ComConsult Research

Der Netzwerk Insider

Oktober 2013

Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

Trunk-Verkabelungen im Rechenzentrum, Fluch oder Segen?

von Dipl.-Ing. Hartmut Kell

Anforderungen, im Rechenzentrum Datenraten von 40 Gbit/s und mehr bereitzustellen zu können führen zwangsläufig zu der Pflicht des Verkabelungsplaners, sich zumindest im Bereich der Glasfaserübertragung mit scheinbar neuen Verkabelungslösungen wie z.B. Mehrfasertechniken auseinanderzusetzen. Für den Fall einer unmittelbar anstehenden Einführung von 40 Gbit/s über Multimodefaser gibt es keinen Weg daran vorbei. Wie ist es aber bei einer neuen RZ-Verkabelung, die zunächst nur für maximal 10 Gbit/s genutzt werden soll? Sollte man diese bereits für die nächsten Skalierungsschritte vorbereiten, kann man das oder muss man sich auf Neuverkabelungen für jede neue Datenrate einstellen?

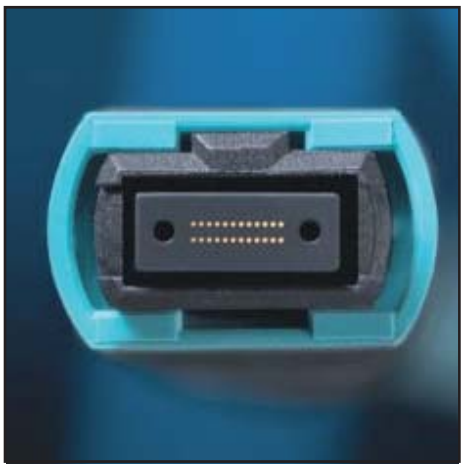


Bild: RdM

Der nachfolgende Artikel beschäftigt sich mit Glasfaserverkabelungstechniken, die diese Einführung vereinfachen sollen und den Vorteil haben, deutlich platzsparender in Punkto Kabelmenge wie auch 19“-Montagefläche zu sein.

weiter auf Seite 14

Zweitthema

Gefahr durch IPv6?

von Markus Schaub

Um das Fazit des Artikels gleich vorweg zu nehmen: wer IPv6 ignoriert lebt gefährlich. Wer nun glaubt, dass professionelles Hackerwerkzeug nötig ist, um mittels IPv6 einen Man in the Middle Angriff zu fahren, irrt gewaltig. Alles, was man braucht, ist eine Standard-Linux-Distribution und ein wenig Ahnung. Alles andere liefern die Hersteller der gängigen Betriebssysteme und die IETF frei Haus.

Im Folgenden werden zwei Bereiche betrachtet, in denen schon heute IPv6 Gefahren lauern: zum einen das LAN, zum anderen die DMZ. Der Unterschied ist hierbei die Gefahrenquelle: im LAN entsteht sie durch die aktivierten IPv6 Stacks moderner Betriebssysteme, selbst wenn eigentlich kein IPv6 im Campus betrieben wird; bei der DMZ existiert sie, sobald man einen einzigen Server (bspw. das Web-Portal) auf Dual-IP umstellt.

weiter Seite 22

Geleit

Stirbt das Kabel mit dem Desktop?

von Dr. Jürgen Suppan

ab Seite 2

Standpunkt

Virtualisierte Sicherheitskomponenten als Konsequenz moderner RZ-Konzepte!?

ab Seite 20

Aktuelle Kongresse

Rechenzentrum Infrastruktur-Redesign Forum 2013
Wireless Forum 2013
TK-, UC- und Videokonferenzforum 2013

ab Seite 4

Kongress

IPv6-Forum 2013

auf Seite 29

Intensiv-Update

Winterschule 2013

auf Seite 21

Zum Geleit

Stirbt das Kabel mit dem Desktop?

Gegen Ende des Jahres werden erstmals mehr Tablets verkauft als Desktop-und Laptop-Systeme zusammen. Intel konzentriert seine Chipentwicklung immer mehr auf Mobilsysteme, der neue Broadwell 14 nm Prozessor wurde erst gar nicht mehr für Desktop-Systeme vorgestellt. Microsoft sieht seine Zukunft bei 2-in-1-Systemen. Gleichzeitig bieten neue WLAN-Standards mit maximal 7 Gbit/s Bandbreite erstmals auch Netto-Kapazitäten, die der bisherigen Kabel-Versorgung entsprechen. Ist das Kabel zum Endgerät damit tot? Mit welchen Infrastrukturen versorgen wir denn unsere Gebäude in Zukunft? (siehe Abbildung 1)

Die Netzwerke in unseren Gebäuden haben eine zentrale Aufgabe: die Verbindung von Endgeräten mit Servern und Applikationen. Seit 1999 steht hier die Netzwerk-Technik still. Gigabit-Ethernet hat sich bewährt und als ausreichend erwiesen. Dementsprechend sind die Netzwerke, die diese Versorgung leisten, inzwischen so langweilig, dass sie auch als Commodity ausgesourced werden könnten. (siehe Abbildung 2)

Nun verändert sich die Endgeräte-Technik dramatisch. Es fing langsam an, aber inzwischen stehen wir vor einer Lawine, die alles mitreißt, was sich in den Weg stellt. Wurde bei der Vorstellung des ersten iPads noch diskutiert was man wohl mit diesem Gerät anfangen sollte, so sprechen Anbieter wie Intel, Apple, Google und auch Microsoft inzwischen von Desktop Performance bei der Hardware-Ausstattung dieser Geräte (siehe Intel Bay Trail, Apple A7). Tatsächlich ist die Situation für Intel und auch Microsoft durchaus ernst. Bei der Vorstellung des iPhones hat Nokia noch geschmunzelt, nun wurden die Überbleibsel in einer Notaktion von Microsoft gekauft. Dies hat 5 Jahre gedauert. Über 90% aller verkauften Tablet-Computer arbeiten mit Googles Android oder Apples IOS. Gleichzeitig ist eine Versorgungs-Infrastruktur in der Cloud entstanden, die auch auf der Applikations-Seite Microsoft überflüssig macht. Die Surface-Geräte der ersten Generation, Microsofts Antwort auf diese Entwicklung, waren Versager. Entweder waren keine Applikationen verfügbar (RT) oder die Batterie-Leistung war indiskutabel (Pro). Nun liegt die zweite Generation vor. RT macht weiterhin keinen Sinn, aber beim Surface Pro haben wir vermutlich zum ersten Mal einen ernstzunehmenden Konkurrenten für die Platzhirsche. Trotzdem ist die Zukunft ungewiss. Intel und Microsoft suchen ihr Heil in 2-in-1-Systemen, also Systemen, die sowohl Laptop als auch Tablet sind. Auf dem gerade beendeten Intel Developer Forum IDF 2013 wurde diese Geräte-Gattung gepuscht wie keine andere. Und das nicht ohne Grund. Floppt diese Geräte-Idee, dann stehen Intel und Microsoft auf einer schiefen Ebene mit dem Weg nach unten. Aus Microsoft-Sicht hängt alles an der Akzeptanz von Windows 8.1, also an der Frage, ob die kombinierte Nutzung von Maus und Gesten-Steuerung besser ist als eine reine Gestensteuerung. In jedem Fall war die Lage in den letzten 20 Jahren nie so gefährlich für Microsoft wie jetzt. Google und das Cloud-Imperium aus vielen neuen und sehr kreativen Anwendungen entwickeln sich so schnell und dynamisch, dass nicht viel Zeit für Fehlentwicklungen bleibt. (siehe Abbildung 3)

Wie immer man diese dramatische und durchaus spannende Entwicklung einschätzt, eine zentrale Komponente ist in allen denkbaren Szenarien identisch: das zukünftige Endgerät wird mit hoher Wahrscheinlichkeit über eine WLAN-Schnittstelle in Netzwerke integriert. Die Frage nach

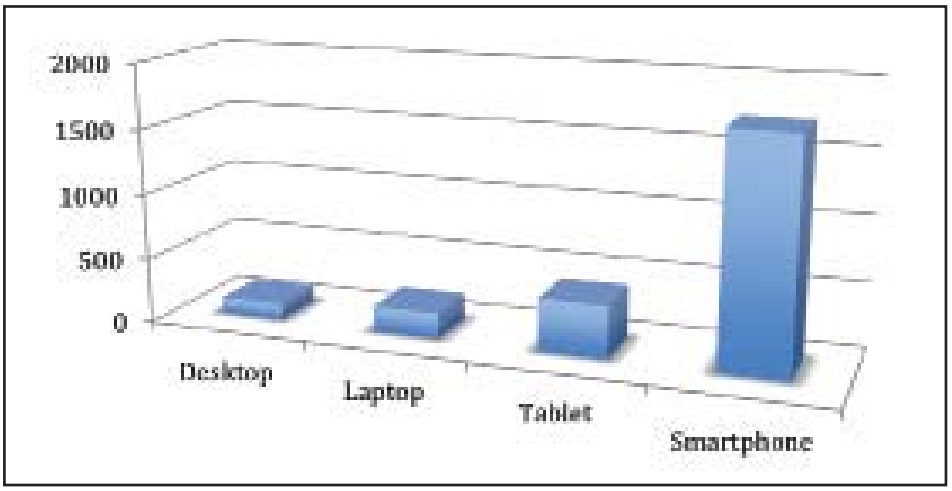


Abbildung 1: Endgeräte Markt im Jahr 2017 Quelle: IDC

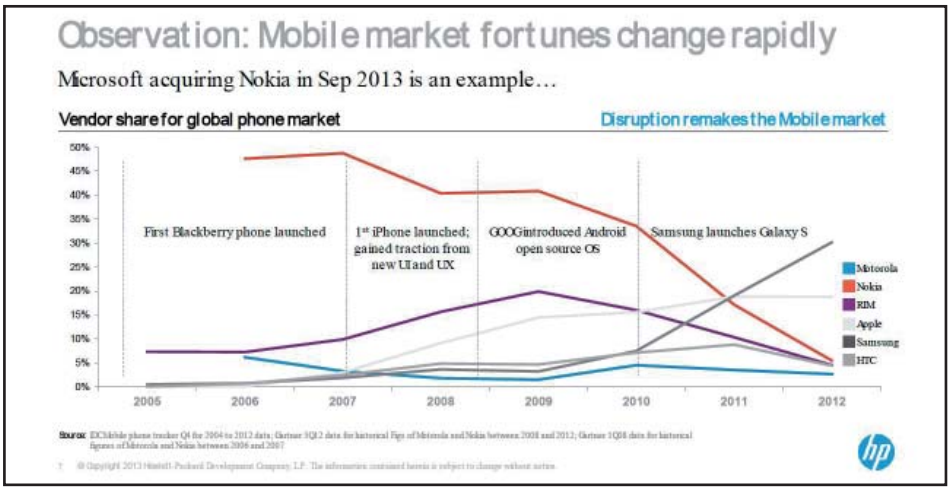


Abbildung 2: Innovation als Unternehmens-Killer Quelle: HP/ IDF 2013

Stirbt das Kabel mit dem Desktop?

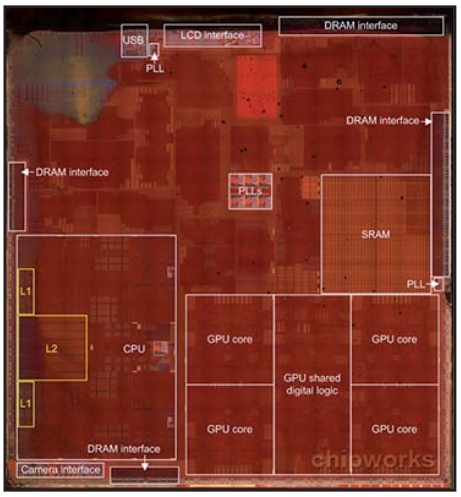


Abbildung 3: Abkehr von der traditionellen CPU, hin zum System on a Chip, ist das unsere Zukunft? Hier Apple A7 Quelle: Chipworks

dem Kabel stellt sich gar nicht mehr. Theoretisch könnte es sein, dass auch alle zukünftigen Ansätze eine Form von Docking-Station wie die gerade von Dell für IEEE 802.11ad vorgestellte beinhalten werden. Dann kann die Integration weiterhin über das Kabel erfolgen. Auch bei Apple ist dies mit den Thunderbolt-Docking-Stations für die Laptops weiterhin eine Option. Aber es wäre sehr unrealistisch, wenn man den Funkanteil in der zukünftigen Versorgung unterschätzen würde. Was wäre denn der Best-Case aus der Sicht des Kabels? Nun ganz einfach, dass beide Infrastrukturen in vollem Umfang vorhanden sind. Eine Zukunft ohne eine flächendeckende und leistungsfähige WLAN-Versorgung wäre bei der aktuellen Entwicklung sehr unrealistisch. Wenn aber WLAN in jedem Fall gebraucht wird, wäre dann die totale Orientierung an einer Funkversorgung nicht der naheliegende Weg?

Zur Beantwortung dieser Frage muss man in die Details der neuen Funkstandards IEEE 802.11ac und ad einsteigen. Und die haben es in sich. Das sehr gute und hochgelobte Video von Dr. Hoff zu diesem Thema bei ComConsult-Study.tv stellt die Details vor und macht klar wie groß der Schritt in diese Technologien ist. (siehe Abbildung 4)

Das Problem in der Gebäudeplanung mit beiden WLAN-Standards lässt sich auf einige Kernfakten beschränken:

- Die hohe Bandbreite von 11ac lässt sich nur mit einer signifikant höheren Anzahl von Access-Punkten bereitstellen. Wir sprechen dabei mindestens von einer Verdopplung, im Maximalfall von einer Vervierfachung.

Abbildung 4: Gigabit-WLANs: Konsequenzen für das Design, Dr. Simon Hoff analysiert in diesem hochaktuellen Video bei ComConsult-Study.tv wohin der Weg in die Zukunft geht

- IEEE 802.11ad kann im 60 GHz-Band nur sehr kleine Zellen umsetzen, die dann aber ideal für lokale Busverlängerungen zur Integration von Bildschirmen und Peripherie geeignet sind. Pro ein oder zwei Arbeitsplätze oder anders formuliert alle 10 bis 20 qm kann mit einem Access-Punkt kalkuliert werden.

- Die traditionellen Controller-basierten WLAN-Architekturen, die alle Datenströme durch einen zentralen Controller führen, sind so nicht mehr benutzbar. Neue Ansätze sind erforderlich und auch von den führenden Herstellern vorgestellt worden. Spannenderweise haben die Hersteller sehr unterschiedliche Wege gewählt. (siehe Abbildung 5)

Damit sind wir für eine zukunftsorientierte flächendeckende WLAN-Versorgung bei zwei entscheidenden Punkten:

- Die Kosten der Gesamtlösung werden direkt von den Kosten eines Access-Punktes getragen. Auf keinen Fall kann diese Entwicklung auf dem heutigen Preisniveau erfolgen. Hier haben wir aus den Labors einiger führender Hersteller aber durchaus die Botschaft, dass man für derartige Designs in Kombination mit einem deutlich höheren Bedarf auch mit einem dramatisch niedrigeren Preis rechnet (bis zu 90% unter dem heutigen Niveau).

- Die vielen Access-Punkte brauchen eine Kabelversorgung. Je mehr Access-Punkte wir brauchen desto mehr Kabel brauchen wir. Die zentrale Frage ist, ob wir hier eventuell von denselben Kabeln sprechen, die wir für eine Desktop-Versorgung bräuchten. Ob also in Zukunft die heute passive Dose durch einen aktiven Access-Punkt ersetzt würde. Es gibt einige funktechnische Überlegungen, die gegen diese Annahme sprechen. Mindestens bei 802.11ad sollten keine Objekte zwischen AP und Endsystem sein. Die Frage ist also wo in Zukunft die Access-Punkte angeordnet wären.

- Aus heutiger Sicht würde man zumindest in den ersten Jahren bei Gigabit-Versorgungen für die Access-Punkte bleiben. Danach würden vermutlich neue Produkte zur Verfügung stehen, die auch 10 Gigabit auf Twisted Pair zusammen mit der notwendigen Stromversorgung leisten würden (die Normung dafür hat gerade erst begonnen, hier muss abgewartet werden).

Ist an dieser Stelle eine klare Schlussfolgerung möglich? Ist das heutige Kabel damit gestorben und Friede seiner Asche? Es spricht einiges dafür, dass die Zukunft im WLAN liegt. Die Frage ist nur was das im Detail bedeutet. Das betrifft sowohl das Endgerät und die IT-Architektur zur Versorgung des Endgeräts mit Applikationen und Daten als auch die Frage der Planung von Gigabit WLANs. Und was machen Unternehmen, die gerade mit der Planung neuer Gebäude angefangen haben?

Wir greifen diese zentralen und wichtigen Themen in unserem ComConsult Rechenzentrum Infrastruktur-Redesign Forum 2013, in unserem ComConsult Wireless Forum und in der Winterschule 2013 auf.

Ihr
Dr. Jürgen Suppan

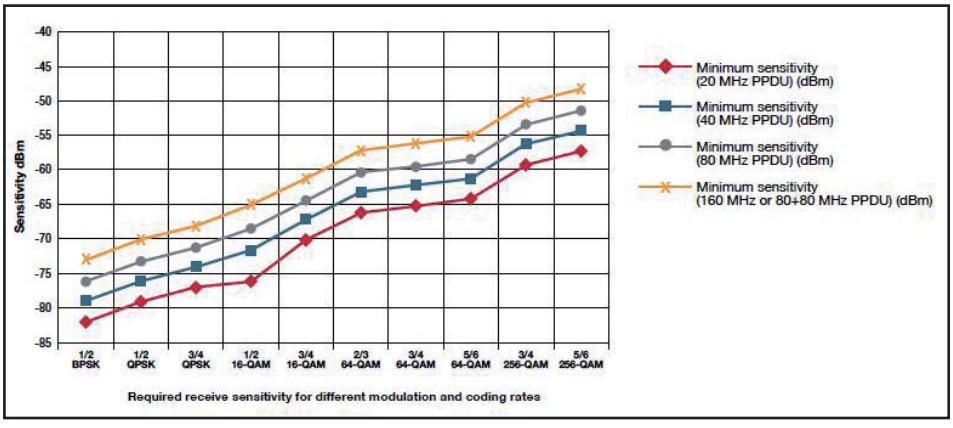


Abbildung 5: Mindest-Empfindlichkeit in der Zellplanung von 11ac Quelle: Aruba

Aktueller Kongress

ComConsult Rechenzentrum Infrastruktur-Redesign Forum 2013

11.11. - 14.11.13 in Düsseldorf

Die ComConsult Akademie veranstaltet vom 11.11. bis 14.11.13 ihr "ComConsult Rechenzentrum Infrastruktur-Redesign Forum 2013" in Düsseldorf.

Das ComConsult RZ-Forum 2013 analysiert die neuesten Entwicklungen im RZ-Bereich und zeigt auf wie die verschiedenen Technologie-Bereiche harmonisch und wirtschaftlich zu einer Gesamt-Architektur integriert werden können. Der Fokus liegt dabei auf:

- Betriebsoptimierung und Katastrophenvorhersorge
- Integration mobiler Endgeräte
- Nutzwert-Analyse Cloud-Services
- Integration neuer Technologien zu einer harmonischen Gesamt-Architektur

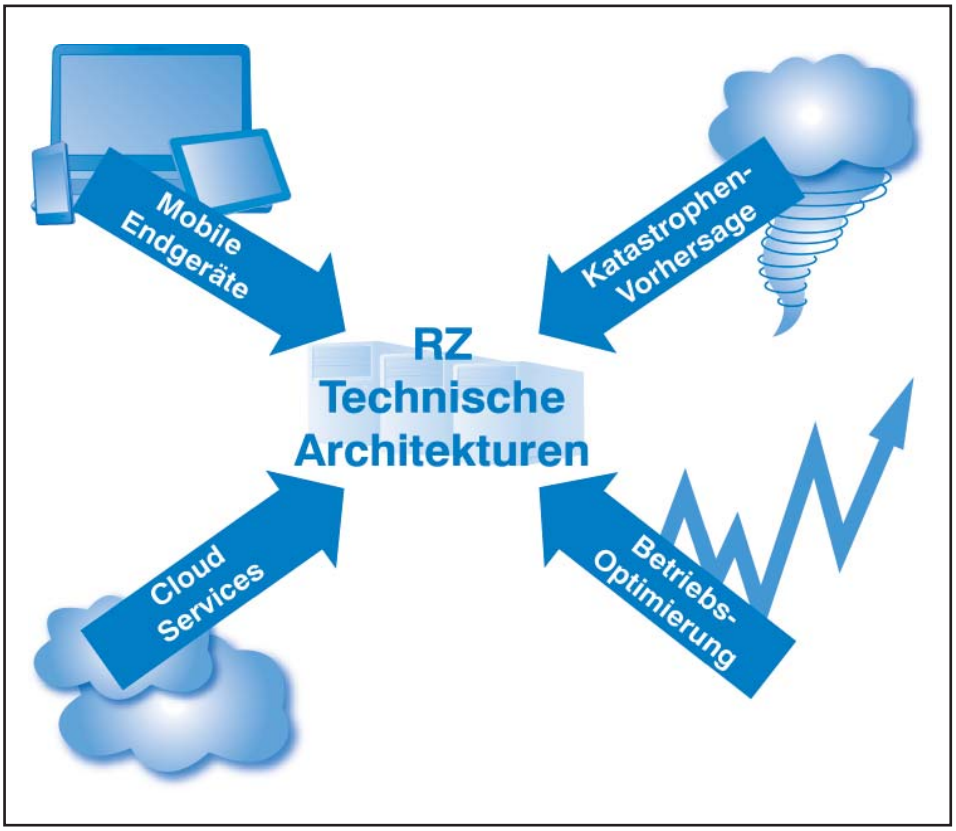
Das Forum ist in folgende inhaltliche Blöcke unterteilt:

Keynotes: Top-Experten bewerten die technologische Entwicklung

- Dr. Jürgen Suppan: mobile Endgeräte, Cloud, Software Defined Data Center: vom Hype zur tragfähigen Lösung
- Dr. Franz-Joachim Kauffels: die Entwicklung der Hardware: zwischen Leistung und Betriebsoptimierung

1. Technologie-Bausteine als Teil einer Gesamtarchitektur

- Netzwerk-Fabric-Architekturen: Integration von Leistung, Wirtschaftlichkeit und Flexibilität im RZ, Vergleich der Alternativen
- Netzwerk-Integration virtueller Server: traditionelle Methoden kontra SDN, wo liegt die technische und wirtschaftliche Zukunft?
- Speicher-Technologien: immer mehr für immer weniger Geld, immer mehr Software und Komplexität: wie sieht eine tragfähige Speicher-Strategie aus?
- Server: Blade kontra Rack, bringen neue Server-Technologien neue Antworten?



- Sicherheit: Erzwingen mobile Endgeräte Zonen-Konzepte und wie aufwendig wird der Betrieb?

2. Versorgungs-Infrastrukturen

- Energie-Management: wie kann es wirkungsvoll umgesetzt werden und was bringt es?
- Elektrische Infrastrukturen 2013: was sind die Herausforderungen?
- Infrastruktur-Management: wo kann optimiert werden?

3. Cloud und mobile Endgeräte

- Cloud-Services: Nutzwert-Analyse
- Kollaborations-Plattformen im Vergleich
- Auswirkungen mobiler Endgeräte auf RZ-Infrastrukturen

4. Betriebsoptimierung und Katastrophenvorhersorge

- Katastrophenvorhersorge: Bedarf, Alternativen und Erfahrungen
- Sind Self-Service-Architekturen die Zukunft?
- Software-Defined Data Center: was bringt es wirklich?
- Software-Defined-Networking: unverzichtbare Voraussetzung für Automatisierung?

Am 4. Tag haben wir unseren traditionellen Vertiefungstag, bei dem wir eines der Top-Themen einer besonderen und intensiven Analyse unterwerfen. Dies ist in jedem Jahr ein Highlight des Forums und in der Regel der am höchsten bewertete Teil.

In diesem Jahr nehmen wir in die Mangel:

Vertiefungstag

Software Defined Data Center und Software Defined Networking: Hype oder unverzichtbare Evolutions-Stufe?

Programmübersicht - ComConsult Rechenzentrum Infrastruktur-Redesign Forum 2013

Montag, den 11.11.2013

Block: RZ Technologie-Bausteine als Teil einer Gesamt-Architektur

9:30 bis 11:00 Uhr
Keynote: Das Rechenzentrum im Jahre 2018: die wichtigsten Entwicklungen in der Analyse
- Netzwerke: mehr Leistung, mehr Verfügbarkeit, mehr Flexibilität, geringere Kosten, was bleibt?
- Speicher: immer mehr Optionen, immer preiswerter, was nun?
- Server: Universell kontra Spezial, was ist wichtiger?
- Endgeräte der Zukunft und ihre Auswirkungen auf das RZ
- Cloud: Integration, wo und wie?
- Veränderung der Technologie-Bausteine und die Auswirkung auf die Gesamt-Architektur
- Software Defined: Hype oder Mehrwert?
- Betriebsoptimierung und Automatisierung: Potenziale kontra Kosten
- Hersteller-Strategien im Wandel

Dr. Jürgen Suppan, ComConsult Research Ltd.

11:00 bis 11:30 Uhr Kaffeepause

11:30 bis 12:30 Uhr
Fabrics: Kern des RZ-Netzwerks, Architekturen im Vergleich
- Anforderungen an das RZ-Netzwerk der Zukunft
- Die Rolle der Fabrics
- Architekturen im Vergleich
- Preiswerter, besser, flexibler: ist das die Realität?

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

12:30 bis 13:45 Uhr Mittagspause

13:45 bis 14:30 Uhr
Netzwerkintegration virtueller Server: traditionelle Lösungen kontra SDN
- Wie sind die Limitierungen aktueller Server-Virtualisierungen
- SDN kontra Netzwerk-Virtualisierung
- Overlays, Protokolle, Beispiele
- Kann SDN im traditionellen RZ helfen?

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

14:30 bis 15:30 Uhr
Storage und Netzwerk: Herausforderungen und Lösungen
- Virtualisierung überall, was bedeutet das für Daten?
- Desaster Recovery: Auslagerung von Daten als Performance Bremse
- FC, FCoE, iSCSI oder NAS, die Qual der Wahl
- Verkabelung für Speichernetze: kommt jetzt die Singlemode-Faser?

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

15:30 bis 16:00 Uhr Kaffeepause

16:00 bis 16:45 Uhr
Blade- versus Rack-Server versus integrierte Compute-/Storage-/Netzlösungen
- Blade versus Rack-Server
- Was steckt hinter integrierten Compute-/Storage-/Netzlösungen?
- Betriebsaspekte
- Wie realistisch sind Erwartungen bzgl. der Effizienz von Gesamtlösungen?

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

16:45 bis 17:45 Uhr
Sicherheit: Im heutigen RZ unvermeidlich: Zonenkonzept
- Warum Sicherheitsstandards wie ISO 27001 Zonenkonzepte implizieren
- Zwiebelschalenmodelle und andere Zonenkonzepte in der Praxis
- Zonenkonzepte und Virtualisierung
- Integration von Storage-Lösungen
- Kurzschlussvermeidung; Umgang mit Load Balancern und Dual-Homed Servern
- Trennung von funktionalem und administrativem Verkehr: Konzepte zur sicheren Administration

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

Ab 18:00 Uhr Get Together

Dienstag, den 12.11.2013

Block: RZ Versorgungsinfrastrukturen

9:00 bis 10:00 Uhr
Cisco EnergyWise (JouleX) für Rechenzentren
- Kapazitätsmanagement für Rechenzentren
- 100% Visibiliät für Auslastung, Energieverbrauch und Performance
- Lastadaptiver Rechenzentrumsbetrieb
- Virtuelles, physikalisches und logisches Device und Asset Management

Josef Brunner, Cisco Systems GmbH

10:00 bis 11:00 Uhr
Neue Wege gehen im Rechenzentrum durch Nutzung von Trunk-Verkabelungen
- Multipath-push-on versus klassische Verkabelung im Rechenzentrum
- Sinnvoller und weniger sinnvoller Einsatz, für welche Teilsysteme ist diese Technik sinnvoll für welche nicht • Wann wird MPO unvermeidbar? Was ist zu beachten? • Das Polaritätsproblem bei MPO-Systemen • Wie berücksichtigt die EN 50174 derartige Systeme?
- Produkte und Hersteller

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

11:00 bis 11:30 Uhr Kaffeepause

11:30 bis 12:15 Uhr
Data Center Infrastructure Management
- DCIM-Software: Wachstumsmarkt in der Analyse
- DCIM: welche Funktionen werden abgedeckt?
- Anforderung moderner RZs und Provider
- Architekturen verschiedener DCIM-Ansätze im Vergleich
- Einsparpotentiale und Grenzen einer gesamtheitlichen Lösung
- Schlussfolgerungen und Empfehlungen

Holger Nickel M.A., AixpertSoft GmbH

12:15 bis 12:30 Uhr
Ausstellerpräsentation:
Mit Shortest Path Bridging zum Software Defined Data Center

Heinz Behrens, Avaya Deutschland GmbH

12:30 bis 12:45 Uhr
Ausstellerpräsentation:
Software Defined Data Center in der Fabric leicht gemacht

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

12:45 bis 14:00 Uhr Mittagspause

Block: Cloud und Mobile Endgeräte

14:00 bis 14:45 Uhr
Alles aus der Cloud - Wie Cloud-Dienste die IT-Landschaft verändern
- Begriffsdefinition Cloud – Private-, Public- und Hybrid-Cloud
- Public Cloud - keine gute Idee?
- Auswirkungen von Cloud Services auf die Infrastruktur
- Cloud-Szenarien aus der Praxis

Dominik Zöller, ComConsult Beratung und Planung GmbH

14:45 bis 15:30 Uhr
Auswirkungen mobiler Endgeräte auf das RZ und seine Infrastrukturen
- Cloud Computing, Server-based Computing und Virtualisierung für mobile Endgeräte
- Infrastrukturen zur sicheren Integration von Smartphones und Tablets
- Mobile Device Management und BYOD

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

15:30 bis 16:00 Uhr Kaffeepause

Block: Betriebsoptimierung und Katastrophenvorsorge

16:00 bis 17:00 Uhr
Auf dem Weg zu Self-Service-Architekturen im Unternehmen: OpenStack, die Wolke für Jedermann?
- Warum OpenStack?
- Haupt-Konzepte
- Ist-Zustand: was ist heute möglich?
- Die Zukunft: wo führt der Weg hin?

Jose Moreno, Cisco Systems GmbH

Programmübersicht - ComConsult Rechenzentrum Infrastruktur-Redesign Forum 2013

Mittwoch, den 13.11.2013

9:00 bis 10:00 Uhr
Katastrophenvorsorge für das RZ
- Motivation für Georedundanz
- Zentrale Bedeutung der Ziele hinsichtlich Recovery Point und Recovery Time
- Synchrone versus asynchrone Replikation
- Lösungen führender Hersteller
- Bewertung und Empfehlung

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

10:00 bis 11:00 Uhr
Software Defined Data Center: Funktionen, Aufwand, Vorteile
Dipl.-Ing. Axel Simon, Hewlett-Packard GmbH

11:00 bis 11:30 Uhr Kaffeepause

11:30 bis 12:30 Uhr
Next Generation Data Center Fabric
- Application Centric Infrastructure
- Revolutionäres Lösungs-Portfolio für die Zukunft des RZ

Ulrich Hamm, Cisco Systems GmbH

12:30 bis 12:45 Uhr
Ausstellerpräsentation: Alcatel-Lucent schafft den Backbone ab
- Single Hop, Lossless Ethernet

Torsten Leyh, Alcatel-Lucent Deutschland AG

12:45 bis 14:00 Uhr Mittagspause

14:00 bis 15:00 Uhr
Der Weg zur bedarfsorientierten IT Notfallvorsorge
- Zielentwicklung
- Analysen, Bewertungen und Wegfindung
- Umsetzung einer nachhaltigen Lösung

Thomas Peter Siebrasse, IBM Deutschland GmbH

15:00 bis 16:00 Uhr
Software Defined Networking:
Basis für alle Automatisierungen der Zukunft?
- Das programmierbare Netzwerk: Vision oder Grauen?
- Wie funktioniert es?
- Wo steht die Technologie?
- Kriterien zur Bewertung erster Produkte
- Analyse und Bewertung der Technologie

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

16:00 Ende der 3-tägigen Veranstaltung
Kaffeepause für Teilnehmer der 4-tägigen Veranstaltung

Donnerstag, den 14.11.2013 - Vertiefungstag: SDN und SDDC

9:00 bis 10:30 Uhr
Software Defined Networking in der Analyse:
Welche Rolle wird es spielen, wie verändert es den Markt, wann ist es für wen nutzbar?
- Zielmärkte und Relevanz
- Architektur-Elemente
- Programmierbarkeit von Netzwerken durch Anwendungen: wie muss man sich das vorstellen?
- Beispiele für den Mehrwert:
  - Dynamische Provisionierung
  - Desaster Recovery
  - Dynamische Sicherheits-Lösungen
- Reine Lehre kontra Hybrid: was bedeutet das eigentlich?
- Offenheit, Interoperabilität und Skalierbarkeit: Wunschdenken?
- Was passiert im Markt
  - Open Daylight und die Bedeutung für den Markt
  - ONF und ONS
  - Cisco OnePK: wie ist das zu bewerten?
- Roadmap für die nächsten Jahre

Dr. Jürgen Suppan, ComConsult Research Ltd.

10:30 bis 11:00 Uhr Kaffeepause

11:00 bis 12:30 Uhr
SDN/SDDC: Am Bedarf vorbei oder richtiger Ansatz zum richtigen Zeitpunkt?
- Wichtige Anforderungen von RZ-Betreibern
- Was bedeuten verschiedene Modi der Verteilung der Intelligenz im RZ für den Betrieb?
- Abgrenzung: Software Defined Network vs. Software Defined Data Center
- Wie realistisch ist ein Zusammenspiel von Compute, Virtualisierung, Netz und Storage?

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

12:30 bis 13:45 Uhr Mittagspause

13:45 bis 15:00 Uhr
Bewertung von Herstellerstrategien
- Nicira/VMware
- Microsoft
- HP
- Switch-Hersteller
- Firewall-Hersteller

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

15:00 bis 16:00 Uhr
Ist SDN ein Gewinn für Informationssicherheit?
- Problemstellung der Vielzahl der Sicherheitsübergänge
- Vision: Software Defined Security
- Realität: Stand der Funktionen von SDN und OpenFlow

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

16:00 Ende der 4-tägigen Veranstaltung

Der Veranstalter halt behält sich Änderungen im Programm vor

Aktueller Kongress

ComConsult TK-, UC- und Videokonferenzforum 2013

Kommunikation im Wandel: wie reagieren die Hersteller, was wird aus den Produkten?

25.11. - 28.11.13 in Düsseldorf

Die ComConsult Akademie veranstaltet vom 25.11. bis 28.11.13 ihr "ComConsult TK-, UC- und Videokonferenzforum 2013" in Düsseldorf.

Unified Communications ist auf dem „Plateau der Produktivität“ angekommen. Viele Kunden haben bereits Erfahrungen mit UC-Lösungen gesammelt, migrieren vielleicht schon zur UC-Lösung der zweiten Generation. Dennoch sind Lösungsanbieter auf viele spannende Prob-lemstellungen eine Antwort schuldig geblieben – Wie integriert man UCC in eine Virtual Desktop Infrastructure? Wie wird der Netzübergang zwischen „alter“ und „neuer“ Welt gestaltet – und welche Leistungsmerkmale bleiben hierbei auf der Strecke? Und welche Folgekosten sind mit der Entscheidung für eine Lösung verbunden? Diese und andere Fragen werden wir mit Ihnen und einer Vielzahl hochkarätiger Referenten auf dem diesjährigen ComConsult TK-, UC- und Videokonferenzforum diskutieren.

Die Zentralisierung und Virtualisierung des Desktops ist nicht mehr aufzuhalten. Zu beste-chend sind die Vorteile von standardisierter Provisionierung und zentralisiertem Betrieb. Desktop-as-a-Service – ob aus der Public oder der Private Cloud – wird das Bereitstel-lungsmodell der nächsten fünf Jahre werden. Doch was ist mit der Echtzeitkommunikation? Müssen doch wieder Tischtelefone und andere proprietäre Hardwarelösungen herhalten? Und wird die Webtechnologie der VDI-Technologie den Rang ablaufen? Mit WebRTC zeichnet sich hier ein heißer Konkurrenzstandard zu Citrix & Co. ab, der auch die Geschäftspro-zessoptimierung im B2B- und B2C-Umfeld revolutionieren könnte. Wir freuen uns auf eine lebhafte Diskussion mit Ihnen, welche Folgen dies für die Auswahl einer geeigneten UC-Lösung hat und ob es überhaupt noch „die eine“ Kommunikationslösung geben wird.

UC endet heute immer noch an der Unternehmensgrenze! Aber es gibt einen entscheidenden Bedarf, Zulieferer und Kunden in effiziente Kommunikationsab-

läufe einzubinden. Bestehende Lösungen auf der Basis von Föderationen sind zu unhandlich, komplex und fehlerbehaftet. Hersteller und Provider haben diesen Markt lange ignoriert. Doch jetzt entstehen Alternativen außerhalb der „klassischen“ UC-Angebote. Die Frage ist, hat damit UC an Bedeutung verloren und sind die Kosten der UC-Projekte überhaupt noch zu rechtfertigen? Wie sehen die alternativen Lösungen aus?

H.264 High-Profile und H.264 SVC haben Einzug in fast jedes Produkt-Portfolio auf dem Markt gehalten (nicht frei von Tücken, der Teufel liegt im Detail). Nun kommt mit H.265 eine neue Technologie, die nicht nur den Bandbreitenbedarf noch einmal um 40% senkt, sondern vor allem bei schlechten Verbindungen zu deutlich besseren Bildern führt. Parallel verfallen die Preise. Aus dem Bereich der mobilen Teilnehmer kommen auf der Basis von VP8 und VP9 als Codec kostenfreie Lösungen, deren Qualität immer besser wird. In Kombination mit WebRTC und sozialen Plattformen entsteht eine komplett neue Video-Welt. Aber die Gesamt-Situation ist komplex. Wie sieht eine zukunftssichere Lösung aus?

Gehostete UC- und TK-Lösungen konnten sich bisher nicht durchsetzen. Aber das kann sich schnell ändern. Cloud-Dienste haben ein neues Potenzial für gehostete Dienste mit einem völlig neuen Preis-Leistungs-Verhältnis geschaffen. Einsparungen von über 70% gegenüber selbst betriebenen Lösungen erzwingen eine Evaluierung dieses Bereiches. Ob UC oder Collaboration aus der Cloud. Ob Public oder Private Cloud, ob SaaS-Anbieter oder Carrier – es entstehen vielfältige Serviceangebote. Die Überlegungen reichen bis hin zu einer vollständigen Ablösung von festnetzgestützter Kommunikation. Doch wie gestaltet man ein Ser-viceportfolio auf Basis von Cloud-Lösungen? Ist die Verfügbarkeit der angebotenen Architek-turen ausreichend? Sind die Funktionen wirklich vergleichbar mit heutigen Kommunikationslösungen?

Mit der zunehmenden Mobilisierung der Mitarbeiterschaft nimmt die Bedeutung von Kollaborations-Lösungen im Unternehmen stark zu. Deren Definition überschneidet sich mit dem Verständnis von Unified Communications und muss zukünftig ein integrierter Baustein einer Gesamt-Lösung sein. Wir analysieren den aktuellen Status und zeigen auf, wie Lösungen aussehen können.

Von der reinen TK bis hin zum Cloud-Service: egal wie das Projekt positioniert wird, es muss sich an das neue technologische Umfeld anpassen. Einige der Anbieter tun das mehr als andere. Im Endeffekt stellt sich der Markt neu auf. War im letzten Jahr noch Microsoft der Angreifer auf die traditionelle TK, so greift in diesem Jahr Google mit WebRTC und der breiten Android-Basis an. Android ist Googles trojanisches Pferd. Auf der Basis einer zunehmenden Marktbedeutung entstehen neue Abhängigkeiten und werden neue Dienste in den Markt gedrückt. Für den Videokonferenz-Markt wird dies zur Zerreißprobe. Google positioniert den VP9 Codec direkt gegen H.265. Und VP9 ist bereits da, auch wenn es von keinem Browser außer Chrome bisher unterstützt wird. H.265 kommt erst 2014. Kommt es zu spät? Wie werden Unternehmen die große Anzahl mobiler Teilnehmer integrieren, wenn kostenfreien und zunehmend guten Lösungen ältere und kostenpflichtige Lösungen der traditionellen Welt gegenüber stehen? Nichts beschreibt den aktuellen Zustand des Kommunikations-Marktes besser als dieser Konflikt.

Programmübersicht - ComConsult TK-, UC- und Videokonferenzforum 2013

Montag, den 25.11.2013

9:30 bis 10:30 Uhr
Keynote – aktuelle Trends im Kommunikationsmarkt
- Wie entwickelt sich der Markt für TK, UC und Video?
- Welche Trends beeinflussen die aktuelle Produktsituation?
- Welchen Herausforderungen müssen sich UC-Kunden stellen?
- Wie positionieren sich die Hersteller?

Dominik Zöller, ComConsult Beratung und Planung GmbH

10:30 - 11:00 Uhr Kaffeepause

11:00 bis 12:00 Uhr
UC etabliert sich im Enterprise
- Architektur
- Vollständigkeit aktueller UC-Lösungen
- Stärken und Schwächen von UC
- Vergleich von marktrelevanten Herstellern

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

12:00 bis 12:45 Uhr
UC als B2B Tool
- Wieviel UC funktioniert über die Unternehmens-Grenze hinweg?
  - IM, Präsenz, Voice, Video
- Enterprise-Federations mit XMPP und SIP
- Was machen die etablierten Hersteller?
- Föderationen mit UCaaS

Markus Geller, ComConsult Research GmbH

12:45 bis 14:00 Uhr Mittagspause

14:00 bis 14:30 Uhr
Erfahrungsbericht UC@2013
- Die Einführung von MS Lync 2010 im Kundenumfeld
- Herausforderungen während der Migrationsphase
- Benefits von Unified Communications für Vodafone
- Praxiserfahrungen mit Microsoft Lync 2010
- Strategie zu Lync 2013

Arno Knoop, Vodafone Group Deutschland

14:30 bis 15:15 Uhr
What's new? Aktuelle Endgeräte im Überblick
- Aktuelle Marktzahlen
- Tischtelefone versus Softclients
- Stromverbrauch aktueller Endgeräte
- Energy Efficient Ethernet für Telefone und Videosysteme?
- Endgeräte in der Ausschreibung: virtueller Strompreis

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

15:15 bis 15:30 Uhr
Aussteller-Präsentation - Live-Demo innovaphone myPBX

Lars Dietrichkeit und Benjamin Starmann, innovaphone AG

15:30 bis 16:00 Uhr Kaffeepause

16:00 bis 16:45 Uhr
Das Ansible-Projekt – die neue Client-Strategie von SEN
- Was ist Ansible?
- Die Strategie hinter OpenScape UC und Ansible
- Was unterscheidet Ansible von den Produkten des Mitbewerbs?

Jan Hickisch, Siemens Enterprise Communications GmbH & Co KG

16:45 bis 17:30 Uhr
WebRTC: UC als Web-Anwendung?
- Warum ist WebRTC strategisch spannend?
- Was bedeutet WebRTC für den UC-Markt?
- Was bedeutet WebRTC für das Tischtelefon?
- Erzwingen mobile Endgeräte automatisch WebRTC?
- Wo steht WebRTC heute?
  - WebRTC, RTCWeb

Markus Geller, ComConsult Research GmbH

Ab 18:00 Uhr Get Together

Dienstag, den 26.11.2013

9:00 bis 9:45 Uhr
WebRTC: Funktionsweise, Architektur, Codecs
- HTML5 • JavaScript • WebRTC Framework
- Signalisierung • Freie vs. lizenzpflichtige Codecs

Markus Geller, ComConsult Research GmbH

9:45 bis 10:00 Uhr
Geschäftsprozessoptimierung mit WebRTC
- Wertschöpfungspotenziale durch CEBP
- WebRTC am Beispiel eCommerce

Raphael Bossek, ESTOS GmbH

10:00 bis 10:45 Uhr
Multimedia Collaboration 2.0
- Die Evolution zur nahtlosen, multimedialen Zusammenarbeit
- Anwendungsbeispiele für Multimedia Messaging
- Recording von Multimedia-Kommunikation in der Praxis
- Strategischer Ausblick – wohin entwickelt sich Collaboration?

Thomas Römer, Avaya Deutschland GmbH

10:45 bis 11:15 Uhr Kaffeepause

11:15 bis 12:00 Uhr
Der lange Weg zu UC –
technisch und wirtschaftlich sinnvolle Migrationspfade
- Migrationsszenarien von klassischer TK zu Unified Communications
- Kundenszenarien aus der Praxis
- Technologie- und Herstellerauswahl
- Kostenbetrachtungen und Investitionsschutz

Dipl.-Ing. Martin Egerter, ComConsult Beratung und Planung GmbH

12:00 bis 12:30 Uhr
Drahtlose Kommunikation – Was tun mit der DECT-Infrastruktur?
- Migrations-Fähigkeit von DECT-Infrastrukturen
- Macht IP-DECT Sinn? • Ist VoWLAN eine echte Alternative zu DECT?
- Sollte die DECT-Infrastruktur beibehalten werden?
  - Erfahrungen aus der Praxis • Projektbeispiele
- Mögliche Nachfolge-Technologien zu DECT

N.N., Siemens Enterprise Communications GmbH & Co KG

12:30 bis 12:45 Uhr
Die Zukunft spricht Lync. Sprechen Sie mit!
- Microsoft Lync 2013 • Strategischer Ausblick MS Lync

André Liesenfeld, Microsoft Deutschland GmbH

12:45 bis 14:15 Uhr Mittagspause

14:15 bis 15:00 Uhr
Herausforderungen und Lösungsansätze aus der Migrationspraxis
- Fax- Dienste und Abhängigkeiten zur VoIP-Infrastruktur
- Spezialdienste im GSM: die Zusammenhänge zwischen CSD, ISDN/UDI, V.110 mit 9k6 • Der Einsatz von G.clear und die Migration hin zu reinen IP-Übergabeschnittstellen (RFC4040)
- Optionen zum Notrufrouting bei Zentralisierung der ISDN-Übergänge und späterer Umstellung auf SIP-Trunks

Bert-Henrik Czaya, Cisco Systems GmbH

15:00 bis 15:30 Uhr
VoIP Migration und der Übergangs-Punkt zur non-IP Welt
- Migrationsszenario TDM – Motivation und Ausgangslage
- Vorgehensweisen zur VoIP-Migration
- Umgang mit Bestandslösungen
- Fallstricke bei der VoIP-Migration

Lars Dietrichkeit und Benjamin Starmann, innovaphone AG

15:30 bis 16:00 Uhr Kaffeepause

16:00 bis 16:45 Uhr
Der ComConsult Communications Index und
das ComConsult Hybrid Cloud Testbed
- Idee und Ziel des Hybrid Cloud Testbed
- Anwendungsszenario Communications & Collaboration Index
- Herausforderungen und Grenzen
- Die Cloud-Benefits in Zahlen

Florian Hojnacki und Dominik Zöller,
ComConsult Beratung und Planung GmbH

16:45 bis 17:45 Uhr
CCI - Ergebnisse der UC-Marktstudie
- Marktüberblick und Herstellerauswahl
- Die Herstellerbewertungen im Detail
- Fazit und Markteinschätzung

Leonie Herden, ComConsult Beratung und Planung GmbH

ComConsult TK-, UC- und Videokonferenzforum 2013

Mittwoch, den 27.11.2013

9:00 bis 9:45 Uhr
Trends im Videomarkt
- Ist H.3xx tot? (H.320, H.323)
- Wo steht H.264? (AVC, SVC)
- Neue Standardisierung: H.265 / HEVC
  - Verbesserungen • Hersteller-Positionierung

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

9:45 bis 10:30 Uhr
Unternehmensübergreifendes Video – B2B & B2C
- Unternehmensübergreifende Anwendungsszenarien
- Protokolle: H.264 AVC/SVC, TIP
- Peering B2B, B2C, C2C

N.N, Controlware GmbH

10:30 bis 11:00 Uhr Kaffeepause

11:00 bis 11:30 Uhr
Im Kreuzfeuer von Marktentwicklung und UC-Planung - Videokonferenz im Wandel
- Neuer Trend: Cloud Lösungen für Video und UC als zunehmender Ersatz von On-Premise-Lösungen
- Cloud-fähige UC/Video-Architektur mit Social Media Zugang
- Einsatz von Standard-Codecs: H.264 AVC und SVC vs. H.265
- Welche Innovationstrends bei Raumsystemen gibt es?
- Video-UC Integration: Polycom und Microsoft Lync, IBM Sametime, Siemens OpenScape UC

Dipl.-Ing. Sascha Hirschoff, Polycom GmbH

11:30 bis 12:15 Uhr
AVB: konventionelle Studiotechnik wandert ins Ethernet – was sind die Folgen für den Enterprise Video Markt?
- Motivation: Warum Ethernet für konventionelle Audio/Video-Technik?
- Die avnu Allianz
- LAN Standards: IEEE AVB (Audio/Video Bridging)
  - IEEE 802.1AS, IEEE 802.1Q-at , IEEE 802.1Q-av
- Folgen für den Enterprise Video Markt

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

12:15 bis 12:45 Uhr
Erfahrungsbericht Videokonsolidierung

12:45 bis 14:15 Uhr Mittagspause

14:15 bis 15:00 Uhr
Outsourcing des (UC-)Desktops
- Wie sieht der Desktop der Zukunft aus?
- Skaleneffekte durch Virtualisierung und Automatisierung
- Lösungsarchitektur
- Desktop-as-a-Service in Zahlen

Thomas W. Müller, T-Systems GmbH

15:00 bis 15:15 Uhr
Aussteller-Präsentation - Rise of the Cloud
- Der Einfluss der Cloud auf den Kommunikationsmarkt
- Referenzarchitektur für UCaaS auf Basis von Alcatel

Christian Sailer, Alcatel-Lucent Deutschland AG

15:15 bis 16:00 Uhr
Thin-Client Lösungen: Desktop-Virtualisierung und UC / Web-basierte UC-Desktops
- Hairpinning-Problem und nailed Media Streams
- Welche Dienste funktionieren heute in VDI-Umgebungen?
- Medienströme bei Web-basierten Desktops & Clients?
- Die Rolle von WebRTC und HTML 5 bei der Produktion von UC-Desktops

Dominik Zöller, ComConsult Beratung und Planung GmbH

16:00 bis 16:15 Uhr
Zusammenfassung und Wrap-Up

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

16:15 Ende der 3-tägigen Veranstaltung

Kaffeepause für Teilnehmer der 4-tägigen Veranstaltung

Donnerstag, den 28.11.2013 - Hypes, Trends und Technologien

9:30 bis 10:00 Uhr
Hypes, Trends und Technologien
- Welche Trends bewegen den UC-Markt, die Hersteller und die Kundschaft?
- Marktüberblick und Marktentwicklung

Dominik Zöller, ComConsult Beratung und Planung GmbH

10:00 bis 10:45 Uhr
Internet of Things und der Kundenkanal
- Das Internet of Things und sein Einfluss auf die Kommunikation
- Wenn das Werkstück spricht – welche Kommunikationskanäle werden zukünftig wichtig?
- Intelligente Contact Center Lösungen

N.N.

10:45 bis 11:15 Uhr Kaffeepause

11:15 bis 12:00 Uhr
Smart Buildings – Wie Kommunikationstechnik und Gebäudeautomatisierung verschmelzen
- Moderne Gebäudeautomatisierung im Überblick
- Integrationspunkte und Schnittstellen zur Kommunikationstechnik
- Anwendungsbeispiele aus der Praxis

Thomas Römer, Avaya Deutschland GmbH

12:00 bis 12:45 Uhr
Der Mobile Client – Abschied von PC und Fixed Voice?
- Mobile Endgeräte dominieren (in Zukunft?) den Arbeitsplatz – was bedeutet das?
- (Wann) ersetzt das Tablet den PC-Client?
- „Mobile only" – kann das Mobiltelefon die TK-Anlage ersetzen?

Dominik Zöller, ComConsult Beratung und Planung GmbH

12:45 bis 14:00 Uhr Mittagspause

14:00 bis 14:30 Uhr
Collaboration aus der Cloud – Ein Marktüberblick

14:30 bis 15:15 Uhr
Integration von Social Media in die Kommunikationskanäle
- Anwendungen für Social Media in der Enterprise-Kommunikation
- Verschmelzung von UC&C und Social Networks
- Kundenanforderungen und Projekterfahrungen

N.N., Siemens Enterprise Communications GmbH

15:15 bis 15:30 Uhr Kaffeepause

15:30 bis 16:15 Uhr
SharePoint und Lync 2013 – Social Enterprise und die Geschäftsprozesse
- Funktionsüberblick MS SharePoint 2013
- Integrationspunkte von MS SharePoint, Lync und sozialen Medien
- Lösungsarchitekturen für Social Enterprise
- Praxisnahe Beispiele

N.N., Microsoft Deutschland GmbH

16:15 bis 16:30 Uhr
Zusammenfassung und Wrap-Up

Dominik Zöller, ComConsult Beratung und Planung GmbH

16:30 Ende der 4-tägigen Veranstaltung

Kongress-Anmeldung

Anmeldung

Fax-Antwort an ComConsult 02408/955-399

ComConsult Rechenzentrum Infrastruktur-Redesign Forum 2013 11.11. - 14.11.2013 in Düsseldorf

Ich buche den Kongress
ComConsult Rechenzentrum Infrastruktur-Redesign Forum 2013

☐ vom 11.11. - 14.11.13 in Düsseldorf
zum Preis € 2.490,-- netto

☐ vom 11.11. - 13.11.13 in Düsseldorf
zum Preis € 2.090,-- netto

☐ am 14.11.13 in Düsseldorf
zum Preis € 990,-- netto

☐ inkl. Report "RZ Netzwerk-Infrastruktur Redesign - 6. Auflage (März 2013)" zum Sonderpreis von € 338,--

☐ Bitte reservieren Sie mir ein Zimmer

vom _____ bis_____ 13

_____ Vorname

_____ Nachname

_____ Firma

_____ Telefon/Fax

_____ Straße

_____ PLZ,Ort

_____ eMail

_____ Unterschrift

ComConsult TK-, UC- und Videokonferenzforum 2013 25.11. - 28.11.13 in Düsseldorf

Ich buche den Kongress
ComConsult TK-, UC- und Videokonferenzforum 2013

☐ vom 25.11. - 28.11.13 in Düsseldorf
zum Preis € 2.490,-- netto

☐ vom 25.11. - 27.11.13 in Düsseldorf
zum Preis € 2.090,-- netto

☐ am 28.11.13 in Düsseldorf
zum Preis € 990,-- netto

☐ Bitte reservieren Sie mir ein Zimmer

vom _____ bis_____ 13

_____ Vorname

_____ Nachname

_____ Firma

_____ Telefon/Fax

_____ Straße

_____ PLZ,Ort

_____ eMail

_____ Unterschrift

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

Aktueller Kongress

ComConsult Wireless Forum 2013
18.11. - 19.11.13 in Bonn

Die ComConsult Akademie veranstaltet vom 18.11. bis 19.11.13 ihr "ComConsult Wireless Forum 2013" in Bonn.

Mobilfunk ist inzwischen fast „schneller“ als so manches WLAN. Aber auch WLAN kommt in absehbarer Zeit mit Datenraten im Gigabit-Bereich daher. Alle tragen inzwischen mobile Endgeräte mit sich herum und sind ständig „online“. Brauchen wir also das gute alte LAN mit seinen armdicken Kabelbündeln in Gebäuden zukünftig noch? Und wie sieht es mit den Sicherheitsaspekten aus, wenn alles nur noch drahtlos abläuft? Diese und andere Fragen werden wir auf dem ComConsult Wireless Forum 2013 beleuchten. Wie immer mit kompetenten Vorträgen zu Standards, Technik, Visionen und praktischer Umsetzung.

Was fällt Ihnen zu dem Begriff „Industrie 4.0“ ein? Er impliziert, dass sich industrielle Produktion an einem Wendepunkt befindet, einer Art industrieller Revolution. Werkzeuge, Maschinen und vor allem die Werkstücke selbst sind mit Eigenintelligenz und Kommunikationsfähigkeit ausgestattet. In diesem „Internet of Things“ entsteht etwas, das die Fachleute als „Cyber-physikalische Systeme“ bezeichnen. Werkstücke kennen ihren aktuellen Bearbeitungsstand und das für sie vorgesehene Endprodukt. Sie steuern mit diesem Wissen die sie bearbeitenden Maschinen und Werkzeuge – es entsteht ein Fertigungsprozess mit ungeahnter Flexibilität.

Dass dafür vor allem drahtlose Kommunikationsfähigkeit vonnöten ist, versteht sich von selbst. Dem Wireless LAN steht also eine großartige Zukunft bevor. Die dafür erforderlichen Techniken werden wir im ComConsult Wireless Forum 2013 beleuchten und uns unter anderem mit den folgenden Themen befassen: •Das Internet of Things ist nur eine neue Anwendungsform von Wireless LAN. Zukünftig werden unsere Automobile drahtlos kommunizieren und dabei helfen, Unfälle zu vermeiden und Maut einzuziehen. Wir werden Systeme durch Gesten unsere Hände steuern können, ohne sie zu berühren. Drahtlose Ortungssysteme auf WLAN-Basis werden immer weiter verfeinert. Die Liste kann schier endlos fortgesetzt werden. Wir geben einen Überblick und die sich daraus ergebenden Anforderungen an drahtlose Kommunikation.

- Inzwischen haben mobile Endgeräte wie Smartphones und Tablets den klassischen PC abgehängt und damit hat die Bedeutung des drahtlosen Anschlusses per WLAN und LTE massiv an Bedeutung zugenommen. Unified Communications & Collaboration (UCC), Mobile Device Management (MDM) und Bring Your Own Device (BYOD) haben Gestaltung und Nutzung von drahtlosen System erheblich beeinflusst.
- Die neuen WLAN-Techniken der IEEE 802.11ac und 11ad beginnen sich zu etablieren. Die Standardisierungsgremien haben ihre Arbeit größtenteils abgeschlossen und Produkte werden verfügbar. Das Gigabit-WLAN wird zur Realität. Wir geben einen tiefen Einblick in die Funktionsweise dieser WLAN-Techniken und zeigen Ihnen, welchen praktischen Einfluss das auf Design und Betrieb Ihrer Netze haben wird.
- Wireless LAN Controller sind seit Jahren das Rückgrat vieler WLANs. Damit sie der ständig wachsenden Anzahl von Wireless Access Points und der darüber ausgetauschten Datenmengen Herr werden, steigt deren Leistung unaufhaltsam. Darüber hinaus haben die Hersteller inzwischen neue Controller-Konzepte vorgestellt, die auf eine weitgehende Integration von WLAN und LAN abzielen. Wir stellen diese Konzepte im Detail vor.
- Software Defined Networks (SDN) sind in aller Munde. Es gibt heute keinen Hersteller von Netzwerktechnik, der nicht behauptet, dieses Paradigma in irgendeiner Form zu unterstützen. Wir stellen die Frage, was SDN im Umfeld von WLAN bedeutet und wie entsprechende Produkte aussehen werden.
- Die ungebremste Ausbreitung von Funksystemen führt zu immer mehr Störungen. Gleichzeitig wird den Funknetzen immer mehr Verantwortung für einen reibungslosen Ablauf von Geschäfts- und Produktionsprozessen aufgebürdet. Wie passt das zusammen und welche Maßnahmen für einen Störungs-freien Betrieb lassen sich treffen?
- Hacker-Angriffe auf Industrieanlagen scheinen mehr und mehr in Mode zu kommen. Und bietet nicht gerade die Funktechnik dafür ungeahnte Schlupflöcher? Die Sicherheit von Wireless LANs ist und bleibt also ein Dauerbrenner. Und es müssen neue Konzepte für neue Anwendungsformen ersonnen werden.

Das ComConsult Wireless Forum 2013 ist die zentrale Veranstaltung des Jahres 2013 zur drahtlosen Kommunikation. Sie ist für jeden Entscheider, IT-Architekten, Planer und Betreiber in diesem Bereich ein absolutes Muss. Hier trifft sich die Branche.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Ich buche den Kongress
ComConsult Wireless Forum 2013

☐ vom 18.11. - 19.11.13 in Bonn
zum Preis € 1.890,-- netto

☐ Bitte reservieren Sie mir ein Zimmer

vom _____ bis_____ 13

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

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

Programmübersicht - ComConsult Wireless Forum 2013

Montag, den 18.11.2013

9:30 - 10:30 Uhr
Keynote: Wireless-Techniken im Wandel
- Auf dem Weg zu Multi-Gigabit im WLAN und im Mobilfunk
- Wird das Kabel zur Client-Anbindung zur Nischenlösung?
- SDN und OpenFlow - Hype oder greifbarer Nutzen für WLAN-Infrastrukturen?
- LTE kommt. Werden WLAN überflüssig?
- Smartphones und Tablets: Eine neue Geräteklasse erobert die IT-Infrastruktur
- Neue Nutzungsformen der IT mit Enterprise Mobility und die Konsequenzen für drahtlose Anbindungen an die IT
- Drahtlose Kommunikationstechniken im Internet of Things (IoT)

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

10:30 - 11:30 Uhr
Gigabit WLAN kommen
- Wie IEEE802.11ac auf fast 7 Gbit/s Bruttodatenrate kommt
- Maximal 8 Spatial Streams, Mega-Modulation 256-QAM und Mini-Coderate 5/6: Welche Datenraten sind realistisch?
- Auswirkungen auf Ausleuchtung und WLAN-Planung bzw. WLAN-Migration
- Was leisten die verfügbaren Produkte zu IEEE 802.11ac?
- IEEE 802.11ad: Bei 60 GHz mit einer Kanalbandbreite von 2000 MHz aus dem Vollen schöpfen
- Eigenschaften des 60-GHz-Bereichs und die Folgen für die WLAN-Ausleuchtung und Access-Point-Dichte
- Langfristige Konsequenzen für das kabelbasierte LAN und die Tertiärverkabelung

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

11:30 - 12:00 Uhr Kaffeepause

WLAN Design und Betrieb

12:00 - 12:45 Uhr
Controller-basiertes WLAN-Design:
Maximale Anforderungen an Leistung, Verfügbarkeit und Management
- Controller-Konzepte der WLAN-Ausrüster: Wie unterscheiden sich die Produkte?
- Alptraum Controller-Ausfall: Was leisten die Redundanzkonzepte der Hersteller?
- Betrieb von Controller-basierten WLANs: Software-Update im Controller-Cluster
- Wie kann im Controller-basierten Design mit Multi-Gigabit-Funkübertragung umgegangen werden?
- Macht zentrales Bridging am WLAN Controller noch Sinn?
- Trennung von Control und Data Plane: Neue Controller-Architekturen und Integration von WLAN Controllern und LAN Switches

Dipl.-Ing. Michael Schneiders, ComConsult Beratung und Planung GmbH

12:45 - 13:15 Uhr
Controller-Konzepte der WLAN-Ausrüster - Beispiel 1

13:15 - 14:15 Uhr Mittagspause

14:15 - 15:15 Uhr
Controller-Konzepte der WLAN-Ausrüster - Beispiel 2 und 3

15:15 - 15:45 Uhr
Podiumsdiskussion: Controller-Konzepte im Vergleich

Vertreter der Hersteller, Dr. Joachim Wetzlar, Dr. Simon Hoff, Dipl.-Ing. Michael Schneiders, ComConsult Beratung und Planung GmbH

15:45 - 16:15 Uhr Kaffeepause

16:15 - 17:00 Uhr
Betrieb und Trouble Shooting von WLAN
- WLAN-Management, was ist anders als im LAN?
- Die Management-Disziplinen und ihre Umsetzung bei WLAN
- Schweizer Taschenmesser oder Spezialwerkzeuge?
- Welche Werkzeuge sind sinnvoll, welche nicht?

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

WLAN-Sicherheit

17:00 - 17:45 Uhr
Vorsicht Falle: Sicherheit in WLAN
- Ist WPA2 Enterprise mit IEEE 802.1X und CCMP (AES) noch sicher?
- Fallstricke bei IEEE 802.1X und WPA2: Was kann man in Theorie und Praxis kompromittieren und was kann man dagegen tun?
- Welche weiteren Schwachstellen gibt es und welche Maßnahmen kann man dagegen einsetzen?
- Der Innentäter im WLAN
- Umgang mit Pre-Shared Keys
- Absicherung von Management Frames
- Aufbau von sicheren mandantenfähigen WLAN-Infrastrukturen

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

ab 18:00 Uhr Happy Hour

Dienstag, den 19.11.2013

Mobile Computing

9:00 - 10:00 Uhr
Konkurrenz zu WLAN durch LTE
- Was leistet LTE: Netzdesign und Übertragungstechniken
- Gigabit im Mobilfunk: Geht das überhaupt?
- Stand der LTE-Einführung international und in Deutschland
- LTE und WLAN: Konkurrenz oder sinnvolle Ergänzung?
- Problembereich Indoor-Versorgung: Nanozellen und andere Techniken

Dipl.-Ing. Martin Egerter, ComConsult Beratung und Planung GmbH

10:00 - 10:30 Uhr Kaffeepause

10:30 - 11:30 Uhr
Enterprise Mobility mit Smartphones und Tablets
- Warum bei Smartphones und Tablets im WLAN mit weniger Performance zu rechnen ist
- Gefährdungen bei iOS, Android und Co.
- Architekturen für die sichere Anbindung von Smartphones und Tablets an die Infrastruktur
- Bring Your Own Device (BYOD) und Mobile Device Management (MDM)
- Container-Lösungen mit App Sandboxing und Virtualisierung von Smartphones: Möglichkeiten zur Sicherung von Unternehmensdaten auf privaten Endgeräten
- MDM für iOS und Android: Was geht wirklich und wo sind die Grenzen?

Dominik Zöller, ComConsult Beratung und Planung GmbH

Anwendungen

11:30 - 12:15 Uhr
Besondere Eigenschaften von WLAN im industriellen Einsatz
- Spezielle Anforderungen in industriellen Umgebungen
- Roaming im industriellen Umfeld
- Warum IT-Sicherheit für Industrial WLAN leichter gesagt als getan ist
- PROFINET und Co.: Umgang mit Echtzeitanforderungen
- Einsatz von speziellen Antennen, z.B. Leckwellenleitern
- Spielt hier der zukünftige Standard 802.11 ac eine Rolle?

Heinrich Merz, ads-tec GmbH

12:15 - 13:45 Uhr Mittagspause

13:45 - 14:30 Uhr
Das vernetzte Fahrzeug
- IT eines modernen Automobils
- RFID, Sensoren, Smartphones, Tablets im Fahrzeug: Risiken von Standard-IT-Komponenten
- Interaktion und Zusammenarbeit / Intelligente Umgebung: Fahrzeuge im Internet of Things
- Einsatz von Wireless-Techniken für Telematikanwendungen
- Schnittstellen und Angriffsmöglichkeiten: Gehackte Autos - Beispiele und mögliche Szenarien

Prof. Dr. Marko Schuba, FH Aachen

14:30 - 15:15 Uhr
Das Internet of Things
- Internet of Things: wen betrifft das überhaupt?
- Was kommt auf Unternehmensnetze zu?
- Welche drahtlosen Techniken werden eingesetzt ?
- Verbund oder Inselnetze?
- Bisherige und künftige Gefährdungen
- Was heute schon für die IoT-Sicherheit getan werden kann

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

Ende der Veranstaltung 15:30 Uhr

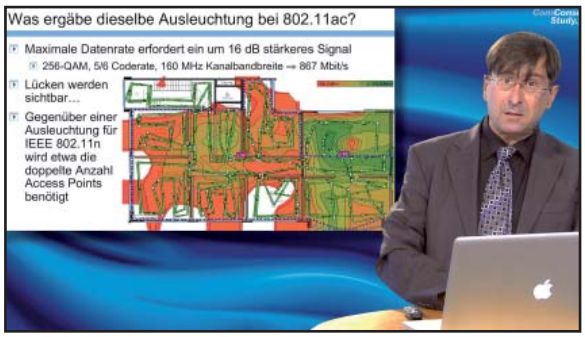
ComConsult-Study.tv

Gigabit WLAN Spezial im Oktober bei ComConsult-Study.tv

802.11ac ist keine Fiktion mehr. Immer mehr Produkte kommen auf den Markt und bei neuen Endgeräten wird es zum Standard. Mehrere Gigabit in der „Luft“ macht aber nur dann Sinn, wenn das Kabelnetzwerk das auch hergibt. In dem Video „Gigabit WLANs: Konsequenzen für das Design“ geht Dr. Hoff der Frage nach, ob ein neues Design für die Einführung von 802.11ac in Unternehmen notwendig ist.

In dem Video „Netzwerk Access 2018: Kabel oder Funk, wohin geht die Reise?“ analysiert Dr. Suppan, ob und warum die Gigabit WLAN Standards IEEE 802.11ac und 802.11ad notwendig sind.

Abgerundet wird dieses Paket durch das Video „Das neue WLAN IEEE 802.11ac: was bringt es?“ von Dr. Kauffels, in dem er die dem Standard zugrunde liegende Technik verständlich darstellt und der Frage nachgeht, wieviel Marketing in der Behauptung 7 Gigabit/s steckt und was wir in der Praxis erwarten können.

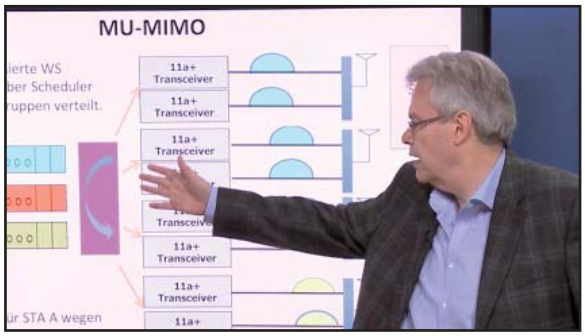


Gigabit WLANs: Konsequenzen für das Design
Referent: **Dr. Simon Hoff**
Zeit: 00:56:22
Einzelpreis: 59,00 € netto
Im Abo: kostenlos

IEEE 802.11ac und ad kommen mit maximalen Datenraten von 7 Gbit/s. Um dies zu erreichen, wurde die Funktechnik erheblich überarbeitet. Damit sind bestehende Planungsansätze nicht mehr nutzbar. Tatsächlich brauchen wir ein neues Verständnis von WLAN-Technik. Dr. Hoff analysiert was die neuen Standards wirklich leisten, wie die WLANs der Zukunft aussehen und wie sich die Zell-Planung und die Integration ins Kabel-Netzwerk ändert.

Netzwerk Access 2018: Kabel oder Funk, wohin geht die Reise?
Referent: **Dr. Jürgen Suppan**
Zeit: 00:54:52
Einzelpreis: 49,00 € netto
Im Abo: kostenlos

Gigabit-WLAN, immer mehr mobile Endgeräte: hat das Kabel zum Endgerät ausgedient? Wie sieht der Desktop der Zukunft aus? Was passiert bei Applikationen und Servern? Dr. Suppan analysiert in diesem hochaktuellen Video wohin die Reise im Netzwerk-Access-Bereich geht. Er entwirft ein Bild für die Netzwerk-Zukunft am Arbeitsplatz.



Das neue WLAN IEEE 802.11ac: was bringt es?
Referent: **Dr. Franz-Joachim Kauffels**
Zeit: 00:41:51
Einzelpreis: 39,00 € netto
Im Abo: kostenlos

Mit der starken Zunahme mobiler Teilnehmer ist das bisherige WLAN nach IEEE 802.11n am Ende. Zwei neue Standards kämpfen um die Gunst des Kunden. Speziell IEEE 802.11ac verspricht 7 Gbit/s zum Preis von 11n. Lernen Sie in diesem Video was der neue Standard IEEE 802.11ac für Sie bedeutet und welche Auswirkung er auf aktuelle Planungen hat.

Das Bundle bestehend aus den drei Videos nur € 102,90*

*Dieses Angebot gilt nur im Oktober 2013.- Regulärer Preis € 147,-- netto

Weitere Details finden Sie auf unserer Homepage unter www.comconsult-study.tv

Schwerpunktthema

Trunk-Verkabelungen im Rechenzentrum, Fluch oder Segen?

Fortsetzung von Seite 1

Dipl.-Ing. Hartmut Kell kann bis heute auf eine mehr als 20-jährige Berufserfahrung in dem Bereich der Datenkommunikation bei lokalen Netzen verweisen. Als Leiter des Competence Center IT-Infrastrukturen der ComConsult Beratung und Planung GmbH hat er umfangreiche Praxiserfahrungen bei der Planung, Projektüberwachung, Qualitätssicherung und Einmessung von Netzwerken gesammelt und vermittelt sein Fachwissen in Form von Publikationen und Seminaren.

Ziel und Rahmenbedingungen

Das Ziel einer leistungsfähigen Rechenzentrums-Verkabelung besteht darin, dass eine sehr hohe Anzahl von Ports auf einer kleinen Fläche bzw. Volumeneinheit realisiert werden muss. Im vorliegenden Artikel bezeichnet das Wort „Rechenzentrum“ den Bereich, in dem die Server inkl. der Netzwerkkomponenten für diese Geräte positioniert werden. Die immer vorhandene räumliche Peripherie um diesen Serverraum herum (Testbereiche etc.) wie auch die Verbindung zwischen zwei Serverräumen steht nicht im Fokus, da aus Sicht des Autors die Auswahl an Übertragungsmedien stark eingeschränkt ist, das bevorzugte Medium wird Glasfaser sein und die bevorzugte Verkabelungstechnik wird „klassisch“ sein. Damit beschränkt sich der Artikel auf Verkabelungslösungen innerhalb eines Raumes. Eine derartige Verkabelung muss eine leichte Anpassung bei Nutzungsänderungen möglich machen, nach Möglichkeit ohne aufwendige Installationsmaßnahmen. Bedingt durch die sehr unterschiedlichen Server-Systeme ist die Bereitstellung einer Vielfalt an verschiedenen Datenraten über verschiedene Medien gefordert. Zusammengefasst: Ein Rechenzentrum muss mit einer bedarfsorientierten IT-Verkabelung ausgestattet werden, die in kürzester Zeit an jedem Punkt im Raum eine beliebige Anzahl von Datenschnittstellen in beliebigen Übertragungstechniken in optional höchsten Verfügbarkeitsstufen bereitstellen kann, ohne dass nicht mehr benutzte Verbindungen andere Infrastrukturelemente wie Kühlung oder Stromversorgung erheblich beeinträchtigt werden.

Bei der Suche nach einer praktikablen Lösung sind grundsätzlich zwei fundamentale Rahmenbedingungen zu berücksichtigen:

- Es ist eine hierarchische (baum/sternförmige) Topologie aufzubauen, denn nur diese ist im Betrieb einfach zu erweitern, bietet vielfältige Möglichkeiten zum Aufbau von Redundanzen, lässt die Verwendung von unterschiedlichen Medien zu und erlaubt eine unterschiedliche Festlegung dieser Medien für verschiedene Ebenen.

- Es ist eine strukturierte Verkabelung aufzubauen, bei der es darum geht, rauminterne größere Strecken mit Installationskabel statt mit langen Patchkabeln zu überbrücken, und diese dann bedarfsorientiert bei jeder Nutzungsänderung zu entfernen oder neu zu verlegen. Es sind hochwertige Installationskabel mit einem Abschluss in Form von aufschaltbaren Anschlusstechniken wie Buchsen oder Kupplungen vorzusehen, die dann durch Anschluss- oder Rangierschnüre beschaltet werden.

Neben diesen beiden elementaren Rahmenbedingungen zeigen viele Planungen von RZ-Verkabelungen und Betriebserfahrungen, dass weitere Anforderungen berücksichtigt werden müssen, einige nachfolgend beschrieben. Im Unterschied zu einer herkömmlichen Tertiärverkabelung z.B. im Bürobereich, deren Planungsansatz eine Nutzbarkeit von weit über 10 Jahren ohne Nach- oder Neuverkabelung sicherstellen muss, ist im Rechenzentrum mit deutlich mehr Dynamik zu rechnen, die Änderungen der Verkabelung erforderlich machen können. Es beginnt bereits beim Aufbau der Verkabelung, gerade in existierenden Rechenzentren stellt die Einführung einer neuen Verkabelung eine besondere Herausforderung dar. Hier muss durch Freiräumen von belegten Flächen und Schaffen von Swing-Areas eine sukzessiv aufgebaute Verkabelung geplant werden, die möglichweise von unterschiedlichen Systemen im Laufe der Zeit unterschiedlich genutzt werden wird. Werden z.B. heute in einem Bereich SAN-Komponenten mit Glasfaseranschluss aufgrund eines temporären Umzugs zwischengelagert, so müssen in 3 Jahren möglicherweise dort Server mit Twisted-Pair-Anschlüssen untergebracht werden. Damit wird es unwahrscheinlich, in einem Rechenzentrum eine Infrastruktur aufbauen zu können, die vollkommen ohne Änderungen im Nutzungszeitraum auskommt.

Eine von den aktiven Komponenten (Switches) losgelöste Planung der Verkabelung kann nicht zielführend sein, sowohl Topologie als auch Verkabelungskomponenten müssen beispielsweise ein 2-stufiges, 3-stufiges Netz oder auch ein Collapsed Backbone möglich machen, am besten zu jedem Zeitpunkt ohne vollkommenen Umbau des Rechenzentrums. Derzeit zeichnet sich ab, dass Lösungen mit zentral aufgestellten Server-Access-Switches und dort angeschlossenen Server-Komponenten kaum realisierbar sind, der dazu notwendige Verkabelungsaufwand wäre viel zu hoch. Mag das mit Glasfaser noch denkbar sein, so wird bei einer hohen Menge an LAN-Anschlüssen mit Twisted Pair die Kabelmenge und das Volumen im Doppelboden so hoch werden, dass eine Änderung des Lüftungskonzeptes im Doppelboden die Folge sein könnte. Die bevorzugten Lösungen werden demzufolge Top-of-the-Rack (TotR), Middle-of-the-Row (MotR) und End-of-the-Row (EotR) sein, diese müssen leicht realisiert werden können.

Betrachtete Verkabelungsebene

Die EN 50173-5 unterteilt die Verkabelung in 3 Ebenen (weitere Erläuterungen siehe auch März-Insider 2009 bzw. die EN 50173-5):

Trunk-Verkabelungen im Rechenzentrum, Fluch oder Segen?

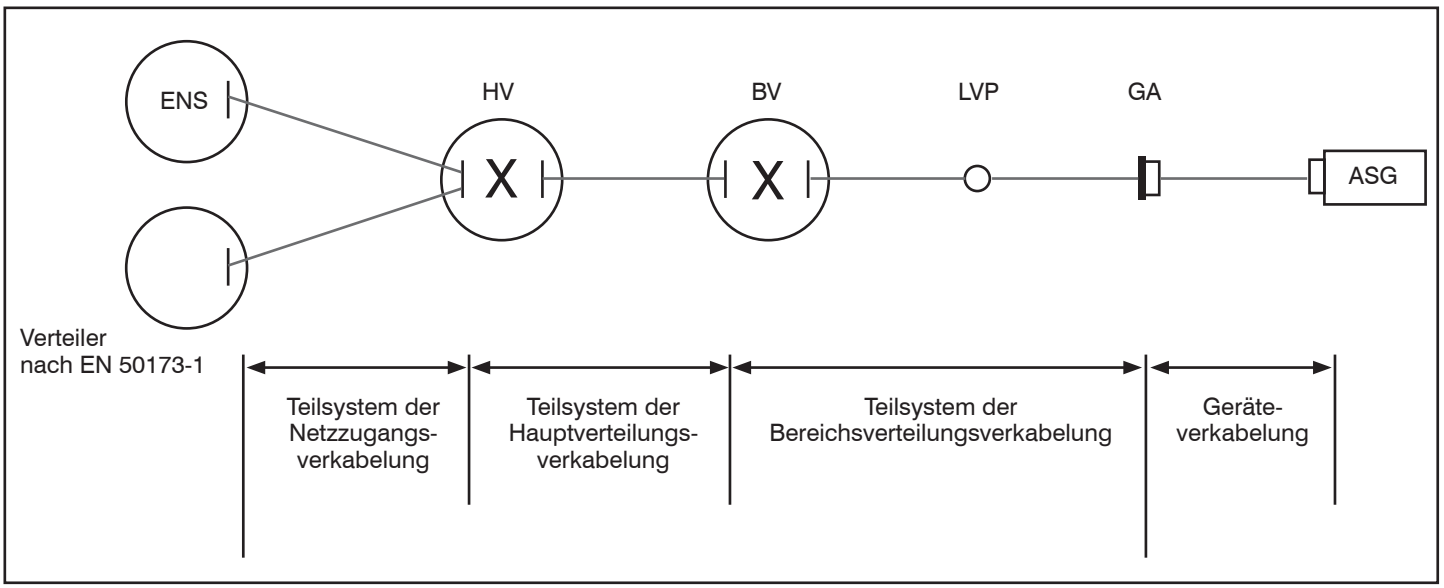


Abbildung 1: Übersicht der Verkabelungsebenen

- Netzzugangsverkabelung (TIA 942: network access cabling system)
- Hauptverteilungsverkabelung (TIA 942: main distribution cabling system)
- Bereichsverteilungsverkabelung (TIA 942: zone distribution cabling system)

Eine Netzzugangsverkabelung erfolgt in der Regel über große Distanzen hinweg, durch unterschiedliche Räume mit unterschiedlichen Kabelführungssystemen. Brandschotts werden durchquert, Trassen mit Datenkabel oder auch mit Starkstromkabel müssen genutzt werden. Mit Nachverkabelungen von anderen technischen Gewerken wie Telefonverkabelungen o.ä. muss bei diesen Kabelwegen gerechnet werden und entsprechende robuste Kabel wie z.B. nagetiergeschützte Universalkabel können sinnvoll sein. Insbesondere ein Aufmaß zur Ermittlung der genauen Länge ist schwer durchzuführen, man wird „klassisch“ verkabeln, indem Kabel von einer Trommel vor Ort nach Bedarf abgetrommelt und anschließend konfektioniert bzw. gespleißt werden. Techniken mit vorkonfektionierten Kabeln machen wenig Sinn. Damit beschränkt sich die Eignung von vorkonfektionierten Kabeln oder ähnlichen Techniken auf den Serverraum, also auf die Hauptverteilungsverkabelung (HVK) bzw. Bereichsverteilungsverkabelung (BVK).

Geht man davon aus, dass die HVK primär dazu dienen wird, Inter-Switch-Verbindungen aufzubauen, so wird das präferierte Medium dafür Lichtwellenleiter sein, Twisted Pair wird selten benötigt und kann möglicherweise sogar ganz vermieden werden. Auf eine detaillierte Diskussion der Vor- und Nachteile der verschiedenen Fasertypen wird im Artikel verzichtet, dazu sei nochmals auf den Netzwerk-Insider März 2009 hingewiesen. Als Best-Practice-Standard im Rechenzentrum haben sich OM3 oder OM4 für Multimodefasern etabliert und OS1 für Singlemodefasern (vereinzelt werden auch OS2 verwendet).

Anders dagegen sieht es in der BVK aus, sowohl OM3/OM4 (für alle Datenraten) als auch Twisted Pair (bis maximal 10 Gbit/s über Klasse-EA-Verkabelung) müssen vorgesehen werden, um Serveranschlüsse aber auch kostengünstige Inter-Switch-Verbindungen realisieren zu können. Die Singlemodefaser wird nur selten für Serveranschlüsse eingesetzt werden können, ganz ausgeschlossen werden sollte sie aber nicht. Viele Untersuchungen unterschiedlichster Kabelhersteller haben gezeigt, dass die maximalen Distanzen der BVK in den meisten Rechenzentren unter 100 m liegen. Folgt man der oben beschriebenen Annahme, dass sich verstärkt TotR, MotR oder EotR durchsetzen werden, reduziert sich die zu erwartende Maximallänge der Kabel in der BVK nochmals auf ca. 20-25 m (maximal 15 Schränke pro Reihe mit je 80 cm Breite plus Höhe im Schrank). Damit sind beide HVK und BVK am ehesten geeignet, mit vorkonfektionierten Kabeln ausgestattet zu werden.

Anforderungen an die Verkabelung

Ausgehend davon, dass die oben bereits beschriebenen übertragungstechnischen Qualitäten der Kabelmedien eingehalten werden, gilt es nun, die darüber hinausgehenden Anforderungen zu beschreiben. Dies sind kurz aufgezählt:

- Geringer Platzbedarf der Anschlusstechnik

- Hohe Zuverlässigkeit der mechanischen Verbindungstellen zur Sicherstellung einer reproduzierbaren guten Dämpfung und Reflexionsdämpfung
- Leichte Bedienbarkeit der Steckverbindungen
- Leichte Neuverlegung der Installationskabel und Änderung der Installation
- Geringer Platzbedarf der Verkabelung
- Komfortable Techniken zur Führung der Rangierkabel

Eine starke Reduzierung des benötigten Platzbedarfes, in der Regel ausgedrückt durch eine geringe Anzahl von Höheneinheiten pro Portanzahl, wird immer dann von Bedeutung sein, wenn mit einer hohen Anzahl von Ports zu rechnen ist. Deshalb ist diese Forderung wichtig für die BVK, in einer hierarchischen Struktur wird die Portanzahl bei der HVK eher gering sein. Ausgehend von klassischen Rangierfeldern ergeben sich üblicherweise 24 Ports pro Höheneinheit plus 19"-Kabelführung (ebenfalls 1 HE). Natürlich gibt es auch klassische Rangierfelder mit 48 Ports pro HE, aber die Praxiserfahrungen mit derartigen Systemen sind eher negativ zu bewerten. Damit lassen sich bei 24 Ports z.B. 24 Twisted-Pair-Anschlüsse (RJ45 oder auch andere Systeme) oder 48 Fasern auf zwei Höheneinheiten inkl. 19"-Kabelführung unterbringen (24 LC-Duplex bzw. SC-Duplex). Soll mit einer Abkehr von der klassischen Verkabelung eine Reduzierung des Platzbedarfes erreicht werden, wäre insbesondere bei Glasfaser die Faseranzahl pro HE zu erhöhen, bei Kupfer kann eine Möglichkeit zur massiven Erhöhung derzeit ausgeschlossen werden.

Es gibt zwei Möglichkeiten die Portdichte zu erhöhen: die eine besteht darin, dass man die vorhandenen LC-Anschlüsse (SC kann aufgrund seiner Größe grundsätzlich als Steckertechnik im Rechenzentrum ausgeschlossen werden) dichter packt und damit die gewohnte LC-Duplex-Technik beibehält. Bei Möglichkeit zwei werde andere Steckertechniken in den Rangierfeldern zum Einsatz gebracht. Diese Steckertechniken sollten die gleiche Zuverlässigkeit und gleiche Bedienbarkeit haben wie LC.

Die einfache Neuverlegung bzw. Möglichkeit zur Änderung der verlegten vollständigen Strecken (also Kabel plus Abschluss) stellt eine spezielle Anforderung im Rechenzentrum dar. Man ist bestrebt, möglichst schnell und ohne Einsatz von komplizierten Montagetechniken wie Spleißen von Pigtails oder Kleben von Steckern auszukommen. Es kommen nur Lösungen in Frage, bei denen vorkonfektionierte Kabel verlegt werden, dies kann im Prinzip ohne speziell ausgebildete Handwerker erfolgen. Diese Kabel, in der Regel als Trunk-Kabel bezeichnet, müssen sich leicht durch enge Öffnungen und um enge Kurven verlegen lassen, ohne dass die bereits angeschlossenen Stecksysteme beschädigt werden können. Das macht enge Minimalbiegeradien und Einziehschutzhilfen (z.B. Zugstrümpfe am Ende der Kabel) sinnvoll. Die installierte Verkabelung wird möglicherweise nicht statisch sein, denkbare Änderungen sind beispielsweise:

- Ein vorhandenes Server-Rack soll umgestellt werden, dabei soll die Trunk-Verkabelung auch am neuen Standort weiterverwendet werden können.

- An einem Trunk-Kabel mit einem Abschluss in mehreren LC-Duplex-Steckern soll eine Nutzungsänderung erfolgen, die es möglich macht, 8-faserige oder 20-faserige Techniken zu nutzen. Auch das Umgekehrte wäre denkbar, ein Mehrfaserstecker soll in Duplex-Anschlüsse umgewandelt werden.

Insbesondere das zweite Beispiel ist eine weitere wichtige Anforderung, die es zu beachten gilt, denn der Wechsel von verschiedenen Gigabit-Ethernet-Techniken lässt sich nicht unter Beibehaltung derselben Steckertechnik vornehmen.

Im Bereich der BVK ist mit einer hohen Menge an bereitzustellenden physikalischen Kanälen zu rechnen, was je nach Kabelmedium zu einer hohen Anzahl von Installationskabeln und damit zu einem großen Volumen führt. Eine Reduzierung des Volumens bringt folgende Vorteile mit sich:

- Im Falle einer Führung der Kabel durch den Doppelboden kann der kühlende Luftstrom besser durchfließen.
- Im Falle einer Führung der Kabel durch eine Schrankreihe selber (z.B. bei MotR-Lösungen) können die Kabelführungssysteme kleiner dimensioniert werden.
- Bei Kabelführung in Trassensystemen oberhalb der Schränke können diese kleiner dimensioniert werden.
- Das Zurückziehen von Kabeln wird leichter.
- Die schrankrückseitige Zuführung der Kabel zu Rangierfeldern wird deutlich übersichtlicher und macht „handwerkliche" Arbeiten in diesem Bereich einfacher.

Zwangsläufige Konsequenz einer Verdichtung der Ports im 19"-Bereich wird sein, dass bei einer umfangreichen Beschaltung der Ports eine sehr hohe Anzahl von Rangier- oder Anschlussschnüren von den Feldern wegzuführen ist. Dies muss möglich sein, ohne dass es zu Problemen bei den Biegeradien kommt, ohne dass ein Beschalten zu Beschädigungen der Stecker führt, ohne dass ein Lösen von Steckverbindungen besonderes Werkzeug erfordert. Da nie davon auszugehen ist, dass die Länge der Anschlusskabel genau passend ist, müssen die Überlängen in irgendeiner Form abgelegt werden, so dass ein Entfernen der Anschlusskabel oder eine Änderung der Aufschaltung davon wenig beeinträchtigt werden. Eine Verdichtung von Ports um jeden Preis wird ohne Einbeziehung der beschriebenen Folgen kontraproduktiv sein, die ver-

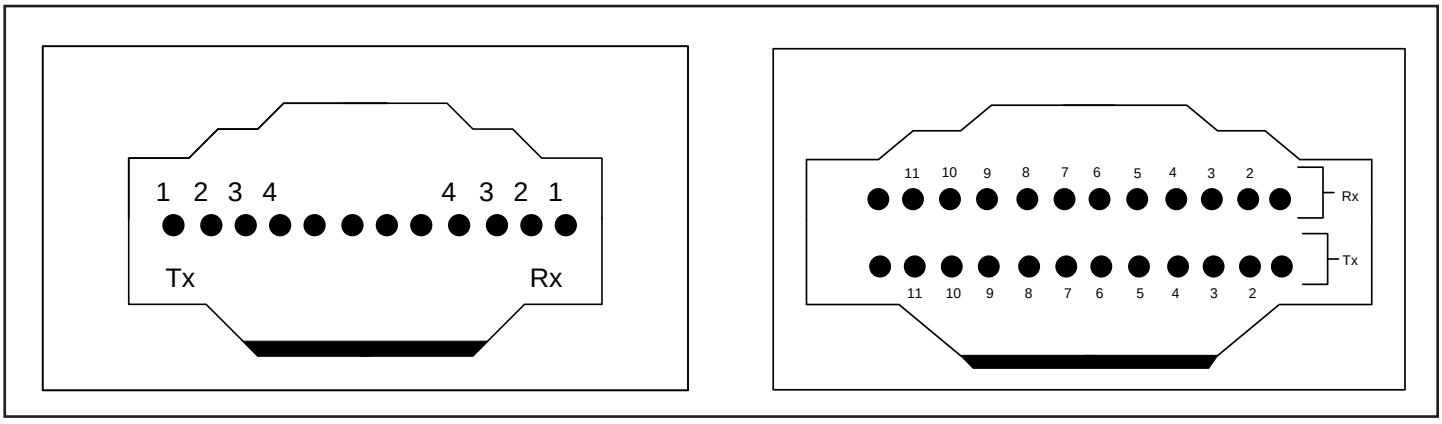


Abbildung 2: Genutzte Fasern im MPO-Stecker (links 40GE, rechts 100GE)

Trunk-Verkabelungen im Rechenzentrum, Fluch oder Segen?

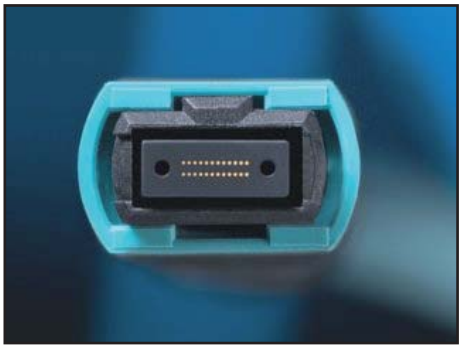


Abbildung 3: MPO-Stecker Bildquelle: RdM

schiedenen Herstellerlösungen müssen auch in diesem Punkte verglichen werden.

Allgemeine Lösungen für vorkonfektionierte Verkabelungen

Im nächsten Teil des Artikels werden die grundsätzlichen Lösungsansätze ohne gezielten Vergleich der Hersteller dargestellt werden, ein ausführlicher Herstellervergleich wird in einem Folgeartikel des Netzwerk-Insiders erfolgen (Vorabergebnisse geplant auf dem „ComConsult Rechenzentrum Infrastruktur-Redesign Forum 2013“). Zwei unterschiedliche Strategien sind zu nennen:

Bei der Lösung 1 werden High-Density-Installationskabel (z.B. mit bis zu 144 Fasern) werksseitig bereits mit LC-Steckern versehen, mit Hilfe eines Einziehstrumpfes verlegt und auf hochverdichtete Rangierfelder aufgelegt. Die Möglichkeit zu einer Änderung der Anschlusstechnik am Rangierfeld würde sich etwas schwieriger gestalten, hier wird eine Neukonfektionierung im Schrank oder gar eine Neuverlegung eines Kabels mit anderen Anschlusstechniken notwendig. Gerade diese Möglichkeit der „physikalischen Skalierbarkeit“ ist aber für alle Nutzer wichtig, die einfach zwischen den Datenraten 10 Gbit/s und 40/100 Gbit/s über Multimodefaser wechseln können möchten. Damit ist dieser Lösungsansatz nicht ausreichend.

	Standard Multimode MT-Ferrule	Elite Multimode MT-Ferrule
Einfügedämpfung	0,1 dB typisch über alle Fasern 0,35 dB maximum	0,2 dB typisch über alle Fasern 0,6 dB maximum
Rückfluss-dämpfung	> 20 dB	> 20 dB

Tabelle 1: Technische Werte MTP® nach US Conec

Bei der Lösung 2 kommen ebenfalls High-Density-Installationskabel zum Einsatz, diese „enden“ jedoch in einem Mehrfachstecker. Konkret gibt es derzeit bei allen Systemanbietern dazu nur einen Typ: Sogenannte MPO-Systeme (multipath push-on). Bereits vor der Entwicklung von 40/100 Gigabit über Ethernet, welche den Einsatz einer neuen Steckverbindertechnik mit mehr als 2 Multimodefasern zwingend notwendig macht, berücksichtigten erste Herstellerlösungen für Glasfaseranschlusstechniken diesen Vielfachstecker. Er ist keine neue Erfindung, sondern wurde bereits Anfang der 80er-Jahre entwickelt. Definiert ist der Stecker in der IEC61754-7 und TIA/EIA 604-5, er wird in einer PC- wie auch in einer APC-Version (Singlemode) eingesetzt. Ein MPO-Stecker bzw. eine MPO-Ferrule kann bis zu 72 Fasern aufnehmen (6 Reihen mit je 12 Fasern), im Umfeld der Ethernet-Technologien werden aber nur zwei Typen benötigt, beide nur für Multimode, das ist für 40 Gbit/s die Version mit 12 Fasern und für 100 Gbit/s die Version mit 24 Fasern. Im nachfolgenden Bild ist zu erkennen, dass nicht alle Fasern genutzt werden. Bei 40GE sind es nur die äußeren 8 Fasern und bei 100GE nur die inneren 20 Fasern. Es ist erkennbar, dass ein 24er-MPO mit 24 Fasern nicht geeignet sein wird für rein 12-faserige Dienste, damit ist die Steckverbindertechnik von 100GE nicht ohne weiteres abwärtskompatibel zu 40GE-Techniken. (siehe Abbildungen 2 und 3)

In der Beschreibung einiger Herstellerlösungen speziell für das RZ-Umfeld taucht aber die Bezeichnung MTP® (Abkürzung steht für Mechanical Transfer Push-On) statt MPO auf, dies ist ein von US Conec weiterentwickelter MPO (IEC 61754-5) mit besseren technischen Eigenschaften, bedingt durch eine andere, präzisere Ferrulenführung. Der MTP® ist nach Angaben der ihn verwendenden Anbieter von Verkabelungssystemen abwärtskompatibel zu herkömmlichen MPO-Systemen. (siehe Tabelle 1)

Standard-High-Density-Kabel fassen in der Regel maximal 144 Fasern, es ließen sich damit Trunkkabel mit 12 MPOs zu jeweils 12 Fasern (= 12 40GE-Verbindungen) oder mit 6 MPOs zu jeweils 24 Fasern (= 6 100GE-Verbindungen) realisieren. Multimode-Trunk-Kabel müssen nicht zwangsläufig in MPOs enden, es können auch sogenannte Hydra-Kabel (oder auch Haarness oder Assemblies) mit entsprechenden LC-Duplex-Abschlüssen direkt bestellt werden. Derartige Kabel sollten aber nicht über größere Distanzen bzw. komplexere Kabelwege verlegt werden, da die meisten Hersteller keine Adaptierung von vorhandenen Hydra-Kabel auf MPO vorsehen und es dann zu einem Austausch des Hydra-Kabels kommen müsste. Es ist sinnvoller, die Trunk-Kabel grundsätzlich mit MPO-Ab-

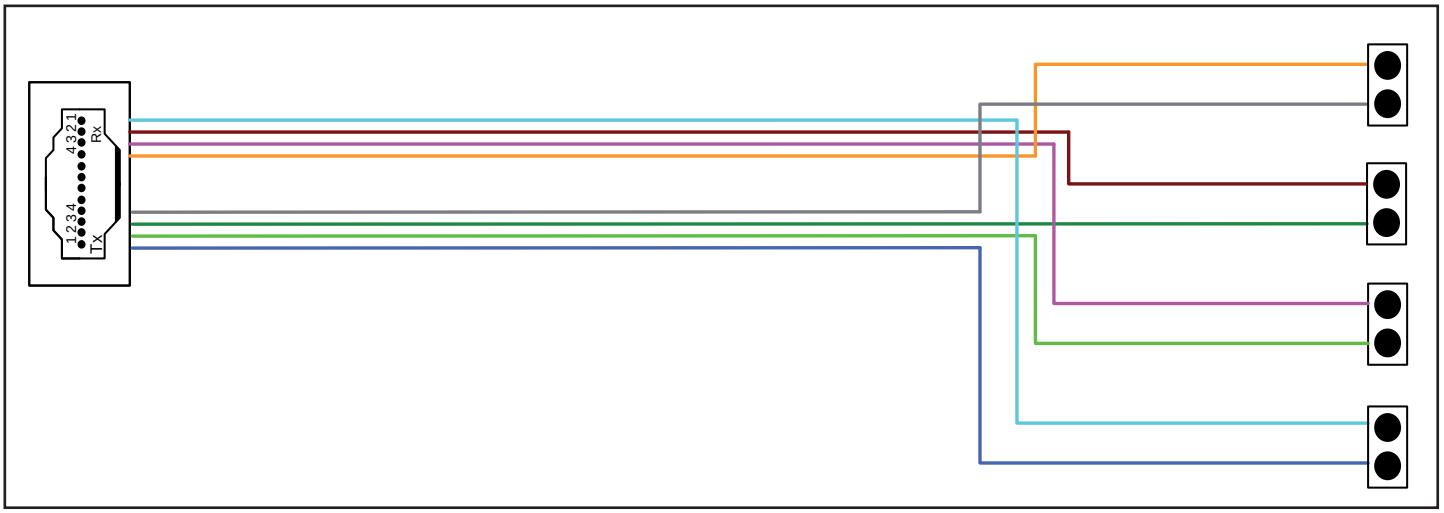


Abbildung 4: Hydra-Kabel mit 4 LC-Duplex

schlüssen einzusetzen und mit Hilfe von Adaptierungstechniken diese bei Bedarf auf LC-Duplex zu konvertieren. Dazu stehen zwei Techniken zur Verfügung:

Das erste wäre die bereits angesprochene Hydra-Technik. Ein Hydra-Kabel besteht aus einem MPO und mehreren LC-Duplex-Enden und wird auf den MPO des Trunks gesteckt. Die LC-Duplex können dann auf verschiedene Rangierfeldsysteme aufgesteckt werden oder gar direkt auf die aktiven Komponenten. (siehe Abbildung 4)

Ein „elegantere“ Lösung zur Adaptierung besteht darin, 19“-Aufteilmodule einzusetzen, die einen rückseitigen MPO-Anschluss haben für das Trunk-Kabel und frontseitig entsprechend mehrere LC-Duplex-Anschlüsse zur Beschaltung (es sind also zwei Steckverbindungen enthalten). Diese 19“-Aufteilmodule werden in speziellen 19“-Modulhaltern montiert. Bei den meisten Herstellern haben sich Modulhalter mit bis zu 3 oder 4 Modulen pro HE durchgesetzt (keine Kompatibilität zwischen den Herstellern) und der Platz auf einem Modul reicht für maximal 12 LC-Duplex aus, es lassen sich auf 1 HE also 72 bzw. 96 Fasern in LC-Duplex abschließen; entspricht also einer Verdopplung der Faseranzahl gegenüber klassischen Rangierfeldern. Bei einem Einsatz dieser Module ist zu beachten, dass der Dämpfungswert des gesamten Modules im Dämpfungsbudget einberechnet wird, hier liegen die Werte der besseren Systeme unter 0,5 dB.

Ein typisches kleines Beispiel für die Neuverkabelung von vielen RZs zeigt, wie diese Technik optimal bei Erhöhung von benötigen Datenraten genutzt werden kann: Die Mehrzahl der Schnittstellen in dem Bereich, in dem Trunk-Techniken sinnvoll sein können, stellen heute 10GE-Techniken dar. Als Konsequenz werden fast ausschließlich LC-Duplex im Rangierfeld benötigt. Der Schritt zu 40GE-Techniken ließe sich mit der beschriebenen Modultechnik sehr einfach machen, das Trunk-Kabel würde bleiben und die Aufteilboxen würden ausgetauscht gegen Boxen, die lediglich eine MPO/MPO-Kupplung haben.

Trunk-Techniken bieten also Vorteile in Zusammenhang mit einer Reduzierung von 19“-Montagefläche (und damit auch Racks im Rechenzentrum), einer Reduzierung des Kabelvolumens und einer deutlich besseren Skalierbarkeit bei kurz- und mittelfristig benötigten höheren Datenraten. Trunk-Techniken bieten keinen Kostenvorteil bei der reinen Erstinvestition für die Verkabelung selber. Die Kostenersparnis entsteht „erst“ im Laufe des Betriebs, bedingt durch ein einfacheres Handling. Eine Einführung von Trunk-Techniken, resultierend aus dem Gedanken, eine kostengünstigere Verkabelung einzuführen wäre grundfalsch, Investitionskosten werden nur gespart, wenn eine Reduzierung der Schrankanzahl im Rechenzentrum das Ergebnis wäre.

Doch leider führt die Einführung von Vielfachsteckern zu einer deutlichen Steigerung der Planungskomplexität und erschwert den Alltagsbetrieb, wie nachfolgend gezeigt wird.

Besonderheiten des MPO/MTP®

Eine erste besondere, sowohl bei der Planung wie auch beim Betrieb zu beachtenden Eigenschaft von MPO-Verbindungen (nachfolgend steht im Artikel MPO auch für MTP®, sofern es keine explizite Unterscheidung gibt) besteht darin, dass eine einfache 1:1-Verkabelung wie bei zweifaserigen Systemen nicht mehr durch Änderung der Faserkreuzung in den Patchkabeln möglich ist. Stattdessen muss man sich bereits bei dem Erwerb bzw. der Verlegung von MPO/MPO-Strecken Gedanken machen, wie die Fasern an beiden Enden zueinander aufgelegt wurden. Auch für den Fall, dass ein MPO mit Hilfe von Hydra-Kabeln oder Aufteilboxen (Kassetten) in mehrere LC-Duplex-Anschlüsse umgewandelt wird, muss dieses entsprechend berücksichtigt werden. Um diesen Polaritätswechsel auch im Betrieb möglich zu machen, wurde eine Führungsnut (Bezeichnung der EN 50174: Kodiernase) an der Oberseite jedes MPO-Steckers und jedes Kupplungsanschlusses vorgesehen, die dazu führt, dass der MPO wahlweise nach oben oder nach unten in die Kupplung gesteckt werden kann. Es gibt Kupplungen, bei denen die Nut vorne und hinten nach oben ausgerichtet ist (key-up to key-up) und es gibt Kupplungen, bei denen ist die Nut einmal oben und einmal nach unten (key-up to key-down) ausgerichtet. Die Kupplung mit unterschiedlichen Nut-Positionen führt zu einem Polaritätswechsel und wird in Form von drei, in der TIA/EIA-568-C.3 normierten Varianten für den 12-faserigen MPO zugelassen. In der Kupplung kann aber der Stecker nicht zunächst mit Nut nach oben eingesteckt werden und später dann gedreht nach unten, mit der Auswahl der Kupplung ist das fest vorgegeben. Der Hersteller Panduit bietet einen Stecker an, bei dem die Nut-Position sowie Male/Female (siehe Abbildung 5) einfach geändert werden können.

Es kommt noch eine weitere, nicht unbedingt den Betrieb vereinfachende Besonderheit hinzu: Zur Erzielung einer hochpräzisen Ferrulen-Führung beim Zusammenstecken von zwei MPO-Verbindern besitzen die Male-Stecker 2 Führungsstifte, die Female-Stecker entsprechend 2 Öffnungen (Schiebehülsen). Die Ausrichtung der Fasern wird dann beim Zusammenstecken durch die Führungsstifte gesteuert. Man muss bereits bei der Planung der festen MPO-Strecken festlegen, ob ein Male- oder Female-Stecker verwendet werden soll. Steckt man irrtümlich zwei Male-Stecker oder zwei Female-Stecker zusammen, wird es keine akzeptable Einfügedämpfung geben, der Link könnte möglicherweise nicht zustande kommen. Schlimmer aber ist bei Male-Male-Verbindungen, dass sich dabei die Führungsstifte verbiegen können und damit der Male-Stecker unbrauchbar wird. Daraus resultiert die Empfehlung der EN 50174-1, bewegliche MPO-Stecker (z.B. an Patchkabeln) in Female auszuführen und den Male-Anschluss an geschützten MPO-Steckern, z.B. an Trunk-Kabeln oder an Modulen/Kassetten vorzusehen. Da an den SFPs der aktiven Komponenten zumeist Female-Anschlüsse sind (was Beschädigung von Stiften im SFP ausschließt), würden für diesen Fall Female-Male-Patchkabel (Female an der Trunk-Kupplung und Male an dem SFP) benötigt, die aber nicht umgedreht angeschlossen werden dürfen.

Entsprechende Problematik ergibt sich auch bei Hydra-Kabeln: Zum Anschluss an ein SFP (z.B. bei einem Cisco QSFP-Port) muss der MPO als Male-Anschluss ausgelegt sein. Dieses Kabel darf man

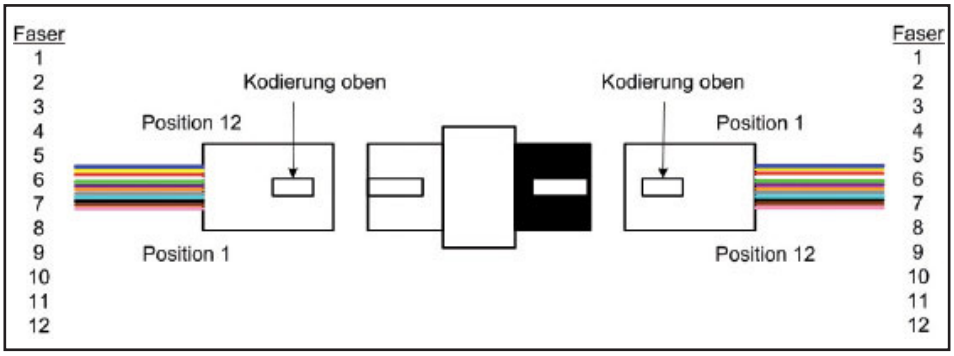


Abbildung 5: Adapter für Mehrfachsteckverbinder Quelle: EN 50174-1

aber nicht an einen Trunk-Port anschließen, falls dieser ebenfalls in Male ausgelegt ist. Somit müssen auch hier unterschiedliche Hydra-Kabel verwendet werden, welche am besten deutlich gekennzeichnet sind.

Die vorausgehend beschriebenen Spezialitäten machen deutlich, dass eine Migration von einer einmal eingerichteten 40Gbit/s-MPO-Verkabelung nur durch einfaches Austauschen der Hydra-Kabel oder Adapter auf 100Gbit/s nicht so einfach möglich ist, zu unterschiedlich sind die MPO-Belegungen. Stattdessen muss damit gerechnet werden, in die Infrastruktur der festverlegten Trunk-Kabel einzugreifen. Trunk-Kabel, die in 12-faserigen MPO-Steckern enden, müssen ausgetauscht werden oder durch ein zweites 12-faseriges ergänzt und mit Y-Kabeln zusammen zu 24 Fasern gekoppelt werden.

Ob der Einsatz von Trunk-Technologien tatsächlich eine Ersparnis bei den Betriebskosten mit sich bringen wird, hängt sehr stark davon ab, wie häufig Fehlbedienungen zu Beschädigungen oder zu anderen Problemen führen werden und wie einfach die Vorratshaltung der unterschiedlichen Steck-Systeme sein wird. Die seitens der Hersteller angepriesene Betriebs- und Investitionssicherheit wird nur erzielt, wenn erhebliche Reserven beim Aufbau der Verkabelung eingeplant werden wie z.B. 24-faserige MPO-Systeme statt 12-faserige Systeme.

Fazit

Aus Sicht des Autors gab es bisher in der Historie der IT-Verkabelung keine Technik, die ein derart starkes Umdenken erfordert und einen schwierigen Einstieg notwendig macht wie der Einsatz von MPO-Techniken. Die Einführung dieser neuen Technik basiert nicht auf der Überzeugung oder Notwendigkeit, eine Verbesserung der grundsätzlichen Stecker-Handhabung zu erzielen, sondern sie basiert ausschließlich darauf, dass die Entwicklung im Bereich der aktiven Netzwerktechnik nicht in der Lage war, 40/100-Gbit/s auf einer einfachen 2-Faser-Lösung mit Multimode umzusetzen. Würden die Kosten der SFPs bei zweifaseriger Singlemode-Technik auch nur ansatzweise ähnlich sein zu den Kosten der vielfaserigen Multimode-Technik, so könnte sehr stark davon ausgegangen werden, dass niemand diese sehr komplexen MPO-Techniken einführen würde. Da dem so aber nicht ist, werden alle kurzfristigen Realisierungen von 40/100-Gbit/s, insbesondere bei einer größeren Anzahl von Links, ohne eine Verwendung dieser Technik kaum möglich sein und dem Planer kann nur angeraten werden, sich frühzeitig mit den Tücken - aber auch Chancen - dieser Technik auseinanderzusetzen.

Allen, die kurz- und mittelfristig weder eine Einführung von größeren Mengen an 40/100-Gbit/s-Ports planen noch mit erheblichen Platzproblemen im Rechenzentrum zu rechnen haben, wird von einer Verwendung von MPO-basierenden Trunk-Techniken in einem zu frühen Zeitraum abgeraten.

Standpunkt Sicherheit

Virtualisierte Sicherheits-komponenten als Konsequenz moderner RZ-Konzepte

Der Standpunkt Sicherheit 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.

Durch die Virtualisierungstechnik werden Aufbau und Betrieb eines modernen Rechenzentrums (RZ) signifikant neu geprägt. Das aktuelle Schlüsselthema ist hierbei die RZ-Automatisierung. Dabei geht es insbesondere um die automatische Provisionierung, d.h. die Zuweisung von Virtuellen Maschinen (VMs) zu Virtualisierungs-Hosts, die automatische Herstellung der notwendigen Netzanbindungen und den automatischen Lastausgleich zwischen Hosts.

Einrichtung und Zuweisung eines neuen Dienstes, einer neuen Applikation dürfen hierzu keine physikalische Änderung der Infrastruktur erfordern. Die physikalische Infrastruktur muss von Diensten, Applikationen und damit den logischen Strukturen so weit entkoppelt werden, dass die Einrichtung von Diensten und Applikationen ausschließlich auf der logischen Ebene erfolgen kann. In Summe bedeutet das Virtualisierung auf allen Ebenen der Infrastruktur.

Bereits dies hat erhebliche Konsequenzen für die Informationssicherheit. In der Vergangenheit war die physische Trennung von Systemen mit erheblich unterschiedlichem Sicherheitsniveau eine gängige Praxis. Es ist bis heute üblich Systeme und Netze in einer Internet Demilitarized Zone (DMZ) von solchen im Intranet physisch zu trennen, d.h. es gibt eigene Virtualisierungs-Hosts, sonstige Server, Switches und Gateways für eine Internet DMZ. Zusätzlich führt man auch oft auch eine physische Trennung von Systemen mit hohem Schutzbedarf von solchen mit normalem Schutzbedarf durch. Eine solche physische Trennung widerspricht allerdings dem Gedanken der RZ-Automatisierung recht deutlich, denn für jeden physisch getrennten Strang müssten beispielsweise eigene, unabhängige Automatisierungsinstanzen vorgesehen werden.

Wir müssen uns daher bewusst sein, dass aus wirtschaftlichen Gründen im RZ eine

maximale Konsolidierung immer stärker gefordert wird. Das RZ stellt letztendlich eine (!) physische Infrastruktur zur Verfügung, auf der VMs provisioniert werden. Als Folge könnten auf einem physischen Server VMs einer Internet DMZ gemeinsam mit hochkritischen internen Datenbanken laufen, lediglich getrennt durch die Mittel der Virtualisierungslösung und durch eine logische Netztrennung auf Switches.

Maximale Konsolidierung erfordert zwingend eine entsprechende Härtung auf Ebene der Virtualisierungs-Hosts und des Netzes. Hier bietet sich zunächst die Anwendung des Bausteins B 3.304 „Virtualisierung“ der IT-Grundschutz-Kataloge des Bundesamts für Sicherheit in der Informationstechnik (BSI) an, ergänzt um die Anwendung der herstellerspezifischen Vorgaben für den Einsatz von Virtualisierungstechniken in exponierten Bereichen und solchen mit erhöhtem Schutzbedarf. Für VMware wäre dies beispielsweise verbunden mit der Umsetzung der Maßnahmen der Profile 3 und 2 des vSphere 5.1 Security Hardening Guide. Bei entsprechenden Sicherheitsanforderung bzw. hohem Schutzbedarf würden dann zumindest selektiv auch Maßnahmen des Profils 1 in Betracht zu ziehen sein.

Mit dem skizzierten Einsatz von Virtualisierungstechniken etabliert sich im Virtualisierungs-Host zwingend ein Mikrokosmos der Netzinfrastruktur, da VMs durch den Einsatz von virtualisierten Switches vernetzt werden und die entsprechenden VLAN-Konfigurationen dynamisch per RZ-Automatisierung bereitgestellt werden müssen. Aus dem Blickwinkel der Informationssicherheit passiert hier etwas Wesentliches: Die Vernetzung der Elemente unterschiedlicher Gruppen von VMs, insbesondere Sicherheitszonen ist dynamisch und spielt sich ggf. innerhalb des Virtualisierung-Hosts ab und ist außen z.B. für eine Firewall nicht mehr sichtbar.

Dies hat bereits seit geraumer Zeit dazu geführt, dass Firewall-Hersteller virtualisierte Firewall Appliances entwickelt haben, die – eine entsprechende virtualisierte Vernetzung vorausgesetzt – innerhalb des Mikrokosmos Virtualisierungs-Host die Kommunikation zwischen Sicherheitszonen filtern können. Da hier eine Firewall (oder eine andere Sicherheitskomponente) als VM realisiert würde, vererben sich alle Gefährdungen für VMs auf die virtualisierte Firewall und außerdem lässt die Performance zu wünschen übrig.

Durch eine stärkere Integration in den Hypervisor bzw. in die virtualisierten Switches, bei der z.B. mit einer sogenannten VMNIC Firewall eine Firewall-Instanz vor den virtualisierten NIC einer VM gesetzt werden kann, können zumindest die Leistungsengpässe vermieden werden. Als weitere Alternative bietet sich die Kooperation von Hypervisor bzw. virtualisiertem Switch und einer externen (physischen) Firewall an (als Service Insertion bezeichnet). Bei dieser Technik wird der Verkehr systematisch vom Virtualisierungs-Host zur Inspektion an die externe Firewall geleitet und dort die Filterentscheidung getroffen und zurück zur Virtualisierungslösung kommuniziert.

Diese Techniken dürfen keinesfalls unterschätzt werden. Da die eigentliche Vernetzung von VMs sich auf Ebene der Virtualisierungs-Host abspielt, wird die physische RZ-Netzinfrastruktur nur noch zum hochperformanten Transport benötigt. Die Idee ist erschreckend einfach: Virtualisierungs-Hosts werden über das RZ-Netz mit den Mitteln von Ethernet und IP statisch vernetzt. Die Kommunikation der VMs erfolgt dann über einen Tunnel, der Layer-2-Pakete transportiert. Es entstehen Overlay-Netze im RZ, welche automatisiert den jeweiligen Konnektivitätsanforderungen

entsprechend dynamisch erzeugt werden und die statische Vernetzung des RZs als Basis nutzen. Natürlich zeichnen sich hier schon entsprechende Standards ab, z.B. bei der IETF mit Network Virtualization Overlay (NVO). Es ist nicht überraschend, dass NVO auch die Möglichkeit der Verschlüsselung solcher Tunnel zwischen Virtualisierungs-Hosts vorsieht.

Damit sind wir automatisch wieder beim Thema Verkehrskontrolle und -filterung durch Sicherheitselemente. Eine Firewall müsste nun in die Tunnel zwischen den Virtualisierungs-Hosts hinein schauen können, um sinnvolle Entscheidungen zu treffen. Dies wäre auch denkbar schwer, wenn der Verkehr zudem noch verschlüsselt wäre. Also muss die Firewall zwangsläufig in die Nähe der eigentlich zu filternden Netze, d.h. der Virtualisierungs-Hosts rücken, was eine der genannten technischen Lösungen zur Virtualisierung von Firewalls impliziert. Wir werden also Sicherheitselemente als Bestandteil von Virtualisierungslösungen in Betracht ziehen müssen.

Winterschule 2013

General Erneuerung LAN, WAN und IT-Architekturen

09.12. - 13.12.13 in Aachen

Die ComConsult Akademie veranstaltet vom 09.12. bis 13.12.13 ihre "ComConsult Winterschule 2013" in Aachen.

Das technologische Umfeld von Netzwerken befindet sich in einem der intensivsten Änderungsprozesse der letzten 20 Jahre. Das betrifft Endgeräte, das Rechenzentrum, Anforderungen an einen immer effizienteren Betrieb bis hin zu Unified Communications und einem Wandel unseres Verständnisses von Kommunikation. Die ComConsult Winterschule 2013 analysiert diese Veränderungen und zeigt auf, wie Netzwerke und Infrastrukturen diesem Wandel begegnen können.

Die Winterschule 2013 ist unterteilt in die Themenbereiche:

1. IT-Architekturen und Auswirkungen auf Netzwerke
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 hingeht und wie Netzwerke aussehen müssen, um diesen Weg zu unterstützen.

2. IPv6
Der Wechsel kommt und er kommt immer schneller. Die technischen Details sind komplex, hier geht es um viel mehr als nur um neue Adressen. IPv6 arbeitet einfach anders als IPv4. Das schafft neue Herausforderungen in allen Bereichen. Wir zeigen auf, wie ein gutes Design aussehen kann und speziell welche neuen und alten Sicherheits-Risiken mit IPv6 verbunden sind und wie sie vermieden werden.

3. LAN-Technologien: aktuelle Entwicklungen
LAN-Technik wird im Moment neu erfunden. Neue Anforderungen erfordern neue Lösungen. Programmierbare Netzwerke als Teil des Software Defined Data Center und als Teil von Software Defined Infrastrukturen sind ein Beispiel dafür. Neue Fabric-Konzepte, ein Umdenken bei VLAN-Technik, eine Neupositionierung von QoS und neue Nutzungsformen im Rahmen von Audio-/Video-Bridging sind herausragende Beispiele. Wir erklären, was im Moment passiert und wie sie sich auf die Zukunft vorbereiten.

4. RZ-Technik
Das gerade abgeschlossene Intel Developer Forum IDF 2013 und die Oracle Open World haben es auf den Punkt gebracht: das Rechenzentrum der Zukunft wird sich deutlich von unserem traditionellen Verständnis unterscheiden. Mehr Effizienz, weniger Aufwand, mehr Flexibilität im Umfeld neuer Service-Modelle sind die Ziele. Wir diskutieren mit Ihnen, wo Server und Virtualisierung hingehen und wie Speicher-Lösungen sich in das Bild einfügen.

5. WLAN und LTE
Mit dem Desktop stirbt das Kabel. Oder auch nicht. Der Wechsel zu mobilen Endgeräten erfordert ein Umdenken bei der Versorgung von Endgeräten. Im Mittelpunkt der Diskussion stehen die neuen Gigabit-Wireless-Standards, die enorme Konsequenzen auf die zukünftige Gestaltung haben. Die bisherigen Planungsansätze sind praktisch tot. Das WLAN der Zukunft ist der Kern der Endgeräteversorgung und es sieht anders aus als die bisherigen Lösungen. Wir zeigen auf, wo der Weg hingeht und warum er technisch nicht ohne Probleme ist.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Ich buche das Intensiv-Seminar
ComConsult Winterschule 2013

☐ vom 09.12. - 13.12.13 in Aachen
zum Preis € 2.290,-- netto*
* gültig bis zum 31.10.13

☐ Bitte reservieren Sie mir ein Zimmer

vom _____ bis_____ 13

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

_____ Vorname

_____ Nachname

_____ Firma

_____ Telefon/Fax

_____ Straße

_____ PLZ,Ort

_____ eMail

_____ Unterschrift

Zweitthema

Gefahr durch IPv6?

Fortsetzung von Seite 1

Markus Schaub ist seit 2009 Leiter von ComConsult-Study.tv. Er verfügt über umfangreiche Berufserfahrung in den Bereichen Netzwerken und VoIP und ist seit mehr als 13 Jahren bei ComConsult beschäftigt. Seine Schwerpunkte liegen im Netzwerk-Design, IP-Infrastrukturdiensten und SIP, zu denen er viele Vorträge auf Kongressen hielt, erfolgreich Seminare durchführte und zahlreiche Veröffentlichungen schrieb.

Die Gefahr lauert schon beim Booten

Neben IPv4 wird schon seit geraumer Zeit bei allen gängigen Betriebssystemen auch IPv6 gestartet. Abbildung 1 zeigt die Einstellung von Windows 7. Wie leicht zu erkennen, ist IPv6 auf Autokonfiguration eingestellt.

Dasselbe gilt aber auch für andere Betriebssysteme wie OS X beim Mac und diverse Linux-Distributionen wie die Abbildungen 2 und 3 zeigen.

Findet ein Rechner bei IPv4 keinen DHCP Server und wurde auch nicht manuell konfiguriert, so griffen einige Hersteller auf eine Art „zeroconf“ zurück und der Rechner hatte anschließend eine Adresse aus dem Bereich 169.254.1.0 bis 169.254.254.255. Kommuniziert werden konnte damit eigentlich, war es doch in aller Regel der einzige Rechner in diesem Subnetz. Es ist eher nervig als hilfreich, eine ordentliche Fehlermeldung der Art „Es konnte keine gültige IP Adresse bestimmt werden“, wäre sinnvoller. So scheint es, als wäre alles ok, nur kommunizieren kann man nicht.

Bei IPv6 ist das anders: die „Stateless Address Autoconfiguration“ (SLAAC) ist kein Add-On, sondern immanenter Bestandteil des Protokolls. Auch wer DHCPv6 einsetzt kommt nicht umhin, Teile davon nutzen zu müssen. Und wer glaubt, gar kein IPv6 zu nutzen, hat trotzdem eine gültige IP Adresse pro Interface, mittels derer er mit seinen Nachbarn kommunizieren kann, wenn diese auch einen aktivierten IPv6 Stack haben.

Eine aktive IP Adresse ist aber immer auch ein Einfallstor für Angreifer.

Die Angriffsfläche

Schauen wir uns darum zunächst einmal den Bootvorgang an. (vgl. Abbildung 4)

Neben einigen optionalen Schritten werden immer folgende Schritte durchlaufen:

1. Generierung einer Link-Local Adresse
2. Duplicate Address Detection für die Link-Local Adresse (DAD, Paket 1)
3. Router Solicitation (Pakete 2 und 4)
4. Router Advertisement (Paket 5)
5. Generierung einer Globalen Adresse
6. Duplicate Address Detection für die Globale Adresse (DAD, Paket 6)

Diese Abfolge wird mit Ausnahme von Punkt 5 auch bei Einsatz von DHCPv6 durchlaufen. Es kommen zwischen 4 und 6 nur noch einige weitere Schritte hinzu, für die Kommunikation mit dem DHCP-Server. Drei wunderbare Angriffspunkte findet man bei 2., 4. und 6.

Schritt 2 und 6 sind im Grunde identisch: der Rechner generiert eine Adresse und prüft, ob diese bereits von einem anderen Gerät im Lokalen Netzwerk genutzt wird. Ist dem nicht so, aktiviert er die Adresse, ist dem so, lässt er es bleiben und generiert eine neue. Hier kann ein Angreifer natürlich sehr einfach einen Denial of Service Angriff fahren:

Abbildung 5 zeigt das Vorgehen: jeder Test des Clients wird durch den Angrei-

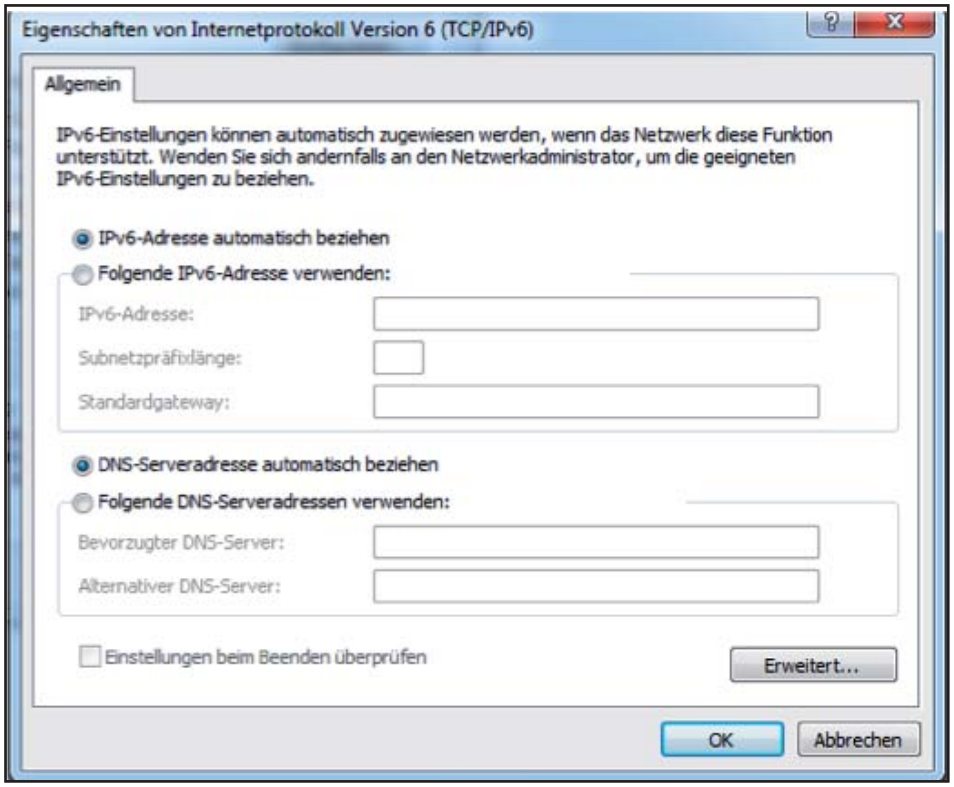


Abbildung 1: Defaulteinstellung von Windows 7

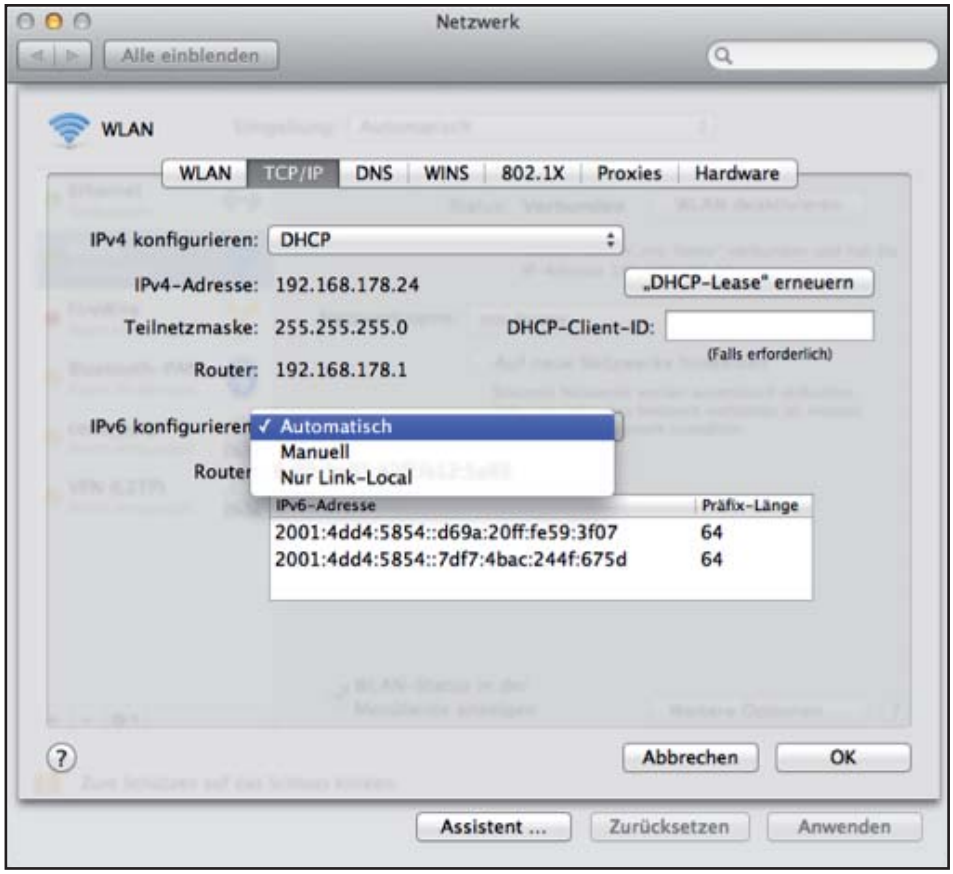


Abbildung 2: Defaulteinstellung von OS X

wand aufgetaucht.

Spannender wird es, wenn man sich die Schritte 4 und 5 genauer anschaut: die Zuweisung des Globalen IPv6 Präfixes. Hier ergeben sich völlig neue Möglichkeiten.

Nachdem der Client eine gültige Link-Local Adresse erworben hat, nutzt er diese um seinen Router zu finden. Dazu sendet er ein so genanntes Router Solicitation Paket an die Multicast-Adresse ff02::2, also an alle Router eines Subnetzes. Diese Pakete werden von einer Layer 2 Infrastruktur an alle Systeme desselben Layer 2 Netzes weitergeleitet, um sicher zu stellen, dass auch alle Router sie bekommen. Somit erreichen sie auch einen potentiellen Angreifer im selben LAN. Dieser sendet nun seinerseits Router Advertisements (RA, vgl. Abbildung 6).

Das Schöne an diesen Router Advertisements ist die Fülle an Möglichkeiten, die sie für Angriffe bieten.

Da wären zunächst einmal die beiden Flags M und O zu nennen. M steht für „Mananged" und O für „Other". Ist das Managed Flag gesetzt, so bedeutet das, der Client darf sich selbst keine IP Adresse geben, sondern muss sie sich anderswo besorgen. Aktuell bedeutet das: von

```
eth0      Link encap:Ethernet  Hardware Adresse 00:0c:12:34:56:78
          inet Adresse:192.168.178.26  Bcast:192.168.178.255  Maske:255.255.255.0
          inet6-Adresse: 2001:db8:7b52:0:20c:12ff:fe34:5678/64 Gültigkeitsbereich:Global
          inet6-Adresse: fe80::20c:12ff:fe34:5678/64 Gültigkeitsbereich:Verbindung
```

Abbildung 3: Debian Minimalinstallation nach dem Boot

No.	Time	Source	Destination	Info
1	0.000000	::	ff02::1:ff59:3f07	Neighbor Solicitation f
2	0.000096	fe80::d69a:20ff:fe59:ff02::2		Router Solicitation
3	1.000425	fe80::d69a:20ff:fe59:ff02::1		Neighbor Advertisement
4	4.699502	fe80::d69a:20ff:fe59:ff02::2		Router Solicitation fro
5	4.813736	fe80::be05:43ff:fe12:ff02::1		Router Advertisement fr
6	4.813964	::	ff02::1:ff59:3f07	Neighbor Solicitation f

Abbildung 4: Startvorgang mit Wireshark

fer mit einem „Ja ich nutze diese Adresse" beantwortet. Das Spiel kann man so lange spielen, bis der Client aufgibt, oder bis zum Sanktnimmerleinstag.

Allerdings hat ein Angreifer damit „nur" verhindert, dass ein Client mit einer gültigen IPv6 Adresse ins Netz kommt. Das mag ggf. ärgerlich sein, da aber IPv4 ja weiterhin ein gültiger, wahrscheinlich sogar der einzig mögliche Weg ins Unternehmensnetz ist, hat der Angreifer eigentlich nichts gewonnen. Außerdem ist so etwas Ähnliches auch bei IPv4 möglich. Eine neue Gefährdung ist also nicht entstanden, nur eine „alte" in neuem Ge-

einem DHCPv6-Server. Das Other-Flag gibt an, ob er sich weitere IP-Konfigurationsoptionen bei einem DHCP-Server erfragen soll. Dazu gehören bspw. DNS-, NTP- oder SIP-Server. Grundsätzlich gilt dabei Folgendes: ist das M Flag gesetzt, so wird auch das O Flag gesetzt, jedoch kann das M Flag auf 0 stehen und das O

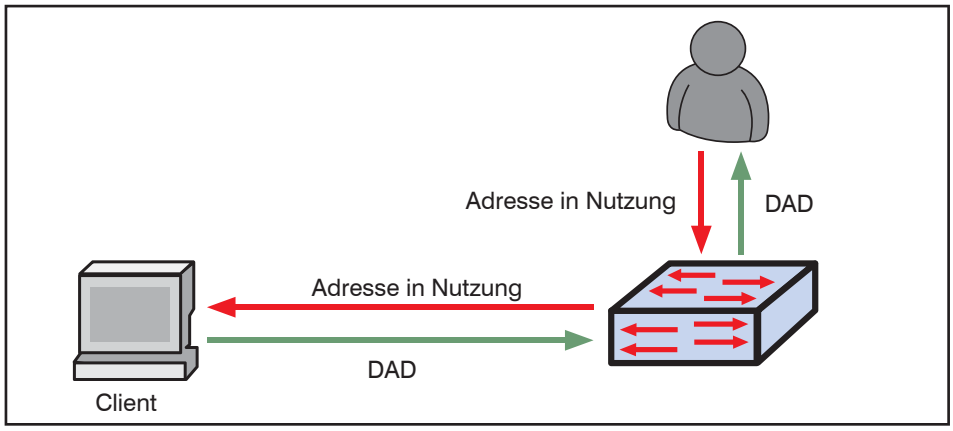


Abbildung 5: DoS bei DAD

So kann er beispielsweise auf seinem System einen BIND und einen Apache installieren und den Clients beliebige Webseiten vorgaukeln. Angefangen bei beliebten Einkaufsportalen bis hin zu Online-Banking-Webseiten. Das ist allerdings zugegebener Weise ziemlich aufwendig. Spätestens wenn nicht die richtigen Umsätze beim Online Banking angezeigt werden oder schlechte Nachbildungen der Amazon Webseite im Browser erscheinen, schöpfen die User Verdacht.

RA + DNS + NAT64

Eine andere Alternative wäre es, auf den Nachbau von Webseiten zu verzichten, und stattdessen auf dem Angriffsrechner

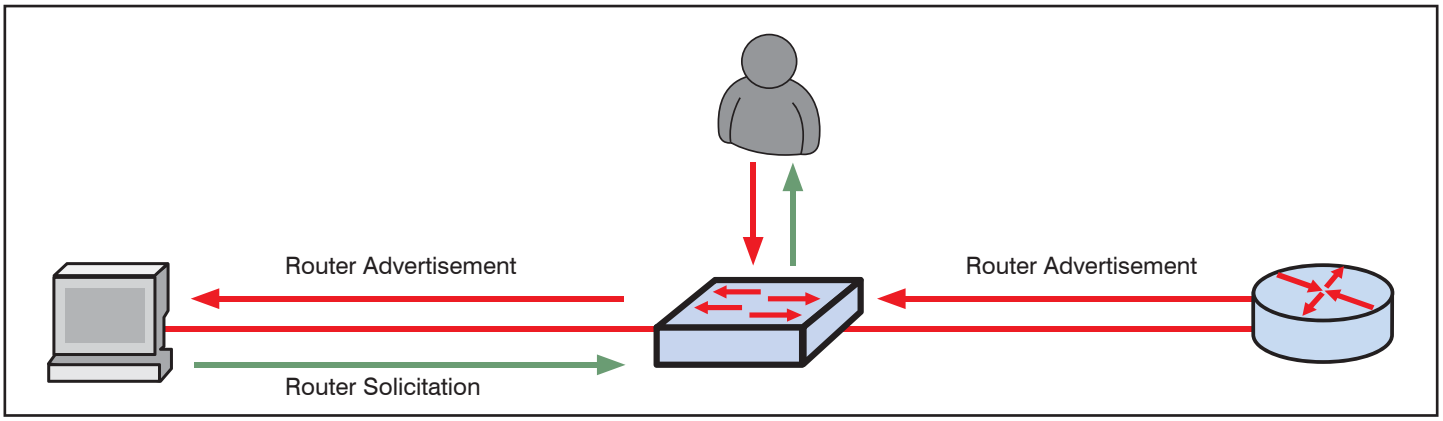


Abbildung 6: Angreifer sendet Router Advertisement

auf 1. Oder in Prosa: wird die IP Adresse zugewiesen, so werden auch alle anderen Optionen per DHCPv6 übermittelt, jedoch ist es möglich, dass die IP Adresse vom Client selbst generiert wird, wohingegen die Zusatzoptionen anderweitig zugewiesen werden.

Für einen Angreifer ist insb. das O Flag interessant. Ob er hingegen das M Flag setzt oder nicht, ist davon abhängig, wie viel Arbeit er sich machen möchte. Gängige Optionen wie ein recursiver DNS-Server können nämlich gleich mit dem Router Advertisement übermittelt werden, ein DHCP Server ist gar nicht erst nötig. (vgl. Abbildung 7)

RA + DNS + Web-Server

Es ist offensichtlich, dass sich damit viel Schindluder treiben lässt:

Ein Angreifer ist so in der Lage den Clients im selben Lokalen Netzwerk zu verkünden, dass er a) der Default Router und b) der DNS-Server ist.

Die Clients wiederum verfügen nun über eine aus ihrer Perspektive vollwertige IPv6 Konfiguration inkl. Default-Router und DNS-Server. Nimmt man nun noch

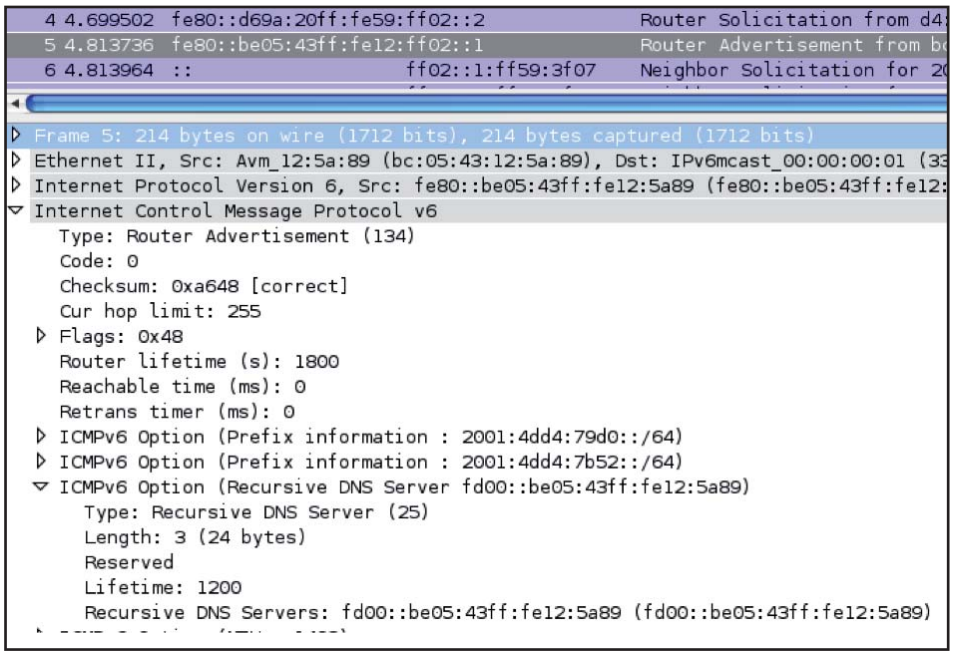


Abbildung 7: Recursiver DNS-Server per Router Advertisement

hinzu, dass IPv6 gegenüber IPv4 zu bevorzugen ist, stehen dem Angreifer eine Reihe von Möglichkeiten zur Verfügung.

NAT64 zu installieren. Den DNS kann man dann auch gleich rekursiv betreiben, was den Aufwand auch an dieser Stelle verringert.

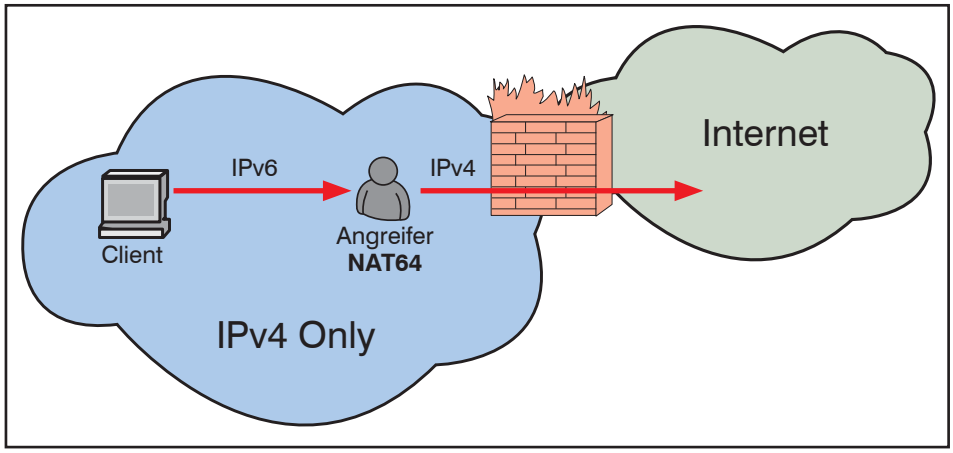


Abbildung 8: Angriff mit NAT64

Die Clients werden auch in diesem Fall IPv6 nutzen und die Pakete an den fingierten Router senden, wann immer dies möglich ist. Der Angreifer übersetzt diese nun per NAT64 von IPv6 nach IPv4 und leitet sie weiter. Auch die Antwort-Pakete wird er bekommen, da der Router schließlich die IPv4 Adresse des Angreifers für den Empfänger hält.

Alles, was er nun noch benötigt, ist ein Protokollanalysator wie bspw. Wireshark, um die Pakete mitzuschneiden. Nachteil an dieser Methode ist, dass er in verschlüsselten Verkehr keinen Einblick bekommt. Da müsste er schon mehr Aufwand betreiben.

Zwischenfazit

Was zeigen diese beiden exemplarischen Angriffsvarianten:

1. **IPv6 Angriffe bedrohen auch scheinbare IPv4-Only Netzwerke**
   Sicherheitsbeauftragte, die bislang glaubten, IPv6 ignorieren zu können, weil im Unternehmen kein IPv6 im Einsatz ist, irren ganz gewaltig!
   Moderne Betriebssysteme haben alle IPv6 per Default aktiviert. Im Falle von Microsoft droht sogar der Verlust des Supports, wenn man den IPv6 Stack deaktiviert. Bei OS X ist es nur über die Kommandozeile möglich.
   Hinzu kommt, dass per Standard (!) IPv6 bevorzugt wird.
   Die Folge ist, dass scheinbar reine IPv4 Netze noch bedrohter sind als IPv6 oder Dual-IP Netze, da der Angreifer als einziger „Router“ tun und lassen kann, was er will und kaum jemand nachschauen wird, ob es Router Advertisements in einem Netzwerk-Segment gibt.

2. **Weder großartiges Know-How noch spezielle Hackertools sind notwendig**
   Ist Ihnen aufgefallen, dass in den beiden Szenarien nicht eine einzige Hacker-Software vorgekommen ist? Alles was man braucht findet sich in vielen Standard-Distributionen von Linux, da es gängige Software ist:

   a. RADV für Router Advertisments
   b. BIND für DNS
   c. Apache für Web
   d. tnat64 oder tayga für NAT64
   e. wireshark als Packetanalyser

Das Zwischenfazit kann also nur sein, dass die Lage ernst ist. Aber ist sie auch hoffnungslos?

Versuch einer Verteidigung

Wo liegt der ursächliche Grund für die Verwundbarkeit? Ganz einfach: man vertraut seinen Nachbarn – und zwar bedingungslos. Weder IPv6 noch das Neighbor Discovery Protokoll (NDP), das für die Adresszuweisung zuständig ist, sehen zunächst einmal eine Authentifizierung von Nachrichten vor. Genau genommen war die ursprüngliche Idee IPsec zur Absicherung der Nachrichten zu nutzen. Jedem, der sich mit IPsec beschäftigt hat, ist sofort klar, dass diese Idee völlig utopisch ist: der Aufwand für die notwendige Schlüsselverwaltung für die Authentifizierung wäre deutlich größer, als würde man die Neighbor Tables gleich per der Hand auf allen Rechnern verteilen.

Secure Neighbor Discovery Protocol (SeND)

Dem soll mit dem Secure Neighbor Discovery Protocol (SeND) abgeholfen werden. Der Standardentwurf (RFC 3972) stammt schon aus dem Jahr 2005. Die Idee hinter SeND ist, NDP Messages mittels Zertifikaten abzusichern und so die Authentizität des Senders sicher zu stellen. Das Verfahren setzt somit eine Zertifikatsstruktur im Unternehmen voraus. Hier liegt aber genau genommen auch schon die Krux im Verfahren: NDP ist schließlich auch am Bootprozess und dem Erwerb der IP Konfiguration beteiligt, erst danach kann eine übergeordnete Zertifikatsinstanz erreicht werden. Das Root-Zertifikat muss somit bereits beim Booten des Systems installiert sein, sprich beim Aufsetzen ausgerollt werden. Da stellt sich aber die Frage, was ist mit all den Systemen, bei denen das nicht oder zumindest nicht ohne Weiteres möglich ist? Beispiele sind Fremdrechner von externen Mitarbeitern und der gesamte Kontext von BYoD. Natürlich gibt es grundsätzlich Lösungen dafür, aber wie komplex das ist und wie wenig es bislang gefordert zu werden scheint, zeigt ein Blick auf die aktuellen Implementierungen von SeND: bei den Herstellern von Routern, Layer 3 Switches und Firewalls sucht man oft vergeblich danach. Wobei es hier durchaus Ausnahmen wie beispielsweise Juniper oder Cisco gibt. Ein Blick in die Manuels des eigenen Herstellers könn-

Name	Betriebssystem	Kommentar
NDprotector	Linux	Aktuelle Version: 0.5 vom 30.06.**2010**
ipv6-send-cga	Linux	Letzte Aktualisierung: Dezember **2009**
Easy-SEND	n/a (Java)	It is aimed to be used for **learning and testing** purposes.
Native SeND kernel API	freeBSD	04.09.**2009**
TrustRouter	**„will be available“**: Windows, Linux, OS X	Aktuell: Version 1.1, 18.04.2012: „TrustRouter does not implement CGAs and **does not secure neighbor advertisements** as of yet. TrustRouter will be available as a one-click solution that can be installed on clients running Linux, Mac OS X, and Windows. In addition to that, TrustRouter will also be integrated in the router advertisement daemon radvd.“
WinSEND	Windows	**Not available** for public yet!

Tabelle 1: Stand der SeND Implementierungen

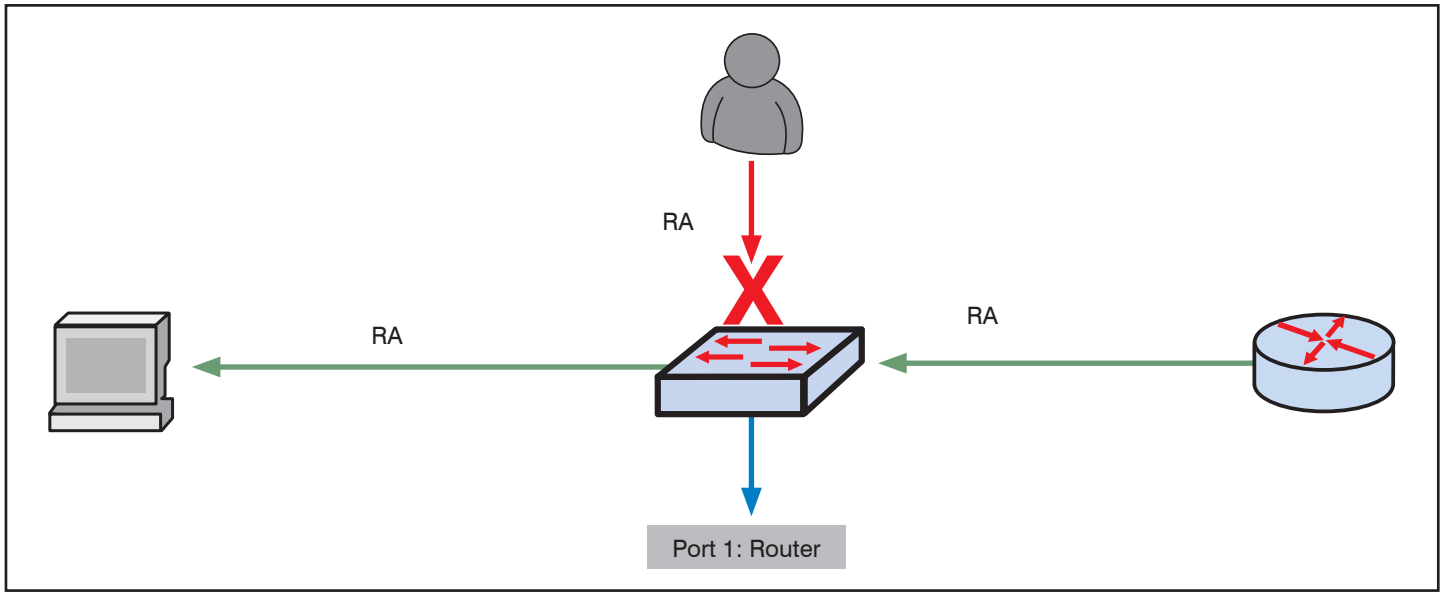


Abbildung 9: RA Guard

te durchaus lohnen. Solange die Funktion aber von den gängigen Betriebssystemen nicht nativ unterstützt wird, nutzt das wenig. Einen herstellereigenen Protokollstack von SeND sucht man jedoch bei Microsoft und Apple vergeblich.

Was es gibt, sind eine Handvoll von Implementierungen (vgl. Tabelle 1). Was dabei auffällt, sind Versionsnummern kleiner 1, letzte Aktualisierungen die älter als 3 Jahre sind und Formulierungen wie „Testing“ bzw. „not availabale“. Böse Zungen sagen schon heute, dass es nie kommen wird.

Was also sind die heute verfügbaren Alternativen?

Route Guard

Im Grunde ist das Problem ja nicht wirklich neu: auch DHCP ist von Hause aus ein ungesicherter Dienst und der ARP wird auch nicht authentifiziert. Die Idee, ähnliche Abwehrmechanismen zu nutzen wie bei diesen Protokollen liegt auf der Hand.

So gibt es zum „Absichern“ der Router Advertisements die Möglichkeit des Router Advertisement Guards.

Abbildung 9 zeigt das prinzipielle Vorgehen:

Der Layer 2 Switch „weiß“, über welche Ports Router, respektive Layer 3 Switches erreichbar sind und an welchen nicht. Alle Router Advertisements, die der Switch auf anderen Ports empfängt, werden verworfen. Etwas Vergleichbares ist der DHCP Guard für IPv4. Die Idee ist charmant: das Verfahren ist einfach und der Konfigurationsaufwand hält sich in Grenzen. Allerdings setzt das Verfahren voraus, dass ein Layer 2 Switch eben nicht nur Layer 2 Informationen verarbeitet, sondern auch begrenzt Layer 3 Funktionen auswerten kann: der Switch muss einen „all node“ Multicast erkennen, zurückhalten und auswerten können, bevor er ihn weiterleitet. Dass es sich dabei nicht um die günstigsten Switches handelt, dürfte klar sein.

Ein weiterer Nachteil ist, dass der RA Guard nur das „Problem“ der fingierten Router Advertisements angeht, was nur einen Teil des NDP ausmacht. So wird das Problem falscher Neighbor Advertisements damit nicht gelöst, denn die darf zunächst einmal jeder senden. Ein Neighor Advertisement kann in diesem Zusammenhang vereinfacht als Nachfolger des ARP angesehen werden. Schließlich kann ein Switch nicht per se wissen, welche IP Adresse an welchem Port angeschlossen ist.

Source Guard

Auch hierfür gibt es Herstellerlösungen wie den „Source Guard“ bei Cisco: hier versucht der Layer 2 Switch mittels Mithören von DCHPv6 Nachrichten und ähnlicher Mechanismen dynamisch eine Tabelle aufzubauen, die Ports und IPv6 Adressen einander zuordnet, um dann – wie beim Route Guard – nur solche Pakete durchzulassen, bei denen Port und Absendeadresse zusammenpassen. Schaut man sich das Verfahren an (bspw. im „IPv6: Sicherheit am LAN-Zugang“ bei ComConsult Study.tv), so erkennt man, dass auch dieses alles andere als trivial ist. Solange es funktioniert, braucht man es „nur“ einschalten. Im Fehlerfall wird das Troubleshooting aber wohl zum Graus, wenn plötzlich einige Verbindungen nicht mehr funktionieren, andere aber sehr wohl.

Der Source Guard verhindert neben gefälschten Neighbor Advertisements jedoch auch DAD Angriffe.

Zwischenfazit: Verteidigung

So recht mag keines der Verfahren wirklich überzeugen. Das wohl größte Manko ist, dass man Source und Route Guard für IPv6 einschalten muss, obwohl man gar kein IPv6 betreibt, will man die eingangs skizzierten Angriffe im LAN verhindern. Hinzu kommt, dass das einzig standardisierte Verfahren SeND wenig Herstellerresonanz hat und die anderen proprietär und teils mit Patenten belegt sind.

Eigentlich müsste man nun empfehlen IPv6 ganz auszuschalten, wenn man es nicht betreibt. Das ist jedoch entweder aufwendig oder man verliert automatisch den Hersteller-Support.

Andererseits kann man aber auch feststellen, dass wirklich Neues nicht dabei ist: statt (nur) DHCP Spoofing gibt es nun zusätzlich noch RA Spoofing und statt des bekannten ARP Poisioning kommt mit IPv6 Neighbor Discovery Spoofing. Wer schon die IPv4 Mechanismen für sich als „nicht relevant“ angesehen hat, kann auch die neuen IPv6 Mechanismen ignorieren. Eine Empfehlung ist das aber ganz sicher nicht!

Gefahr in der DMZ

Sind die Gefahren im LAN durch die Grenzen des Layer 2 Netzes jeweils begrenzt, so gibt es bei der DMZ auch Angriffsvarianten aus der „Ferne“. Als Beispiel soll hier die „NDP Exhaustion“ dienen.

```
#!/opt/local/bin/perl
use FileHandle;
use strict;
my $out_bin = new FileHandle ">./bin_file";


for (my $a=0; $a < 256; $a++) {
        for (my $b=0; $b < 256; $b++) {
                for (my $c=0; $c < 256; $c++) {
                        for (my $d=0; $d < 256; $d++) {
                                print $out_bin chr($a).chr($b).chr($c).
chr($d);
                        };
                };
        };
};

undef $out;
```

Abbildung 10: Perl Skript, das eine Binärdatei mit allen IPv4 Adressen ohne Trennzeichen generiert

Schwachpunkt Speicher

„Was meinst du mit ‚Schwachpunkt Speicher'?", fragte Dr. Simon Hoff, als wir für das ComConsult Sicherheitsforum 2013 die Unterpunkte meines Vortrages zum Thema „Sicherheit und IPv6" vorbereiteten. Mir selbst war dieses Sicherheitsproblem von IPv6 auch lange nicht bewusst. Dabei liegt es auf der Hand und Tools, die es ausnutzen, existieren auch bereits – für Sicherheitstests ... versteht sich. Und das besonders Schöne daran: es gibt sogar Remote-Angriffsvarianten, die diese „Schwäche" ausnutzen können.

Zunächst ein kleines Gedanken-Experiment:

Es gibt 2^{32} IPv4 Adressen, das sind ca. 4,3 * 10^9 Adressen. Jede Adresse ist 4 Byte lang. Wollte man alle IPv4 Adressen aufschreiben und auf Festplatte speichern, so würde man rund 1,7 * 10^{10} Byte, also um die 17 Gigabyte benötigen. Das passt zwar nicht mehr ins RAM, aber immerhin noch locker auf die Festplatte meines Rechners. Wer es ausprobieren will, kann das in Abbildung 10 dargestellte kleine Perl-Skript nutzen (zugegeben: rekursiv wäre eleganter, aber weniger verständlich).

Überträgt man diese Rechnung auf IPv6 erkennt man schnell, dass allein für die möglichen Interfache-Adresse-Anteile eines einzelnen /64 Prefixes der Speicherbedarf in astronomische Dimensionen vorstößt, selbst wenn man das Präfix nicht mit aufschreibt, da es sich ja nicht ändert:

2^{64} Adresse je 8 Byte = 1,48 * 10^{20} Byte = 148 Exabyte

Selbst intelligente Hash- und Kompressionsmechanismen stoßen hier an ihre Grenzen.

Wie man an dem Perl-Skript auch sehen kann, ist es recht einfach, die Adressen zu erzeugen. Jedoch ist es unmöglich, diese auch zu speichern. Damit liegt auf der Hand, dass diese immanente Schwäche von IPv6 für Angriffe interessant ist, die auf einen Memory Overflow von Adresstabellen hinauslaufen.

NDP Exhaustion

Wieder ist es das Neighbor Discovery Protocol, das für den Angriff herhalten muss. Ein Angriff dieser Art läuft dabei ab wie in Abbildung 11 dargestellt.

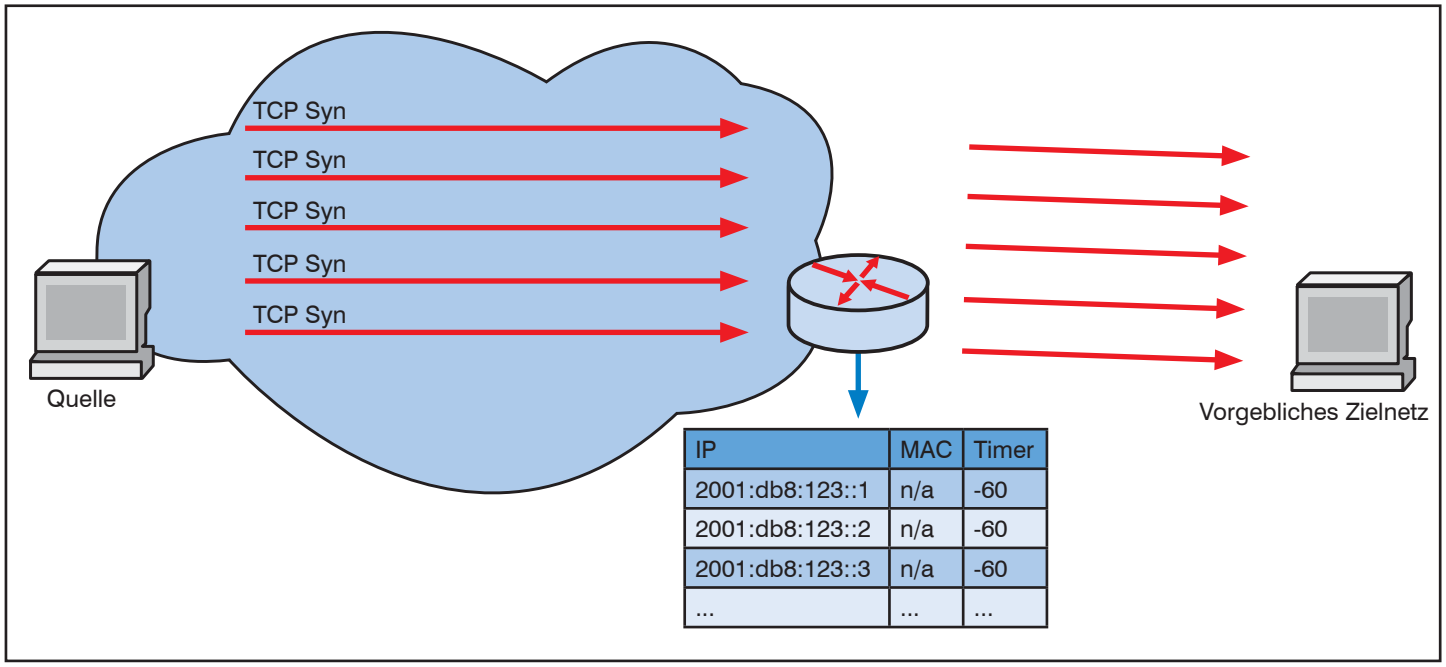


Abbildung 11: NDP Exhaustion

Bekommt ein Router / Layer 3 Switch ein Paket für eine ihm (bislang) unbekannte Interfaceadresse, so versucht er sie mittels Neighbor Solicitation aufzulösen. Um für ein und dieselbe Adresse nicht mehrere Anfragen zu stellen, pflegt er eine Tabelle, in der die offenen Anfragen stehen. Jede Adresse bekommt noch einen Timer, damit der Eintrag nicht ewig offen bleibt. Ist der Timer abgelaufen, sendet der Router ein „Host unreachable“ an den Sender und löscht den Eintrag aus der Tabelle, bzw. hält einen negativen Cache Eintrag für einige Zeit parat für den Fall, dass nochmals eine Anfrage an denselben Host kommt.

Bei IPv4 stellt sich dieses Problem nicht, da typische Subnetzgrößen sich auf 254 Hostadressen beschränken und die Tabellen entsprechend überschaubar sind. Bei IPv6 taucht diese Problematik wegen der gewaltigen Menge von Adressen pro Prefix erstmalig auf.

Die IETF beschreibt dieses Problem selbst in RFC 6583 und gibt auch gleich an, dass zum Zeitpunkt, als der RFC geschrieben wurde (März 2012), 4 parallele nmap Sessions auf einem einzelnen „low-end computer“ ausreichten, um selbst „the largest modern router“ lahm zu legen. Mit anderen Worten David gegen Goliath, bzw. Aldi-PC gegen Internet-Knoten.

Lösungsversuche

SeND ist in diesem Fall keine Lösung, selbst wenn es existieren würde, da ein entfernter Rechner nicht mittels SeND geprüft werden kann.

Möglich ist die Beschränkung des Speicherplatzes. Doch die ist letztlich wenig hilfreich, da sie auch erlaubte Anfragen treffen würde.

Für eine DMZ mit überschaubar vielen Systemen kann die Neighbor Table natürlich auch händisch gepflegt werden. Jedoch sollte man sich des Aufwandes in diesem Fall bewusst sein. Gerade in Zeiten, in denen viel über „wandernde virtuelle Maschinen“ geredet und geschrieben wird, muss man sich klar machen, dass diese Neighbor Tables bei Wanderung auch mit gepflegt werden müssen.

Betreibt man IPv6 bereits im Core, so kann man Access Bereiche oder Rechenzentren gegen interne Angriffe dieser Art nur schwer schützen. Aktuell ist das ohnehin Theorie, hier müssen die Hersteller von Firewalls und Routern sich noch einiges einfallen lassen.

RA Flooding

Aber nicht nur für die DMZ, auch im LAN gibt es Szenarien für einen Memory Overflow:

Betrachten wir dafür das Beispiel „RA Flooding“, das man bspw. mit dem Tool „flood_router6“ von Marc Heuse nachstellen kann: ein beliebiger Client sendet so lange Router Advertisements mit fiktiven Absende-/ Routeradressen, bis die Clients im selben Subnetz die Grätsche machen. (vgl. Abbildung 12)

Das Fatale an diesem Vorgehen ist, dass sich ein Client gegen diese Form der DoS Attacke nicht wehren kann. Zwar kann man die Anzahl der Einträge einschränken und damit einen Memory Overflow effektiv begrenzen, doch wer garantiert, dass erstens der richtige Router eingetragen wird und zweitens dieser Router auch noch die größte Priorität erhält? Richtig: Niemand.

Was die Abwehr eines solchen Angriffs angeht, gilt im Prinzip alles, was bereits vorher zum LAN gesagt wurde. Zwar ist der Angriffsvektor ein anderer, aber Mechanismen wie SeND, RA Guard und/oder Source Guard würden helfen.

Zwischenfazit: Speicher

Was ist also das Fazit aus diesen beiden Beispielen: (verteilte) DoS Attacken konnten noch nie vollständig abgewehrt werden, ohne auch gewünschte Kommunikationsflüsse zu behindern. Mit IPv6 kommt eine Fülle von Möglichkeiten dazu, deren Ursache in der unglaublichen Anzahl von möglichen Adressen liegt. Es bleibt abzuwarten, inwiefern diese Lücken in Zukunft zu einem Problem werden und ob nicht doch sinnvolle Verteidigungsmechanismen entwickelt werden können.

Fazit

IPv6 bietet eine Reihe neuer Angriffsvektoren. Viele der Mechanismen sind jedoch in ähnlicher Form von IPv4 bekannt und können – je nach Hersteller der Netzwerkkomponenten – grundsätzlich in den Griff bekommen werden. Anders sieht es mit den DoS Atacken aus dem Internet aus. Doch auch das ist nicht grundsätzlich neu und abzuwehren waren diese noch nie wirklich.

Was neu ist, ist, dass die IPv6 Angriffe zumindest im LAN auch heute schon erfolgreich sind, selbst wenn ansonsten kein IPv6 betrieben wird. Daraus folgt aber, dass Sicherheitskonzepte bereits heute IPv6 berücksichtigen müssen. Für Sicherheitsbeauftragte ist es darum unumgänglich sich mit dem „neuen“ Protokoll auseinander zu setzen, um das Gefahrenpotential für das eigene Unternehmen einschätzen zu können und ggf. entsprechende Maßnahmen einzuleiten.

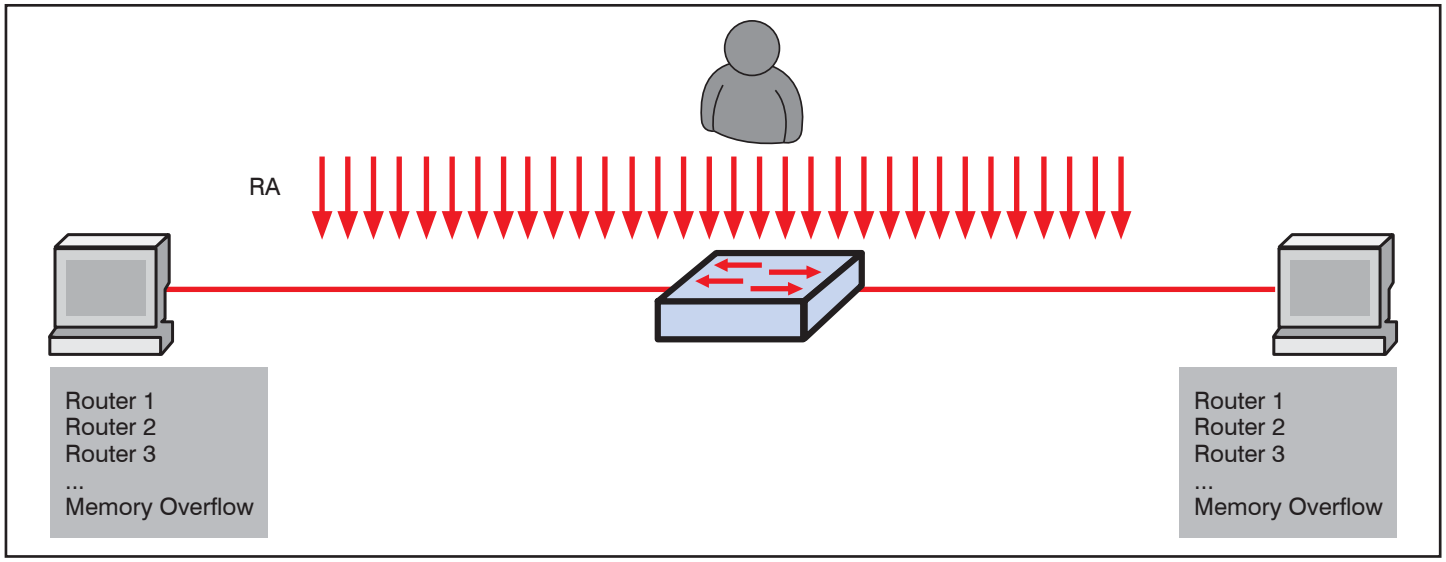


Abbildung 12: RA Flooding

Aktueller Kongress

ComConsult IPv6-Forum 2013

02.12. - 03.12.13 in Euskirchen

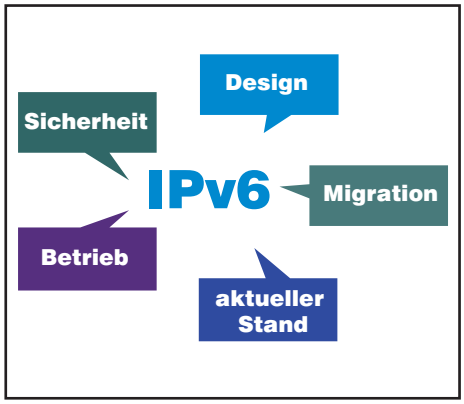
Die ComConsult Akademie veranstaltet vom 2.12. bis 03.12.13 in ihr "ComConsult IPv6-Forum 2013" in Euskirchen.

Viele Unternehmen drücken sich zur Zeit um die Einführung von IPv6. Und schaut man sich die aktuellen Statistiken des DE-CIX an, scheinen diese eine solche Haltung zu unterstützen: stehen dort doch rund 1500 Gigabit IPv4 Traffic 7,4 Gigabit V6 gegenüber, das ist rund 200x mehr. 0,5 Promille kann man doch getrost ignorieren.

Aber so einfach kann man es sich nicht mehr machen.

Beispiel 1: Provider-Migration
Von vielen unbemerkt hat die Migration der Provider zu IPv6 begonnen. Dabei gibt es verschiedene Vorgehensweisen: Während die einen auf den parallelen Betrieb beider Protokollversionen setzten, nutzen andere ISPs Tunnel-/Translationsmechanismen, um ihr Backbone komplett mit IPv6 zu betreiben. Das hat Konsequenzen für die Anwender. Je nach eingesetztem Translationsmechanismus werden nicht mehr alle höheren Protokolle transportiert. Das wiederum hat Auswirkungen auf den IT-Betrieb von Unternehmen, da z.B. bestimmte VPN Techniken nicht mehr funktionieren.

Auch ist es nur eine Frage der Zeit, bis nicht nur Endkundennetze auf IPv6 umgestellt werden, sondern auch Unternehmensanschlüsse.



Die Betreiber der Netzzugänge und VPN-Techniken können sich somit nicht mehr erlauben, IPv6 zu ignorieren. Spätestens wenn die ersten Mitarbeiter sich nicht mehr „einwählen“ können, sollten sie gewappnet sein.

Beispiel 2: Betriebssysteme
Alle gängigen Betriebssysteme kommen mit aktiviertem IPv6 Stack. Anders als bei IPv4 ist kein Mechanismus wie DHCP notwendig, Endgeräte mit gültigen IP Adressen zu versorgen. Autokonfiguration ist immanenter Bestandteil des Protokolls.

Die Folge ist, dass man schon heute IPv6 Traffic im Netz hat: Adressen werden auf Duplikate getestet, die eigene Adresse wird per Multicast bekannt gegeben, Router werden gesucht, etc.

Auch ist es möglich über diese Adressen zu kommunizieren. Häufig lassen die Personal Firewalls auf den Endsystemen jeglichen IPv6 Verkehr zu, wenn sie diesen überhaupt filtern können. Damit wird aber u.U. ein Bypass zu bestehenden Sicherheitsregeln geschaffen.

Hinzu kommt, dass es möglich ist, IPv6 zu nutzen, um Kommunkationsflüsse umzuleiten und auszuspionieren.

Sicherheitsbeauftragte müssen sich somit intensiv mit der Frage auseinandersetzen, wie man die Sicherheitskonzepte an diese Gegebenheiten anpasst.

Das ComConsult IPv6-Forum 2013 greift diese Themen auf. Weitere Themenblöcke sind:

- Aktueller Stand
- Sicherheit
- Design & Migration
- Umgang mit nicht IPv6 kompatibler Hard- und Software

Damit ist das ComConsult IPv6 Forum ein Muss für alle Betreiber und Planer von Netzwerken, Endgeräten, Servern, Speichersystemen und Applikationen im Netzwerk. Versäumen Sie nicht, sich rechtzeitig einen Platz auf dieser herausragenden Veranstaltung zu sichern.

Frühbucherphase nur noch bis zum 15.10.2013

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Ich buche den Kongress
ComConsult IPv6-Forum 2013

☐ vom 02.12. - 03.12.13 in Euskirchen
zum Preis € 1.690,-- netto*
*gültig bis zum 15.10.13

☐ Bitte reservieren Sie mir ein Zimmer

vom _____ bis_____ 13

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

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

ComConsult Veranstaltungskalender

Aktuelle Veranstaltungen

Internetworking: optimales Netzwerk-Design mit Switching und Routing, 14.10. - 18.10.13 in Aachen

Dieses 5-tägige Seminar vermittelt Netzwerkbetreibern und Planern Methoden und Technologien zur erfolgreichen Strukturierung von Enterprise Netzwerken. Dabei wird das komplette Spektrum vom L2/L3 Switching über Redundanz/Routing bis hin zu Themen wie VLAN, WLAN-Integration, Multicast-Routing, VPN, MPLS, abgedeckt.Es werden sowohl die theoretischen Hintergrundkenntnisse als auch die Konsequenzen für den praktischen Betrieb von Netzwerken dargestellt. Fallstudien und Gruppenübungen mit Planungsbeispiel vermitteln Informationen, die in der Praxis sofort umgesetzt werden können.

Preis: € 2.490,-- netto

Rechenzentrumsdesign - Technologien neuester Stand, 14.10. - 16.10.13 in Siegburg

Dieses Seminar analysiert die neuesten Technologie-Trends im Rechenzentrum. Sie lernen von der Verkabelung über die Stromversorgung, die Klimatisierung und den Schrankaufbau, wie ein ausfallsicheres und energieeffizientes Rechenzentrum heute strukturiert wird. Mechanismen für Redundanz im Netzwerk, Lastverteilung und Standort-übergreifende Hochverfügbarkeit werden diskutiert und es wird untersucht wie diese mit dem fortwährenden Trend zur Virtualisierung zusammenspielen. Abschließend werden aktuelle Speichersysteme, deren Anbindung über die am Markt verfügbaren Übertragungsprotokolle sowie Aspekte zur Datensicherung und Disaster Recovery diskutiert.

Preis: € 2.290,-- netto

Aufbau und Management von Internet-DMZ und internen Sicherheitszonen, 14.10. - 16.10.13 in Aachen

Dieses Seminar analysiert die verschiedenen aktuellen technischen Konzepte und Architekturen für den Aufbau und Betrieb von Internet DMZs und internen Sicherheitszonen. Anhand konkreter Projektbeispiele wird die Umsetzung dieser Konzepte illustriert.

Preis: € 1.890,-- netto

Recht und Datenschutz bei Einführung von Voice over IP, 14.10. - 15.10.13 in Siegburg

Durch die Einführung von Voice over IP ergeben sich zahlreiche neue Funktionen einer Telefonanlage und eine wesentlich bessere Zusammenarbeit von TK- mit CRM- und anderen IT-Systemen. Gleichzeitig lassen sich auf diese Weise erhebliche Kostensenkungen durch gemeinsame Nutzung der IT-Infrastruktur mit der TK erzielen. Dabei entstehen jedoch zahlreiche Gefahren in Bezug auf Datenschutz und Datensicherheit der Mitarbeiter. Bei Überwachungsfunktionen sollten Geschäftsführung und Mitarbeiter bzw. Betriebs- oder Personalrat offen Vor- und Nachteile bestimmter Funktionen diskutieren und abstimmen.

Preis: € 1.590,-- netto

WAN: Konzept, Planung und Ausschreibung, 04.11. - 05.11.13 in Bonn

Das Programm dieses Seminars bietet wertvolle Tipps und Empfehlungen sowohl zu technischen als auch zu organisatorischen Aspekten der Konzeption, der Planung, der Ausschreibung und des Betriebs von Wide Area Networks. Die Referenten des Seminars blicken auf langjährige Erfahrungen im WAN-Bereich zurück und vermitteln im Seminar Erkenntnisse aus Dutzenden von Projekten, in denen Wide Area Networks entworfen, ausgeschrieben und optimiert wurden. Der große Erfahrungsschatz von ComConsult bei der Lösung von Problemen und der Lokalisierung von Fehlern in standort-übergreifenden Netzen fließt ebenso in das Seminarprogramm ein wie die Expertise der Referenten bei der Gestaltung sinnvoller Service Level Agreements (SLA) im WAN-Betrieb.

Preis: € 1.590,-- netto

Umfassende Absicherung von Voice over IP und Unified Communications, 04.11. - 05.11.13 in Bonn

Dieses Seminar zeigt Gefährdungspotenziale und erforderliche Sicherheitsmaßnahmen für den Einsatz von Voice over IP und Unified Communications im Rahmen geschäftsentscheidender Kommunikation auf.

Preis: € 1.590,-- netto

Trouble Shooting für Netzwerk-Anwendungen, 05.11. - 08.11.13 in Aachen

Dieses Seminar beschreibt die typischen Störsituationen im Umfeld moderner Anwendungen, gibt Einblick in bisher als Black Box benutzte Mechanismen und Abläufe und trainiert die systematische und methodische Diagnose und Fehlerbeseitigung. Dabei wird die Theorie mit praktischen Übungen und vielen 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 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

Servicialisierung - Leitkonzept für verlässliche Service-Erbringung, 07.11. - 08.11.13 in Bonn

Verlässliche, rationelle und rentable Service-Erbringung bzw. Dienst-Leistung ist die erfolgskritische Kernaufgabe eines jeden Service Providers bzw. Dienst-Leisters, sei es eine unternehmensinterne Organisationseinheit oder eine eigenständige Firma. Es bedarf einer fundierten und durchgängigen Methodik, um diese Aufgabe dauerhaft und ergiebig zu meistern.

Preis: € 1.590,-- netto

Die Führungskraft in IT und Telekommunikation, 07.11. - 08.11.13 in Bonn

Verlässliche, rationelle und rentable Service-Erbringung bzw. Dienst-Leistung ist die erfolgskritische Kernaufgabe eines jeden Service Providers bzw. Dienst-Leisters, sei es eine unternehmensinterne Organisationseinheit oder eine eigenständige Firma. Es bedarf einer fundierten und durchgängigen Methodik, um diese Aufgabe dauerhaft und ergiebig zu meistern.

Preis: € 1.590,-- netto

Zertifizierungen

ComConsult Certified Network Engineer

Lokale Netze
25.11. - 29.11.13 in Aachen
27.01. - 31.01.14 in Aachen
05.05. - 09.05.14 in Aachen

TCP/IP intensiv und kompakt
10.03. - 14.03.14 in Stuttgart
02.06. - 06.06.14 in Düsseldorf

Internetworking
14.10. - 18.10.13 in Aachen
07.04. - 11.04.14 in Aachen
23.06. - 27.06.14 in Aachen

Paketpreis für alle drei Seminare € 6.720,-- netto (Einzelpreise: je € 2.490,-- netto)

ComConsult Certified Trouble Shooter

Trouble Shooting in vernetzten Infrastrukturen
25.02. - 28.02.14 in Aachen
20.05. - 23.05.14 in Aachen

Trouble Shooting für Netzwerk-Anwendungen
05.11. - 08.11.13 in Aachen
18.03. - 21.03.14 in Aachen
24.06. - 27.06.14 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
09.12. - 11.12.13 in Köln
24.02. - 26.02.14 in Düsseldorf
05.05. - 07.05.14 in Bonn

Session Initiation Protocol Basis-Technologie der IP-Telefonie
10.03. - 12.03.14 in Stuttgart

Umfassende Absicherung von Voice over IP und Unified Communications
04.11. - 05.11.13 in Bonn
17.03. - 18.03.14 in Bonn
30.06. - 01.07.14 in Bonn

Optionales Einsteiger-Seminar: IP-Wissen für TK-Mitarbeiter
10.02. - 11.02.14 in Bonn

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: € 4.840,-- netto statt € 5.370,-- 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
http://www.comconsult-research.de

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

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