ComConsult Research

# Der Netzwerk Insider

Januar 2009

Systematische Weiterbildung für Netzwerk- und IT-Professionals

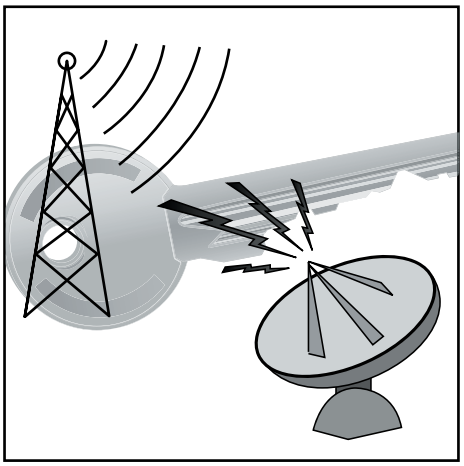
Schwerpunktthema

# Sicherheitsaspekte öffentlicher Mobilfunknetze

## Teil 2: Maßnahmen zur Sicherung der mobilen Kommunikation

**von Dominik Zöller, Dr. Michael Wallbaum, Dr. Frank Imhoff**

**Wie im ersten Teil dieses Artikels in der Insider-Ausgabe Dezember 2008 beschrieben, lauern bei der Verwendung von öffentlichen Mobilfunknetzen eine Reihe von Gefahren. Daher gilt es zu bedenken, welche konkrete Risiken der Datensicherheit man als Privatperson oder Unternehmen in Kauf zu nehmen bereit ist. Die nicht tolerierbaren Risiken müssen isoliert und durch entsprechende Gegenmaßnahmen ausgeräumt werden.**



**Freie Netzwahl**

Im Falle der zugrundeliegenden Netztechnologie hat das einzelne Unternehmen nur geringe bis keine Einflussmöglichkeiten. Die Absicherung des Netzes gegen Angriffe von außen oder gegen Innentäter liegt ausschließlich in den Händen der Betreiber. Zudem ist - auch bei der Nutzung von Mobiltelefonen mit UMTS oder einer der möglichen Nachfolgetechnologien - nicht sichergestellt, dass die gesamte Infrastruktur diese Technik unterstützt. Die Umrüstung geschieht - den wirtschaftlichen Zwängen geschuldet - schrittweise und immer mit Rücksicht auf Abwärtskompatibilität. Für den Einzelnen ist es im Zweifelsfall nicht erkennbar, ob eine Netzinfrastruktur sicher ist oder nicht.

weiter auf Seite 20

Zweitthema

# 40 GBASE-T

**von Dr. Franz-Joachim Kauffels**

**Die Erfahrung lehrt, dass eine neue Geschwindigkeitsstufe vom Markt erst dann in breiterem Maße akzeptiert wird, wenn es auch eine Variante für Twisted Pair gibt. Bis vor Kurzem konnte niemand sagen, ob eine 40 Gigabit-Ethernet Variante auch auf Twisted Pair möglich ist. Das hat sich mittlerweile geändert, es wird definitiv 40 GBASE-T geben. Auch wenn ein entsprechender Standard noch ein paar Jahre dauert, können wir heute schon sagen, welche Art der Verkabelung für diesen Zweck mit Sicherheit geeignet ist. Das ist ein sehr wichtiges Ergebnis vor dem Hintergrund der Lebensdauer von Verkabelungssystemen. Natürlich blicken wir in diesem Artikel auch auf die Möglichkeiten für die Transceivertechnik.**

Die Standards für 10 GbE über Glasfaser gibt es schon seit 2003. Zunächst haben sich aber nur wenige Anwender dafür interessiert. Das änderte sich erst mit der Verfügbarkeit einer Version über Twisted Pair, eben 10 GBASE-T. Auch wenn viele Betreiber bei der Einführung von 10 GbE schließlich doch zur Faser neigen, scheint alleine die Existenz einer Twisted Pair Version eine erhebliche Beruhigung zu sein.

weiter auf Seite 10

Neuer Kongress

## Verkabelungs- und Infrastrukturforum 2009

ab Seite 8

Geleit

## Netzwerk-Technologie 2009: wohin geht der Weg?

ab Seite 2

Kongress des Jahres 2009

## Netzwerk-Redesign Forum 2009

ab Seite 4

Zum Geleit

# Netzwerk-Technologie 2009: wohin geht der Weg?

**Die Analyse von ComConsult Research: Netzwerk-Technologie 2009 wird die Basis der Keynote für unser diesjähriges Netzwerk-Redesign Forum im März sein. Wir geben in diesem Geleit Ausschnitte der auf dem Forum anstehenden Diskussion wieder.**

Die Verbesserung der Wirtschaftlichkeit und die Erhöhung der Arbeitseffizienz stehen zur Zeit ganz oben auf der Aktionsliste von Unternehmen und Behörden. Die technologischen Ansätze, um dies zu erreichen, sind weitreichend und betreffen ganz unterschiedliche Technologien:

- Neue Formen von Anwendungsarchitekturen basierend auf Webtechnologien (der Browser als moderne Laufzeitumgebung?)
- Umsetzung einer an Geschäftsprozessen orientierten Kommunikation mit Unified Communications und anderen Technologien
- Unterstützung von Team-Prozessen mit Portalen wie Sharepoint oder durch eine Mischung aus Webdesign, Blogs, Wikis und WebDAV
- Redesign von Rechenzentren, weitere Konzentration von Rechenleistung durch neue Formen virtueller Infrastrukturen, durch verbessertes Loadbalancing und Standort-übergreifende Architekturen
- Konsolisierung von Speicher- und Server-Technologie
- gezielte Untestützung mobiler Mitarbeiter durch sichere Bereitstellung von Daten und Applikationen unabhängig vom Ort der Nutzung
- Plattformneutrale und Versions-unabhängige Nutzung kritischer Applikationen durch Applikations- und Desktop-Virtualisierung

Die Liste könnte sicher ohne Probleme weiter verlängert werden. Tatsächlich bieten uns neue Technologien heute weitreichende Möglichkeiten, um effizienter und wirtschaftlicher zu arbeiten.

Dabei haben alle angesprochenen Themen und Projekte etwas gemein:

- sie stellen neue und erweiterte Anforderungen an bestehende Netzwerke
- sie verändern noch einmal unser Verständnis von Verfügbarkeit

Zwei Beispiele sollen das unterstreichen:

- Fast alle neuen Technologien setzen die Verfügbarkeit eines Netzwerk-Zugangs voraus, hier seien insbesondere Web-Applikationen, UC und Server-/Speicher-Konsolidierung in Kombination mit Virtualisierung genannt. Die Zeiten, in denen bei Ausfall eines Netzwerks an einem Fat-Client weiter gearbeitet werden konnte, sind bis auf Basis-Anwendungen deutlich vorbei. Ohne Netzwerk geht nichts mehr und dieser Trend wird sich noch weiter verstärken
- Neue Formen von Kommunikation inklusive der traditionellen Sprach- und Video-Kommunikation stellen immer mehr die Frage, ob es akzeptabel ist, wenn ein Netzwerk-Fehler zum Abbruch einer laufenden Kommunikation führt. Bisher hat man diese Anforderung auf Hochverfügbarkeit auf isolierte Nutzungspunkte wie die High-End-Videokonferenz des Vorstands reduziert. Aber mit einer Ausweitung dieser Art von Kommunikation auf immer mehr Teilnehmer und mit immer mehr wichtigen Kommunikations-Vorgängen stellt sich die Frage, in welchem Umfang ein Netzwerk hochverfügbar sein muss (dabei erfolgt die Definition von Hochverfügbarkeit immer aus der Sicht der Anwendung und dem Ausmaß der Beeinträchtigung für eine einzelne Anwendung)

Betrachtet man die Anforderungen an Netzwerke, dann fallen besonders folgende Bereiche auf:

- Wir laufen in eine neue Layer-2 und Layer-3-Diskussion. Bestehende Layer-2-Bereiche dehnen sich gerade in Rechenzentren und auch in Industrieumgebungen immer weiter aus. Dies wird kombiniert mit dem Wunsch, räumlich verteilte Layer-2-Bereiche zu verbinden
- Die im Layer-2 bestehenden genormten Redundanzverfahren sind auf einfache Formen der Datenübertragung optimiert. Sie haben für Sprach- und Videoübertragung sowie im Umfeld von Rechnenzentren und Produktionsumgebungen klare Nachteile. Für die Konsolidierung von Speichernetzen sind sie gar komplett ungeeignet. Einzelne Hersteller haben geeignete Technologien zur Beseitigung dieses Problems vorgestellt, aber auch diese Technologien sind nicht allgemein nutzbar und sie sind Hersteller-spezifisch
- Seit dem Beginn der Datenkommunikation gibt es den Effekt, dass Teile von Provider-Lösungen in die normalen LAN´s und WAN´s absinken und dort neue und technisch sehr leistungsfähige Lösungen bieten. Nun steht mit Carrier Ethernet eine Technologie vor der Tür, die nur unwesentlich teurer ist als bestehende Backbone-Technologie und die neue Türen für hochverfügbare Netzwerke aufstösst. Doch Carrier Ethernet ist eine Layer-2-Technologie und hat zudem einige Handhabungsnachteile. Wie können wir die ohne Frage bestehenden Potenziale dieser Technologie nutzen?
- Die zunehmende Konzentration im Server-Bereich und die Konsolidierung von Speicher- und Server-Technologien erfordert neue Dimensionen von Bandbreiten. Parallel ist 10 Gigabit-Ethernet in die Normalität eingetreten und wird von einer Reihe von Blade-Herstellern direkt On-Board unterstützt. Mit der Konsolidierung von Speicher-Netzwerken werden diese Bandbreiten in virtualisierten Umgebungen auch genutzt werden. Damit ist zumindest für den Kern unserer Netzwerke der Sprung in die nächste Bandbreiten-Generation gekommen. Die Hersteller haben mit

einer Reihe neuer Switch-Familien reagiert, weitere werden in den nächsten Monaten folgen. Doch gerade diese neuen Familien werfen Fragen zur Investitions-Sicherheit der bisherigen Produkte auf. Auf Dauer macht ein zu breites Produktangebot für die Hersteller keinen Sinn. Anders formuliert: einige Produktfamilien müssen vom Markt verschwinden. Was macht also ein Anwender, der die neuen Bandbreiten noch nicht braucht, aber trotzdem Zukunfts-orientiert investieren will?

- Mit neuen Bandbreiten kommen neue Kabel, das ist eine der endlosen Geschichten der Datenkommunikation. Diesmal ist es der Kampf zwischen Kat 6a und 7a im Twisted Pair verbunden mit der Steckerfrage und der Kampf OM3 kontra Single Mode im LWL-Bereich, auch hier mit weitgehenden Stecker-Diskussionen verbunden. Wie immer bei einer neuen Generation von Kabeln kommen die unvermeidbaren Begleitfragen: was macht der Anwender, der Kat 5 hat, wo steht OM2, was passiert mit alten Steckern, welchen Weg gehen die Komponenten-Hersteller?

- Das ganze wird gewürzt mit der Frage, ob wir Kabel im Access-Bereich überhaupt noch brauchen. Wireless-Netzwerke mit 802.11n bieten bis zu 600 Mbit/s theoretischer Bandbreite und erlauben es, im Bereich einer räumlich begrenzten Funk-Zelle im Endeffekt bis zu 10 Endgeräten die Leistung bisheriger 100 Mbit/s-Anschlüsse zu geben (unter Berücksichtigung einer statistisch verteilten Ungleichzeitigkeit der Kommunikation). Die neue Wireless-Welt ist deutlich stabiler als ältere Technologien, die Ausleuchtung ist besser und der Betrieb hat sich der Kabel-Stabilität weitgehend angenähert

- Eine umfangreichere Nutzung von Wireless-Netzwerken setzt Wireless-Controller voraus, auch um mobile Teilnehmer sauber unterstützen zu können. Wireless-Controller-Technologie ist bisher Hersteller-spezifisch. Der entsprechende Standard, um diese untragbare Situation, die die Kombination von Produkten unterschiedlicher Hersteller unterbindet, zu beenden ist CAPWAP und liegt nun in einer neuen Version vor. Verschiedene führende Hersteller zeigen sich nun diesem Standard gegenüber offen. Wir sind auf dem Weg in eine Hersteller-übergreifende standardisierte Wireless-Infrastruktur. Wird CAPWAP damit zum KO-Kriterium für die Beschaffung derartiger Produkte?

- Je mehr wir mit Netzwerken machen und je weitgehender Netzwerk-gebundene Applikationen das Feld beherrschen desto mehr kommt die Frage eines umfassenden Sicherheits-Konzepts wieder ins Spiel. Neue Technologien drängen hier quasi pausenlos in den Markt, der neueste Trend ist MAC-sec. Doch je mehr Technologien zur Auswahl stehen, desto größer wird das Problem, ein handhabbares Gesamtpaket für die Lösung zu schnüren. Diese wilde Mischung von Technologien muss 2009 ihren Kinderschuhen entwachsen und zu einer harmonischen Gesamtkonzeption geführt werden

- Mehr Bandbreite im LAN erfordert auch mehr Bandbreite im WAN. Da diese durch die Provider auch immer umfangreicher geschaffen wird, werden umgekehrt Anwendungen im LAN wieder attraktiv, die in der Vergangenheit mangels Bandbreite nicht nutzbar waren. So wird insbesondere Video und der gesamte Bereich der Desktop- und Applikations-Virtualisierung sich sprunghaft ausweiten

Wie diese Liste der Anforderungen und Technologieabwägungen zeigt, stehen Netzwerke 2009 wieder einmal vor deutlichen Umwälzungen. Erschwert wird die ganze Situation - wie immer - um den Aspekt, dass Netzwerke in der Regel für 3 bis 6 Jahre geplant werden. Wer also heute sein Netzwerk anfasst, der muss deutlich in die Zukunft denken. Bei Kabeln sind das sogar in der Regel 10 Jahre. Aus diesem Blickwinkel können neue Anwendungsbereiche, die heute noch klein und harmlos erscheinen, schon in wenigen Jahren zu deutlichen Herausforderungen im Netzwerkbereich werden. Man mache sich zum Beispiel klar, dass technisch gesehen für Provider die gelieferte Bandbreite unwichtig wird (von der Belastung des Core-Netzwerks einmal abgesehen), wenn man erst einmal den Schritt weg von 34 Mbit/s hin zu Glasfaser und Ethernet gemacht hat. Da wir genau an dieser Schwelle stehen und führende Provider mehr und mehr ihre Kunden in Richtung 100 MBit/s und Gigabit-Ethernet im WAN drängen, muss man sich auch der Frage stellen, was das eigentlich in drei Jahren bedeutet, wenn für große Unternehmen das Gigabit-WAN die Normalität wird. An dieser Stelle sei noch einmal auf die Liste zu Beginn dieses Geleitworts verwiesen. Neue Applikations-Architekturen und mehr Bandbreite gehen Hand in Hand. Gleiches gilt für die Konzentration von Servern und Speicher im Rechenzentrum. Hier besteht ein ernsthaftes Risiko, dass dies bei der Neuplanung von Netzwerken unterschätzt wird. Auch ein Seitenvermerk an dieser Stelle: würde die Einführung von Terabit-Switches durch die Hersteller reduziert auf den RZ-Bereich für die Hersteller wirklich Sinn machen? Diese neue Generation von Terabit-Switchen ist der Vorbote einer generellen neuen Generation von Backbone- oder Core-Geräten. Wie weit muss man nun nach vorne schauen, um bewährte aber in die Jahre gekommene Switch-Familien, die sie alle kennen, in Frage zu stellen?

Wie Sie sehen, wird 2009 wieder einmal ein spannendes Jahr. Ohne Netzwerke wird in Zukunft nichts mehr gehen, aber damit es mit Netzwerken geht, müssen diese weiter entwickelt werden.

In diesem Sinne freue ich mich auf viele und kontroverse Diskussionen auf dem ComConsult Netzwerk-Redesign Forum 2009 .

Ihr
Dr. Jürgen Suppan

Aktueller Kongress

# Netzwerk-Redesign Forum 2009

**Die ComConsult Akademie veranstaltet vom 09.03. - 12.03.09 ihren Kongress „ComConsult Netzwerk-Redesign Forum 2009“ in Königswinter.**

Netzwerke sind der Lebensnerv unserer Unternehmen. Sie unterliegen einer permanenten Weiterentwicklung und Veränderung. Aus einem Mix aus Bedarf und technischen Möglichkeiten muss das individuelle Optimum für ein Unternehmen gefunden werden. Dieses Optimum muss zugleich an der Zukunft orientiert sein, da Netzwerk-Komponenten über einen langen Zeitraum stabil und ohne permanente Änderungen betrieben werden müssen.

Hier setzt das ComConsult Netzwerk-Redesign Forum 2009 an. Es analysiert die wichtigsten Bedarfsentwicklungen, stellt diesen die neuesten Netzwerk-Technologien gegenüber und erarbeitet Empfehlungen für ein erfolgreiches Netzwerk-Design, eine Zukunfts-oriente Auslegung und einen stabilen und zuverlässigen Betrieb.

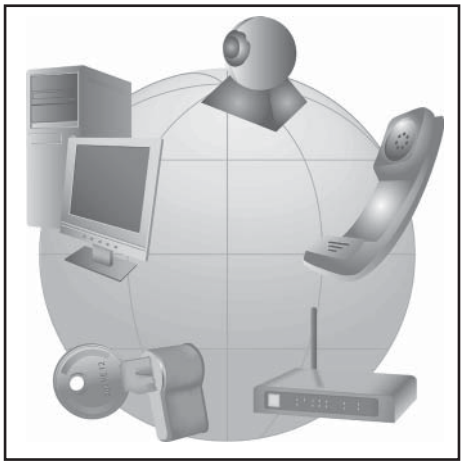
Die Schwerpunktthemen des ComConsult Netzwerk-Redesign Forums 2009 sind:

**Neue Redundanz-Verfahren**
Wieder einmal sind Redundanz-Verfahren im Mittelpunkt der Diskussion. Immer wieder wird in Projekten eine Art von Netzwerk-Redundanz gefordert, die laufende Sprach- und Video-Verbindungen nicht unterbricht. Dies wird häufig mit Umschaltzeiten von unter 100 ms verbunden. Traditionelle Redundanz-Verfahren leisten sich Umschaltzeiten bis in den Minuten-Bereich und stehen immer häufiger in der Kritik.

Wir analysieren:

- Was ist Stand der Redundanz-Technik in Layer-2 und Layer-3?
- Was kommt auf uns zu?
- Was passiert im direkten Umfeld von Server und Speicher-Systemen?
- Welchen Stellenwert haben Hersteller-Spezifische Lösungen?
- Cisco, Enterasys, Extreme, Foundry, HP, Juniper, Nortel: wer macht was?
- Standardisierung: was ist Zukunfts-orientiert, wie können Investitionen und ein stabiler Betrieb geschützt werden?

**Layer-2 kontra Layer-3**
Ein altes Thema, aber wieder hochaktuell. Immer wieder besteht der Bedarf nach großen und auch Flächen-deckenden Layer-2-Netzwerken. Zum Teil wird auch eine Layer-2-Verbindung zwischen Standorten



gefordert. Rechenzentren, Industrie-Umgebungen und Remote Speicher-Kopplungen sind Beispiele dafür.

Wir analysieren:

- Große Layer-2-Netzwerke: wo liegen die Probleme heute?
- Integration oder Parallelbetrieb mit Layer-3: welche Optionen bestehen?
- Standort-Kopplungen mit Layer-2: Proprietär kontra Standard, welcher Weg ist Zukunfts-orientiert?

**Verkabelung 2009**
Cat 6, 6a, 7, 7a, immer mehr Stecker-Alternativen, Multimode OM2, OM3, OM4, auch hier immer mehr Alternativen im Stecker. Dies kombiniert mit Anforderungen im Rechenzentrum für 10 und zukünftig 40 Gigabit: wie sieht die Zukunfts-sichere Verkabelung aus? Betrachtet man die zu erwartende Nutzungsdauer von 10 Jahren und mehr, dann muss bei Neuinstallationen auch 100 Gigabit berücksichtigt werden. Die aktuellen und in Arbeit befindlichen Standards bieten viele Alternativen, doch welche werden sich durchsetzen? Schon heute unterstützen nicht alle Hersteller alle Varianten.

Wir analysieren:

- Verkabelungstechnik 2009: wo stehen wir?
- Twisted Pair: welche Kabel-Qualität, welcher Stecker?
- Glasfaser: Multimode kontra Singlemode, OM2 kontra OM3 kontra OM4, welcher Stecker prägt die Zukunft?
- Was unterstützen die Hersteller?
- Hoher Bestand aus Cat 5 oder Cat 6 und OM2: was ist zu tun?

**MPLS kontra Carrier-Ethernet kontra OSPF**
Mit Carrier-Ethernet geht ein neuer Stern am Horizont auf. Dabei ist der Name mehr als irreführend, da die Technologie nicht auf Carrier begrenzt ist. Real ist die Technologie in verschiedensten Einsatz-Szenarien interessant. Diese reichen vom Corporate-Netzwerk zwischen verschiedenen Standorten über große Backbone-Netzwerke bis hin zu Spezial-Anwendungen im Industrie-Bereich. Carrier-Ethernet realisiert standardisierte Layer-2-Netzwerke mit extrem kurzen Umschaltzeiten in der Redundanz. Damit ist auch die Basis für jede denkbare Diskussion gelegt (siehe: Layer 2 kontra Layer 3).

Wir analysieren:

- Was ist Carrier-Ethernet, für wen ist es eine Option?
- CE kontra MPLS: ist dies das Ende von MPLS?
- CE im Unternehmens-Backbone: wirklich eine Alternative?
- Große Layer-2-Netzwerke in der Industrie: wird CE die bisher dort dominierenden Verfahren verdrängen?

**Wireless-Netzwerke**
Atheros hat das Ende von 802.11g eingeläutet. 802.11n ist nun das Maß aller Dinge. Gleichzeitig werden Wireless-Switches in professionellen Installationen fast unvermeidbar. Dies kombiniert mit besonderen Anforderungen spezieller Umgebungen von der Industrie bis zur Filial-Organisation ergibt einen brisanten Technologie-Mix.

Wir analysieren:

- Was passiert zurzeit bei Wireless-Technologien, wohin geht der Weg?
- Was leistet 802.11n? Als Ersatz für Kabel-gebundene Netzwerke geeignet?
- Strombedarf der Access-Points: ein Auswahl-Kriterium?
- Wie viele Radioteile sind für eine Zukunfts-Orientierung sinnvoll?
- Was leisten Wireless-Switches? Wo unterscheiden sich die Produkte? Zeit für einen Standard, wo steht CAPWAP?
- Ist MESH die Zukunft? Ist dies mehr als eine Wireless-Technologie, ist dies die Basis für eine neue Art von Kommunikations-Architektur?
- Wireless LAN in der Industrie: was ist anders?
- Wireless LAN in Filial-Organisationen: welche Technologie ist optimal?

Netzwerk-Redesign Forum 2009

**Sicherheit**
Der Bedarf nach Sicherheit wächst immer weiter. Dies umfasst sowohl die Kontrolle des Zugangs zu wichtigen Servern, Applikationen und Daten als auch die Verhinderung einer gegenseitigen Beeinflussung von Applikationen im Netzwerk. In keinem Fall darf ein Fehlverhalten einer Applikation oder eines Benutzers andere Applikationen oder Benutzer stören. Die technologischen Ansätze im Bereich Sicherheit sind weitreichend und vielfältig, aber zum Teil Hersteller-gebunden und inkompatibel. Wie kann man hier zu einer sinnvollen und noch beherrschbaren Lösung kommen?

Wir analysieren:

- Was bietet der Markt?
- Was leisten neue Standards wie MACsec und 802.1X-REV?
- Wie können Benutzer- und Applikationstrennung realisiert werden?
- NAC, 802.1x und ähnliche Technologien: wie kann in diesem Wald aus Hersteller-spezifischen und zum Teil nicht kompatiblen Lösungen ein sinnvoller und angemessener Weg gefunden werden, der nicht zum Overkill wird?

**Integration mobiler Mitarbeiter/Fixed-Mobile-Konvergenz**
Einbindung aller relevanten Mitarbeiter in die wichtigen Geschäftsprozesse, egal wo sich diese befinden. Das Thema ist nicht neu, aber die technischen Möglichkeiten verändern sich. Mehr Bandbreite, neue Gerätetechnologien, andere Applikations-Architekturen schaffen die Voraussetzung für mehr Effizienz und Erfolg mobiler Mitarbeiter.

Wir analysieren:

- Fixed-Mobile-Konvergenz: was bedeutet das?
- Wohin geht der weitere Weg? Wie groß sind die Potenziale wirklich?
- Wie gut und nutzbar sind die Produkte?

**WAN-Redesign**
Weiterverkehrs-Konzepte sind im Umbruch. Das zunehmende Angebot von Gigabit Ethernet in Ballungsräumen, der weitere Verfall der Preise, das alles schafft die Basis für neue IT-Architekturen. Wichtige neue Anwendungsbereiche wie SOA basieren auf dieser Weiterentwicklung. Desaster Recovery bekommt ohne Frage eine neue Dimension.

- Wir geben den Überblick: was passiert im WAN?
- Welche Leistungen entstehen, wie weit kann das gehen?

Das ComConsult Netzwerk-Redesign Forum 2009 ist die zentrale Netzwerk-Veranstaltung des Jahres 2009. Sie ist für jeden Entscheider, Planer und Betreiber in diesem Bereich ein absolutes Muss. Hier trifft sich die Branche.

Sichern Sie sich rechtzeitig einen Platz in dieser herausragenden Veranstaltung!

Fax-Antwort an ComConsult 02408/955-399

# Anmeldung
# Netzwerk-Redesign Forum 2009

Ich buche den Kongress
**Netzwerk-Redesign Forum 2009**
09.03. - 12.03.09 in Königswinter

**mit „Ein-Tages-Intensiv-Trainings zum Preis von € 2.290,- zzgl. MwSt.**

☐ Session 1: Der ComConsult Design-Wettbewerb 2009

☐ Session 2: Projektbericht: IT-Konzept für Filialen

☐ Session 3: Ethernet im Wandel

☐ **ohne „Ein-Tages-Intensiv-Trainings zum Preis von € 1.890,- zzgl. MwSt.**

☐ Bitte reservieren Sie für mich ein Hotelzimmer

vom_____ bis_____09

Buchen Sie über unsere Web-Seite
**www.comconsult-akademie.de**

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

# Programmübersicht Netzwerk-Redesign Forum 2009

## Montag, den 09.03.2009

**9:30 bis 10:45 Uhr**
**Bedarfsanalyse: was muss ein Netzwerk in Zukunft leisten?**
- IT-Architekturen und Netzwerk-Strukturen: Teilnehmer, Orte, Datenströme
- Anwendungs-Technologien und Architekturen: was ist kritisch?
- Server-Technologien und Rechenzentren: was muss das Netzwerk leisten?
- Resultierendes Anforderungsprofil: Netzwerk der Zukunft
  - Bandbreite • Antwortzeit
  - Verfügbarkeit • Layer 2 kontra Layer 3
  - Verfügbarkeit und Reaktion auf Störungen
- Konsequenzen für bestehende Netzwerke
- Konfliktpunkte im Redesign

*Dr. Jürgen Suppan, ComConsult Research*

**11:15 bis 12:30 Uhr**
**Redundanzverfahren im Vergleich**
- Neue Anforderungen an Redundanz: was ist zu tun?
  - Kurze Konvergenzzeiten für Voice- und Video
  - Verfügbarkeit: Parallelnutzung kontra Standby
  - Layer-2-Redundanz im Rechenzentrum und der Produktion
- Redundanzverfahren auf verschiedenen Protokollebenen im Vergleich:
  - Protection auf SDH- und OTN-Ebene, Link Aggregation in der Weiterentwicklung, Spanning Tree, Virtuelle Switchsysteme / Virtuelle Router, Routing-Protokolle, Cluster Services
- Empfehlungen zum Einsatz

*Dipl.-Inform. Petra Borowka, Unternehmensberatung Netzwerke UBN*

**14:00 bis 14:45 Uhr**
**Layer-2 kontra Layer-3:**
**neue Anforderungen ändern Netzwerk-Design**
- Neuer Bedarf für große Layer-2-Bereiche: was tun?
  - Rechenzentren • Produktionsumgebungen
  - Speicher-Netzwerke • Standort-Kopplungen
- Vor- und Nachteile von Layer-2- und Layer-3-Strukturen
- Einsetzbare Technologien
- Ist Layer 2 im WAN sinnvoll?
- Empfehlungen und Lösungsansätze

*Dipl.-Inform. Petra Borowka, Unternehmensberatung Netzwerke UBN*

**14:45 bis 16:00 Uhr**
**Carrier Ethernet auch für Unternehmensnetze,**
**werden bestehende Backbone-Technologien in Frage gestellt?**
- Motivation: Grenzen bisheriger Backbone-Technologien
- Carrier Ethernet Standards: MEF, IEEE, ITU
- Carrier Ethernet Services: E-Line, E-LAN, E-Tree
- Carrier Ethernet im Detail: Vor- und Nachteile
- Kontra MPLS: wer wird gewinnen?
- Ist Carrier Ethernet auch für Unternehmensnetze geeignet?

*Dr. Franz-Joachim Kauffels, Unternehmensberater*

**16:30 bis 17:15 Uhr**
**Technologie-Analyse: Verkabelung 2009**
- Welche Anforderungen werden die nächsten 10 Jahre prägen?
- Kupfer versus LWL: Bringt High Speed Ethernet den Durchbruch der Glasfasern?
- Kategorie 6, 6A, 7: was ist besser?
- OM-2, OM-3, OM-4 und Singlemode: welche Fasern wo einsetzen?
- Welche Stecker für Kupfer und LWL?
- Hoher Bestand aus Kategorie 5/6 und OM-2: was tun?

*Dipl.-Ing. Hartmut Kell, ComConsult Beratung und Planung GmbH*

**17:15 bis 18:00 Uhr**
**Netzwerk-Technologien der nächsten Jahre:**
**von Gigabit Wireless bis Terabit Ethernet**
- Impulse aus der optischen Übertragungstechnologie
- 10/40/100 Gb Ethernet
- Generisches optisches Transceiverdesign
- Gigabit Wireless: was kommt nach 802.11n ?
- Zusammenfassende Prognose und Konsequenzen

*Dr. Franz-Joachim Kauffels, Unternehmensberater*

**10:45 - 11:15 Uhr Kaffeepause**
**12:30 - 14:00 Uhr Mittagspause**
**16:00 - 16:30 Uhr Kaffeepause**
**ab 18:00 Uhr Happy Hour**

## Dienstag, den 10.03.2009

**9:00 bis 10:15 Uhr**
**Was ist die richtige Lösung für mandantenfähige Netze?**
**Wie kann eine dynamische Zuordnung von Endgeräten erfolgen?**
- VLAN, VRF, MPLS, Port-basierende Policies und Filter: wie sie funktionieren
- Was ist die richtige Lösung?
- Tücken der dynamischen Zuordnung von Endgeräten in mandantenfähigen Netzen
  - Wie funktioniert die dynamische VLAN-Zuordnung?
  - Was müssen die Access Switches leisten?
  - Was müssen die Authentisierungsserver leisten?
  - Gibt es spezielle Anforderungen an Endgeräte und Netzbetriebssysteme?
  - Sind mandantenfähige Netze mit gemischten Produkten möglich?

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

**10:15 bis 11:15 Uhr**
**Von der Geräteauthentisierung bis zu sicheren Netzen**
- Grenzen der reinen Geräteauthentisierung
- MAC Security gemäß IEEE 802.1AE
- Ausblick auf die neue Version von IEEE 802.1X
- Pre-Standard-Lösungen und was gibt es neben Cisco TrustSec?
- Konsequenzen für den Aufbau von Sicherheitszonen

*Dr. Simon Hoff, ComConsult Beratung und Planung GmbH*

**11:45 bis 12:30 Uhr**
**Cisco-Systems: Investitionssicherheit,**
**wohin tendieren die Produktlinien?**
- Positionierung Nexus Switches
- Hat der Catalyst 6500 eine Zukunft?

*N.N.*

**14:00 bis 14:45 Uhr**
**Enterasys: Architekturen für Netzwerk-Sicherheit,**
**wohin geht der Weg?**
- Wie viel Sicherheit und Kontrolle brauchen LANs?
- Intelligenz auf den Clients und Servern, im Kern oder am Rand des Netzes?
- Wo steht NAC?
- Integrierte LAN-Voice-Sicherheit: was bringt die Integration mit Siemens EN?

*Dipl.-Ing. Markus Nispel, Enterasys Networks Deutschland GmbH*

**14:45 bis 15:30 Uhr**
**HP Procurve: wo positioniert sich HP in Zukunft?**
- Was ist besser: MPLS, VRF oder Port-basierende Policies?
- Kommt ProCurve auch in die Rechenzentren?

*Thorsten Meudt, Hewlett-Packard Deutschland GmbH*

**16:00 bis 16:45 Uhr**
**Juniper-Networks: wohin geht der Markt für Access Switches?**
- LANs mit heterogenen oder homogenen Produkten?
- Access-Switches: Ist das ein Markt für Billig- oder Premiumanbieter?

*Willi Duetsch, Juniper Networks*

**17:00 bis 17:30 Uhr**
**Podiums-Diskussion: Netzwerke 2009: wohin geht der Weg?**
- Bedeutung von Carrier Ethernet
- Bedarf für neue Redundanz-Technologien
- Layer-2 kontra Layer-3: Neupositionierung erforderlich
- Wie wichtig sind Standards?

**11:15 - 11:45 Uhr Kaffeepause**
**12:30 - 14:00 Uhr Mittagspause**
**15:30 - 16:00 Uhr Kaffeepause**

# Programmübersicht Netzwerk-Redesign Forum 2009

## Mittwoch, den 11.03.2009

**09:00 bis 10:00 Uhr**

**Wireless-Technologien: eine echte Alternative zum Kabel?**

- Aktuelle Trends der Wireless-Technik
- Ist IEEE 802.11n als Ersatz für kabelgebundene Netze geeignet?
- Strombedarf der Access Points: ein Auswahlkriterium?
- Wie viele Radioteile sind für eine Zukunftsorientierung sinnvoll?
- Unterschiede zwischen Wireless-Switches, wie wichtig sind die?
- Wireless Mesh Networks: Megatrend oder nur eine von mehreren denkbaren Varianten?
- WLAN in der Industrie: was ist anders?
- Welche WLAN-Variante in Filialen?

*Dipl.-Ing. Björn Korall, Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH*

**10:00 bis 10:45 Uhr**

**CAPWAP: Wireless-Controller verschiedener Hersteller mischen?**

- Was leistet CAPWAP?
- Wie stehen die Hersteller dazu?
- KO-Kriterium für die Ausschreibung?
- Neueste Entwicklung: Femtocell Security

*Dipl.-Inform. Petra Borowka, Unternehmensberatung Netzwerke UBN*

**11:15 bis 12:00 Uhr**

**Stromversorgung im Wandel**

- IEEE 802.3at und die Folgen
- Stromsparende Netzkomponenten
- Stromsparende Netzstrukturen

*Dr. Michael Wallbaum, Dipl.-Inform. Matthias Egerland, ComConsult Beratung und Planung GmbH*

**12:00 bis 12:30 Uhr**

**Applikationsoptimierung versus Verkehrsoptimierung im WAN**

- Grundsätze der Applikationsoptimierung
- Sinn und Grenzen der Verkehrsoptimierung durch WAN Optimizer
- Empfehlungen zum Einsatz

*Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH*

**14:00 bis 14:45 Uhr**

**Integration mobiler Mitarbeiter**

- Mobile Endgeräte mit diversen Netzschnittstellen: Albtraum für die IT-Sicherheit?
- Wie lassen sich mobile Endgeräte in unterschiedlich sicheren Umgebungen einsetzen?
- Management von Smart Phones - eine Sysiphosarbeit?

*Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH*

**14:45 bis 16:15 Uhr**

**Unified Communications und die Folgen für Netze**

- Von VoIP zu Unified Communications
- Bedarf für mehr als Telefonie und E-Mail
- VoIP und Video
- Konzepte der Hersteller
- Die besondere Rolle Microsofts
- Konsequenzen für Netzwerke

*Dr. Frank Imhoff, ComConsult Beratung und Planung GmbH*

**10:45 - 11:15 Uhr Kaffeepause**
**12:30 - 14:00 Uhr Mittagspause**
**15:30 - 15:45 Uhr Kaffeepause**

## Donnerstag, den 12.03.2009 - Ein-Tages-Intensiv-Trainings/Workshops - 09:00 - 15:30 Uhr

**Die Sessions laufen parallel über den ganzen Tag!**
**BITTE BEI DER ANMELDUNG EIN THEMA ANKREUZEN!!**

**Session 1:**

**Der ComConsult Design-Wettbewerb 2009**

Teilnehmende Hersteller: Ausschreibung läuft zur Zeit

- Vorstellung der Design-Aufgabe
- Hersteller präsentieren ihre Lösung
- Diskussion der vorgestellten Lösungen mit den Teilnehmern

*Dipl.-Inform. Petra Borowka, Unternehmensberatung Netzwerke UBN*

**Session 2:**

**Projektbericht: IT-Konzept für Filialen**

- Definition von Standards und Warenkörben
- Bereitstellung zentraler Infrastrukturdienste
- IP, Active Directory, Exchange, Dateidienste, Softwareverteilung …
- Definition und Integration verschiedener Standortklassen (Headquarter, Kontinentmanagement, Produktion, Office ...), Ressourcenplanung bzw. –prüfung für die einzelnen Klassen (teilweise personalfreier Betrieb?)
- Konzipierung und Rollout eines Standardclients
- Prozessorientiertes Vorgehen bei der Migration
- Projektplanung, Projektkommunikation (verschiedene Länder – verschiedene Sitten)
- Planung und Durchführung der weltweiten Migration
- Weiterentwicklung auf Basis der Erfahrung einer 3rd-Level-Betreuung
- Integration neuer Techniken (Unified Communications, Windows Server 2008, Exchange 2007, Virtualisierung)

*Markus Holländer, Dipl.-Inform. Michael van Laak, ComConsult Beratung und Planung GmbH*

**Session 3:**

**Ethernet im Wandel**

- 10/40/100 Ethernet
  - Wozu mehr Bandbreite? Auswirkung des Virtualisierungstrends auf die Netze
  - 10 GBASE-LRM, preiswert auf Multimode: Anforderungen an die Verkabelung
  - IEEE 802.3 ba 40/100 Gigabit Ethernet: Struktur und Varianten für WAN/RZ
  - Pre-Standard-Produkte: 40 GBASE-LX(4) schon jetzt zu sehen
- Data Centre der Zukunft
  - Data Centre Ethernet (DCE) und Converged Enhanced Ethernet CEE
  - Fiber Channel over Ethernet vs. iSCSI: Lossless Ethernet, Congestion Control
  - Brocade, Cisco, EMC, HP etc.: Wer ist der Gewinner der neuen Trends?
- Die bunte Welt der neuen Zugangstechniken
  - FTTx: Fiber To The Home, Curb etc.
  - EFM: Ethernet in the First Mile
  - EPONs: Ethernet over Passive Optical Networks
- Ausgewählte Hersteller präsentieren ihre Lösungsansätze
  - Was können Provider-Technologien in Unternehmensnetzwerken leisten?
- Was ist besser: Q-in-Q, PBB, VPLS?

*Dr. Franz-Joachim Kauffels, Unternehmensberater*

**10:30 - 11:00 Uhr Kaffeepause**
**13:00 - 14:00 Uhr Mittagspause**
**15:30 Ende der Veranstaltung**

Der Veranstalter behält sich Änderungen im Programm vor! Irrtümer und Tippfehler vorbehalten!

Neuer Kongress

# ComConsult Verkabelungs- und Infrastrukturforum 2009

**Die ComConsult Akademie veranstaltet vom 27.04 - 28.04.09 ihren Kongress „ComConsult Verkabelungs- und Infrastrukturforum 2009“ in Bonn.**

Verkabelungsprojekte werden aktuell mit einer Reihe komplexer Fragen konfrontiert, die insbesondere dadurch erschwert werden, dass eine anwendungsneutrale Kommunikationsverkabelung in der Regel auf 10 Jahre Nutzungsdauer ausgelegt wird:

Twisted Pair Fragen

- mit welchen Datenraten ist in den nächsten 10 Jahren an welchen Stellen zu rechnen?
- Kat 6a kontra Kat 7a, was ist das richtige Kabel? Welchen Mehrwert bringt die im Vergleich deutlich teurere 7a-Verkabelung?
- wie ist mit bestehenden Kat 5 und Kat 6 Verkabelungen umzugehen, müssen diese ersetzt werden oder gibt es wirtschaftliche „Aufrüst“-Lösungen?
- welchem Stecker gehört die Zukunft? Wohin tendieren die Komponenten-Hersteller?
- wie ist mit Kabel-Sharing umzugehen, hat das noch eine Zukunft?
- IP-Telefonie und Datenverkabelung: separat oder integriert? Was ist die wirtschaftlich und technisch optimale Anschlussdichte?

Glasfaser-Fragen

- mit welchen Datenraten ist in den nächsten 10 Jahren an welchen Stellen zu rechnen, ist bei 40 oder 100 Gigabit ein sinnvolles Maximum erreicht?
- welche Faser ist für welche Entfernung und welche Datenrate optimal?
- Hat sich die OM3-Faser im Multimode-Bereich durchgesetzt und wie können mögliche Vorteile genutzt werden?
- Müssen Nutzer von OM2-fasern mit Nachteilen rechnen? Was ist hier zu tun?
- Sollte überhaupt noch Multimode verlegt werden oder ist nun endlich die Zeit der reinen Single.Mode-Verkabelung gekommen?
- Brauchen wir einen neuen Glasfasersteckertyp? Welche Stecker werden diskutiert? Wo liegen Vor- und Nachteile? Was machen die Komponenten-Hersteller, die dieses Rennen letztendlich entscheiden?
- Lassen sich Umgebungen mit gemischten LWL-Steckertypen überhaupt vermeiden, wie ist damit umzugehen?

Spezialthema:
Rechenzentrumsverkabelung

- Welche Bandbreiten werden hier gefordert?
- Wird überhaupt eine spezielle Verkabelung gefordert oder reicht die bestehende Technik der Arbeitsplatzverkabelung aus?
- Welche Kabel- und Steckertechnik wird durch die Server- und Speicher-Hersteller bevorzugt werden?
- Wie ist mit den extrem hohen Packungsdichten umzugehen?
- Was machen die Switch-Hersteller, wie sieht das zukünftige Aktiv-Szenario für das Rechenzentrum aus?

An diesen Fragen setzt unser hochaktuelles ComConsult-Verkabelungsforum 2009 an. Top-Verkabelungsexperten informieren Sie über die neuesten Entwicklungen und stellen sich der Diskussion. Diese Veranstaltung ist ein absolutes Muss für jedes Verkabelungs-Projekt.

Folgende Vorträge sind geplant (Änderungen vorbehalten!):

- Videoüberwachung mit Hilfe von Lokalen Netzwerken
- Gigabit-Netzwerk-Technologien und ihre Anforderungen an Kabel und Anschlusstechnik: Anforderungen bei Einführung von mehr als 10 Gbit/s über Kupfer
- Kabelstandardisierung: was ist neu, was passiert hinter den Kulissen
- Installations-„Sünden“ bei der Kommunikationsverkabelung
- Nutzbarkeit von modernen Kommunikationsverkabelungen für Meldeanlagen und Automatisierungsbereiche
- Sanierung bestehender Verkabelungen in Rechenzentren und Serverräumen: wo und wann besteht Bedarf, welche Vorgehensweise ist zu empfehlen, welche Alternativen bestehen
- Elektrische Sicherheit beim Redesign von RZ-Infrastrukturen
- Green IT im RZ
- Netzwerk-Dokumentation gestern und heute
- Normen und Standards zur Messtechnik: Notwendigkeit, Defizite und Ergänzungen
- Zukunftssicherheit durch Glasfaser bis zum Arbeitsplatz, Illusion oder Realität?
- Moderner Brandschutz bei IT-Verkabelung; Lösungen, Techniken und Gefahren

Dieses Forum bietet die ideale Basis für eine Standortbestimmung. Wer immer sich für die zukünftigen neuen Aufgaben einer Kommunikationsverkabelung vorbereiten muss, wer nach sinnvollen Alternativen und Empfehlungen für optimale Lösungen sucht, der sollte dieses Forum nicht verpassen. Die Frühbucherphase für diesen Kongress läuft nur bis Donnerstag. Melden Sie sich jetzt an!

ComConsult Verkabelungs- und Infrastrukturforum 2009

# Frühbucherrabatt bis 15.01.09

# ComConsult Verkabelungs- und Infrastrukturforum 2009

## 27.04. - 28.04.09 in Bonn

**Für Besucher unserer bisherigen Kongresse bzw. für die Teilnehmer am VIP-Verteiler bieten wir Ihnen exklusiv eine Vorbuchungsphase für das ComConsult Verkabelungs- und Infrastruktur-forum 2009 bis zum 15.01.2009 für eine rabattierte Teilnahmegebühr an.**

**ComConsult Verkabelungs- und Infrastrukturforum 2009**
**zum Preis bei Buchung bis 15.01.09 von € 1.490,-**
**statt regulär € 1.690,- zzg. MwSt.**

**Die Buchung innerhalb der Frühbucherphase ist verbindlich, kann aber jederzeit auf einen anderen Mitarbeiter Ihres Unternehmens übertragen werden.**

Fax-Antwort an ComConsult 02408/955-399

# Anmeldung

# ComConsult Verkabelungs- und Infrastrukturforum 2009

Ich buche den Kongress
☐ **ComConsult Verkabelungs- und Infrastrukturforum 2009**
27.04. - 28.04.09 in Bonn
zum Preis von € 1.490,-* zzgl. MwSt.

*gültig bis zum 15.01.09 - dann regulärer Preis € 1.690,- zzgl. MwSt.

☐ Bitte reservieren Sie für mich ein Hotelzimmer

Buchen Sie über unsere Web-Seite
**www.comconsult-akademie.de**

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

Zweitthema

# 40 GBASE-T

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.

Die CX-Varianten über Twinax-Kabel sind zwar technisch hervorragend und werden häufig verbaut, alleine weil Hersteller wie HP sie in den Switch Blades der Blade-Server einbauen, haben aber längst nicht die psychologische Wirkung.

Die brennende Frage ist jetzt natürlich, ob es auch 40 GBASE-T geben wird. Bis zum Spätherbst 2008 konnte niemand diese Frage beantworten. Dann gelang Wissenschaftlern der Penn State University jedoch der Durchbruch:

50 Gigabit pro Sekunde über 100m Twisted Pair Kabel der Kategorie 7A!!!

Damit wurden schon zwei für die Planung enorm wichtige Dinge erarbeitet:

- es gibt ein Twisted Pair Kabel, welches für 40 GBASE-T geeignet ist
- es gibt einen geeigneten Stecker

Dieses Ergebnis hat eine herausragende Rolle bei der Planung. Selbst wenn es momentan noch keinen Standard für 40 GBASE-T gibt und selbst wenn man in absehbarer Zeit noch kein 40 GbE einsetzen wird, kann man die Verkabelung bereits zukunftsfest planen. Das ist enorm wichtig vor dem Hintergrund der langen Lebensdauer von Verkabelungssystemen.

Aber auch für die Standardisierung ist dieses Ergebnis besonders wichtig. Beim Entwurf des Standards für die Transceiver und deren Eigenschaften kann man nämlich auf die bereits festliegenden Charakteristika des Kabels oder des durch das Kabel gebildeten physikalischen Übertragungskanals zurückgreifen. Die Standardisierung von 10 GBASE-T war deshalb so langwierig, weil es zunächst einen derartigen Zusammenhang nicht gegeben hat. So gab es innerhalb des Standardisierungsprozesses eine Vielzahl von Alternativen für unterschiedliche reale und gedachte Kabelspezifikationen. Das hat ja in der Folge dazu geführt, dass zunächst der Standard für 10 GBASE-T festgeschrieben wurde und erst anschließend der Standard für das dazu passende Kat. 6A-Kabel.

Es sei allerdings hier direkt angemerkt, dass es einen erheblichen Unterschied zwischen der Standardisierung von 10 GBASE-T und 40 GBASE-T gibt. Im Bereich 10 GbE hat man viel Zeit damit verloren, einen Standard für ungeschirmte UTP-Kabel (Kat 5) zu entwickeln. Bei 40 GbE ist von Anfang an klar, dass es eine Lösung nur für geschirmte STP-Kabel geben kann.

Auch das Kabel der Kat. 7A befindet sich z. Zt. in der Normung. Allerdings gibt es schon einige Hersteller, die ein solches Kabel anbieten. Wir beziehen uns im Folgenden auf das Produkt LANmark 7A von Nexans.

Das 7A-Kabel ist in seinen Eigenschaften bis 1000 bzw. 1200 MHz definiert, geht also weit über den bisher definierten Bereich hinaus. Das 6A-Kabel ist in der Norm nur bis 250 MHz definiert, normtreue Produkte sind bis zu 500 MHz spezifiziert.

Die Eckdaten des 7A-Kabels sind:

- NEXT (Nahnebensprechdämpfung): 60 dB bei 1000 MHz
- FEXT (Fernnebensprechdämpfung): 50 dB bei 1000 MHz
- RL (Return Loss): 8 dB bei 1000 MHz
- ANEXT (Fremdnebensprechdämpfung): 0 dB bei 1000 MHz (!!!)

ANEXT wird auch häufig als „Alien Crosstalk“ bezeichnet, das kommt von den „Alien“-Filmen und bezeichnet die Angst vor diesem Effekt. Das LANmark7A-Kabel ist völlig abgeschirmt (natürlich nur bei richtiger Installation), so dass die „Aliens“ hier keinen weiteren Schaden anrichten können.

→ Cat. 6A für 10 GBASE-T spezifiert

→ Cat. 7A in der Diskussion, aber es gibt schon Punkte, Beispiel Nexans LANmark-7A

| | **LANmark-7A** | **Category 6A** |
|---|---|---|
| • NEXT | 60dB at 1000MHz | 30dB at 500MHz |
| • FEXT | 50dB at 1000MHz | 25dB at 500MHz |
| • RL | 8dB at 1000MHz | 8dB at 500MHz |

→ NEXT: Nahnebensprechdämpfung

→ FEXT: Fernnebensprechdämpfung

→ RL: Return Loss

Abbildung 1: Cat. 6A und Cat. 7A

Das sind Werte, die die von bisher bekannten Kabeln erheblich in den Schatten stellen. Zum Vergleich siehe Abbildung 1.

Der ANEXT-Wert ist sensationell. Eine Schwierigkeit bei 10 GBASE-T war es, das für ein Kabel relativ empfindliche Signal vor den von außen kommenden Störeinflüssen zu retten. In anfänglichen Versionen konnte das Signal auch schon mal völlig untergehen. Erreicht wird diese Qualität durch eine S/FTP-Konstruktion mit vier geschirmten Paaren und einem Gesamtschirm.

→ S/FTP-Konstruktion mit vier individuell geschirmten Paaren
→ Leistung bis zu 1200 MHz
→ KEIN (!!!) Fremdnebensprechen

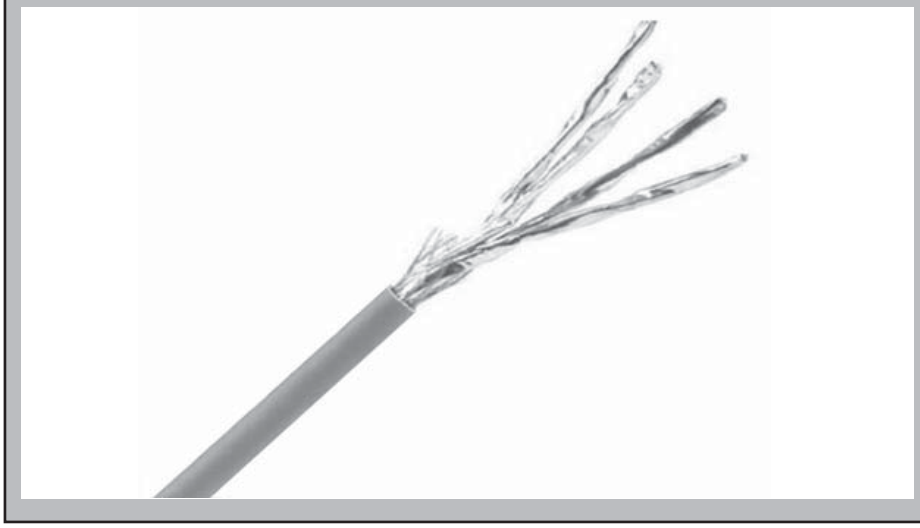


Abbildung 2: Cat. 7A-Kabel

Nun brauchen wir noch den passenden Stecker. Da bietet sich der GG45-Stecker an. Der GG45-Stecker hat 12 Kontakte. Der „2in1“ Connector kombiniert RJ45 und GG 45. Dadurch entstehen zwei Modi:

- RJ45 Modus bis 500 MHz für 1 und 10 GBASE-T
- GG45-Modus bis 1000 MHz für 40 GBASE-T

Der GG45-Stecker passt zu Cat 7A-Kabeln. Er ist bereits jetzt völlig standardisiert ISO/IEC 60603-7-7. Der RJ45-Modus ist zwingend nach ISO 11801 für die Gewährung von Rückwärtskompatibilität. (siehe Abbildung 3)

Ein alternativer Stecker wäre der IEC 61076-3-104-Stecker, der von Siemon entwickelt wurde. Er hat ein neues Steckergesicht und ist deshalb nicht rückwärtskompatibel. Außerdem wurde das eingangs genannte Ergebnis mit einer Kombination des LANmark 7A-Kabels und GG45-Steckern erzielt. Wir beziehen und im Folgenden also ausschließlich darauf.

**Anwendungen für 40 GBASE-T**

Was sind mögliche Anwendungen für 40 GBASE-T? Zunächst geht es um eine Marktverbreiterung für 40 Gigabit Ethernet schlechthin. Auch bei Gigabit Ethernet und 10 GbE war es ja schließlich so, dass der Markt erst dann richtig zugegriffen hat, als die Kupferversionen verfügbar waren. Komischerweise wurden dann auch massenhaft Glasfaserschnittstellen gekauft. Der Markt ist nicht wirklich logisch, aber hinsichtlich seiner grundsätzlichen Mechanismen ganz gut durchschaubar. Über die Anwendungsmöglichkeiten von 40 Gigabit Ethernet habe ich schon vielfach berichtet, aber natürlich gibt es hier im Standard trotz der vielen PHY-Varianten eine schmerzliche Lücke. Wenn man einmal genau hinsieht, gibt es zwar Schnittstellen für die Überwindung hunderter Kilometer, aber nur vergleichsweise wenig, was man im Datencenter wirklich brauchen kann. Und wenn wir über 40 Gigabit Ethernet sprechen, sprechen wir auch über 40 Gigabit Fiber Channel, weil dieser Standard zwar ein anderes Paketformat benutzt, sich ansonsten heute aber bei den physikalischen Schnittstellen an den 10 GbE-Definitionen orientiert, wenn auch teilweise mit kleinem Formfaktor. Es gibt keinen Grund, warum die FC-Arbeitsgruppen von dieser bislang sehr erfolgreichen Strategie abweichen sollten. Schließlich diskutieren wir ja auch noch über FCoE, dann ist es von der Technik her ohnehin identisch.

Wo ist denn nun im 40/100 Gigabit-Standard die Lösung, mit der man wirklich preiswert unter Nutzung bestehender Verkabelung Server untereinander zusammenschalten kann oder Server mit Speichern verbindet? Die vierkanalige Variante 40 GBASE-LX-4 für die Nutzung von 10 km Singlemodefaser ist für das RZ nicht wirklich befriedigend und die eigentlich immer „vergessene“ vierkanalige Twinaxversion 40 GBASE-CX-4 mit ihren 10 Metern Reichweite erst recht nicht. Die Multimodevariante 40 GBASE-SR hat nach Standard noch keine elektronische Dispersionskompensation. Hersteller wie AMCC können das aber schon heute realisieren. Also wird es früher oder später noch eine Variante 40 GBASE-LRM geben, in Analogie zu 10 GBASE-LRM. Das wäre die einzig geeignete RZ-Variante. Wenn man eine millionenschwere SAN-Investition tätigt, macht die Anschaffung einiger Meter neuer Glasfasern auch schon nichts mehr. Aber was ist mit den vielen anderen Fällen, wo man z. B. einen einzelnen File-Server, der 85 m weg steht, ordentlich einbinden möchte? Wo man SAP-Applikationsserver miteinander verbinden möchte? Wo man eines dieser wunderschönen


Abbildung 3: GG45-Stecker

Foto: GG45-Alliance

neuen Tapedecks einbinden möchte? Was passiert, wenn man plötzlich“ merkt, dass die Virtualisierung dazu führt, dass die 10 GbE-Lösung nicht mehr ausreicht? Es ist ja nett von den Komponentenherstellern, schon jetzt preiswerte Transceiver und Serverboards in Aussicht zu stellen, wirklich hilfreich ist es aber nur für den Besitzer einer strukturierten Glasfaserverkabelung mit den „richtigen“ Fasern. Also, Anwendungsbereiche hin und her, ohne sinnfällige Kupfervariante ist der Standard für 40 Gigabit Ethernet ziemlich unvollständig und nützt z. Zt. hauptsächlich Metronetz-Providern. Weil ich ja immer etwas böse bin, möchte ich sogar hinzufügen, dass der Standard in seiner jetzigen Form der Schaffung einer glatten, hochperformanten Netzwerk-Infrastruktur eher schadet als nützt, weil wegen des Fehlens einer brauchbaren Kupferversion (und diese ist auch durch eine Low Cost Fiberversion nicht zu ersetzen) im Markt momentan noch eine Zurückhaltung zu verspüren ist, die in letzter Konsequenz zu recht ungesundem und teuren Fummeln mit anderen Lösungen führt.

Blickt man etwas nach vorne, wird wie bei 10 Gigabit Ethernet auch, die überwiegende Mehrheit der installierten Basis von 40 Gigabit Ethernet in den Datencentern zu finden sein. Hier möchte man die installierte Basis an Rechnern einfach unter Nutzung der installierten Basis an strukturierter Verkabelung besser und performanter unterstützen. Dies umfasst nicht nur die Server-zu-Server oder Server-zu-Speicher-Kopplung, sondern auch den Übergang zu Switches und DWDM-Systemen für die Realisierung von Fernverbindungen. Seit mindestens zwei Jahren sprechen wir vom Wachstum der 10 Gigabit-Schnittstellen für Server. Hier ist es einfach die normative Kraft des Faktischen, die zu einer autosensenden 1000/10000 Chipsatz-Generation führt und alleine aus Erwägungen der Stückzahl werden sich die Chiphersteller darauf kaprizieren, unabhängig davon, ob ein Anwender diese Datenrate wirklich benötigt. Es geht einfach nur um den Preis und die Stückzahl. Angesichts dieser Entwicklung bleibt momentan nur übrig, im Etagen- und Steigbereich mit allerbrutalstem Oversubscribing zu arbeiten. Wie bei Shared Medium System selig hofft man inständig, dass alle Benutzer schlafen mögen und ja nicht auf die Idee kommen, die mögliche Leistung zum Endgerät zu nutzen. Widersinnigerweise verlegt man zwar Kat. 7 Kabel, damit das Gigabit auch ja heil bis zum nächsten Verteiler kommt, verbindet die Etagen untereinander aber auch nur mit einem Gigabit, weil es nichts anderes gibt, was man bezahlen könnte.

Ein weiterer Standard, der allen Unkenrufen zum Trotz dabei ist, sich langsam aber sicher immer weiter zu verbreiten, ist iSCSI, die Abbildung von Speicherblocktransfers auf IP-Päckchen und - Netze. Sieht man sich die Leistungsgrenzen heutiger Geräte an und entwickelt sie, wie das so üblich ist, gemäß Moore´s Law weiter, werden wir binnen 4 - 5 Jahren eine Leistungsverzehnfachung haben. Plötzlich packen wir etwas aufs Netz, was dort vorher nicht war: den Fileserver-zu-Fileserver, Filerserver-zu-Application Server und Fileserver-zu- Backupmedium-Verkehr. Da gehen schon einmal einige Gigabit durch den Schornstein. Dann packen wir noch ein paar Wireless-VLANs drauf, hier darf man pro Zelle, also pro 11n-Access Point, demnächst auch mit 500 Mbit/s. rechnen und bei hochperformanten Zellen dürfen diese nicht zu groß werden, also ergeben sich summa summarum hunderte Zellen mit je ca. 4 - 8 Benutzern, und schon wieder haben wir eine Backboneleistung von 10 Gigabit verwurschtelt. Verzeihen Sie mir die flapsige Ausdrucksweise, aber vom vornehmen Ausdruck wird es auch nicht weniger.

Das sind die Dinge, die Sie kennen. Aber das ist noch nicht alles. Ich rechne in absehbarer Zeit vor allem im Zuge der Virtualisierung noch mit folgenden Tendenzen: Hardware-unterstütztes CPU Load Balancing wird sich nicht mehr auf Prozessoren beschränken, die zufällig in einem Gehäuse wohnen, sondern auch via Highspeednetz zumindest in benachbarte Rechner übergreifen. Hier benötigen wir Reaktionszeiten im Submikrosekundenbereich und jede Menge rohe Performance. Es wird so genannte TCP/IP Offloader geben, die nichts weiter tun, als alle Aufgaben, die im TCP/IP-Umfeld anfallen, zu übernehmen. Da wir alles mit TCP/IP machen, wird das viel Arbeit. Die Netzprozessoren können komplett TCP/IP auf einem Chip abarbeiten und damit ist es nicht mehr hinzunehmen, wenn z. B. ein Server allzulange über TCP/IP-Fragen überlegt. Wir bekommen einen Vorgeschmack darauf bei den iSCSI-Hardwarebeschleunigern. Insgesamt wird sich die Verarbeitungsgeschwindigkeit für Protokolle durch die Hardwareprozessoren und die Offloader dramatisch erhöhen, so dass sich ein Netz nicht mehr darauf verlassen kann, dass die kommunizierenden Recherchen schon so langweilig an den Protokollen herumrechnen, dass sie nur relativ langsam und mit langen Pausen Daten ausspucken können. Schließlich gibt es noch so nette Neuigkeiten wie RDMA, das Remote Direct Memory Access Protokoll, was, wie der Name schon sagt, DMA auf einem fremden Rechner unterstützt.

Ziele für eine Standardisierung von 40 GBASE-T werden sein:

- Überwindung von 100 m Distanz auf Cat 7/7A oder besseren Twisted Pairs
- Bewahrung existierender Investitionen in Verkabelung in Datencentern und strukturierten Verkabelungsbereichen
- Unterstützung von 10 GBASE-T und 40 GBASE-T mit einer einzigen PHY mit

Autonegatiation im Rahmen des so genannten „skalierbaren Ethernet“

- Unterstützung der 40 Gigabit XLAUI-Schnittstelle
- Multiple PHYs für höhere Geschwindigkeiten mit Trunking

Dazu gesellen sich die üblichen Ziele einer Ethernet-Standardisierung, wie

- Erhaltung des 802.3/Ethernet Frame Formats an der MAC-Schnittstelle
- Erhaltung der funktionalen Anforderungen von 802 mit Ausnahme der Hamming Distanz
- Erhaltung der minimalen und maximalen Frame Größen
- Alleinige Unterstützung des Vollduplex-Betriebes
- Unterstützung der sternförmigen Netzwerktopologie mit Punkt-zu-Punkt Verbindungen im Rahmen der strukturierten Verkabelung
- Spezifikation eines optionalen Media Independent Interfaces MII
- Unterstützung der P802.3ad Link Aggregation
- 40.000 Mbps an der MAC/PLS Dienstschnittstelle

**40 Gigabit auf Twisted Pair und die Gesetze von Shannon**

In Abbildung 4 sehen wir die angestrebte Konfiguration: von 40 Gigabit zu 40 Gigabit Transceiver über 90 + 5 + 5 = 100 m STP-Kabel, acht Adern in vier Paaren wie bei 10 GBASE-T, eigentlich „nur“ ein Upgrade von letzerem.

Um dies zu erreichen, muss man ein wenig nachdenken. Grundsätzlich gelten die Gesetze von Shannon, nach denen man höchstens zwei Informationsschritte pro Sekunde in ein Hertz zur Verfügung stehender Bandbreite packen kann. Kam man bei 10 Megabit Ethernet noch locker aus, hat man sich schon bei 100 Megabit Gedanken darüber gemacht und eine dreiwertige Codierung verwendet, die auf einem Kabel zu einer benötigten Bandbreite von 33 MHz geführt hat. Bei Gigabit Ethernet über Twisted Pair verwendet man eine fünfwertige Codierung, bei der mittels der Trellis Codierung acht Informationsbits plus ein Kontrollbit in vier fünfwertige Signale konvertiert werden. Bei linearer binärer Leitungscodierung würde man schon für Gigabit Ethernet 500 MHz Bandbreite benötigen, verteilt dies aber zunächst auf vier nachrichtentechnisch unabhängige Kanäle, so dass man auf jedem dieser Kanäle nur noch eine Bandbreite von 125 MHz und durch die mehrwertige Übertragung schließlich nur noch 67,5 MHz pro Richtung benötigt. Durch den Vollduplexbetrieb werden daraus am Ende wieder 125 MHz pro Drähtchenpaar. Dieses Konzept hat allerdings auch seine Grenzen. Wollten wir die gleiche Vorgehensweise wie bei Gigabit Ethernet vollziehen, kämen eben 320 Bits statt 8 in den Codierer. Vier Gruppen à 80 Bits bringen es auf ca. 4 Millionen unterschiedlicher Zustände pro Gruppe. Eine wesentlich höherwertigere Logik hilft uns da auch nicht mehr weiter.

Die Limits von Shannon sind keineswegs von der Modulationstechnik abhängig. Es ist umgekehrt so, dass sie ein Maß für die Güte einer Modulationstechnik darstellen, weil eine Technik umso besser ist, desto näher sie dem theoretisch überhaupt möglichen Limit kommt.

Sehen wir uns 1000 BASE-T aber einmal genauer an, stellen wir fest, dass es eine Reihe von Annahmen gibt, die damals bei der Definition gemacht worden sind und die bis zum heutigen Tage völlig unwidersprochen im Raum stehen. Da geht es z.B. um die Dämpfung. Man nimmt an, welche Bandbreite für die Übertragung zur Verfügung steht. Und diese Annahme wird z.B. in einem Verkabelungsstandard festgelegt. Viele Token Ring Besitzer haben damals auch nur angenommen, dass das Kabel lediglich 16 Mbit/s. schafft, bis sie eines Besseren belehrt wurden. Weiterhin nimmt man an, dass es irreduzible Rauschquellen gibt, wie z.B. das Hintergrundrauschen, das Nebensprechen aus den anderen Kabelpaaren, fremdes Nebensprechen („Alien Noise“) und Rauschen vom Transceiver. Alle diese Annahmen sind ja nett und gut, aber im Grunde genommen beruhen sie auf Phantasie mit Schneegestöber. Damit kommt man meistens unbeobachtet „durch“, weil sich die Meisten gar nicht dafür interessieren, wie es wirklich ist, sondern vielmehr lediglich an einer Anweisung interessiert sind, wieweit sie das Kabel abrollen dürfen, damit es noch funktioniert. Diese Situation ist nicht neu und existiert auch bei Funksystemen und Optischen Netzen. Der Markt schreit geradezu nach einem Kästchensystem, nicht mitdenken, sondern abhaken heißt die Devise.

Und wenn man 40 Gigabit/s. auf acht Drähtchen Twisted Pair übertragen möchte, muss man im Wesentlichen zunächst umdenken und die Fakten prüfen.

Abbildung 5 fasst die Störeinflüsse noch einmal zusammen: Nahnebensprechen NEXT von den benachbarten Kabelpaaren, Fernnebensprechen FEXT vom Transceiver und den benachbarten Kabelpaaren, allgemeine Dämpfung und „Alien Crosstalk“, also elektromagnetische Interferenz.

Ein kategorisiertes Kabel muss von hoher Qualität mit geringen durch das Material bedingten Abweichungen sein, um die Anforderungen nach TIA-568 zu erfüllen. Der

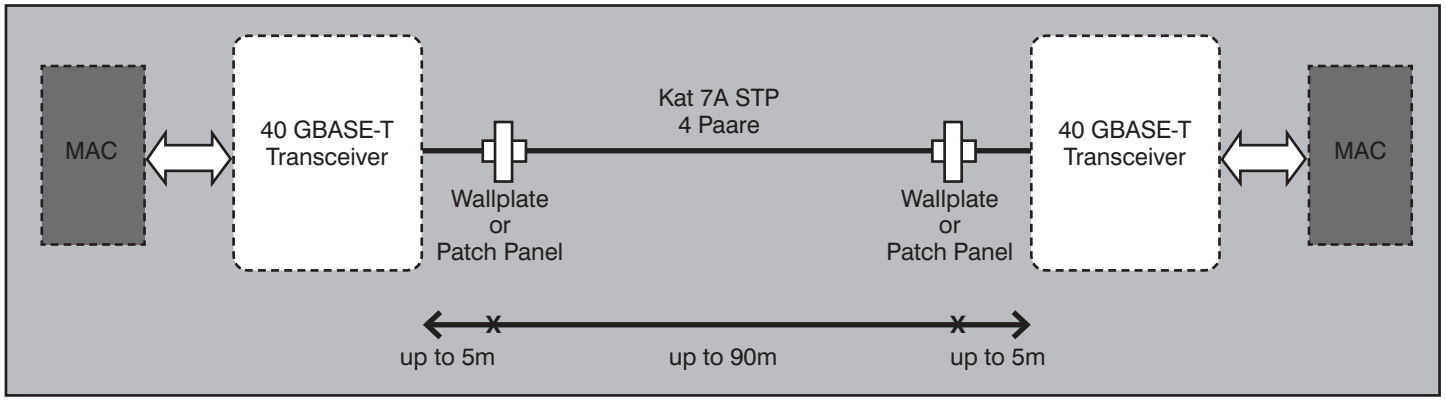



Abbildung 4: Konfiguration

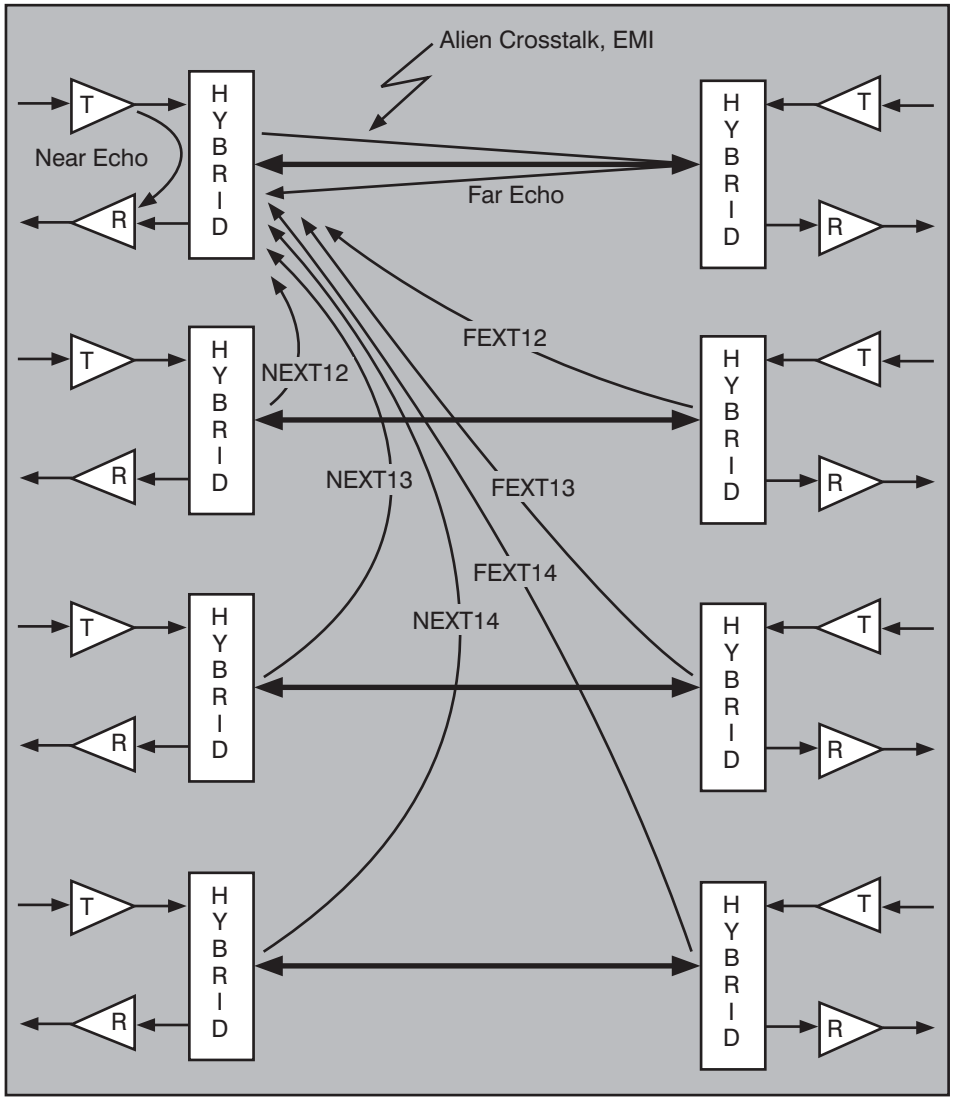



Abbildung 5: Störeinflüsse, gesamt

Standard gibt Bandbreiten vor, in denen bestimmte Eigenschaften erfüllt sein müssen. Dies ist aber nur eine Anforderung auf dem Papier, denn die modernen Kabel erreichen durchaus die gleichen Leistungen bei höheren Bandbreiten. Das hängt hauptsächlich von der Übertragungsgeometrie und den Materialeigenschaften ab. Geringfügige strukturelle Abweichungen und Unregelmäßigkeiten in den Steckern können diese Werte zwar verschlechtern, aber bei modernen Systemen nicht wirklich wesentlich. Wenn ein Anbieter Ihnen heute den sicheren Betrieb des Kabels bis sagen wir z.B. 600 MHz garantiert, ist das ein Wert, der unter den ungünstigsten Voraussetzungen erzielt wird. Damit das klappt, müssen alle Komponenten viel viel besser sein und erreichen unter normalen Bedingungen sicher 1,5 .... 2 GHz Bandbreite.

Das ist der Grund dafür, warum wir manchmal so schwimmende Grenzen bekommen, bei denen eigentlich laut Standard eine Verbindung nicht mehr funktionieren kann, es in der Praxis mit einem System eines Herstellers aber doch tut.

So kann man z.B. ausrechnen, dass die Kat 7 nach ISO für den Betrieb von 40 GbE grade nicht mehr ausreicht. Es gibt aber durchaus Kat 7-Systeme von Herstellern, die die Übertragungsrate dennoch realisieren könnten. Wir zeigen in der nächsten Abbildung einmal eine solche Darstellung, wieder bezogen auf den Hersteller Nexans. (siehe Abbildung 6)

Die Entwicklung von 40 GBASE-T kann natürlich von den Ergebnissen der 10 GBASE-T-Standardisierung, die teilweise unter großer Mühe zustande kamen, massiv profitieren. Man weiß z.B., dass die Nahnebensprechdämpfung jenseits der 200 MHz schlimmstenfalls um ca. 8 dB wächst und nicht irgendwie ins Unermessliche steigt. Das wäre auch nicht anders zu erwarten gewesen, denn die Nahnebensprechung entsteht durch einen induktiven Effekt, der auf dem betroffenen Adernpaar durch Einstreuung eines elektromagnetischen Feldes, welches von einem anderen Adernpaar erzeugt wird, entsteht. Die Leistung des elektromagnetischen Feldes nimmt aber mit der Frequenz bei gleichbleibender Distanz ab. Das kompensiert die an und für sich mit höheren Frequenzen wachsende „Empfindlichkeit“ des anderen Adernpaars für diese Art von Störung deutlich. Diese vergleichsweise lächerlichen 8 dB ließen sich übrigens vollständig wegkompensieren, wenn man die Eingangsleistung, die man an das „störende“ Kabel gibt, um etwa 1-2 dB herabsetzt.

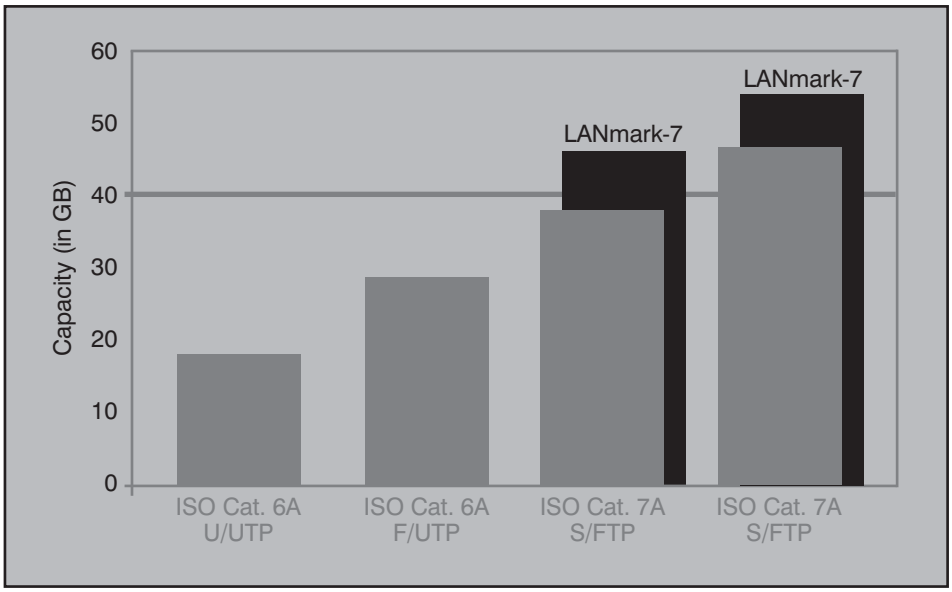



Abbildung 6: „Shannon-Kapazität“ für 4-paarige Kabel Quelle: Nexans

Die Fernnebensprechdämpfung ist nämlich z.B. bei 1000 MHz wesentlich geringer als bei 200 oder 500 MHz. Dies hängt wie bei der Nahnebensprechdämpfung schon erläutert mit dem Intensitätsverlust des „störenden“ Signals bei höheren Frequenzen zusammen. Eine Extrapolation der Standard-Werte erübrigt sich deshalb. Der FEXT-Wert von 50 dB des LANmark 7A-Kabels ist daher weniger ein Verdienst des Herstellers, sondern der Physik als solcher.

Diese Effekte heben sich in gewisser Weise gegenseitig auf. Die Dämpfung durch die Leistungssumme aller Nebensprechdämpfungen werden durch den Begriff „NEXT Power Sum“ zusammengefasst. Zwischen 200 und 400 MHz ergibt sich eine erstaunliche Stagnation und erst in Richtung 500 MHz haben wir einen, wenn auch nicht wirklich nennenswerten Anstieg zu verzeichnen. Dieses „Sammelmaß“ ist aber letztlich wirklich leistungsbestimmend, denn die genannten Effekte treten in der Realität niemals isoliert, sondern immer zusammen auf.

Eine weitere wichtige Frage ist, ob nicht durch den Betrieb mit höheren Frequenzen durch das Kabel andere Funkdienste gestört werden. Ich sehe ja schon wieder die besorgten Gesichter, die fürchten, dass der Betrieb von 40 Gigabit Ethernet auf Twisted Pair die heiligen Funkzellen stören könnte. Dem ist definitiv nicht so, weil für 40 GBASE-T nur ein vollständig abgeschirmtes Kabel in Frage kommt. Eine Störung könnte übrigens nur dann entstehen, wenn eine Harmonische der Betriebsfrequenz auf dem Kabel ausgerechnet eine Frequenz in einem WLAN-Bereich hätte und darüberhinaus über die hinreichende Intensität verfügen würde. Damit die Leser diesen Artikel noch zu Ende lesen, will ich das jetzt nicht vorrechnen, aber wie schon gesagt, nimmt die Intensität stark mit der Frequenz ab und das Risiko einer „Bedrohung“ durch eine Harmonische von 500, 1000 oder 1200 MHz ist geringer oder höchstens genau so groß wie das Risiko einer Bedrohung durch eine Harmonische von 66, 125 oder 250 MHz. Aber, wie gesagt, wegen der Schirmung findet eine derartige Beeinflussung ja überhaupt nicht statt.

Umgekehrt kann man aber auch sehen, was passiert, wenn die Schirmung nicht vorgenommen wird, versagt oder defekt ist: das 10 oder 40 GbE-Nutzsignal würde in den allgemeinen Funkstörungen gnadenlos untergehen! Backgroundstörungen (Grundrauschen) sind nämlich praktisch frequenzunabhängig.

Es gibt aber noch weitere interessante Zusammenhänge. Wie schon weiter oben erwähnt, wurden in der Vergangenheit Verbesserungen hinsichtlich der Bandbreiteausnutzung vor allem dadurch erzielt, dass man statt eines binären Leitungscodes ternäre oder quinäre Signale erzeugt und über das Kabel schickt. So kann man in einem Übertragungsschritt, der ja üblicherweise auch mit dem Maß Baud angegeben wird, mehr Bits pro Sekunde unterbringen. Nun hat alles seinen Preis. Die logischen Niveaus liegen bei mehrwertiger Übertragung enger zusammen und sind deshalb anfälliger gegen Störungen bzw. man muss am Empfänger mehr Aufwand betreiben, um sie ordentlich auseinanderzuhalten und richtig zu decodieren. Letztlich ist auch hier das Signal/Rauschverhältnis maßgebend. Nach einigem Rechnen kommt man zu dem Ergebnis, dass man für zwei logische Niveaus mehr 6 dB mehr Störspannungsabstand benötigt. Das ist ein relativ abstraktes Ergebnis und viele können damit nichts anfangen. In Abbildung 7 sehen wir aber einmal eine etwas andere Darstellung. Betrachtet wird eine Übertragungsstrecke mit Kat 5/5e Kabel, die mit den weiter oben angegebenen Parametern hinsichtlich besserer Dämpfung der bestimmbaren Parameter wie NEXT und FEXT ausgestattet wurde. Die Graphik zeigt an, wie viele Bits pro Sekunde pro Schritt unter den angegebenen Umständen bei einer vorgegebenen maximalen Übertragungsfrequenz untergebracht werden können. Mit Entsetzen sehen wir: es werden immer weniger, desto höher die Frequenz ist. Das raubt uns massiv die Hoffnung, mit einer weiteren wesentlichen Steigerung der logischen Stufen etwas ausrichten zu können.

An und für sich ist dieses Ergebnis nicht unerwartet, weil die Störungen mit der Frequenz insgesamt zunehmen und wir durch die verbesserte Kompensation lediglich das Signal/Rauschverhältnis soweit verbessert haben, dass die gewünschte Distanz so eben grade noch überwunden werden kann. Bei den gemessenen Ergebnissen ist es sogar so, dass wir jenseits der 400 MHz sogar wieder linear binär leitungscodieren müssen.

Die neuen 6/6A/7/7A-Kabel schieben diese Grenze immer weiter nach oben. So können wir bei einem 7/7A-Kabel einen Frequenzbereich von 1000 MHz bzw. 1200 MHz mit verdichteter Leitungscodierung nutzen.

Fasst man diese Voruntersuchung zusammen, ergibt sich Folgendes:

- Die Übertragung von 40 Gigabit/s. auf STP Kat 7 oder 7A ist möglich
- Man benötigt eine Übertragungsbandbreite von 1000 - 1200 MHz
- Die Nahnebensprechdämpfung muss für 40 GBASE-T gegenüber Kat. 6A (für 10 GbE) um ca. 20-30 dB reduziert werden
- Die Fernnebensprechdämpfung muss

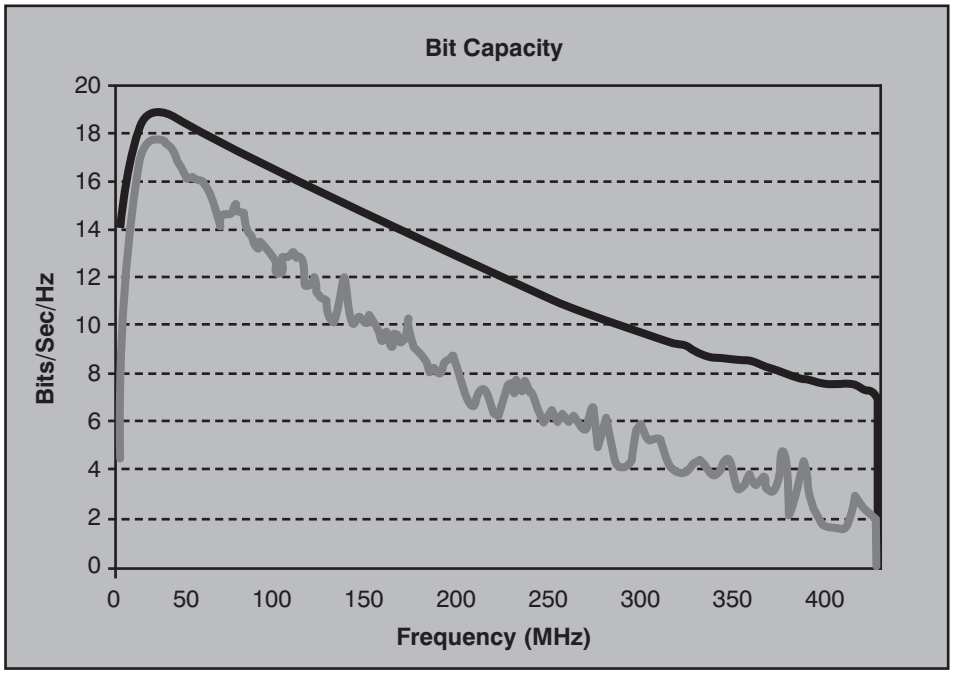



Abbildung 7: „Bitpackrate“ vs. Frequenz

für 40 GBASE-T gegenüber Kat 6A um 20 dB oder mehr reduziert werden

- Die Launch Power (Einspeiseleistung) sollte zwischen 10 und 12 dBm liegen

- Der Return Loss stellt keine erhöhten Anforderungen. Hie sind die schon mit 6A erreichten 8 dB ausreichend

Die Gesetze von Shannon setzen keine Grenzen, es wird lediglich etwas komplizierter.

**Zum Aufbau der Transceiverschaltkreise**

Um den Anforderungen für die Randbedingungen der Übertragung von 40 Gigabit auf STP entsprechen zu können, benötigt man ein Schaltkreisdesign, welches moderne Signalverarbeitungsalgorithmen hinreichend breitbandig mit Schaltkreisen geringer Leistungsaufnahme realisiert. Dafür benötigt man ein hochparalleles, für diese Zwecke optimiertes Design. Obwohl das im Einzelnen hochinteressant ist, werde ich für die Zwecke dieser Darstellungen nur eine oberflächliche Sicht geben können. Es sind z. Zt. kleinere Firmen, wie z. B. Solar Flare, die sich um das Design entsprechender Schaltkreise bemühen. Dabei müssen sie von sehr ungünstigen Voraussetzungen ausgehen, damit ein Schaltkreis in Serie auch nachher immer funktioniert. Andererseits, wenn man auf die Entwicklung der xDSL-Schaltungen zurückblickt, hat man damit Erfahrung. Auch hier wurden letztlich verschiedene Dinge einfach ausprobiert, um die eigentlich immer angenommenen Grenzen der Übertragungskapazität von Telefonkabeln in der Last Mile zu überwinden. Wie man sieht, mit Erfolg.

Die mögliche Entscheidung ist es, Pulsamplitudenmodulation PAM zu verwenden. Diese Modulationsform hat sich auch bei xDSL bewährt und schafft einen hinreichenden Grad an Designfreiheit, ohne von vorneherein Randbedingungen z. B. hinsichtlich der in einen Schritt zu codierenden Informationsmenge fest zu zementieren. Außerdem möchte man 40 Gigabit durch die systematische Weiterentwicklung von 10 GBASE-T erreichen. Das hat mehrere Gründe. 10 GBASE-T ist bewährt und ausgesprochen kostengünstig. Die Anwender besitzen normalerweise bereits eine Struktur, auf der 10 GBASE-T läuft, wenn sie über 40 GBASE-T nachdenken. In alter Tradition wird es nicht das Ziel sein, Chips zu entwickeln, die nur 10 GBASE-T können, sondern autosensende 1/10/40 GBASE-T-Lösungen, weil diese es auf viel höhere Stückzahlen bringen und den Anwendern die sanfte Migration erlauben. Die Anforderungen von 40 GBASE-T an die Übertragungseigenschaften der Verkabelung und ihrer Umgebung sind relativ hoch. Im Zuge der Entwicklung passender Chips könnte man diese Anforderungen etwas entzerren oder herunternehmen.

Im Folgenden wird eine mögliche Lösung für die Übertragung beschrieben. Es geht hier zunächst einmal darum, zu zeigen, dass die Übertragung überhaupt möglich ist. In einer Standardisierungsphase werden noch andere Übertragungsvarianten auftreten und diskutiert werden. Firmen wie Intel werden sich auch von kleineren Herstellern nicht die Butter vom Brot nehmen lassen. Bei 10 Gigabit über Fiber ist das ja so ausgegangen, dass Intel die kleine Firma mit der besten Technologie aufgekauft hat. Es wird auch dieses Mal eine Phase geben, in der sich kleinere Entwickler ein Rennen liefern, dessen Sieger gekauft werden möchte.

Betrachtet man die dargelegten Zusammenhänge, scheint eine Bandbreite von 1000 MHz auf dem Kabel relativ optimal zu sein. Jenseits der 1000 MHz schlagen bestimmte Effekte relativ bösartig zu und der Aufwand zur Kompensierung wäre hoch, wenn nicht gar unmöglich.

Ein konkreter Implementierungsvorschlag könnte eine Baudrate von 833 MHz vorsehen, also 833 Millionen Übertragungsschritte pro Sekunde. Dann benötigt man für die 40 Gigabit 48 Bits pro Baud, was sehr viel ist. Andererseits haben wir vier Kabelpaare, so dass sich dies auf 12 Bits pro Baud pro Kabelpaar reduziert.

Bei 10 GBASE-T wird eine PAM-16 Modulation benutzt. PAM-16 definiert sechzehn verschiedene Konstallationspunkte in der Kombination von Amplituden- und Phasenlage und kann somit pro Schritt vier Bits codieren. Das ist keine besonders anspruchsvolle Modulationstechnik, vergleichsweise verwendet man z. B. bei den IEEE 802.11a WLANs bis zu 64 Konstellationspunkte in der QAM-64. Ein Ziel bei der Standardisierung ist es aber auch, die Bitfehlerrate zu verbessern. Viele Ethernetstandards arbeiten noch auf den alten Vorgaben der Norm, die lediglich 10 EXP -8 verlangt. Dies ist aber nicht mehr zeitgemäß und der Standard für 10 Gigabit Ethernet auf Fiber definiert PHY-Varianten, die es mindestens auf 10 EXP -12 bringen. Dem möchte man sich auch hier anpassen. Mit einer PAM-16 würde man die allgemeinen Anforderungen von IEEE 802.3 erfüllen. Für eine ordentliche Kombination von Kontrollsignalen und Trellis Codierung braucht man aber eine PAM-16 mit zehn tatsächlich benutzten Konstellationspunkten pro Schritt. Die Trellis Codierung ist mathematisch sehr kompliziert, aber man hat ja bei 1000 BASE-T gesehen, wie gut sie funktioniert und dass es relativ einfach zu sein scheint, entsprechende Schaltungen zu bauen. Für 10 GBASE-T wurde die bisher dreidimensionale Trellis Codierung auf vier Dimensionen erweitert und diese vier Dimensionen werden jeweils auf ein Kabelpaar übertragen. Es ist nicht so ohne Weiteres möglich, die Trellis Dimensionen einleuchtend

zu erklären. Aber ich will es einmal versuchen. Bei einer zweidimensionalen Trellis Codierung entsteht eine Fläche, die man sich meinethalben wie ein Fliegengitter vorstellen kann. Jedes Kästchen des Fliegengitters kann wie bei einer hundsgewöhnlichen Matrix durch zwei Koordinaten adressiert werden. Je nach gewünschter Codierungsdichte nimmt man mehr oder weniger Fliegengitterkästchen, die dann natürlich auch jeweils ein Stück auseinanderliegen. Um jedes Fliegengitterkästchen herum entsteht dadurch ein Feld und wenn z. B. bei der Übertragung eine Koordinate verfälscht wurde, dann lässt sich das ursprünglich „gemeinte“ Signal wiedererkennen. Das ist eine systematische Anwendung der Hamming-Distanz aus der einfachen linearen Codierung. Nun wählt man geschickterweise die Felder nicht so, dass benachbarte Nachrichtenelemente auf benachbarte Codesymbode fallen, sondern man legt sie so weit auseinander wie möglich. Dadurch kann man eine viel größere Sicherheit gegenüber Fehlern erzielen. Bei einer dreidimensionalen Trellis Codierung wendet man die eben beschriebene Vorgehensweise auf einen Körper an, von mir aus einen Würfel, in dem man die Codesymbole ebenso geschickt unterbringt. Und für die vierdimensionale Trellis Codierung nimmt man eben einen vierdimensionalen Raum, den man mathematisch gut beschreiben kann. Die Idee, eine vierdimensionale Trellis Codierung zu verwenden und dann die vier Dimensionen auf die Kabelpaare abzubilden, ist fast schon als genial zu bezeichnen, weil dadurch ein Modulations-Prozessgewinn entsteht, der sich mittelbar so niederschlägt, dass wir relativ zu uncodierter PAM-16 6 dB gewinnen. 6 dB ist in diesem Zusammenhang sehr viel. Durch die vierdimensionale Trellis Codierung gewinnen wir also diese 6 dB und erhöhen gleichzeitig die Fehlerrate auf z.B. 10 EXP -12. Um diese Fehlerrate zu erzielen, benötigen wir auf der Übertragungsstrecke für die Trellis-Codierung übrigens ein Signal/Rauschverhältnis von ca. 26 dB.

Wie kommen wir jetzt nur bei 40 GBASE-T weiter? Mit der bislang skizzierten Idee müssten mindestens 12 Bits auf ein Baud abgebildet werden. Mit einer normalen PAM- oder QAM schaffen wir aber höchstens 8 Bits auf ein Baud bei QAM-256.

Die QAM-256 ist aber sehr störanfällig und letztlich ungeeignet. Stattdessen muss ein weiterer Zwischenschritt bei der Codierung eingeführt werden. Die Information der 12 Bits pro Schritt muss auf eine höherwertige Codierung abgebildet werden, z.B. auf eine ternäre Codierung. 12 Bits ergeben 4096 verschiedene mögliche Zustände. 8 Ternärsymbole ergeben 6561 verschiedene mögliche Zustände, so dass wir auch noch Reserve hätten. Eine einfache Leitungscodierung für Ternärsymbole würde Phase und Amplitude kombinieren, also könnten wir hier direkt PAM-64 nehmen. PAM-64 auf der Leitung ist allerdings auch nicht wirklich optimal, da die einzelnen Signalniveaus doch sehr eng beieinander liegen.

Besser ist allerdings die Verwendung von OFDM, wie wir es aus den WLANs kennen. Das Signal ist außerordentlich stabil. Wir können die PAM-64 Konstellationspunkte direkt für die Modulation der Unterträger verwenden. Die anschließende Signalsynthetisierung auf der Basis der iFFT führt bekanntlich zu einem sehr störungsunanfälligen Signal. OFDM ist keineswegs auf die Verwendung bei Funknetzen beschränkt. In DWDM-Systemen ist 40 Gb/sec. pro DWDM-Kanal die aktuelle Basisrate. Für den Übergang zu einer Basisrate von 100 Mb (sec. pro DWDM-Kanal diskutiert man schon seit längerem die Verwendung von OFDM.

Ein 40 GBASE-T-Transceiver entsteht durch Fortsetzung der älteren Wege, die auch bei 10 GBASE-T erfolgreich waren:

- Verschiebung der analogen Signalverarbeitung
- Verbesserung der Codierung
  - traditionell
    - Gallagher LDPC
    - Co-Set-Partitionierung
    - Tomlinson-Harashima
    - 16 oder 64 PAM
  - revolutionär
    - QAM statt PAM
    - OFDM
- Oversampling

Es gibt nämlich eine Reihe weiterer Möglichkeiten zur Verbesserung der Codierung auch ohne OFDM. Gallagher´s Low Density Parity Check LDPC Block Code z. B. erzielt erhebliche Senkung der BER als Funktion der SNR als konkatenierter Konvolutionscode (Turbo Code). 12 dB Co-Set-Partitionierung sorgt für verbesserte Toleranz gegenüber Rauschen. In Gigabit Ethernet wird 6 dB Co-Set-Partitionierung vorgenommen. 1000 BASE-T 4DPAM-5 überträgt 5 Niveaus und ist so unempfindlich wie 3 Niveaus. 12 dB CSP 4 DPAM-8 überträgt 8 Niveaus und ist so unempfindlich wie 2 Niveaus. Tomlinson-Harashima Vorcodierung schließlich sorgt für die Reduktion der Komplexität des Empfängers. Sie erlaubt spektrale Signalaufarbeitung im Transmitter zur Reduktion der Einflüsse der Einkopplung von Alien Crosstalk und eliminiert die Weiterpropagation von Fehlern im Decision Feedback Equalizer (DFE), auch bei großen DFE-Koeffizienten.

Ein weiterer Bereich zur Problemlösung ist generell das Oversampling. Es gibt drei Alternativen für Transmit Front-End: Simple, Baseline, Oversampled. Bei „Simple“: gibt es keine digitale Filterung, 3200 Msymbole/sek., einfache R/C-Signalglättung, das Sendesignal hängt von ungenauen Analog-Komponenten ab und es gibt keine spektralen Nullstellen bei DC und 1/2T, was eine schlechte Rückflussdämpfung bedeutet. „Baseline“: wie „Simple“, aber mit RLC Frontline-Filter mit konstanter Ausgangsimpedanz, zwar immer noch keine ordentlichen spektralen Nullstellen, aber wesentlich bessere Rückflussdämpfung. „Oversampled“: digitale Filterung und Interpolation, 6400 Msymbole/sek., einfache RC Signalglättung mit Basisfrequenz 1 GHz, wohldefinierte Nullstellen bei DC und 1/2 T, sehr gute Rückflussdämpfung. Möglich ist hier auch das Training von PMA-Sequenzen in Analogie zu Training von OFDM-Symbolen bei schnellem Wireless.

All diese Dinge können kombiniert werden, um das 40 GbE100m-Distanzziel auch für Kat. 7/7A-Verkabelung zu erreichen. Die Aufgabe der Standardisierung besteht lediglich daraus, die hinsichtlich der Wirtschaftlichkeit, des Stromverbrauchs und der Stabilität günstigste Lösung herauszuarbeiten.

Nach diesen Vorüberlegungen kann man die Anforderungen an die Übertragungsstrecke neu formulieren: für ein aggregates Signal/Rauschverhältnis von z. B. 25 - 26 dB über die Strecke müssen die einzelnen fünf SNR Hauptfaktoren um 32 dB liegen. Diese Hauptfaktoren sind:

- Ungleichheiten auf den Kanälen
- Intersymbol-Interferenz ISI
- Echo
- Nahnebensprechdämpfung NEXT
- Fernnebensprechdämpfung FEXT

Die ersten zwei Punkte bekommt man nur durch eine Kombination von Feedforward- und Feedback-Equalizing in den Griff. Man schickt z. B. eine definierte Symbolfolge aus und betrachtet das Ergebnis. Physikalisch gesehen hat jedes der in einer Verkabelung existierenden Kabelpärchen eine andere Bandbreite und eine ggf. minimal abweichende Signalverzögerung. Die Bandbreite drückt auf die Intersymbol-Interferenz und die Signalverzögerung verzerrt das durch die Trellis-Codierung in den vier Dimensionen zusammenhängende 4 X PAM-64 oder OFDM Nutzsignal. Es

muss also eine Einsynchronisierung erfolgen. Diese Problematik ist bekannt, seit es Ethernet gibt. Schon bei der Basisversion 10 BASE 5 mussten sich die Empfänger auf das ankommende Signal einsysnchronisieren. Das ist der Grund für die Existenz der Präambel im Ethernet Paket. Da auch bei 10 GBASE-T immer noch klassische Ethernet-Pakete versendet werden, steht z. B. der Raum in den Präambeln für derartige Zwecke zur Verfügung. Selbst bei maximal langen Paketen von ca. 1500 Byte sind das 8 Byte Präambel und somit 0,5 % der Gesamtbandbreite. Das reicht in jedem Fall.

Wegen der limitierten Bandbreite muss man vollduplex arbeiten. Die Echokompensation lässt sich also in einem Zug mit der Richtungstrennung durchführen. Allerdings muss ein größerer Aufwand getrieben werden, denn wegen möglicher Fehlanpassungen bei der Impedanz muss man schon auf eine Unterdrückung im Bereich von 40 - 50 dB abzielen.

Die Nahnebensprechdämpfung ist eine hochgradige Störung zwischen benachbarten Receivern. Auch wenn man sich mit der Trellis Codierung noch so große Mühe gibt, entsteht ein sehr großer Aufwand für die Entzerrung. Auch hier sollte man sicherheitshalber auf 40 dB Entzerrungsleistung abzielen.

Die Fernnebensprechung wird bei 1000 BASE-T mittels eines Ausgleichsparameters beschrieben (ELFEXT), der aber durch die Schaltungen selbst nicht weiter kompensiert wird. Das kann man sich ab 10 GBASE-T und besonders bei 40 GBASE-T nicht erlauben und muss wenigstens eine FEXT-Unterdrückung im Bereich von 20 dB erzielen.

Wie schon gesagt, um diese Anforderungen, die zu einem SNR von ca. 26 dB führen, erfüllen zu können, benötigt man ein komplexes Schaltungsdesign unter massiver Nutzung paralleler Strukturen. Man darf nicht vergessen, dass ein Teil der Arbeit ja auch in analoger Signalverarbeitung besteht, die sich im Gegensatz zur rein digitalen Verarbeitung nicht völlig beliebig zusammenintegrieren lässt.

Um die geforderte Leistung zu erreichen, muss man einen MIMO (Multiple Input Multiple Output) Schaltkreis bauen, der alle auftretenden Signalströme als Matrixfilter gleichartig behandelt. Dieser Matrixfilter hat eine Reihe von Vorzügen. So ist z.B. die Nebensprechunterdrückung ein immer gleichartig auftretender Vorgang. Ein Kabelpaar wird die anderen Kabelpaare im Wesentlichen gleichartig stören, weil die Störung ja mit dem gleichen Ausgangssignal entsteht. Die Nebensprechunterdrückung für NEXT 1, 2, NEXT 1, 3 und NEXT 1,4, also die drei Einflüsse, die von Kabelpaar 1 auf die Kabelpaare 2, 3, und 4 ausgeübt werden, sind sehr ähnlich, werden aber z. B. im Rahmen des 1000 BASE-T-Designs an drei verschiedenen Stellen lokal zu den jeweils gestörten Kabelpaaren ausgeführt. Diese Operation kann man z. B. geeignet zusammenfassen. Durch entsprechende Korrelationsfunktionen kann die Interferenz zwischen den Kanälen weiter gesenkt werden. Bei 1000 BASE-T tut man noch immer so, als sei jedes Signal in jedem Moment überraschend und völlig neuartig. Das stimmt natürlich überhaupt nicht, denn man kennt das Signal sehr gut, weil man es doch im Schaltkreis selbst erzeugt. Ein entsprechend ausgestatteter Schaltkreis könnte z.B. Signale erzeugen, die von vorne herein so beschaffen sind, dass sie in einer bestimmten Umgebung weniger Störungen erzeugen als ein unbearbeitetes Signal.

Diese Korellationsfunktionen kann man aber nur dann ausführen, wenn man das gesamte Signal in einem Schaltkreis vorliegen hat und nicht wie bislang auf vier getrennte, miteinander nicht in Verbindung stehende Schaltkreise aufteilt.

Es sollte klar sein, dass es nicht reicht, diese Korrelationen nur auf der Senderseite vorzunehmen.

Der Transmitter muss eine Linearität von mehr als 50 dB aufweisen, der hybrid aufgebaute Empfänger ebenfalls. Insgesamt benötigt man eine Operationstaktrate von ca. 833 MHz.

*Das bedeutet, dass man die Schaltung wie bisher in konventioneller CMOS-Technologie ausführen kann.*

Über die Schirmung muss man gesondert nachdenken. Wenn man ein System für UTP-Kabel entwickelt, kann man das nicht so ohne Weiteres auf geschirmte Umgebungen übertragen. Die Schirmung selbst führt zu einem weiteren Störeinfluss durch Reflexionen am Schirm. Man muss diese durch die Kompensation für das allgemeine Grundrauschen in den Filtern abdecken. Andererseits entspricht das reflektierte Signal ja dem Signal auf den Adernpaaren mit einem äußerst geringen Zeitversatz und sollte auch im Rahmen der Echo-Kompensation abgefiltert werden können.

Noch ein paar Worte zu den Kosten. Wie immer in der Geschichte der Ethernet-Standardisierung, möchte man die zehnfache Leistung zum ca. dreifachen Preis. Das hat sich am Markt bewährt und hat ja in der Vergangenheit auch immer funktioniert. Bei 40 und 100 GbE wird dieser Mechanismus jedoch außer Kraft gesetzt. Das Ziel ist die n-fache Leistung zum n-fachen Preis oder darunter. Heute kostet ein 10 GBASE-T-Board ca. 300 Euro. Das bedeutet, man würde 1200 Euro als angemessenen Preis für ein 40 GBASE-T-Board empfinden. Die ersten 40 GBASE-T-Boards werden erfahrungsgemäß aber das acht- bis neunfache ihrer 10-Gigabit-Brüder kosten und dann im Preis fallen.

Das bedeutet im Klartext, dass die ersten 10 GBASE-T Boards für ca. 1000 US$ herauskommen werden und dann auf unter 500 US$ fallen. Damit wären sie am Anfang nicht billiger als die entsprechenden Multimode-Boards, aber insgesamt muss man natürlich sehen, dass die Neuanlage einer Glasfaserverkabelung z.B. für die Anbindung von ein paar Servern insgesamt erheblich teurer werden kann als eine entsprechende Twisted Pair Verkabelung. Dies gilt natürlich besonders dann, wenn es schon eine strukturierte STP-Verkabelung gibt, die man nutzen könnte. Insgesamt ist zu erwarten, dass 40 GBASE-T am Server zu Beginn ca. 40% einer adäquaten Glasfaserlösung kosten wird, diese Kosten werden im Laufe der Zeit auf ca. 10% relativ gesehen sinken. Generell gilt dies natürlich nur für Verbindungen mit einer Länge von max. 100 m und im Vergleich zwischen Kupfer und Multimode.

Insgesamt werden die 40 GBASE-T-Lösungen vom allgemeinen Entwicklungsprozess bei den Integrierten Schaltungen profitieren, weil bekannte Standard-Prozesse benutzt werden können, mehrere Transceiver zusammen integriert werden können und ein beachtliches Marktpotenzial besteht.

Wie wir in den letzten zwei Jahren gesehen haben, ist die Entwicklung von 10 Gigabit Ethernet zwar zügig vorangegangen, es gab jedoch auch einige technologische Verwerfungen. Wie schon mehrfach berichtet, übertreffen bei 40 GBASE selbst die Vorserienprodukte im optischen Bereich die Vorgaben des Standards deutlich. Alleine die Androhung von 40 GBASE-T wird dazu führen, dass die Hersteller von optischen Komponenten noch mehr auf die Tube und auf die Preise drücken. Das war bei Gigabit Ethernet genauso. Auch wenn sich sämtlichen mir bekannten Fünfjahresplankoryphäen die Haare zu Berge stellen, empfehle ich, 40 Gigabit Ethernet relativ spontan zu implementieren, immer dann, wenn man es benötigt. Die Notwendigkeit für 40 Gigabit Ethernet ist in etwa so plötzlich und unerwartet wie Heiligabend. Aber Sie wissen genau: der Hartgesottene bekommt die günstigsten Preise. Wer schon im November Weihnachtsgeschenke einkauft, ist selbst schuld. Am 24. Morgens ist es meist billiger. Und die preiswertesten Geschenke bekommt man nach dem 26.12.. Obwohl es zunächst verwirrend aussieht, es gibt ja bezogen auf einen Anwendungsfall gar nicht so viele Alternativen für die 40 GbE-PHY. Wenn man die Komponenten aber übereilt kauft, greift man in jedem Fall in ein fallendes Messer. Weiter oben hatte ich Zielpreise angegeben. Der Markt wird sich erst einigermaßen stabilisieren, wenn wir bei diesen Preisen angekommen sind. Wer jetzt eine Serveranbindung mit 40 Gigabit benötigt, kann nicht auf 40 GBASE-T warten, sondern nimmt eben eine preiswerte Multimodelösung. Wer jetzt ein Citynetz aufbauen möchte, kann mit einer Kupferlösung ohnehin nichts anfangen. Aber wer die Infrastruktur für ein Rechenzentrum neu plant, braucht nicht davon auszugehen, dass alle Geräte mit Monomode untereinander verbunden werden.

### Konsequenzen für die Unternehmensnetze

Wie üblich wird IEEE 802 dafür sorgen, dass die konventionellen Glasfaservarianten einen Vorsprung bekommen, damit sie verkauft werden. Das kann ganz einfach über den Project Authorisation Request gesteuert werden. Der Standardisierungsprozess als solcher kann dann schnell gehen. Erste 40 GBASE-T-Boards werden wir also 2011/2012 sehen. Dies liegt eindeutig innerhalb der Lebensspanne heute neu geplanter Verkabelungslösungen. Also müssen diese dementsprechend ausgelegt werden.

Mit absoluter Sicherheit reicht eine durchgängige Kat 7A-Verkabelung für 40 GbE aus. Man kann noch über den Stecker diskutieren, aber es ist kein Grund zu sehen, warum nicht sowohl der GG45 als auch der Siemon-Stecker hinreichend funktionieren sollten.

Interessant ist natürlich die Frage, was mit einer Kat 7-Verkabelung ist, die ja schon vielfach installiert ist. Hier kommt es darauf an, ob die Verkabelung die Spezifikation nur grade eben erreicht oder ob aufgrund der Konstruktion durch den Hersteller eine entsprechende Leistungsreserve besteht. Ich habe mit Absicht die gesamte Darstellung der Transceivertechnik auf eine Taktrate von 833 MHz abgestimmt, man könnte natürlich auch höhere Raten nehmen. Aber eine Rate in diesem Bereich passt optimal zum bestehenden VLSI-Prozess. Die Verwendung höherer Raten wird ggf. zu Problemen mit diesem Entwurfsprozess führen, aber das weiß man nicht genau, denn dieser Prozess macht manchmal Sprünge. Eine Taktrate von 833 MHz würde es aber ermöglichen, dass auch eine Kat.7-Verkabelung für 40 GBASE-T reichen würde.

Eine Kat 6A-Verkabelung reicht definitiv nicht.

Fassen wir generell zusammen:

- 40 GBASE kommt, früher oder später, auch zu Ihnen
- Je später, desto billiger
- 40 GBASE-LR4 und 40 GBASE-SR müssen nur noch von den bekannten Herstellern verbaut werden, die Komponenten sind da, das passiert spätestens 2009
- Die Situation bei Switches ist abhängig von deren Grundleistung, z. B. ein Cisco 6500 kann max. 2 40 GBASE-Adapter vertragen, also wird es bei diesem Hersteller ggf. ein Nexus werden. Andererseits kann die Reihe 15.000 schon 96 X 40 Gb
- 40 GBASE-LRM ist technisch sofort möglich (AMCC), aber nicht standardisiert, kann aber 2009/10 kommen
- 40 GBASE-T wird ab 2009 von der Standardisierung aufgenommen, es gibt schon passende Kabel und Stecker, das geht dann schnell

Schwerpunktthema

Dominik Zöller ist seit 2006 Berater bei der ComConsult Beratung und Planung. Während seines Studiums konzentrierte er sich auf die Themengebiete der Kommunikationsnetze und der Betriebssysteme. Bei ComConsult ist er vorwiegend mit der Evaluierung, Planung und Ausschreibung professioneller Unified Communications, Kollaborations- und Videokonferenz-Systeme befasst.

Dr. Michael Wallbaum ist Senior Consultant der ComConsult Beratung und Planung GmbH. Er blickt auf jahrelange Projekterfahrung in Forschung, Entwicklung und Betrieb im Bereich mobiler Kommunikationssysteme, Voice-over-IP und Groupware zurück. Zu diesen Themenbereichen sind von ihm zahlreiche Veröffentlichungen und Buchbeiträge erschienen.

Dr. Frank Imhoff ist technischer Direktor und Senior Consultant der ComConsult Beratung und Planung GmbH. Er blickt auf jahrelange Erfahrung in Forschung, Entwicklung und Betrieb von lokalen Netzen, Voice-over-IP, Wireless Local Area Networks sowie anderen Mobilfunk- und Telekommunikationssystemen zurück. Zu diesen Themenbereichen sind von ihm bereits zahlreiche Veröffentlichungen erschienen und Seminare betreut worden.

# Sicherheitsaspekte öffentlicher Mobilfunknetze Teil 2: Maßnahmen zur Sicherung der mobilen Kommunikation

Fortsetzung von Seite 1

Die einzige Möglichkeit, die sich dem Kunden bietet, ist, bei der Auswahl des Providers nicht alleine nach Kostengesichtspunkten vorzugehen. Der Nachweis sicherer Infrastrukturen kann von den Betreibern durch regelmäßige Sicherheits-Audits und Zertifizierungen durch unabhängige Sachverständige erbracht werden. Doch auch wenn der Kunde sich im Vorfeld informiert und bei dem Betreiber auf solche Nachweise drängt - ein tiefgehender Einblick in die Sicherheitsaspekte des Netzes wird ihm in der Regel verwehrt bleiben. Auch personelle und organisatorische Risikofaktoren im Betreiberunternehmen entziehen sich in der Regel seiner Kenntnis. Als Grundannahme muss also - ähnlich dem Internet - immer die Unsicherheit des verwendeten Mobilfunknetzes unterstellt werden. Die Sicherheitsproblematik der Mobilfunknetze - von unzuverlässigen Verschlüsselungsverfahren bis zur Ortung von Endgeräten durch Unbefugte - macht deutlich, dass Unternehmen, deren Mitarbeiter auf die Nutzung mobiler Endgeräte angewiesen sind, ihrerseits Schutzmaßnahmen ergreifen müssen.

### Dienstabstinenz

Trotz geringer Einflussmöglichkeiten auf die Sicherheit des Netzes selbst, lassen sich einige Vorsichtsmaßnahmen treffen. Diese betreffen in erster Linie Komfortmerkmale der Endgeräte sowie vom Netz erbrachte Dienste. Ein Beispiel wäre die Ortung von Endgeräten durch externe Dienstleister. Innerhalb des Netzes ist immer eine Zuordnung von Benutzer (IMSI) und Endgerät (IMEI) zu einem Aufenthaltsort (LAI) möglich. Die im Netz verfügbaren Informationen können bei Bedarf, die Zustimmung des Teilnehmers vorausgesetzt, von externen Dienstanbietern für die Lokalisierung von Endgeräten genutzt werden. Hierfür gibt es viele sinnvolle Anwendungsgebiete, wie etwa die Ortung medizinischer Notfälle oder das Auffinden von mit GSM-Geräten ausgestatteten Fahrzeugen im Falle eines Diebstahls.

Das Endgerät muss für die Nutzung solcher Dienste registriert werden. Die Freischaltung geschieht durch zwei SMS, eine an eine Servicerufnummer des Providers und eine an die des Dienstanbieters. Danach kann das Handy, z.B. per Webinterface, geortet werden. Befindet sich ein Angreifer kurzzeitig im Besitz des Endgerätes, so kann es für die Ortung frei geschaltet und die verräterischen Bestätigungs-SMS gelöscht werden. Nicht jeder Dienstanbieter informiert den Endgerätebesitzer per SMS über einen Ortungsvorgang. So ist eine Ortung ohne Zustimmung oder Kenntnis des Besitzers möglich. Das Deaktivieren eines Ortungsdienstes geschieht, wie auch die Frei-

## Sicherheitsaspekte öffentlicher Mobilfunknetze - Teil 2

schaltung, per SMS. Jedoch gibt es für den Anwender keine automatisierte Möglichkeit, sich über den aktuellen Status solcher Freischaltungen zu informieren. Eine Nachfrage beim Mobilfunkanbieter kann hierüber im Zweifel Aufschluss geben. Eine generelle Deaktivierung solcher Funktionen ist nicht vorgesehen und muss - wenn überhaupt möglich - separat mit dem Netzbetreiber vereinbart werden. Falls das nicht möglich ist, können im konkreten Verdachtsfall an bekannte Servicenummern des Netzbetreibers SMS zur Deaktivierung geschickt werden. Hierdurch wird eine erneute Aktivierung aber nicht verhindert. (siehe Abbildung 1)


Abbildung 1: Nach Freischaltung per SMS ist eine (grobe) Ortung per Webinterface möglich

Den besten Schutz vor Ortung bietet die Anonymisierung. Zum Beispiel existieren Tauschbörsen für Endgeräte und Prepaid-Verträge, wodurch die eindeutige Zuordnung von Orts- und Personeninformationen erschwert wird. Den mit solchen Tauschverfahren verbundenen Aufwand halten in der Regel jedoch nur Drogendealer und Mafiosi für gerechtfertigt - für Unternehmen und Organisationen ist dieser Ansatz unpraktikabel.

An diesem Beispiel sieht man, dass durch eine Vielzahl von Diensten – so nützlich sie auch in ihrer ursprünglichen Intention sein mögen - Gefährdungen für den Schutz von Daten und Privatsphäre entstehen können. Es ist daher für Unternehmen und Behörden sinnvoll, sich im Vorfeld beim jeweiligen Mobilfunkbetreiber über Dienste und Leistungsmerkmale zu informieren. Die Angaben der Betreiber, ob Dienste generell deaktiviert werden können, weichen voneinander ab. Falls die Möglichkeit besteht, sollten in jeden Fall alle nicht benötigten Dienste abgeschaltet werden. Dazu zählen Ortungsdienste gleichermaßen wie Push-To-Talk (PTT) oder ähnliche Leistungsmerkmale.

Ein weiterer wichtiger Aspekt bei der Planung einer sicheren Kommunikationsumgebung, neben Wahl und Konfiguration des Netzes, ist die Endgerätesicherheit. Wie in Unternehmensnetzen die Clients besonderer Aufmerksamkeit bedürfen, so trifft dies im selben Maße auch auf mobile Endgeräte zu. Was nutzen sichere Netze, wenn ihre Endpunkte Angriffen schutzlos ausgeliefert sind? Sie dienen als Ein- und Ausgabegerät, zur Datenverarbeitung ebenso wie zur Kommunikation. Es werden Daten und persönliche Informationen auf ihnen gespeichert und die Kontrolle über ein Endgerät zu erlangen kommt in mancher Hinsicht der Übername der Identität des Besitzers gleich. Und eines unterscheidet sie vom herkömmlichen Arbeitsplatzrechner: sie sind klein, leicht und transportabel. So ist die Gefahr besonders groß, dass sie unbemerkt verloren oder entwendet werden. Es ist also insbesondere wichtig, mobile Endgeräte vor unbefugtem Zugriff, Datendiebstahl und Manipulation zu schützen.

### Vorspiegelung falscher Tatsachen

Das Endgerät wird durch die Personal Identification Number (PIN) vor Zugriff geschützt. Das jedenfalls ist der Eindruck, der sich dem Benutzer eines Mobiltelefons aufdrängt. In Wahrheit wird nicht das Endgerät vor Zugriff geschützt, sondern die PIN dient lediglich zur Authentisierung des Benutzers am Subscriber Authentication Module (SIM). Das SIM ist ein funktionaler Bestandteil der SIM-Karte und enthält die zur Authentisierung des Benutzers notwendigen Informationen, also International Mobile Subscriber Identity (IMSI) sowie das Shared Secret, welches, wie im ersten Teil dieses Artikels beschrieben, als Schlüssel für die Authentisierung dient. Die neuere Variante Universal Subscriber Identification Module (USIM), die im Zuge von UMTS eingeführt wurde, bietet ein sichereres Design der implementierten Authentisierungsmethoden. Es nimmt aber dieselbe Rolle in der Authentisierung ein wie die SIM, weshalb hier nicht weiter zwischen beiden Modulen unterschieden wird. Per PIN authentisiert sich also der Benutzer gegenüber seiner (U)SIM und kann daraufhin auf Grundlage der darin implementierten Funktionen die Authentisierung gegenüber dem Mobilfunknetz vornehmen. Das geschieht standardmäßig beim Einschalten des Mobiltelefons,

weshalb der Eindruck entsteht, der Anwender authentisiere sich für den Zugriff auf das Endgerät. Die Inhalte und Funktionen des Endgeräts werden hierdurch aber in keiner Weise geschützt.

### Identität im Netz

Da die SIM ab dem Zeitpunkt der Anmeldung im Netz die „digitale Identität" des Teilnehmers gegenüber dem Netz darstellt, ist ein umsichtiges Management der SIM-Karten in Unternehmen und Behörden erforderlich. Insbesondere müssen abhanden gekommene SIM-Karten umgehend beim Provider gesperrt werden, da ansonsten ein Missbrauch der SIM zur Vortäuschung einer falschen Identität nicht auszuschließen ist. Besonders dringend ist aber ein vorsichtiger Umgang mit der PIN geboten, da sie die SIM vor Missbrauch schützt. Gleiches gilt für den Personal Unblocking Key (PUK), der dem Nutzer das Zurücksetzen der PIN erlaubt. Dem Anwender werde sowohl PIN als auch PUK von seinem Mobilfunkbetreiber zugewiesen, weshalb dieser zunächst keinen Einfluss auf deren Beschaffenheit haben. Allerdings sollten beim Zurücksetzen der PIN darauf geachtet werden, dass die PIN nicht leicht zu erraten ist. Da eine PIN immer eine vierstellige Zahl ist, können zwar nicht dieselben Maßstäbe an die Komplexität gestellt werden, wie an alphanumerische Passwörter (siehe z.B. „Regelungen des Passwortgebrauchs", IT-Grundschutzkatalog des BSI http://www.bsi.de/gshb/deutsch/m/m02011.htm). Grundregeln, wie die Verwendung von Zufallszahlen und die sichere Aufbewahrung der PIN gelten aber universell. Beispielsweise sind Unterlagen, die PIN oder PUK enthalten, gesichert aufzubewahren oder - falls möglich - umgehend zu vernichten. Unternehmen müssen, falls PIN und PUK der Firmenhandys zentral verwaltet werden, die betroffenen Unterlagen als schutzbedürftig einstufen und den Zugriff auf einen autorisierten Personenkreis beschränken. Einige Endgeräte bieten das Abspeichern der PIN aus Komfortgründen um zum Beispiel den Wechsel der SIM-Karte im laufenden Betrieb komfortabler zu machen. Hierdurch wird aber der Zugriffschutz auf das Netz unterminiert.

Da die PIN also den Zugriff auf das Netz schützt, nicht aber den auf das Endgerät, muss für dieses unbedingt ein Passwort gesetzt werden. Die meisten Endgeräte bieten diese Möglichkeit. Falls möglich, sollte ein alphanumerisches Kennwort unter Berücksichtigung der Empfehlungen des IT-Grundschutzkataloges (http://www.bsi.de/gshb/index.htm) gewählt werden, zumindest aber ein von der PIN verschiedener Code. Zu bemängeln ist, dass dieses Kennwort meist nur beim Einschalten eines Endgeräts abgefragt wird. Die flächendeckend vorhandene Tastensperre für den laufenden Betrieb lässt sich aber in den seltensten Fällen durch ein Passwort sichern. So ist das Endgerät zwar vor der Weiterverwendung nach einem Diebstahl geschützt, dem Dieb steht aber zunächst einmal der Zugriff auf sämtliche Daten offen. Falls das Mobiltelefon zudem den Wechsel der SIM-Karte im laufenden Betrieb erlaubt, ohne auf erneute Eingabe des Passwortes zu bestehen, so ist auch die Weiterverwendung eines gestohlenen Endgerätes möglich. Bietet das Betriebssystem die Wahl, so sollten Abstriche im Komfort in Kauf genommen werden und sämtliche Änderungen am Endgerät passwortgeschützt werden. (siehe Abbildung 2)

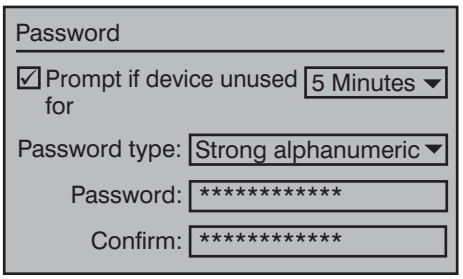



Abbildung 2: Endgeräte sollten durch ein starkes, alphanumerisches Passwort geschützt werden

### Zugang verweigern

Was für die Benutzeroberfläche des Endgerätes gilt, trifft in ähnlicher Weise auch auf die Vielzahl möglicher Schnittstellen zu. Zum einen gibt es die herstellerspezifischen Schnittstellen, die zum Anschluss externen Zubehörs wie etwa Headsets oder zur Synchronisation mit dem PC per USB dienen. Darüber hinaus ist oft die Peripherieanbindung und Datenübertragung mittels Infrarot-Schnittstelle oder Bluetooth möglich. Der beste Weg, diese Schnittstellen zu sichern, ist, sie komplett abzuschalten. Das ist nicht immer möglich oder erwünscht. Eine temporäre Aktivierung bei Bedarf stellt aber einen guten Kompromiss dar. Nach Möglichkeit sollten diese Schnittstellen mit einem separaten Passwort gesichert werden. (siehe Abbildung 3)

Im Falle von Bluetooth empfiehlt sich die Nutzung des „unsichtbaren" Modus, in dem die Endgeräte-Kennung nicht über die Funkschnittstelle gebroadcastet wird. In jedem Fall ist zu beachten, dass die momentan eingesetzten Versionen 1.2 und 2.0 nur eine einseitige Authentisierung verwenden, die Man-in-Middle-Attacken ermöglichen. Verschlüsselung findet bei diesen Versionen nur auf Grundlage einer nutzerdefinierten PIN oder eines gerätespezifischen Schlüssels statt. Erst die Version 2.1 wird mit Secure Simple Pairing, dass auf einem Public Key Verfahren basiert, einen wirksamen Schutz vor Man-in-the-Middle bieten. Bis zur flächendeckenden Verfügbarkeit von Version 2.1 sollte bei erhöhtem Schutzbedarf auf die Verwendung von Bluetooth verzichtet werden. Im Fall von Bluetooth-Headsets empfiehlt sich alternativ, auf Modelle zurückzugreifen, die den Datenstrom vor der Übertragung über die Luftschnittstelle zusätzlich verschlüsseln.

### Taschendiebe

Sind alle Schnittstellen gesichert, so verbleibt trotzdem ein Restrisiko für Datendiebstahl. Wer kennt es nicht: Man steht kurz auf und lässt das Handy am Platz liegen. Ob aus Vergesslichkeit oder dem Gefühl heraus, dass während der kurzen Abwesenheit ja nichts passieren könne. Ein unbemerkter Handgriff und der Datendieb ist im Besitz des Endgeräts. Selbst falls der Zugriff auf das Endgerät per Passwort genügender Stärke gesichert ist, muss das Endgerät nicht entwendet werden, um in langwieriger Arbeit die Passwortmechanismen außer Kraft zu setzen. Zum einen hat die Datenmenge, die auf Endgeräten durchschnittlich gespeichert wird, so zugenommen, dass sie in der Regel nicht mehr auf internem Flash-Speicher des Endgeräts - geschweige denn auf der SIM-Karte - untergebracht werden kann. Da der Einbau eines sehr großen Flash-Speichers fester Größe unwirtschaftlich und unflexibel ist, wird zumeist auf auswechselbare Speicherkarten zurückgegriffen. Sie bieten dem Anwender höheren

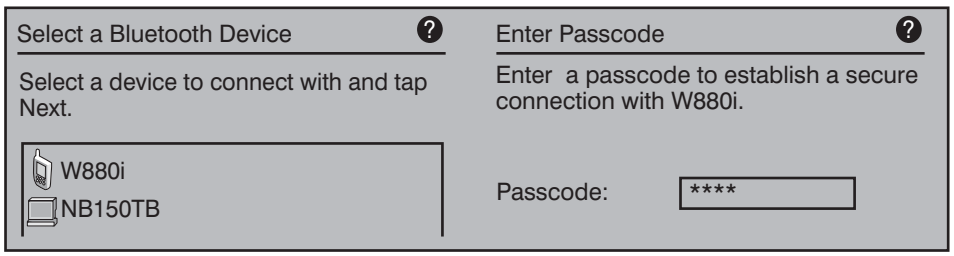



Abbildung 3: Bluetooth unterstützte in frühen Versionen nur die Authentisierung per PIN

Sicherheitsaspekte öffentlicher Mobilfunknetze - Teil 2

Komfort und mehr Flexibilität bei der Verwaltung von größeren Datenmengen und das zu einem sehr günstigen Preis. Und nicht nur Musikdateien, Klingeltöne, Videos, Fotos und andere im Consumer-Segment sehr verbreitete Datenformate werden auf solchen Karten abgelegt. Auch Kontakte, Kurzmitteilungen, Zusatzapplikationen und andere - eventuell sensible - Daten können hierauf gespeichert werden. Der große Nachteil ist, dass eine solche Speicherkarte mit ein paar Handgriffen entnommen und kopiert oder ausgetauscht werden kann.

**„Forensik“**

Der nächstliegende Gedanke zur Sicherung sensibler Daten wäre also, diese ausschließlich auf dem kleineren, fest verbauten Flash-Speicher des Endgeräts abzulegen. Doch angesichts der Tatsache, dass heutzutage große Datenmengen in Form von Emails mit Anhängen, Grafiken und Dokumenten aller Art auf dem mobilen Endgerät zum Arbeitsalltag gehören, ist das eine kaum gangbare Methode. Auch kann man den Einschub für Speicherkarten kaum physikalisch gegen Entnahme der Speicherkarten sichern. Zudem lässt sich über die herstellerspezifische Synchronisationsschnittstelle ein physikalisches Abbild der im Endgerät vorhandenen Speichermedien machen. Hierfür kann entweder ein Standard-PC mit passendem Adapterkabel und einer entsprechenden Software für den „forensischen“ Einsatz verwendet werden. Alternativ bieten Hersteller von Produkten für „mobile forensics“ mittlerweile kompakte Geräte mit ähnlichen Abmessungen wie ein mobiles Endgerät. (siehe Abbildung 4)

Mit Hilfe solcher Werkzeuge kann unauffällig ein Speicherabbild zur späteren Analyse an einem leistungsfähigen Rechner erstellt werden. Sowohl diese Geräte


Abbildung 4: Forensische Hardware von Paraben

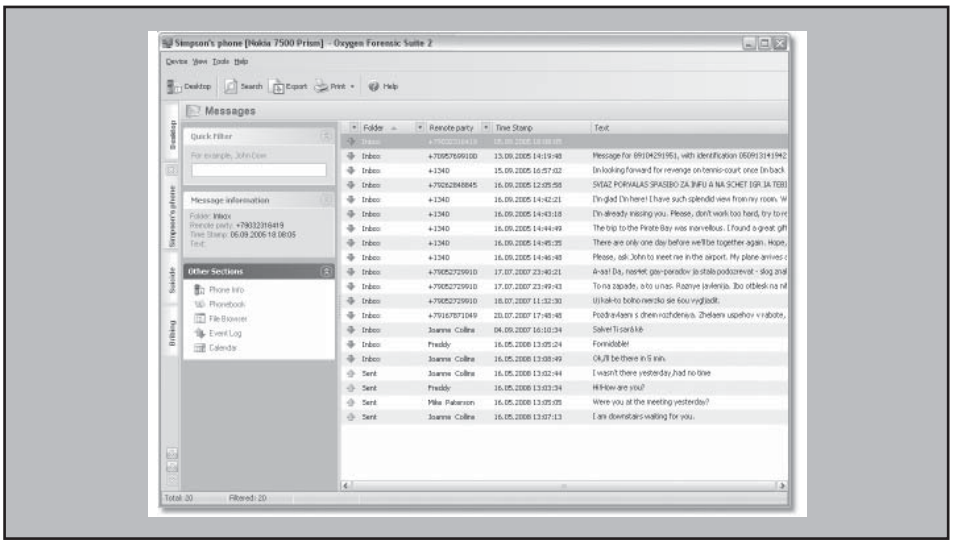



Abbildung 5: Analysesoftware von Oxygen Forensics

als auch die Software zur Analyse der so gewonnenen Daten haben die legale Intention der Datenwiederherstellung und der digitalen Beweisführung für Unternehmen und Behörden. Der Erwerb ist problemlos möglich, der beschriebene Einsatz zum Datendiebstahl stellt allerdings in Deutschland einen Straftatbestand dar. Industriespione oder Betrüger, die es auf sensible Daten abgesehen haben, wird das wohl kaum abschrecken. (siehe Abbildung 5)

**Verschlüsselter Datenbestand**

Da bleibt dem Nutzer schließlich nur eine Wahl: wenn er die Daten schon nicht vor dem Zugriff Dritter schützen kann, muss er durch Verschlüsselung dafür sorgen, dass sie für Unbefugte nutzlos sind. Aktuelle Verschlüsselungsverfahren mit Block- und Schlüssellängen von 128 bis 2048 Bit wie z.B. das, auch als Advanced Encryption Standard (AES) bekannte, Rijndael-Verfahren, bieten dem aktuellen Erkenntnisstand nach einen zuverlässigen Schutz. AES ist beispielsweise auch für höchste behördliche Geheimhaltungsstufen zulässig. Darüber hinaus ist der Algorithmus bei korrekter Implementierung performant genug, um Prozessoren aktueller Smartphones nicht über die Maßen auszulasten. Dennoch sind immer leichte, wenn auch vielleicht nicht wahrnehmbare, Performanceeinbußen zu erwarten. Die Verschlüsselung insbesondere sensibler Daten ist trotzdem unverzichtbar. Darunter fallen:

- Persönliche Informationen
- Kontaktdaten
- Nachrichten sensiblen Inhalts
- Passwörter und Zertifikate

Diese Informationen stellen das absolute Minimum der zu schützenden Daten dar. Hinzu kommen Dateien aus Office- und Unternehmensanwendungen. Da der Anwender nicht immer im laufenden Betrieb zwischen sensiblen und weniger sensiblen Informationen unterscheiden kann, sollten der Einfachheit halber sämtliche Daten bzw. das komplette Speichermedium verschlüsselt werden. Die einzige Ausnahme sollten Daten sein, die in Echtzeitanwendungen zum Einsatz kommen und nicht mit der notwendigen Geschwindigkeit vom Endgerät entschlüsselt werden können. Deren Inhalt darf allerdings nicht sensibel sein. Ein Beispiel sind privat genutzte Musikdateien. (siehe Abbildung 6)

Einige moderne Endgeräte bieten die Möglichkeit, sämtliche enthaltenen Daten zu verschlüsseln. Wenn dies nicht der Fall ist, oder falls die gebotenen Verschlüsselungsmechanismen keine ausreichende Sicherheit bieten, kann die Verschlüsselung durch Drittanbieterapplikationen implementiert werden. Für die sichere Speicherung von Passwörtern und Zertifikaten zur Authentisierung stehen ebenfalls verschiedene Software-Lösungen zur Verfügung, die den Zugriff durch ein oder mehrere Masterpasswörter regulieren. Produkte zur Verschlüsselung sorgen dafür, dass benötigte Daten im laufenden Betrieb - ohne Zutun des Nutzers - entschlüsselt werden. Idealerweise sind die Daten auch während dieser Nutzungszeiträume weiterhin vor Zugriff geschützt, zum Beispiel durch konkrete Freigabe für bestimmte Applikationen. Weiterer Vorteil einer solchen, applikationsbasierten Freigabe ist es, dass ein zusätzlicher Schutz vor eventuell von außen eingeschleppter Schadsoftware geschaffen wird.

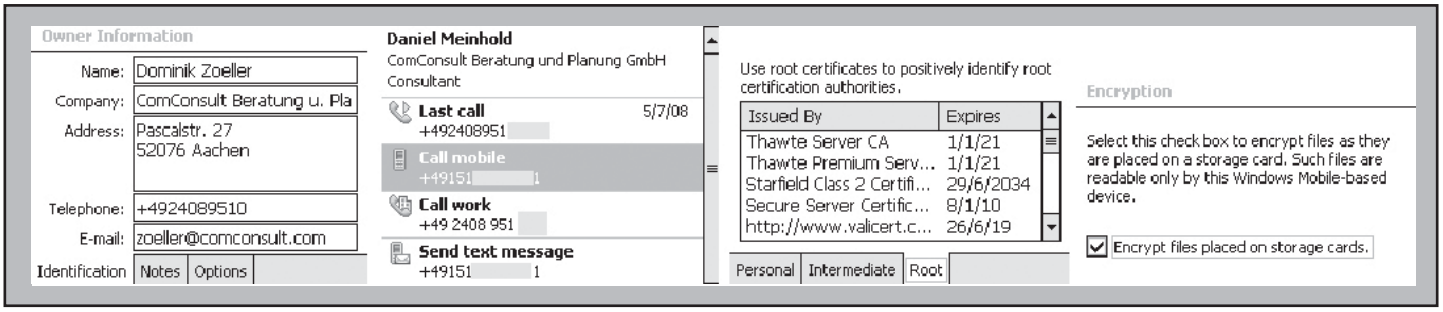



Abbildung 6: Kontaktdaten und andere sensible Daten werden durch Verschlüsselung geschützt

### Einheitlich anfällig

Aktuelle Smartphones sind kleine Computer mit eigenem Betriebssystem. Ob Symbian, Windows Mobile, ob Mac OS.X in der iPhone-Variante oder Googles Android - auch wenn sich die Zahl der Viren und Trojaner noch in Grenzen hält, wird mit der steigenden Verbreitung intelligenter Telefone die Zahl solcher Schadprogramme zunehmen. Das liegt zum einen an der häufigeren Nutzung von Mobiltelefonen im Allgemeinen und den vielen Sicherheits-Schwachstellen, die die Endgeräte in Folge sehr kurzer Entwicklungs- und Produktzyklen mit sich bringen. Zum anderen benötigen Schadprogramme immer eine möglichst einheitliche Plattform zu ihrer Verbreitung. Diese Basis wird erst durch die Nutzung geräteunabhängiger Betriebssysteme geschaffen. Was allerdings auf der einen Seite eine größere Angriffsfläche für Schadprogramme bietet, ist in vieler Hinsicht ein sicherheitstechnischer Vorteil. Durch die geräteunabhängige Weiterentwicklung wird der Nachteil der kurzen Produktzyklen teilweise kompensiert. Zudem befördert es auch die einfachere Entwicklung robuster und sicherer Applikationen, welche unabhängig vom Endgerät eingesetzt werden können. (siehe Abbildung 7)

Zu diesen Applikationen zählen auch Instrumente für den Schutz der Endgeräte, allen voran Virenscanner und Software zum Aufspüren von Spyware und Trojanern. Hier bieten viele namhafte, teils bereits aus dem PC-Bereich bekannte Hersteller entsprechende Produkte an. Selbiges gilt für Personal Firewalls, die sich bei der Verwendung mobiler Datendienste empfehlen und einen wirksamen Schutz vor unbefugtem Zugriff über die Netzwerkschnittstellen bieten können.

### Zentralkomitee

Die Absicherung der Endgeräte setzt, neben der Installation von Zusatzapplikationen, die Konfiguration einer Vielzahl von Parametern voraus. Hinzu kommen Deployment von Betriebssystem, Zertifikaten und nutzerspezifischen Konfigurationen. Um in großen Unternehmen und Organisationen dem einzelnen Anwender eine manuelle Konfiguration zu ersparen, empfiehlt sich der Einsatz einer Lösung für das Mobile Device Management (MDM). So kann die versehentliche oder absichtliche Fehlkonfiguration von Endgeräten vermieden und der Technische Support entlastet werden. Solche Lösungen sind von vielen Herstellern verfügbar (z.B. RIM, iAnywhere, Synchronica, ubitexx) und erlauben die Verwaltung verschiedenster Endgeräte und Betriebssysteme. Die Kompatibilität mit dem gewünschten Betriebssystem und den Endgeräten muss im Einzelnen vor Anschaffung geprüft werden.

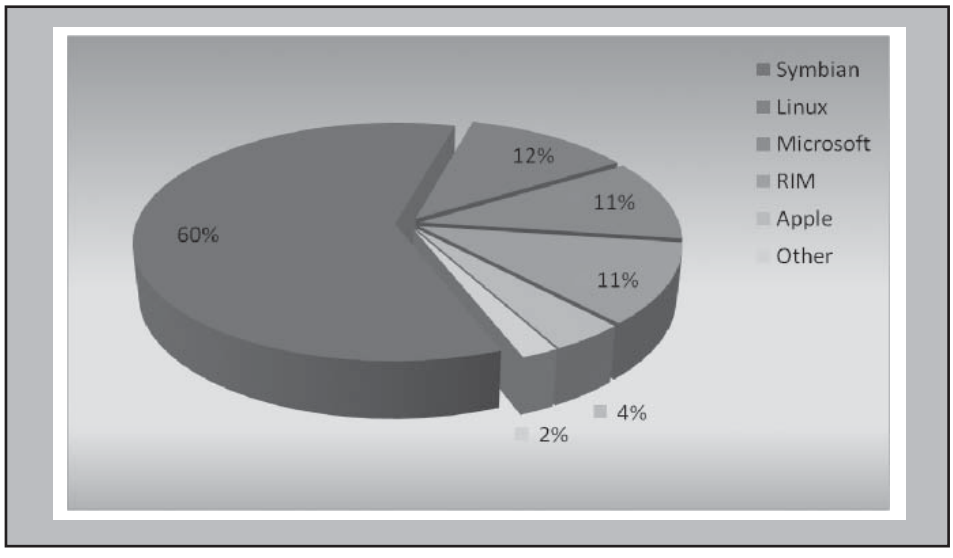



Abbildung 7: Einige wenige Betriebssysteme teilen sich den Markt der mobilen Endgeräte
(Quelle: Symbian Foundation, Stand Q1/2008)

Vor Einführung eines MDM muss eine detaillierte Richtlinie für die Endgerätesicherheit erstellt werden. Insbesondere sollten folgende Punkte erfasst werden (siehe Abbildung 8):

- Benutzergruppen und -hierarchie
- Kategorisierung sensibler Daten
- Richtlinien zur Speicherung und Verschlüsselung von Daten
- Einschränkung benötigter und genehmigter Zusatzapplikationen
- Einschränkung benötigter Dienste und Leistungsmerkmale
- Konfiguration für den Zugriff auf die Unternehmensinfrastruktur
- Festlegung unveränderlicher Konfigurationsparameter

Diese Richtlinie wird dann anhand des MDM als Templates für alle Benutzergruppen und Endgerätetypen umgesetzt. Weiterer Vorteil einer solchen Lösung ist, dass die verwalteten Mobiltelefone im laufenden Betrieb administriert werden können. Sobald eine Datenverbindung verfügbar ist, können Konfigurationsdaten zentral verwaltet und so Nachbesserungen an den Sicherheitsrichtlinien schnell umgesetzt werden. Außerdem ist das Zurücksetzen des kompletten Mobiltelefons auf den Werkszustand möglich. Des Weiteren erlauben einige Lösungen, die Daten auf verloren gegangenen Endgeräten per Fernzugriff zu vernichten, so dass die Gefahr eines Datendiebstahls verringert wird. Diese Möglichkeiten wiegen den

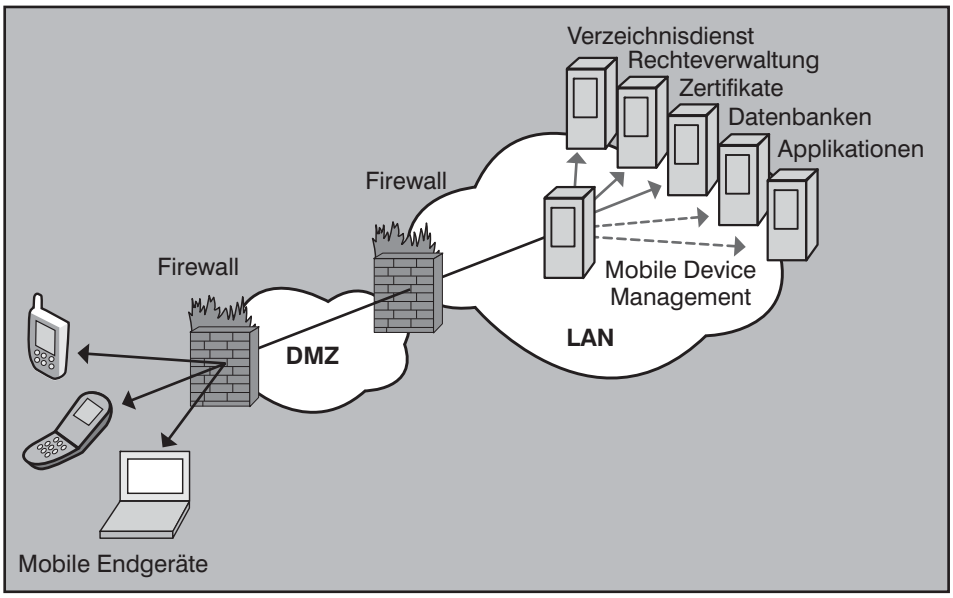



Abbildung 8: Mobile Device Management verwaltet Endgeräte und Zugriffsrechte

Aufwand und die Kosten der notwendigen Infrastruktur auf und machen MDM für Unternehmen mit vielen mobilen Mitarbeitern sehr attraktiv.

### Überwachung des Luftraums

Sind die Endgeräte gegen den direkten Zugriff gesichert, stellt sich immer noch die Frage der Übertragungssicherheit. Einige Endgeräte bieten die Möglichkeit, den Verschlüsselungsstatus der Luftschnittstelle anzeigen zu lassen. In der Regel wird eine verschlüsselte Verbindung durch ein kleines Schloss-Symbol im Display angezeigt. Das bietet dem Anwender zumindest eine gewisse Transparenz in Bezug auf die Verbindungssicherheit. Wünschenswert wäre auch eine Anzeige, welche Form der Verschlüsselung verwendet wird, also A5/1, A5/2 oder das momentan als sicher geltende Kasumi. Nachteil der grafischen Signalisierung ist, dass sich der Status auch während eines Gesprächs ändern kann, beispielsweise beim Zellwechsel oder beim Roaming durch verschiedene Betreibernetze. Eine solche Änderung wird von einigen Endgeräten zusätzlich akustisch mitgeteilt. Aber auch das Wissen um die Verschlüsselung der Luftschnittstelle kann die Abhörgefahr nur eindämmen, nicht aber ausräumen. Wie im ersten Teil beschrieben, endet die Verschlüsselung der Sprach- und Datenkommunikation bei Eintritt in das Providernetzwerk. Da ist es am Unternehmen, eine einheitliche Lösung für die Ende-zu-Ende-Verschlüsselung der Kommunikation ihrer Mitarbeiter bereitzustellen. Hier stehen verschiedene Varianten zur Verfügung.

### Sichere Klassiker

Die wohl wasserdichteste Möglichkeit, die Sprachkommunikation abzusichern, ist der Einsatz von speziellen Kryptographie-Endgeräten. Verschiedene Hersteller wie z.B. die Rohde & Schwarz SIT GmbH bieten solche mit speziellem Kryptographiechip ausgestattete Mobiltelefone. Das Betriebssystem des als Basis verwendeten Standard-Mobiltelefons wird derart angepasst, dass sich die Verschlüsselung der Sprachdaten einschalten lässt, falls die Gegenseite über ein gleichartiges Verschlüsselungssystem verfügt. Alle namhaften Hersteller garantieren durch Zertifizierungen für die Sicherheit der eingesetzten Verfahren. Allerdings ist die sichere Kommunikation damit in der Regel auf Endgeräte desselben Herstellers beschränkt. Zudem ergibt sich durch die hardwareseitige Realisierung ein weiterer Nachteil: die Implementierung findet auf Basis bereits auf dem Markt befindlicher, bewährter Endgeräte statt. Die technische Basis des Endgeräts hinkt also dem aktuellen Stand der Technik immer ein wenig hinterher. Neben den technischen Einschränkungen, die sich hieraus ergeben, stellt sich hier die Frage der Akzeptanz im Unternehmen. Gerade im geschäftlichen Umfeld ist das Handy heute nicht nur Kommunikationsmittel, sondern immer auch Prestige-Objekt und Spiegel der technischen Aktualität des Unternehmens. Auch wenn es unter Sicherheitsaspekten sinnvoll sein mag, wird kaum ein Vorstandsmitglied gerne sein iPhone gegen ein TopSEC GSM auf Basis des zuverlässigen, aber betagten Siemens S35i eintauschen. Die Abhängigkeit vom verwendeten Endgerät kann also die Einführung deutlich erschweren. Hinzu kommt ein vergleichsweise hoher Preis der Endgeräte, der den flächendeckenden Einsatz im Unternehmen unwirtschaftlich werden lässt.

### Von Ohr zu Ohr

Unabhängig vom mobilen Endgerät sind kryptographiefähige Headsets. In der

## Sicherheitsaspekte öffentlicher Mobilfunknetze - Teil 2

Festnetz-Telefonie werden bei erhöhtem Schutzbedarf gerne so genannte „Kryptographie-Boxen“ eingesetzt. Diese Hardware verschlüsselt die Sprachdaten im Zusammenspiel mit einer weiteren Crypto Box auf der Gegenseite. So entsteht ein virtueller, gesicherter Sprachkanal. Kryptographiefähige Headsets funktionieren nach einem ähnlichen Prinzip. Während der eigentliche Übertragungskanal unbeeinflusst bleibt, werden die übermittelten Sprachdaten verschlüsselt. Dies geschieht bereits im Headset, so dass selbst im Endgerät die Sprachdaten niemals unverschlüsselt vorliegen. So ist, sogar bei Kompromittierung der Übertragungswege oder des Endgeräts, die Sicherheit der Sprachdaten immer gewährleistet. Das Problem dieser Lösung liegt darin, dass die Gegenstelle meist über ein identisches Headset verfügen muss. Zwar kommen standardisierte Verfahren für Schlüsseltausch und Verschlüsselung zum Einsatz, die Kompatibilität ist aber in der Regel auf Geräte desselben Typs, zumindest aber Produkte desselben Herstellers beschränkt. Das führt zu dem organisatorischen Problem, sämtliche Gesprächspartner mit der notwendigen Technik auszustatten. Der Aufwand lohnt in der Regel nur für abgeschlossene Personenkreise, die regelmäßig untereinander sensible Informationen austauschen. Bestes Beispiel wären Mitglieder der Geschäftsleitung oder Unternehmensvorstände. (siehe Abbildung 9)

Eine weitere Möglichkeit unter Einsatz von Kryptographie-Hardware sind spezielle Speicherkarten im SD-Format (Secure Digital), welche für den mobilen Einsatz in unsicheren Umgebungen konzipiert sind. Sie bieten eine Reihe von Sicherheitsfunktionen, wie z.B. verschlüsselter Speicherplatz, interne Schlüsselgenerierung und sichere Speicherung von Schlüsseln und Zertifikaten. Auf Basis dieser Funktionen wird dann ein Kommunikationsframework aufgesetzt, welches für die automatische Aushandlung der Verschlüsselung übertragener (Sprach-)Daten sorgt. Die notwendige Software wird oft für mehrere Betriebssysteme angeboten, so dass der Einsatz nicht auf Mobiltelefone beschränkt ist. Auch ein Einsatz auf Notebooks mit SD-Card Leser ist möglich. Des Weiteren erlauben verschiedene Lösungen auch das zentrale Management solcher SD-Karten. So ist ein unternehmensweiter Einsatz leichter zu implementieren. Auf diesem Verfahren können verschiedene Software-Lösungen für verschlüsselte Sprach- und Datenkommunikation realisiert werden. (siehe Abbildung 10)


Abbildung 9: Crypto-Hardware von DICA

### Unified Security

Der software-basierte Ansatz ist wohl die flexibelste Variante verschlüsselter Telefonie. Es wird eine Kommunikationssoftware eingesetzt, die sämtliche Sprachdaten vor der Übertragung verschlüsselt. Hier stehen diverse Produkte zur Auswahl. Nahezu jeder Voice-over-IP (VoIP) Client besitzt die Fähigkeit zur Verschlüsselung. Der Vorteil liegt in der Verfügbarkeit solcher Lösungen für eine Vielzahl von Endgeräten und Betriebssystemen. Der Einsatz ist nicht alleine auf mobile Endgeräte beschränkt, was eine Integration in die Kommunikationsinfrastruktur eines Unternehmens erleichtert. Zu beachten ist, dass die Sprachdaten dann aber nicht, wie im Fall von Kryptographie-Endgeräten oder - Headsets, über die Sprachkanäle des Mobilfunknetzes übertragen werden. Hierfür werden - im Falle von VoIP - IP-fähige Datenkanäle wie GPRS, EDGE oder UMTS verwendet. Dabei können Daten zur Signalisierung zwischen Client und Kommunikationsserver, also beispielsweise SIP oder H.323, auf dem kompletten Übertragungsweg durch Verwendung von Protokollen wie TLS (Transport Layer Security) geschützt werden. Da die Sprachdaten, im Gegensatz zu den Signalisierungsdaten, bei VoIP mittels Real Time Protocol (RTP) direkt zwischen den Teilnehmern geroutet werden, muss man diese separat verschlüsseln. Hierfür kommt die Variante Secure Real-Time Protocol (SRTP) zum Einsatz, die auf dem AES Algorithmus basiert. Der Schutz der notwendigen Zertifikate und gespeicherten Zugangsdaten muss - unabhängig von der eingesetzten Kommunikationssoftware - durch verschlüsselte Datenträger, spezielle SD-Cards oder Applikationen zur Aufbewahrung von Passwörtern erfolgen. (siehe Abbildung 11)

Abbildung 10: Crypto-Headset von Rohde&Schwarz

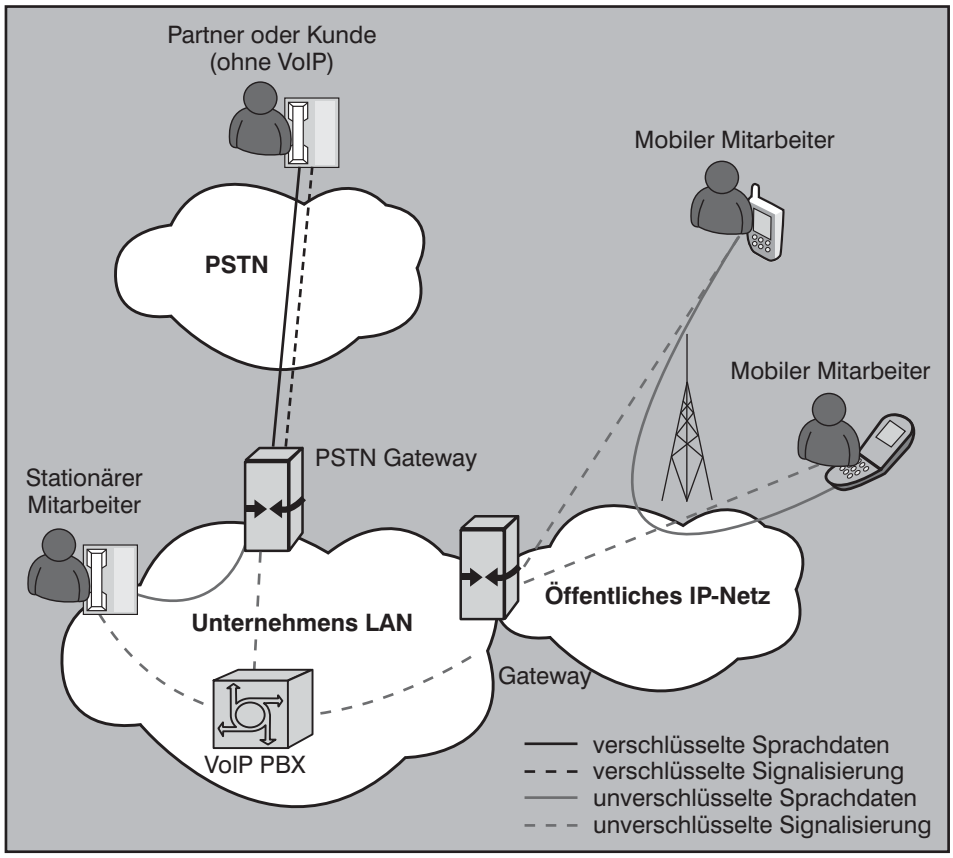



Abbildung 11: Verschlüsselte VoIP-Telefonie ermöglicht sichere Kommunikation im Mobilfunknetz

Nachteil einer solchen Lösung sind die - je nach Tarif deutlich höheren - Gebühren, die für die Übertragung über Datenkanäle anfallen. Ohne entsprechende Datentarife oder Flatrates ist eine solche Lösung kaum wirtschaftlich zu betreiben. Hinzu kommt, dass für die Telefonie ins öffentliche Telefonnetz (Public Switched Telephony Network, PSTN) Gateways benötigt werden. Während Privatanwender und kleinere Unternehmen hier auf Dienstanbieter für IP-Telefonie zurückgreifen können, bietet es sich für mittlere und große Unternehmen an, solche Gateways im Rahmen der unternehmensweiten Kommunikationslösung im eigenen Haus bereitzustellen. Allerdings fallen in beiden Fällen zusätzliche Verbindungsgebühren für den Übergang ins öffentliche Telefonnetz an. Zudem ist zu beachten, dass der RTP-Strom am PSTN-Gateway neu kodiert wird. Die Verschlüsselung endet somit beim Übergang ins öffentliche Telefonnetz. Ende-zu-Ende Verschlüsselung liegt also nur dann vor, wenn das Gespräch zwischen zwei SRTP-fähigen VoIP-Clients geführt wird. Ab dem Gateway können dann - für ausgewählte Verbindungen - bei Bedarf dieselben Verfahren eingesetzt werden, wie sie auch bislang zur Verschlüsselung von Festnetz-Telefonie angewendet wurden.

Trotzdem bleibt der Vorteil, dass vom Endgerät bis zum Gateway, welches sich optimalerweise in einer abgeschotteten Netzwerkumgebung befindet, die Sprachdaten hinreichend geschützt sind. Zudem kann bei unternehmensweiter Einführung von VoIP und den zugehörigen Verschlüsselungsverfahren die Sicherheit der gesamten internen Kommunikation erhöht werden. Ein weiterer Vorteil ist, dass man ohne großen Mehraufwand, anstelle reiner VoIP-Lösungen, umfangreiche Unified Communications Produkte einsetzen kann. Diese bieten neben der Telefonie weitere nutzbringende Kommunikationsformen wie Instant Messaging, Presence oder Videokonferenz. Instant Messaging (IM) kann hier als Alternative zur Verwendung von Kurzmitteilungen (Short Message Service, SMS) dienen. Andernfalls müssten diese, um ihre Vertraulichkeit zu wahren, ebenfalls einer Inhaltsverschlüsselung unterzogen werden, da - wie auch bei der Sprachkommunikation - netzseitig keine Ende-zu-Ende Verschlüsselung möglich ist. IM kann im Rahmen einer unternehmensweiten Unified Communications Lösung sicher übertragen werden und stellt somit eine Alternative zu SMS innerhalb des Unternehmens dar. Unter Verwendung einer Unified Communications Lösung wird das Mobiltelefon also zum integralen Bestandteil der Unternehmenskommunikation, statt eine ungesicherte Insel und ein Einfallstor ins Unternehmensnetz zu bilden.

**Datentunnel**

Neben der Telefonie ist auch die mobile Datenkommunikation besonderen Gefährdungen ausgesetzt. Der Zugriff auf das Unternehmensnetzwerk - sei es zum Abrufen von Emails oder für den Zugriff auf sensible Daten - muss daher zusätzlich geschützt werden. Hierfür empfiehlt sich der Aufbau eines Virtual Private Network (VPN). Dabei stellt der Client, nach erfolgreicher Authentisierung, eine gesicherte Verbindung ins Unternehmensnetz her und erhält eine IP-Adresse aus diesem Netz zugewiesen. Durch diese Verbindung werden dann sämtliche Daten „getunnelt“, der Client befindet sich vermeintlich innerhalb des Unternehmensnetzwerkes. Hieraus ergeben sich einige Vor- und Nachteile. Nachteil von VPN-Tunneln ist die im Vergleich zu unverschlüsselten Verbindungen reduzierte effektive Datenrate. Der durch VPN entstehende Overhead treibt das übertragene Datenvolumen in die Höhe, was die Nutzbarkeit schmalbandiger Datendienste wie GPRS deutlich einschränkt. Zudem entstehen dadurch erhöhte Kosten, so dass ein Einsatz von VPN nur bei gelegentlicher Nutzung oder aber entsprechenden Datentarifen in Frage kommt. Nachteilig ist mit Sicherheit auch, dass das Endgerät zur Schwachstelle des Unternehmensnetzes wird. Ist es nicht ausreichend gesichert, so besteht die Gefahr, dass ein Angreifer sich des Endgeräts bemächtigt und so Zugriff auf die Daten des Unternehmens erhält. (siehe Abbildung 12)

Hiergegen kann man eine Reihe von zusätzlichen Vorsichtsmaßnahmen ergreifen. Idealerweise werden den Endgeräten IP-Adressen aus einem gesonderten Subnetz zugewiesen, welches von den sensiblen Subnetzen des Unternehmens durch eine Firewall getrennt wird. Diese reguliert den Zugriff auf die für die mobilen Endgeräte zugänglichen Daten und Dienste im Unternehmen. Diese Dienste können zusätzlich von vorgelagerten Proxy Servern erbracht werden, so dass kein direkter Zugriff auf die sensiblen Subnetze notwendig ist und somit das Produktivnetz vor eventuell kompromittierten Endgeräten geschützt wird. Als Schutz vor verlorenen oder gestohlenen Endgeräten empfiehlt es sich, zum Aufbau des Tunnels IPsec mit zertifikatsbasierter Authentisierung zu nutzen. Die Zertifikate können zentral verwaltet und im Verlustfall einfach

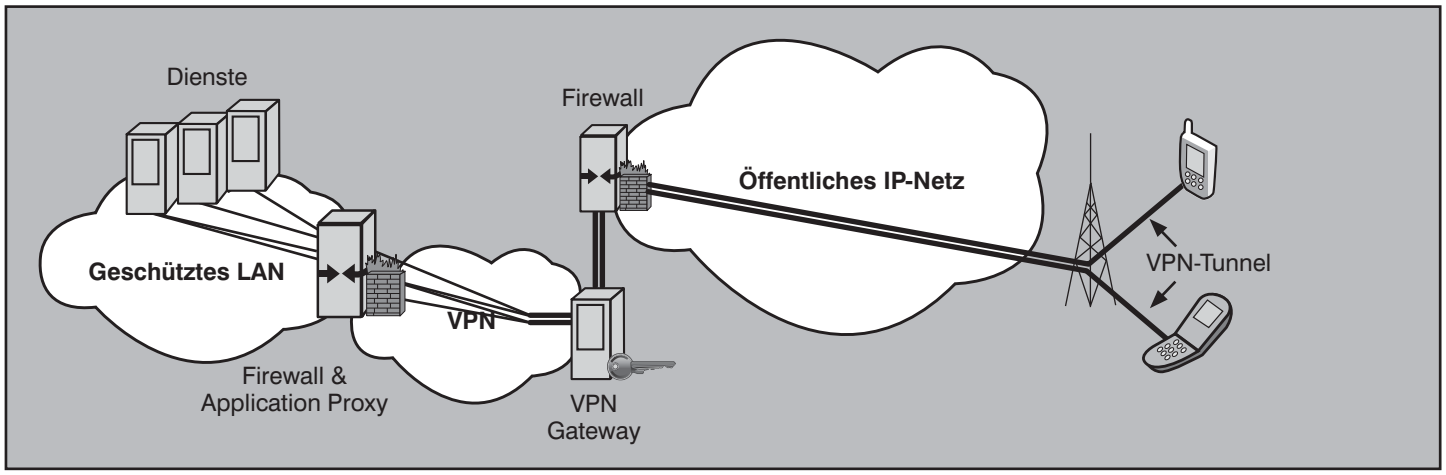



Abbildung 12: Mögliche Architektur einer VPN-Lösung für den mobilen Zugriff

gesperrt werden. Das Subnetz für den VPN-Zugang kann - bis auf den VPN-Server - vom WAN vollständig getrennt werden, oder aber durch eine Firewall und weitere Komponenten, wie einen Web Proxy, einen kontrollierten Zugang auf das WAN erlauben. So ist es auch möglich, den Zugriff auf Dienste im Internet generell über das Unternehmensnetzwerk umzuleiten und durch Proxies die Nutzung der Dienste entsprechend der Unternehmensrichtlinien einzuschränken. Die Bereitstellung weiterer Infrastruktur wie WAP Proxies und Synchronisationsserver für Push Mail sind eine sinnvolle Ergänzung einer solchen Infrastruktur.

### Schutz vor Dritten

All diese Maßnahmen dienen dazu, die Benutzung der Endgeräte im täglichen Gebrauch sicherer zu machen. Während man solche Maßnahmen für sämtliche Endgeräte innerhalb von Unternehmen und Organisationen relativ problemlos realisieren kann, gibt es keine Möglichkeit diese Maßnahmen auf Endgeräte anzuwenden, die von Partnern, Kunden oder Besuchern in die Firmenumgebung mitgebracht werden. So besteht prinzipiell immer die Möglichkeit, dass schlecht administrierte und dadurch anfällige Endgeräte Dritter die Vertraulichkeit von Informationen gefährden. Das gilt insbesondere für schützenswerte Bereiche in Unternehmen und Behörden wie etwa Entwicklungsabteilungen, Vorstandsbüros, Rechenzentren und Konferenzräume in denen vertrauliche Besprechungen stattfinden. Da man nicht sicher stellen kann, dass Personen, die solche Umgebungen betreten, ihre Endgeräte entsprechend umsichtig konfiguriert haben, muss die Verwendung von Mobilfunk in solch sensiblen Bereichen unterbunden werden. Ansonsten wäre es möglich, dass ein Angreifer das Endgerät eines Anwesenden zum Abhören von Besprechungen oder für den Diebstahl von Daten aus geschützten Umgebungen verwendet. (siehe Abbildungen 13 und 14)

Der einzig wirksame Schutz hiervor ist es, klare Verhaltensmaßregeln und Richtlinien für die Verwendung von mobilen Endgeräten im Unternehmen zu erstellen. Eine Zutrittskontrolle, bei der jeder Anwesende auf das Mitführen eines Endgeräts untersucht wird, ist in der Regel weder wirtschaftlich noch organisatorisch sinnvoll durchzuführen. Sie lohnt nur in Bereichen besonders hoher Gefährdungsstufe und selbst hier verkommen entsprechende Vorschriften meist zu reiner Symbolik. Alle Autoren dieses Artikels verfügen über mindestens zwei aktiv genutzte Mobilfunkgeräte - für Industriespione dürfte das gleiche gelten. Unter diesen Umständen fällt es leicht ein Alibi-Gerät beim Pförtner zu hinterlassen. Ohne zumindest stichprobenartige Taschenkontrollen und Leibesvisitationen wird jedes Handyverbot zur Farce.

Ein anderer denkbarer Weg wäre das Unterbinden sämtlicher Mobilkommunikation durch aktive Störsender (engl. „jammer“). Der Einsatz ist allerdings für die Privatwirtschaft in Deutschland nicht zugelassen und auch im behördlichen Umfeld nur äußerst eingeschränkt möglich. Die Abschirmung von Räumen gegen elektromagnetische Strahlung und somit auch gegen die Funkwellen der Mobilfunknetze ist technisch unproblematisch möglich, aber sehr aufwändig und teuer. Auch diese Maßnahme ist nur für Räumlichkeiten mit sehr hoher Geheimhaltungsstufe sinnvoll. Da bleibt nur die Möglichkeit, eingeschaltete und eventuell sendende Endgeräte mithilfe von Detektoren aufzuspüren, um die Einhaltung der Sicherheitsrichtlinien zu überprüfen. Mobilfunkdetektoren unterscheiden sich in aktive und passive Geräte. Aktive Detektoren senden selbst,

Abbildung 13: Passiver GSM-Detektor
(Quelle: Starport international)


Abbildung 14: GSM-Jammer OMS-105T
(Quelle: Omnis)

wie auch eine Basisstation des Mobilfunknetzes, Statusanfragen, die durch eingeschaltete Endgeräte auch im Stand-By Modus beantwortet werden. Solche Detektoren sind in Deutschland, wie auch aktive Störsender, nicht zulässig. Einzig die Nutzung passiver Detektoren, die Endgeräte mit einer aktiven Verbindung aufspüren können, können auch im privatwirtschaftlichen Umfeld eingesetzt werden. Sie bieten damit Schutz vor aktivem Abhören durch eine stehende Sprachverbindung oder der Übertragung von Daten aus dem Unternehmen heraus. Allerdings können sie keine Endgeräte detektieren, die eingeschaltet sind und eventuell ein vertrauliches Gespräch aufzeichnen, um diese zu einem späteren Zeitpunkt zu übertragen.

**Klare Richtlinien**

Ob die Absicherung von geschützten Bereichen, die Konfiguration und das Management der Endgeräte oder die Auswahl der genutzten Netze und Dienste - Unternehmen, Organisationen und Behörden müssen gleichermaßen klare Richtlinien für den Umgang mit mobilen Kommunikationsmitteln schaffen. Diese Richtlinien müssen dem technischen Stand bei Einführung entsprechen und die Sicherheitserfordernisse der verwendeten Dokumente in den verschiedenen Nutzergruppen widerspiegeln. Hierzu sollte auf einer bestehenden Klassifizierung unternehmensinterner Dokumente aufgesetzt werden. Anhand der Nutzergruppen und ihrer Aufgabengebiete lassen sich dann Anforderungen an Netze, Endgeräte und Software definieren und die notwendige Infrastruktur aufbauen. Analog sollten diese Richtlinien auf bestehende Mobilfunklösungen angewendet und diese einer Revision unter Sicherheitsaspekten unterzogen werden.

Aufgrund der rasanten technischen Entwicklung und nutzergetriebener Innovation in diesem Sektor fällt es schwer, diese Richtlinien immer dem aktuellen technischen Stand von Netzen und Endgeräten anzupassen. Umso wichtiger wäre es, die Mitarbeiterschaft davon zu überzeugen, dass Sicherheitskonzepte nur durch ihr aktives Zutun wirksam werden können. Jenseits aller technischen Schutzmaßnahmen ist es immer noch der Mensch, der täglich mit dieser Technik arbeitet. Problembewusstsein und ein adäquates Basiswissen zum Umgang mit sensiblen Daten sind daher ebenso wichtig wie technische Maßnahmen. Die Praxis sieht leider meist anders aus. Vorsorge dieser Art ist auf Dauer jedoch immer preiswerter, als das Risiko von unkontrolliert versickernden Informationsströmen.

**Quellen & Literaturhinweise**


Broschüre „Öffentliche Mobilfunknetze und ihre Sicherheitsaspekte“, Bundesamt für Sicherheit in der Informationstechnik, http://www.bsi.de/literat/doc/oefms/index.htm (zuletzt überprüft: 22.09.2008)

Maßnahmenkatalog Organisation, M2.188 „Sicherheitsrichtlinien und Regelungen für die Mobilfunknutzung“, Bundesamt für Sicherheit in der Informationstechnik, http://www.bsi.bund.de/gshb/deutsch/m/m02188.htm (zuletzt überprüft: 15.10.2008)

Report „VPN-Technologien: Alternativen und Bausteine einer erfolgreichen Lösung“, ComConsult-Research / ComConsult Technologie-Information GmbH, http://www.comconsult-research.de/de/vpn_r.htm (zuletzt überprüft: 15.10.2008)

Artikel „Passwörter und PINs auf dem Handy sicher speichern“, Bernd Reder, www.networkcomputing.de / CMP-WEKA Verlag GmbH & Co. KG, http://www.networkcomputing.de/passwoerter-und-pins-auf-dem-handy-sicher-speichern/ (zuletzt überprüft: 15.10.2008)

Artikel „Wie man Spitzel austrickst“, www.stern.de / stern.de GmbH, http://www.stern.de/computer-technik/telefon/:Kryptografie-Wie-Spitzel/631568.html (zuletzt überprüft: 15.10.2008)

Artikel „Verschlüsselte Mobiltelefonie“, www.compliancemagazin.de / PMK Presse, Messe & Kongresse Verlags GmbH, http://www.compliancemagazin.de/produkte/verschluesselung/rohdeschwarz230307.html (zuletzt überprüft: 15.10.2008)

ComConsult Veranstaltungskalender

# Aktuelle Veranstaltungen

### IP-Wissen für TK-Mitarbeiter: was Sie für IP-Telefonie über IP wissen müssen, 02.02. - 03.02.09 in Bonn

Dieses Seminar vermittelt kompakt und effizient das IP-Wissen, das TK-Mitarbeiter ohne Vorkenntnisse zur Planung und zum Betrieb von IP-basierten Telefonie-Lösungen benötigen.

Preis: € 1.390,- zzgl. MwSt.

### Trouble Shooting in vernetzten Infrastrukturen, 03.02. - 06.02.09 in Aachen

Dieses Seminar vermittelt, welche Methoden und Werkzeuge die Basis für eine erfolgreiche Fehlersuche sind. Es zeigt typische Fehler, erklärt deren Erscheinungsformen im laufenden Betrieb und trainiert ihre systematische Diagnose und die zielgerichtete Beseitigung. Dabei wird das für eine erfolgreiche Analyse erforderliche Hintergrundwissen vermittelt und mit praktischen Übungen und Fallbeispielen in einem Trainings-Netzwerk kombiniert. Die Teilnehmer werden durch dieses kombinierte Training in die Lage versetzt, das Gelernte sofort in der Praxis umzusetzen. Als Protokoll-Analysator-Software kommt Wireshark zum Einsatz. Preis: € 2.190,- zzgl. MwSt.

### Sicherheitsmechanismen für Voice over IP, 09.02. - 10.02.09 in Hamburg

Angesichts der Offenheit und geringeren Verfügbarkeit von Datennetzen ist das Thema Sicherheit das zentrale Projektthema bei der Umsetzung von Voice over IP. VoIP benötigt Sicherheitsmechanismen, die mindestens ein den konventionellen Telekommunikationsnetzen entsprechendes Niveau an Vertraulichkeit, Verlässlichkeit, Verfügbarkeit und Integrität sicherstellen. Darüber hinaus bietet die Umstellung die Chance, die Sicherheit der Sprachkommunikation über das bisherige Niveau hinaus zu verbessern.

Preis: € 1.390,- zzgl. MwSt.

### Sicherheit 1: Grundlagen und Kernbausteine zur erfolgreichen IT-Sicherheit, 09.02. - 13.02.09 in Hamburg

Bedrohungen der IT-Sicherheit bestehen für praktisch alle Elemente einer vernetzten IT-Infrastruktur. Die Quelle der Bedrohung kann sowohl von außen auf das Netz wirken als auch von innen stammen. Sicherheit entsteht erst, wenn alle signifikanten Gefahrenbereiche systematisch verriegelt werden. Dieses Seminar identifiziert die wesentlichen Gefahrenbereiche und zeigt effiziente und wirtschaftliche Maßnahmen zur Umsetzung einer erfolgreichen Lösung auf. Dabei wird jeder einzelne Baustein detailliert erklärt und anhand typischer Einsatzszenarien wird der Weg zu einer erfolgreichen Sicherheits-Lösung aufgezeigt. Preis: € 2.290,- zzgl. MwSt.

### Internetworking: Optimales Netzwerkdesign mit Switching und Routing, 09.02. - 13.02.09 in Aachen

Dieses 5-Tages-Intensiv-Seminar vermittelt Netzwerkbetreibern und Planern Methoden und Technologien zur erfolgreichen Strukturierung von Enterprise Netzwerken. Dabei wird das komplette Spektrum vom L2/L3 Switching über Redundanz/Routing bis hin zu Themen wie VLAN, WLAN-Integration, Multicast-Routing, VPN, MPLS, abgedeckt. Es werden sowohl die theoretischen Hintergrundkenntnisse als auch die Konsequenzen für den praktischen Betrieb von Netzwerken dargestellt. Preis: € 2.290,- zzgl. MwSt.

### TCP/IP und SNMP, 16.02. - 20.02.09 in Bonn

LAN-, WLAN- und WAN-Netzwerke sind heutzutage IP-Netze, und ein Verzicht auf Nutzung des IP-basierten Internet undenkbar. Auch für früher nur mit herstellerspezifischen Protokollen in Verbindung gebrachte Anwendungsgebiete wie Telefonie oder Produktionsumgebungen gibt es mittlerweile geeignete IP-basierte Lösungen. Hersteller und Dienstanbieter versuchen den Eindruck zu vermitteln, die Nutzung sei kinderleicht, fast schon plug and play - man trägt ein paar Adressen ein (wenn überhaupt), und es kann losgehen. Falsch!

Preis: € 2.290,- zzgl. MwSt.

### Sicherheit im LAN mit IEEE 802.1X, 16.02. - 17.02.09 in Bonn

Dieses 2-tägige Seminar vermittelt den optimalen Umgang mit IEEE 802.1X, erläutert die Einsatzvarianten, beschreibt die gegebenen Fallstricke und liefert die ideale Basis zur Vorbereitung eines Einsatzes.

Preis: € 1.390,- zzgl. MwSt.

### IP-Telefonie: Vorbereitung, Migration, Management, 16.02. - 18.02.09 in Bonn

Die Vorbereitung der Netze auf IP-Telefonie, die Migration von der klassischen Telekommunikation zu Voice over IP sowie der Betrieb der dadurch entstehenden komplexen Netz- und Anwendungsarchitektur konfrontieren alle Unternehmen mit neuen Herausforderungen. Das Wissen aus verschiedenen Bereichen, von der Netzinfrastruktur bis hin zu neuen und etablierten Kommunikationsapplikationen, muss zu einem interdisziplinären Know-how verdichtet und neu geordnet werden. Diesem Ziel dient das Seminar.

Preis: € 1.690,- zzgl. MwSt.

### Projekt-Erfahrungsbericht: Cisco CallManager Rollout und Migration CUCM Version 6, 02.03. - 03.03.09 in Aachen

Dieses 2-tägige Seminar beschreibt Planung, Installation und den Betrieb einer großen verteilten IP-Telefonie-Lösung auf der Basis des Cisco CallManagers. Es macht deutlich, in welchem Umfang die Standard-Installation angepasst und erweitert werden musste, um den Anforderungen der Teilnehmer zu entsprechen. Auch die Umstellung traditioneller Betriebsabläufe im Änderungs-Management und deren Auswirkung auf die Konfiguration des CallManagers wird beschrieben. In diesem Zusammenhang werden insbesondere auf die Akzeptanz der Benutzer und die damit notwendigen Änderungen in der Bedienung der Telefone eingegangen.

Preis: € 1.390,- zzgl. MwSt.

Zertifizierungen

## ComConsult Certified Network Engineer

**Lokale Netze**
26.01. - 30.01.09 in Aachen
11.05. - 15.05.09 in Aachen
31.08. - 04.09.09 in Frankfurt
23.11. - 27.11.09 in Hamburg

**TCP/IP und SNMP**
16.02. - 20.02.09 in Bonn
25.05. - 29.05.09 in Aachen
21.09. - 25.09.09 in Bonn

**Internetworking**
09.02. - 13.02.09 in Aachen
11.05. - 15.05.09 in Aachen
05.10. - 09.10.09 in Frankfurt

Paketpreis für alle drei Seminare € 6.183,-- zzgl. MwSt. (Einzelpreise: je € 2.290.--)

## ComConsult Certified Trouble Shooter

**Trouble Shooting 1**
03.02. - 06.02.09 in Aachen
05.05. - 08.05.09 in Aachen
06.10. - 09.10.09 in Aachen

**Trouble Shooting 2**
17.03. - 20.03.09 in Aachen
16.06. - 19.06.09 in Aachen
03.11. - 06.11.09 in Aachen

Paketpreis für beide Seminare, eine digitale Stromzange, die Prüfung und den Report „Fehlersuche in konvergenten Netzen“ € 3.940.-- zzgl. MwSt. (Einzelpreise: je € 2.190.--)

## ComConsult Certified Security Expert

**Sicherheit 1: Grundlagen und Kernbausteine zur erfolgreichen IT-Sicherheit**
09.02. - 13.02.09 in Hamburg
14.09. - 18.09.09 in Köln

**Sicherheit 2: Erarbeitung und Umsetzung von Sicherheitskonzepten**
30.03. - 03.04.09 in Berlin
26.10. - 30.10.09 in Aachen

**Sicherheit 3: Praxis-Intensiv-Seminar zur erfolgreichen Konfiguration von Firewalls, VPNs, Windows Clients und WLANs**
22.06. - 26.06.09 in Aachen
23.11. - 27.11.09 in Aachen

Paketpreis für alle drei Seminare und die beiden Reports „VPN-Technologien: Alternativen und Bausteine einer erfolgreichen Lösung“ und „Sicherheit in Wireless LANs“. € 6.183.-- zzgl. MwSt. (Einzelpreise: je € 2.290.--)

## ComConsult Certified Voice Engineer

**Basis-Seminar: Session Initiation Protocol-Basis-Technologie der IP-Telefonie**
30.03. - 01.04.09 in Berlin
15.06. - 17.06.09 in Stuttgart
28.09. - 30.09.09 in Bad Neuenahr
23.11. - 25.11.09 in Hamburg

**Basis-Seminar: Sicherheitsmechanismen für Voice over IP**
09.02. - 10.02.09 in Hamburg
14.05. - 15.05.09 in Bonn
05.10. - 06.10.09 in Frankfurt

**Alternative 1: IP-Telefonie evaluieren, planen, betreiben**
02.03. - 04.03.09 in Stuttgart
25.05. - 27.05.09 in Hamburg
14.09. - 16.09.09 in Köln
02.11. - 04.11.09 in Frankfurt

**Alternative 2: IP-Telefonie: Vorbereitung, Migration, Management**
16.02. - 18.02.09 in Bonn
15.06. - 17.06.09 in Stuttgart
26.10. - 28.10.09 in Berlin

**Optionales Einsteiger-Seminar: IP-Wissen für TK-Mitarbeiter**
02.02. - 03.02.09 in Bonn
04.05. - 05.05.09 in Königswinter
07.09. - 08.09.09 in Aachen
09.11. - 10.11.09 in Königswinter

Basis-Paket Alternative 1: Beinhaltet die zwei Basis-Seminare und Seminar „Alternative 1“ Grundpreis: € 4.250,-- zzgl. MwSt. statt € 4.770,-- zzgl. MwSt.

Basis-Paket Alternative 2: Beinhaltet die zwei Basis-Seminare und Seminar „Alternative 2“ Grundpreis: € 4.250,-- zzgl. MwSt. statt € 4.770,-- zzgl. MwSt.

Optionales Einsteigerseminar: Aufpreis € 990,-- zzgl. MwSt. statt € 1.390,-- zzgl. MwSt.

Impressum

Verlag:
ComConsult Technology Information Ltd.
ComConsult Research
64 Johns Rd
Christchurch 8051
GST Number 84-302-181
Registration number 1260709
German Hotline 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