aktuelle WLAN-Technologiegeneration liegt hinsichtlich der RF-EMF Feldstärke und der durch sie entstehenden spezifischen Absorptionsrate im menschlichen Gewebe jedoch um Faktoren zwischen 1.000 und 100.000 unter den Grenzwerten, die entstehen, wenn man die neuen Studien berücksichtigt. Schon mit dieser Technologiegeneration ist eine Planung mit möglichst geringer persönlicher Belastung möglich und sinnvoll. Allerdings müssen die Kommunikationseinrichtungen von Hand einzeln kalibriert werden.
Neue Standards wie IEEE 802.11 h und n sowie IEEE 802.16 WiMAX ermöglichen eine hinsichtlich der RF-EMF-Belastung weiter optimierte und im Betrieb automatisch kalibrierende kabellose Infrastruktur.Die Optimierung der Belastung hinsichtlich minimal möglicher Werte setzt die Beachtung einiger wesentlicher, einfacher Grundregeln ganz früh im Designprozess voraus.Insgesamt sind mit den neuen Technologien Versorgungsstrukturen denkbar, deren Gesamtbelastung bei gleicher oder erweiterter Funktionalität weit unter der durch existierende kabellose Systeme wie GPRS, UMTS oder DECT liegt.
Das in der Studie eingeführte TERW-Designkonzept unterstützt die Planung funktional reichhaltiger und gleichzeitig besonders belastungsarmer drahtloser Infrastrukturen in einer frühen Stufe.
Eine Planung unter besonderer Berücksichtigung der Minimierung der persönlichen RF-EMF-Belastung führt zu einem System, welches, wenn überhaupt, nur marginale Mehrkosten gegenüber einem funktional äquivalenten Design, welches auf die Belastung keine Rücksicht nimmt, aufweist.

Eine Befolgung des TERW-Designkonzepts kann dazu beitragen, die durchschnittlichen jährlichen Kosten der drahtlosen Kommunikation eines Unternehmens oder einer Organisation auf etwa 20% der bisherigen Kosten zu drücken und gleichzeitig die RF-EMF-Belastung durchschnittlich um den Faktor 100 - 200 zu senken. Ein wesentliches Instrument in diesem Zusammenhang ist die Substitution von betriebsintern genutzten GSM-Handys durch VoWLAN-“Handys“ und die Einführung einer drahtlosen „Voice Ready“ Infrastruktur.

Da Elektrosmog völlig unabhängig von der - z.Zt. nicht mit Sicherheit endgültig abzuklärenden - Beantwortung der Frage, ob und ab welchen Grenzwerten er eine nachweisbar negative Auswirkung auf den menschlichen Organismus hat, für nichts weiter nutze ist, sollte man von Anfang an darauf hinwirken, ihn so weit wie möglich zu minimieren.

Autor und Referent
Dr. Franz-Joachim Kauffels ist einer der erfahrensten und bekanntesten Referenten der gesamten Netzwerkszene (über 20 Fachbücher und unzählige Artikel) und bekannt für lebendige und mitreißende Seminare.

Fax-Antwort an ComConsult 02408/955-399

Bestellung/Anmeldung

Planung Elektrosmog-reduzierter WLANs - Das TERW-Konzept

☐ Ich bestelle den Report

Planung Elektrosmog-reduzierter WLANs - Das TERW-Konzept
(Preis € 998.-- zzgl. MwSt. und Versand)

☐ Gleichzeitig nehme ich kostenfrei an der gleichnamigen Veranstaltung am 27.06.05 in Bonn teil.

☐ Bitte reservieren Sie für mich ein Hotelzimmer vom_____bis_____05

Bestellen Sie über unsere Web-Seite **www.comconsult-research.de**

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

Schwerpunktthema

Messung der VoIP-Tauglichkeit von Netzwerken

Fortsetzung von Seite 1

Im Anschluss an sein Studium als Nachrichtentechniker spezialisierte sich Dipl.-Ing. Hartmut Kell auf die Datenkommunikation in lokalen Netzen und kann bis heute auf eine mehr als 10-jährige Berufserfahrungen in diesem Bereich verweisen. Als langjähriger Mitarbeiter der ComConsult Beratung und Planung GmbH hat er umfangreiche Praxiserfahrungen bei der Planung, Projektüberwachung, Qualitätssicherung und Einmessung von Netzwerken gesammelt. Ergänzend zu diesen projektbezogenen Arbeiten vermittelt Herr Kell sein umfangreiches Fachwissen in Form von Fachpublikationen und Seminaren.

Der vorliegende Artikel wird ein Messverfahren mit dem Chariot-System der Firma Ixia (ehemals bei NetIQ) beschreiben, mit dem man prüfen kann, ob ein vorhandenes Netz eine VoIP-Tauglichkeit besitzt oder nicht. Anhand von Szenarien, die in einem kleineren Netz praktisch angewendet wurden, werden die Möglichkeiten der Auswertung und Interpretation veranschaulicht. Erfahrungen, die ComConsult Beratung und Planung GmbH im Rahmen von erbrachten VoIP-Readiness-Überprüfungen vor Ort gemacht hat schließen den Artikel ab.

Bevor man sich mit den Möglichkeiten zur Eignungsprüfung auseinandersetzt sind zuerst einmal die Parameter zu betrachten und definieren, die für die Sprachqualität einer VoIP-Anwendung relevant sind.

Komponenten einer VoIP-Lösung

Die Abwicklung von Sprachanwendungen über IP-Netze unter Einhaltung der Anforderungen im Bereich Sprachqualität und Verfügbarkeit setzt den Einsatz verschiedener Komponenten voraus, auf die im Folgenden eingegangen wird.

Zunächst muss ein Signalisierungsprotokoll dafür sorgen, dass Gespräche auf- und abgebaut werden. Die Aufgaben der Signalisierungsprotokolle sind die Lokalisierung des Kommunikationspartners, der Auf- und Abbau der Verbindung, die Aushandlung der Verbindungsmerkmale wie Kompressionsverfahren, die Verwaltung von Hinzufügen und Entfernen von Konferenzteilnehmern im Falle von Telefonkonferenzen und die Implementierung von bestimmten Dienstmerkmalen wie Weiterleitung von Anrufen. Zur Lokalisierung von Kommunikationspartnern und bestimmten Ressourcen im Netz müssen Verzeichnisdienste in einem IP-Netz genutzt werden.

Die zuverlässige Nutzung eines Netzes für VoIP setzt voraus, dass bestimmte Gütekriterien eingehalten werden, dies genau kann das hier beschriebene Testverfahren verifizieren. Die beim Testverfahren berücksichtigten VoIP-Komponenten bzw. der damit aufgebaute Übertragungspfad sind im nachfolgenden dargestellt. (siehe Abbildung 1)

Sprachsignale sind akustische, analoge Informationen, die zwecks Übertragung über ein digitales Paketnetz in digitale Signale umgewandelt (kodiert) und auf der Empfängerseite wieder als akustische Signale interpretiert (dekodiert) werden müssen. Dabei können die digitalen Signale auch komprimiert werden. Die tatsächliche Übertragung von Sprachsignalen erfolgt in einem Paketnetz mit Hilfe eines Transportprotokolls, das z. B. für das Versehen der Pakete mit Zeitstempeln und / oder Sequenznummern sorgt. Das analoge Audiosignal wird mithilfe eines sogenannten Encoders digitalisiert. Am Ausgang des Encoders liegt dann ein Bitstrom vor, der zur Übertragung über ein IP-Netz in Pakete zu zerlegen ist. Diese Pakete werden über das IP-Netz übertragen und beim Empfänger zunächst einmal zwischengespeichert, damit sich der Empfänger mit dem Sender synchronisieren kann und die Laufzeitschwankungen

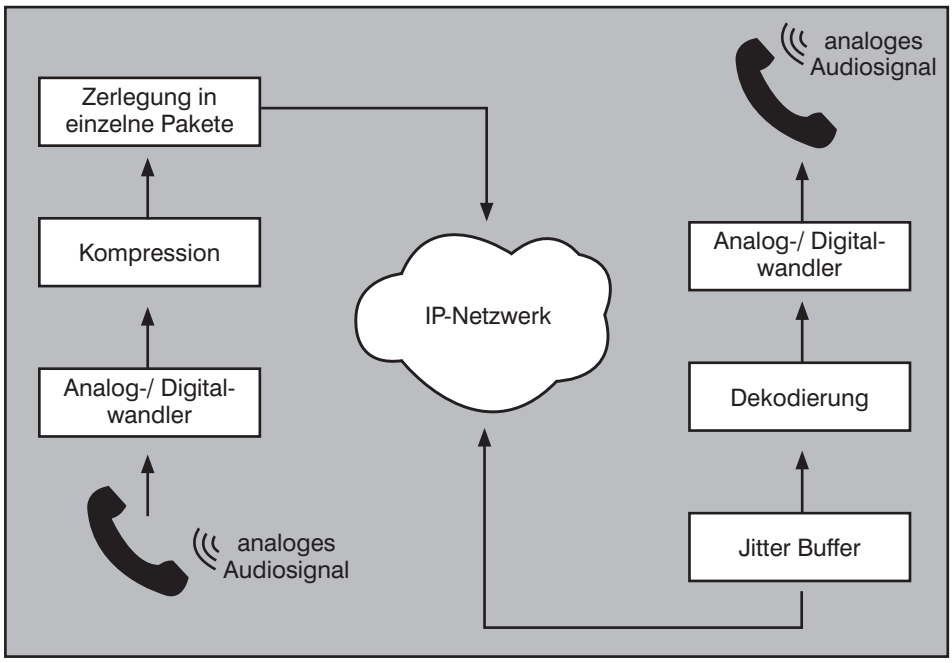


Abbildung 1

im Netz kompensiert werden können. Erst durch diese Zwischenspeicherung kann ein kontinuierlicher Bitstrom mit der selben Taktrate wie vom Sender erzeugt hergestellt und dem sogenannten Decoder übergeben werden. Dieser gewinnt aus dem digitalen Signal das Audiosignal zurück.

Die Bereiche Codecs und Paketierung von VoIP sind weitgehend standardisiert und basieren auf der G.7xx-Standardfamilie und RTP/RTCP (Realtime Transport Protocol / Realtime Transport Control Protocol). Bevor diese Standards und die darin spezifizierten Verfahren und Mechanismen beschrieben werden, sind zunächst die 3 elementaren Parameter zu analysieren, die für eine gute Sprachqualität relevant sind: Verzögerung (Delay), Verzögerungsschwankungen (Jitter) und Paketverluste (Packet Loss).

Kritischer Parameter: Delay

Die sensiblen Benutzer empfinden Verbindungen mit Delays von mehr als 150 ms „vom Mund zum Ohr“ als eine Art „Wechselsprechen“ und nicht als interaktives Gespräch. Maßgeblich für die Aufstellung eines sogenannten Delay Budgets für einen Netzbetreiber ist daher die Grenze 300 ms für die Signalumlaufzeit, d. h. 150 ms für den Weg vom Sprecher zum Hörer. Insbesondere die Wartezeiten der Pakete in Koppelelementen (Switches, Router etc.) und die unterschiedlichen Übertragungswege erzeugen in einem Netz einen variablen, schwer vorzubestimmenden Anteil an Verzögerung (Delay). Dieser Anteil ist im Wesentlichen von der Auslastung der Netze auf der Strecke vom Sender zum Empfänger abhängig. Je höher die Auslastung, desto größer die Paketlaufzeit. Aber selbst bei einer Auslastung gegen 0 % muss mit einem Verzögerungsanteil ungleich 0 gerechnet werden, da jede Netzkomponente grundsätzlich eine nicht infinitesimale Zeit für die Verarbeitung des Paketes benötigt. In einem theoretischen Ansatz wird mit einer Faustregel davon ausgegangen, dass pro Netzkomponente (Switch oder Router) eine Millisekunde als Verzögerung zu berücksichtigen ist.

Es lässt sich leicht vorstellen, dass wie beschrieben ein zu hohes Delay einen unmittelbaren Einfluss auf die Sprachqualität nehmen kann. Interessanterweise übt das Delay aber auch einen direkten bzw. indirekten Einfluss auf die beiden weiteren Kenngrößen „Verzögerungsschwankung“ (Jitter) und „Paketverlust“ (Packet Loss) aus.

Kritischer Parameter: Jitter

Bestimmte Bestandteile der Verzögerung sind fest, und zwar in der Regel jene Bestandteile, die mit der Kodierung und Dekodierung zusammenhängen. Die durch das Netz verursachte Verzögerung ist jedoch variabel. Der variable Anteil der Verzögerung (d. h. die Laufzeitschwankung) wird mit dem Begriff „Jitter“ umschrieben. Jitter führt dazu, dass die vom Kodierer erzeugten Pakete unterschiedlich schnell beim Dekodierer ankommen. Der Dekodierer ist jedoch auf einen quasi kontinuierlichen Paketstrom angewiesen, um auch einen kontinuierlichen Bitstrom als Voraussetzung für ein nicht verzerrtes Audiosignal generieren zu können. Daher müssen zum Ausgleich der Laufzeitschwankungen im Netz Puffer an Empfängern implementiert werden, sogenannte Jitter Buffer. Im Jitter Buffer werden die Pakete kurzzeitig gespeichert und dann gleichmäßig weitergeleitet. Ist dieser Jitter Buffer zu klein, kann er die Schwankungen nicht auffangen; die Sprachqualität sinkt. Ist dieser Jitter Buffer zu groß und die Paketlaufzeit erhöht sich zu sehr, sinkt die Sprachqualität ebenfalls. Beispiel: Beträgt die Laufzeitschwankung im Netz 10 ms, müssen die ankommenden Pakete für genau diese Zeit zwischengespeichert werden. Man stelle sich vor, auf ein besonders „schnelles“ Paket folgt ein besonders

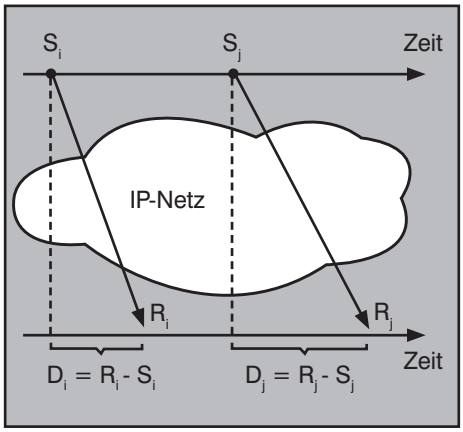


Abbildung 2

„langsames“ Paket. Die Ankunftszeit dieser beiden Pakete wird dann um maximal 10 ms länger auseinanderliegen als die Zeit zwischen der Generierung des ersten und der Generierung des zweiten Paketes. Das erste Paket muss daher künstlich um 10 ms verzögert werden, wofür der Jitter Buffer sorgt.

Der Wert des Jitters wird mit Hilfe einer Formel aus dem RFC 1889 berechnet und diese lässt sich relativ einfach am nachfolgenden Bild (Quelle: www.gandalf.interest.de) erläutern (s. Abb. 2).

Die obere Zeitachse kennzeichnet den Sendezeitpunkt eines Signals S, die un-

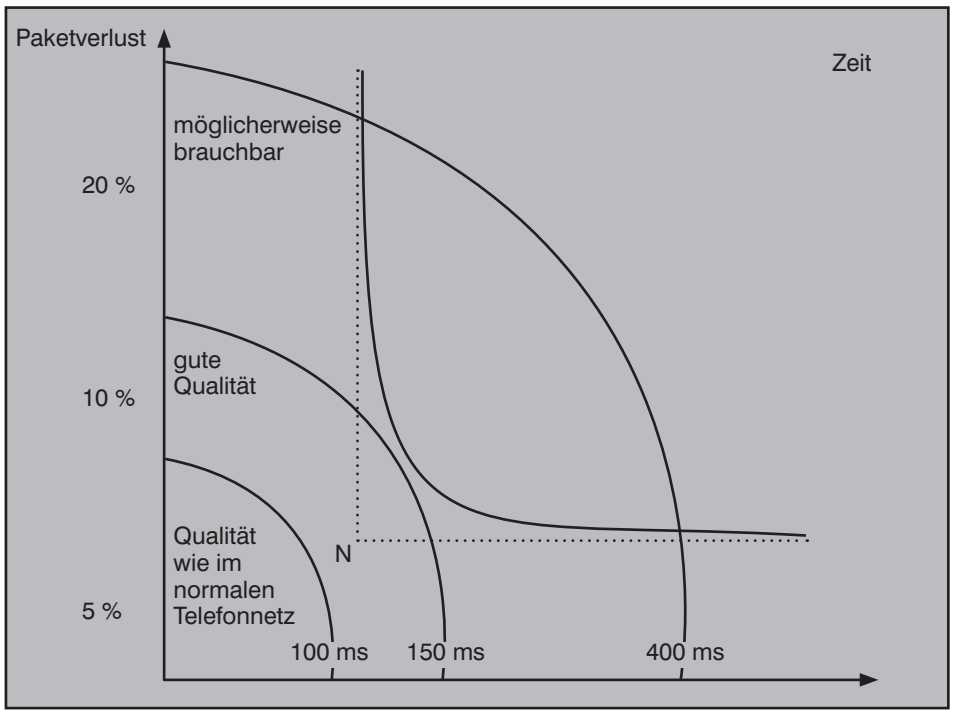


Abbildung 3: Zusammenhang zwischen Delay, Paketverlust und Sprachqualität

tere Zeitachse den Empfangszeitpunkt R. Der Wert D beschreibt jeweils den Zeitunterschied zwischen Senden und Empfang. Bei zwei unterschiedlichen Signalen kann dieser Wert D ebenfalls unterschiedlich sein. Die Differenz des Wertes D für beide Signale ergibt den Jitter J:

$$J(j,i) = D_j - D_i = (R_j - S_j) - (R_i - S_i) = (R_j - R_i) - (S_j - S_i)$$

Die bereits im Absatz „Delay“ beschriebenen Probleme bei Verwendung von Analysatoren verhindern ebenfalls, dass ein reiner Analysatoreinsatz zu einer VoIP-Tauglichkeitsmessung eines Netzes unter Berücksichtigung der spezifischen Größe „Jitter“ herangezogen werden können. Der Jitter Buffer als einstellbarer Bestandteil des VoIP-Endgerätes ist nicht zwangsläufig Gegenstand der Tauglichkeitsprüfung eines Netzes, doch es wäre sehr sinnvoll, zu testen wie sich ein VoIP-Datenverkehr bei unterschiedlichem Jitter Buffer verhält, auch dies kann natürlich mit herkömmlichen Analysatoren nicht untersucht werden.

Kritischer Parameter: Paketverlust

Wie bei jeder Applikation ist auch bei VoIP damit zu rechnen, dass Pakete verloren gehen können. Da aber VoIP keinen verbindungsorientierten Dienst bietet, erfährt der Sender nicht vom Verlust eines Paketes. Neben einem Übertragungsfehler kann auch hier eine zu hohe Netzlast (im Vergleich zur bereitgestellten Bandbreite) die Fehlerursache sein. Zusätzlich gibt es jedoch bei VoIP noch einen weiteren, speziellen Grund: Treffen bedingt durch Jitter (also letztendlich durch Delay) die Pakete am Ziel zeitlich so verzögert ein, dass der Empfänger trotz eines Jitter Buffers nicht mehr in der Lage ist, alle Pakete zu erfassen, so wird er die am langsamsten eintreffenden Pakete möglicherweise verwerfen. Stellen diese aber einen Bestandteil der Anfangssequenz im VoIP-Stream dar, so werden auch die vorausgegangenen und im Jitter Buffer gespeicherten Pakete nicht weiter genutzt werden können. Es kommt zu Qualitätseinbußen bei der Sprache, die insbesondere über mehr oder weniger starke Sprachlücken bemerkt werden. Da hilft im ersten Schritt die Vergrößerung des Buffers, doch hat dieses wiederum einen höheren Delay für den gesamten Kommunikationspfad zur Folge.

Den Zusammenhang zwischen Delay, Paketverlust und Sprachqualität zeigt u.a. Abbildung 3.

Auf der horizontalen Achse ist der Delay dargestellt, auf der vertikalen Achse die prozentuale Verlustrate bei den Paketen. Je nach Kombination dieser beiden Werte ist die Sprachqualität sehr gut, gut oder bedingt brauchbar.

Ist die Laufzeit des Signals sehr klein, können mit aufwändigen Dekodierungsmaßnahmen die Paketverluste zu einem Teil ausgeglichen werden, sodass auch bei relativ hohen Paketverlusten die Qualität des Sprachsignals verbessert werden kann. Dieser Spielraum sinkt mit steigenden Delay-Werten. Andererseits ist bei sehr niedrigen Paketverlustraten eine aufwändige Kodierung nicht erforderlich, sodass mehr Spielraum für Netz-Delay übrig bleibt. Dieser Spielraum sinkt mit steigender Paketverlustrate, die vom Kodierungsverfahren ausgeglichen werden muss.

Es stellt sich jetzt die Frage, ob es im Falle eines angenommenen oder gar bekannten geringen Paketverlustes Verfahren gibt, diesen zu kompensieren. Derartige Verfahren werden unter dem Oberbegriff PLC (Packet Loss Concealment) zusammengefasst, allen Verfahren gemeinsam ist, dass sie nur einen geringen Paketverlust kompensieren können. Zu nennen sind folgende Verfahren:

- Silence Substitution oder Silence Insertion: Es wird bei der Dekodierung eine Zwangspause im Sprachfluss eingerichtet.
- Packet Repetition oder Replay Last Packet: Das letzte korrekt empfangene Sprachpaket wird nochmals wiedergegeben. Dazu wird ein Teil des Paketes in die Lücke eingespielt und der Pegel schrittweise gedämpft. Der gleitende Übergang in das nachfolgende, richtig empfangene Paket soll die Störwirkung reduzieren.
- Packet Repetition: Die verlorenen Pakete werden durch ein synthetisches Sprachmodell abgeschätzt (funktioniert gut bei G.723.1 und G.729, schlecht bei G.711).
- Forward Error Correction: Das n-te Paket enthält das n-1-te Paket in komprimierter Form (Nachteil: Höhere Bandbreite und Verzögerung).
- Frame Interleaving: Sprachrahmen werden auf verschiedene Pakete aufgeteilt.

Die jeweilige Art der Kompensation wird durch den Codec bereitgestellt. Tests zeigen, dass bei hinsichtlich PLC besonders ausgereiften Kodierungsverfahren bis zu 10 % unkorrelierter Verlust wenig Einfluss auf die Qualität der Sprachübertragung haben (unkorrelierter Verlust liegt dann vor, wenn z. B. keine längeren Paketverlustphasen (loss bursts) vorkommen). Da jedoch davon auszugehen ist, dass im LAN zum Erreichen einer optimalen Sprachqualität möglicherweise auf Kompression und aufwändige Kodierung

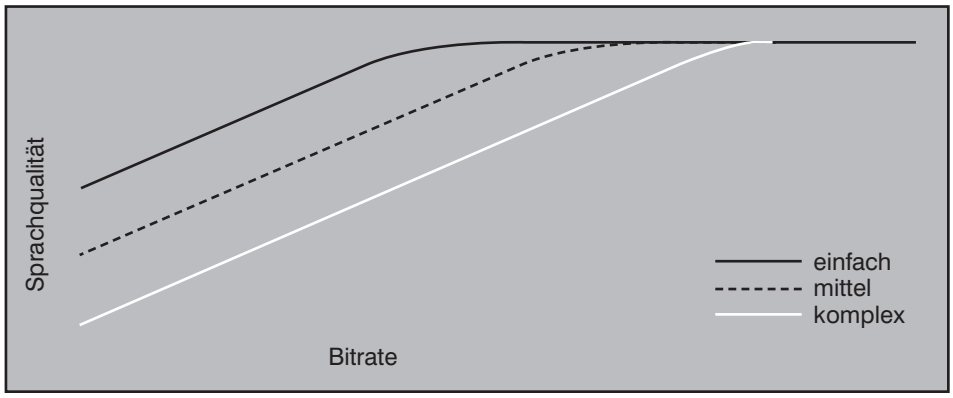


Abbildung 4: Abhängigkeit der Sprachqualität von der Bitrate und Kodierung

verzichtet wird, sollten die Anforderungen der sensibelsten Codecs an maximale Verlustraten zum Maßstab gemacht werden. Hier ist ein maximaler Verlustwert von 1 % ausschlaggebend.

Sprachkompression

In jedem Netz ist die verfügbare Bandbreite endlich und muss dazu noch von vielen Kommunikationspartnern geteilt werden. Da der Mensch seit der Erfindung der Telefonie eine schlechtere Sprachqualität im Vergleich zur Kommunikation von Angesicht zu Angesicht akzeptiert, arbeiten die TK-Lösungen immer mit Verfahren zur Begrenzung der für die Sprachübertragung erforderlichen Bandbreite, um den Aufwand für die Realisierung der Netze, der mit der erforderlichen Bandbreite steigt, in Grenzen zu halten. Eine analoge Telefonleitung hat z. B. eine begrenzte Bandbreite und dämpft die Signalanteile mit hoher Frequenz, die in der menschlichen Stimme enthalten sind. Im digitalen Netz bedeutet allein die Kodierung mit endlicher Abtastrate eine Reduzierung der zu übertragenden Informationsmenge.

Aber selbst diese reduzierte Informationsmenge pro Zeiteinheit (64 kbit/s) muss zwecks Übertragung über schmalbandige Medien wie z. B. Mobilfunk weiter reduziert werden. Dies erfolgt durch die sogenannte Kompression. Bei jeder Kompression werden die sich wiederholenden Bitsequenzen durch die Angabe der Sequenz und der Anzahl der Wiederholungen ersetzt. Dies reicht zur 1:1-Wiederherstellung des Signals aus. Bei der Sprachübertragung muss jedoch das Signal nicht 1:1 wiederhergestellt werden, da dem menschlichen Hörer leichte Modifizierungen des Signals nicht auffallen. Somit entsteht ein weiteres Kompressionspotenzial durch diese Anpassungen. Im Mobilfunkbereich ist beispielsweise ein Kompressionsfaktor von acht üblich, d. h. bei einem digitalisierten Signal mit der Bitrate 64 kbit/s arbeitet das tatsächlich übertragene Signal mit 8 kbit/s.

Bei gleichem Kompressionsalgorithmus gilt: Je stärker die Kompression und damit je höher der Kompressionsfaktor, desto größer sind die Abweichungen des übertragenen Signals vom ursprünglichen Signal. Ein weiteres Optimierungspotenzial gibt es jedoch auch beim Kompressionsalgorithmus. Aufwändige Kompressionsalgorithmen können bei gleicher Sprachqualität im Vergleich zu einfachen Algorithmen höhere Kompressionsfaktoren erreichen. Je einfacher der Algorithmus, desto kleiner ist der erzielbare Kompressionsfaktor bei gleicher Sprachqualität.

Der Zusammenhang zwischen Kompressionsfaktor (Einsparung der erforderlichen Bandbreite), Komplexität des Algorithmus und der Sprachqualität ist in Abbildung 4 dargestellt.

Wenn man z. B. eine bessere Sprachqualität erreichen möchte, muss man entweder eine höhere Bitrate bei der Übertragung vorsehen oder einen komplexeren Kompressionsalgorithmus einsetzen. Dabei ist ein komplexerer Kompressionsalgorithmus stets mit einem größeren Zeitverzug bei der Kodierung und Dekodierung verbunden, sodass den über komplexere Algorithmen erzielbaren Einsparpotenzialen Grenzen gesetzt sind.

In geswitchten LANs kann in der Regel G..711 zum Einsatz kommen, da solche LANs genügend Kapazität für den Verzicht auf Kompression bieten. Es ist jedoch zu berücksichtigen, dass mit 64 kbit/s nur eine Nettorate angegeben ist, zu der ein Paketierungs-Overhead hinzu kommt; dieser Overhead beträgt ca. 23 kbit/s.

Gesamtbeurteilung der Sprachqualität mit Hilfe von MOS und R-Faktor

Die Klarheit der Sprache (Erkennung von Lauten und Wörtern, Erkennung der Stimme des Kommunikationspartners, Erkennung von Nuancen wie „Untertöne“ etc.) ist relativ schwer zu quantifizie-

ren. Ein bereits genutztes Verfahren dazu wird als „Mean Opinion Score“ (MOS) bezeichnet und basiert auf der subjektiven Bewertung der Sprachqualität durch eine Referenzgruppe von Menschen. Auf einer Skala zwischen 1 und 5 wird die Sprachqualität bewertet, wobei ein höherer Wert einer besseren Qualität entspricht.

Alternativ zum empirischen und daher aufwändigen MOS-Verfahren können jedoch heute auch analytische Verfahren der Qualitätsmessung eingesetzt werden. Diese Verfahren werden vor allem von Entwicklern eingesetzt und dienen dazu, das Verhalten von Kodierern / Dekodieren (Codecs) und anderen Komponenten einer VoIP-Umgebung im Labor zu testen, ohne eine MOS-Bewertung durchführen zu müssen. Im Zusammenhang mit dem in diesem Artikel beschriebenen Verfahren zur VoIP-Tauglichkeitsprüfung eines Netzes stellt die analytische MOS-Bewertung ebenfalls eine Basis dar, um die Qualität des Netzes zu beurteilen. Diese Bewertung berücksichtigt nicht nur die „netzspezifischen“ Anteile wie Delay, Jitter und Packet Loss sondern auch die abschließenden Kodierungsverfahren und z.B. auch die Jitter Buffer Größe, die je nach Wahl und Spezifikation gegebenenfalls schlechte „Netzkennwerte“ kompensieren könnten.

Die analytischen Verfahren zur Beurteilung der Sprachqualität teilen sich in zwei Haupttypen auf, den Verfahren auf Basis eines „Perceptual Models“ und den Verfahren auf Basis eines „E-Models“. Beim ersteren wird im Prinzip das empfangene Sprachsignal mit dem gesendeten verglichen und auf dieser Basis erfolgt eine Bewertung.

Ein Beispiel für ein solches analytisches Verfahren ist in dem von der International Telecommunications Union (ITU) herausgegebenen Dokument ITU-T P.861 unter dem Titel „Perceptual Speech Quality Measurement (PSQM)“ beschrieben. Ein weiteres Verfahren mit dem Namen „Perceptual Analysis/Measurement System (PAMS)“ wurde von British Telecom entwickelt. Beide Verfahren simulieren Sprachsignale und messen die Veränderungen, die durch den zu testenden Sprachkanal verursacht werden. Bei der Simulation wird auf die repräsentative Mischung aus männlichen und weiblichen Stimmen und aus verschiedenen Lauten geachtet.

Grundsätzlich werden dazu vier Schritte unternommen:

- Das Sende- und Empfangssignal werden zeitlich abgestimmt (z. B. durch Herausfinden des Maximums der wechselseitigen mathematischen Korrelationsfunktion).
- Sende- und Empfangssignal werden hinsichtlich des Signalpegels abgestimmt (aufeinander justiert).
- Es erfolgt dann eine Transformation in die Frequenzdomäne (Erstellung des Frequenzspektrums) und die Zuordnung der Frequenzanteile zu den hörbaren Frequenzbändern. Zwei Signale lassen sich in der Frequenzdomäne besser vergleichen als in der Zeitdomäne.
- Schließlich werden die Unterschiede zwischen Sende- und Empfangssignal ermittelt.

Ein Nachteil bei den „Perceptual Models“ ist, dass diese Bewertung nur in einer Kommunikationsrichtung erfolgt, ein bei der Sprachkommunikation aber übliche bidrektionale Bewertung bzw. hierauf einfließende Störung erfolgt nicht. Dieses Verfahren stellt nicht den unmittelbaren Zusammenhang zwischen netztypischen Störungen in Form von Jitter, Delay oder Packet Loss her, es bewertet letztendlich ausschließlich die Folge von „irgendwelchen“ Störungen auf dem Kommunikationspfad zwischen „sprechendem“ und „hörendem“ Partner. In Folge dessen sind diese Verfahren unzureichend bei der Bewertung der Netzqualität und Lokalisierung von Schwachpunkten in einem Netz.

Anders bewertet dagegen das Verfahren auf Basis des E-Models (ITU-T G.107), bei diesem Verfahren wird über die Bildung eines sogenannten „R-Faktors“ eine Aussage über die Qualität getroffen. Dabei verzichtet dieses Modell auf einer ausschließlich direkten Auswertung von Sprachsignalen, statt dessen wird neben den Einflüssen des gewählten Codecs, eingestellten Jitter Buffer u.a. auch über die Ermittlung von den netztypischen Effekten wie Delay und Paketverlust eine Qualitätsaussage macht.

Tabelle 1 (Quelle: Peter Tschulik „Quality of Service“) macht den Zusammenhang zwischen dem Wert und der Qualität deutlich, ergänzt wird die ebenfalls mögliche Zuordnung zu einem vergleichbaren und gewohnten MOS-Wert.

RTP

Wie der Bereich Codecs ist auch der Bereich Paketbildung weitgehend standardisiert. Der dazu maßgebliche Standard RTP (Real-time Transport Protocol) wird bei allen VoIP-Lösungen eingesetzt. RTP wurde von der IETF (Internet Enginee-

Rating-Faktor	Kundenzufriedenheit	Typische Anwendung	MOS-Wert
90 ≤ R ≤ 100	alle sehr zufieden	lokale Gespräche innerhalb einer Nebenstellenanlage	besser 4,34
80 ≤ R < 90	zufrieden	nationale Gespräche	4,03 bis 4,34
70 ≤ R < 80	einige unzufrieden	internationale Gespräche ohne Kompression	3,60 bis 4,02
60 ≤ R < 70	viele unzufrieden	nationale Gespräche von Fest- nach Mobilnetz	3,10 bis 3,59
50 ≤ R < 60	alle unzufrieden	Satellitenverbindungen ohne Kompression	2,58 bis 3,09

Tabelle 1

ring Task Force) in Request for Comments (RFC) 1889 standardisiert, wird aber auch von der ITU genutzt. RTP setzt auf UDP (User Datagram Protocol) auf und umfasst folgende Funktionen:

- Erkennung des Typs der Information
- Identifizierung des Senders
- Synchronisation
- Loss Detection
- Segmentation und Reassembly
- Sicherheit (durch Verschlüsselung, optional).

RTP wird in der Regel zusammen mit dem Real Time Transport Control Protocol (RTCP) eingesetzt, das zum Austausch der Informationen über Paketverluste und Verzögerungen verwendet wird. RTCP spezifiziert folgende Kontrollnachrichten:

- Sender Report: beinhaltet Informationen über gesendete Informationen und Zeitstempel
- Receiver Report: beinhaltet Informationen über empfangene Informationen, Verluste, Verzögerungsschwankung und Verzögerung
- Source Description: Name, E-Mail-Adresse, Telefonnummer, Identifikation

Messverfahren beim Chariot-System

Das Chariot-System basiert auf einem relativ simplen Grundprinzip: Auf einem oder mehreren Netz-PCs wird jeweils ein Prozess (einfacher EXE-File) installiert und gestartet, der solange weiterläuft, bis er gezielt gestoppt wird oder der PC bzw. User sich abmeldet. Am Prozess muss nichts eingestellt werden, er muss lediglich gestartet werden. Dieser Prozess stört in der Regel keine der restlichen Applikationen und kann damit auf beliebigen produktiven Rechnern installiert werden (diese Rechner stellen dann sogenannte „Endpoints“ dar). Auf einem weiteren PC wird die Chariot-Software installiert, die als Konsole dient. Von dieser Konsole aus werden jetzt virtuelle Verbindungen (sogenannte „pairs“) eingerichtet, die einen simulierten, applikationsabhängigen Datenverkehr zwischen den Endpoints verursachen (im Prinzip können die Endpoints auch auf der Konsole eingerichtet werden). (siehe Abbildung 5)

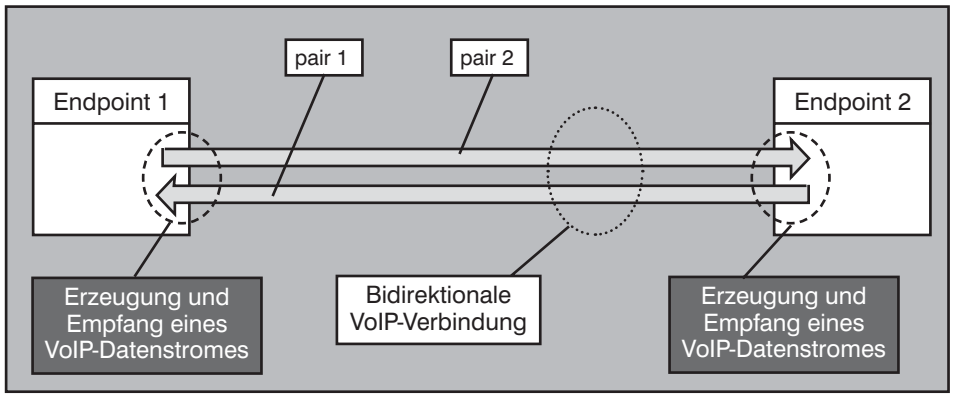


Abbildung 5: Prinzip der Bildung von pairs

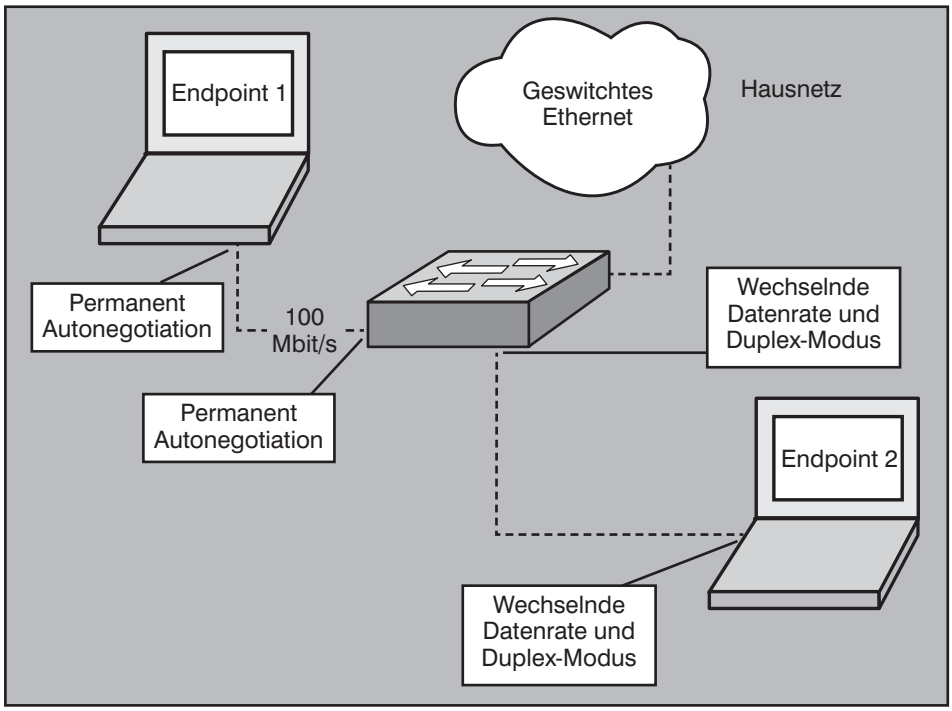


Abbildung 6: Testgrundaufbau

Im Falle des hier betrachten VoIP-Tauglichkeitstests können somit mit „n“ Endpoints „n/2“ bidirektionale, also Full-Duplex-VoIP-Verbindungen simuliert werden. Positioniert man diese Endpoints an entsprechend exponierten Stellen im Netz, so wird der Einfluss aller Netzkomponenten in den Verbindungswegen der Lines berücksichtigt.

Beim Chariot-System wird der Messung bzw. Bewertung ein leicht modifiziertes E-Model zugrundegelegt. Dabei werden folgende Hauptfaktoren zur Bewertung herangezogen:

- One-Way Delay
- End-to-End-Delay

Bei der Ermittlung des One-Way Delay werden sämtliche Parameter, die durch das

Lokale Netz beeinflusst werden können berücksichtigt (selbstverständlich kann die Prüfung dieses Faktors auch über ein Lokales Netz hinaus erweitert werden, z.B. zur Ermittlung der Qualität einer WAN-Verbindung). Damit beginnt die Messung mit der Auswertung der RTP-spezifischen Parameter und umfasst ergänzend alle für VoIP relevanten Netzparameter. Die Ergebnisse dieser Auswertung lassen demzufolge eine Aussage über die grundsätzliche VoIP-Tauglichkeit des Netzes zu. Der Faktor des End-to-End-Delay geht noch einen Schritt weiter: Hierbei wird angenommen, dass man zusätzlich zur reinen Netz-Qualität prüfen möchte, ob VoIP-Endsysteme mit ganz konkreter Konfiguration über das Netz kommunizieren können und in welcher R-Faktor- bzw. MOS-Qualität. Es wird somit eine Mund-zu-Ohr-Kommunikation simuliert und dabei kann auch getestet werden, welchen Einfluss die Veränderung von Netzparametern (Bandbreite, QoS-Einstellungen aber auch z.B. Spanning Tree Konvergenzzeiten) oder Einstellungen an den Sprachendgeräten (gewählter Codec, Jitter Buffer, PLC etc.) auf die Qualität haben können.

Erfahrungen mit dem System im Labornetz

Zur gezielten Simulation von Störeffekten auf eine VoIP-Kommunikation wurde ein kleines Netz aufgebaut (bestehend aus einem Layer-2-Switch und zwei Notebooks) und dieses wurde an ein produktiv – auch für VoIP - genutztes lokales Netz angeschlossen (siehe Abbildung 6).

Uns interessierte zunächst einmal, ob man bereits in einer kleinen Umgebung mit Hilfe des Chariot-Systems Effekte messen kann, die auch in großen Netzen zu Übertragungsproblemen bei VoIP führen würden. Im ersten Schritt wurden beide Notebooks als Endpoints eingerichtet (mit 100 Mbit/s und Autonegotiation an allen Ports) und von der Chariot-Konsole aus wurden in diesen Endpoints jeweils ein VoIP-Gespräch zwischen beiden Endpunkten simuliert (Messung 1). Das heißt, dass die Konsole durch Kommunikation mit dem auf den Endpoints laufenden Prozess beide Endgeräte „zwingt“, wie zwei VoIP-Telefone (im Prinzip werden zwei Softphones simuliert) zu arbeiten und einen dementsprechenden Datenverkehr zu erzeugen. Die wichtigsten Setup-Einstellungen lauteten:

- Kodierungsverfahren nach G.711u
- Kein PLC
- Kein Silence Suppression
- Jitter Buffer 40 ms

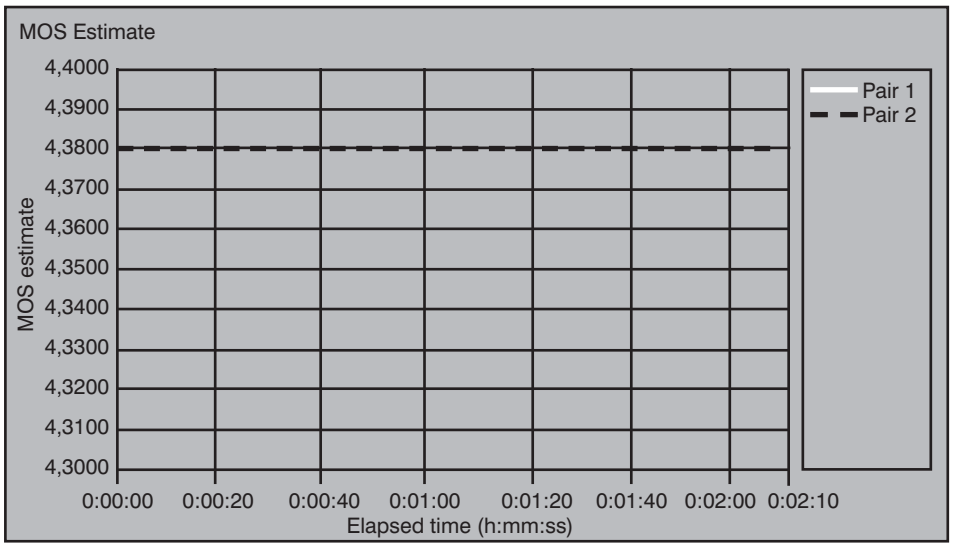


Abbildung 7: MOS-Wert bei Messung 1

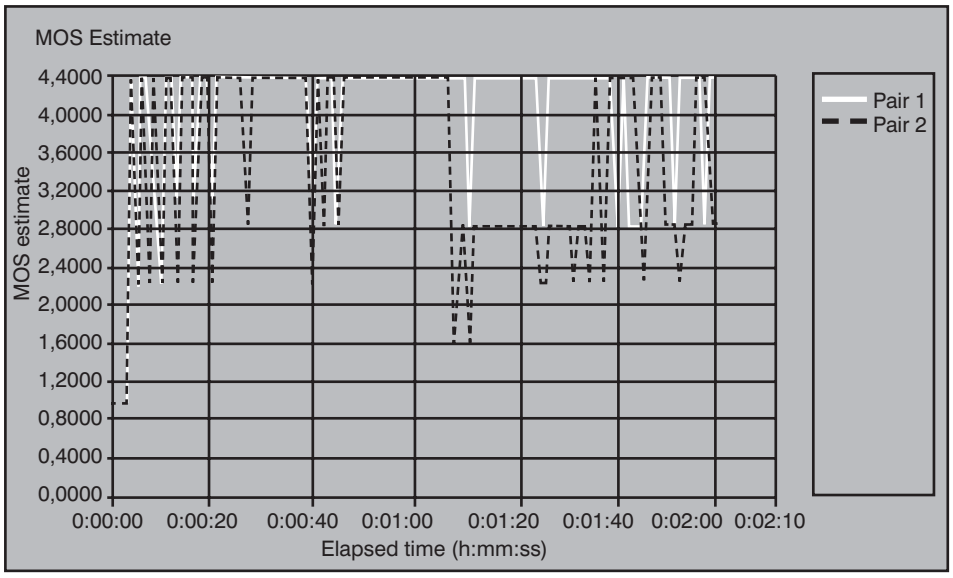


Abbildung 8: MOS-Wert bei Messung 3 (Duplex-Mismatch)

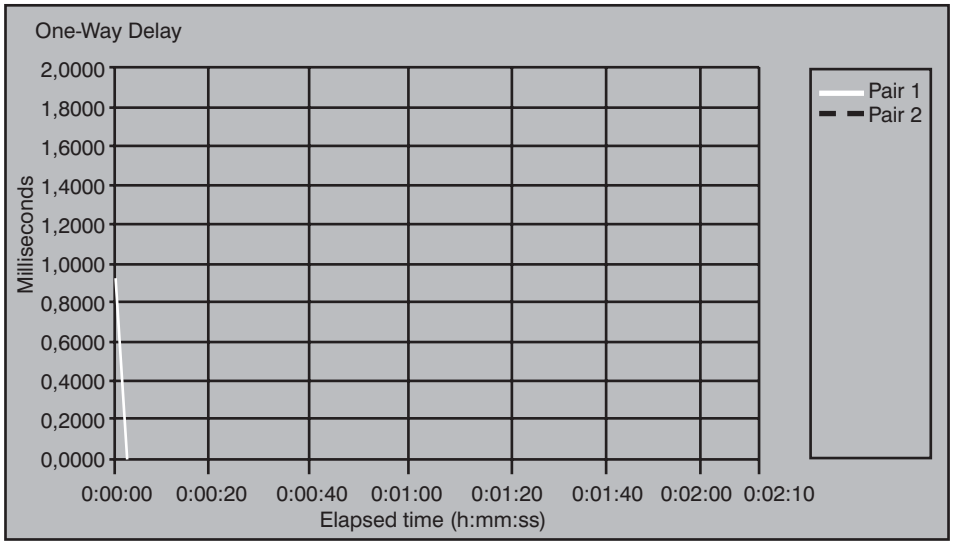


Abbildung 9: Netz-Delay bei Messung 3 (Duplex-Mismatch)

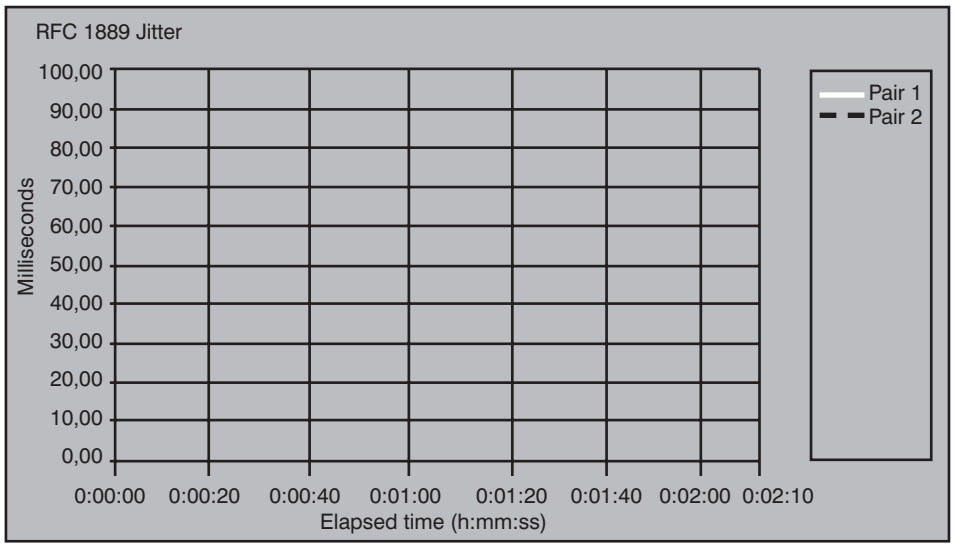


Abbildung 10: Jitter bei Messung 3 (Duplex-Mismatch)

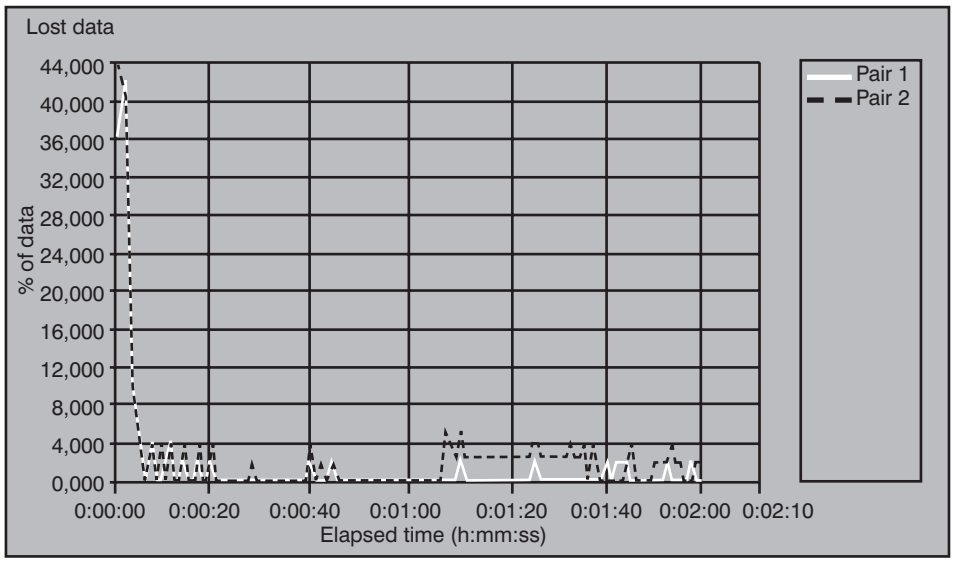


Abbildung 11: Paketverlust bei Messung 3 (Duplex-Mismatch)

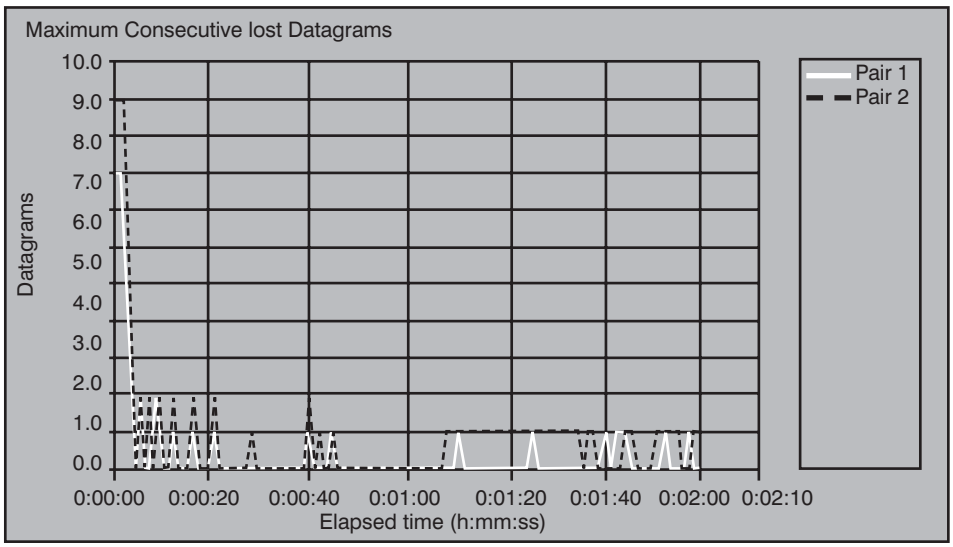


Abbildung 12: Maximale Paketverlustrate bei Messung 3 (Duplex-Mismatch)

Wie bereits oben erläutert wird zu einer Gesamtbewertung der Sprachkommunikation der MOS-Wert herangezogen, dieser stellt also die erste zu überprüfende Größe dar. Erwartungsgemäß wurde in diesem Mini-Netz konstant über die Messdauer von 2 Minuten hinweg ein hoher MOS-Wert von 4,38 gemessen (genauer gesagt auf Basis des oben erläuterten Modells errechnet). Der mittlere Datendurchsatz lag ebenfalls erwartungsgemäß bei 64 kbit/s und es gab keinen messbaren Netz-Delay und keinen Paketverlust.

Die in Abb. 7 in der Legende gekennzeichneten Paare 1 und 2 stehen jeweils für die Kommunikation zweier Endgerätepaare (daher auch der Begriff „Pair“ beim Chariot) bzw. für eine Übertragungsrichtung. In dieser Abbildung liegen beide Linien übereinander, so dass nur eine gestrichelte Linie erkennbar ist.

Im nächsten Schritt wurde an einem der beiden Notebooks bzw. auch an dem betreffenden Switch-Port die Ethernet-Einstellung auf 10 Mbit/s Halbduplex eingestellt. Es konnten keinerlei Verschlechterungen im Vergleich zu Messung 1 festgestellt werden. Bei den Messungen 3 und 4 wurde ein Szenario eingestellt, dass zu einem Duplex-Mismatch führt:

- Messung 3: Ethernet-Port am Endgerät auf 10 Mbit/s Vollduplex und Switch-Port auf Autonegotiation
- Messung 4: Ethernet-Port am Endgerät auf 100 Mbit/s Vollduplex und Switch-Port auf Autonegotiation
- Die Einstellung des anderen Endpoints bzw. der Ethernet-Verbindungen blieb.

Diese, nicht selten in Netzen zu findende Fehleinstellung führt dazu, dass bei einer Kommunikation zwischen den beiden „fehlkonfigurierten“ Ports Pakete verloren gehen müssten, deshalb wurde hier eine Verschlechterung der VoIP-Kommunikation erwartet (s. Abb. 8).

Der betrachtete zeitliche Verlauf des MOS-Wertes wich erheblich von der ersten gemessenen Kurve ab (s. Abb. 9). Weiter ist (bei farblicher Auflösung der Kurve) erkennbar, dass eine von beiden Verbindungen besonders schlecht war, wir also ein unsymmetrisches Störverhalten haben. Auch das passte zu dem Test, denn während der Messung wurde auf einem Notebook gleichzeitig eine Internet-Recherche gefahren. Unter Heranziehung der Abb. 8 ist deutlich erkennbar, dass ein in dieser Zeit geführtes Telefongespräch sehr viele Qualitätseinbußen gehabt hätte, welche vom normalen Nutzer nicht mehr akzeptiert worden wäre. Woran kann dies gelegen haben? Dazu die Grafiken für die 3 wichtigen Kennwerte Delay (Netz-Delay!), Jitter und Packet Loss. (s. Abb. 9-11)

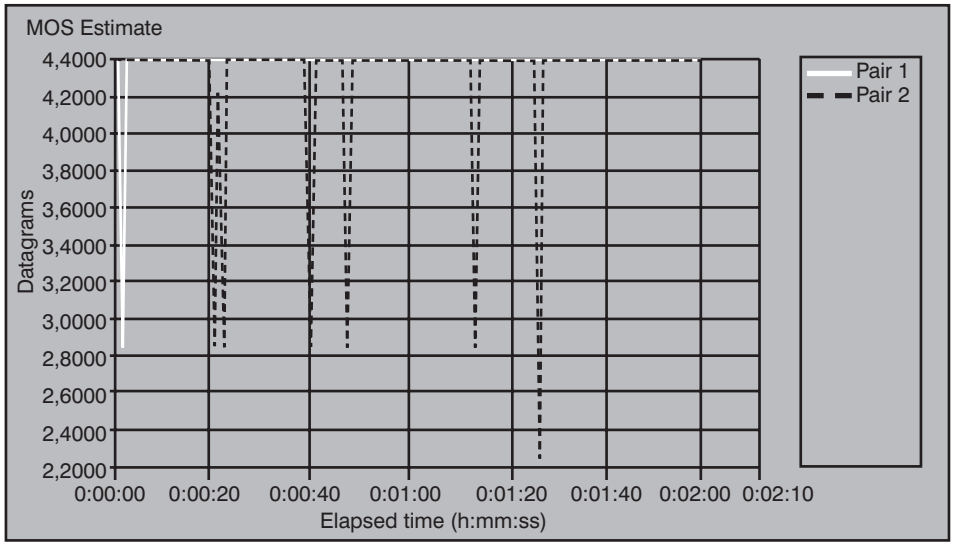


Abbildung 13: MOS-Wert bei Messung 4 (Duplex-Mismatch)

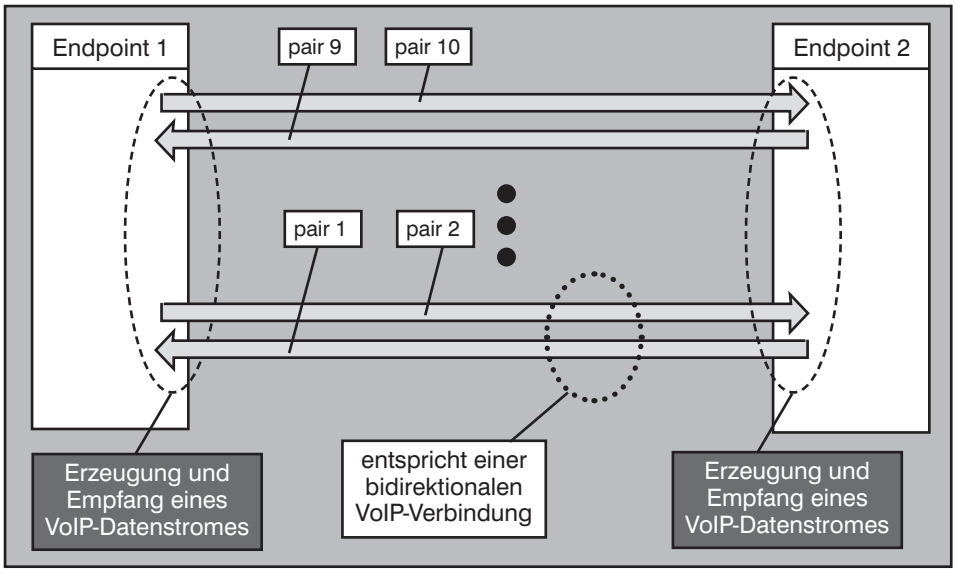


Abbildung 14: MOS-Wert bei Messung 4 (Duplex-Mismatch)

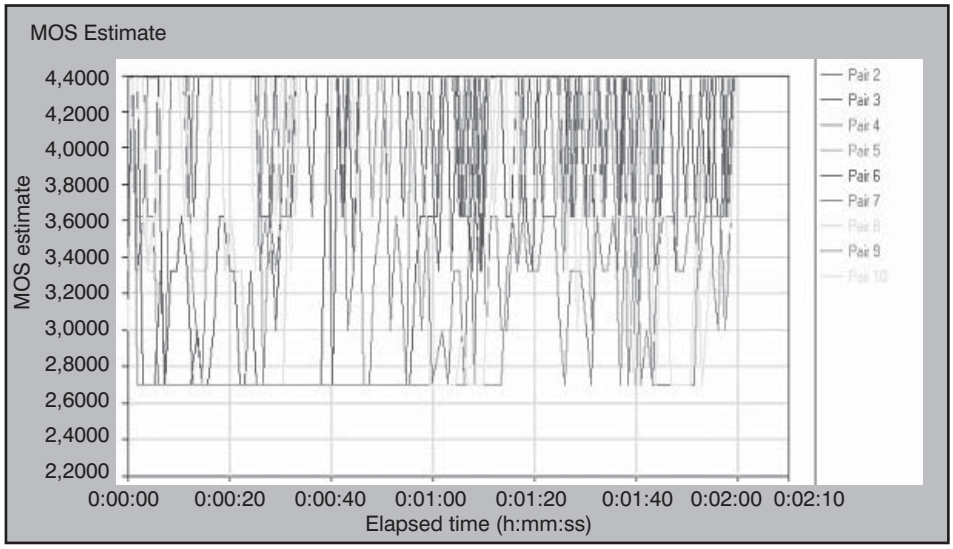


Abbildung 15: MOS-Wert bei Messung 7 (Duplex-Mismatch)

Es ist deutlich zu erkennen, dass das Duplex-Mismatch-Phänomen einen Einfluss auf die Paketverlustrate hat, die beiden anderen Werte bleiben bei 0 stehen. Kennt man den durch Duplex-Mismatch entstehenden Effekt, so ist dieses nachvollziehbar. Interessant ist die Wirkung von auch relativ kleinen Verlustraten: Nach ca. 1 min 10 sek steigt die Paketfehlerrate zweimal auf ca. 6% an, der MOS-Wert fällt dann auf den sehr schlechten Wert von 1,6. Selbst die geringen Paketverlust-peaks der unteren Linie bis ca. 2% Verlust führen zu MOS-Werten im Bereich von 2,8 bis 2,9, das wäre bereits vollkommen unakzeptabel in einem VoIP-Netz. Bei der Frage, um wie viele verlorengegangene Pakete es sich denn überhaupt handelt, hilft eine weitere Messauswertung des Chariots weiter. (s. Abb. 12)

Es handelt sich also nicht um sehr viele Pakete pro Zeiteinheit, die verloren gehen, sondern die maximale Verlustrate liegt meist bei 1 bis 2 Datagramme. Dies macht deutlich, wie empfindlich ein VoIP-Kommunikation auf Netzanomalien reagieren kann.

Bei der Messung 4 wurde der Aufbau von Messung 3 beibehalten, mit Ausnahme der Datenrate, diese wurde verzehnfacht (100 Mbit/s). Konnten wir bei dem Vergleich der Datenraten in einem fehlerlosen Netz noch keine Unterschiede feststellen (Messung 1 und Messung 2), so ist dies jetzt nicht mehr der Fall. (s. Abb. 13)

Folgendes ist erkennbar:

- Die maximale MOS-Verschlechterung ist deutlich geringer (Messung 3 mit min. MOS-Wert von 1,6; Messung 4 mit min. MOS-Wert von 2,2)

- Bei Paar 1 bleibt der MOS-Wert konstant auf 4,4. Dies würde in der Praxis bedeuten, dass einer der beiden Gesprächspartner einen guten Empfang hat, der andere aber nicht.

- Interessanter aber ist die Feststellung, dass die Häufigkeit der MOS-Wert-Unterschreitung deutlich zurückgegangen ist (noch 6 mal). In einem 2-Minuten Gespräch würde ein Partner also 6 mal eine Empfangsbeeinträchtigung spüren. Bei Messung 3 würden beide Partner über 20 mal gestört werden.

Falls diese gestellte Fehlersituation auch im realen Netz zu erwarten ist, würde eine grundsätzliche 100 Mbit/s-Einstellung an Switch und Endgerät die Störwirkung möglicherweise reduzieren.

Group/ Pair	MOS Average	MOS Minimum	MOS Maximum	End-to-End Delay Average (ms)	One-Way Delay Average (ms)	RFC 1889 Jitter Average (ms)	Percent Bytes Lost E1 to E2	Maximum Consecutive Lost Datagrams	Jitter Buffer Lost Datagrams
All Pairs	4,37	1	4,38	42	1	0,029	0	25	16.731
Pair 1	4,38	4,38	4,38	43,294	2	0	0	0	0
Pair 2	4,38	2,86	4,38	41,427	0	0	0	1	0
Pair 3	4,37	1	4,38	41,17	0	0,012	0	25	1.147
Pair 4	4,36	2,22	4,38	41,405	0	0,02	0	0	1.847
Pair 5	4,36	2,83	4,38	41,422	0	0,045	0	0	2.357
Pair 6	4,36	2,22	4,38	41,095	0	0,05	0	0	2.481
Pair 7	4,36	2,83	4,38	41,399	0	0,045	0	0	2.357
Pair 8	4,36	2,77	4,38	41,709	1	0,047	0	0	2.342
Pair 9	4,36	2,83	4,38	41,602	1	0,021	0	0	1.858
Pair 10	4,36	2,83	4,38	41,475	0	0,046	0	0	2.342
Totals:	4,37	1	4,38	42	1	0,029	0	25	16.731

Tabelle 2: Übersicht der wichtigsten Parameter für den Zeitraum A

MOS-Werte und Jitter:	**siehe Erläuterungen oben**
End-to-End-Delay:	Dieser Wert beschreibt die Ende-zu-Ende-Verzögerung einer VoIP-Kommunikation inklusive der LAN-spezifischen Parameter (Verkabelung, Switches, Router, NIC) und der VoIP-spezifischen Parameter (Codec, Jitter Buffer, eingestellte Kompensationsverfahren). Der Wert darf 150 ms nicht überschreiten.
One-Way-Delay:	Dieser Wert beinhaltet ausschließlich die Verzögerungen, die durch die Komponenten des lokalen Netzes entstehen (Verkabelung, Switches, Router, NIC). Dieser Wert spielt insbesondere dann eine Rolle, wenn der Wert des End-to-End-Delay oder der MOS-Wert zu hoch ist und analysiert werden muss, welcher Bestandteil des VoIP-Kanals hierfür verantwortlich ist.
Percent Bytes Lost E1 to E2:	Der prozentuale Anteil der verlorenen Bytes zwischen den beiden Endpunkten (eine Richtung) des jeweiligen Paares. Bei einem schlechten MOS-Wert und einem Verlust von 1 % und mehr wäre gegebenenfalls mit Hilfe des Jitter Buffers oder PLC-Maßnahmen zu versuchen, hier eine Verbesserung zu erzielen. Dies wären dann Maßnahmen, die bei der Einrichtung des VoIP an den VoIP-Terminals berücksichtigt werden müssten.
Maximum Consecutive Lost Datagrams:	Falls in einem Sample-Intervall zwischen Sender und Empfänger Pakete verloren gegangen sind, so werden diese gezählt. Die höchste Anzahl dieser Pakete innerhalb eines Sample-Intervalls wird bei diesem Wert erfasst. Im Falle eines permanent schlechten MOS-Wertes wäre der Paketverlust dafür möglicherweise die Ursache.
Jitter Buffer Lost Datagrams:	Falls ein Jitter Buffer eingestellt wird, prüft Chariot bei einem Datenstrom nach, ob es Pakete gegeben hat, die nicht durch den Buffer „laufen“ konnten und damit verloren gegangen sind.

Tabelle 3

Die zweite Staffel der Messreihe wurde mit den gleichen Einstellungen wie die erste gemacht, mit Ausnahme dessen, dass jetzt statt einem bidirektionalen Kommunikationspaar fünf solcher Paare auf beiden Endpoints simuliert wurden (Achtung: Chariot nennt dies 10 „pairs“). Der MOS-Wert aller Verbindungen lag in den beiden ersten Messungen 5 und 6 (entspricht den Messungen 1 und 2 aus der ersten Reihe) konstant bei 4,38. (siehe Abbildung 14)

Die MOS-Kurve in Abbildung 15 für die Messung 7 (entspricht der Messung 3 aus der ersten Reihe) macht deutlich, wie miserabel eine Duplex-Mismatch-Situation bei mehr als einem Kommunikationspaar wäre. Auf eine Darstellung der anderen Messparameter wird verzichtet, diese sieht entsprechend aus.

Konnten wir bei Messung 4 einen Vorteil durch eine höhere Datenrate an den angeschlossenen Ports nachweisen, so ließ sich bei Messung 8 dieser Nutzen zwar für die einzelnen Verbindungen auch noch feststellen, insgesamt aber würden bei einer solchen Fehleinstellung zu viele Kommunikationspartner von Störungen betroffen sein (auf eine Darstellung der Kurve für Messung 8 wird verzichtet).

Erfahrungen mit dem System im Feld

Ergänzend zu den Erfahrungen im Labor wurden praktische Erfahrungen mit dem System bei der Überprüfung von VoIP-Readiness in vorhandenen lokalen Netzen gemacht. Beispielsweise wurde in einem Netz mit mehreren tausend Netzteilnehmern mit Hilfe von 5 eingerichteten bidirektionalen Verbindungen ein VoIP-Verkehr zwischen 7 Endpunkten simuliert.

Zu Beginn des Tests wurden auf 7 Standard-PCs unter dem Betriebssystem Windows XP Endpoints eingerichtet. Die

Chariot-Endpoint-Prozesse stellten neben den Standard-Prozessen des Betriebssystems die einzigen Prozesse dar, die während der Messung liefen. Ein großes Problem kristallisierte sich bereits im Laufe der ersten Minuten heraus: Die Chariot-Prozesse konnten nicht über einen Zeitraum von mehreren Minuten oder gar Stunden stabil aufrechterhalten werden, sukzessive wurden fast alle Prozesse mit Fehlermeldungen abgebrochen. Der Fehler war dem Software-Hersteller bzw. Distributor bekannt und als einzige zuverlässige Lösung wurde die Einrichtung von LINUX als Betriebssystem bei den Endpoints empfohlen. Diese Lösung führte im konkreten Fall zum Erfolg, so dass jetzt eine Langzeitmessung möglich war. Ebenfalls zeigte sich, dass die Konsole nicht auf beliebigen Plattformen läuft, erst Windows 2000 konnte hier einen stabilen Betrieb sicherstellen.

Das Chariot-System erlaubt die Überprüfung der Wirksamkeit von Techniken, die später auf den eingeführten VoIP-Terminals/Geräten eine Verbesserung der Sprachqualität möglich machen könnte. Chariot simuliert bei entsprechend vorgenommener Einstellung folgende Optionen:

- Verwendung eines Jitter Buffers
- Verwendung von Silence Supression
- Verwendung von packet loss concealment

Mit Hilfe des Chariot-Systems konnte im genannten Beispiel über einen längeren Zeitraum eine sehr große Menge VoIP-relevanter Werte gemessen bzw. berechnet werden (eine Messung über 48 Stunden liefert beim kleinsten eingestellten Messintervall eine über 300 MByte große CSV-Datei!), die Tabelle 2 beinhaltet nur die Übersicht der Ergebnisse aus einem Messzeitraum von mehreren Tagen.

Tabelle 3 beinhaltet eine Übersicht bzw. Erklärung der Chariot-spezifischen Messwerte.

Weiter ist zur richtigen Interpretation der Tabelle 3 zu verstehen, dass Chariot im wahlweise veränderbaren Messintervall (in diesem Falle wurde 1 sec gewählt) eine konkrete Anzahl von VoIP-Paketen zwischen den jeweiligen Endpoints überträgt und anhand der empfangenen Pakete in jedem Endpoint eine Auswertung durchführt. Dies bedeutet u.a. aber auch, dass ein einziges Messintervall von mehreren hunderttausend Messintervallen mit schlechten Werten in der Minima/Maxima-Anzeige erfasst wird, ohne dass dieser aufgeführte Wert eine wirkliche Relevanz für eine Sprachqualität hätte. Demzufolge reicht die ausschließliche Auswertung der zusammenfassenden Tabelle 3 nicht aus, statt dessen muss mit Hilfe der exportierten Daten für die „schlechten“ Messintervalle geprüft werden,

- wie häufig diese „schlechten“ Messintervalle auftreten
- ob mehrere dieser Messintervalle hintereinander festgestellt werden können (dies könnte dann ein Zeichen für eine schlechte VoIP-Verbindung sein)
- aufgrund welcher Sprachparameter (delay, jitter oder Paketverlust) z.B. der MOS-Wert zustande kommt.

Im konkreten Beispiel konnte mit Hilfe von mehreren Messungen reproduzierbar bestätigt werden, dass das vorhandene Lokale Netz unter den aktuellen Rahmenbedingungen bereit ist, VoIP einzuführen.

Fazit

Viele Betreiber von Lokalen Netzen stehen heute vor der Frage, ob das Lokale Netz in der aktuellen Form bereits bereit ist für die Einführung von VoIP. Mit dem System Chariot wird dem Betreiber/Planer grundsätzlich die Möglichkeit gegeben, das Netz bereits lange vor der Einführung auf diese Bereitschaft hin zu prüfen. Die Chariot-Simulation liefert alle Parameter, die für eine Beurteilung der zu erwartenden Sprachqualität notwendig sind und lässt bei Ergänzung durch entsprechend beigelegte Baselining-Informationen auch eine gezielte Suche nach den Schwachpunktens des Netzes zu. Die vom Software-Hersteller suggerierte Einfachheit in der Anwendung kann nicht bestätigt werden, es ist sowohl beim Messaufbau wie auch bei der Auswertung mit einem hohen Aufwand zu rechnen, der erst bei zunehmender Routine im Umgang mit dem Werkzeug zu einer zeit- und kostenoptimierten Überprüfungsmöglichkeit führen wird.

CCNE

ComConsult Certified Network Engineer

Lokale Netze
27.06. - 01.07.05 in Aachen
12.09. - 16.09.05 in Aachen
28.11. - 02.12.05 in Aachen

Internetworking
06.06. - 10.06.05 in Aachen
26.09. - 30.09.05 in Aachen
28.11. - 02.12.05 in Aachen

TCP/IP und SNMP
20.06. - 24.06.05 in Köln
26.09. - 30.09.05 in Berlin
14.11. - 18.11.05 in Bonn

Ethernet Technologien - neuester Stand
20.06. - 24.06.05 in Aachen
19.09. - 23.09.05 in Aachen
14.11. - 18.11.05 in Aachen

Paketpreis für alle vier Seminare € 8.170.-- zzgl. MwSt.
(Einzelpreise: je € 2.290.--)

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.com

CCTS

ComConsult Certified Trouble Shooter

Trouble Shooting in Lokalen Netzwerken - Grundlagen
06.06. - 10.06.05 in Aachen
12.09. - 16.09.05 in Aachen
07.11. - 11.11.05 in Aachen

Trouble Shooting für TCP/IP- und Windows-Umgebungen
30.05. - 03.06.05 in Aachen
24.10. - 28.10.05 in Aachen

Trouble Shooting in geswitchten Ethernet-Umgebungen
04.07. - 08.07.05 in Aachen
17.10. - 21.10.05 in Aachen
28.11. - 02.12.05 in Aachen

Paketpreis für alle drei Seminare € 7.500.-- zzgl. MwSt.
(Einzelpreise: je € 2.490.--)

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.com

CCSE

ComConsult Certified Security Expert

Sicherheitslösungen I: Von den Einzelbausteinen zur integrierten Lösung
06.06. - 10.06.05 in Köln
26.09. - 30.09.05 in Nürnberg

Sicherheitslösungen II: IP-VPNs, der Kern einer Sicherheits-Infrastruktur
30.05. - 01.06.05 in Köln
19.09. - 21.09.05 in Bonn
07.11. - 09.11.05 in Köln

Sicherheitslösungen III: Planung und praktische Konfiguration
27.06. - 01.07.05 in Aachen
17.10. - 21.10.05 in Aachen
05.12. - 09.12.05 in Aachen

Paketpreis für alle drei Seminare € 5.330.-- zzgl. MwSt.
(Einzelpreise: € 2.290.-- / € 1.690.-- / € 2.290.--)

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.com

Impressum

Verlag:
ComConsult Technology Information Ltd.
121 Paton Rd.
RD1
Richmond
New Zealand
GST Number 84-302-181
Registration number 1260709
Phone: 0064 3 5444632
Fax: 0064 3 5444237

German Hot-line of ComConsult-Research: 02408-955300
E-Mail: insider@comconsult-akademie.de
http://www.comconsult-research.de

Herausgeber und verantwortlich im Sinne des Presserechts:
Dr. Jürgen Suppan
Chefredakteur: Dr. Jürgen Suppan
Erscheinungweise: Monatlich, 12 Ausgaben im Jahr
Bezug: Kostenlos als PDF-Datei
über den eMail-VIP-Service der ComConsult Akademie