

Schwerpunktthema

## Entwicklung von Anwendungen, Verkehrslasten und neuen drahtlosen Übertragungssystemen

in den nächsten Jahren und Konsequenzen für unterstützende Infrastrukturen

von Dr. Franz-Joachim Kauffels

Wir haben in den letzten Monaten viel über drahtlose Übertragungssysteme (WLAN, Mikrozelle, Mobilfunk) diskutiert, weil ja aktuell viele Neuheiten anstehen. Dabei ist die Frage ein wenig unter die Räder gekommen, welche Anforderungen an die Infrastrukturen gestellt werden müssen, die die neuen Systeme im Rahmen der Implementierung flächendeckender Versorgungsstrukturen in privaten Netzen bei Unternehmen und Organisationen unterstützen sollen. „Wireless“ heißt nicht unbedingt „weniger Kabel“, ganz im Gegenteil. In 2015 kamen neue Standards und Produkte für 2,5 und 5 GbE zur Unterstützung der neuen 802.11ac Wave2 Access Points auf. Der



vordringliche Charme dieser Lösungen ist, dass man mit ihnen auch alte Cat.5 und Cat.6 Verkabelungen für die WLAN Switching-Infrastruktur nutzen kann.

Blickt man aber etwas über den Teller-Rand auf Systeme, die zwar nach 11ac, aber noch innerhalb des üblichen Planungszeitraums von 5-10 Jahren für Verkabelungssysteme kommen werden, sieht man schnell, dass hier auch 2,5 und 5 GbE kläglich versagen werden, es muss schon mindestens eine 10 Gigabit-Infrastruktur sein.

weiter auf Seite 5

Zweitthema

## Redesign von WAN- und Internet-Zugängen

von Dr. Behrooz Moayeri

Jahrelang wurden WAN- und Internet-Zugänge vieler Unternehmen weitgehend unabhängig voneinander geplant.

Das private Wide Area Network (WAN) dient per definitionem der Übertragung

von Daten im Rahmen unternehmensinterner Applikationen. Unternehmen nutzen dagegen das Internet, um mit anderen Unternehmen, Kunden, Zulieferern und in einem Wort dem Rest der Welt zu kommunizieren. Auf den ersten Blick handelt es

sich also um zwei verschiedene Einsatzgebiete. Die unabhängige Planung des WAN und der Internet-Zugänge schien daher einleuchtend. Jetzt ändert sich dies.

weiter auf Seite 18

Geleit

## NFV und SD-WAN: auf dem Weg zu einem mehr dynamischen Netzwerk-Design

auf Seite 2

Standpunkt

## Schwachstellenmanagement:

Eine Kunst, die Cyber-Kriminelle perfekt beherrschen, die IT jedoch anscheinend oft nicht

auf Seite 16

5 Tage Intensiv-Update

**ComConsult  
Sommerschule 2016**

auf Seite 3

Neue Sonderveranstaltung

**Wireless und Mobility**

auf Seite 15

Aktuelles Seminar

## IT-Kommunikation im Umfeld von Fertigung und Automation

auf Seite 17

Zum Geleit

# NFV und SD-WAN: auf dem Weg zu einem mehr dynamischen Netzwerk-Design

Was ist eigentlich ein WAN? So einfach die Basis-Definition der Vergangenheit ist, die die Laufzeit einer Verbindung in den Vordergrund stellt, so komplex ist die Realität, die wir momentan sehen und die uns in den nächsten Jahren bevorsteht. Dabei kommen mehrere Faktoren zusammen:

- die Suche nach einer optimalen Wirtschaftlichkeit
- die Notwendigkeit des Zugangs zu externen Ressourcen
- der Wunsch nach einer einfachen Konfiguration
- die Angst vor einem Verlust von Kontrolle und Sicherheit
- die schwere Kalkulierbarkeit der zukünftigen Kapazitäten

Die Kombination aus Wirtschaftlichkeit und der Notwendigkeit des Zugangs zu externen Ressourcen lässt das traditionelle WAN mit Internet-Verbindungen zusammenwachsen. Damit sind diverse Probleme verbunden, die in dem Artikel von Dr. Moayeri diskutiert werden und die wir auch zu einem der Schwerpunkte der ComConsult Sommerschule gemacht haben. Im Kern entsteht das Problem der effizienten Steuerung von Verkehrsströmen zwischen Standorten und hin zum Internet. Ein zentrales Gateway als Internet-Zugang wird dabei in einer zunehmenden Menge von Fällen als ungeeignet angesehen werden müssen. Dezentrale Zugänge erhöhen aber die Komplexität und erfordern geeignete Sicherheits-Lösungen.

Kombiniert man diese Situation mit einem erhöhten Bedarf nach Skalierbarkeit, der gerade und speziell aus dem Zugang zu Cloud-Ressourcen entsteht, dann wird Software Defined WAN in Kombination mit Network Function Virtualization zu einer der wichtigen Zukunftstechnologien in diesem Bereich. Speziell an NFV führt in Zukunft kein Weg vorbei. Die Nutzung virtueller Maschinen anstelle von spezialisierten Hardware-Kisten ist nicht nur die Basis für eine einfachere Skalierbarkeit, sie ist auch Ortsneutral und kann ohne Probleme mit Netzwerk-Architekturen in der Cloud kombiniert werden. Damit wird auch die Einbindung Sicherheits-spezifischer Cloud-Ressourcen ohne Probleme möglich.

Dieser Weg in Richtung NFV und SD-WAN ist unvermeidbar und wird in den nächsten 5 Jahren je nach Unternehmensgröße ohne Zweifel erfolgen. Die Herausforde-



rung besteht nun darin, eine offene Lösung zu erreichen. Schon bei dem normalen SDN können wir sehen wie die großen Hersteller relativ erfolgreiche offene Lösungen blockieren. Dies muss gerade in offenen Internet-Architekturen verhindert werden oder wir verlieren den Vorteil einer freien Architektur-Gestaltung mit Einbeziehung externer Ressourcen. Unter diesem Blickwinkel sind die aktuell laufenden Normierungs-Bestrebungen in diesem Bereich von erheblicher Bedeutung. Hier geht es nicht um die Vermeidung von Hersteller-Bindung wie man vielleicht auf den ersten Blick meinen mag. Unser zukünftiges WAN wird ein Gebilde sein, das Cloud-Ressourcen der verschiedensten Art und der verschiedensten Anbieter integrieren muss. Dies wird nur über eine offene Lösung gehen. Auch die gesamte Skalierbarkeit wird deutlich von der Offenheit bestimmt werden.

Diese gesamte Entwicklung ist dabei gleichzeitig mit dem schon mehrfach an dieser Stelle diskutierten Wandel des Berufs des Netzwerk-Ingenieurs verbunden. In Zukunft wird es weniger um die Fähigkeit gehen, die Produkte eines oder mehrerer Hersteller auf CLI-Ebene konfigurieren zu können (dies wird natürlich weiterhin erforderlich sein, auch wenn wir in den nächsten Jahren mehr Automatismen in Form eines über dem CLI liegenden Steuerungs-Layers und einer eher regelbasierten Konfiguration erleben werden). Der zumindest teilweise erfolgreiche Einzug von SDN und die Notwendigkeit von der Virtualisierung des WAN mit NFV wird eine eher programmatische Steuerung der Ressourcen erfordern. Dies ist keine Bedrohung des Berufs des Netzwerk-Ingenieurs, da dies ein schon seit

längerem zu beobachtender Trend ist, den die meisten Administratoren auch erfolgreich bestreiten. Trotzdem macht diese Entwicklung klar, dass ein Netzwerk-Admin in 5 oder 10 Jahren völlig anders arbeiten wird als heute. Ressourcen werden eben dynamischer als bisher sein und die optimale Kontrolle und Steuerung dieser dynamischen Ressourcen wird im Vordergrund stehen.

Ist das klassische Netzwerk-Design tot? Im Gegenteil. Aus unserer Sicht muss gerade im LAN eine Rückbesinnung zu einem einfachen und offenen Design ohne Hersteller-Bindung erfolgen. Die aktuellen Angebote der führenden Hersteller sind einfach nicht handhabbar. Sie sind zu komplex und zu speziell. Und tatsächlich gibt es ja offene und leistungsfähige Lösungen. Die großen Cloud-Rechenzentren machen es uns ja vor (auch wenn sie eine einfachere beziehungsweise andere Aufgabe in Form einer massenhaften Skalierung identischer Basis-Bausteine haben). Wir diskutieren diese Design-Herausforderung auf der Sommerschule und legen dabei alle beteiligten Technologien auf den Prüfstand. NFV, SDN, Layer-2, Layer-3 und Layer-4 werden von unseren Experten diskutiert und der aktuelle Stand und die Roadmap der nächsten Jahre vorgestellt.

Ihr  
Dr. Jürgen Suppan

## Intensiv-Seminar

**Sommerschule 2016 -**

**Intensiv-Update  
auf den neuesten  
Stand der Netzwerk-  
technik**

**27.06. - 01.07.16  
in Aachen**



Buchen Sie über unsere Web-Seite

[www.comconsult-akademie.de](http://www.comconsult-akademie.de)

Intensiv-Update auf den neuesten Stand der Netzwerktechnik

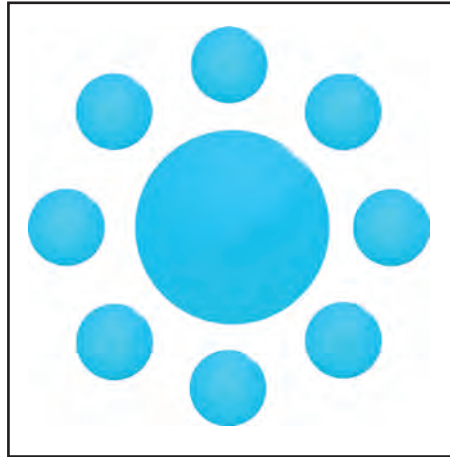
# ComConsult Sommerschule 2016

## 27.06. - 01.07.16 in Aachen

Die ComConsult Akademie veranstaltet vom 27.06. bis 01.07.16 ihre "ComConsult Sommerschule 2016" in Aachen.

Die Sommerschule 2016 bringt Sie in 5 Intensiv-Tagen auf den letzten Stand der Netzwerk-, Kommunikations- und Infrastruktur-Technik. Wir analysieren für Sie:

- Wie verändern sich IT-Architekturen und welche Anforderungen generiert das auf Infrastrukturen, welche neuen Anforderungen entstehen speziell im Rechenzentrum?
- Was passiert auf der WAN-Seite, wie sieht eine Zukunfts-orientierte WAN-Lösung aus?
- Wie sieht die Zukunft des LAN aus? Welche der neuen Technologien werden sich durchsetzen? Wie können skalierbare und sichere LAN-Infrastrukturen geschaffen werden?



- Unified Communications, das Ende von ISDN: wie sieht die Kommunikations-Lösung der Zukunft aus? Was bedeutet das für Infrastrukturen?

- WLAN-Technik erreicht immer neue Leistungsklassen: aber wie sieht die Zukunft aus? Wo ist die Abgrenzung zum Mobilfunk?

- IPv6 ist Realität: wie sieht eine erfolgreiche Migration aus? Welche Projekterfahrungen können helfen?

- Sicherheit wird immer mehr zum Schlüssel für erfolgreiche IT-Infrastrukturen: Cloud-Computing und mobile Endgeräte, wie passt das in ein Sicherheits-Konzept?

Top Experten der Branche gestalten das Programm dieser Intensiv-Schulung und bringen systematisch die Erfahrungen laufender Projekte und neuester Technologie-Entwicklungen in diesen Kurs ein. Treffen Sie einige der besten Experten, die die deutsche Netzwerk-Landschaft zu bieten hat.

## Frühbucherphase bis zum 31.05.2016

Fax-Anmeldung an ComConsult 02408/955-399

# ComConsult Sommerschule 2016


Ich buche das Seminar

**ComConsult Sommerschule 2016**

- 27.06.-01.07.16 in Aachen  
zum Preis von € 2.290,-\*

\*Frühbucherpreis bis zum 31.05.2016  
Dann regulär € 2.490,-

- Bitte buchen Sie mir ein Hotelzimmer

 Buchen Sie über unsere Web-Seite  
[www.comconsult-akademie.de](http://www.comconsult-akademie.de)

Vorname

Nachname

Firma

Telefon/Fax

Straße

PLZ, Ort

eMail

Unterschrift

## Programmübersicht Sommerschule 2016

### Montag, der 27.06.16 - IT-Architekturen und Auswirkungen auf Infrastrukturen

#### Architekturen

IT-Architekturen sind geprägt von Endgeräten, die lokale Anwendungen ausführen und auf Applikationen auf Server zugreifen. Im Moment ändert sich hier alles. Unser Verständnis von Endgerät, Betriebssystem und Server muss auf den Prüfstand. Ohne Zweifel wird unsere IT-Landschaft in fünf Jahren dramatisch anders aussehen als heute. Und Netzwerke haben die zentrale, tragende Rolle für diese Entwicklung. Wir analysieren wo es hinget und wie Netzwerke aussehen müssen, um diesen Weg zu unterstützen.

#### 10:00 - 12:30 Uhr

Wir analysieren für Sie:

- Wie ändert sich IT und welche Auswirkungen hat das auf Infrastrukturen?
- Was passiert auf der Netzwerk-Seite, um diesen

Anforderungen zu entsprechen?

- Welche neuen Technologien müssen speziell bei den Planungen für die nächsten Jahre beachtet werden?

*Dr. Franz-Joachim Kauffels, Technologie-Analyst*

#### 14:00 - 17:00 Uhr

**Rechenzentren: neue Arten von Infrastrukturen gefragt**  
Rechenzentren sind unter Druck:

- Die Cloud puscht das Thema Wirtschaftlichkeit, Kosten und Transparenz
- Mobile Endgeräte erfordern mindestens eine Private Cloud Infrastruktur und einen Übergang zu Benutzer-zentrischen Lösungen
- Server- und Speicher-Konsolidierung gehen permanent weiter, hoch-skalierende Infrastrukturen sind gefordert

- Virtualisierung geht in die nächste Runde und öffnet die Tür zu automatischen Lastausgleichen und Provisionierungen mit erheblichen Anforderungen an Infrastrukturen

Wir analysieren für Sie:

Strategien für das Rechenzentrum der Zukunft:

- Software-Defined Data Networks SDN
- Cloud Computing

*Dipl.-Math. Cornelius Höchel-Winter,  
ComConsult Research GmbH*

#### 11:00 - 11:15 Uhr Kaffeepause

#### 12:30 - 14:00 Uhr Mittagspause

#### 15:00 - 15:15 Uhr Kaffeepause

#### ab 19:00 Uhr Happy Hour

### Dienstag, der 28.06.16 - Netzwerk-Technologien: aktuelle Entwicklungen

#### 9:00 - 10:30 Uhr

**Das Internet of Things: wo stehen wir?**

Mehr und mehr Produkte drängen in den Markt. Daraus leitet sich die Frage ab, welche Anforderungen an Infrastrukturen hier auf uns zukommen. Dieser Vortrag zeigt wo wir stehen und was auf uns zukommt.

Sie lernen:

- Was ist IoT?
- Anwendungsbereiche und Einsatzszenarien
- Infrastrukturen
- Roadmap

#### 10:45 - 12:30 Uhr

**SDN und NFV in der Analyse**

- Wo steht der Markt?
- Was ist NFV und wo setzen wir es wann ein?
- Welchen Stellenwert hat Hardware in den neuen Technologien?
- Wie hängen SDN und NFV zusammen?

*Dipl.-Inform. Petra Borowka-Gatzweiler, UBN*

#### 14:00 - 17:00 Uhr

**Netzwerk-Design-Lösungen im direkten Vergleich**

Wir haben im Moment wesentliche Design-Entwicklungen, die sich direkt widersprechen. Gleichzeitig sind einige der neuen Ansätze auch sehr komplex. Hier stellt

sich die Frage, wie man mit möglichst wenig Aufwand ein maximal gutes Design erreichen kann.

Wir diskutieren mit Ihnen:

- Layer 3 Design
- Layer 4 Design
- Sonderfälle
- Empfehlungen

*Markus Geller, ComConsult Research GmbH*

#### 10:30 - 10:45 Uhr Kaffeepause

#### 12:30 - 14:00 Uhr Mittagspause

#### 15:00 - 15:15 Uhr Kaffeepause

### Mittwoch, der 29.06.16 - UC, das Ende von ISDN: wie sieht die Kommunikations-Lösung der Zukunft aus?

UC-Projekte haben in den letzten Jahren deutlich an Komplexität gewonnen. Zwar haben sich die Produkte weiter entwickelt, doch gleichzeitig hat sich ein neues Verständnis von Kommunikation mit einer gleichzeitigen Verschiebung der Funktionsbereiche ergeben. Moderne Browser beinhalten heutzutage die komplette Funktionalität eines UC-Clients für Sprache und Video und generieren die Frage nach der Zukunft des Telefons. Gleichzeitig ist ISDN am Ende, es wird 2017 abgeschaltet. Dies erfordert eine Neubestimmung des Verständnisses von Kommunikation: was gehört dazu, wie kommunizieren wir in Zukunft mit Externen?

#### 9:00 - 17:00 Uhr

Wir analysieren für Sie:

- Motivation: Warum All-IP? Einführung in das Thema
- SIP Trunking vs. PSTN: Was sind die wesentlichen Unterschiede?
- Standards für Enterprise- und Provider-Peering
- Session Border Controller: Funktionalität und Markt
- Provider-Marktübersicht: Geschäftsmodelle und Angebote
- Was kommt nach 2018?
- Architektur einer globalen All-IP Kommunikation

*Dipl.-Inform. Petra Borowka-Gatzweiler, UBN*

*Markus Geller, ComConsult Research GmbH*

#### 10:30 - 10:45 Uhr Kaffeepause

#### 12:30 - 14:00 Uhr Mittagspause

#### 15:00 - 15:15 Uhr Kaffeepause

### Donnerstag, der 30.06.16 - WLAN und Mobilfunk

Mit der rasanten Zunahme mobiler Endgeräte bekommt der Zugang dieser Geräte zu den Unternehmens-Infrastrukturen eine zentrale Bedeutung. In Zukunft werden deutlich mehr Endgeräte diesen Zugang wählen als die Kabel-basierte Alternative. Denkt man einen Schritt weiter zum Internet of Everything, dann wird die zukünftige strategische Bedeutung des Zugangs über WLAN und Mobilfunk deutlich. Sowohl die schiere Anzahl der Teilnehmer als auch der damit verbundene Schutz- und Kontrollbedarf machen Änderungen an der Netzwerk-Infrastruktur erforderlich.

#### 9:00 - 16:30 Uhr

In diesem Themenblock lernen Sie:

- Welche Optionen Ihnen das moderne WLAN bietet
- Wie sich Mobilfunk-Alternativen demgegenüber positionieren
- Neue WLAN-Technologien und ihr Einfluss auf Enterprise WLANs

*Dr. Franz-Joachim Kauffels, Technologie-Analyst*

*Dr. Joachim Wetzlar,*

*ComConsult Beratung und Planung GmbH*

#### 10:30 - 10:45 Uhr Kaffeepause

#### 12:30 - 14:00 Uhr Mittagspause

#### 15:00 - 15:15 Uhr Kaffeepause

### Freitag, der 01.07.16 - Sicherheit / WAN und Internet

Sicherheit in der IT wird zum dominierenden Thema der nächsten Jahre. Aber hier geht es nicht um hochfliegende Träume sondern um Informationssicherheit als integraler Bestandteil der IT-Architektur.

#### 9:00 - 12:30 Uhr

Sie lernen in diesem Themenblock:

- Abwehr zielgerichteter Angriffe: Notwendigkeit system- und anwendungsübergreifender Strategien
- Netzbasierte Sicherheit: Praxiserfahrungen aus den Bereichen Verschlüsselung, Zonenkonzepte, NAC und Testumgebungen
- Sicheres Cloud Computing und sicheres Mobile Computing: Möglichkeiten und Grenzen
- Sicherheit und UC: Immer offener und immer sicherer, ist das ein unlösbarer Widerspruch?

*Dr. Simon Hoff,*

*ComConsult Beratung und Planung GmbH*

WAN und Internet wachsen untrennbar zusammen. Es gilt das beste aus den jeweils verfügbaren Lösungen zu nutzen und gleichzeitig mögliche Risiken zu vermeiden. Im Ergebnis geht es um eine schlüssige Weiterverkehrs-Architektur für alle bestehenden Anwendungsbereiche.

#### 14:00 - 15:30 Uhr

Sie lernen in diesem Themenblock:

- Welchen technologischen Trends folgen die WAN Provider (MPLS, OTN, Ethernet, ...)?
- Wie wirkt sich der Cloud-Trend auf die WANs aus?
- Kupfer, Glasfasern oder drahtlos: was sitzt sich als WAN Access durch?
- Welche Folgen haben aktuelle Entwicklungen in den Bereichen Voice und Video für das WAN?
- Welche Anwendungen sind WAN-tauglich, welche nicht?

- Was bedeuten aktuelle WAN Trends für Außenstellenkonzepte von Unternehmen?

*Dr. Behrooz Moayeri,*

*ComConsult Beratung und Planung GmbH*

#### 10:30 - 10:45 Uhr Kaffeepause

#### 13:00 - 14:00 Uhr Mittagspause

#### 15:30 Uhr Ende der Veranstaltung

## Schwerpunktthema

## Entwicklung von Anwendungen, Verkehrslasten und neuen drahtlosen Übertragungssystemen in den nächsten Jahren und Konsequenzen für unterstützende Infrastrukturen



Dr. Franz-Joachim Kauffels ist Technologie- und Industrie-Analyst und Autor. Seit über 30 Jahren unabhängiger, kritischer und oft unbequemer Bestandteil der Netzwerkszene. Verfasser von über 20 Büchern in über 70 Ausgaben sowie über 2000 Artikeln, Videos und Reports.

Fortsetzung von Seite 1

Der Artikel blickt auf die Prognosen hinsichtlich der Entwicklung von Anwendungen und Verkehrslasten und stellt dann alle bekannten mit hoher Wahrscheinlichkeit in naher Zukunft auftretenden Wireless-Systeme kurz vor und beleuchtet sie hinsichtlich der Frage nach ihrem Grundbedarf. Dies geschieht auch im Hinblick auf eine sehr zügige Einführung von 5G-Mobilfunk.

Die allgemeine Diskussion über Wireless Systeme, sei es im Sinne klassischer WLANs oder auch als Systeme für Arbeitsplatzzellen wie 802.11ad sowie die Beobachtung der Weiterentwicklung von LTE betrachtet primär die den Endgeräten unmittelbar zugewandten Radio-Systeme. Die zur sinnfälligen Versorgung dieser Radio-Systeme in Form von Access Points notwendigen Infrastrukturen werden nur am Rande erwähnt.

Das hat zwei Gründe. Das größte zusammenhängende Netzwerk mit drahtloser Versorgung der Teilnehmer ist natürlich ein Mobilfunknetz. Hier haben sich über die Jahrzehnte sehr viele Standards entwickelt, auf die wir hier kaum eingehen können. Der den mobilen Geräten zugewandte Teil heißt aber immer „Radio Access Network“, kurz RAN. Ein Generationenwechsel findet hauptsächlich genau am RAN statt. So waren der Übergang von 2G-Mobilfunk auf 3G sowie der Übergang von 3G auf LTE hauptsächlich durch diese RANs definiert. In der Welt der Providernetze wird es als selbstverständlich angesehen, einem nach außen gerichteten Netzelement immer genug Leistung zu liefern. Das passiert technisch meist über DWDM-Systeme mit komplexer optischer Übertragung auf Lichtwellenleitern. Diese Systeme haben sich in den vergangenen Jahrzehnten

genau so dramatisch weiterentwickelt wie die WLANs oder Mobilfunk-RANs. Das wurde aber bei Diskussionen um die Entwicklung privat betriebener Netze kaum zur Kenntnis genommen, weil das ja eigentlich nur die Provider betrifft. Zwischen RAN und DWDM-Backbone liegt vor allem eine sehr komplexe Welt aus vielen unterschiedlichen Schnittstellen und Protokollen, die von internationalen Gremien in einem nicht abreißen Prozess definiert werden. Es müssen ja nicht nur sehr unterschiedliche technische Systeme in verschiedenen Generationen unterstützt werden, sondern auch jederzeit eine allumfassende Kompatibilität.

Wir kommen später nochmals darauf zurück, aber die Weiterentwicklung von LTE ist natürlich 5G Mobilfunk. Und das Ziel von 5G ist ganz klar **1 bis 10 Gbps pro mobilem Endgerät!** Es gibt jetzt Leute, die sich zurücklehnen und sagen, dass das ja erst nach 2020 kommt. Denen möchte der Autor entgegenhalten, dass Verizon den Plan hat, bereits 2017 mit entsprechenden Angeboten an den Markt zu gehen. Aktuelle (Frühjahr 2016) Berichte von den ersten Phasen des Versuchsbetriebs sprechen davon, dass die Technik komplett verfügbar sei, lediglich die Standardisierung müsse noch nachziehen. Wenn Verizon anfängt, wird sich AT&T nicht in den Regen stellen und T-Mobile US als neue drittstärkste Kraft wird auch nicht nachstehen wollen.

Technisch gesehen ein Sonderfall, quantitativ aber enorm wichtig sind die Versorgungssysteme für private Haushalte. Auch hier ist ja in den meisten Fällen ein WLAN-basierter Router die Schnittstelle zwischen den Endgeräten und dem Leistungsan-

gebot des Providers. Neben den DSL-Schnittstellen als Weiterentwicklung der Telefontechnik haben sich über die DOCSIS-Protokolle auch sehr leistungsfähige Alternativen mit Koaxialkabeln aus der TV-Verteiltechnik und in geringerem Maße Glasfasersysteme, die in die Haushalte reichen (FTTH), etabliert.

Da wir einmal dabei sind, können wir deren weitere Entwicklung kurz charakterisieren. In Deutschland können die meisten Haushalte heute problemlos Anschlüsse mit 50 Mbps bekommen, was für normales HDTV und einfacherer Ansprüche ausreicht. In 2015 haben Provider auch damit begonnen, 150 und 200 Mbps anzubieten. Das bleibt aber schon jetzt hinter den technischen Möglichkeiten. In den USA statten Provider wie AT&T und Verizon schon die ersten Städte mit Gigabit-Leistung zu übersichtlichen Kosten, ca. 70 US\$ pro Monat pro Anschluss, aus.

In meinem Beitrag im Insider 3/2016 wurde ja ausführlich erläutert, in welcher Weise WLANs und Mobilfunk zusammenwachsen werden. Das wird sich mit 5G noch verstärken.

Also werden sowohl die Versorgungsstrukturen für private Haushalte als auch die Zellen-Technologie für kleine Zellen (Arbeitsplatzzellen, Mikrozellen, Femtozellen ...) bis 2020 auf das 5G-Ziel nachziehen: **1 bis 10 Gbps pro mobilem Endgerät!**

*Damit haben wir im Grunde genommen eine gute Hausnummer für das, was die Infrastruktur mindestens unterstützen können muss, wenn ein privates flächendeckendes drahtloses Netz aufgebaut werden soll.*

## Entwicklung von Anwendungen, Verkehrslasten und neuen drahtlosen Übertragungssystemen ...

In diesem Kapitel betrachten wir zunächst exemplarisch die Entwicklungen bei Anwendungen, Endgeräten und Versorgungsstrukturen.

In einem weiteren Unterkapitel kommen wir zu wichtigen Entwicklungen bei den Technologien für die Versorgungs-Infrastrukturen und diskutieren die Sinnfälligkeit von 2,5 und 5 GbE gegenüber 10 GBASE-T sowie den spannenden Punkt Power over 10GBASE-T.

Im dritten Unterkapitel reihen wir alle in den nächsten Jahren wichtigen Standards für WLANs, Arbeitsplatz- oder Mikro-Zellen sowie LTE-Ableger und beschreiben für jede, welche Anforderungen in den nächsten Jahren beim Einsatz einer Technologie an die unterstützenden Infrastrukturen gestellt werden. Die Entwicklung von 5G gibt wichtige Anhaltspunkte für die zeitliche Anordnung und Bewertung.

### 1. Entwicklungen bei Anwendungen, Endgeräten und Versorgungsstrukturen

Es gibt ein ganzes Heer von Marktforschern, die die zukünftigen Entwicklungen bei Anwendungen, Endgeräten und Versorgungsstrukturen abschätzen. Das ist sehr wichtig für wirklich jeden, der irgendwie mit dieser Thematik befasst ist, vom Provider, der die Aufrüstung seiner Versorgungs-Infrastruktur planen muss, über die Hersteller aller Geräte und Einzelteile in dieser Wertschöpfungskette bis hin zum Rentner, der teilweise von Erträgen aus Technologie-Aktien leben möchte. Natürlich schwankt die Qualität derartiger Prognosen. In den letzten Jahren hatten aber besonders die Prognosen von Cisco eine besonders gute Zielsicherheit, auch wenn man dem Unternehmen natürlich zunächst einmal Eigeninteresse vorhalten möchte. Zur Mobilfunkmesse in Barcelona Beginn 2016 gab es eine Aktualisierung des aus 2015 stammenden Visual Networking Indexes. Der steht jedermann vollständig gratis zur Verfügung, wir diskutieren hier nur einige Aussagen, die speziell zur Thematik dieses Artikels gut passen.

In Abbildung 1 sehen wir, dass das Wachstum des globalen Mobilfunkverkehrs längst noch nicht abschwächt, wie viele denken. Tatsache ist natürlich, dass in hoch industrialisierten Ländern langsam gewisse Sättigungen erreicht werden können, dafür die weniger entwickelten Länder einen immer weiter steigenden Bedarf haben. Natürlich erzeugt man mit jeder wirklichen technischen Verbesserung auch neues Wachstum. Mit LTE sind deutlich mehr Funktionen möglich als mit 3G. Mit 5G werden sich weitere Steigerungen ergeben. Nach wie vor ist das Smartphone das Top-

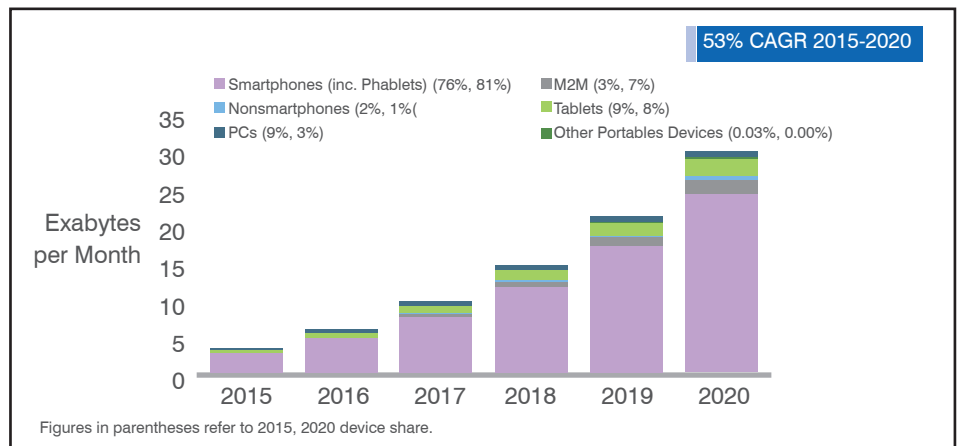


Abbildung 1: Wachstum des globalen Mobilfunkverkehrs nach Gerätetyp

Quelle: Cisco VNI Mobile, 2016

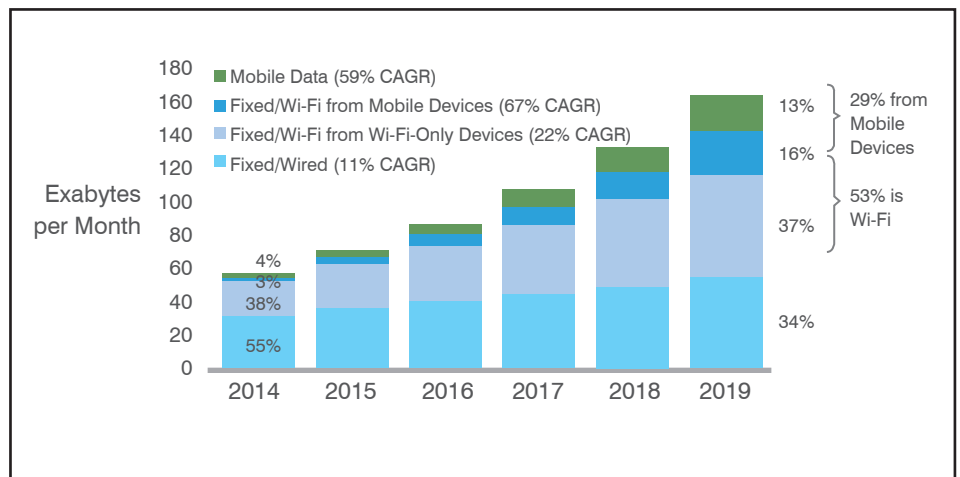


Abbildung 2: IP-Verkehr nach Zugangstechnologie

Quelle: Cisco VNI Mobile, 2016

Gerät. Das bedeutet letztlich eine recht unsymmetrische Auslegung der Funkzellen, die Endgeräte versorgen sollen. Das Endgerät kann nachrichtentechnisch recht wenig und man muss mit einer Reihe von Kompromissen leben, besonders, was die Antennentechnik betrifft.

Für WLANs bedeutet das schlicht und ergreifend, dass die Befindlichkeiten größerer Endgeräte wie Tablets, Notebooks oder PCs nicht wirklich zählen: mit rund 80% Anteil ist das Smartphone der Maßstab aller Dinge bei der Versorgung. Für privat betriebene WLAN-Infrastrukturen ist das eine Kultur-Revolution, denn Zelldichte und Gesamtversorgung müssen auf die kleineren Geräte ausgerichtet werden. Bei diesen gibt es aber ein erschreckendes Spektrum. Der Autor verrät freiwillig, dass er noch ein iPhone 4 verwendet. Wie sagt die nette Oma aus der Telekom-Werbung: „Ihr Handy ist ja älter als meine Schildkröte!“ Von daher sind Technologien wie MU-MIMO, die auch die Einbindung sehr unterschiedlicher Geräte sinnvoll im-

plementieren können, ein absolutes Muss. Die zunehmende Kommunikation zwischen Maschinen im IoT erfordert Sonderwege. Diese können wir hier leider nicht ausdiskutieren, generell geben aber kommende Mobilfunk- und WLAN-Standards entsprechende Hilfsmittel.

Richtig spannend ist auch die Prognose auf Abbildung 2.

Sie zeigt nämlich, welcher Anteil des Gesamtverkehrs auf welchen Strukturen zu erwarten ist. Natürlich gibt es rein mobile Daten, die auch mit 59% pro Jahr wachsen, aber diese Daten, die über eine reinrassige Mobilfunk-Struktur überragen werden, sind in der Minderzahl. Wesentlich wachsen wird der Verkehr auf Basis der im LTE-Artikel beschriebenen Kooperation zwischen Mobilfunk und assoziierten WiFi-Zellen. Das einfachste Beispiel ist hier sicher das Video: der Nutzer „bestellt“ es mit geringer notwendiger Datenrate im Mobilfunksystem und bekommt es via WiFi geliefert. Voraussetzung dazu sind End-

## Entwicklung von Anwendungen, Verkehrslasten und neuen drahtlosen Übertragungssystemen ...

geräte, die WiFi und Mobilfunk-Standards gleichzeitig unterstützen. Wie aus den Ausführungen in Kapitel 4 hervorgeht, werden das mit der Zeit fast alle sein, denn diese Mobil/WiFi-Kombination ist das dominierende Betriebsmodell.

Natürlich wird es weiterhin auch „Fixed WiFi“-Versorgungsstrukturen geben, das sind vor allem die privaten Haushalte. Und der ein oder andere bekommt auch noch Daten über Kabel, das wächst auch noch ein wenig, Primär werden das aber die DSL- und DOCSIS-Home-Router sein, die dann ihrerseits wieder mit WiFi unterverteilen.

Zusammenfassend kann man sagen, dass WiFi die Versorgungsstruktur ist, die die meisten Daten zu bewältigen hat, deutlich über die Hälfte. Und damit sie das kann, muss auch die Infrastruktur entsprechend leistungsfähig ausgelegt werden.

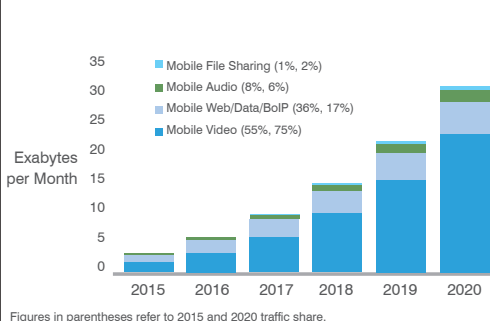
Zu der Entwicklung bei Anwendungen hatten wir in den Insider Artikeln zu Beginn 2016 ja bereits Einiges gesagt. Aus der Perspektive der Belastung der Infrastruktur ist aber ohne Zweifel Video der wichtigste Bereich. (siehe dazu Abbildung 3)

Man sieht sofort, dass Video nicht nur der umfangreichste Bereich ist, sondern alle anderen Verkehrsflüsse zusammen nur gerade einmal ungefähr ein Drittel ausmachen. Das hat die Tendenz, mit der Zeit noch „schlimmer“ zu werden, weil zumindest seit Beginn 2016 die Welle der VR und Augmented Reality läuft, natürlich in 3D und HD, am besten UHD. Niemand wird hier auf Dauer am Kabel hängen wollen, sondern kleine Zellen im Heimbereich oder Arbeitsplatzzellen in Unternehmen sind eine angemessene Versorgungsstruktur. Man kann durchaus prognostizieren, dass in diesen Sektoren auch die 10 Gbps-Schranke gerissen wird und es fröhlich eher auf 30 Gbps Zellenleistung zu geht. Allerdings kann man dieser Entwicklung eher gelassen entgegensehen, in den nächsten 5 Jahren wird das kaum, in den nächsten 5 bis 10 Jahren noch nicht mit beunruhigender Breite passieren.

Es gibt aber durchaus andere, wesentlich näherliegende Anwendungsbereiche, bei denen die 10 Gbps als Versorgung nicht mehr reichen könnten. Auf Präsentationen von IEEE für die Weiterentwicklung der Ultra-Nahbereichs-Kommunikation werden Bilder gezeigt wie in Abbildung 4.

Hier geht es um wirklich praktische Dinge. So könnte man z.B. beim Zugang zu einer U-Bahn oder Magnetschwebbahn „schnell mal“ Musikvideos, eine Zeitung oder einen Film laden, den man während seiner Fahrt z.B. zur Arbeit sehen möch-

Mobiles Video wird 2020 drei Viertel des Mobilverkehrs ausmachen ...



... und mittelfristig nicht bei "normalen" Video-Inhalten stoppen.



- Unterstützung von 3D HD-Video
- Unterstützung aller Bewegungen
- Indoor wenigstens 3-5m

Abbildung 3: Mobiles Video und unmittelbare Weiterentwicklungen

Quelle: links Cisco VNI Mobile 2016, rechts IEEE

te. Das funktioniert auf der Grundlage eines digitalen Kiosk-Konzeptes. Beispielsweise könnte man schon auf dem Weg zum Bahnhof in den Kiosk einloggen und das gewünschte Produkt bestellen, beim Überstreichen des „Kontaktfeldes“ wird nicht nur das gewünschte Produkt geladen, sondern direkt über das gewählte digitale Zahlungssystem (paypal, ApplePay, ...) bezahlt. Im Bild 4 sind ja Beispiele für Ladezeiten angegeben.

Aus der Perspektive des Betreibers einer solchen Struktur ergibt sich der Vorteil, dass der Kunde das Produkt ja schon vorher bestellt hat und dass es nicht in Echtzeit bereitgestellt werden muss, sondern schon geladen werden kann, bevor der Kunde das Kontaktfeld erreicht.

Das Beispiel mit dem Bahnhofszugang ist sehr allgemein und schnell verständlich. Innerhalb von Unternehmen werden sich jedoch viele derartige Anwendungen ergeben. Eine Kontext-sensitive Versorgung ei-

nes Mitarbeiters mit den Daten, die er an der Stelle, wo er sich befindet, zu genau dem Zeitpunkt, wann er dort ist, kann für viele Anwendungen ein sehr großer Vorteil sein.

Ein weiterer wichtiger Bereich ist der Ersatz von Kabeln in der unmittelbaren Umgebung von Endgeräten. Es gibt einfaches Cable Replacement und Docking als wesentliche Varianten. Bei Docking werden wir noch sehen, wie sich das letztlich am Markt entwickelt, vordringlich ist daher die Betrachtung der Ablösung von Kabeln bei gewöhnlichen Standard-Schnittstellen, von denen es ja wirklich genügend gibt.

Die Abbildung 5 zeigt die benötigten maximalen Datenraten für bestimmte wichtige Schnittstellen in einer Übersicht.

Das ist eine Anwendung, die wirklich jeder möchte. Der Anschluss eines größeren, hochauflösenden Bildschirms über irgendwelche Drähte gehört in die Steinzeit.

- Sehr kleine Distanzen zwischen Sender und Empfänger, typisch unter 10 cm
- Sehr hohe Ladegeschwindigkeit, z.B. CD (700 MB) 0,2 s bei 30 Gbps oder HD-Video zwei Stunden (3,6 GB) 0,6 s bei 50 Gbps

Abbildung 4: High Speed Download Services

Quelle: IEEE

## Entwicklung von Anwendungen, Verkehrslasten und neuen drahtlosen Übertragungssystemen ...

Interface	Version	Approx. max. data rate (Gbps)
DisplayPort	1.0-1.1	8.6
	1.2	17.3
HDMI	1.0-1.2a	5
	1.3-1.4a	10.2
	2.0	18
USB	2.0	0.48
	3.0	5
	3.1	10
Thunderbolt	1.0	10
	2.0	20

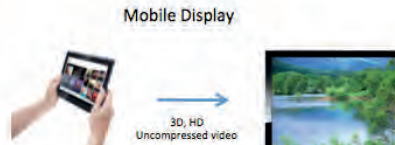


Abbildung 5: Benötigte Leistung für die drahtlose Unterstützung von Standard-Schnittstellen

Quelle: IEEE

Je mehr Smartphones und Tablets hier leisten, desto wichtiger werden derartige drahtlose Schnittstellen. Hier ist es natürlich mit Bluetooth nicht getan.

Was bedeutet das? Nach fester Überzeugung des Autors ist der Standard IEEE 802.11ad / WiGig nur der Anfang einer fulminanten Weiterentwicklung. Interessenten wie AT&T oder Verizon versuchen schon heute, Frequenzbänder im Millimeterwellen-Bereich zu reservieren, weil sie genau wissen, wie entscheidend das für die Zukunft ihrer mit 5G kommunizierenden Mikro- oder Arbeitsplatzzellen ist. Auch hierfür ist bereits ein Standard in Arbeit, nämlich **IEEE 802.11ay**. Mit MIMO und Bündelung von vier Kanälen im 60 GHz-Band soll er in Zukunft bis zu **100 Gbps pro Zelle** erreichen. Nun, das wird noch etwas dauern, es gibt ja noch gar keine Endgeräte, die eine derartige Leistung „verdauen“ könnten, aber die Tendenz ist klar. Innerhalb der nächsten fünf Jahre wird man mit einer Zellenleistung von rund 30 Gbps rechnen können. Für die zugrundeliegenden Versorgungs-Infrastrukturen bedeutet dies aber, dass 10 Gbps mit einer gewissen Zwischenpufferung das absolute Minimum für die Versorgung eines jeden Access Points ist.

Letztlich wird diese Entwicklung nicht innerhalb von Immobilien stehen bleiben, sondern ihrerseits auch wieder mobil werden. Man geht zwar heute meist davon aus, dass jeder ohnehin mindestens ein, wenn nicht mehrere Endgeräte mit sich herumträgt. Es sind aber durchaus auch Anwendungsfälle denkbar, bei denen Fahrzeuge mit einer entsprechenden Technik ausgestattet werden, wenn auch nicht grade so ein alter Bus wie auf der Abbildung 6.

## 2. Wichtige Entwicklungen bei den Versorgungs-Infrastrukturen

Im Laufe der Darstellungen wird klar wer-

den, dass für die sinnfällige Versorgung von Wireless Access Points der nächsten Technologie-Generationen durchgängig eine Datenrate von mindestens 10 Gbps erforderlich ist, also kurzum 10 GBASE-T. Dennoch gibt es aktuell im Schlepptau der Ausbreitung von IEEE 802.11ac eine deutliche Initiative, auf bestehenden Verkabelungen, die die Leistungsmerkmale für 10 GBASE-T nicht erfüllen, dennoch höhere Datenraten als 1 Gbps einzuführen, nämlich 2,5 und 5. Dies ist ein Irrweg, mit dem wir uns aber dennoch auseinandersetzen müssen, was wir in diesem Abschnitt tun.

Eine weitere Frage ist die Implementierung von PoE über 10 GBASE-T. Auch wenn man eine Reihe von Einwänden gegen PoE anführen kann, wie z.B. die generelle Nicht-Eignung von für vergleichsweise hochfrequente Nachrichtenübertragung optimierte Kabel für die

Übertragung von Leistung und die damit verbundenen Verlustleistungsprobleme, ist und bleibt es dennoch eine sehr beliebte Technik, zu der es in vielen Fällen gar keine Alternativen gibt. Die Weiterentwicklung von PoE ist ebenfalls Bestandteil dieses Abschnitts.

### 2.1 Next Generation BASE-T Access

Auch wenn man manchmal den Eindruck hat: die Standardisierungsgremien schlafen nicht immer. Schon im November 2014 bei IEEE 802.3 wurde ein Call for Interest zur Bereitstellung kostenoptimierter Verbindungen in Ethernet Access Netzen mit Datenraten zwischen 1 und 10 Gbit/s unter Nutzung strukturierter UTP-Verkabelungen durchgeführt. Es sollen neue MAC-Datenraten und PHY-Schnittstellen definiert werden, die sich unmittelbar aus der 10 GBASE-T PHY-Technologie ergeben und die Datenraten über installierte strukturierte Verkabelung (z.B. 100 m über Cat 5e oder besser) optimieren.

Sinn ist das Upgrade bestehender Gigabit Ethernet Versorgungsstrukturen, um diese den neuen Bedarfen besser anpassen zu können:

- 1000 BASE-T ist eine extrem erfolgreiche Technik
- Endgeräte wachsen aber in Anzahl und Kapazität schneller, als Verkabelungen aufgerüstet werden können
- Viele Endgeräte nutzen daher auch wegen der Vorzüge der Mobilität zunehmend drahtlosen Zugang nach IEEE 802.11 statt des kabelgebundenen 1000 BASE-T
- Die IEEE 802.11 ac Access Points der nächsten Generation (Second Wave) sind der primäre Bedarfstreiber

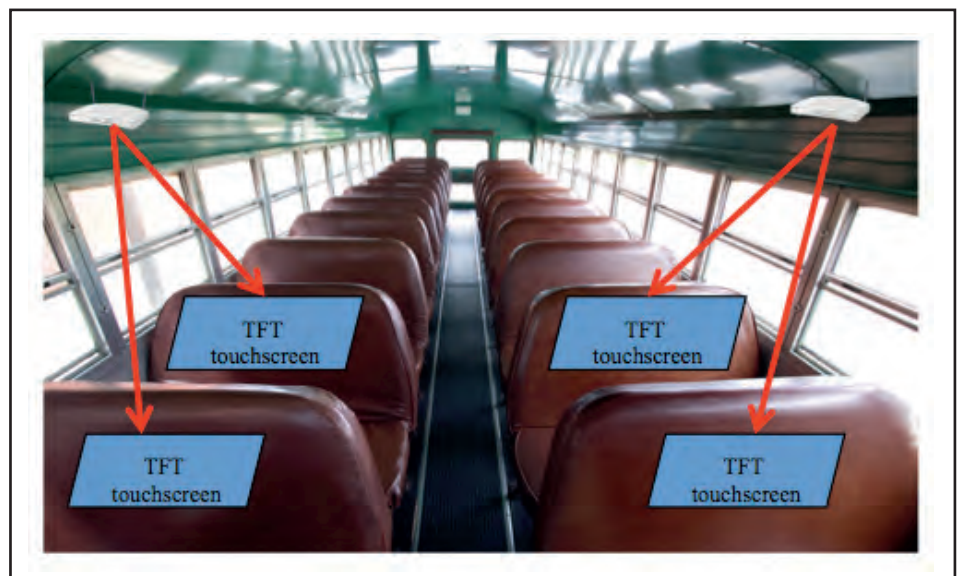


Abbildung 6: InFlight-, Train-, Ship-, Bus-, Car-Entertainment

Quelle: IEEE

---

 Entwicklung von Anwendungen, Verkehrslasten und neuen drahtlosen Übertragungssystemen ...
 

---

Der Standard für WLANs nach IEEE 802.11ac wurde im Dezember 2013 verabschiedet. Das bedeutet aber, dass aktuell noch sehr viele Access Points, die heute für den Enterprise-Markt angeboten werden, nur die Funktionen des „WiFi Certified ac“-Programms haben und sich auf maximal 80 MHz-Kanäle mit Single User MIMO (SU-MIMO) beschränken. Diese „Wave 1“-Produkte haben eine Gesamtleistung, die deutlich unter 1 Gbit/s. pro Zelle liegt, die wir nicht nur in vielen theoretischen Darstellungen beschrieben, sondern auch in praktischen Tests vorliegen haben.

Das wird aber nicht so bleiben, denn die „Wave 2“-Produkte befinden sich bereits in der Auslieferung. Sie werden dann auch je nach Sachlage der Frequenzfreigabe 160 MHz-Kanäle, Multi-User MIMO und bis zu vier Spatial Streams haben. Eigentlich sind nur diese für eine wirkliche Leistungssteigerung verantwortlich, denn die 160 MHz-Kanäle kann man im Rahmen einer flächendeckenden WLAN-Planung nicht brauchen, weil man mindestens drei unterschiedliche Kanäle für ein störungsarmes 2D-Muster benötigt, womit es bei 80 MHz-Kanälen bleibt. Das MU-MIMO ist ein Verfahren, welches es ermöglicht, einen Teil der MIMO-Kanäle nur auf eine einzige Station zu konzentrieren, die damit deutlich mehr individuelle Leistung bekommt, was aber zu Lasten der anderen Stationen geht. Die Leistung einer Zelle wird dadurch also nicht erhöht, sondern nur anders verteilt.

Bei der CFI-Sitzung der IEEE Ende 2014 war man der Ansicht, dass die Wave 2-Produkte bis Ende 2015 zu Leistungsanforderungen im Bereich von 2 GbE für einen AP und 2016 - 2017 zu Anforderungen im Bereich von 4 GbE für einen AP führen werden.

Selbst wenn die Zeitangaben etwas eilig erscheinen, liegt alles dennoch im unmittelbaren Planungshorizont. Klar ist auch:

- 1 GbE ist schon jetzt dauerhaft zu wenig
- Die von Herstellern (z.B. Broadcom) angebotene Möglichkeit der Link-Aggregation z.B. von zwei 1 GbE-Links kann nur eine Notlösung sein, weil sie auf die Dauer nicht nur sehr unpraktisch, sondern auch zu teuer ist
- 10 GbE wird jedoch von 11ac kaum je erreicht werden, stellt höhere Anforderungen an die Verkabelung und die Switches und ist auf den ersten Blick erheblich zu teuer

Als Daumenregel hat man sich darauf verständigt, dass die Anbindung eines APs mindestens 75% der Nominalleistung haben sollte, damit das Access System nicht zum Engpass wird.

**Die bis heute spannende Frage ist, warum IEEE 802.3 mit der Prognose bei 2017 stehen geblieben ist. Wie wir noch sehen werden, war damals schon klar, dass die nach IEEE 802.11ac Wave 2 kommenden WLANs und Systeme für Mikro- oder Arbeitsplatzzellen noch deutlich mehr brauchen werden, nämlich die Anbindung mit 10 GBASE-T. Das klappt aber nicht mehr auf Cat. 5 oder simplen Cat.6-Kabeln!**

Man kann jetzt schon konstatieren, dass 11ac den Markt schneller erobert hat als damals 11n. Wir hatten schon nach 5 Quartalen der Auslieferung von Wave 1-Produkten einen Anteil von 21 % erreicht. Die Wave 2-Produkte werden bei geeigneter Planung den Unternehmen deutlich mehr Leistung bringen können als dies heute mit 11n möglich ist, auch wenn nach wie vor das DCF-Verfahren die Systeme ungünstig beeinflusst und in unnötiger Weise in der Leistungsentfaltung behindert. Noch wichtiger ist, dass die Akzeptanz von 11 ac bei den Endgeräten (Smartphones, Tablets, Notebooks, ...) fast schon als enorm bezeichnet werden kann. Innerhalb eines Zeitraums von weniger als fünf Jahren werden daher alle Endgeräte 11ac unterstützen, viele davon mit mehreren parallelen Spatial Streams.

*Die Gremien haben das zwar versucht elegant zu verbrämen, aber der normale Mensch würde sagen: 2,5 und 5 GbE-Switches sind kastrierte 10 GbE-Switches.*

Es hat sich schnell herausgestellt, dass eine „verlangsamte“ 10 GbE-Schnittstelle die beste technische Lösung ist. Für die 10 GBASE-T-Schnittstelle liegt eine große Menge von Erfahrungen, Berechnungen und Versuchen im Zusammenhang mit aktuellen Kabeltypen vor. Die 10-wertige Codierung (PAM 10) bei 10 GBASE-T führt zu einer besseren Ausnutzung des zur Verfügung stehenden Übertragungsfensters auf dem Kabel. Leitet man die 2,5 GbE von 10 GBASE-T ab, kommt man dank der dichteren Codierung mit einer Bandbreite von 100 MHz aus. Und das macht z.B. einen deutlichen Unterschied bei der Nutzung von Cat 5e-Kabel, das ja bei einer Länge von maximal 100m im Rahmen einer strukturierten Verkabelung bis 100 MHz spezifiziert ist. Ein 5 GbE-System würde auf Basis einer verlangsamten 10 GBASE-T-Schnittstelle eine Bandbreite von 200 MHz benötigen und käme somit durchaus mit normalem Cat.6-Kabel aus. Und es geht ja bei solchen Überlegungen nicht nur um Kabel, sondern auch um Stecker und Patchfelder.

Eine solche Lösung funktioniert für 2,5 Gbps sofort mit allen existierenden 5e, 6

und 6A-Verkabelungen. Für 5 GbE auf dieser Basis können bei schlechteren Kabeln Längenbeschränkungen unter 100m für 5e eintreten. Üblicherweise haben die Hersteller aber Systeme geliefert, die die Spezifikationen der Standards teilweise weit übertroffen haben. Speziell in Deutschland können wir von einer günstigen Situation ausgehen.

Folgende Punkte sind aber mittlerweile in der Diskussion interessant geworden:

- Die Switch-Chips für 10 GbE sind mittlerweile recht preiswert geworden. Der Markt für 2,5 und 5 GbE-Switches ist im Frühjahr 2016 in einer desaströsen Phase. Es wurden kaum Produkte angekündigt und bei einem Billig-Hersteller ist der 2,5/5 GbE-Switch mit der Begründung der Verfügbarkeit von PoE sogar teurer als ein vergleichbarer 10 GbE-Switch. Man kann förmlich greifen, dass die möglichen Kunden nicht wirklich überzeugt sind, obwohl sie solche Switches für die Einführung von 11ac Wave2 WLANs eigentlich dringend brauchen würden.
- Die wesentlichen Kosten liegen nach wie vor in der Verkabelung. Wenn man also die bisher nur für die Anbindung von Endgeräten gedachte Verkabelung weitest gehend für die 11ac Access Points nutzen kann, entstehen zunächst Kostenvorteile. Die Freude daran ist aber nur von kurzer Dauer. Alle Wireless-Technologien jenseits von IEEE 802.11ac Wave2 kommen mit 2,5 oder 5 GbE-Anbindungen auf Dauer nicht aus, wie wir noch sehen werden.
- Energy Efficient Ethernet ist für 1 und 10 GBASE-T verfügbar. Bei modernen Chips ist es eine serienmäßige Funktion, die natürlich auch für abgeleitete Datenraten zur Verfügung steht.
- Ein wichtiger Punkt ist PoE. Erst wenn in breitem Maße Switches mit PoE für 10 GBASE-T verfügbar sind, wird wirklich Bewegung in die Sache kommen.

## 2.2 PoE für 10 GBASE-T

Ein Problem, das schon seit einiger Zeit heftig diskutiert wird, ist die Stromversorgung der Access Points. Bei den heutigen 1 GbE Access Switches ist man die bequeme PoE-Versorgung gewohnt. Für 10 GBASE-T ist aber PoE noch nicht endgültig definiert. Das liegt hauptsächlich daran, dass die Funktion von 10 GBASE-T durch eine Reihe aufeinander gestapelter nachrichtentechnischer Tricks realisiert wird. Ein Kabel, wie z.B. vom Typ 6A, ist nicht wirklich für die Übertragung von Strom-Leistung ausgelegt. Überträgt man dennoch wie

## Entwicklung von Anwendungen, Verkehrslasten und neuen drahtlosen Übertragungssystemen ...

heute üblich Versorgungsstrom auf solchen Leitungen, verändern sich ihre physikalischen Parameter. Sie werden z.B. bis zu 10 Grad wärmer, was durch die hohe Verlustleistung sofort einleuchtet.

Eine Technik für PoE über 10 GBASE-T benötigt eine intelligentere Nutzung der einzelnen Drähte als bisher, z.B. mit PoE über vier statt bisher zwei Paare, siehe dazu Abbildung 7 und 8. Eigentlich sind dafür auch keine wesentlichen Änderungen am Standard notwendig. Schon 2013 zeigte die IEEE 802.3 4-Pair Power over Ethernet Study Group eine Machbarkeitsstudie mit dem Aufbau in Abbildung 7.

Die erste Sitzung der entsprechenden Interessengruppe war im Januar 2015, die Standardisierung liegt bei der Gruppe **IEEE 802.3bt**. Allerdings sollten sie auch nicht trödeln, wonach es aber momentan aussieht Ein Hersteller wie Cisco könnte wegen der bereits komplett bestehenden Technologie im Handumdrehen entsprechende Lösungen für die eigenen Access Points auf den Markt bringen. Es gibt durchaus verschiedene Alternativen für die Implementierung von Po10GBASE-T, z.B. auch eine sehr beliebte aus dem HD-Video-Bereich. Cisco hat schon 2011 eine eigene PoE-Variante mit dem Namen UPOE (Universal Power Over Ethernet) vorgestellt, die bereits seit Jahren 4 Paare nutzt.

Das wäre jetzt keine wirkliche Katastrophe, da ein Betreiber einer flächendeckenden WLAN-Lösung üblicherweise bei einem Hersteller bleibt, aber angesichts der Dynamik der Entwicklung wäre es doch ganz nett, wenn die Standardisierung ausnahmsweise einmal nicht **viel** zu langsam wäre.

Es gibt aber eine Reihe wichtiger Erkenntnisse, die hier nur kurz gestreift werden können. Ein deutliches Problem entsteht, wenn man viele Kabel mit PoE in einem Bündel zusammenführt. Es zeigt sich aber deutlich, dass die jeweils besseren Kabel, wie z.B. Cat. 6A oder Cat. 8 sich bei diesem Problem deutlich besser schlagen als die billigeren Varianten, siehe dazu Abbildung 9 und 10. Allgemein ist eine Erwärmung von mehr als 15 Grad unerwünscht.

### 3. Anforderungen an die unterstützende Verkabelungs-Infrastruktur kommender Systeme für drahtlose Datenübertragung

Ob nun der „wireless Leistungshunger“ in einer Kombination aus Steigerung der Anzahl der mobilen Geräte und der individuell von ihnen verlangten Leistung in flächendeckenden Infrastrukturen in den

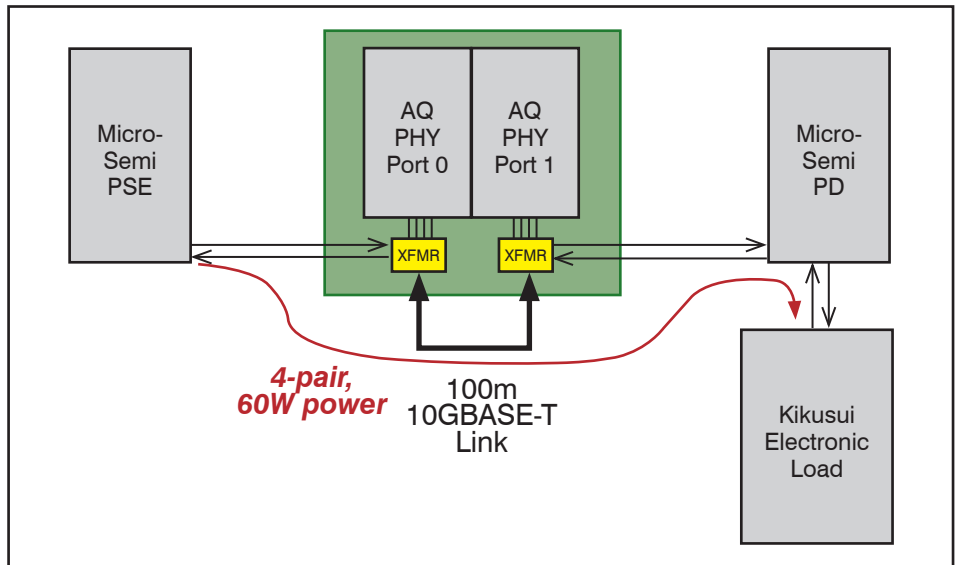


Abbildung 7: 10 GBASE-T PoE über 4 Paare, Machbarkeits-Demonstration

Quelle: IEEE

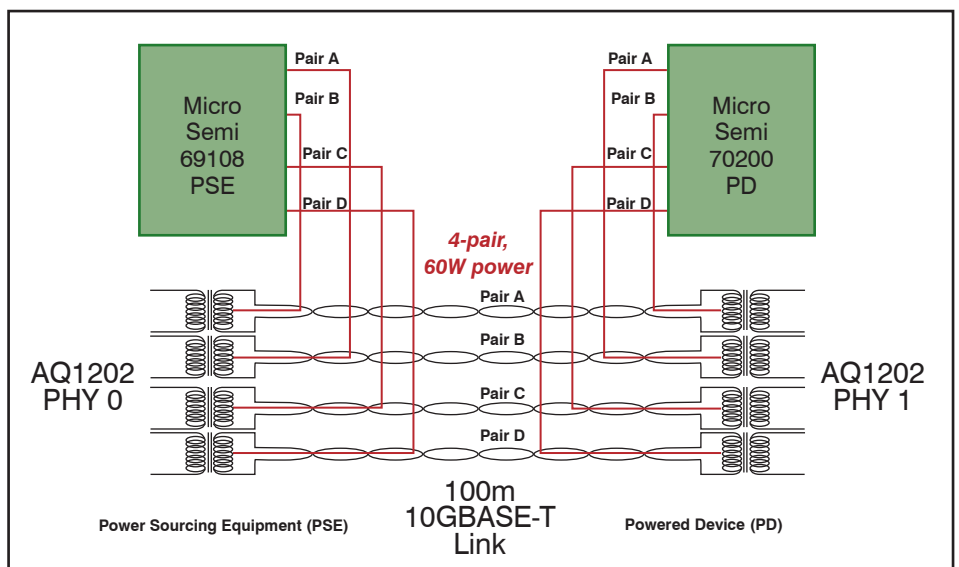


Abbildung 8: 10 GBASE-T PoE über 4 Paare, Systemaufbau

Quelle: IEEE

nächsten Jahren tatsächlich den Faktor 1000 erreicht, wie es nicht nur der Hersteller Qualcomm verkündet, sei dahingestellt. Die ersten Planungen für 5G gehen aber ebenfalls von dieser Dimension aus. Innerhalb privater Netze herrschen jedoch etwas andere Bedingungen, so wird sicher kein Unternehmen Video-Streaming im gleichen Umfang unterstützen müssen wie Provider mit überwiegend privaten Endanwendern. Vielmehr ist zu erwarten, dass Lösungen nach wie vor primär die durch die im Unternehmen vorhandenen „wertschöpfenden“ Prozesse angemessen unterstützen müssen, wobei neue kooperative Anwendungen, wie sie z.B. IBM und Apple entwickeln sowie ein geändertes Verständnis von Unified Communications wesentliche Impulse setzen werden. Aber, da sich ak-

tuell keine am Bedarf professioneller Anwender orientierte Video-Plattform durchsetzen konnte, kann man YouTube wohl vielfach in Zukunft in Unternehmen und Organisationen nicht so einfach sperren wie Netflix.

Um es kurz zu machen: der Bedarf wird massiv wachsen, wie stark genau, hängt vom Einzelfall ab.

Wie können wir die beschriebenen Technologien in diesem Zusammenhang bewerten?

#### 3.1 IEEE 802.11ac

**IEEE 802.11ac** erreicht mit **Wave2** endlich halbwegs professionelles Niveau. Es ist sicherlich die für die meisten privaten Betreiber die erste Wahl. Investitionen

## Entwicklung von Anwendungen, Verkehrslasten und neuen drahtlosen Übertragungssystemen ...

in Wave1 oder gar 11n lohnen sich nicht mehr. Alle wichtigen Hersteller unterstützen diesen Standard. Man wird mehr Zellen benötigen als bei 11n, wenn man eine wirkliche Leistungssteigerung sehen möchte. Die bisher erfahrenen Planer werden auch das bravourös bewältigen. Durch die neuen Ethernet-Standards mit 2,5 und 5 Gbps sollten wir auch rechtzeitig die Geräte für den Aufbau einer Infrastruktur für die Vernetzung der vielen APs mit älteren Kabeln bekommen. Aktuell sieht es aber nicht so gut damit aus.

**ABER: die Verwendung einer 2,5 und 5 Gbps-Lösung auf minderwertigen Cat.5-Verkabelungen ist wirklich nur in Ausnahmefällen erträglich, z. B. wenn genau feststeht, dass das Gebäude, was hier betroffen ist, innerhalb der nächsten 2-5 Jahre ohnehin abgerissen, in ein Schwimmbad umgewandelt oder kernsaniert werden soll. Soll die Verkabelung 5 Jahre oder länger halten, reicht das einfach nicht.**

Nochmal zusammengefasst die Gründe:

- Mit 2,5 und 5 Gbps kann man wirklich nur noch im Zusammenhang mit 802.11ac Wave2 etwas anfangen, schon ab der von zwei Herstellern vorgestellten „Wave3“ wird man damit nicht mehr auskommen, sondern benötigt eine 10 Gbps-Infrastruktur.
- „Wave3“ ist keine leere Drohung, sondern wird bei allen wichtigen Herstellern innerhalb der nächsten zwei Jahre kommen. Der Standard gibt die Funktionen grundsätzlich her und auch bei den Endgeräten wird man in die passende Leistungsklasse aufsteigen können.
- Der mögliche Kostenvorteil von 2,5 und 5 GbE liegt wirklich ausschließlich in der Möglichkeit der Verwendung alter Kabel. Die Switches sind nicht deutlich billiger, wie sollten sie auch: ein 2,5/5 GbE Switch ist nichts weiter als ein 10 GbE-Switch mit modifizierten (um nicht zu sagen kastrierten) Ein- und Ausgangsports. Es werden eben nur Teile der für diese Stufe wichtigen SERDES-Schaltkreise benötigt (Serialisierer/Deserialisierer). Außerdem gibt es leichte Veränderungen in dem Teil der Transceiver-Elektronik, der den Kabeln zugewandt ist, damit die Übertragung über die minderwertigen Kabel auch funktioniert. Unter Beobachtung der üblichen Marktstreams ist es durchaus denkbar, dass reinrasige 10 GbE-Switches dauerhaft gesehen sogar deutlich billiger werden als 2,5/5/10 GbE-Switches, einfach weil mehr davon verkauft werden.

Number of Bundled Cables	Temperature Rise (°C) - 1000mA per pair			
	Cat 53 (24AWG)	Cat 6 (23.5 AWG)	Cat 6A (23 AWG)	Cat 8 (22.5 AWG)
52	15.0	12.4	10.9	10.1
61	17.4	14.5	12.7	11.7
64	18.1	15.0	13.1	12.2
74	20.7	17.2	15.0	13.9
91	25.4	21.1	18.3	16.9

Abbildung 9: Temperaturanstieg in Kabelbündeln

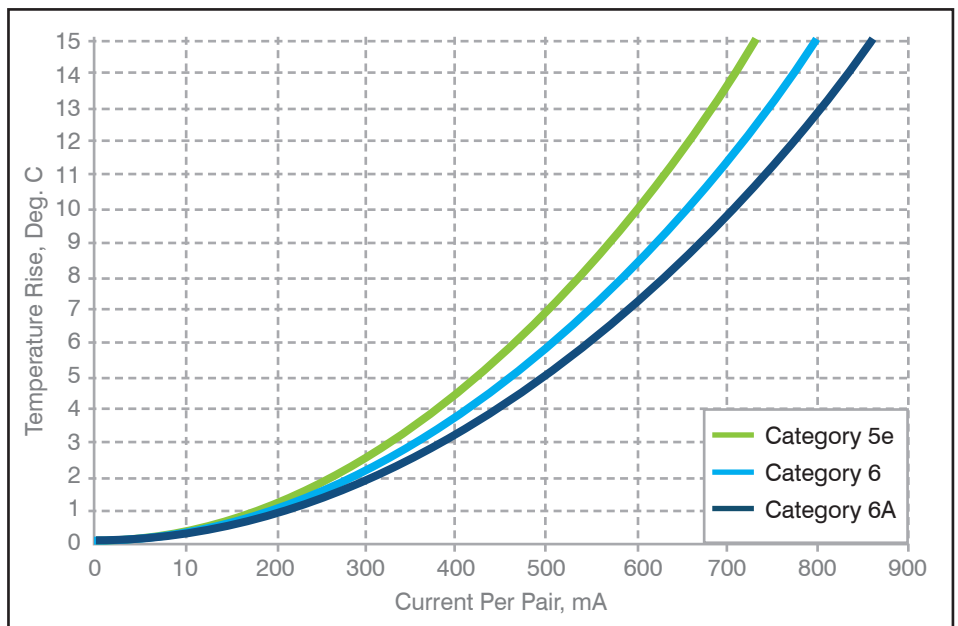


Abbildung 10: Erwärmung in Abhängigkeit vom Strom

Quelle: TIA TSB-184

- Die Lösung 2,5 und 5 GbE ist ein Kompromiss bei der Standardisierung, weil sich sonst Länder, die eine überwiegende Cat-5-Verkabelung haben, wie z.B. die USA, bei anderen Projekten einfach querstellen, wenn sie hier ihren Willen nicht bekommen. Das bedeutet für einen Europäischen Betreiber aber nicht unbedingt, dass er sich hier anschließen muss.

Die persönliche Meinung des Autors ist, dass hinsichtlich des Betriebs gewichteter Infrastrukturen für die Versorgung von Wireless-Bereichen solchen Konzepten, wie sie von Meraki (gehört jetzt Cisco) entworfen wurden, die Zukunft gehört: Steuerung der wireless Infrastruktur aus einer nicht nur hinsichtlich der Anzahl zu versorgender Endgeräte, sondern auch der Funktionen in Automation, Orchestrierung und Sicherheit massiv skalierbaren Cloud. Und das Ganze natürlich auch bei langsameren Geschwindigkeiten als 10 GbE auf Kabeln mindestens der Qualität Cat. 6A, weil sonst auch schon wieder Ungemach mit PoE drohen könnte.

### 3.2 IEEE 802.11ax

IEEE 802.11ax ist die Nachfolgetechnik zu IEEE 802.11ac. Aus der Erfahrung weiß man, dass es immer eine recht hohe Trägheit beim Übergang gibt, weil der jeweilige Vorgängerstandard noch auf seinem Einsatz beharrt. Die Technik von IEEE 802.11ax ist eigentlich sonnenklar: alleine die Verwendung von OFDMA, was sich bei LTE ja bereits bestens bewährt hat, statt des unseligen noch aus dem letzten Jahrtausend stammenden DCF-Steuerungsverfahrens bringt eine Leistungssteigerung von durchaus 50% bei ansonsten gegenüber 11ac unveränderten Transceiverparametern, weil DCF der grottenschlechte Fluch der WLANs ist. Alleine damit könnte 11ax schon sicher in den Leistungsbereich „echte“ 5-7 Gbps vordringen. Aber, die Entwicklung macht hier noch ein paar zusätzliche Schritte. Das MU-MIMO ist bei 11ac auf den Downlink beschränkt. Mit der Einführung ausgedehnterer Multi-Antennentechnik auch in Endgeräten einschließlich Smartphones kann man MU-MIMO auch auf den Uplink bringen. Auch wenn es sicher nicht so häufig in Einsatz kommen

---

## Entwicklung von Anwendungen, Verkehrslasten und neuen drahtlosen Übertragungssystemen ...

---

wird, wird 11ax das dichtere Modulationsverfahren QAM-1024 benutzen. Schließlich wird es noch eine weitere Funktion geben, die man am einfachsten als „Party-WLAN“ erklären kann. Bei einer Party reden eigentlich alle durcheinander, aber dennoch ist es möglich, dass viele Personengruppen, die jeweils eng zusammenstehen, problemlos kommunizieren können. Bei einem WLAN heutiger Bauart ist es so, dass sich ein Sender panikartig von einem Kanal, den er eigentlich benutzen wollte, zurückzieht, wenn auf diesem Kanal auch nur ein Hauch von Kommunikation einer anderen Station zu ertasten ist. Daher sieht die Gegenstelle einer Station, die den Kanalzugriff „gewonnen“ hat, ein sehr gutes Signal/Rauschverhältnis, weil alle Stationen im Umkreis auf dem gewählten Kanal still sind. Das ist so, als würde man auf einer Party, wo ja alle den gleichen „Kanal“ zwischen 300 und 400 Hz benutzen, den benachbarten Gruppen sagen, sie sollen doch still sein. Letztlich führt das aber zu einer ineffizienten Nutzung des Spektrums. Wenn eine Station einen für sie optimalen Signal/Rauschabstand hat, sendet sie auch mit der ihr möglichen höchsten Datenrate. Eine weitere Verbesserung des Signal-/Rauschverhältnisses bringt dann nichts mehr. Also kann man durch ein mehr dynamisiertes Verfahren durchaus erlauben, dass zwei oder sogar noch mehr Stationen auf dem gleichen Kanal senden, sofern dadurch das Signal/Rauschverhältnis jeweils nicht deutlich verschlechtert wird. Solche Funktionen kann man natürlich nur mit verbesserter Signalverarbeitung implementieren, aber offensichtlich wird es funktionieren, wie die Hersteller versichern. **Damit kommt IEEE 802.11ax leichtfüßig auf 10 Gbps pro Zelle.** Die Konsequenz ist klar: wer ein solches System nur mit 2,5 oder 5 GbE in der Infrastruktur unterstützen will, kann es auch ganz lassen. 10 GbE ist auch hier das Minimum. Letzte Frage: wann kommt das?

Die Diskussionen über die einzusetzenden Technologien haben schon jetzt einen extrem hohen Reifegrad. Es wurden sicher längst Prototypen für die Chips entwickelt. So kann man davon ausgehen, dass spätestens 2017 die Fertigungsvorstufe erreicht ist und Chip-Muster an interessierte Hersteller gehen können. Erste Produkte könnten Ende 2018 vorgestellt werden, das wäre dann harmonisch mit der Entwicklung bei 5G, sozusagen bis **10 Gbps für jedes mobile Endgerät!**

### 3.3 IEEE 802.11ad

**IEEE 802.11ad.** Das 5 GHz-Band ist rappellvoll und das 2,4 GHz-Band hat überhaupt keine Leistung, die zu den neuen Anforderungen passen würde. Das Aus-

weichen auf den Millimeterwellenbereich ist daher zwangsläufig, wenn man wirkliche Gigabit-Datenraten dauerhaft erzielen möchte. Der Nachteil der Millimeterwellen ist einfach, dass sie sehr empfindlich sind und schon kleine Hindernisse ausreichen, damit sie nicht weiterkommen. Für bestimmte Raumszenarien, wie Büros, Wohnzimmer, Besprechungsräume und andere kleinere Räume ist das aber kein wirkliches Problem mehr. Das haben wir in im Artikel zu 802.11ad im Insider Ausgabe Februar 2016 ja auch ausführlich besprochen. Es gibt aber noch ein anderes Problem in der heutigen Realität: die massive Überlastung des 5 GHz-Bandes führt vielfach dazu, dass eigentlich niemand mehr etwas von seinem WLAN hat. Am deutlichsten tritt das Phänomen in Mehrfamilien-Wohnanlagen zu tage. Auch der Autor hat weit über ein Dutzend WLANs in seinem Wohnzimmer, aber nur eins davon ist seins. Zu Zeiten, wo alle ihr WLAN benutzen, führt das gegenseitige automatische Ausweichen der WLANs untereinander zu fürchterlichen Performance-Verlusten. Je mehr Leute man fragt, desto mehr sind davon auch offensichtlich betroffen.

Was bedeutet das für den Betreiber einer privaten Infrastruktur? Ganz einfach. Wie jeder Provider muss er sich mit der Frage von Mikrozellen befassen, im Extremfall für jedes kleinere Büro oder sogar jeden Arbeitsplatz eine. Jede dieser Zellen kann deutlich mehr als 5 Gbps, also wäre es völliger Unsinn, sie einzuführen und dann mit einer zu schlechten Verkabelung abzuwürgen. Auch wenn verschiedene Produkte das heute noch nicht unterstützen, gehört die Zukunft der **Anbindung eindeutig der 10 GbE-Technik.** Also sind entsprechende Kabel hier das Minimum.

### 3.4 IEEE 802.11ay

**IEEE 802.11ay** ist die mögliche Nachfolgegeneration von 802.11ad. Einfach könnte man auch sagen, es ist 802.11ad auf Speed. 802.11ad ist der erste Ansatz, den Millimeterwellenbereich für die Zwecke eines Arbeitsplatz-Netzes, einer Mikro-Zelle oder wie immer man es nennen mag, zu nutzen. Bei der Entwicklung standen daher zunächst die eigentlichen Transceiver-Komponenten im Vordergrund, aber nicht die Optimierung des Signalfusses. Bei „normalen“ WLANs hatten wir zunächst sehr einfache Verfahren zur Vordcodierung, die mit den Systemen 11b und 11g eine bescheidene Leistung von nominal maximal 11 Mbps gebracht haben. Mit 11a und 11n wurde OFDM als grundsätzliches Übertragungsverfahren eingeführt, was die nominale maximale Leistung auf bis zu 54 Mbps an hob. Mit 802.11n kam denn die Multi-Antennentechnik hinzu, MI-

MO-OFDM. Theoretisch sollten damit bis zu 600 Mbps erzielt werden, in der Praxis wurde das nie erreicht. Mit 11ac kommen weitere Verbesserungen an dieser Stelle wie z.B. MU-MIMO-OFDM, 11ax geht dann auf OFDMA. Man sieht, dass diese Stelle, wo aus den vorcodierten Digitalsignalen mit geschickter Modulationstechnik ein Funksignal synthetisiert wird, ganz entscheidend ist. Das gilt übrigens nicht nur für die Übertragung über das Medium Luft. Auch Systeme mit metallischen Leitern und vor allem optische Übertragungssysteme haben sich mit genau den gleichen Methoden in den letzten zehn Jahren massiv verbessert. So bekommt 802.11ay direkt MIMO-OFDM statt der sehr simplen Modulationstechnik in 802.11ad. Das steigert die mögliche Leistung auf einem der knapp 2 GHz breiten Kanäle auf rund 25 Gbps. Die übrigen Parameter bleiben im Großen und Ganzen erhalten, auch an der geringen Reichweite ändert sich substantiell wenig. Genau das ist aber wieder ein Vorteil. Wenn die Systeme ohnehin eine sehr geringe Reichweite haben, benötigt man auch keinen Kanalplan für die Überlappungsfreiheit, weil sich selbst benachbarte Mikro-Zellen kaum überlappen. Daher spricht nichts dagegen, für eine Übertragung nicht nur einen, sondern direkt alle vier aktuell bereitstehenden Übertragungskanäle im Millimeterwellenbereich parallel zu nutzen. Somit kommt 802.11ay voraussichtlich auf eine aggregierte Gesamtleistung von rund 100 Gbps. Auch wenn bislang keine Anwendungen zu sehen sind, die das wirklich brauchen, wird das System aktuell dennoch weiterentwickelt, denn, wie die Erfahrung gelehrt hat: man kann nie wissen, ob sich nicht doch recht plötzlich entsprechende Anwendungsszenarien ergeben. Das System wird sicher eher erst 2020 oder später kommen, wenn es aber auch nur annähernd so viel leistet wie geplant, werden wir über völlig neue Arten der Infrastruktur nachdenken müssen, denn 10 GbE sind hier sicher auf Dauer ebenfalls zu wenig. Man könnte an optische Unterverteilung mit FTTH denken, aber aktuell ist kein Kostenmodell vorstellbar, was hier noch einigermaßen erschwinglich wäre.

### 3.5 LTE-U und LAA

**LTE-U und LAA.** Sollte tatsächlich LTE in unlicenzierten Bereichen kommen, müssen sich viele private Betreiber sehr warm anziehen. Aus einer 50-jährigen Erfahrung mit Funkübertragungssystemen neigt der Autor der Fraktion zu, die eine erhebliche Degradation der WiFi-Services befürchtet. Populär: treffen sich LTE und WiFi in einem Frequenzbereich, wird WiFi platt wie Flunder. Das liegt einfach daran, dass WiFi durch und durch eine Billig-Techno-

## Entwicklung von Anwendungen, Verkehrslasten und neuen drahtlosen Übertragungssystemen ...

logie ist und es ein Wunder wie bei „My Fair Lady“ (oder „Pretty Woman“) bei WiFi nicht gibt. Man könnte auch sagen: man bekommt WiFi aus der Gasse, aber die Gasse nie aus WiFi! So oder so sollten private Betreiber aber immer die funktechnisch möglichst beste Produktstufe installieren, und das wäre aktuell 802.11ac Wave2.

### 3.6 MuLTEfire

**MuLTEfire** ist momentan noch eine singuläre Entwicklung eines Chip-Herstellers. Natürlich wäre es schön, wenn private Betreiber endlich eine sinnvolle Alternative zu WiFi bekommen könnten, die wenigstens zu einem guten Teil dem aktuellen Stand der seriösen Funktechnik entspricht. Leider müssen wir es abwarten. Wenn es kommt, wird es eher in Richtung der 5G-Parameter gehen als bei den aktuellen LTE Datenraten verharren. Möchte man es dann in einer privaten Infrastruktur nutzen, wird man ebenfalls nicht mit 2,5 oder 5 GbE auskommen, sondern 10 GbE-Anbindung für die dann sehr leistungsfähigen „Private Base Stations“ benötigen.

### 3.7 Der Einfluss von 5G

**5G**, die nächste Mobilfunkgeneration. Wie schon mehrfach angesprochen, befindet sich 5G in einer sehr dynamischen Entwicklungs- und Test-Phase. Während man in Europa noch vor hat, mindestens bis 2020 über Standards zu debattieren, testen in den USA mindestens AT&T sowie Verizon sehr engagiert die offensichtlich schon jetzt verfügbaren Vorseerienprodukte. Ausgehend von den sehr umfangreichen Aufrüstungen bei den optischen Versorgungsstrukturen, besonders den DWDM-Backbones, hoffen die Provider, bereits 2018 mit 5G-Angeboten an den Markt gehen zu können. Da LTE gefühlt noch nicht sehr lange bei uns ist, stellt sich mancher die Frage, wieso schon wieder ein neuer Mobilfunkstandard benötigt wird. Etwa alle 10 Jahre gibt es eine neue Evolutionsstufe:

- 1982 Nordic Mobile Telephone: 1G
- 1992 erstes 2G (GSM) aus der Standardisierung
- 2001 erstes 3G (UMTS) aus der Standardisierung
- Standardisierung von 4G (LTE) begann 2001

Es wird also einfach wieder Zeit. Moore's Law schafft in zehn Jahren ca. 6 „Zyklen“, die Anzahl der Transistoren, die man auf einer Wafer-Fläche unterbringen kann, steigt dramatisch und man kann einfach erheblich mehr Funktionen jeder Art unterbringen. Eine entsprechende Weiterentwicklung der Funkübertragung ist ver-

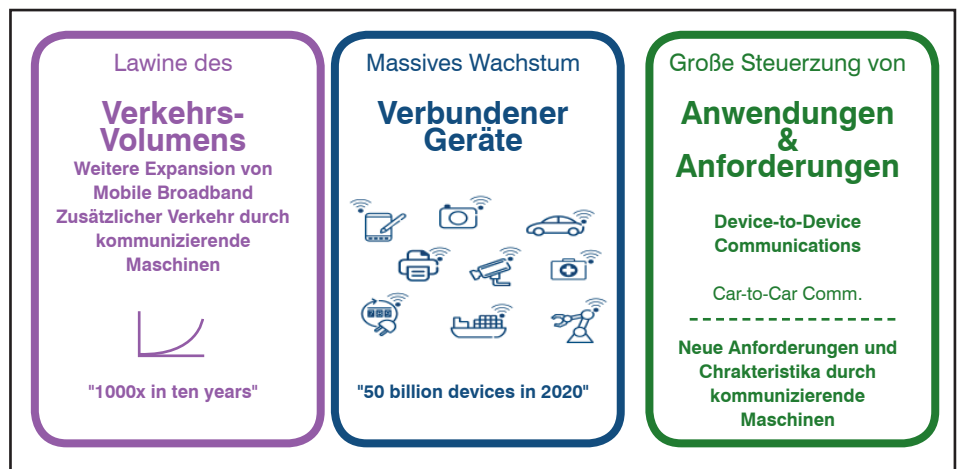


Abbildung 11: Herausforderungen an 5G

gleichsweise in diesem Szenario die größere Herausforderung.

Es gibt allerdings auch ein ganzes Bündel neu aufgekommener Anwendungsgebiete, die übersichtshalber in Abbildung 11 dargestellt sind.

Da dies in der allgemeinen Presse häufig diskutiert wird, möchte der Autor an dieser Stelle auf eine weitere Aufzählung verzichten. Man kann es aber einfach auf den Punkt bringen: die allgemeine Entwicklung führt letztlich zu wüsten Steigerungen in folgenden Bereichen:

- das Verkehrsvolumen steigt um den Faktor 1000 innerhalb von 10 Jahren
- die Anzahl der verbundenen Geräte steigt durch das IoT auf 50 Milliarden
- wir erhalten eine große Streuung von Anwendungen und Anforderungen

Bei 1G und 2G ging es um das Telefonieren. Bei 3G kam ein halbwegs sinnvoller Umgang mit Daten hinzu. Die Entwicklung und der Erfolg der Smartphones ist letztlich der Anlass für 4G/LTE. Mit der Kommunikation von Maschinen untereinander (IoT) treten nochmals ganz neue Anforderungen hinzu. Das Telefonieren ist jetzt nur noch eine kleine Anwendung unter vielen.

Es gibt durchaus verschiedene, fast schon philosophisch unterschiedliche, Visionen für 5G:

- Super-effizientes Mobilnetz mit besserer Leistung bei geringeren Investitionskosten
- Super-schnelles Mobilnetz für die Clustering der nächsten Generation von „Small Cells“ wenigstens im Stadtbereich
- Konvergierendes Fiber-Wireless Netz unter heftiger Nutzung des Millimeterwellen-Bereichs
- Latenz < 5ms E2E, mehr als 100 Geräte/qm möglich

Wie auch 4G/LTE wird sich 5G nach seiner Einführung sofort weiterentwickeln. Für den Start können wir Folgendes erwarten:

- Minimale Datenraten von mehreren 10 Mbps für mehrere 10.000 Nutzer parallel
- Minimal 1 Gbps simultan für alle Nutzer auf dem gleichen Flur, Ziel 10 Gbps
- Mehrere 100.000 simultane Verbindungen für Sensoren
- Spektrale Effizienz erheblich besser als bei 4G
- Generell verbesserte Abdeckung
- Verbesserte Signalisierungs-Effizienz
- Latenz deutlich geringer als bei LTE

Viele glauben, 5G falle irgendwann plötzlich vom Himmel. Dem ist nicht so, wie eine kleine, willkürlich auszugsweise Liste der Standardisierungsaktivitäten zeigt:

- 2008 Süd-Korea IT R&D-Programm 5G mobile
- 2012 UK 5G Innovation Centre at Univ. of Surrey
- 2012 US NYU Wireless multidisziplinäres Forschungs-Zentrum
- 2012 EU European Commission METIS Projekt (Mobile and wireless communications Enablers für the Twenty-twenty Information Society)
- 2012 EU ICT FP7 Programm für RAN as a Service (RANaaS)
- 2013 EU CROWD (Connectivity management for eneRgy Optimized Wireless Dense Networks)
- 2013 US Rutgers Univ NJ dynamisches Provisioning mit Cloud Radio Access Network (C-RAN) für NSF
- 2015 Huawei investiert 600 Mio USD in 5G-Forschung, Testnetz Malta
- 2015 Huawei und Ericsson testen 5G in den nördlichen Niederlanden
- 2015 5GNORMA Projekt vereinigt wesentliche Hersteller unter EU-Fahne
- 2015 European H2020 5G Public-Private Partnership 5G PPP

---

 Entwicklung von Anwendungen, Verkehrslasten und neuen drahtlosen Übertragungssystemen ...
 

---

- 2016 Google will ein 5G Netzwerk mittels stationärer Drohnen (SkyBender) entwickeln

Nach ersten Versuchen schon 2008 ist die Entwicklung seit 2012 in vollem Gange. Das ist auch der Grund dafür, warum den US-Providern schon jetzt Testsysteme zur Verfügung stehen. Der nächste Knackpunkt wird die Verteilung neuer Frequenzbereiche im Rahmen entsprechender Auktionen weltweit sein.

Ohne weitere Erläuterung stellen wir jetzt noch kurz die wichtigsten Techniken zusammen, mit denen 5G diese ambitionierten Ziele erreichen wird:

- Umfangreiche Nutzung von Millimeterwellen sowohl indoor als auch outdoor, 28,38,60 und 72,73 GHz-Bänder, zusätzlich 90 GHz Bänder und mehr für Backhaul
- Massives MIMO
- Proaktives Content Caching an den Netzkanten (wie z.B. Cisco Fog Computing)
- Fortschrittliches Interferenz- und Mobility-Management
- Effiziente Unterstützung von „IoT-Teilnehmern“
- Multiple-Hop Networks Wireless
- Network Virtualization
- Kognitive Radio Technologie (Smart Radio) erlaubt verschiedenen Radio-Technologien die effiziente gleichzeitige Nutzung des gleichen Spektrums durch adaptives Suchen nach unbenutzten Teilen des Spektrums und deren Nutzung
- Dynamische Ad Hoc Wireless Networks (DAWN)
- Vandermode-Subspace Frequency Division Multiplexing für Smart Radio
- IPv6
- World Wide Wireless Web WWWW

Was nehmen wir nun aus der 5G-Entwicklung für die Planung der Gestaltung der Infrastruktur für die Implementierung von flächendeckenden Wireless-Versorgungsstrukturen mit?

**Nun, alles, was man in den nächsten Jahren in dieser Hinsicht macht, muss sich letztlich an 5G messen lassen. Ein Mitarbeiter eines Unternehmens oder einer Organisation, der privat 5G benutzt, wird in seinem Arbeitsumfeld nicht mit weniger Leistung für die Anbindung seiner mobilen Endgeräte zufrieden sein. Das konnte man schon bei der ersten BYOD-Welle, die ja parallel zur Einführung von LTE verlief, deutlich feststellen.**

Da nehmen wir jetzt einfach das oben genannte Ziel „1 Gbps simultan für alle Nut-

zer auf den gleichen Flur“. Das bedeutet schlicht und ergreifend beim Einsatz von IEEE 802.11ac Wave 2 eine einstellige Nutzerzahl pro WLAN-Zelle und (wenigstens mit der Zeit) eine Anbindung des WLAN Access Points mit 10 Gbps. Darüber ist nicht weiter zu diskutieren. Bei allen anderen Zielen sieht das ähnlich aus.

#### 4. Konsequenzen für die Betreiber privater IT-Versorgungsstrukturen

Die Anforderungen an die mobile Versorgung steigen stark und man wird darauf Antworten finden müssen. Es wird sicher nicht zu weniger, sondern eher zu mehr WLAN- oder Mikro-Zellen kommen. Bei mehr Zellen, mehr Teilnehmern und mehr Leistung pro Teilnehmer rücken natürlich die betrieblichen Aspekte und die Sicherheitsfragen noch deutlicher in den Vordergrund. Hier gibt es viele interessante Lösungen, auch Cloud-basiert, die uns noch beschäftigen werden.

Bei der reinen Zellen-Technologie kann man konstatieren, dass IEEE 802.11ac Wave 2 einen deutlichen qualitativen Fort-

schritt bringt, weil es die erste 11ac-Generation ist, die nicht rein für den „Hausgebrauch“ entwickelt wurde. Neueste Techniken für Filter, Antennen-Switches und Verstärker geben Hoffnung auf einen deutlich stabileren Betrieb.

Natürlich werden WLANs und LTE-Angebote zusammenwachsen, es sollte für einen Mitarbeiter problemlos möglich sein, die Abdeckung der unternehmenseigenen flächendeckenden WLAN-Umgebung zu verlassen ohne dass seine Verbindungen abreißen, die dann eben von LTE unterstützt werden.

Auf die Perspektive von 5 Jahren oder mehr wird dieses Zusammenwachsen von Mobilfunk (dann 5G) und WLAN- sowie Mikrozellen-Technik dazu führen, dass die Benutzer immer anspruchsvoller werden und sich kein privater Betreiber leisten können wird, hier erhebliche Abstriche gegenüber der Leistung von 5G zu machen. Um das geeignet vorzubereiten, sollte man schon jetzt an eine vernünftige Verkabelung denken, mindestens nach den Normen für 10 GBASE-T.

## Intensiv-Seminar

### Sommerschule 2016 - Intensiv-Update auf den neuesten Stand der Netzwerktechnik 27.06.-01.07.16 in Aachen

Die Sommerschule 2016 bringt Sie in 5 Intensiv-Tagen auf den letzten Stand der Netzwerk-, Kommunikations- und Infrastruktur-Technik. Wir analysieren für Sie:

- Wie verändern sich IT-Architekturen und welche Anforderungen generiert das auf Infrastrukturen, welche neuen Anforderungen entstehen speziell im Rechenzentrum?
- Was passiert auf der WAN-Seite, wie sieht eine Zukunfts-orientierte WAN-Lösung aus?
- Wie sieht die Zukunft des LAN aus? Welche der neuen Technologien werden sich durchsetzen? Wie können skalierbare und sichere LAN-Infrastrukturen geschaffen werden?
- Unified Communications, das Ende von ISDN: wie sieht die Kommunikations-Lösung der Zukunft aus? Was bedeutet das für Infrastrukturen?
- WLAN-Technik erreicht immer neue Leistungsklassen: aber wie sieht die Zukunft aus? Wo ist die Abgrenzung zum Mobilfunk?
- IPv6 ist Realität: wie sieht eine erfolgreiche Migration aus? Welche Projekterfahrungen können helfen?
- Sicherheit wird immer mehr zum Schlüssel für erfolgreiche IT-Infrastrukturen: Cloud-Computing und mobile Endgeräte, wie passt das in ein Sicherheits-Konzept?

Preis: € 2.290,- netto\*

\*Frühbucherpreis bis zum 31.05.16 - dann regulärer Preis € 2.490,- netto



Buchen Sie über unsere Web-Seite

[www.comconsult-akademie.de](http://www.comconsult-akademie.de)

Aktuelle Sonderveranstaltung

# Sonderveranstaltung Wireless und Mobility 12.12. - 13.12.16 in Köln

Die ComConsult Akademie veranstaltet vom 12.12. bis 13.12.16 ihre Sonderveranstaltung "Wireless und Mobility" in Köln.

Die permanente Steigerung der Anzahl mobiler Endgeräte mit immer mehr Leistung ist mit den einhergehenden geänderten modernen Arbeitsmodellen ein längst nicht mehr aufzuhaltender Trend. Mobilität wird Normalität! Neuartige Anwendungssoftware bindet die neuen Endgeräte effektiv in optimierte mobilisierte Arbeitsprozesse ein.

Zusätzlich entstehen auch völlig neue Anwendungsbereiche, mit denen vor wenigen Jahren kaum jemand gerechnet hätte. Hier ist ganz besonders an das IoT zu denken, die automatische Kommunikation von Maschinen, Sensoren und Aktoren untereinander. Es zeichnet sich jetzt schon ab, dass der überwiegende Teil dieser Verbindungen ebenfalls drahtlos ausgeführt werden wird. Das erzeugt eine völlig neue Dimension von Anforderungen, Leistungsprofilen und Spezial-Technologien.

Provider sind nicht nur aus diesen Gründen seit einiger Zeit dabei, die Mobilfunknetze deutlich aufzurüsten. Mobiles Video-Streaming und nunmehr auf den leistungsfähigen Endgeräten mögliche Spiele mit gesteigertem Realismus



sind nur zwei der Gründe, warum man damit rechnet, innerhalb weniger Jahre eine deutliche Leistungssteigerung der Mobilfunknetze, man spricht gerne anschaulich von einem Faktor 1000, vornehmen zu müssen. Und schon jetzt wirft die nächste Mobilfunk-Generation mit 5G ihre Schatten voraus.

Dies betrifft auch Betreiber privater wireless Infrastrukturen, mit einem (hoffentlich) etwas geringeren Faktor. Sie werden kaum Videos oder Spiele in großem Umfang unterstützen müssen. Man kann aber davon ausgehen, dass die hohe Leistung der mo-

bilen Endgeräte auch für die Realisierung eines verbesserten Benutzer-Erlebnisses bei bestehenden und neuen Anwendungen genutzt wird. Dies betrifft alle denkbaren Bereiche und ist eigentlich immer eine Kombination aus Steigerung der Anzahl der mobilen Endgeräte, der Qualität dieser Endgeräte und der für die Entfaltung der Möglichkeiten dieser Endgeräte erforderlichen Kommunikationsleistung.

Passend zu diesen Entwicklungen kommen nicht nur neue Wireless-Technologien auf den Markt, sondern es ist auch die verstärkte Bestrebung zu spüren, Mobilfunk mit Wireless Small Cells wesentlich stärker zu unterstützen als bisher.

Wichtige Fragen sind also z.B.:

- welche Anforderungen bestehen aktuell und in den nächsten Jahren?
- welche neuen Technologien sind für private Betreiber wirklich nützlich?
- machen privat betriebene Infrastrukturen angesichts der Entwicklung im Mobilfunk überhaupt noch Sinn?
- welche Empfehlungen können aus konkreten Projekten für die wichtigen Anwendungsbereiche abgeleitet werden?

Hochkarätige erfahrene Spezialisten, Berater und Anbieter diskutieren in dieser einzigartigen Sonder-Veranstaltung Probleme, Lösungen, Technologien und Perspektive!

Fax-Antwort an ComConsult 02408/955-399

## Anmeldung Sonderveranstaltung Wireless und Mobility

Ich buche die Sonderveranstaltung  
**Wireless und Mobility**

12.12. - 13.12.16 in Köln  
zum Preis von € 1.990,- netto

Bitte buchen Sie mir ein Hotelzimmer

Vorname

Nachname

Firma

Telefon/Fax

Straße

PLZ, Ort

eMail

Unterschrift



Buchen Sie über unsere Web-Seite

[www.comconsult-akademie.de](http://www.comconsult-akademie.de)

Standpunkt

# Schwachstellenmanagement

## Eine Kunst, die Cyber-Kriminelle perfekt beherrschen, die IT jedoch anscheinend oft nicht

Der Standpunkt von Dr. Simon Hoff greift als regelmäßiger Bestandteil des ComConsult Netzwerk Insiders technologische Argumente auf, die Sie so schnell nicht in den öffentlichen Medien finden und korreliert sie mit allgemeinen Trends.

Für die Sicherheit der IT einer Institution ist es natürlich von entscheidender Bedeutung, dass man die eigenen Schwächen kennt, denn nur so kann zielgerichtet über eine Risikobetrachtung mit dem potentiellen Schaden umgegangen werden. Kernelement ist ein Prozess, der für die systematische Erfassung und Bewertung von Schwachstellen bzw. Verwundbarkeiten, die Planung von Korrekturmaßnahmen und die Kontrolle von Umsetzung und Wirksamkeit der Maßnahmen sorgt. Ein solcher Prozess zum Schwachstellenmanagement (Vulnerability Management) ähnelt dabei durchaus einem Prozess zur Behandlung von Sicherheitsvorfällen [1], nur handelt es sich hier um einen proaktiven Prozess, denn der Schaden ist (zuletzt) noch nicht eingetreten.

Die konsequente Umsetzung eines solchen Prozesses sollte es eigentlich ermöglichen, dass die Schwachstellen einer IT-Infrastruktur mit der Zeit sichtbar abnehmen und durch die Verringerung der Angriffsfläche auch die Auswirkung von Sicherheitsvorfällen entsprechend zurückgeht.

Nur scheint es in der Praxis ausgesprochen schwer zu sein einen solchen Prozess geeignet umzusetzen, wie folgendes Beispiel illustriert: Die Sicherheitslücke Heartbleed [2], bei der durch einen einfachen Softwarefehler ein unangenehmer Datendiebstahl über eine SSL/TLS-geschützte Verbindung möglich ist, ist inzwischen „kalter Kaffee“ und eigentlich sollte es keine Web-Server mehr geben, deren SSL/TLS-Implementierung diese Schwachstelle aufweist (schließlich ist der Softwarefehler in OpenSSL seit April 2014 behoben). Die Nachricht, dass der Web-Auftritt des Bundesministeriums für Verkehr und digitale Infrastruktur noch vor wenigen Tagen durch Heartbleed kompromittierbar war, ist daher erschreckend [3]. Dass es etwas mehr als zwei Tage gedauert hat, bis nach Bekanntwerden die Lücke geschlossen wurde, ist umso schlimmer.

Wenn es zu einer solchen oder einer ver-



gleichbaren Situation kommt, liegt der Verdacht ausgesprochen nahe: Das Schwachstellenmanagement der betreffenden Institution könnte möglicherweise unzureichend sein.

Eine übliche Regelung im Schwachstellenmanagement ist: Der jeweilige IT-System- oder Anwendungsverantwortliche ist für die systematische Sammlung von Informationen hinsichtlich Schwachstellen des von ihm betreuten Systems und für das Einspielen von Patches zuständig. Das sagt sich so leicht. In der Praxis stelle ich immer wieder fest, dass es genau hier klemmt. Immer wieder kommt es vor, dass Administratoren und sonstige Systemverantwortliche nicht über Schwachstellen ihrer Systeme genügend informiert sind, geschweige denn einen in der Informationssicherheit spezifizierten Prozess zum Schwachstellenmanagement überhaupt kennen. Hier liegt das eigentliche Problem: Alle Beteiligten an der IT müssen aktiv und eigenverantwortlich mitmachen!

Im Schwachstellenmanagement ist es außerdem üblich insbesondere Web-Anwendungen einem Penetrationstest oder zumindest einem Test mit einem Schwachstellenscanner zu unterziehen, bevor die Anwendung in Produktion geht und über das Internet erreichbar ist. Hier wäre die oben geschilderte Heartbleed-Peinlichkeit selbstverständlich sofort aufgefallen. Daneben können durchaus auch produktive Systeme in regelmäßigen Abständen oder auf Stichprobenbasis über einen Schwachstellenscanner geprüft werden. Es wäre schließlich nicht das erste Mal, dass bei einem Softwareupdate plötzlich eine Sicher-

heitslücke wieder da ist, die man eigentlich für geschlossen hielt.

Schauen wir uns nun die Seite der Angreifer auf die IT an. Kürzlich ist eine neue Version des Data Breach Investigations Report von Verizon erschienen [4], die einmal mehr deutlich macht, dass seit Jahren bewährte Angriffe immer noch bestens funktionieren und Angreifer auf bestehende (oft öffentlich verfügbare) Angriffswerkzeuge zurückgreifen können. Auch dies ist ein Anzeichen, dass das Verwundbarkeitsmanagement in vielen Institutionen noch nicht ernst genug genommen wird.

Als letztes Beispiel kann in diesem Zusammenhang der Bundesstags-Hack [5] dienen. Hier wurde festgestellt, dass bei dem Angriff keineswegs teure Day Zero Exploits im Darknet [6] erworben und genutzt wurden, sondern mit frei verfügbaren Werkzeugen gearbeitet wurde. Zu nennen ist hier insbesondere mimikatz [7], ein bewährtes Werkzeug, um in Microsoft Windows Administrator-Credentials und private Schlüssel von Zertifikaten zu stehlen (was erst ab Windows 8.1 bzw. Server 2012 nicht mehr so ohne weiteres geht). Für das Schwachstellenmanagement ist es essentiell zu wissen, wie Angreifer vorgehen und welche Techniken und Werkzeuge sie nutzen, um Gegenmaßnahmen zu erarbeiten.

Die Gefahr, die durch Cybercrime für die eigene IT ausgeht, darf nicht unterschätzt werden und im Bereich Schwachstellenmanagement sind Cyber-Gangster Profis! Dies bedeutet aber auch, wer für die eigene IT ein Schwachstellenmanagement nicht wirksam und nachhaltig implementiert, handelt eigentlich grob fahrlässig.

### Verweise

- [1] „Der Netzwerk Insider“, März 2016
- [2] <http://heartbleed.com/>
- [3] <http://www.heise.de/security/meldung/Ministerium-fuer-digitale-Infrastruktur-pfuscht-beim-eigenen-Web-Server-3186960.html>
- [4] [http://www.verizonenterprise.com/resources/reports/rp\\_DBIR\\_2016\\_Report\\_en\\_xg.pdf](http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf)
- [5] <http://www.golem.de/news/malware-interne-dokumente-geben-aufschluss-ueber-bundestagshack-1603-119608.html>
- [6] <https://www.wired.com/2015/04/thereal-zero-day-exploits/>
- [7] <http://blog.gentilkiwi.com/mimikatz>

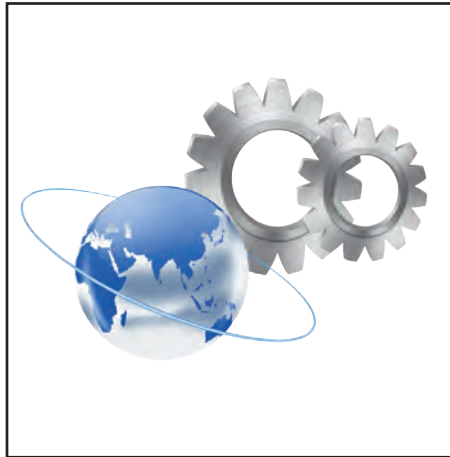
Aktuelles Seminar

# IT-Kommunikation im Umfeld von Fertigung und Automation 13.06. - 14.06.16 in Bonn

Die ComConsult Akademie veranstaltet vom 13.06. bis 14.06.16 ihr Seminar "IT-Kommunikation im Umfeld von Fertigung und Automation" in Bonn.

Mit der aktuellen Technologie-Entwicklung stellt sich immer mehr die Frage, ob eine klare Trennung zwischen Büro und Fertigung in Zukunft noch erreichbar sein wird. Dieses Seminar analysiert wie Fertigungsnetzwerke auf diese Herausforderungen reagieren können und wie mit geeigneten Technologien Sicherheit, Leistung und Flexibilität gewährleistet werden kann.

Netze in Fertigung und Automation unterscheiden sich von Büronetzen. In Fertigungsnetzen werden eine hohe Verfügbarkeit, die Vermeidung unnötiger Bedrohungen und trotzdem hohe Flexibilität erwartet. Mit der aktuellen Technologie-Entwicklung stellt sich aber immer mehr die Frage, ob eine klare Trennung zwischen Büro und Fertigung / Automation in Zukunft erreichbar sein wird. Es stellt sich auch die Frage, ob wir nicht über genügend leistungsfähige Architekturen und Werkzeuge verfügen, um einen Grad an Schutz und Kontrolle zu etablieren, der die Kombination aus Sicherheit, Leistung und Flexibilität möglich macht.



Während über Konzepte wie Internet of Things (IoT) und Smart Home überwiegend visionär gesprochen wird, haben produzierende Unternehmen schon seit Jahren eine stark steigende Anzahl von Geräten in ihren Industrienetzen. Insofern ist für diese Firmen die Industrie 4.0, d.h. die vierte industrielle Revolution, kein Bruch mit dem Bisherigen, sondern die konsequente Fortsetzung der dritten industriellen Revolution, nämlich der Automatisierung.

Der explosionsartige Anstieg der Zahl der Geräte in der Fertigung stellt die IT-Infrastruktur in den Hallen und im Campus vor nie dagewesene Herausforderungen. Das Netzkonzept muss in vieler Hinsicht an die neue Situation angepasst werden.

Das Seminar richtet sich an IT-Architekten, IT-Planer und IT-Betreiber, die Netze aus Fertigung und Automation in ihre IT-Landschaft integrieren müssen, sowie Planer und Betreiber von Fertigungsnetzwerken.

Dieses Seminar stellt die Fragen:

- Wo stehen wir technologisch im Bereich Fertigungsnetze?
- Was wollen wir oder wozu werden wir gezwungen?
- Wie kann ein guter Weg in die Zukunft aussehen?

Diese und weitere Fragen im Zusammenhang mit der IT-Kommunikation im Umfeld von Fertigung und Automation werden unsere Experten mit langjähriger Praxis in der Beratung, Dipl.-Ing. Hartmut Kell, Dr. Stefan Muthmann, Dr. Simon Hoff und Dr. Joachim Wetzlar, von Industrieunternehmen auf dieser Veranstaltung mit Ihnen diskutieren.

Fax-Antwort an ComConsult 02408/955-399

## Anmeldung IT-Kommunikation im Umfeld von Fertigung und Automation

Ich buche das Seminar  
**IT-Kommunikation im Umfeld von  
Fertigung und Automation**

13.06.-14.06.16 in Bonn  
zum Preis von € 1.590,-- netto

Bitte buchen Sie mir ein Hotelzimmer

Vorname

Nachname

Firma

Telefon/Fax

Straße

PLZ, Ort

eMail

Unterschrift



Buchen Sie über unsere Web-Seite

[www.comconsult-akademie.de](http://www.comconsult-akademie.de)

## Zweitthema

# Redesign von WAN- und Internet-Zugängen

Fortsetzung von Seite 1



Dr.-Ing. Behrooz Moayeri hat viele Großprojekte mit dem Schwerpunkt standortübergreifende Kommunikation geleitet. Er gehört der Geschäftsleitung der ComConsult Beratung und Planung GmbH an und betätigt sich als Berater, Autor und Seminarleiter.

## Rasanten Internet-Wachstum

Wer kennt das nicht: Auf immer mehr Webseiten im Internet laufen kleine Filmchen im Hintergrund. Meistens handelt es sich dabei um Werbung. Ob man sie haben will oder nicht, Video ist im Internet zum Alltag geworden. Die Bildauflösung wird dabei immer besser. Es ist klar: wer will schon mit groben Pixeln für das eigene Produkt werben?

Das Ganze hat aber einen Preis: Verkehrsvolumen. Das Internet muss vor allem aufgrund von immer mehr und immer höher auflösenden Bildern ständig aufgerüstet werden. Dies gilt sowohl für die Backbones der Internet Service Provider (ISPs) als auch für die Zugänge der Kunden. Die ISPs müssen diese ständige Ertüchtigung ihrer Netze fast vollständig über die Gebühren finanzieren, die sie für die Internet-Zugänge bekommen. Bekanntlich bekommen die ISPs kaum etwas von dem Kuchen ab, den die Werbewirtschaft spendiert. Dieser Kuchen geht fast vollständig an Google & Co. Haben Sie aber schon mal erlebt, dass Google Ihr Gebäude mit Glasfasern anbindet? Sie müssen diese Anbindung bezahlen, und zwar über den Preis, den Sie an Ihren ISP entrichten. Der ISP muss aber auch an seine künftigen Geschäfte denken. Er muss – und das ist gar nicht so böswillig wie es klingt – für eine künstliche Verknappung des Netzdurchsatzes sorgen, damit Sie auch morgen und übermorgen ihn bezahlen, und zwar für mehr Netzdurchsatz.

So kommt es, dass der Durchsatz des Internet-Zugangs immer wieder auf eine Grenze stoßen muss. Dann wenden Sie sich an den ISP, egal ob als Endverbraucher oder Unternehmen, und bekommen meistens für mehr oder weniger die gleichen Monatsgebühren mehr Netzdurch-

satz. Bis zu einem bestimmten Durchsatzwert geht das über bereits vorhandene Kabel, meistens klassische Kupferkabel, die jahrzehntelang zum Telefonieren genutzt worden sind. Die über Telefonkabelanschlüsse übertragbare Bitrate wurde in den letzten zwanzig Jahren von ein paar hundert Kilobits pro Sekunde auf jetzt ein paar hundert Megabits pro Sekunde erhöht. Aber irgendwann sind die Grenzen der Physik erreicht, und man braucht Glasfasern. Sind diese erst mal verlegt, wird die maximale Bitrate nur noch durch die eingesetzten aktiven Komponenten bestimmt, nach oben praktisch unbegrenzt.

Aber selbst mit Glasfasern muss der ISP den Netzdurchsatz auf der Internet-Zuleitung begrenzen. Und da die Provider ihre Netze und den Bedarf ihrer Kunden gut messen können, sorgen sie dafür, dass die Zuleitung für den einzelnen Kunden nur bezahlbar bleibt, wenn sich der Kunde auf eine Durchsatzgrenze einlässt. Diese Grenze wird im Moment immer schneller erreicht. Und schon kann der Provider Abhilfe schaffen, in der Regel mit viel mehr Durchsatz, und wenn er geschickt ist für etwas mehr Geld.

Diesen Zyklus erleben Endverbraucher und Unternehmen gleichermaßen. ComConsult berät letztere als eigene Kunden. Rein statistisch ist es einleuchtend, was unsere Kunden zurzeit erleben: Es gibt immer einen bestimmten Prozentsatz unserer Kunden, bei denen die Bitrate des Internet-Anschlusses ausgeschöpft ist. Einige sehen nicht ein, dass sie nach einer gar nicht so lange zurück liegenden Aufforderung schon wieder mehr Durchsatz für den Internet-Anschluss bestellen müssen. Sie fragen uns regelmäßig an, was man sonst tun kann. Andere wiederum führen die Symptome erst einmal nicht auf die häufigste Ursache zurück, und stellen nur

fest, dass wichtige auf das Internet angewiesene Anwendungen, zum Beispiel Virtual Private Networks (VPNs) immer mehr beeinträchtigt werden. Hier ein Tipp: Meistens liegt das daran, dass entweder am nahen oder am entfernten Ende zu viele Pakete verworfen werden, weil die Kapazität eines Zugangs ausgeschöpft ist.

Noch schlimmer trifft es Unternehmen, die aus Sicherheitsgründen ihren gesamten Internetverkehr über einen zentralen Zugang wie in der Abbildung 1 dargestellt führen.

Wie in der Abbildung 1 ersichtlich wird bei einem zentralen Internetzugang der Internetverkehr teilweise über das WAN geführt. Dies ist dann der Fall, wenn der Standort des zentralen Internetzugangs vom Standort des mit dem Internet kommunizierenden Gerätes aus nur über das WAN erreichbar ist. In diesem Fall muss das Unternehmen die Zunahme des Internetverkehrs doppelt bezahlen: durch die Erhöhung der Kapazität der Internetleitung selbst und zusätzlich durch mehr Volumen im privaten WAN.

Letzteres ist meistens wesentlich teurer als über das Internet zu übertragendes Volumen. Auch beim WAN müssen die Provider an die eigene Zukunft denken, indem sie ihren Kunden nicht endlos Netzdurchsatz spendieren, sondern nur wohl dosiert. Aus mehreren Gründen ist der Preis dafür wesentlich höher als im Internet:

- Erstens gibt es im WAN-Markt weniger Wettbewerb als im ISP-Markt.
- Zweitens wird das WAN von vielen Unternehmen für sehr geschäftskritische Anwendungen genutzt, sodass die Unternehmen bereit sind, mehr Geld dafür auszugeben.

## Redesign von WAN- und Internet-Zugängen

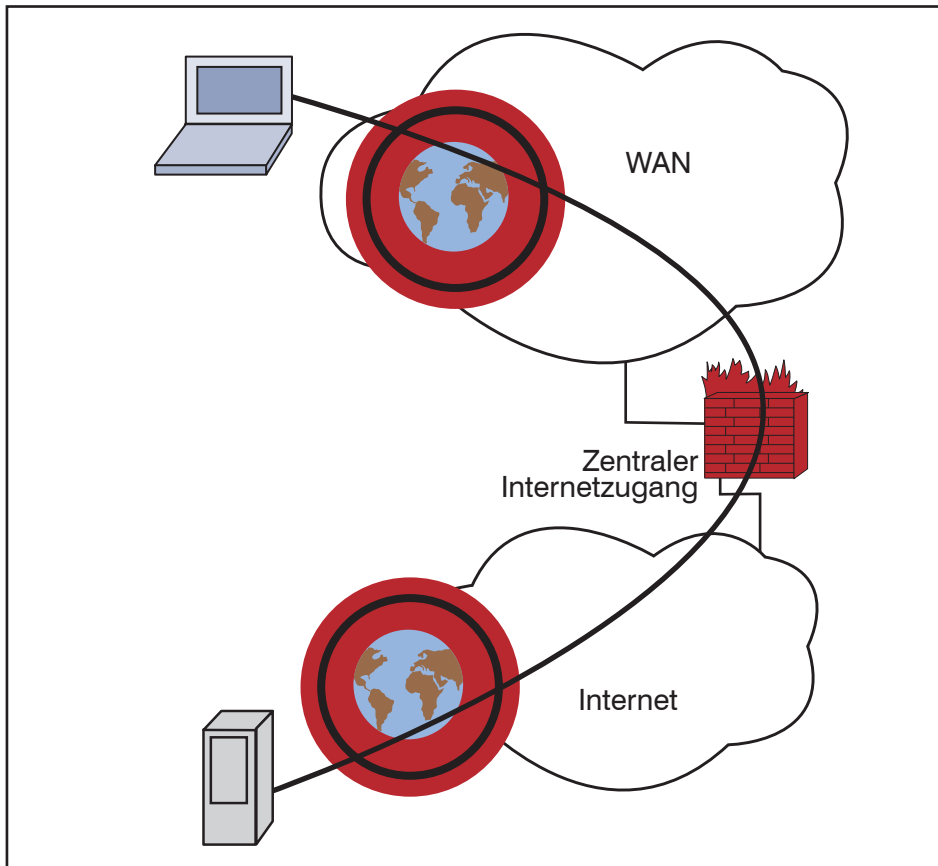


Abbildung 1: Zentraler Internetzugang

- Drittens erwarten die Kunden vom Betreiber einer privaten WAN-Plattform, dass er viel strengere Service Level Agreements (SLAs) einhält als ein ISP. Das bindet Ressourcen sowie Personal und kostet Geld.
- Viertens gibt es bei einer privaten WAN-Plattform kein so dichtes Netz an Points of Presence (PoP), sodass die Zuleitungen länger und teurer sind.

So kommt es, dass das rasante Internet-Wachstum für viele Unternehmen nicht nur direkte, sondern auch indirekte Kosten, nämlich WAN-Kosten, verursacht. Die indirekten Kosten betragen in nicht wenigen Fällen ein Vielfaches der direkten Kosten.

Wie aus der Abbildung 1 hervorgeht, gibt es nicht nur ein Kostenproblem. Unternehmen, die Standorte in verschiedenen Kontinenten haben und den Internet-Verkehr teilweise über Grenzen der Kontinente hinweg im WAN übertragen müssen, kennen das Phänomen, dass darunter die Antwortzeiten beim Internetzugriff leiden. Dieser Verkehr wird nämlich zweimal über ein weltweites Netz geführt, über das WAN und das Internet. Dementsprechend summiert sich die Signalübertragungszeit. Hier hilft auch keine Bitratenerhöhung. Die Ausbreitungsgeschwindigkeit optischer und elektrischer

Signale ist endlich. Die Grenze liegt, wenn nicht gerade das Vakuum als Medium genutzt wird, wesentlich unter den aus dem Physikunterricht bekannten 300.000 Kilometern pro Sekunde. Im Glas breitet sich Licht mit ungefähr 200.000 Kilometern pro Sekunde aus. Interkontinentale Kabelwege können zehntausende Kilometer lang sein. Hin und zurück kommt man dann auf mehrere hundert Millisekunden. Nicht bei jeder Applikation sind solche Werte zu vernachlässigen.

Wäre das Internet für die Geschäftsprozesse der meisten Unternehmen relativ unwichtig wie es vor vielleicht zwanzig Jahren war, könnte man über schlechte Performance von Internet-Anwendungen hinwegsehen. Die Situation hat sich aber in den letzten zwei Jahrzehnten in vieler Hinsicht geändert. Auf einige Veränderungen sei hier hingewiesen:

- Der Alltag vieler Arbeitsplätze in Unternehmen ist durch das Internet geprägt. Ob man eine Information dringend benötigt, die am schnellsten über das Internet eingeholt werden kann, oder die nächste Dienstreise planen will: Ohne Internetzugriff kommt man nicht mehr aus.
- Viele Unternehmen wickeln ihre Geschäfte über das Internet ab. Vor zwanzig

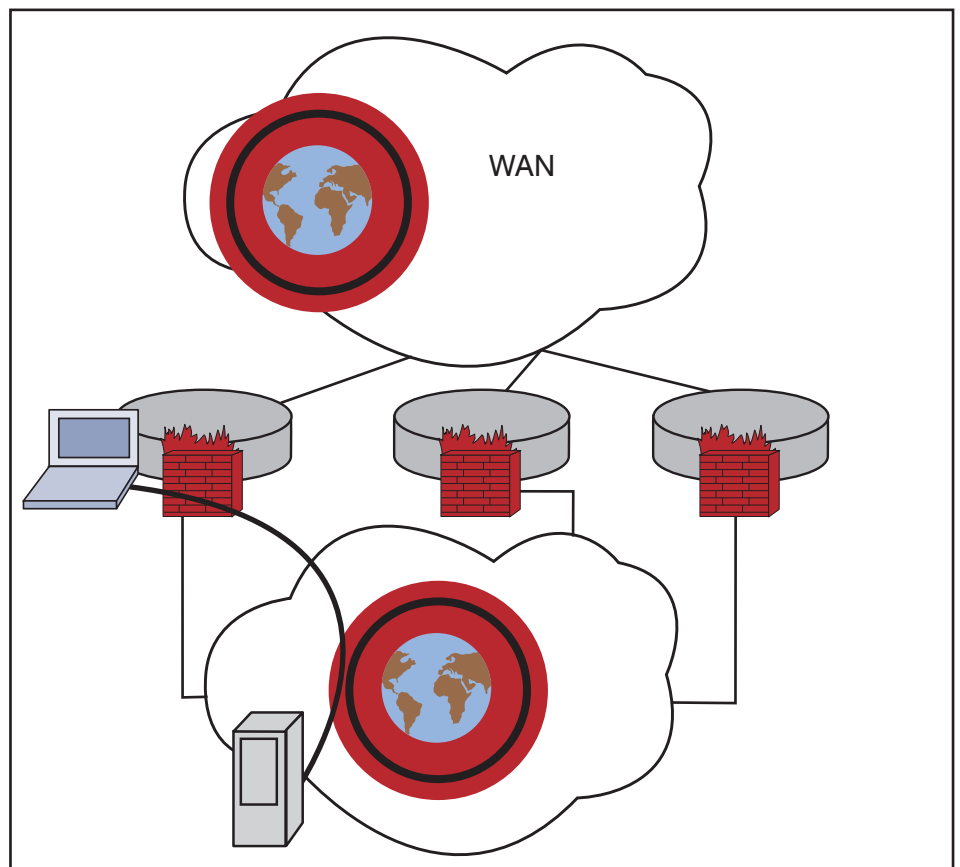


Abbildung 2: Verteilte Internetanschlüsse

## Redesign von WAN- und Internet-Zugängen

zig Jahren für viele in der Automobilindustrie unvorstellbar: Heute kann es existenzgefährdend sein, wenn man zwar dank einem stabilen internen Netz Autos am laufenden Band produzieren kann, diese aber von vielen Kunden nicht bestellt werden können, weil die Internetverbindung unterbrochen, langsam oder unzuverlässig ist.

- Viele Unternehmen verlagern Standardanwendungen wie Büroapplikationen in öffentliche Clouds. Antwortzeiten solcher Anwendungen hängen direkt von der Performance des Internetzugangs ab.

### Neuer Trend: Dezentrale Internetzugänge

Um das für viele wichtige Prozesse lebenswichtige private WAN als eine relativ teure Ressource zu entlasten und die Performance des Internetverkehrs zu verbessern, rücken viele Unternehmen vom bisher strikt zentralen Internetzugang ab. Insbesondere für weltweit agierende Unternehmen sind dezentrale Internetzugänge der neue Trend. Abbildung 2 zeigt einen solchen Ansatz.

Wie aus der Abbildung 2 hervorgeht, kann ein Standort sowohl mit dem privaten WAN als auch mit dem Internet verbunden sein. Der Zugriff auf Inhalte und Anwendungen im Internet muss dabei nicht über das WAN geführt werden. Das WAN wird entlastet. Der WAN-Zugang muss nicht aufgrund des rasanten Wachstums des Internetverkehrs ständig aufgerüstet werden. Die Anwender erleben bessere Antwortzeiten von Internet-Anwendungen, weil dafür der kürzeste Übertragungsweg über einen lokalen Internetanschluss genutzt wird.

Scheut man den Aufwand für den Betrieb und die Absicherung einer Vielzahl von Internetzugängen, muss man es mit der Dezentralisierung der Internetzugänge nicht übertreiben. Manchmal hilft es schon, wenn man pro Kontinent bzw. Weltregion einen Internetanschluss betreibt, der von allen Standorten der Region genutzt wird. Eine wichtige Voraussetzung für einen solchen Kompromiss besteht darin, dass in der jeweiligen Region die Summe aus den Betriebskosten für einen leistungsfähigen, sicheren Internetzugang sowie den Mehrkosten durch die Nutzung des regionalen WAN für den Internetverkehr niedriger ist als die Betriebskosten für mehrere genau so gut abgesicherte Internetzugänge.

### Bleibt die IT-Sicherheit auf der Strecke?

„Genauso gut abgesicherte dezentrale Internetzugänge“ bleibt für viele Entscheider in Unternehmen ein Widerspruch in sich. Nicht von ungefähr haben sie manchmal

in einem mühsamen Prozess dafür gesorgt, dass der Zugriff auf das Internet zentralisiert und über eine „Perimeter Security“ genannte Umgebung mit Firewalls, Proxies, Virensclannern etc. geführt wird. Lockert man diese strikte Richtlinie, ist die Gefahr nicht von der Hand zu weisen, dass die Mehrzahl der neuen Internetzugänge an irgendeiner Stelle Risiken und Angriffen aus dem Internet Tür und Tor öffnet. An solchen Risiken der Internetnutzung gibt es wahrlich nicht wenig, sondern immer mehr. Man muss nur täglich Nachrichten verfolgen um das zu wissen.

Bleibt also bei der Dezentralisierung oder Regionalisierung der Internetzugänge die IT-Sicherheit auf der Strecke? Ist weniger Sicherheit der Preis, den man für zunehmenden Internet-Verkehr und die Lösung von Performance-Problemen zahlen muss?

Von einem IT-Berater erwarten Sie, liebe Leserinnen und Leser, doch nicht, dass er diese Frage bejaht. Nein, Sie erwarten von ihm, dass er eine Lösung aufzeigt, die gleichzeitig leistungsfähig und sicher ist.

Das will der Berater hier versuchen. Dabei kann er gleich mehr als nur eine Lösung aufzeigen. Dass keine Lösung zum Nulltarif zu haben ist sollte einleuchten.

Die erste Lösung, die einem einfällt, ist die bereits erwähnte Regionalisierung als Kompromiss zwischen den beiden Extremen der absoluten Zentralisierung und der vollständigen Dezentralisierung. Ist die An-

zahl der regionalen Internetzugänge überschaubar, kann man sie einheitlich und mit den gleichen Sicherheitskomponenten ausstatten. Egal ob Firewalls, Proxies oder Virensclanner: der Anspruch muss lauten, dass diese Komponenten trotz der geografischen Verteilung demselben Management unterliegen und mit denselben Regeln konfiguriert werden. Dieser Anspruch wird von so vielen Unternehmen erhoben, dass die führenden Hersteller dieser Komponenten nicht umhinkommen diese Anforderung zu erfüllen. Zu jedem für den Unternehmenseinsatz tauglichen Firewall-, Proxy- oder Virenschutzsystem gehört heutzutage ein zentrales Management, mit dem die Regeln auf mehreren Instanzen solcher Systeme einheitlich konfiguriert und kontrolliert werden können.

Die wichtigsten Vorteile dieser Lösung sind die folgenden:

- Die bewährten Erfahrungen aus dem Betrieb von eigenen zentralen Sicherheitskomponenten kann man weiter nutzen. Man muss die Konzepte nur leicht anpassen.
- Die Sicherheit von Internetzugängen bleibt in eigener, zentraler Hand.
- Die Performance der Internetzugriffe leidet nicht mehr unter Signallaufzeiten zwischen verschiedenen Kontinenten.

Aber dieser Ansatz hat auch einige Nachteile:

## Seminar

### Sonderveranstaltung

**Voice und Video im WAN - 30.05.16 in Köln**

**All-IP, B2B, B2C und Daten kämpfen um die Kapazität, wie kann das beherrscht werden?**

Wie kann die Übertragung von Sprache und Video im WAN optimiert werden ohne andere Anwendungen zu gefährden? Wie gehen wir mit einem immer größeren Anteil und vor allem der Integration von Video in wesentliche Geschäftsprozesse um? Neue Kollaborations-Lösungen erhöhen zudem den Druck auf die Infrastrukturen. Verkehrslasten werden dabei immer dynamischer und einfache statische Regeln wie traditionelles QoS stoßen an ihre Grenzen.

Die Sonderveranstaltung beleuchtet den Status Quo, die Zukunftsaussichten, mögliche Optionen und eventuellen Investitionsbedarf für den sicheren Betrieb aller Anwendungen.

Referenten: Dipl.-Math. Leonie Herden, Dipl.-Ing. Dominik Zöller

Preis: € 1.090,- netto



Buchen Sie über unsere Web-Seite

[www.comconsult-akademie.de](http://www.comconsult-akademie.de)

## Redesign von WAN- und Internet-Zugängen

- Die Beschaffungskosten für Perimeter Security steigen durch die Regionalisierung wesentlich.
- Der Internetverkehr belastet zumindest innerhalb der Regionen das WAN.
- Hat man Standorte, die sich in verschiedenen Zeitzonen arbeiten, muss man einen zentralen Betrieb aufrechterhalten, der die zunehmenden Ansprüche an die Verfügbarkeit der Internetzugänge erfüllt. Nicht selten sind dafür First und Second Level Support rund um die Uhr erforderlich.
- Zunehmende Probleme mit dem klassischen Ansatz der Absicherung des Internetzugangs bleiben ungelöst. Trotz der konsequenten Nutzung einer eigenen Umgebung für die Absicherung des Internetzugangs ist es in den letzten Jahren immer wieder zu Sicherheitsvorfällen durch Internetnutzung gekommen. Dies ist vor allem darauf zurückzuführen, dass die Risiken und Angriffsmuster im Internet immer komplexer werden und vor allem neue Angriffsmuster mit einer im Alleingang betriebenen Sicherheitsumgebung kaum entdeckt werden können.

Und so kommt es, dass viele Unternehmen eine andere Lösung wählen.

### Internet-Sicherheit aus der Cloud

Sowohl Hacker, die es gezielt auf ein Unternehmen abgesehen haben als auch automatisch in großem Maßstab verbreitete Schadprogramme nutzen meistens die

Schwächen und Sicherheitslücken verbreiteter Software wie Betriebssysteme, Browser und Standardanwendungen. Der bisherige Kampf gegen solche Angriffe basierte auf einem reaktiven Ansatz. Sobald ein solches Angriffsmuster bekannt wird, muss man entweder selbst tätig werden oder auf eine entsprechende Reaktion eines Herstellers warten. Ersteres geschieht, indem man zum Beispiel eine neue Regel auf Firewalls oder Proxies einstellt. Schlimmer ist der Fall, in dem eine solche neue Regel nicht möglich ist, weil sie automatisch auch die legitime und erforderliche Nutzung beeinträchtigt. Nicht selten ist man zum Beispiel darauf angewiesen, dass der Browserhersteller durch eine entsprechende Programmierung die Sicherheitslücke schließt.

In der IT-Sicherheitsgemeinde gibt es aber schon seit über zwei Jahrzehnten auch einen anderen Ansatz. Wenn die Nutzergruppe groß genug ist, kommt die Lösung – zum Beispiel bei Einsatz von Open Source – aus der Gemeinde selbst. Und das oft viel schneller als ein einziger Hersteller überhaupt sein kann.

Ein Aspekt dabei ist die Möglichkeit, Open Source Software selbst verändern zu können. Ein anderer Aspekt ist aber auch der Vorteil, der auf die Größe der Gemeinde zurückzuführen ist. Indem viele betroffen sind, suchen entsprechend viele eine Lösung. Sie wird so schneller gefunden.

Zwei Faktoren spielen dabei eine wesentliche Rolle: erstens die Bündelung der IT-Sicherheitskompetenz einer großen Gemeinde und zweitens die erhöhte Wahr-

scheinlichkeit der Entdeckung von Sicherheitslücken durch die Größe der Gemeinde.

Man stelle sich vor, dass viele Unternehmen sich zusammenschließen, ihre Expertise bündeln und sofort nach Bekanntwerden eines Sicherheitsvorfalls irgendwo in einem der Unternehmen eine Lösung herbeiführen. Die Lösung kann weniger komplex sein, zum Beispiel indem man Phishing Mails mit einem neuen Filter auf deren Quelle bekämpft, oder komplexer, zum Beispiel indem man ein Angriffsmuster erkennt und blockiert. So funktioniert übrigens der bewährte Ansatz von Computer Emergency Response Teams (CERTs) schon seit Jahrzehnten.

Nun kann ein Unternehmen dies auch als kommerzielles Angebot gestalten. Es kann eine Art Cloud realisieren, über die der Zugriff vieler Unternehmen auf das Internet geführt wird. Sicherheitskomponenten wären dann in dieser Cloud angesiedelt. Von der Erfahrungen jedes angeschlossenen Unternehmens mit Sicherheitsvorfällen profitieren sofort auch alle anderen. In der großen Cloud werden Angriffsmuster schneller erkannt als in einzelnen Unternehmen.

Das ist die Idee hinter Internet-Sicherheit aus der Cloud, vereinfacht dargestellt in der Abbildung 3.

Wie aus der Abbildung 3 hervorgeht, kann bei direktem Anschluss jedes Standortes an das Internet eine einfache Regel dafür sorgen, dass über diesen Anschluss nur die Security Cloud erreichbar ist. Der Zugriff auf jedes Ziel im Internet erfolgt über diese Security Cloud. Diese muss natür-

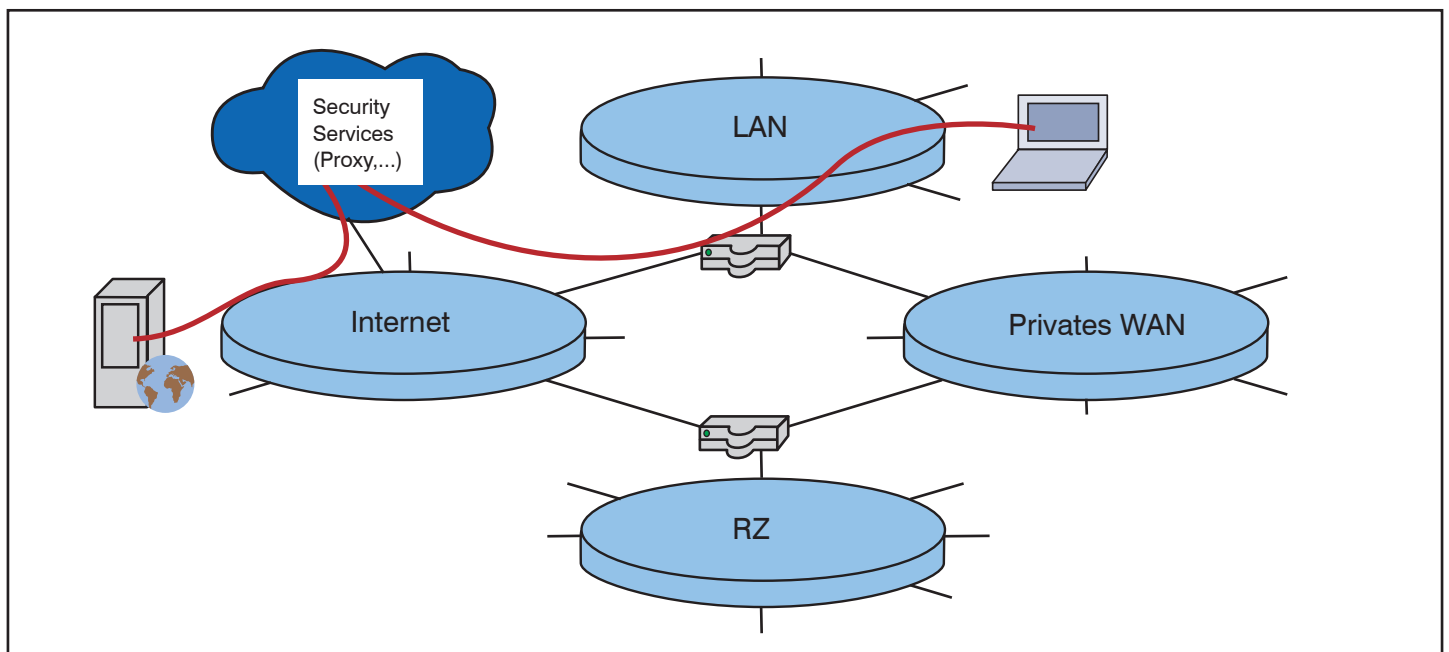


Abbildung 3: Internet-Sicherheit aus der Cloud

## Redesign von WAN- und Internet-Zugängen

lich die entsprechende geografische Verteilung aufweisen. Sonst kommt es zu ungünstigen Übertragungspfaden, die mit zu langen Antwortzeiten verbunden sind. Je mehr Kunden die Cloud nutzen, umso dichter wird in der Regel das PoP-Netz des Cloud-Anbieters sein. Die größere Kundengemeinde hat auch Sicherheitsvorteile, wie bereits erwähnt.

Was für den ausgehenden Internetzugang erst seit wenigen Jahren üblich geworden ist, gibt es für den eingehenden Internetzugang bereits seit fast zwei Jahrzehnten – aber aus anderen Gründen. Content Distribution Networks, kurz CDNs, sind nichts anderes als Clouds, die das Internet überlagern. Sie sorgen dafür, dass der über das Internet erreichbare Inhalt „näher zum Anwender“ verlagert wird. Der Kunde, der einen Konfigurator für sein neues Auto nutzt, greift darauf oft über ein CDN zu. Das CDN ist unter anderem ein Zwischenspeicher für die bunten, schönen, hoch auflösenden Bilder. Diese müssen nicht den langen Weg vom zentralen Server des Automobilherstellers bis zum Kaufinteressenten am anderen Ende der Welt zurücklegen, sondern stehen in dessen Region abrufbereit im CDN, heute sagt man in der Cloud.

Aber die Funktion der Internet Security Cloud ist in erster Linie nicht die Zwischenspeicherung voluminöser Inhalte. Einige führende Anbieter solcher Clouds haben überhaupt keine Caches in ihrer Lösung implementiert. Die Hauptfunktion einer solchen Cloud besteht nämlich darin, Sicherheit und günstige Übertragungswege miteinander zu verbinden.

Von einigen Eigenschaften und Funktionen einer solchen Cloud wollen viele Unternehmen gleichermaßen profitieren. Ein Beispiel hierfür ist die Abwehr von neuen Angriffsmustern. Aber Unternehmen agieren unterschiedlich und haben ihre eigenen Richtlinien. Ein Unternehmen kann seinen Mitarbeitern den Zugriff auf soziale Netzwerke erlauben, während ein anderes vorzieht, einen solchen Zugriff zu unterbinden. Daher muss die Nutzung der Cloud an die Richtlinien und Regeln einzelner Kunden anpassbar sein, am besten über ein kundenspezifisches Administrationsportal.

Ist eine Internet Security Cloud die beste Lösung für alle Unternehmen, eine Art Allheilmittel? Die Antwort ist ein eindeutiges Nein. Nicht jedes Unternehmen ist mit der adäquaten Absicherung des selbst betriebenen Internetzugangs überfordert. Nicht jedes Unternehmen hat weltweit verteilte Standorte, die von der Cloud profitieren würden. Und einige Bedenken gegen die Nutzung einer solchen Cloud sind ernst zu nehmen:

- Unabhängig davon, ob man die Authentisierungsdaten für einzelne Anwender im eigenen Netz hält oder in der Cloud, ist der Cloud-Anbieter in der Lage, einiges über die Kommunikationspartner und Internet-Datenströme seiner Kunden in Erfahrung zu bringen. Ein ISP kann das auch. Aber der ISP unterliegt möglicherweise anders als der Betreiber der weltweiten Cloud der Gesetzgebung des eigenen Landes.
- Mit der Cloud-Nutzung sind Kosten in der Regel proportional zur Anzahl der Anwender verbunden. Diese können höher als die Kosten für eine eigene Lösung sein, je nach Szenario.
- In der Fehlersuche ist man auf die kompetente und schlagfertige Mitwirkung des Cloud-Anbieters angewiesen.

### Neue Ansätze zur Erhöhung der WAN-Verfügbarkeit

Damit nicht der Eindruck entsteht, dass der Bedarf am Redesign von WAN- und Internet-Zugängen auf Szenarien beschränkt ist, in denen die Nutzung einer Internet Security Cloud sinnvoll ist, müssen wir hier auch auf neue Ansätze zur Erhöhung der WAN-Verfügbarkeit eingehen.

Viele Unternehmen sind mit der Verfügbarkeit ihres privaten WAN trotz abgeschlossener SLAs nicht zufrieden. Bei Verletzung von SLAs muss der Provider bestenfalls eine Vertragsstrafe nur in Höhe eines Bruchteils des Produktivitätsausfalls zahlen, der mit einem WAN-Ausfall einhergeht. Selbst wenn der Provider das SLA penibel einhält, ist angesichts der wachsenden Bedeutung des WAN für Unternehmen jeder WAN-Ausfall ein Ärgernis. Jede wesentliche Erhöhung der Service-

Qualität, zum Beispiel Erhöhung der prozentualen Verfügbarkeit oder Verkürzung der Obergrenzen für die Entstörungszeiten, ist meistens mit erheblichen WAN-Mehrkosten verbunden.

Deshalb implementieren immer mehr Unternehmen neue Ansätze zur Erhöhung der WAN-Verfügbarkeit. Diese Ansätze basieren darauf, dass das Internet in allen Ländern immer leistungsfähiger und als Bestandteil der kritischen Infrastruktur immer zuverlässiger werden muss. Ergänzt man das private WAN um davon unabhängige Übertragungswege über das Internet, bekommt man ein Gesamtkonstrukt, das eine höhere Verfügbarkeit aufweist als jeder einzelne Zugang zum WAN oder Internet.

Abbildung 4 stellt diesen Ansatz dar. Dabei wird ein Standort-Netz (Local Area Network, LAN) sowohl mit dem privaten WAN als auch mit dem Internet verbunden. Über beides – privates WAN und Internet – kann ein Standort-LAN mit dem Rechenzentrum (RZ) des Unternehmens verbunden werden. Dieses Konstrukt mit unabhängigen parallelen Wegen weist in der Regel eine höhere Verfügbarkeit auf als jeder einzelne der Pfade. Die für den Anschluss des Standortnetzes an die beiden Weitverkehrsnetze eingesetzten Komponenten müssen folgende Funktionen erfüllen:

- VPN: Die Komponenten müssen ein Virtual Private Network über das Internet terminieren.
- FW: Eine (wenn auch rudimentäre) Firewall-Funktion ist erforderlich, um das Standortnetz vor Angriffen aus dem Internet zu schützen.
- PBR: Policy-Based Routing kann ermöglichen, dass Kommunikationsströ-

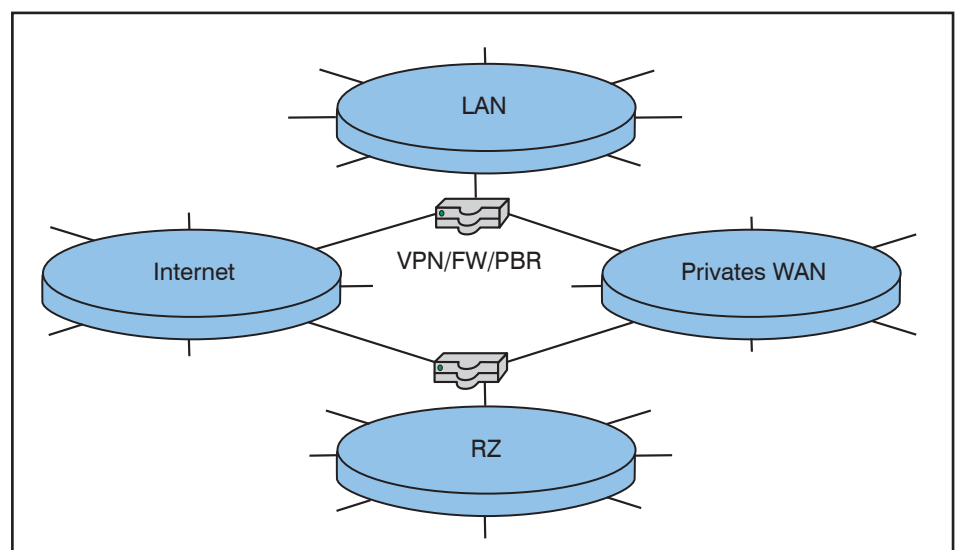


Abbildung 4: Kombination aus Internet und privatem WAN

## Redesign von WAN- und Internet-Zugängen

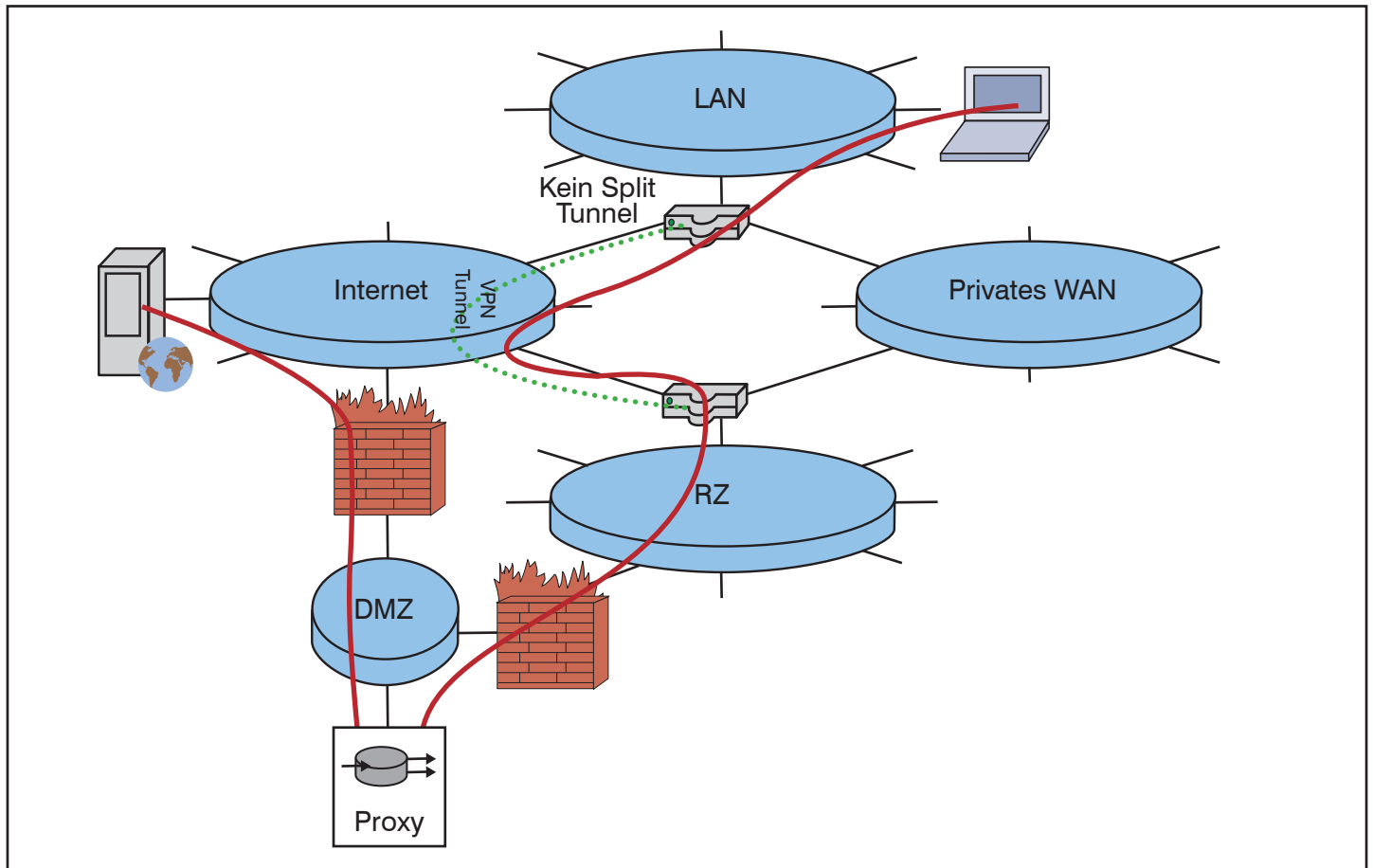


Abbildung 5: VPN-Szenario ohne Split Tunnel

me verschiedener Anwendungen auf die beiden Übertragungswege verteilt werden. So kann zum Beispiel die Übertragung von E-Mails über das Internet-VPN das private WAN entlasten.

Nachteilig in der Konstellation gemäß Abbildung 4 sind vor allem die folgenden Umstände:

- Man braucht neue Komponenten mit den genannten Funktionen und Eigenschaften.
- Das Management des Netzes wird komplexer.

Folgt man dem in der Abbildung 4 dargestellten Ansatz, kommt man dafür in den Genuss folgender Vorteile:

- Erhöhung der Gesamtverfügbarkeit der Anbindung eines Standortnetzes
- Entlastung des privaten WAN, in dem Übertragungskapazität in der Regel wesentlich teurer als im Internet ist
- Beschleunigung der Antwortzeiten von Anwendungen im privaten WAN, weil dieses ein Stück weit entlastet wird

- Erhöhung der WAN-Sicherheit, denn die eingesetzten Komponenten können neben dem Internet- auch den WAN-Verkehr verschlüsseln

- Reduzierung der Kosten für das private WAN, indem man statt der bisher hohen SLAs und der doppelten WAN-Anbindung eine preiswertere einfache Anbindung einsetzt, die durch die Internet-Verbindung abgesichert wird

- Möglichkeit des direkten Zugriffs auf das Internet zum Beispiel durch Nutzung einer Internet Security Cloud

**Split Tunnel: Ja oder Nein?**

Letzteres erfordert jedoch die Abkehr von dem in vielen Unternehmen etablierten Prinzip, das im Zusammenhang mit Internet-VPN keinen sogenannten Split Tunnel vorsieht. Die Abneigung gegen den Split Tunnel ist auf Sicherheitsbedenken zurückzuführen. Ein Internet-Zugang gilt als relativ sicher, wenn darüber ausschließlich ein VPN-Tunnel gebildet wird. Am VPN-Tunnel vorbei erlaubt der VPN Gateway keinerlei Kommunikation, wie in der Abbildung 5 dargestellt. In diesem Fall kann es keinen direkten Zugriff aus dem Stand-

ortnetz auf das Internet geben. Der „Ausbruch“ (Break-out) in das Internet ist nur am zentralen Ende des VPN-Tunnels möglich, wo der Internet-Zugriff über eine Sicherheitsumgebung geführt wird.

Jahrelang war die in der Abbildung 5 dargestellte Konstellation die favorisierte Variante in der Gestaltung von Internet-VPNs. Dagegen ist nach wie vor nichts einzuwenden, wenn sämtlicher Zugriff auf das Internet über zentrale oder regionale Anschlüsse erfolgt. Soll aber ein lokaler Internetanschluss auch für Zugriffe auf fremde Inhalte im Internet genutzt werden, ohne dass der möglicherweise lange Umweg über den zentralen oder regionalen Internetanschluss genommen werden soll, muss der direkte Zugriff am VPN-Tunnel vorbei ermöglicht werden.

Dies ist in der Abbildung 6 dargestellt. In dieser Konstellation dient der Internet-Anschluss des Standortnetzes zwei Zwecken: zum einen der Nutzung durch den VPN-Tunnel, der den Standort mit den Ressourcen im RZ des Unternehmens verbindet, und zum anderen dem direkten ausgehenden Zugriff des Standorts auf das Internet. Abbildung 6 zeigt ein Split-Tunnel-Szenario mit eigenen lokalen Si-

## Redesign von WAN- und Internet-Zugängen

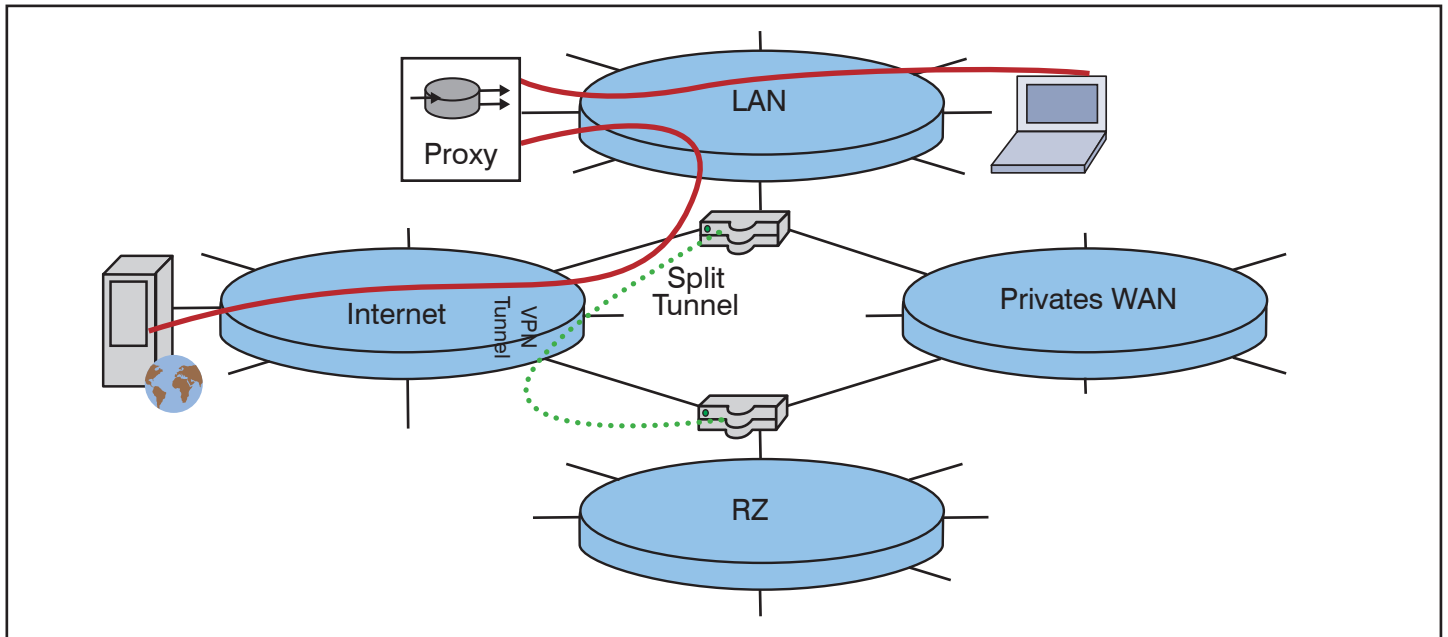


Abbildung 6: VPN-Szenario mit Split Tunnel

cherheitskomponenten wie Proxies. Das Prinzip bleibt aber dasselbe, wenn man statt einer eigenen Sicherheitsumgebung die entsprechenden Funktionen in einer Internet Security Cloud nutzt.

**Fazit**

Es gibt neue Entwicklungen im Internet, die ein Redesign des Gesamtkonstrukts aus WAN- und Internet-Zugängen gleichzeitig erzwingen und ermöglichen. Einerseits

wächst der Internetverkehr so stark, dass es oft nicht mehr wirtschaftlich ist, dafür teure Kapazitäten im privaten WAN zu belegen. Diese sollten Applikationen vorbehalten bleiben, die anders als der Internetzugriff meistens ein moderates Verkehrsvolumen aufweisen, aber so wichtig sind, dass man dafür hochverfügbare, mit SLAs abgesicherte Netzstrukturen braucht.

Andererseits wird das Internet zunehmend zu einer kritischen Infrastruktur, die immer

leistungsfähiger und zuverlässiger werden muss. Es liegt nahe, diese Infrastruktur auch für die standortübergreifende Kommunikation des eigenen Unternehmens zu nutzen.

Keine zeitgemäße Planung der standortübergreifenden Kommunikation kann daher WAN- und Internet-Zugänge isoliert betrachten, wie es in vielen Unternehmen jahrelang üblich war. Die beiden Infrastrukturen werden immer mehr zu Bestandteilen einer Gesamtstruktur.

**Intensiv-Seminar****Sommerschule 2016 -****Intensiv-Update auf den neuesten Stand der Netzwerktechnik****27.06. - 01.07.16 in Aachen**

Das technologische Umfeld von Netzwerken befindet sich in einem der intensivsten Änderungsprozesse der letzten 20 Jahre. Das betrifft das Rechenzentrum, neue IT-Architekturen, neue Client-Technologien bis hin zu Unified Communications. Hand in Hand mit dem Bedarf ändern sich Netzwerk-Technologien selber. Zukunftsorientiertes und wirtschaftlich optimales Design muss dieses Gesamtbild berücksichtigen. Die ComConsult Sommerschule 2016 analysiert und diskutiert diese Änderungen und ihre Auswirkungen speziell auf die Netzwerk-Infrastrukturen.

Top Experten haben das Programm der Sommerschule gestaltet und systematisch die Erfahrungen laufender Projekte und neuester Technologie-Entwicklungen eingearbeitet. Treffen Sie einige der besten Experten, die die deutsche Netzwerk-Landschaft zu bieten hat.

Preis: € 2.290,- netto\*

\*Frühbucherpreis bis zum 31.05.16 - dann regulärer Preis € 2.490,- netto



Buchen Sie über unsere Web-Seite

[www.comconsult-akademie.de](http://www.comconsult-akademie.de)

## ComConsult Veranstaltungskalender

**Lokale Netze für Einsteiger, 09.05.-13.05.16 in Aachen**

Garantietermin

Dieses Seminar vermittelt kompakt und intensiv innerhalb von 5 Tagen die Grundprinzipien des Aufbaus und der Arbeitsweise Lokaler Netzwerke. Dabei werden sowohl die notwendigen theoretischen Hintergrundkenntnisse vermittelt als auch der praktische Aufbau und der Betrieb eines LANs erläutert. Ausgehend von einer Darstellung von Themen der Verkabelung und der grundlegenden Übertragungsprotokolle werden die wichtigen Zusammenhänge zwischen der Arbeitsweise von Switch-Systemen, den darauf aufsetzenden Verfahren und der Anbindung von PCs und Servern systematisch erklärt.

Preis: € 2.490,-- netto

**Trouble Shooting in vernetzten Infrastrukturen, 10.05.-13.05.16 in Aachen**

Garantietermin

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. Einer Verwendung selbst mitgebrachter Analyse-Software, mit deren Bedienung der Teilnehmer vertraut ist, steht nichts im Wege.

Preis: € 2.290,-- netto

**Mobile Device Management: Technik und juristische Rahmenbedingungen, 11.05.-12.05.16 in Bonn**

Garantietermin

Die Anforderung an IT-Abteilungen, mobile (und teilweise auch privat genutzte) Geräte wie Smartphones und Tablets in das Firmennetz einzubinden, wächst rasant. Dieses Seminar erläutert detailliert die technischen und rechtlichen Maßnahmen, um einerseits die IT-Sicherheit zu gewährleisten und auf der anderen Seite Verstöße gegen Datenschutzrecht, Persönlichkeitsrecht und Betriebsverfassungsrecht auszuschließen.

Preis: € 1.590,-- netto

**Voice und Video im WAN, 30.05.16 in Köln**

Wie kann die Übertragung von Sprache und Video im WAN optimiert werden ohne andere Anwendungen zu gefährden? Wie gehen wir mit einem immer größeren Anteil und vor allem der Integration von Video in wesentliche Geschäftsprozesse um? Neue Kollaborations-Lösungen erhöhen zudem den Druck auf die Infrastrukturen. Verkehrslasten werden dabei immer dynamischer und einfache statische Regeln wie traditionelles QoS stoßen an ihre Grenzen. Die Sonderveranstaltung beleuchtet den Status Quo, die Zukunftsaussichten, mögliche Optionen und eventuellen Investitionsbedarf für den sicheren Betrieb aller Anwendungen.

Preis: € 1.090,-- netto

**Verkabelungssysteme für Lokale Netze, alles standardisiert, alles klar?, 30.05.-31.05.16 in Köln**

Dieses Seminar erklärt praxisnah und herstellerneutral wie Sie hohe Qualität, Verfügbarkeit und lange Nutzbarkeit bei der Planung und im Betrieb einer Verkabelungs-Lösung erreichen. Die Bausteine einer Verkabelung werden vorgestellt und zu einem handhabbaren Gesamtsystem kombiniert. Lernen Sie wo sich gute von schlechten Lösungen unterscheiden. Dabei werden die Normen diskutiert und die praktische Handhabung der Normungsvorgaben erklärt. Der 2. Tag widmet sich der konkreten Durchführung einer Planung in kleinen Übungsgruppen.

Preis: € 1.430,-- netto

**IP-Telefonie und Unified Communications erfolgreich planen und umsetzen, 30.05.-01.06.16 in Köln**

Dieses Seminar vermittelt alle notwendigen Projektschritte zu einer erfolgreichen Umsetzung von VoIP Projekten. Diese erstrecken sich über die Einsatz- und Migrations-Szenarien, die einsetzbaren Basis-Technologien und Komponenten und die erweiterten TK-Anwendungen wie IVR, UM oder UC. Es werden Bewertungskriterien für eine TK-Lösung und eine Übersicht über den bestehenden TK-Markt mit allen etablierten Hersteller vorgestellt.

Preis: € 1.890,-- netto

**Netzwerk-Design für Enterprise Netzwerke, 06.06.-08.06.16 in Berlin**

LAN-Technik wird im Moment neu erfunden. Neue Anforderungen erfordern neue Lösungen. Neue Fabric-Konzepte, ein Umdenken bei VLAN-Technik, eine Neupositionierung von QoS und neue Nutzungsformen im Rahmen von Audio-/Video-Bridging sind herausragende Beispiele. Das Seminar zum Thema Netzwerk-Design für Enterprise Netzwerke erklärt, was im Moment passiert und wie Sie sich auf die Zukunft vorbereiten. Es geht auf RZ- und Campus Design-Alternativen im Zeitalter neuer Layer-2 Technologien wie Fabrics, Multichassis-Link Aggregation, Shortest Path Bridging und Hochgeschwindigkeits-Datenraten von 10/40/100 Gbit ein. Darüber hinaus werden Priorisierungs-Techniken wie AVB und DCB sowie der sinnfällige Einsatz von VLAN-Technik und VLAN-Overlays behandelt.

Preis: € 1.890,-- netto

**Interne Absicherung der IT-Infrastruktur, 06.06.-07.06.16 in Berlin**

Garantietermin

In diesem Seminar lernen Sie wie man die Sicherheit von LAN, WAN, Endgeräten, RZ-Bereichen, Servern und SAN erreicht. Konkrete Beispiele aus der Praxis zeigen den Weg zu einer erfolgreichen IT-Sicherheits-Lösung.

Preis: € 1.590,-- netto

**IT-Compliance und IT-Security für Nichtjuristen, 13.06.16 in Bonn**

Die Veranstaltung beinhaltet einen vertiefenden Überblick über die zunehmenden Herausforderungen der Compliance im IT-Bereich. Bei den Teilnehmern soll ein Bewusstsein für die Compliance-Anforderungen an Unternehmen geweckt und Haftungsrisiken für den Fall der Non-Compliance skizziert werden. Schließlich werden praktische Hinweise zur Umsetzung von Compliance-Pflichten vorgestellt.

Preis: € 1.090,-- netto

## Zertifizierungen

### ComConsult Certified Network Engineer

#### Lokale Netze

09.05. - 13.05.16 in Aachen  
19.09. - 23.09.16 in Aachen

#### TCP/IP-Netze erfolgreich betreiben

20.06. - 22.06.16 in Bonn  
24.10. - 26.10.16 in Bonn

#### Internetworking

04.07. - 08.07.16 in Aachen  
14.11. - 18.11.16 in Aachen

Paketpreis für zwei 5-tägige und ein 3-tägiges Intensiv-Seminar € 6.180,-- netto (Einzelpreise: € 2.490,-- netto bzw. 1.890,-- netto)

### ComConsult Certified Trouble Shooter

#### Trouble Shooting in vernetzten Infrastrukturen

10.05. - 13.05.16 in Aachen  
27.09. - 30.09.16 in Aachen

#### Trouble Shooting für Netzwerk-Anwendungen

14.06. - 17.06.16 in Aachen  
15.11. - 18.11.16 in Aachen

Paketpreis für beide Seminare inklusive Prüfung € 4.280,-- netto  
(Seminar-Einzelpreis € 2.290,-- netto , mit Prüfung € 2.470,-- netto)

### ComConsult Certified Voice Engineer

#### IP-Telefonie und Unified Communications erfolgreich planen und umsetzen

30.05. - 01.06.16 in Köln  
24.10. - 26.10.16 in Frankfurt

#### Session Initiation Protocol Basis-Technologie der IP-Telefonie

20.06. - 22.06.16 in Bonn  
09.11. - 11.11.16 in Berlin

#### Umfassende Absicherung von Voice over IP und Unified Communications

04.07. - 06.07.16 in Stuttgart  
28.11. - 30.11.16 in Bonn

#### Optionales Einsteiger-Seminar: IP-Wissen für TK-Mitarbeiter

19.09. - 20.09.16 in Frankfurt

Wir empfehlen die Teilnahme an diesem Seminar "IP-Wissen für TK-Mitarbeiter" all jenen, die die Prüfung zum ComConsult Certified Voice Engineer anstreben, ganz besonders aber den Teilnehmern, die bisher wenig bis kein Netzwerk Know How, insbesondere TCP/IP, DNS, SIP usw., vorweisen können.

Basis-Paket: Beinhaltet die drei Basis-Seminare  
Grundpreis: € 5.100,-- netto statt € 5.670,-- netto  
Optionales Einsteigerseminar: Aufpreis € 1.190,-- netto statt € 1.590,-- netto

## Impressum

Verlag:  
ComConsult Research Ltd.  
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](mailto:insider@comconsult-akademie.de)  
<http://www.comconsult-research.de>

Herausgeber und verantwortlich  
im Sinne des Presserechts:  
Dr. Jürgen Suppan  
Chefredakteur: Dr. Jürgen Suppan  
Erscheinungsweise: Monatlich,  
12 Ausgaben im Jahr

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

Für unverlangte eingesandte Manuskripte  
wird keine Haftung übernommen  
Nachdruck, auch auszugsweise  
nur mit Genehmigung des Verlages  
© ComConsult Research