

Werden SDN und OpenFlow herkömmliche Netzwerke verdrängen?

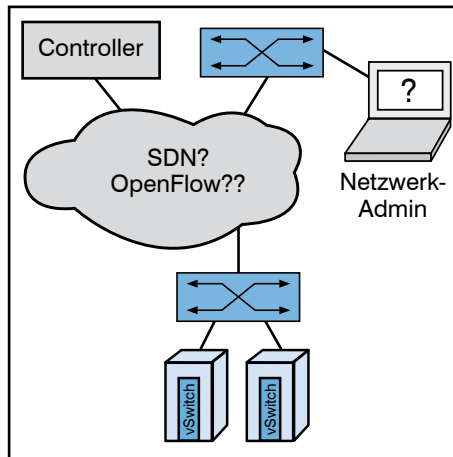
von Dipl.-Inform. Petra Borowka-Gatzweiler

SDN und OpenFlow haben sich zu einem Hype entwickelt. Ist OpenFlow eine Technik, die gekommen ist um zu bleiben? Oder wird sie in den nächsten drei Jahren wieder in der Versenkung der "da war mal was" Technologien verschwinden? Der nachfolgende Beitrag beleuchtet Motivation, Hintergründe, Treiber, Technologie und Erfolgswahrscheinlichkeit von SDN und OpenFlow.

1. Warum SDN und OpenFlow?

1.1 Aktuelle Probleme und Motivation für SDN und OpenFlow

Die Motivation für eine neue Netzwerk-Architektur, wie Software Defined Networking



und OpenFlow sie wollen, liegt in verschiedensten Problembereichen heutiger Netzwerke, die wir nachfolgend näher beleuchtet werden.

Software vs. ASICs: Begeben wir uns einmal zurück in die 70er und 80er Jahre: Damals war ein Router ein Server (typischerweise Unix), der Datenpakete zwischen zwei oder mehreren Netzwerkschnittstellen weiterleitete... Später begann die Entwicklung von ASICs mit ständig wachsender Leistung, Kapazität, Komplexität und hoher Funktions-Robustheit, sowie ständig sinkenden Delay-Werten für die switch-interne Paket-Bearbeitung.

weiter auf Seite 14

Zweitthema

UCC gehört ins Internet!

von Dominik Zöller

Unified Communications (& Collaboration!) gehört ins Internet – diese These dürfte so manchem Sicherheitsbeauftragten den wohlverdienten Schlaf rauben. Doch deswegen ist sie nicht weniger wahr. Nur in und mit dem Internet kann UCC seinen Mehrwert voll entfalten. Um diese These zu überprüfen, müssen wir uns zunächst dem Wesen und dem Versprechen von UCC zuwenden.

Betrachten wir zunächst den prototypischen Entstehungsprozess eines UCC-Projektes. In der Mehrzahl aller Fälle wird über eine Investition in eine neue Telefonie-Infrastruktur nachgedacht. Die Gründe sind vielfältig: Erweiterungsbedarf aufgrund von Neubauten, End-of-Life der bestehenden Lösung, Unsicherheit bezüglich der wirtschaftlichen Zukunft des bisherigen Zulieferers, zunehmende Inhomogenität der Infrastruktur aufgrund von M&A.

Die Liste ließe sich beliebig fortsetzen. Doch das Ziel ist immer dasselbe: wir wollen morgen noch telefonieren und den Betrieb der Infrastruktur bewältigen können. Bei näherer Beschäftigung mit dem Thema wird sofort klar, dass mit Voice-over-IP aus der Telefonie ein Dienst wird, der sich in die bestehende IT-Landschaft integrieren muss. Und dass vielmehr bedacht werden muss, als nur die Telefonie.

weiter auf Seite 30

Geleit

Intel greift an: ist der RISC-Markt am Ende?

ab Seite 2

Standpunkt

Zertifikatsinsuffizienz: Wenn Informationssicherheit zu kompliziert wird

auf Seite 24

Sonderaktion im Oktober

Wireless-Spezial

auf Seite 13

Aktuelles Intensiv-Seminar

Winterschule 2012

ab Seite 26

Zum Geleit

Intel greift an: ist der RISC-Markt am Ende?

Die letzten Quartalszahlen belegen weitere Marktgewinne für x86-Server, der Anteil der verkauften RISC-Systeme geht mehr und mehr zurück. Stehen HP, IBM und Oracle mit dem Rücken an der Wand und ist es nur noch eine Frage der Zeit, bis sie mit ihren RISC-Systemen aufgeben müssen?

Zur Beantwortung dieser Frage dreht sich alles um Verfügbarkeit und weniger um Leistung. 99,999% und bessere Verfügbarkeiten sind nur noch mit Hardware-Automatisierung in der Reaktion auf Störungen zu erreichen. Damit müssen alle Systemkomponenten wie CPU, DIMMs, Bussysteme, Buskarten und die gesamte I/O redundant ausgelegt sein und es muss Mechanismen für die Erkennung von Fehlern und die Ab- und Umschaltung von Komponenten geben. Für menschliche Interaktion bleibt keine Zeit, lediglich Hot-Swap-Eigenschaften für DIMMs und Buskarten zur Vermeidung einer Server-Abschaltung spielen noch eine Rolle in Bezug auf den menschlichen Eingriff.

Mit dem E7 hat Intel im letzten Jahr eine Server-CPU auf den Markt gebracht, die viele RAS-Eigenschaften (RAS= Reliability, Availability, Serviceability) des Itaniums übernommen hat. Intel greift damit direkt die etablierten RISC-Systeme an. Hardware-Redundanz mit Um-/Abschaltung defekter Busse, CPUs und DIMMs sind damit auch in den E7 x86-Servern vorhanden. Im Jahr 2013 wartet die Branche auf den großen Wurf durch Intel. Bisher hat Intel keine Server-CPU im 22nm-Prozess auf den Markt gebracht. Dafür soll 2013 der große Sprung eventuell sogar mit einer neuen Microarchitektur kommen. 3Gate-Transistoren werden allen Voraussicht nach eine neue Messlatte für den Stromverbrauch von Top-Servern setzen. Gleichzeitig wird die Frage diskutiert, was Intel mit den vielen zusätzlichen Transistoren des 22nm-Prozesses machen wird. Als sicher gilt eine Integration des PCI-Express in den CPU-Chip so wie es in der aktuellen 22nm-Desktop-CPU schon erfolgt ist. Aber geht Intel noch weiter? Denkbar wären vier anstelle von zwei Threads pro Core. Das würde die Lücke zu Oracle/Sun etwas schließen und eine bessere Eignung für hochparallele Anwendungen schaffen. Oder ist sogar die Zeit der Ablösung des PCI-Express gekommen? Seit längerer Zeit wird über eine neue I/O-Konstruktion mit einer Integration eines Netzwerk-Adapters und Switches in die CPU spekuliert. Das Problem dieses Konzepts ist, dass es



nicht wirklich rund ist. Es erfordert einen Systemhersteller, der daraus eine sinnvolle Gesamtarchitektur macht. Aber vielleicht müssen wir darauf noch zwei oder drei Server-Generationen warten. Immerhin haben PCI-Express 3.0 und die zukünftige 4.0 Variante eine erhebliche Leistung mit sehr viel Flexibilität. Der Hauptnachteil ist, dass PCI-Express immer eine lokale Bustechnologie ist. Will man den Systembus weiter ausdehnen, um deutlich mehr CPUs oder weitere Peripherie zu integrieren, dann wäre der Wechsel auf eine neue Technologie angesagt.

Also wird 2013 das Ende des RISC-Marktes einläuten? Die Antwort ist aus meiner Sicht ein klares Nein. Für Anwendungen wie Cloud-Computing reichen x86-Server

mit Virtualisierung, Life Migration zwischen Servern und High Availability aus. Hier findet die Redundanz auf Server-Ebene statt und für die meisten Fälle ist das ausreichend. Es gibt also begründeten Anlass, diesen Markt für RISC-Lösungen als verloren anzusehen. Vermutlich wird hier das Thema Performance/Watt, das mit den 22nm-CPU's noch einmal an Marktbedeutung gewinnen wird, einen weiteren Schub in Richtung x86-Server geben.

Für komplexere Datenbank- oder High Performance Computing-Anwendungen reicht das allerdings nicht aus. Intel hat gegenüber der RISC-Konkurrenz einen wesentlichen Nachteil: Hardware, Virtualisierung und Betriebssystem kommen von verschiedenen Herstellern. Eine Machine Check Architecture wie sie der E7 einführt ist ohne eine direkte Unterstützung dieser Eigenschaften im Betriebssystem oder auch der Applikation nutzlos. Abschaltung und Umschaltung von Hardware-Komponenten geht ohne Integration des Betriebssystems und der Anwendungen nicht. Die Serverhardware muss die Alarme und Schaltmechanismen zur Verfügung stellen. Aber die Hardware kann nicht entscheiden, ob und in wie weit ein Komponentenausfall eine Applikation gestört hat und ob ein Zurückgehen auf den letzten Snapshot erforderlich ist. Auch eine Veränderung der Bus- oder I/O-Architektur zu einer weiteren Verbesserung der Systemhardware müsste durch die Betriebssystemhersteller mitgetragen werden. Während der Linux-Markt in sich relativ flexibel ist, muss man bei der

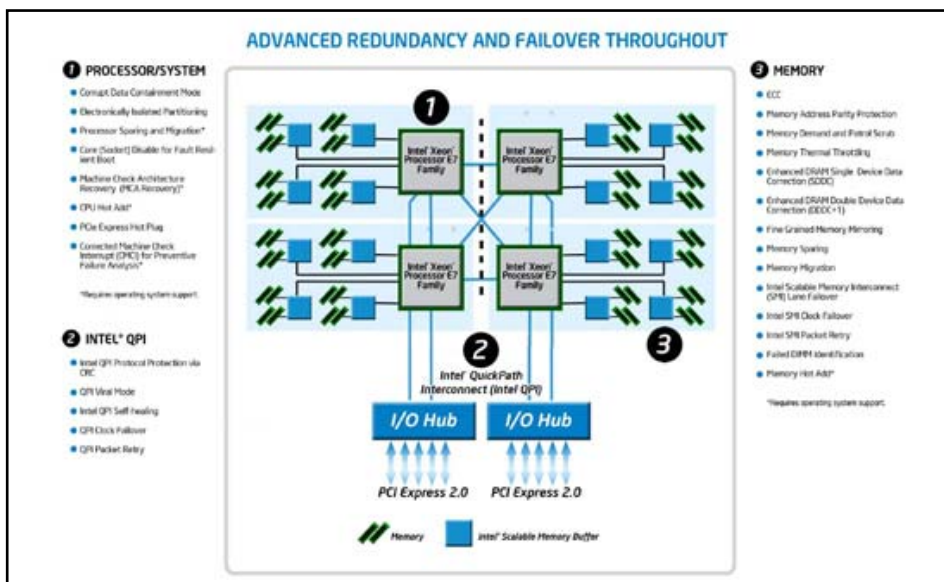


Abbildung 1: Intel E7-RAS-Eigenschaften

Quelle Intel

Intel greift an: ist der RISC-Markt am Ende?

Bereitschaft Microsofts, speziell für diesen Markt Änderungen am Windows-Server durchzuführen, erhebliche Zweifel äußern. Microsoft sieht seinen Zukunftsmarkt eher bei Cloud-Lösungen als im HPC- und Datenbank-Bereich. Für diesen Zielmarkt haben HP, IBM und Oracle alle Karten in der Hand. Die komplette Kontrolle über Hardware, Virtualisierung und Betriebssystem und die spezielle Integration zu einem Gesamtsystem ist der entscheidende Vorteil. Noch eine Stufe weiter wird auch die Applikation in das ganze Konstrukt integriert. Dies ist ein Ansatz, den Oracle mit seiner Datenbank verfolgt. Leider gibt es keine dem Autor bekannten Analysen, in welchem Umfang dadurch die Verfügbarkeit in der täglichen Praxis tatsächlich gesteigert werden kann. Es gibt aber Untersuchungen von Google für seine Rechenzentren, die die Bedeutung von RAS-Eigenschaften speziell für Speicher-DIMMs bestätigt haben.

Es darf an dieser Stelle auch nicht vergessen werden, dass Hardware mehr als eine CPU ist. Bus- und I/O-Systeme spielen eine erhebliche Rolle für sowohl Leistung

als auch Verfügbarkeit. So gut der PCI-Express inzwischen ist, er ist und bleibt ein Bussystem aus der Desktop-Welt und ist von Bussystemen wie IBM sie in seinen Top-Systemen einsetzt weit entfernt. Das Gesamtsystem muss stimmen. Damit stellt sich natürlich auch die Frage, ob vernetzte Lösungen mit Speicherzugriff über FCoE oder NFS jemals die Anforderungen von High-End-Lösungen erfüllen können. Zu viele Komponenten und Verfahren von zu vielen Herstellern kommen zusammen.

Und natürlich sehen auch HP, IBM und Oracle die Wettbewerbssituation und entwickeln ihre Lösungen speziell im Sinne kompletter Schrank-Lösungen weiter. Gerade im High-End-Markt kann man davon ausgehen, das ein Durchschnittsserver einer speziell getunten Plattform unterlegen ist. Wird das ausreichen? Das ist auch die Frage, ob sich UNIX als Betriebssystem weiterhin gegen Linux behaupten kann. Nach wie vor haben UNIX-Systeme wie HP-UX, AIX oder Solaris gegenüber Linux klare Vorteile im Tracen von Fehlersituationen und in der Menge der Feineinstellungen. Linux wird auch nie die Hardware-Integrati-

on dieser UNIX-Systeme erreichen können. Die zentrale Frage ist die des Mengengerüsts. Der RISC-Markt verliert scheinweise gegenüber x86 und je besser die Xeon-Systeme werden, desto mehr Markt geht verloren. Auch hat sich Virtualisierung in der x86-Welt aus den Anfängen einer Bastel-Lösung zu einer ernst zu nehmenden Technologie entwickelt. X86 kann somit fehlende Systemeigenschaften in der Virtualisierung ausgleichen (zum Beispiel Live-Migration), wenn auch nicht auf demselben Niveau wie in der RISC- oder speziell AIX-Welt, da die kleinste Einheit immer der Server bleibt. Da besteht das Risiko, dass RISC eine reine Nischenlösung für große Datenbank- und HPC-Portfolios wird. Wird das ausreichen, um den Entwicklungsaufwand in diese Produkte zu rechtfertigen? Können alle drei Hersteller im Markt bestehen? HP hat schon seine eigene CPU aufgegeben und damit auch einen Teil der Alleinstellungsmerkmale verloren. Über die Zukunft des Itanium-Prozessors wird mit freundlicher Hilfe von IBM und Oracle seit Jahren diskutiert. Wird HP also als erster aus diesem Markt ausscheiden? Ohne Frage sucht HP nach neu-

Kongress

ComConsult Rechenzentrum Infrastruktur-Redesign Forum 2012 05.11. - 08.11.12 in Köln

Unsere Rechenzentren befinden sich in einer der größten Redesign-Phasen der letzten 20 Jahre. Nahezu alle Gestaltungs-Bausteine von den Servern, Speicher-Technologien, Netzwerken bis hin zu den Applikations-Architekturen sind im Umbruch. Gleichzeitig entstehen durch eine Explosion mobiler Teilnehmer auf der einen und durch Cloud-Technologien auf der anderen Seite völlig neue Rahmenbedingungen.

- RZ-Architekturen und Infrastrukturen: wohin geht der Weg?
- Sicherheit in einer immer komplexeren RZ-Umgebung
- Web-Architekturen im RZ
- Netzwerk-Infrastrukturen: die Achillesferse unter Druck
- Mobile Endgeräte und BYOD
- Virtualisierung
- Speicher-Technologien

Wir bieten Ihnen bei der Buchung dieses Kongresses drei Reports zu vergünstigten Teilnehmer-Preisen an:

„RZ Netzwerk-Infrastruktur Redesign“,
„Neue Netzwerk-Architekturen für das Rechenzentrum: TRILL kontra SPB (802.1aq)“ und
„Moderne WAN-Technologien“ oder die komplette
"RZ-Kollektion"

Moderation: Dr. Behrooz Moayeri, Dr. Jürgen Suppan
Kosten: € 2.490,- netto (4 Tage) - € 2.090,- netto (3 Tage) - € 990,- netto (Intensiv-Tag)



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

Intel greift an: ist der RISC-Markt am Ende?

en Nischen. Das Projekt Moonshot zeigt eine Orientierung an hochparallelen Systemen wie sie bei Massendaten-Operationen im Web zum Beispiel zum Einsatz kommen. Moonshot ist klar nicht auf große Datenbank-Anwendungen im traditionellen Sinne ausgelegt. Aber kann HP alleine die dafür notwendige Firmware- und Betriebssystem-Umgebung wirklich stemmen? Moonshot wird abgesehen von speziellen Einzelfällen nur im Markt durchsetzbar sein, wenn die Zuweisung von Servern zu den Mikro-CPU's vollautomatisch erfolgt. Das Mengengerüst von tausenden kleinen Prozessoren kann nicht manuell verarbeitet werden. Das wird eine gewaltige Anstrengung von HP mit erheblichen Investitionen. Ist das HP-Management wirklich gewillt dieses Risiko zu tragen?

Und dann darf die Existenz der Mainframes nicht vergessen werden. IBM baut seine Marktbedeutung in diesem Segment klar aus. Werden HP und Oracle zwischen Mainframe und x86 zerrieben? Oder läuft es im High-End-Bereich auf einen Wettbewerb zwischen den beiden großen Datenbank-Anbietern IBM und Oracle zu?

Abschließend muss natürlich das Thema Cloud erwähnt werden. Auch wenn der Autor zu den Skeptikern im Bereich Cloud gehört, muss natürlich zur Kenntnis genommen werden, dass Cloud-Lösungen zumindest im Provider-Bereich an Bedeutung gewinnen. Ob Self-Provisioning in Private Clouds je eine wirtschaftliche und sinnvolle Lösung darstellen wird, bleibt abzuwarten. Aber die Cloud-Anbieter mit ihren Rechenzentren puschen natürlich eine bestimmte System-Architektur in den Markt. Dabei ist die Rolle des einzelnen Servers eher gering. Die ganze Architektur spielt mit der Verfügbarkeit beliebig vieler Server. Von daher konzentriert sich Redundanz in diesem Umfeld auf den Server als kleinste Einheit. Themen wie Microprocessor Partitioning, die im RISC-Bereich spannend sind, spielen hier einfach keine Rolle. Setzt sich diese Art von Architektur wirklich durch, dann nimmt auch der Bedarf nach leistungsfähigeren CPU-Systemen ab. Die Idee ist mehr die einer parallelen und verteilbaren Last. Dem steht gegenüber, dass nicht jede Art von Anwendung beliebig parallelisiert werden kann. Auch Webanwendungen müssen an irgendeiner Stelle schreibend auf eine Datenbank zugreifen, spätestens hier ist dann Schluss mit Parallelisierung. Ab einem bestimmten Grad an Parallelität wird der Aufwand zur Verwaltung der parallelen Komponenten höher als der Gewinn durch die Parallelisierung, sprich das System skaliert nicht mehr. Auch hier wird sich in den nächsten Jahren die Frage des Mengengerüsts stellen. Wie viele Anwendungen erfordern eher

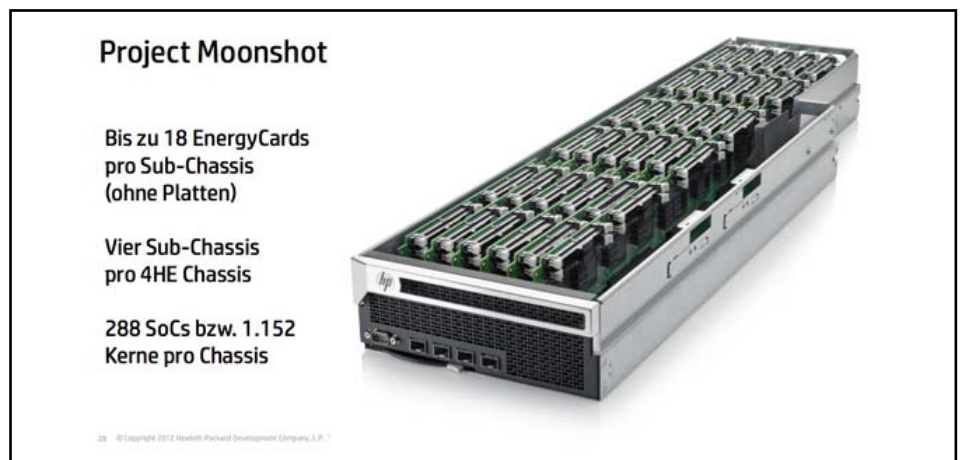


Abbildung 2: Projekt Moonshot, liegt hier die Zukunft für HP?

parallele Architekturen, wie viele sind eher monolithisch in ihrer Architektur. Beobachtet man die Entwicklung bei Intel, dann fällt natürlich auf, dass der Wettbewerb im Bereich der Cores und des Hauptspeichers stagniert. Zwar hat Intel die Zahl der Cores von 8 auf 10 erhöht, aber gemessen an Moores Law ist das Stagnation. Der verfügbare Hauptspeicher hat mit 2 bis 4 TB eine Größenordnung erreicht, die nur von sehr wenigen Kunden überhaupt genutzt wird. Das kann sich zwar nach der letzten Änderung im VMware-Lizenzmodell wieder ändern, aber insgesamt bleibt der Eindruck einer gewissen Stagnation bestehen. Mit

großer Spannung muss deshalb die 22nm-Server-CPU im nächsten Jahr erwartet werden. Was wird Intel mit den vielen zusätzlichen Transistoren machen?

Viele spannende Fragen, die wir in den folgenden Monaten mit Ihnen zusammen analysieren wollen. Diskutieren Sie diese Entwicklung mit uns auf dem ComConsult Rechenzentrum Infrastruktur-Redesign Forum 2012 im November oder auf dem Wissensportal von ComConsult Research.

Ihr
Dr. Jürgen Suppan

Report

RZ Netzwerk-Infrastruktur Redesign Juli 2012 - 520 Seiten



In seinen ersten vier Auflagen war der vorliegende erfolgreiche Report immer ein zuverlässiger Begleiter bei allen anstehenden Entscheidungen. Die 5. Auflage ist mit über 500 Seiten das umfangreichste Werk seiner Art und stellt sowohl bestehende Technologien in ihren aktuellen Ausbaugraden als auch die neuen Ansätze vor und vergleicht sie sofern möglich miteinander. Man findet Diskussionen über FCoE, neue FC-Varianten oder 40/100 GbE genauso wie solche über neue Chip-Konzepte, die unterschiedlichen Alternativen zur Anbindung von VMs bis hin zur Realzeitfähigkeit, Einbindung privater, öffentlicher oder hybrider Cloud-Konzepte oder die Grundsatzdiskussion alte Scale-Up Data Center Fabrics vs. OpenFlow-basierte Scale-Out-Konzepte.

Autor: Dr. Franz-Joachim Kauffels
Preis: € 398,- netto



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

Aktueller Kongress

ComConsult Rechenzentrum Infrastruktur-Redesign Forum 2012

05.11. - 08.11.12 in Köln

Die ComConsult Akademie veranstaltet vom 05.11. - 08.11.12 ihr "ComConsult Rechenzentrum Infrastruktur-Redesign Forum 2012" in Köln.

2012 ist ein anstrengendes Jahr für Planer und Betreiber von Corporate IT-Infrastrukturen. Auch wenn verschiedene technische Einzelfragen der Vergangenheit wie z.B. die Konvergenz von „normalem“ und Speicherverkehr weitest gehend geklärt werden konnten und angesichts der Entwicklung von 10, 40 und 100 GbE auch für einen größeren Zeitraum im Netz hinreichend Leistung zu noch nie dagewesenen günstigen Preisen zur Verfügung stehen wird, verbleiben schwer wiegende

Fragestellungen vor allem hinsichtlich der Zusammenfügung von Einzeltechnologien zu einer modernen, flexiblen, skalierbaren, beherrschbaren und wirtschaftlichen IT-Infrastruktur, deren Herz das RZ ist.

Themenschwerpunkte des Forums

- RZ-Architekturen und Infrastrukturen: wohin geht der Weg?
- Sicherheit in einer immer komplexeren RZ-Umgebung
- Web-Architekturen im RZ
- Netzwerk-Infrastrukturen: die Achillesferse unter Druck
- Mobile Endgeräte und BYOD
- Virtualisierung
- Speicher-Technologien

Das ComConsult Rechenzentrum Infrastruktur-Redesign Forum 2012 ist die zentrale Veranstaltung des Jahres, auf dem die Problemkreise nicht nur singulär, sondern vor allem übergreifend von Spezialisten, Beratern und Herstellern diskutiert werden. Neben dem Hauptforum gibt es vertiefende Workshops und eine Ausstellung, die thematisch tief in das Forum eingebunden ist. Flankiert von Reports, Videos und weiteren Sonderpublikationen entsteht ein einzigartiges Informationsspektrum. Sichern Sie sich frühzeitig einen Platz in dieser meist schnell ausgebuchten Veranstaltung!

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

ComConsult Rechenzentrum Infrastruktur-Redesign Forum 2012

Ich buche den Kongress

**ComConsult Rechenzentrum
Infrastruktur-Redesign Forum 2012**

mit Intensiv-Tag

vom 05.11. - 08.11.12 in Köln
zum Preis von € 2.490,- netto

ohne Intensiv-Tag

vom 05.11. - 07.11.12 in Köln
zum Preis von € 2.090,- netto

nur Intensiv-Tag

am 08.11.12 in Köln
zum Preis von € 990,- netto

Bitte reservieren Sie mir ein Zimmer

vom _____ bis _____ 12

im Radisson Blu Hotel Köln

inkl. Report "RZ Netzwerk-Infrastruktur Redesign" - € 338,- netto

inkl. Report "TRILL kontra SPB (802.1aq)" - € 310,- netto

inkl. Report "Moderne WAN-Technologien" - € 338,- netto

inkl. "RZ-Kollektion" - € 870,- netto

Vorname _____

Nachname _____

Firma _____

Telefon/Fax _____

Straße _____

PLZ, Ort _____

eMail _____

Unterschrift _____



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

Programmübersicht - ComConsult Rechenzentrum Infrastruktur-Redesign Forum 2012

Montag, den 05.11.2012**9:30 bis 10:45 Uhr****Neue IT-Technologien und die Auswirkungen auf RZ-Infrastrukturen**

- Cloud-Technologien im Unternehmen: was bedeutet das?
- Neue Endgeräte-Technologien und Auswirkungen auf Architekturen
- Infrastrukturen für mobile Endgeräte • Gibt es den Server der Zukunft?
- Wie wichtig wird OpenStack? • Virtualisierung: am Anfang oder am Ende?
Dr. Jürgen Suppan, ComConsult Research Ltd.

10:45 - 11:15 Uhr Kaffeepause**11:15 bis 12:30 Uhr****Analyse: Data-Center-Architekturen:**

- Architekturmodell für die Unterstützung kooperierender Web-Anwendungen • Aktuelle Entwicklungen der Schaltkreistechnologie und Auswirkungen auf zukunftssichere Investitionen
- Traditionelle Netzwerke am Ende? SDN und Open Flow ändern unser Verständnis von Netzwerken
- Leistungsfähige Alternativen der VM-Anbindung
Dr. Franz-Joachim Kauffels, freier Unternehmensberater

12:30 bis 14:00 Uhr Mittagspause**14:00 bis 14:45 Uhr****Analyse: Server-based Computing, Virtualisierung und Cloud Computing**

- Kapselung von Daten und Anwendungen im RZ mit Server-based Computing und Desktop Virtualisierung
- Gefährdungen durch Zentralisierung von Clients
- Malware-Schutz: Umdenken ist erforderlich
- Data Center Firewalls: Neue Konzepte und deren Tücken
- Kerndisziplin: Data Loss Prevention (DLP)
- Sicherheitsarchitekturen für Private Clouds
- Rolle von Public Clouds für die Enterprise IT
- Anforderungen an sichere Public Clouds
Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

14:45 bis 15:30 Uhr**Mandantenfähigkeit und Zonenkonzepte im RZ**

- Mandantenfähige RZ-Netze: Techniken und deren Praxistauglichkeit

- Brauchen wir angesichts Server-based Computing und Cloud Computing noch Sicherheitsmaßnahmen im Netz?
- Zonen- und Firewall-Architekturen im RZ
- Zwiebelschalen-Modelle im Widerspruch zu Mehrmandantennetzen
Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

15:30 bis 16:00 Uhr Kaffeepause**16:00 bis 16:45 Uhr****Sicherer Betrieb von Zonenarchitekturen**

- Terminal Server als Jump Host: Möglichkeiten und Grenzen
- Virtualisierungstechniken zur sicheren Entkopplung administrativer Zugriffe
- Zonen für die Administration und Überwachung: Firewall-Infation droht
- SIEM: Sondermülldeponie oder sinnvolles Instrument des Security Incident Management? • Kurzschluss in SAN und NAS vermeiden
Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

16:45 bis 17:30 Uhr**Web-Anwendungen im Rechenzentrum**

- Webanwendungen: mehr als nur Webseiten
- Architektur und Skalierbarkeit
- Integration von Kunden, Partnern und Mitarbeitern
- Windows, Mac, iOS, Android: eine App für alle?
- Sicherheitsrelevante Aspekte • Was bringt die Zukunft?
Markus Schaub, ComConsult Research Ltd.

17:30 bis 18:00 Uhr**Service-basierte Netzwerke: das Ende des normalen Netzwerk-Designs**

- Mandantenfähigkeit und Trennung von Datenströmen über L2/L3-Grenzen gefordert
- MPLS hat im Enterprise ausgedient
- L2/L3-Abgrenzungen sind Diskussionen von Gestern
- VXLAN ohne die Komplexität von PIM /PIM-SM/PIM-SSM etc.
- L2/L3-übergreifende Multicast-Dienste sind erforderlich
- Vision: Anwendungs-orientierte Netzwerk-Services
Heinz Behrens, Avaya GmbH & Co KG

Ab 18:00 Uhr Get Together**Dienstag, den 06.11.2012****9:00 bis 10:00 Uhr****Performance Optimized Data Center POD**

- Bedarf für modulare Data Center Lösungen
- Was ist ein POD (Performance Optimized Data Center, Point of Delivery, Point of Deployment)?
- POD Architektur-Elemente (Container, Server-Block, Storage-Block, Netzwerk-Block) • Referenz-Architekturen
- POD-Beispiele (Cisco VMDC, Dell vStart, HP EcoPOD, IBM PMDC, SGI CloudRack)
Dipl.-Inform. Petra Borowka-Gatzweiler, UBN Unternehmensberatung

10:00 bis 11:00 Uhr**Auf dem Weg zum RZ und den Infrastrukturen der Zukunft**

- Migration DC zum Fabric enabled DC
- POD Design und Cloud Ready
- Überblick SW Router CSR1000v: liegt hier die Zukunft für virtuelle Umgebungen? • Erster Blick auf „onePK“
- Ciscos Sicht zu SDN/OF
Gerd Pflueger, Matthias Wessendorf, Cisco Systems GmbH

11:00 bis 11:30 Uhr Kaffeepause**11:30 bis 12:15 Uhr****Optimierte Switches für den RZ-Bedarf**

- Erfüllen Standard-Chip-Architekturen den Bedarf?
- Vorteile einer offenen Linux-Lösung
- Software Defined Networking
- Low Latency
- Wieviel Stromverbrauch darf es ein?
- Wie wichtig wird VxLAN?
Manfred Felsberg, Frank Laforsch, ARISTA Networks, Inc.

12:15 bis 12:45 Uhr**Technologie-Statements****12:45 bis 14:00 Uhr Mittagspause****14:00 bis 14:45 Uhr****Positionierung der TCP/IP-Intelligenz**

- Welche Alternativen gibt es? • Ist Offload wirklich die beste Lösung?
- Vor- und Nachteile, Empfehlung
Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

14:45 bis 15:30 Uhr**RZ-Netze: Evolution oder Revolution?**

- Mängelbereiche bisheriger Konstruktionen
- Entwicklung von Switching-Substraten mit speicherbasierenden ASICs
- SDN: neuer Provider-Hype oder nutzbar für alle?
- Das RZ im Schrank • Migrationsempfehlungen
Dr. Franz-Joachim Kauffels, freier Unternehmensberater

15:30 bis 16:00 Uhr Kaffeepause**16:00 bis 16:45 Uhr****BYOD, DLP und mobile Virtualisierungs-Technologien**

- Welche Anforderungen stellt BYOD an die Datenhaltung?
- Sind diese Anforderungen auch für Company-owned-Devices relevant?
- Welche Technologien eignen sich zur Trennung privater und geschäftlicher Daten?
- Was ist mobile DLP und eignet es sich zur Umsetzung von BYOD/COD?
- Sandboxing, Server-based Computing und Virtualisierung - ein Überblick
Dominik Zöller, ComConsult Beratung und Planung GmbH

16:45 bis 17:30 Uhr**Smartphones, Tablets und der Gast-Zugang**

- Einsatzszenarien für mobile Endgeräte im Unternehmen
- Mobile und nomadische Nutzung von Smartphones & Tablets
- Netzanbindung via 3G/4G und WLAN
- BYOD, Zonenkonzepte und Gastzugänge
Dominik Zöller, ComConsult Beratung und Planung GmbH

Programmübersicht - ComConsult Rechenzentrum Infrastruktur-Redesign Forum 2012

Mittwoch, den 07.11.2012

9:00 bis 09:45 Uhr

Aktuelle Trends und Entwicklungen am Hypervisor-Markt

- Welche entscheidenden Neuerungen brachte die VMworld 2012 für den VMware ESX?
- Was wurde auf der Synergy 2012 in puncto Citrix XenServer vorgestellt?
- Wie hat Microsoft im Windows Server 2012 seine Virtualisierungsplattform Hyper-V verbessert?
- Welche Relevanz haben diese Entwicklungen auf aktuelle Data Center Designs?
- Wie haben sich die Hersteller damit strategisch positioniert?

Dipl.-Inform. Matthias Egerland, ComConsult Beratung und Planung GmbH

9:45 bis 10:30 Uhr

Automatic Storage Tiering: Wunderwaffe oder technischer Overkill?

- Herausforderung exponentiellen Speicherwachstums
- Hierarchisches Speicher-Management (HSM), Information Lifecycle Management (ILM) und ihre Grenzen
- Voraussetzung: Definition unterschiedlicher Speicherklassen (Storage Tiers)
- Wie funktioniert Automatic Storage Tiering?
- Welche Unterschiede gibt es bei den marktführenden Storage-Systemen?
- An welche Grenzen stößt dieser technische Ansatz?
- Wie positionieren sich die Hersteller?
- Welche Strategie sollte im modernen Data Center verfolgt werden?

Dipl.-Inform. Matthias Egerland, ComConsult Beratung und Planung GmbH

10:30 bis 11:00 Uhr Kaffeepause

11:00 bis 11:45 Uhr

Zukunftsorientierte Speicherlösungen und -methoden

- Herausforderungen an Speicherlösungen
- Senkung der Investitionskosten
- Eindämmung der Betriebskosten
- Enterprise Funktionalitäten zu einem auch für kleine Unternehmen bezahlbaren Preis

Dr. Georgios Rimikis, Hitachi Data Systems GmbH

11:45 bis 12:30 Uhr

Service-orientierte Infrastruktur: Konvergierte HP-Lösungen für das RZ

Florian Bettges, Hewlett-Packard GmbH

12:30 bis 14:00 Uhr Mittagspause

14:00 bis 14:45 Uhr

Aktuelles zu IBM XIV Storage

- Neue Ankündigungen
- Ausblick
- Kundenbeispiel
- Live-Demo

Dirk Vogelsang, IBM Deutschland GmbH

14:45 bis 15:30 Uhr

Projektbericht Datensicherung

- Herausforderung: Einheitliche Backup-Landschaft für eine komplexe Systemumgebung
- Backup2Disk- versus Backup2Tape-Lösungen
- Chancen durch den Einsatz moderner VTLs
- Backup- & Redundanzkonzepte für Datenbanken

Dipl.-Ing. Peter Koch, inforsacom Informationssysteme GmbH

15:30 bis 16:15 Uhr

Virtualisierte Serveranbindung: Kampf der Konzepte

- Software-basierte vSwitches
- Direct I/O
- Probleme bei der vMotion+FT
- Hybrides Treiber-Design, SR-IOV
- Unterstützung der offenen Standards
- VMware vCloud
- VXLAN
- STT
- NVGRE

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

**16:15 Uhr Ende der 3-tägigen Veranstaltung
Kaffeepause für Teilnehmer der 4-tägigen Veranstaltung**

Donnerstag, den 08.11.2012 - Cloud Computing und die Auswirkungen auf das Rechenzentrum der Zukunft

9:00 bis 09:45 Uhr

Analyse: Was leistet Cloud-Computing: was leistet es und wo sind die Grenzen?

- Ziele, Vorteile und Versprechen
- Cloud Service- und Liefermodelle im Vergleich
- Analyse der verschiedenen Lager: wer will was erreichen?
- Vor- und Nachteile von Public Cloud Diensten
- Private Cloud: die Lösung?
- Bewertung: werden die Ziele eingehalten?
- Empfehlungen für eine Cloud-Strategie

Dr. Jürgen Suppan, ComConsult Research Ltd.

9:45 bis 10:30 Uhr

Wie ist eine Private Cloud aufzubauen?

- Betriebliche und technische Anforderungen
- Auswahl des Hypervisors
- Dimensionierung der Virtualisierungsumgebung
- Cluster-Design
- DMZ-Design
- Storage-Design
- Migration und Provisioning
- Monitoring und Reporting

Dipl.-Inform. Matthias Egerland, ComConsult Beratung und Planung GmbH

10:30 bis 10:50 Uhr Kaffeepause

10:50 bis 12:05 Uhr

Virtualisiertes RZ als Basis für die Private Cloud

- Was bedeuten HA, FT, und Disaster Recovery Mechanismen für unsere Ressourcen?
- Globale und regionale RZ-Virtualisierung
- Anforderungen an Storage und Netz

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

12:05 bis 13:00 Uhr

Public-Cloud-Marktübersicht

- Dienste aus der Public Cloud: Übersicht
- Public Cloud Produkte und Anbieter
 - IaaS
 - PaaS
 - SaaS
 - UCaaS

Dominik Zöller, ComConsult Beratung und Planung GmbH

13:00 bis 14:00 Uhr Mittagspause

14:00 bis 14:45 Uhr

Worauf ist bei der Ausschreibung von Cloud-Diensten zu achten?

- Daten- und Rechtssicherheit
- Integration in das Service-Portfolio
- Service-Vereinbarungen
- Anbietersicherheit und Rückmigration

Claus Elfering, ComConsult Beratung und Planung GmbH

14:45 bis 15:45 Uhr

Rechtliche Aspekte bei Public Clouds

- Was ist erlaubt, was nicht?
- Helfen individuelle Verträge?
- Wie wichtig ist die Unternehmens-seitige Verschlüsselung?

Ulrich Emmert, esb Rechtsanwälte

15:45 Uhr Ende der 4-tägigen Veranstaltung

Aktueller Kongress

ComConsult TK-, UC- und Videokonferenzforum 2012

19.11. - 22.11.12 in Düsseldorf

Die ComConsult Akademie veranstaltet vom 19.11. - 22.11.12 ihr "ComConsult TK-, UC- und Videokonferenzforum 2012" in Düsseldorf.

Dieses hochaktuelle Forum analysiert aktuelle Trends, neue Technologien und Produkt-/Hersteller-Strategien im Bereich TK, UC und Videokonferenztechnik. Die Kernthemen sind: wie viel UC braucht TK; zukunftsweisende Client-Strategien; User Centric Communications; der Kunde, das unbekannte UC-Wesen; Videokonferenztechnik der Zukunft.

In diesem Jahr stehen fünf Themen im Mittelpunkt des Forums:

Wie viel UC braucht TK?

Telefonieren muss Jeder, aber wie viel Unified Communication wird wirklich benötigt und welche Alternativen der Umsetzung gibt es? Wir analysieren:

- Wo stehen integrierte Lösungen, die TK und UC aus einem Guss liefern?
- Wie sinnvoll sind Ergänzungs-Lösungen, die mehr TK-orientierte Installationen durch eine externe UC-Lösung ergänzen?
- Was bieten die Hersteller?
- Welche Lösungen werden bevorzugt umgesetzt?
- Welche Anforderungen stellt der Mittelstand an die Kommunikationsinfrastruktur?

Zukunftsweisende Client-Strategien – Welche Bedeutung haben mobile Endgeräte in Zukunft und wie werden sie integriert? Für viele Benutzer ist der zeitgleiche Umgang mit mehreren Endgeräten inzwischen die Normalität. Der traditionelle Ansatz mit Desktop PC und Telefon wird der aktuellen Lage nicht mehr gerecht. Nach Apple und Google wird nun auch Microsoft den Markt der mobilen Endgeräte attackieren – und bietet erstmals eine einheitliche Plattform für alle Endgeräte. Parallel bieten die mobilen Endgeräte ein völlig neues Bedienverständnis, das speziell UC unter erheblichen Druck setzt. Wir analysieren:

- Welche Rolle spielen mobile Endgeräte in Zukunft?
- Lassen mobile Endgeräte die Bedienbarrieren zwischen verschiedenen Apps verschwinden? Brauchen wir dann UC überhaupt noch?
- Wie sieht UC im Umfeld mobiler Endge-

räte aus? Wie spielen die verschiedenen Geräte zusammen?

- Wohin entwickelt sich die Client-Technik auf mobilen Geräten?
- Was passiert mit privaten iPads und iPhones, die dienstlich genutzt werden sollen?

User Centric Communications UCC

Nach der Infrastrukturkonvergenz rückt der Anwender von UC-Lösungen wieder in den Mittelpunkt. UC kann nur funktionieren, wenn der Client alle Funktionen intuitiv nutzbar umsetzt. Hieran scheitern bisher fast alle Lösungen. Anders im Bereich der mobilen Kommunikation: Apple hat mit dem iPhone den Markt verändert und den Benutzer in die Mitte der Architektur gestellt. Traditionelle Anbieter wie Nokia sind mit ihren Bedienkonzepten in der Versenkung verschwunden. iOS und Android prägen heute das Verständnis der Benutzer in der Handhabung auch komplexer Kommunikations-Funktionen. Unter den inzwischen weit verbreiteten Apps auf den mobilen Geräten befinden sich viele Apps, die Funktionalität aus dem Bereich UC anbieten. An diesen Lösungen aus dem Konsumenten-Markt muss sich UC messen lassen. UC wird nur überleben, wenn Benutzer-zentrische Lösungen von den Herstellern auch tatsächlich umgesetzt werden. Wir analysieren:

- Von UC zu UCC: was bedeutet das?
- Die Rolle von Social Media im Unternehmensumfeld
- Neue Messaging Dienste und ihre Nutzung
- UCC aus der Cloud: eine wirkliche Alternative?
- Wie sollte der ideale Client aussehen?
- Sollte es einen einheitlichen Client über alle Plattformen geben?

Der Kunde, das unbekannte UC-Wesen?

Unternehmen verdienen ihr Geld mit Kunden. Aber genau an dieser Stelle hören UC-Lösungen typischerweise auf. Dabei liegt genau hier der größte potenzielle Mehrwert. Das Contact Center ist dabei einer der Angelpunkte der Unternehmenskommunikation. Hier entfalten moderne Kommunikationsplattformen und Social Media ihr volles Potenzial. Wir analysieren:

- Welche Alternativen der Einbindung externer Kommunikationspartner gibt es?
- Wann kommt die wirklich offene UC-Lö-

sung?

- Ist Skype die Lösung und welche Rolle spielt die Skype-Integration in Microsoft Lync?
- Das Contact Center – Zwischen Vermittlungsplatz 2.0 und Social Media Hub.

Videokonferenz in der Sackgasse?

Die Anbieter von Videokonferenz-Lösungen treten seit Jahren auf der Stelle. Genau die im Marketing immer wieder beschworene Integration aller Mitarbeiter und Kunden in eine Gesamtlösung, also der Übergang von einer teuren Lösung für wenige Teilnehmer hin zu einer bezahlbaren Lösung für viele erfolgt im Rahmen von UC bisher nicht. Dabei fordert die Explosion mobiler Endgeräte mit Diensten wie Fuze und WebEX aber genau diesen Übergang. Wir analysieren:

- Wie sieht die Video-Konferenz-Lösung der Zukunft aus?
- Wird die Webkonferenz die Videokonferenz verdrängen?
- Welche neuen Standards sind wann verfügbar und verändern sie die Welt?

In einem weiteren Schwerpunkt widmen wir uns dem aktuellen Portfolio der Hersteller. Mit Cisco Jabber erzielt erstmals ein Konkurrent eine vergleichbar tiefe Integration in die Client-Welt wie Microsoft Lync. Aber auch die Konkurrenz schläft nicht und feilt eifrig an intuitiven Bedienkonzepten. Microsoft legt mit Lync 2013 nach. Wie die Hersteller die Anforderungen der Kunden lösen wollen und wie sie sich strategisch positionieren erfahren Sie im Rahmen des Intensivtages:

- Wie setzt Microsoft den Markt mit dem neuen Release unter Druck?
- Welche Konzepte verfolgen die anderen Hersteller?
- Wie setzen die Hersteller die Kundenanforderungen um?
- Was kommt in den nächsten Jahren?

Das ComConsult TK-, UC- und Videokonferenzforum 2012 bietet Top-aktuelle Information und Analysen mit ausgewählten Experten. Eine ausgewogene Mischung aus Analysen, Hintergrundwissen und Projekterfahrungen in Kombination mit Produktbewertungen und Diskussionen liefert das ideale Umfeld für alle Planer, Betreiber und Verantwortliche solcher Lösungen. Zögern Sie nicht, sich rechtzeitig einen Platz in dieser Veranstaltung zu sichern.

Programmübersicht - ComConsult TK-, UC- und Videokonferenzforum 2012

Montag, den 19.11.2012

9:30 bis 10:30 Uhr

Keynote

- UC 2015 - wo steht UC?
- Auswirkungen mobiler Endgeräte auf die UC-Architektur
- Alle Funktionen auf allen Geräten?
- Welche Auswirkungen werden Windows 8 und iOS 6 haben?
- Ist All-in-One noch eine attraktive Lösung?
- Wie viel Social Media brauchen UC und CC?
- Braucht UC Video Conferencing oder Web Conferencing oder beides?
- Wie viel UCC braucht der Mittelstand?
- ... und was ist mit DECT?
Dipl.-Inform. Petra Borowka-Gatzweiler, UBN Unternehmensberatung

- Bandbreiten im Internet
- Server, Mediagateways
- Neue Codecs
- Konsequenzen und Fazit

Markus Schaub, ComConsult Research

13:00 bis 14:30 Uhr Mittagspause

14:30 bis 15:15 Uhr

Stand der Videokonferenz-Technik

- Integration von Web- und Videoconferencing
- Standardisierungsbemühungen - SVC, H.265 und Co.
- Hardware- vs. Software-MCU

N.N.

10:30 bis 11:00 Uhr

Von UCC zu User-centric Communications

- Von der Infrastruktur-Konvergenz zum intuitiven Bedienkonzept
- Prozessoptimierung durch UCC
- Soziale Medien im Unternehmen
- Konsumerisierung des Clients und der Kommunikation
Dominik Zöller, ComConsult Beratung und Planung GmbH

15:15 bis 15:45 Uhr

UCC, Video und Mobility

- Sinnvolle Anwendungsszenarien von Mobile UCC
- Smartphones & Tablets als Videoendpunkt?
- Bedienkonzepte mobiler UCC-Clients

Mario Seefried, Vidyo GmbH

11:00 bis 11:15 Uhr

Hersteller-Vortrag

11:15 - 11:45 Uhr Kaffeepause

11:45 bis 12:30 Uhr

UCaaS – Kommunikation aus der Cloud

- UCaaS-Architekturen
- Erfahrungen aus der Praxis
- Cloud trifft Realität – Typische Probleme bei der Umsetzung von UCaaS
- Cloud Readiness Assessments – was ist zu beachten?
Tolga Erdogan, Dimension Data Germany AG & Co KG

15:45 bis 16:15 Uhr Kaffeepause

16:15 bis 17:00 Uhr

Clientstrategien

- Workstation, Notebook, Tablet und Smart-phone
- Zukunftsweisende Client-Strategien
- Welche Funktionalität braucht/soll der UCC-Client haben?
Dominik Zöller, ComConsult Beratung und Planung GmbH

17:00 bis 17:30 Uhr

Kontextbasierte Kommunikation

- Medienvielfalt und überforderte Anwender
- Zielgerichtet kommunizieren durch Kontext-basierte Kommunikation
Thomas Römer, Avaya Deutschland GmbH

12:30 bis 13:00 Uhr

Videokonferenz im Wandel

- Merkmale verschiedener Videolösungen aktuell und zukünftig
 - Qualitätsstufen
 - Zusatzfunktionen
 - Erforderliche Hardware und Software
- Merkmale von Webkonferenzen aktuell und zukünftig
 - Präsentations-Anteil
 - Videoanteil
 - Videoqualität
 - Erforderliche Hardware und Software
- Aktuelle technische Veränderungen

17:30 bis 18:00 Uhr

These zum Get Together – UCC gehört ins Internet

- Ist die Cloud-Paranoia gerechtfertigt?
- Wie viel Mehrwert bietet ein geschlossenes Kommunikationssystem?
- Wie könnte eine offene UC-Architektur aussehen?
- Was braucht man zur Umsetzung?
Dominik Zöller, ComConsult Beratung und Planung GmbH

Ab 18:00 Uhr Get Together

Dienstag, den 20.11.2012 - Vormittag

9:00 bis 10:00 Uhr

UC-Lösungs-Ansätze: Best of Breed vs. All-in-One

- All-In-One Lösungen
 - Umfang
 - Schnittstellen
 - Betrieb
- Best-of-Breed Varianten
 - Welche Kombinationen machen Sinn?
 - Frontend Integration
 - Backend Integration
- Wie stehen die Hersteller zu Frontend und Backend Integration?
- Hersteller-Beispiele
 - Alcatel-Lucent
 - Cisco
 - Innovaphone
 - Siemens
- Managed Service
Dipl.-Inform. Petra Borowka-Gatzweiler, UBN Unternehmensberatung

- Hybrid-Cloud-Architektur mit Office 365

André Liesenfeld, Microsoft Deutschland GmbH

10:45 bis 11:15 Uhr Kaffeepause

11:15 bis 12:15 Uhr

Mehrstandort-Konzepte

- Mehrstandort UC-Architekturen
- Datenraten in WAN und Internet
- Managed Service vs. UCaaS
- Providerkonzepte: Integration von On-Premise Managed Service und Hosted PBX
Claus Elfering, ComConsult Beratung und Planung GmbH

12:15 bis 12:45 Uhr

Warum ISPs an Cloud-Produkten scheitern ...

- Welche Rolle spielen Cloud-Produkte im Portfolio der ISPs?
- Warum bleibt der Erfolg aus?
- Wie kann kollaborative Produktentwicklung helfen?
Dipl.-Kfm. Robin Häberle, Bauhaus-Universität Weimar

10:00 bis 10:45 Uhr

Kommunikation und Kollaboration mit Lync 2013

- Neuerungen in Lync 2013 – Video, Voice, Apps
- Client-Integration mit Windows 8

12:45 bis 14:15 Uhr Mittagspause

Programmübersicht - ComConsult TK-, UC- und Videokonferenzforum 2012

Dienstag, den 20.11.2012 - Nachmittag

14:15 bis 15:00 Uhr

Die Kommunikationspläne des Mittelstandes

- Wie viel UC braucht der Mittelstand?
- Was sind unabdingbare Leistungsmerkmale?
- Welche Technik muss integriert werden?
- Wie funktioniert die Migration?

Dominik Zöllner, ComConsult Beratung und Planung GmbH

15:00 bis 15:45 Uhr

State of the Art bei SIP Trunking

- Einsatzpläne der Unternehmen
 - Marktstudien
 - Praxisbeispiele
- Angebote der Provider
 - BT
 - COLT
 - T-Systems
 - Vodafone
 - ...
- Zertifizierungen: Hersteller, Provider, neutrale Gremien
 - SIPconnect oder any-to-any?
 - SIPforum
 - BITkom

Markus Geller, ComConsult Research GmbH

15:45 bis 16:00 Uhr

Hersteller-Vortrag

16:00 bis 16:30 Uhr Kaffeepause

16:30 bis 17:15 Uhr

UC-Integration von Leitständen

- Integration von VoIP und Funksystemen
- Integration der Video-Überwachung
- Kommunikation für Werksfeuerwehr, Werkschutz und Energieversorger
- Herausforderung Notfall-Szenarien

Dr. Alexander Koenen-Dresp, CONET Solutions GmbH

17:15 bis 18:00 Uhr

Integration in heterogene UC- und Applikationslandschaften

- OpenScape UC und Multi-Vendor-Architekturen
- Video-Integration
- Integration in gängige Groupware, Geschäfts- und Cloud Applikationen

Dipl.-Math. Volkmar Rudat, Siemens Enterprise Communications GmbH & Co KG

Mittwoch, den 21.11.2012

9:00 bis 10:00 Uhr

Moderne Contact Center Lösungen

- „Vermittlungsplatz 2.0“
- Integrierte ACD-Lösungen
- Multimedia Contact Center
- Data Mining und Social Media

Claus Elfering, ComConsult Beratung und Planung GmbH

10:00 bis 10:30 Uhr

Self Service Automation und fortschrittliches Wartefeldmanagement im Contact-Center

- Avaya's Innovation durch workflowbasierte Kontaktsteuerung
- Technologiekonzept und Anwendungsfälle

Stefan Dietrich, Avaya Deutschland GmbH

10:30 bis 11:00 Uhr

Customer Collaboration mit Cisco UCCE

- Mit welchen Medien erreicht man zukünftig die Kundschaft?
- Die Rolle von Sozialen Netzen im Kundenkontakt
- Projektbeispiele mit Cisco UCCE und Social Miner

Cisco Systems GmbH

11:00 bis 11:30 Uhr Kaffeepause

11:30 bis 12:15 Uhr

Voxtron Lync CC

- Zusammenspiel von UC und Contact Center
- Contact Center mit Lync
- Kundenszenarien

Dipl.-Betw. Ralf Mühlenhöver, Voxtron GmbH

12:15 bis 12:30 Uhr

Hersteller-Vortrag

12:30 bis 14:00 Uhr Mittagspause

14:00 bis 15:00 Uhr

UC-Firewalls

- Firewall-Architekturen und Zonenkonzepte
- Welche Probleme bestehen bei Firewalling und UC?
- Welche Rolle spielen STUN und ICE?
- UC-Firewalls und Session Border Controller

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

15:00 bis 15:30 Uhr

UC-Firewalls und SBCs

- Gerätetypen, Feature Sets und Einsatzzweck
- Referenzarchitektur(en)
- Erfahrungen aus Kundenprojekten

Andreas Wächter, ACME Packet

15:30 bis 16:00 Uhr

Standpunkt UC

- Wo steht UC heute?
- Wo geht es hin?
- Wrap-up des UC-Forums

Dominik Zöllner, ComConsult Beratung und Planung GmbH

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

Donnerstag, den 22.11.2012 -

Intensivtag User-centric Communications - UC-Clients und Anwendungsszenarien

9:30 bis 16:30 Uhr

Der Intensiv-Tag beginnt mit einer Vorstellung des Tagesprogramms und der aktuellen Fragestellung im Themenfeld UCC.

Im weiteren Tagesverlauf folgen 4 Herstellervorträge mit Präsentationen/ Live Demos zum Thema UC-Clients

Beendet wird dieser Intensiv-Tag mit einem Abschlussvortrag und einem Fazit.

11:00 bis 11:30 Uhr Kaffeepause

12:30 bis 14:00 Uhr Kaffeepause

16:30 Ende der Veranstaltung

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

ComConsult TK-, UC- und Videokonferenzforum 2012

3 Tage

Kongress

vom 19. - 21.11.12 in Düsseldorf
zum Preis von € 2.090,-- netto

4 Tage

Kongress mit Intensiv-Tag

vom 19. - 22.11.12 in Düsseldorf
zum Preis von € 2.490,-- netto*

1 Tag

Intensiv-Tag

am 22.11.12 in Düsseldorf
zum Preis von € 990,-- netto

Bitte reservieren Sie für mich ein Hotelzimmer



vom _____ bis zum _____ 12
im Van der Valk Airporthotel Düsseldorf.

**Selbstzahler-Sonderpreis
von € 139,-- pro
Übernachtung
inklusive Frühstück**

Zusätzlich bestelle ich folgenden Technologie-Report



Session Initiation Protocol -
zum Sonderpreis von 338,- € netto



Sicherheitsmechanismen für Voice
over IP - zum Sonderpreis von 338,- €
netto



Unified Communications: Cisco
versus Microsoft - zum Sonderpreis
von 338,- € netto

VoIP-Kollektion - alle drei Reports
zum Sonderpreis von 890,- € netto

Vorname

E-Mail

Nachname

Ich habe die Kongressbedingungen zur Kenntnis
genommen.

Firma

Unterschrift

Straße

PLZ, Ort

Telefon, Fax

ComConsult
Akademie

Pascalstraße 25 - 52076 Aachen

Telefon +49 (2408) 955-300

info@comconsult-akademie.de

www.comconsult-akademie.de

Das Wissensportal

Das Wissensportal

"Das Wissensportal" ist das neu gestaltete Web-Portal von ComConsult Research. Hier finden Sie eine bunte Mischung aus aktuellen Informationen, persönlichen Meinungen und ausführlichen Grundlagen-Artikeln über die gesamte Themenpalette der IT- und Netzwerkwelt. Die Artikel des ComConsult Wissensportals geben Ihnen die Möglichkeit der Stellungnahme, des Kommentars oder der Diskussion mit anderen Lesern. Nutzen Sie diese Gelegenheit, die Sichtweise anderer Spezialisten zu erfahren. Unser Newsletter informiert Sie hierbei regelmäßig über Neuerscheinungen.

Service-Oriented Networks (SON) statt Software-Defined Networks (SDN)

1. Oktober 2012 von Heinz Behrens



Wie ja hier auch schon in mehreren Artikeln ausgeführt, ist Software-Defined Networking (SDN) ein sehr interessanter Ansatz für die Weiterentwicklung von Netzwerklösungen. Im Fokus von SDN stehen allerdings primär extrem große Firmen wie Google, Deutsche Telekom, Microsoft, Yahoo, etc. (also die Gründungsmitglieder der ONF). Andere Unternehmensnetzwerke, die nicht diese Größe erreichen, haben dagegen typischerweise andere Anforderungen.

[Kompletten Artikel lesen unter www.comconsult-research.de](http://www.comconsult-research.de)

Warum Layer2?

13. September 2012 von Dr. Behrooz Moayeri



Angesichts der Herausforderungen, vor die der Trend zu Layer 2 in Rechenzentren die IT-Verantwortlichen in Unternehmen stellt, ist eine Diskussion um die Frage ent-

brannt, wie es zu diesem Trend kommen konnte, nachdem sich die Entwicklung der unternehmensinternen Netze jahrelang am durch und durch Layer-3-strukturierten Intranet ein Beispiel genommen hatte.

[Kompletten Artikel lesen unter www.comconsult-research.de](http://www.comconsult-research.de)

Die Wirtschaftlichkeit von Intranets

27. September 2012 von Dr. Franz-Joachim Kauffels



Die Frage nach der Wirtschaftlichkeit stellt sich heute vor dem Horizont allfälliger Bedrohungen durch einen verschärften Wettbewerb und die Globalisierung der Märkte sowie die schwindelerregende technische Entwicklung heute mehr denn je. Gerade neue Konzepte wie Intranet müssen schon im Vorfeld auf mögliche Vor- und Nachteile untersucht werden, damit nicht noch einmal das Gleiche wie beim Client/Server-Betriebskostenchaos passiert.

[Kompletten Artikel lesen unter www.comconsult-research.de](http://www.comconsult-research.de)

Schnittstellen im RZ: einfacher oder komplexer?

12. September 2012 von Dr. Behrooz Moayeri



Mit der Servervirtualisierung übernahm die Virtualisierungslösung eine Netzfunktionalität, nämlich das Bereitstellen von virtuellen Switch Ports für die virtuellen Maschinen (VMs). Daher hat der Marktführer VMware diese Funktionalität als den sogenannten vSwitch implementiert. Später wurde zwischen dem in Standard Switch umbenannten einfachen vSwitch und dem Distributed Switch unterschieden. Die Idee beim Distributed Switch ist, dass mehrere vSwitches zu einer logischen Einheit zusammengefasst und an einer Stelle, in der Regel im Rahmen der Managementlösung für die ganze Virtualisierungsumgebung, konfiguriert und administriert werden.

[Kompletten Artikel lesen unter www.comconsult-research.de](http://www.comconsult-research.de)

Software Defined Networking: Quo Vadis

10. September 2012 von Markus Nispel



Endlich! Eine Technologie, die alle Probleme mit der Netzwerkinfrastruktur lösen wird. Wieder einmal. Aber hatten wir das nicht schon einmal? In schöner Regelmäßigkeit sehen wir Technologien dem Gartner Hype und seinen Phasen folgen. Was vor 2 Jahren noch die Fabrics und auch FCoE (Fibre Channel over Ethernet) waren – und wobei FCoE sich gerade im "Through of desillusionment" befindet – ist SDN auf dem "Peak of inflated expectations". Oder kann man die Diskussionen zu den Problemlösungen durch SDN, die Anzahl der Startups in diesem Bereich, eine unklare Definition von SDN und der Kauf eines kleinen Startups für 1,25 Milliarden USD durch VMware anders interpretieren? Klar ist für mich, dass SDN eine Technologie ist, die zum Bleiben gekommen ist. Die Konzepte machen sehr viel Sinn, wir bei Enterasys hatten schon in den frühen 90ern damit experimentiert und forcierten seit einigen Jahren diese Art des Networking, ohne es je SDN genannt zu haben. Viele Kunden setzen die heute erfolgreich ein. Auch in der Telefonie waren IN Intelligente Netze auch schon immer

präsent. Was aber genau ist ein SDN?

[Kompletten Artikel lesen unter www.comconsult-research.de](http://www.comconsult-research.de)

ComConsult-Study.tv

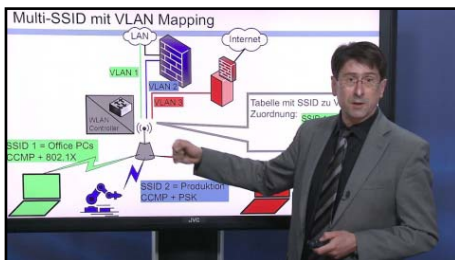
Wireless-Spezial im Oktober bei ComConsult-Study.tv

Ist IEEE 802.11n bereits am Ende? Was bringt der 802.11ac? Dr. Kauffels stellt beide Verfahren vor und analysiert, was sie wirklich fernab der Marketingversprechungen leisten können. Abgerundet wird unser Wireless-Spezial durch ein Video zur WLAN-Sicherheit von Dr. Hoff. Verpassen Sie nicht unser WLAN-Spezial im Oktober passend zum neuen Wireless Report.

Das Paket umfasst folgende Videos:

Sicherheit in Wireless LAN

Referent: **Dr. Simon Hoff**
 Zeit: 0:30:53
 Einzelpreis: 39,00 € netto
 Im Abo: kostenlos



Jede Funk-basierte Übertragung ist automatisch mit der Frage der Sicherheit der Übertragung verbunden. Dr. Hoff erläutert, warum das Thema brisant ist und stellt die verschiedenen Optionen zur Umsetzung von Sicherheit für verschiedene Typen von WLANs vor.

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.

IEEE 802.11n Leistungsanalyse

Referent: **Dr. Franz-Joachim Kauffels**
 Zeit: 0:18:05
 Einzelpreis: 39,00 € netto
 Im Abo: kostenlos



IEEE 802.11n hat sich im Markt als dominante WLAN-Technik durchgesetzt. Doch immer wieder kommt es zu Betriebssystemen, in denen die Leistung deutlich abnimmt. Dieses Video untersucht mit Hilfe der Warteschlangentheorie, wovon die Leistung abhängt, was das Maximum ist und wie sie Zellen gestalten müssen, um ein Optimum an Leistung zu erhalten.

IEEE 802.11n

Referent: **Dr. Franz-Joachim Kauffels**
 Zeit: 00:50:35 gesamt
 Einzelpreis: 59,00 € netto
 Im Abo: kostenlos



IEEE 802.11n hat den Durchbruch für Wireless-Netzwerke geschaffen. Die endgültige Verabschiedung in 2009 legt die Basis für viele neue Produkte. Dr. Kauffels erklärt, wie diese Technologie funktioniert und was Sie maximal von ihr erwarten können.

Bundle-Erweiterung mit neuem Report Moderne Wireless-Technologien

Autor: **Dr. Franz-Joachim Kauffels**
 Einzelpreis: 349,- € netto



Mit diesem Report erhalten Sie ein umfassendes Grundlagenwerk, das die Basis bietet, Entscheidungen mit dem nötigen Fundament zu treffen. Abgesehen von einer grundsätzlichen Einführung in die Möglichkeiten der Implementierung von Multi-Gigabit-WLANs in den bekannten Frequenzbereichen und Bändern werden die Technologien von 11n, 11ac und 11ad vorgestellt und untereinander verglichen.

Das Bundle dieser vier Videos kostet nur € 119,-* netto. Sie sparen über 30%.

*Statt regulärer Preis € 176,- netto. Diese Angebote gelten nur im Oktober 2012.

Video-Bundle + Report nur € 429,-* netto.

*Statt regulärer Preis € 525,- netto.

Schwerpunkthema

Werden SDN und OpenFlow herkömmliche Netzwerke verdrängen?

Fortsetzung von Seite 1



Dipl.-Inform. Petra Borowka-Gatzweiler leitet das Planungsbüro UBN und gehört zu den führenden deutschen Beratern für Kommunikationstechnik. Sie verfügt über langjährige erfolgreiche Praxiserfahrung bei der Planung und Realisierung von Netzwerk-Lösungen und ist seit vielen Jahren Referentin der ComConsult Akademie. Ihre Kenntnisse, internationale Veröffentlichungen, Arbeiten und Praxisorientierung sowie herstellerunabhängige Position sind international anerkannt.

Die ASIC-Technik brachte jedoch auch Nachteile: reduzierte Funktionalität, verlängerte Produktionszyklen, fehlende Änderbarkeit; die Control Plane von Netzwerk-Komponenten, Firmware und auch Software, insbesondere Switches und Routern, ist nun seit vielen Jahren proprietär, gegen einen Zugriff des Betreibers abgeschottet und verbleibt unter der Kontroll-Hoheit der Hersteller. So entstanden Netzwerke mit vertikal integrierter Funktionalität, in denen für jeden Switch dezentral eine umfangreiche Konfiguration eingerichtet und aufrecht erhalten bleiben muss. (siehe Abbildung 1.1)

IP-Prinzip: IP-basierte Netzwerke wurden auf dem Architektur-Prinzip von Autonomen Systemen (AS) gebildet. Dies bedeutet Skalierbarkeit und geografische Ausdehnung durch eine Verbindungslogik, bei der Pakete zu einem Next Hop weitergeleitet werden, der auf der Basis beschränkter Informationen eine vernünftige Zwischentappe auf dem Weg zum Ziel darstellt. Die zu verwaltenden Informationen sind nach diesem Prinzip auf ein Minimum beschränkt, das mit beschränkten Speichermitteln den Aufbau weltweiter Netze erlaubt. Das IP und AS Prinzip hat aber einen bekannten Nachteil: Die Identität ist immer mit der Topologie verknüpft, ein System kann nicht beliebig von A nach B wandern, ohne die Identität im Sinne der Netzwerk-Adresse zu ändern. Über viele Jahre hinweg wurde versucht, diesen Nachteil mit VPN- und VLAN-Technik zu umgehen. Beides reicht jedoch nicht aus, um die Migrations-Bedarfe virtueller Maschinen in heutigen Data Center Strukturen handhaben zu können.

Robustheit vs. Flexibilität: Während viele Jahre lang der Fokus bei Netzdesigns auf der Robustheit und Fehlervermeidung lag, treten jetzt Anforderungen in den Vordergrund, dynamische Zustandsinformati-

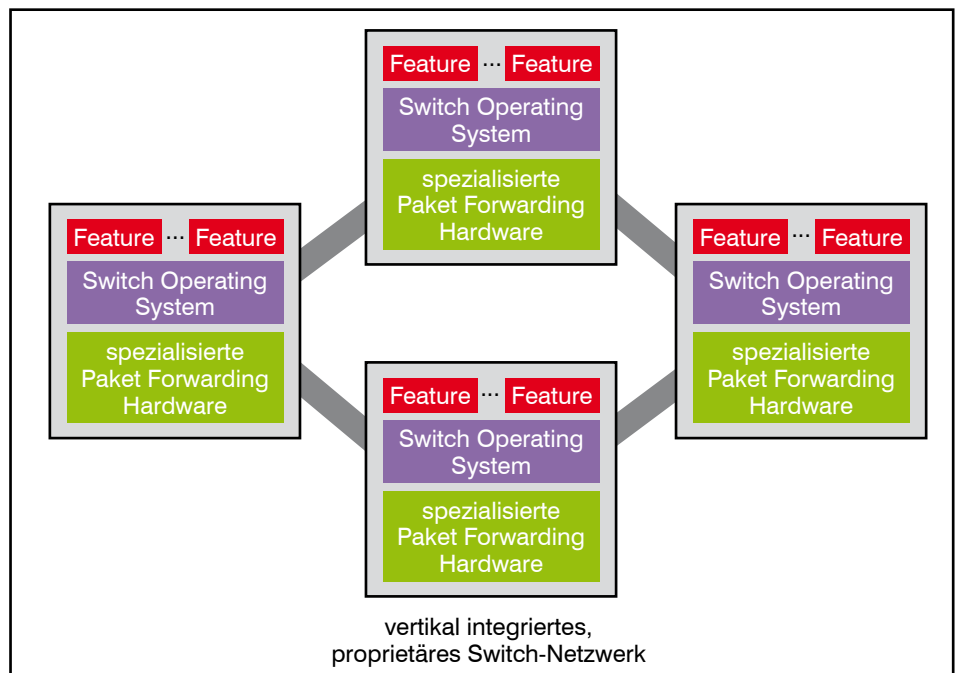


Abbildung 1.1: Vertikale integrierte, proprietäre Switch-Architektur

onen an realen oder virtuellen Switchports zu handhaben und spezifische Verkehrslasten flexibel steuern zu können. Videoanwendungen beispielsweise lassen sich bei Überlast durch Drops oder Drosselung der Eingangsrate auffangen, Finanztransaktionen oder Patientenüberwachung nehmen jeden Paketverlust äußerst übel. Hierauf könnten moderne Netze so reagieren, dass sie unterschiedliche Anwendungen über unterschiedliche Wege transportieren. Anforderungen an eine dynamisch angepasste Paketweiterleitung und Wegwahl treten insbesondere im Zusammenhang mit hochdynamischen Verkehrslasten zwischen virtuellen Servern, "Ost-West-Verkehr", Data Center-Flexibilisierung und Cloud Diensten auf. Für solche dynamischen Verkehrslasten ist das

klassische dezentrale Hop-by-Hop IP Routing Paradigma jedoch nicht wirklich gut geeignet.

Komplexität vs. Flexibilität: Die aktuelle Netzwerk-Technologie besteht aus mehreren voneinander unabhängigen, standardisierten Layer-2 und Layer-3 Protokollen wie STP, LACP, OSPF, VRRP, BGP, IEEE 802.1X, IPsec etc., die Endsysteme zuverlässig und sicher über beliebige Distanzen, Linkgeschwindigkeiten und Topologien miteinander verbinden. Diese Protokolle arbeiten ohne gegenseitige automatische protokoll-übergreifende Konsistenzprüfung, daher liegt es in der Verantwortung des Netzwerk-Administrators, die Parameter der verschiedenen Protokolle aufeinander abzustimmen. Hinzufü-

Werden SDN und OpenFlow herkömmliche Netzwerke verdrängen?

gen oder Ändern einzelner Geräte oder Gerätegruppen führt zu Konfigurations-Änderungen in allen Switches, Routern, Firewalls, Web Authentisierungs-Portalen etc., da ACLs, VLANs, QoS Regeln usw. auf Element-Manager-Basis für jede Netzkomponenten-Gruppe geändert werden müssen. Diese mehr oder weniger statische Natur von Netzwerken wird der dynamischen Natur heutiger Server-Umgebungen nicht mehr gerecht, in der einzelne Applikationen über mehrere VMs auf mehrere Hosts verteilt sind und (in großen Cloud Rechenzentren) VMs dynamisch nach Bedarf bereitgestellt oder deaktiviert werden.

Konsistenz und dynamische Skalierbarkeit: Die Konfiguration einer netzweiten Policy erfordert es gegebenenfalls, Hunderte bis Tausende Netzkomponenten anzufassen und z.B. ihre ACL-Konfiguration anzupassen. Dies kann Stunden bis Tage dauern und birgt bei aller Sorgfalt bei großen Netzen ein erhöhtes Risiko für Konfigurations-Inkonsistenzen, da ja keine komponentenübergreifende Konsistenzprüfung gegeben ist. Das heißt, mit traditioneller Netzwerktechnik können Netze einerseits nicht schnell genug erweitert werden, andererseits wächst die Komplexität tausender separat konfigurierter Netzkomponenten so stark an, dass sie kaum noch beherrschbar ist.

Deterministik vs. Dynamik: Die aktuellen Netzwerk-Verfahren sind auf Verkehrsmuster ausgelegt, die sich vergleichsweise langsam ändern, so dass notwendige Erweiterungen, ggf. unterstützt von Trendberechnungen, im Bedarfsfall manuell durchgeführt werden können. In großen Rechenzentren können die Verkehrsmuster jedoch so dynamisch und über so viele VMs verteilt sein, dass eine Vorhersage und Trendberechnung nicht mehr möglich ist. Large-Scale Parallelprozesse und die zugehörigen Datenbanken sind teilweise über einen kompletten Serverpool verteilt, mit steigender Anzahl Endnutzer-Applikationen (ein Beispiel: Durchsuchen und Indizierung des gesamten Webs und sofortige Rückgabe eines Suchergebnisses zum Endnutzer) steigt das Datenvolumen zwischen vernetzten Knoten auf PetaBytes. Solche Netzwerke müssen Hunderttausende bis Millionen Server verbinden, und dies kann eine manuelle Provisionierung und Konfiguration nicht mehr leisten.

VLAN-Grenzen und Mandantenkonzepte: In großen Umgebungen, insbesondere auch bei Mandantenkonzepten, reicht der VLAN-Nummernbereich von 4096 VLANs nicht mehr aus. Wächst ein Mandant so stark, dass er nicht mehr in ein IP Subnetz hineinpasst oder gibt es überlappende IP/VLAN Adressbereiche, so müssen kom-

plexe Mandanten-Techniken wie VRF, NAT, MPLS oder andere Overlay-Netze greifen. Um ein Vielfaches der 4000 VLANs zu betreiben, sind Overlay-Technologien wie VXLAN, NVGRE, MPLS, LISP notwendig. Mit steigender Anzahl Mandanten und VLANs und Overlay-Technologien ergibt sich wiederum der Bedarf nach zentraler, konsistenter Konfiguration und gegebenenfalls zentral gesteuert dynamischer Anpassung.

Virtuelle Switches: Mit steigender Anzahl virtueller Maschinen auf Hostsystemen steigt auch die Anzahl eingesetzter virtueller Switches (vSwitches). Vielfach werden diese nicht oder nicht ausschließlich vom Netzwerk-Administrator, sondern vom Server-Administrator gehandhabt. Etablierte Switch-Hersteller haben als Antwort darauf eigene Management-Erweiterungen entwickelt, um die Migration von VMs und das Management von vSwitches netzwerkseitig zugreifbar oder einsehbar zu machen. Hier wäre ein deutlicher Fortschritt erreicht, wenn alle vSwitches erstens eine einheitliche Funktionalität hätten (z.B. Open vSwitch) und zweitens mit einem gemeinsamen, vom Server-Management losgelösten Management-Tool provisioniert, administriert und überwacht werden könnten.

Bei all diesen Problemfeldern kommen Software-Defined Networking (SDN) und OpenFlow ins Spiel: Sie wollen die Netzsteuerung auf einen zentralen Controller auslagern und damit vollständig flexibilisieren und dynamisieren.

1.2 Wie hängen ONF, SDN und OpenFlow zusammen?

ONF

Anfang 2011 gründeten die Deutsche Telekom, Facebook, Google, Microsoft, Verizon und Yahoo die Open Networking

Foundation als non-Profit Konsortium mit dem Ziel, Software Defined Networking (SDN) nach vorne zu treiben und für die Netzwerk-Technologie im Markt durchzusetzen. Die Standardisierung einer eigenen Netzwerk-Architektur, die Netze weltweit programmierbar macht, soll die Umsetzung von SDN ermöglichen. Später erfolgte der Beitritt von Broadcom, Brocade, Ciena, Cisco, Citrix, Dell, Ericsson, Force10, HP, IBM, Juniper, Marvell, Microsoft, NEC, Netgear, NTT, Oracle, Riverbed Technology und VMware. Aktuell hat die ONF mehr als 70 Mitglieder aus verschiedenen marktrelevanten Technologiebereichen: Provider, Netzwerk-Komponenten-Hersteller, Chip-Hersteller, Software- und System-Hersteller. (siehe Abbildung 1.2)

Eines der Ziele von ONF ist es, OpenFlow zu standardisieren. Hierfür hat sie technische Arbeitsgruppen ins Leben gerufen, die sich um das Protokoll, die Konfiguration und Multivendor Interoperabilitätstests kümmern.

SDN

Begeben wir uns noch einmal zurück in die 70er und 80er Jahre: Damals war ein Router ein Server (typischerweise Unix), der Datenpakete zwischen zwei oder mehreren Netzwerk-Schnittstellen weiterleitete, z.B. X.25... Heute haben wir skalierbare Mehrkern-Prozessoren und handelsübliche Netzwerkprozessoren, die immer mehr Funktionsmöglichkeiten bieten, Programmierwerkzeuge sind weltweit verfügbar. Warum also nicht Software-Entwicklung für Netzwerke etablieren? Was spricht dagegen, in jedem Rechner einen oder mehrere eigene Prozessoren für Netzwerk-Aufgaben abzustellen?

Hier kommt nun Software Defined Networking ins Spiel. SDN ist eine aufkommen-



Abbildung 1.2: Gründungs-Mitglieder der ONF

Werden SDN und OpenFlow herkömmliche Netzwerke verdrängen?

de Netzwerk-Architektur (siehe Abbildung 1.3), die den bislang proprietären Control Plane Konzepten ein Ende bereiten will: Die Control Plane wird aus den Netzkomponenten auf zentrale Steuerungselemente ausgelagert. Hierdurch wird sie für den Betreiber (mittels remote Software Clients) zugreifbar und programmierbar. Damit sind SDN und OpenFlow eigentlich gar nicht so weit weg von Fabric-Architekturen. Im Unterschied zu diesen soll SDN jedoch herstellerübergreifend in Multivendor-Umgebungen einsetzbar sein. Um dies für alle Produkte zu erreichen, wird die Control Plane offengelegt, es werden offene, standardisierte Protokolle entwickelt, die Control Plane setzt auf einem Standard-Server und Standardbetriebssystem auf.

SDN will die Netzwerk-Kontrolle (Lernen und Weiterleitungs-Entscheidungen) von der Netzwerk-Topologie und Paketweiterleitung (physikalische Verbindungen, Interfaces und deren Beziehung zueinander) entkoppeln.

Da die Control Plane ausgelagert ist, kann sie verschiedenste Arten von Netzkomponenten steuern: vSwitches, Hardware-Switches, Router, WLAN Access Points, Load Balancer, Traffic Shaper, Firewalls etc. Somit kann eine Gesamtsteuerung der kompletten verkabelten und kabelle-

sen Netzwerk-Infrastruktur aus einer gemeinsamen Topologie-Sicht heraus implementiert werden. In diesem Sinn lässt sich SDN als übergeordnete Orchestrierung des Netzwerks und der Netzwerk-Dienste betrachten, bei der die Netzwerk-Dienste von den physikalischen Netzwerk-Interfaces und physikalischen Netzwerk-Infrastrukturen losgelöst sind. Die ONF führt auch Studien zur Entwicklung offener APIs für entsprechende übergreifende Management Tools durch.

Globale Service-Definitionen müssen nicht mehr auf die physikalischen Interfaces gemappt werden, Service-Einheiten (zum Beispiel eine Applikation, eine VM) können zwischen verschiedenen Interfaces migrieren, ohne ihre Identität zu ändern oder getroffene Spezifikationen zu verletzen. In dem Maß, wie globale Service-Definitionen nicht mehr auf alle Interfaces und alle Interface-Lokationen gemappt werden müssen, kann eine Vereinfachung des Netzwerk-Betriebs erreicht werden.

Die neue Control Plane nutzt typischerweise eine Overlay-Netztechnologie, im Regelfall ein Enkapsulierungs-Verfahren.

Die Vision ist nun: Netzwerk-Administratoren können dann anhand der logischen Netzwerk-Abstraktion das Verhalten des Gesamt-Netzwerks programmieren, an-

statt die Konfiguration von tausenden Netzwerk-Komponenten anfassen zu müssen. Über den SDN Controller mit seiner zentralen Intelligenz kann das Netzwerk-Verhalten in Echtzeit geändert werden und können neue Netzwerk-Dienste / -Applikationen innerhalb von Stunden oder Tagen anstelle von Wochen oder Monaten ausgerollt werden. Die logische Gesamtsicht soll zudem die effiziente Ausnutzung aller Netzwerk-Ressourcen (Switches, Router, WLAN-Komponenten, Load Balancer etc.) ermöglichen.

Denkbare Einsatzszenarien über das ganz normale Forwarding hinaus sind zum Beispiel:

- Zentrale Konfiguration einer netzweiten NAC Policy
- Generierung isolierter VLANs mittels statischem Flow-Set und Map auf eine bestimmte VLAN-ID
- IP Mobiltelefonierer: Bei Verbindungsaufbau führt der Controller ein Location Tracking mit anschließender automatisierter Reprogrammierung der Flow-Einträge durch
- Non-IP Netzwerke (Ketzerei !!): Da OpenFlow nicht vom IP Header abhängig ist, könnten auch neue Routing Protokolle unterstützt werden (back to the roots mit Ethertype Klassifizierung...)
- Paket-Bearbeitung anstelle von Flow-Bearbeitung: z.B. für IDSs oder Überlast-Kontrolle, die nicht flow-basiert arbeiten müssen

Man verspricht sich von SDN Vorteile und Ausbreitung in drei Zyklen:

- Innovation durch schnellere Produktzyklen
- Anpassbarkeit: Eigenkonfiguration durch Netzwerk-Administratoren mittels Skripten
- Anwendungsvielfalt: 3rd Party Applikationen und breites Ökosystem für Netzwerke

Im Rahmen von SDN werden recht verschiedene Konzepte gehandelt, zum Beispiel ein symmetrisches oder asymmetrisches Modell: Im asymmetrischen Modell wird die globale Information weitest möglich zentralisiert (was die Konsolidierung erleichtert), während die Steuerung des Netzwerk-Edge weitest möglich verteilt wird (was Verkehrslast-Aggregation und den Enkapsulierungs-Aufwand minimiert). Dies lässt jedoch Fragen über die Kohärenz verschiedener SDN-Elemente, die Scale-Out-Möglichkeiten und HA-Möglichkeiten bei Mehrstandort-Konzepten aufkommen, die das herkömmliche AS-basierte Netzwerkmodell gut gelöst hat. Im symmetrischen Modell wird die Verteilung

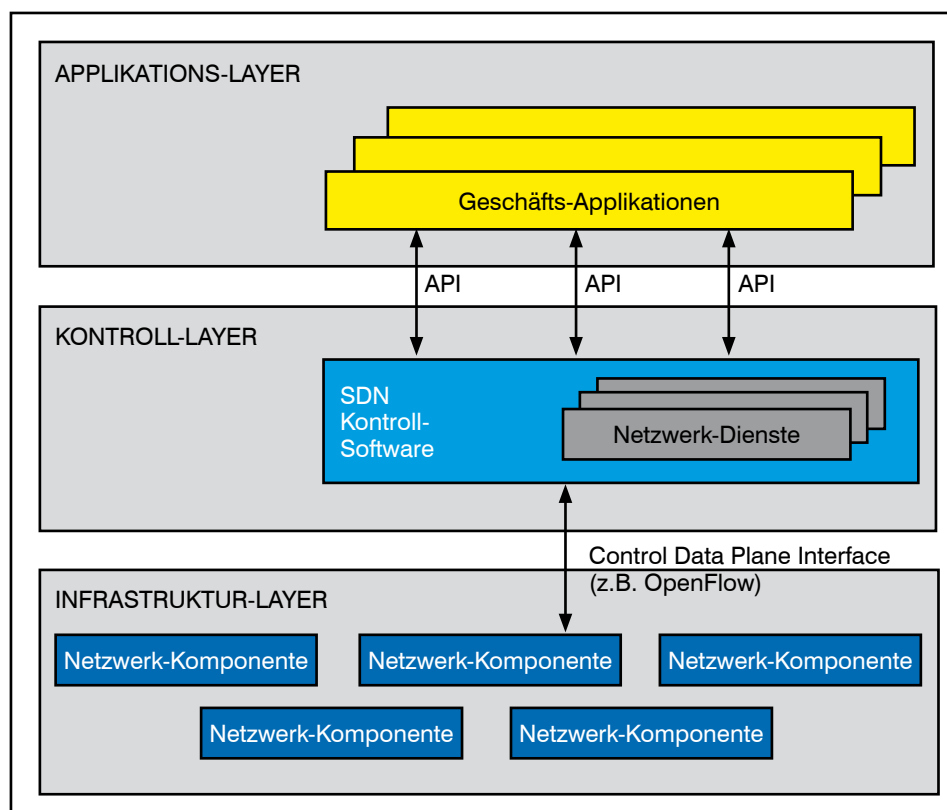


Abbildung 1.3: Logische Übersicht der SDN-Architektur

Werden SDN und OpenFlow herkömmliche Netzwerke verdrängen?

der globalen Informationen erhöht, ebenso die Leistungsfähigkeit von SDN Aggregation in den SDN-Komponenten, die dann im Wesentlichen alle vom selben Komponententyp sind. Die symmetrischen SDN-Komponenten können dann ein SDN Overlay bilden, so lange wie eine Netzwerk-Erreichbarkeit für irgendein Subset der SDN-Komponenten gegeben ist.

Ein weiterer Konzept-Ansatz betrifft Modelle mit oder ohne Fluten der globalen Information: Im Flutungs-basierten Modell werden wesentliche Anteil der globalen Information über well-known Broadcast- und Multicast-Mechanismen gelernt (dies passt zu symmetrischen Modellen). Im Flutungs-losen Modell basiert jede Weiterleitung auf einem exakten Match, der typischerweise mit verteilten Hashtabellen und verteilten Caches von SDN Lookup-Tabellen erreicht wird.

Ein dritter Ansatz befasst sich mit Host-basierten versus netzwerk-zentrischen Konzepten. Der Host-basierte Ansatz fokussiert sich auf Data Center Umgebungen mit einer hohen Anzahl virtueller Maschinen und vMotion. In dieser Umgebung findet die SDN Enkapsulierung stellvertretend für die VMs im Hypervisor statt, das heißt der Host muss die entsprechende Rechenleistung für die Enkapsulierung bereitstellen. Dies entlastet die "Edge Komponenten" des Netzwerks von der SDN Enkapsulierung. Das netzwerk-zentrische Konzept hat eine klarere Demarkationslinie zwischen Netzwerk Edge und Endsystem. In diesem Modell ist der SDN Edge typischerweise der ToR Switch außerhalb des Hosts. Dieses Modell belässt die Routing Funktion und komplexeren Switching Funktionen in den Netzwerk-Komponenten es steht der traditionellen Netzwerktechnik somit näher als das Host-basierte Modell.

Die aufgeführten verschiedenen Modelle (und ihre Kombinations-Spielarten) machen schon deutlich, dass es noch keine ganz klare Sichtweise gibt, was SDN alles beinhaltet und was nicht. Insgesamt gilt Vorsicht: Nicht überall, wo SDN drausteht, ist auch SDN drin.

Die "incumbent" Netzwerk-Hersteller schließen sich zum Beispiel dem Hype an und benennen ihre APIs und SDKs einfach in SDN um, während sie sich in Wirklichkeit davor drücken, ihre Flow Tabellen für externen Zugriff freizugeben.

OpenFlow

OpenFlow ist eine verfügbare Ausprägung von SDN, es ist eine Open Source Option für Control Plane. Andere Control Pla-

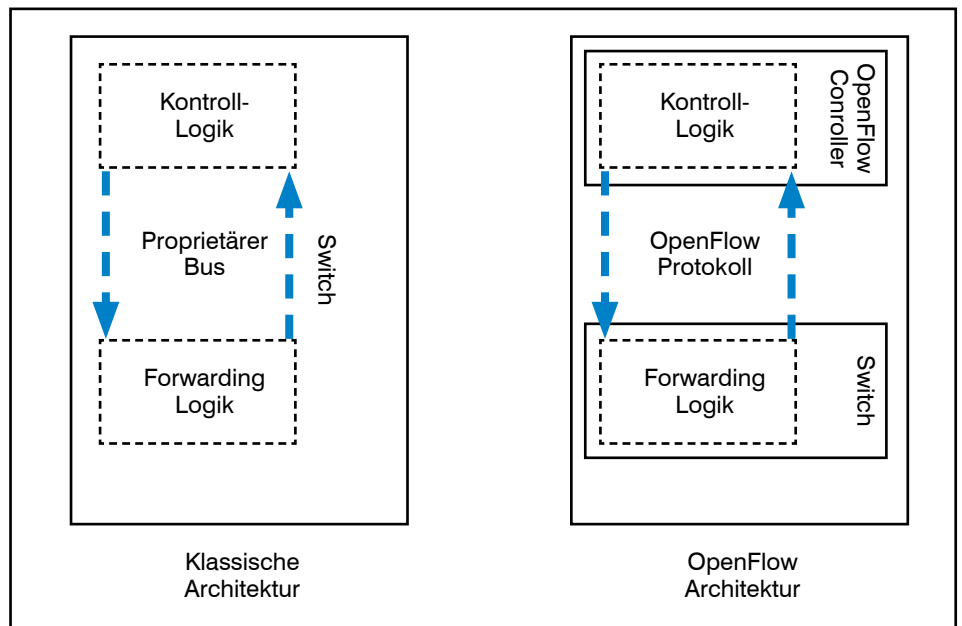


Abbildung 1.4: Klassische dezentrale Switching Architektur und OpenFlow Architektur

ne Protokolle, die teilweise auch schon vor OpenFlow spezifiziert wurden, sind zum Beispiel ALTO, Netconf oder PCE. An die Stelle der proprietären "closed shop" Switch-Architektur tritt ein standard-basierter Controller, das Openflow Protokoll und eine vereinheitlichte, standardisierte Forwarding Logik, wie die Übersicht in Abbildung 1.4 zeigt.

Die Anfänge von OpenFlow gehen im Wesentlichen auf die Stanford Universität mit den Professoren Nick McKeown und Martin Casado (und Team) zurück. Casado und McKeown sind ebenfalls Gründer der Firma Nicira (vor kurzem von VMware übernommen), die einen OpenFlow Controller / Plattform entwickelt hat. Eines der ersten Einsatzszenarios entstand aus dem

Kongress

**ComConsult Rechenzentrum
Infrastruktur-Redesign Forum 2012
05.11. - 08.11.12 in Köln**

Unsere Rechenzentren befinden sich in einer der größten Redesign-Phasen der letzten 20 Jahre. Nahezu alle Gestaltungs-Bausteine von den Servern, Speicher-Technologien, Netzwerken bis hin zu den Applikations-Architekturen sind im Umbruch. Gleichzeitig entstehen durch eine Explosion mobiler Teilnehmer auf der einen und durch Cloud-Technologien auf der anderen Seite völlig neue Rahmenbedingungen.

Das ComConsult Rechenzentrum Infrastruktur-Redesign Forum 2012 greift die herausragenden Fragen der Umsetzung zukunftsorientierter und wirtschaftlicher Rechenzentren auf. Mit nahezu allen betroffenen Technologien im Umbruch ist dies das richtige Forum zum richtigen Zeitpunkt.

Moderation: Dr. Behrooz Moayeri, Dr. Jürgen Suppan

Kosten: 4-tägige Veranstaltung inkl. Intensiv-Tag € 2.490,- netto
3-tägige Veranstaltung ohne Intensiv-Tag € 2.090,- netto
Nur Intensiv-Tag € 990,- netto



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

Werden SDN und OpenFlow herkömmliche Netzwerke verdrängen?

Bedarf nach Skalierung von Ports und Bandbreite in sehr großen Data Centern und massiver Parallelverarbeitung (z.B. Google Suchmaschinen), mit denen auch aktuelle Fabric Architekturen überfordert sind: Es ging um die Lösung des (nach McKeowen) "Million-MAC-Address und Hadoop / MapReduce Problems". OpenFlow wurde so entwickelt, dass es als experimentelles Overlay Netzwerk auf einem produktiven Netzwerk laufen kann, ohne das Produktivnetzwerk direkt zu beeinflussen. Somit erlaubte OpenFlow, neue Protokollmechanismen zu entwickeln und auf einer produktiven (Ethernet-)Netzwerk-Infrastruktur auszutesten.

Im Dezember 2009 entstand die OpenFlow Version 1.0.0, gefolgt von v1.1.0 im Februar 2011 bis hin zu v1.3.0. im April 2012. OpenFlow erweckte – im Gegensatz zu Vorgänger-Protokollen – die Aufmerksamkeit sehr großer Marktspieler und war ein wesentlicher Faktor für die Gründung der ONF.

Setzen sich SDN und OpenFlow durch, stehen im Ergebnis nicht mehr die einzelne Netzkomponenten mit proprietären Features, proprietärem Betriebssystem, proprietärer Hardware und ASICs im Fokus der Netzbetreiber / -administrator sondern das Gesamt-Management-Tool mit verschiedenen Anwendungs-Modulen, das allgemeingültige Features in Switches mit OEM ASICs steuert. Der Mehrwert für den Kunden von Steuerung und Management steigt, der Mehrwert spezieller Hersteller-Hardware sinkt. Einen Vergleich zwischen aktuellen Switch-Netzwerken und OpenFlow-basierten Switch-Netzwerken zeigen Abbildung 1.5 und Abbildung 1.6.

2. OpenFlow Übersicht

2.1 Architektur

OpenFlow setzt die SDN-Architektur für geschwächte Netzwerke um, indem es ein software-gesteuertes Switch-Netzwerk mit einer zentralen Control Plane zur Netzwerk-Steuerung und OpenFlow-fähigen Switches für ein verteiltes Forwarding (Forwarding Plane, Data Plane) definiert. OpenFlow ist das erste verabschiedete Standard-Kommunikations-Interface zwischen der Control Plane und den Forwarding Ebenen der SDN Architektur. Es wird also auf beiden Seiten dieses Interfaces implementiert. OpenFlow bietet für die Implementierung von SDN erstens eine Spezifikation, was ein Controller ist und wie er die Verbindung zu Switches herstellt, zweitens ein Protokoll zwischen Controller und Switches, d.h. eine Spezifikation, wie der Controller die Switching oder Routing Forwarding Tabellen manipuliert und so das Processing am Switch-Eingang so-

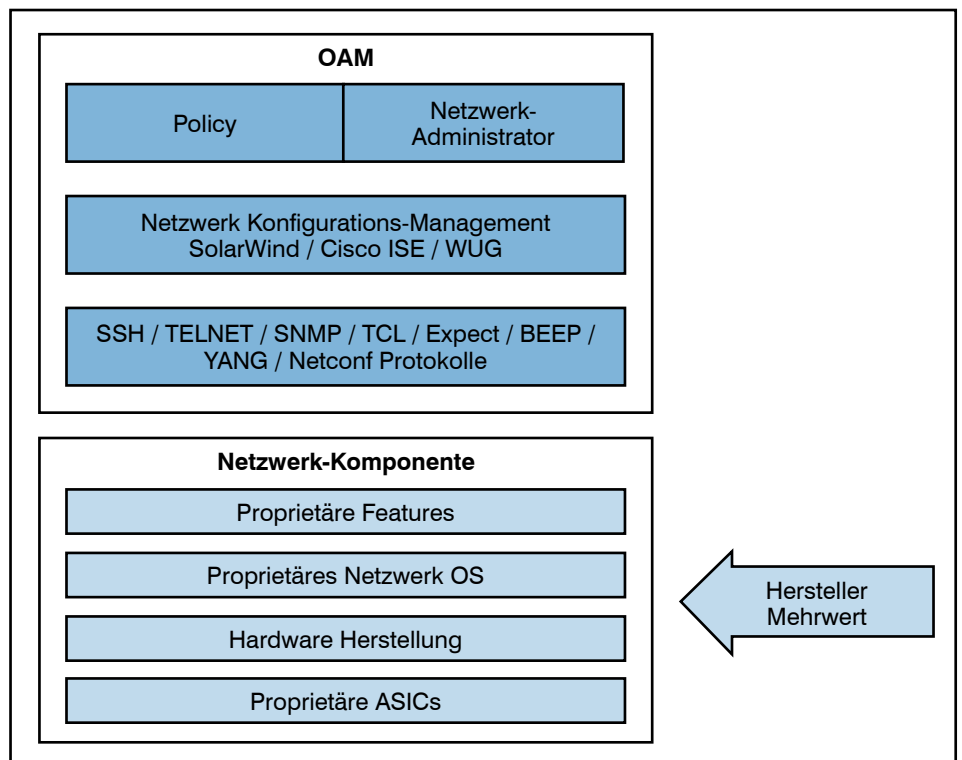


Abbildung 1.5: Mehrwert-Fokus in aktuellen Netzwerken

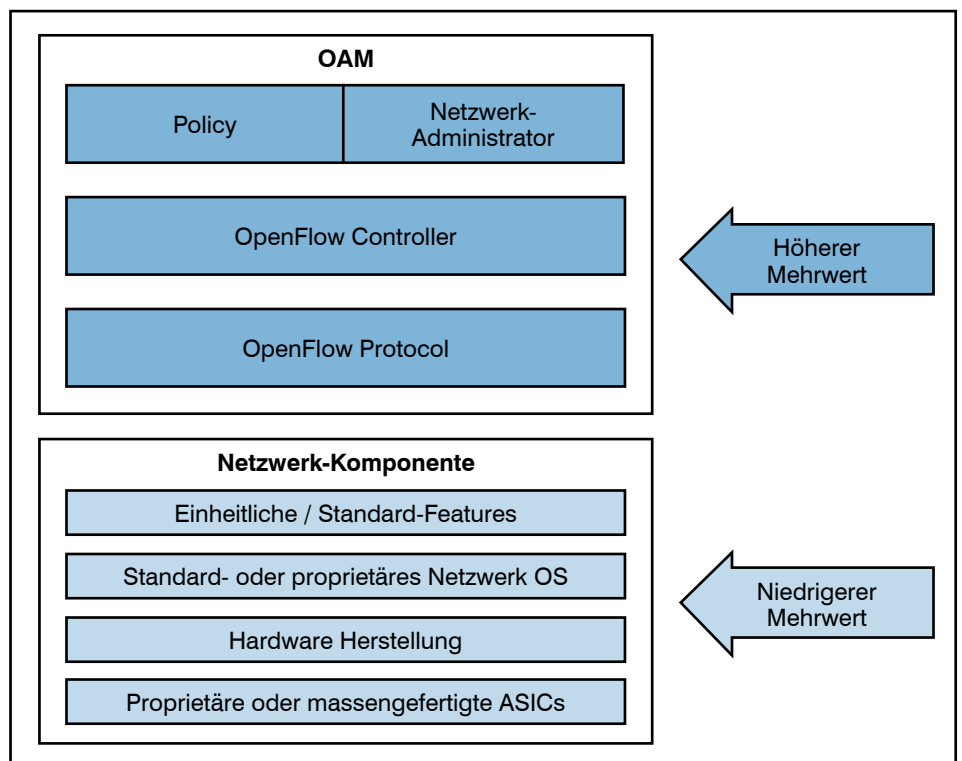


Abbildung 1.6: Mehrwert-Fokus in SDN/OpenFlow Netzwerken

wie das Forwarding steuert.

Die OpenFlow Control Plane wird von einem zentralen Controller realisiert, der die OpenFlow-fähigen Switches und Router –

sowohl physische als auch virtuelle (im Hypervisor) über das OpenFlow Protokoll mit einer gesicherten Verbindung steuert. Eine Architektur-Übersicht zeigt Abbildung 2.1. Ein OpenFlow-fähiger Switch benötigt

Werden SDN und OpenFlow herkömmliche Netzwerke verdrängen?

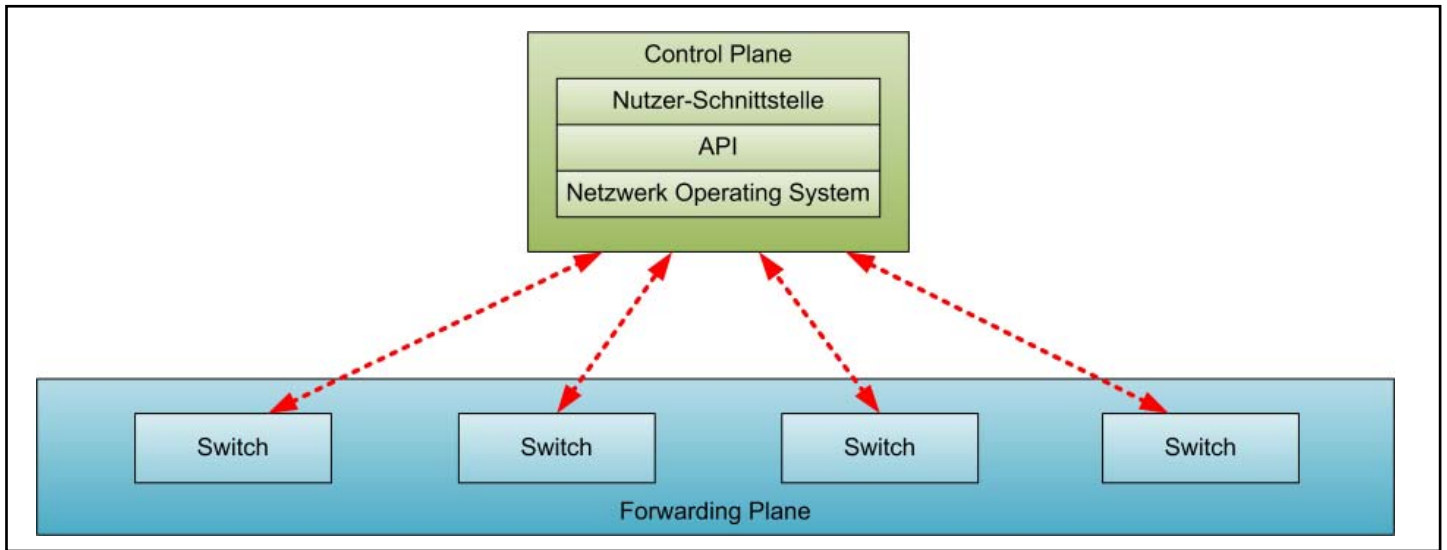


Abbildung 2.1: OpenFlow Architektur

seinerseits eine (gesicherte) Verbindung zum Controller, Flow Tabellen und Gruppentabellen für die Paketbearbeitung und das OpenFlow Protokoll zur Kommunikation mit dem Controller. Die Hauptkomponenten eines OpenFlow Switches zeigt Abbildung 2.2.

Dabei ist nicht davon auszugehen, dass mit der Implementierung von OpenFlow jegliche traditionelle Netzwerk-Technologie (wie RST, LACP, OSPF, VRRP) beseitigt und durch betreiberspezifische Programmierung ersetzt wird – dies hieße das Rad neu zu erfinden. Vielmehr ist die Sichtweise die, dass OpenFlow am Netzwerk Edge ansetzt (vSwitch im Hypervisor oder Access Switch / ToR Switch) und im Core die etablierten Standard-Layer2/3 Proto-

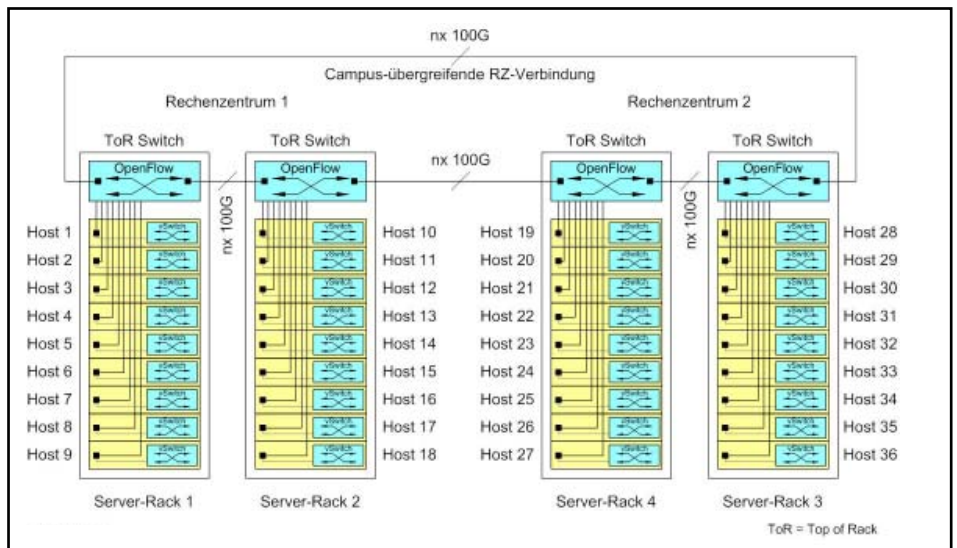


Abbildung 2.3: Einsatz von OpenFlow am Netzwerk Edge im Hypervisor

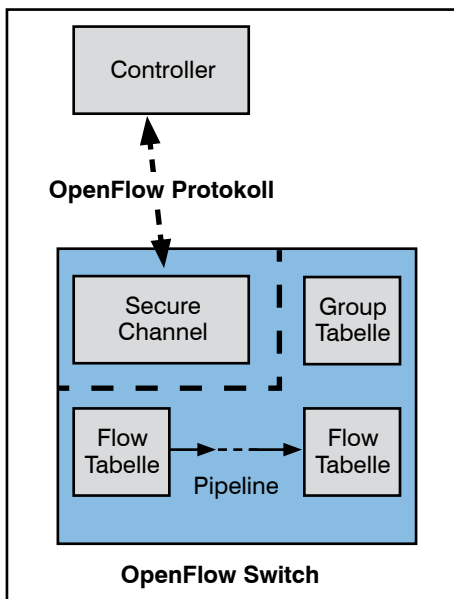


Abbildung 2.2: Hauptkomponenten eines OpenFlow Switches

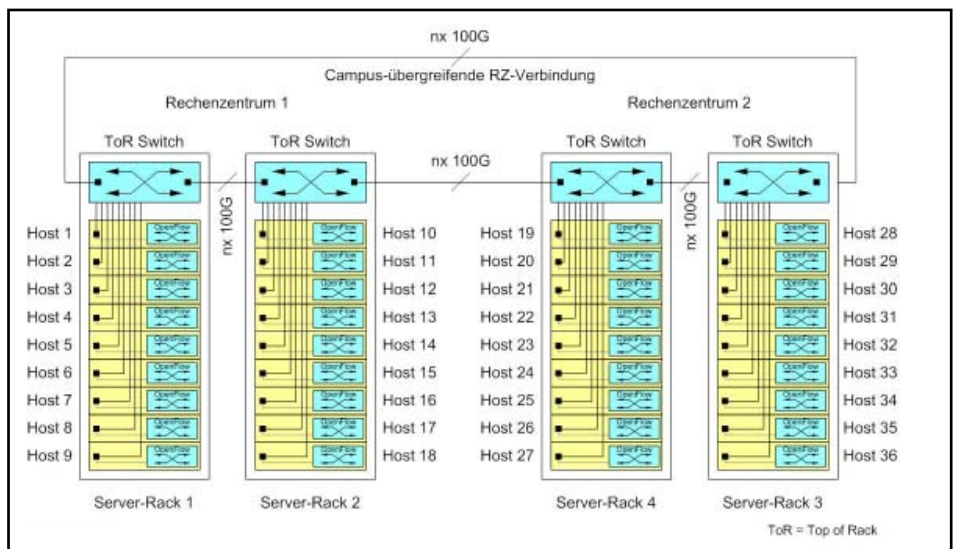


Abbildung 2.4: Einsatz von OpenFlow am Netzwerk Edge im ToR Switch

Werden SDN und OpenFlow herkömmliche Netzwerke verdrängen?

kolle weiterlaufen, die ja unter OpenFlow größtenteils noch nicht "nachspezifiziert" wurden (siehe Abbildung 2.3 und Abbildung 2.4).

Es ist natürlich auch nicht von einem einzigen zentralen Controller auszugehen, der ein großer, dicker Single Point of Failure ist. Reale Produkte implementieren mindestens einen redundanten Controller oder aber vernetzte redundante Controller-Verbunde, gegebenenfalls geo-vernetzte geo-redundante Controller-Verbunde. An dieser Stelle kommt natürlich die Frage auf: Wie verteilt darf es denn für die Controller werden? Im Extremfall hätten wir einen Controller je Switch – und wären wieder bei der heutigen Architektur gelandet ...

2.2 OpenFlow: Protokoll und Arbeitsweise

OpenFlow nutzt zur Steuerung das Konzept, dass der Netzwerkverkehr auf Basis vordefinierter Regeln identifiziert und klassifiziert wird. Diese Regeln können statisch oder dynamisch vom OpenFlow Controller programmiert werden. So wird in den Switches ein Aktions-Regelwerk implementiert, welches ihre Forwarding Tabelle (Flow Tabelle) so beeinflusst, dass der gewünschte Verkehrsfluss entsteht. Zusätzlich lässt sich über das Regelwerk die Erfassung von Statistiken programmieren, die eine Überwachung des Verkehrsverhaltens ermöglichen. Über das Regelwerk ermöglicht OpenFlow dem Betreiber, die Paketweiterleitung auf der Basis bestimmter Parameter wie Verkehrsmuster, Anwendungen oder auch Cloud Ressourcen zu spezifizieren. Damit können Design- und Betriebs-Ziele umgesetzt

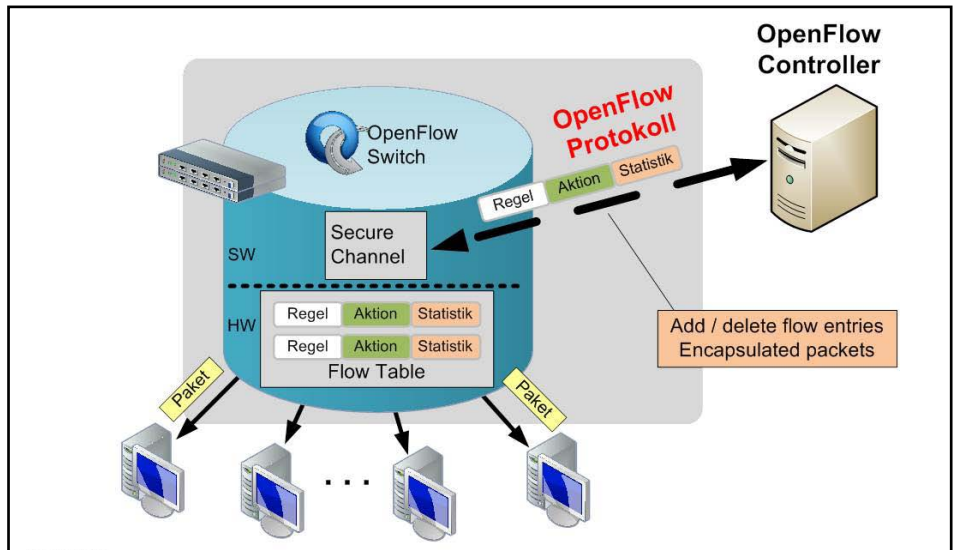


Abbildung 2.5: Zusammenspiel zwischen Controller, OpenFlow Switch und Paket Forwarding

werden wie

- Priorisierung
- flexibles Load Balancing (nicht nur auf Basis von IP oder MAC Adressen)
- NAC
- Quarantäne

Der Controller handhabt und steuert Forwarding und Statistik, indem er entsprechende Einträge in die Forwarding Tabellen (Flow Tables) der Switches einfügt, ändert oder löscht. Hierfür nutzt er eine gesicherte Verbindung (typischerweise TLS, kann aber auch TCP sein!) und die im OpenFlow Protokoll spezifizierten Aktionen. Ein Übersichts-Schema zeigt Abbildung 2.5.

Ein OpenFlow Switch hat für die Weiterleitung die zuvor genannten Flow Tabellen und Gruppentabellen. Anhand dieser Tabellen führt der Switch Paket Lookups und auf der Basis der Lookup-Ergebnisse das Forwarding durch. Die Tabellen haben so genannte Flow Einträge (Entries) Diese bestehen aus Match Feldern, Statistik-Zählern und Aktions-Sets (Instructions) für die Paketbearbeitung, Paketweiterleitung (Forwarding) und Statistik-Erfassung. Der Switch führt die Paketweiterleitung zu den Endsystemen oder anderen Switches entsprechend seines Regelwerks durch.

Die Controller-initiierten Befehle und Konfigurationen werden im Switch in die jeweils proprietären Operating System-Befehle übersetzt (proprietäres Processing), danach aktiviert und ausgeführt. Insofern kann OpenFlow mit dem Instruktionen-Set einer CPU verglichen werden: Es spezifiziert Dienst-Primitive, die eine externe Anwendung flexibel kombinieren und so nutzen kann, um das Weiterleitungs-Verhalten, sprich die Forwarding / Data Plane der Netzkomponenten zu programmieren. Das in Abbildung 2.6 gezeigte Regelwerk gibt zum Beispiel vor, dass alle Pakete mit der MAC Destination Adresse 10:20:* an Port 1 sowie alle Pakete mit der IP Destination 5.6.7.8 an Port 2 statistisch erfasst werden, alle Pakete mit TCP Destination Port 25 verworfen werden, alle Pakete mit der IP Destination 192.* an das lokale Processing gegeben werden und alle sonstigen, d.h. unbekanntenen Pakete an den Controller weitergeleitet werden, der in diesem Fall eine neue Regel erstellen kann.

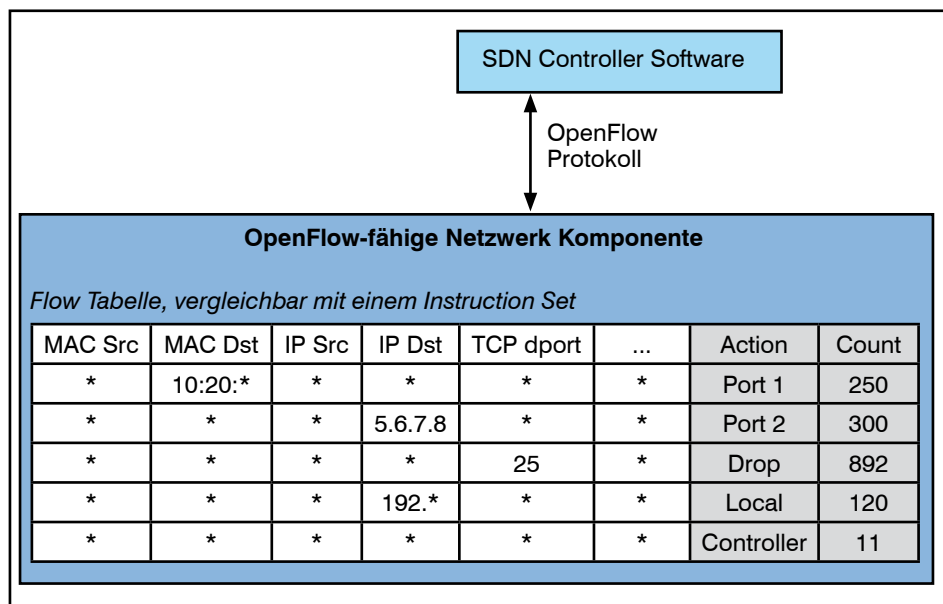


Abbildung 2.6: Beispiel einer Flow Tabelle

Empfängt ein Switch ein Paket, so prüft er, ob es einen Match mit einem Flow Eintrag oder einer Abfolge von Flow-Einträ-

Werden SDN und OpenFlow herkömmliche Netzwerke verdrängen?

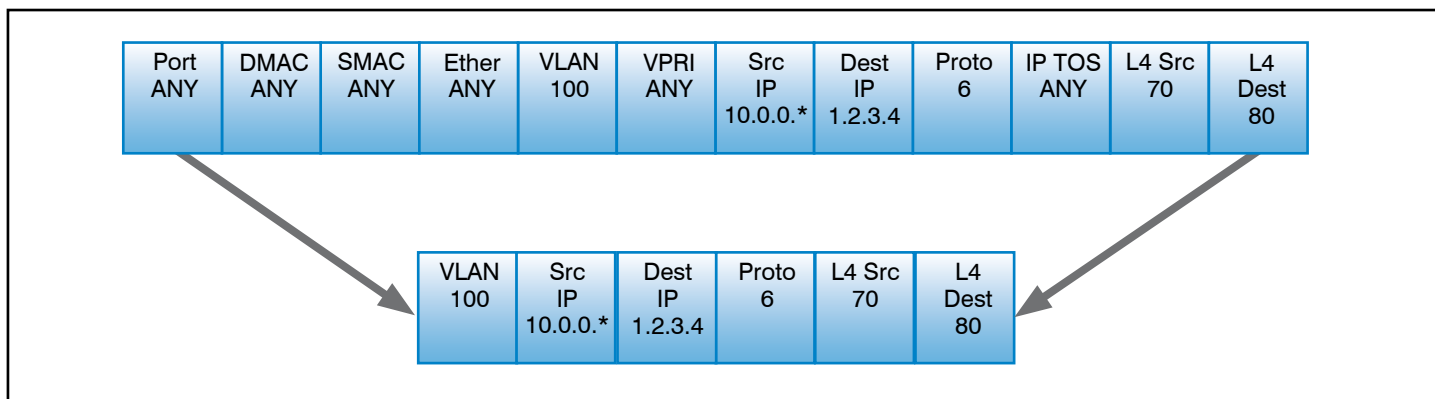


Abbildung 2.7: Beispiel für die Paket-Klassifizierung eines Flow Eintrags

gen gibt. Im Beispiel der Abbildung 2.7 definiert der gezeigte Flow Eintrag einen Match für alle Pakete mit VLAN Tag 100, IP Destination 1.2.3.4 in Kombination mit allen IP Source Adressen 10.0.0.*, Protokoll-Nummer 6, TCP/UDP Quell-Port 70 und TCP/UDP Ziel-Port 80 (HTTP). In diesem Fall bearbeitet er das Paket entsprechend. (siehe auch Abbildung 2.8)

Die Weiterleitung des Paketes erfolgt an einen physischen Port (Hardware Switch), einen virtuellen Port (Hypervisor), einen "logischen Port" oder einen "reservierten Port". Reservierte Ports sind in der OpenFlow Spezifikation definiert und repräsentieren zum Beispiel

- Weiterleitung an den Controller
- Fluten (Broadcast, Multicast)
- Nutzung von non-OpenFlow Paketbearbeitung ("normal processing", "local")

Logische Ports können "Standard-Funktionen" nachbilden beziehungsweise diese über das Switch Operating System nutzen, wie

- Link Aggregation
- Tunnelbildung
- Loopback Interface

Bleibt das Paket ohne Match, so kann die Flow Tabelle als weitere Bearbeitung vorgeben, es zum Controller weiterzuleiten, z.B. bei unbekanntem Paket (d.h. falls der Switch gar nicht weiter weiß). Eine Flow Tabelle kann jedoch auch spezifizieren, dass ein Paket ohne Match verworfen oder an eine andere Flow Tabelle weitergereicht wird. Für die Weiterleitung zum Controller gibt es vielfach einen "Default" Flow der Art "...und ansonsten leite das Paket zum Controller" am Ende der Pipeline.

Mit den ersten Praxiserfahrungen haben die Entwickler gelernt, dass eine einzige sequenzielle Flow Tabelle sehr schnell riesengroß und unhandlich wird. Daher wurde die Flow Tabelle sehr schnell auf meh-

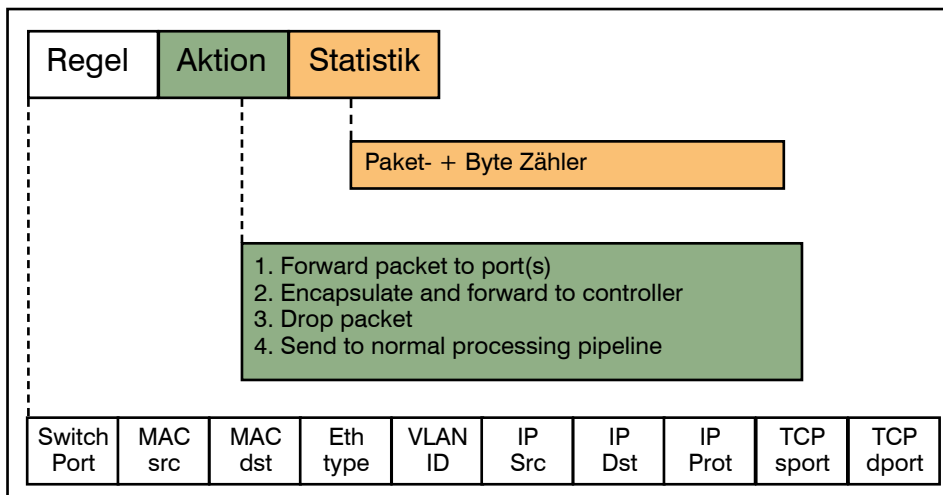


Abbildung 2.8: OpenFlow Tabellen-Eintrag und mögliche Aktionen

rere Flow Tabellen in Kombination mit einem Pipeline-Konzept erweitert. Hierbei wird eine Abfolge von Matches auf Flow Einträge programmiert, es erfolgt ein so genanntes Pipeline Processing (siehe Abbildung 2.9): Ein erster Match verweist auf eine weitere Flow Tabelle, ein dortiger Match auf eine dritte Flow Tabelle und so fort, bis das Ende des Regelwerk-Programms erreicht ist. Mit dem Pipeline-Konzept lassen sich schon recht ausgefeilte Weiterleitungs-Funktionen als umfangreiches, verzweigtes Regelwerk flexibel und tabellen-optimiert programmieren, wie Abbildung 2.10 zeigt. Jede Flow Tabelle in der Pipeline ist reihenfolge-sensibel, das heißt, der erste Eintrag mit einem Match auf das Paket führt zur Ausführung des für diesen Eintrag definierten Instruktionssets (Aktions-Set). Eine Aktion kann nicht nur die Weiterleitung an einen Port oder die nächste Flow Tabelle der Pipeline sein, sondern auch eine Änderung des Paketes beinhalten (Einfügen oder Ausfügen eines VLAN-Tag, MPLS-Label, Setzen / Löschen eines Prioritäts-Wertes auf MAC- oder IP-Ebene etc.).

Die Gruppentabellen dienen dazu, kom-

plexere Funktionen beziehungsweise Aktionen zu spezifizieren: Fluten, Multipath, Next Hop, Failover, Link Aggregation oder ähnliches. In der OpenFlow Spezifikation sind einige Gruppentypen vordefiniert:

- All (mandatory): Fluten, für Broadcast und Multicast
- Select (optional): Auswahl einer von mehreren Alternativen, typischerweise per Hash oder Round Robin, z.B. für Link Aggregation, Load Balancing
- Indirect (mandatory): eine spezielle vordefinierte komplexere Funktion, z.B. Next Hop IP Forwarding
- Fast Failover (optional): Portgruppe, in der jeder Port auf "up and running" überwacht wird. Die Weiterleitung erfolgt an den ersten funktionierenden Port der Gruppe. Dies ermöglicht eine schnelle Fehlerumschaltung, ohne eine neue Regel vom Controller erfragen zu müssen.

Mit OpenFlow sollen auf die oben beschriebene Weise "de facto standardisierte" Switches und ein "de facto standardisiertes" Netzwerk entstehen. Sounds

Werden SDN und OpenFlow herkömmliche Netzwerke verdrängen?

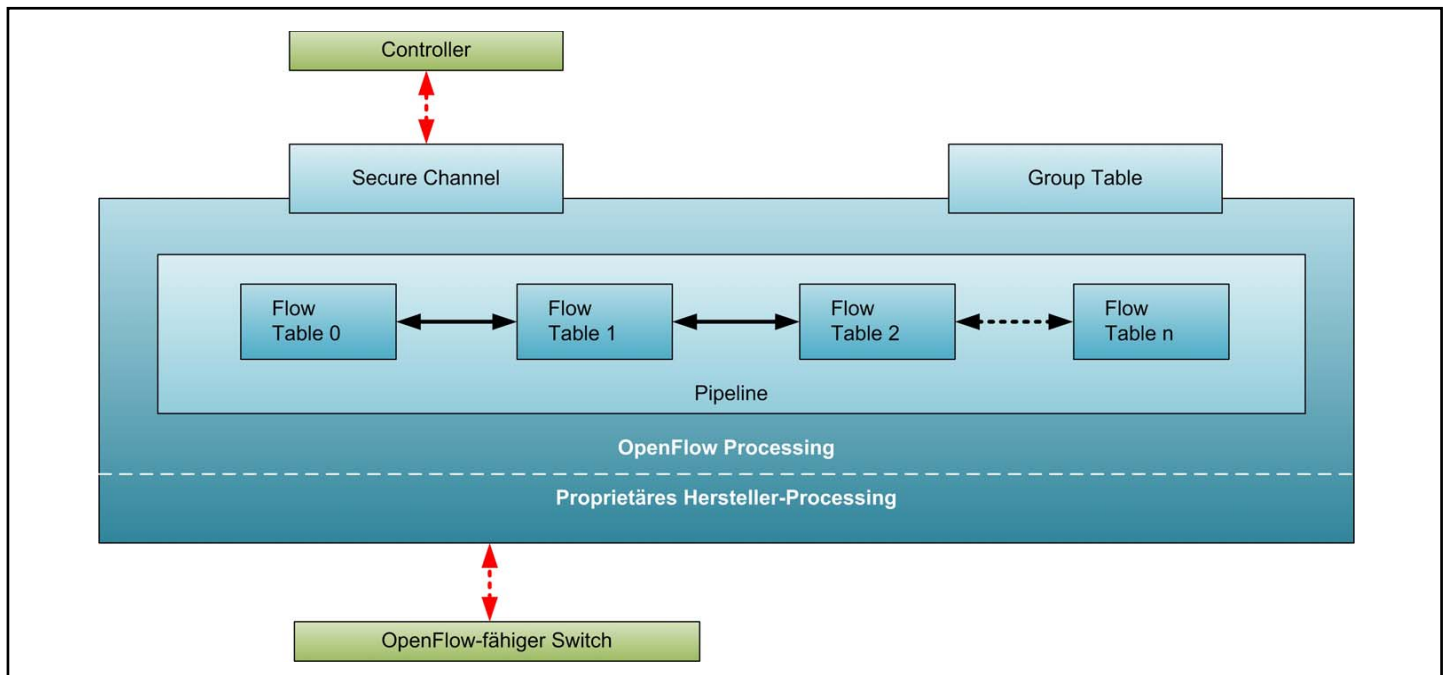


Abbildung 2.9: OpenFlow Prozessmodell mit Pipeline

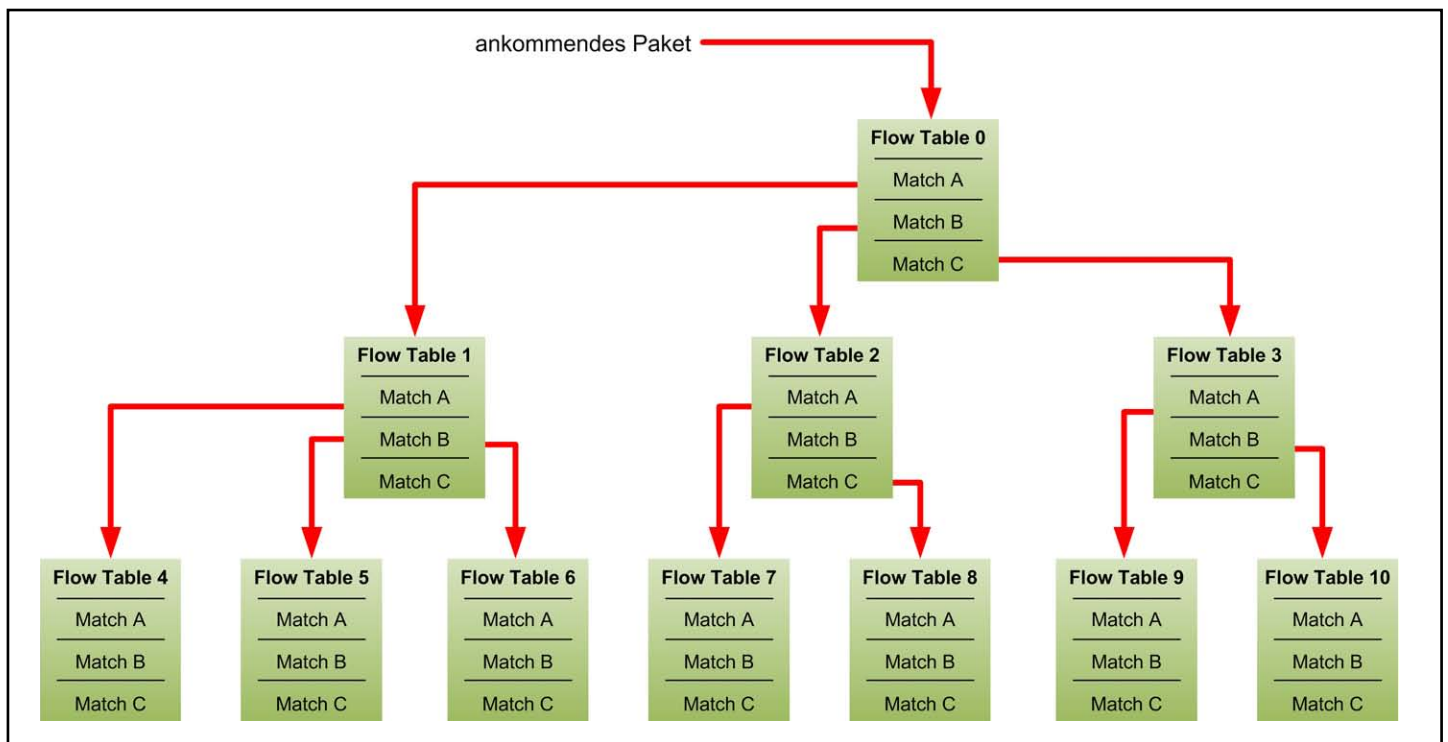


Abbildung 2.10: OpenFlow Pipeline Processing

strange? Denken Sie zurück an die Zeiten von proprietärem HP, IBM und Sun Unix und an die fetten Margen, die damit verdient wurden. Und dann kamen Linux und Microsoft / x86. Heute haben die Big Network IncuAbbildung 2.2mbents fette Margen für ihre 500-Feature-Switches ...

Damit liegen gleichermaßen ein Vorteil und ein Nachteil auf der Hand: OpenFlow wird

zumindest mittelfristig im Vergleich mit etablierten Portfolio-Lösungen eher ein Low Price Low Function Netzwerk sein.

Der Controller stellt für die angestrebten Umgebungen mit Mega-Skalierbarkeit einen potenziellen Bottleneck dar. Wie schnell tatsächlich hochperformante Controller entwickelt werden, bleibt abzuwarten.

Die Marktakzeptanz bei den Netzbetreibern wird stark von der erreichbaren Funktionalität, den Management-Möglichkeiten und der Beherrschbarkeit der Gesamtlösung abhängen.

Eine Anmerkung sei hier erlaubt: Da das komplette Weiterleitungs-Regelwerk frei programmierbar ist, muss der Network Operator schon ganz genau wissen, was

Werden SDN und OpenFlow herkömmliche Netzwerke verdrängen?

er da so treibt... Nach unserer Erfahrung ist das Fehlerpotenzial beim Einsatz von getesteten und etablierten Standardverfahren wesentlich geringer.

Im nächsten Teil lesen Sie:

- Overlay Technologien
- Versions-Unterschiede
- Zielsetzungen von OpenFlow
- Weiterentwicklung von OpenFlow zu OpenFlow Fabrics
- Probleme mit OpenFlow
- Einsatzszenarien und Hersteller-Konzepte mit OpenFlow
- Alternativen zu OpenFlow
- Fazit: Ist OpenFlow eine Revolution, Evolution oder Hype?

Abkürzungen

ACL	Access Control List(e)
ALTO	Application Layer Traffic Optimization
API	Application Programming Interface
AS	Autonome Systeme
ASIC	Application Specific Integrated Circuit
BGP	Border Gateway Protocol
CPU	Central Processing Unit
HA	Home Adresse
HTTP	Hyper Text Transfer Protocol
ID	Identifikator

IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPsec	Internet Protocol Security
L2/L3	Layer-2/ Layer-3
LACP	Link Aggregation Control Protocol
LISP	List Processing
MAC	Media Access Control
MPLS	Multi Protocol Label Switching
NAC	Network Access Control
NAT	Network Address Translation
Netconf	Network Configuration
NVGRE	Network Virtualization using Generic Routing Encapsulation
OEM	Open Equipment Manufacturer
ONF	Open Networking Foundation
OSPF	Open Shortest Path First
PCE	Path Computation Element
QoS	Quality of Service
RST	Rapid Spanning Tree
SDK	Software Development Kit
SDN	Software-Defined Networking
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
TLS	Transport Layer Security
ToR	Top-of-Rack
UDP	User Datagram Protocol

VLAN	Virtual Local Area Network
VM	Virtual Machine
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
VRPP	Virtual Router Redundancy Protocol
vSwitch	virtueller Switch
VXLAN	Virtual Extensible VLAN

Links

- www.openflow.org
- www.opennetworking.org
- www.aristanetworks.com
- www.nicira.com
- www.openflow.stanford.edu/display/OCS/Flowvisor

Literatur

- Networkcomputing: OpenFlow and Network Value, Juni 2011
- ONF: Software-defined Networking: The New Norm for Networks, April 2012
- OpenFlowSwitch.org: FlowVisor: A Network Virtualization Layer, Oktober 2009
- Nicira: Network Virtualization Platform, 2012
- ONF: OpenFlow Switch Specification, April 2012, Version 1.3.0

Kongress

**ComConsult Rechenzentrum Infrastruktur-Redesign Forum 2012
05.11. - 08.11.12 in Köln**

Unsere Rechenzentren befinden sich in einer der größten Redesign-Phasen der letzten 20 Jahre. Nahezu alle Gestaltungs-Bausteine von den Servern, Speicher-Technologien, Netzwerken bis hin zu den Applikations-Architekturen sind im Umbruch. Gleichzeitig entstehen durch eine Explosion mobiler Teilnehmer auf der einen und durch Cloud-Technologien auf der anderen Seite völlig neue Rahmenbedingungen.

- RZ-Architekturen und Infrastrukturen: wohin geht der Weg?
- Sicherheit in einer immer komplexeren RZ-Umgebung
- Web-Architekturen im RZ
- Netzwerk-Infrastrukturen: die Achillesferse unter Druck
- Mobile Endgeräte und BYOD
- Virtualisierung
- Speicher-Technologien

Wir bieten Ihnen bei der Buchung dieses Kongresses drei Reports zum vergünstigten Teilnehmer-Preis an:

- „RZ Netzwerk-Infrastruktur Redesign“,
- „Neue Netzwerk-Architekturen für das Rechenzentrum: TRILL kontra SPB (802.1aq)“ und
- „Moderne WAN-Technologien“ oder die komplette "RZ-Kollektion"

Moderation: Dr. Behrooz Moayeri, Dr. Jürgen Suppan
Kosten: € 2.490,- netto (4 Tage) - € 2.090,- netto (3 Tage) - € 990,- netto (Intensiv-Tag)



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

Standpunkt Sicherheit

Zertifikatsinsuffizienz: Wenn Informationssicherheit zu kompliziert wird

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.

Zertifikatsbasierte Authentisierung ist an allen Ecken und Enden der IT zu finden. Beim Click auf eine HTTPS-Seite authentisiert sich der Web-Server beim Browser. Nutzer oder Geräte wie PCs, IP-Telefone, Drucker authentisieren sich an einem Server, am Netzbetriebssystem oder an einem Netzzugangspunkt. Zertifikate sind standardisiert und seit Jahren ein bewährtes und sicheres Authentisierungsinstrument, das man offensichtlich mit akzeptablem Aufwand in den Griff bekommt (sonst hätte es sich ja nicht durchgesetzt).

Zumindest letzteres ist eine dreiste Über-treibung.

Zunächst ist es in der Vergangenheit durchaus vorgekommen, dass bei einem Einbruch in einer (Stamm-)Zertifizierungsstelle Zertifikate (natürlich inklusive des privaten geheimen Schlüssels) in die falschen Hände gelangt sind. Nun ja, das ist wie mit einem Passwort: Wer es kennt, ist drin, zumindest solange das Passwort gültig bzw. der zugehörige Account nicht gesperrt ist. Daher sollten solche Ereignisse (abgesehen von Schwächen bei der Absicherung von kritischen Infrastrukturen wie Zertifizierungsstellen) nicht überbewertet werden.

Spannender war da schon ein Vorfall von Anfang November 2009, bei dem Sicherheitsexperten eine Schwachstelle in der TLS¹-Spezifikation selbst gefunden hatten². Die Funktion der Renegotiation in TLS (RFC 5246, inkl. SSL v3 und früher) konnte durch verschiedene Angriffe vom Typ Man-in-the-Middle (MITM) missbräuchlich ausgenutzt werden. Der MITM konnte dabei authentisiert durch einen legitimen Nutzer (das Opfer der MITM-Attacke) und geschützt durch TLS eine beliebige HTTP-Transaktion seiner Wahl ausführen. Fehler, die sich für Angriffe ausnutzen lassen, kommen nun mal



nicht nur bei der Implementierung vor, sondern schon bei der Protokollspezifikation. Mit hektischem Patchen und einer Ergänzung des Standards (siehe RFC 5746) lässt sich so etwas natürlich wieder reparieren.

So interessant diese Schwachstelle war, es sind nicht solche Aspekte, an denen die zertifikatsbasierte Authentisierung krankt: **Wir leiden unter mangelhaftem und uneinheitlichem Zertifikatsmanagement.** Dies betrifft unter anderem

das automatisierte Ausrollen von Zertifikaten, die Überprüfung von Zertifikaten und den Umgang mit Sperrlisten.

Auch wenn beispielsweise Microsoft Certificate Services hier wunderbar funktionieren mögen (im Detail sind natürlich auch hier manchmal Klimmzüge nötig), es bleibt zu einem gewissen Grad eine Lösung für reine Windows-Umgebungen. Was ist mit Linux, MacOS, iOS, Android und anderen Betriebssystemen? Als Standard für das Zertifikatsmanagement wird hier schnell der Ruf nach dem Simple Certificate Enrollment Protocol (SCEP) laut. Leider entpuppt sich der vermeintliche allgemein etablierte Standard SCEP immer noch als Internet Draft. Nun gibt es mit dem Certificate Management Protocol (CMP) gemäß RFC 4210 auch einen Standard, dessen Komplexität ist allerdings nicht zu unterschätzen.

Daher ist es nicht überraschend, dass sich manche Hersteller mit dem Zertifikatsmanagement schwer tun und es sogar vorkommt, dass ein Hersteller zwar eine zertifikatsbasierte Authentisierung implementiert, er sich jedoch über ein automatisiertes Zertifikatsmanagement keine (sinnvollen) Gedanken macht. Was

Seminar

Bring Your Own Device - Sichere Integration von mobilen Privatgeräten in die IT-Infrastruktur 30.10.12 in Stuttgart

Dieses Seminar analysiert die Gefährdungen und beschreibt die Wege zur sicheren Anbindung privater und fremder mobiler Endgeräte. Verfügbare technische Lösungen werden vorgestellt und Strategien für den Betrieb dieser Lösungen erarbeitet.

Referenten: Dr. Simon Hoff, Dominik Zöller
Preis: € 990,- netto



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

¹TLS = Transport Layer Security

²Siehe Marsh Ray, Steve Dispensa, "Renegotiating TLS", http://extendedsubset.com/Renegotiating_TLS.pdf

Zertifikatsinsuffizienz: Wenn Informationssicherheit zu kompliziert wird

tut man als Nutzer hier oft notgedrungen? Man verwendet ein Zertifikat für alle Geräte mit sehr, sehr langer Gültigkeit, d.h. man verletzt die Kernanforderungen einer Authentisierung nach individuellen und regelmäßig gewechselten Berechtigungsnachweisen. Das ist leider häufiger der Fall als es einem lieb ist. Ohne konkrete Hersteller zu nennen, man wird bei IP-Telefonen, Netzwerkdruckern, Thin Clients und allen möglichen Spezialgeräten fündig, die über LAN oder WLAN angebunden werden.

Selbst wenn alle relevanten IT-Systeme eine zertifikatsbasierte Authentisierung mit automatisiertem Zertifikatsmanagement zufriedenstellend unterstützten, müssten wir trotzdem damit rechnen, dass parallel mit unterschiedlichsten und weitgehend inkompatiblen Implementierungen eines Zertifikatsmanagements zu arbeiten wäre. Das erhöht zumindest den Betriebsaufwand signifikant.

Natürlich gibt es noch eine Vielzahl weiterer immer wieder auftauchender Probleme, etwa der nachlässige Umgang mit Zertifikaten (z.B. der Verzicht auf eine Prüfung eines Serverzertifikats durch den Client, was sofort zu MITM einlädt) und nachlässige Implementierungen der Hersteller.

Ein sehr schönes aktuelles Beispiel liefert Apple iOS 6. Hier hat Apple eine höchst gefährliche Nachlässigkeit beim Umgang mit Zertifikaten beseitigt, die bereits seit Januar 2010 bekannt ist³. Diese Schwachstelle ist so gravierend, dass bei Geräten vor iOS 6 die Informationssicherheit für den Enterprise-Einsatz streng genommen beide Augen zudrücken muss. Interessanterweise ist die Schwachstelle eng mit dem Apple Mobile Device Management (MDM) verbunden. Wenn im Rahmen von MDM geänderte Konfigurationsparameter auf ein mobiles Endgerät eingespielt werden sollen, ist es natürlich entscheidend, dass das Endgerät prüfen kann, ob die Konfigurationsdatei wirklich von einer vertrauenswürdigen und berechtigten Partei stammt. Es ist naheliegend, hier mit einer zertifikatsbasierten Signatur zu arbeiten. Nur sollte der Kreis der Zertifizierungsstellen, deren Zertifikaten man hier traut, sehr kritisch bedacht werden, und es sollte natürlich genau geprüft werden, ob der Verwendungszweck, für den ein Zertifikat ausgestellt wurde, auch passt (und das Zertifikat nicht beispielsweise für die Signatur und Verschlüsselung von E-Mails gedacht ist). Ist dies nicht der Fall (wie vor iOS 6), darf man sich nicht wundern, wenn einem iOS-Endgerät eine schadenstiftende Konfiguration untergejubelt

werden kann, ohne dass der Zertifikatsschutz hier Alarm schlägt.

Insgesamt muss festgestellt werden, dass eine zertifikatsbasierte Authentisierung offensichtlich nicht nur für viele Nutzer, sondern auch für Hersteller zu kompliziert ist.

Ist nun das Prinzip einer zertifikatsbasierten Authentisierung in Frage zu stellen?

Nein, es ist sogar das Gegenteil der Fall. Die theoretischen, mathematischen Grundlagen behalten ihre Gültigkeit und sie sind gut. Wir müssen also an organisatorischen Aspekten arbeiten. Warum fehlen uns also z.B. etablierte Standards für die Zertifikatsverwaltung, die auch wirklich systemübergreifend breite Anwendung finden?

Vielleicht, weil wir als Nutzer hier nicht genau genug unsere Anforderungen in Ausschreibungen formuliert und entsprechend Druck ausgeübt haben, denn das ist eines der wenigen Argumente, die bei Herstellern wirklich ankommen. Außerdem müssen wir als Nutzer Kompetenz aufbauen und die Konzepte der zertifikatsbasierten Authentisierung besser verstehen, denn wir müssen den Umgang mit den verschiedenen Implementierungen bewerten und planen können und die Nachlässigkeiten von Herstellern in den Griff bekommen. Nur passt so etwas nicht zum klassischen Outsourcing-Gedanken vieler Entscheider, bei dem die IT letztendlich wie Strom aus der Steckdose kommt und wir uns um die Komplexität keine Sorgen mehr machen müssen.

Seminar

Netzzugangskontrolle: Technik, Planung und Betrieb 26.11. - 28.11.12 in Bonn

Dieses 3-tägige Seminar vermittelt den aktuellen Stand der Technik der Netzzugangskontrolle (Network Access Control, NAC) und zeigt die Möglichkeiten aber auch die Grenzen für den Aufbau einer professionellen NAC-Lösung auf. Schwerpunkt bildet die detaillierte Betrachtung der Standards IEEE 802.1X, EAP und RADIUS. Dabei wird mit IEEE 802.1X in der Fassung von 2010 und mit IEEE 802.1AE (MACsec) auch auf neueste Entwicklungen eingegangen.

In diesem Seminar lernen Sie u.a.

- welchen Bedrohungen Ihr LAN durch die Kopplung mit mobilen Endgeräten und Fremdgeräten ausgesetzt ist
- welche Alternativen es zur Zugangskontrolle, zur Trennung von Benutzergruppen und zum Aufbau mandantenfähiger LANs gibt
- die Konzepte kennen, die für eine port-basierte Zugangskontrolle zum LAN relevant sind
- wie der Standard IEEE 802.1X arbeitet
- welche Rolle EAP dabei spielt
- welche Authentisierungsmethoden über EAP für welches Sicherheitsniveau angemessen sind
- welche Rolle der RADIUS-Server dabei spielt
- wie unterschiedliche RADIUS-Server für NAC konfiguriert werden
- wie eine Infrastruktur für IEEE 802.1X in der Praxis umgesetzt werden kann und welche Probleme dabei gelöst werden müssen
- wie ein Gastzugang realisiert werden kann
- wie ein Monitoring und Trouble Shooting einer NAC-Lösung durchgeführt wird und welche typischen Fehlersituationen in der Praxis auftreten und wie mit ihnen umgegangen werden kann
- wo aktuell die Grenzen von IEEE 802.1X liegen
- welche Änderungen mit Version IEEE 802.1X-2010 des Standards einhergehen, welche Rolle IEEE 802.1AE (MACsec) dabei spielt und wie neben Cisco TrustSec die Produktsituation aktuell aussieht

Referenten: Dr. Simon Hoff, Dipl.-Inform. Daniel Prinzen

Preis: € 1.890,- netto



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

³Siehe <http://cryptopath.wordpress.com/2010/01/>

Aktuelles Intensiv-Seminar

Winterschule 2012 - Intensiv-Update auf den neuesten Stand der Netzwerktechnik

Die ComConsult Akademie veranstaltet vom 03.12. - 07.12.12 das Intensiv-Seminar "Winterschule 2012 - Intensiv-Update auf den neuesten Stand der Netzwerktechnik" in Aachen.

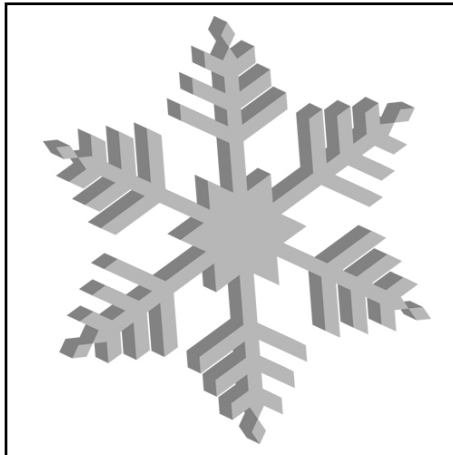
2012 wird allen Netzwerk-Verantwortlichen als ein Jahr in Erinnerung bleiben, in dem mehr technologische und strukturelle Änderungen, Neuheiten, Ideen, Verfahren und Produkte initiiert wurden als sonst in mehreren Jahren zusammen. Ausgehend von teilweise stark modifizierten Erwartungen an die Anwendungen und Vorstellungen über deren erfolgreiche Implementierung haben sich von den physikalischen Schaltkreisen bis hin zur logischen Organisation abstrakter Steuerungsmechanismen über alle Ebenen der Netzwerk-Technologien viele neue Elemente entwickelt, die die Gestalt der Unternehmensnetze dauerhaft verändern können und werden. Manches kann man sofort kaufen, anderes wird Jahrzehnte zu seiner endgültigen Materialisierung benötigen. Von diesen Änderungen werden über Kurz oder Lang alle Bereiche in Firmennetzen betroffen sein. Jede neue Idee oder Technologie wirft aber erhebliche Fragestellungen auf, die es bei Entscheidungen zu bedenken gilt.

Hier ein Überblick über die Inhalte

Unterstützung skalierender Web-Applikationen. Immer mehr klassische Anwendungen werden auf dieses Arbeitsmodell umgestellt und neue Anwendungen basieren ohnehin darauf. Was bedeutet das für die Rechenzentren? Wie stark ist der neu aufkommende Ost-West-Verkehr tatsächlich und welche Maßnahmen sollte man treffen?

Unterstützung von BOYD. Der Trend, dass Mitarbeiter ihre eigenen Endgeräte in die Unternehmen bringen und damit arbeiten möchten, ist ungebrochen. Was bedeutet das für die Implementierung der notwendigen Infrastrukturen und für Datenschutz und Datensicherheit?

Cloud Computing. Der Gedanke, benötigte Leistung von einem Fremdanbieter zu beziehen, ist verlockend. Aber, es sind auch Probleme damit verbunden. Durch Dienste wie BYOD-Unterstützung



wird das Unternehmen aber selbst zum Provider für Dienstleistungen gegenüber seinen Mitarbeitern. Kann das durch private Cloud-Strukturen bewältigt werden?

Virtualisierung. Viele Unternehmen betreiben erfolgreich Virtualisierungslösungen und freuen sich über Zusatzfunktionen wie z.B. unterbrechungsfreien Betrieb. Die Lösungen sind heute aber relativ statisch. Was passiert, wenn man dies flexibilisieren möchte und letztlich die Vision verfolgt, jedem Nutzer bzw. jeder Anwendung dynamisch Leistung via VMs zuzuordnen?

SDN, Software Defined Networking und OpenFlow. Diese konstruktiven Methoden trennen Netzwerk-Hardware und deren Steuerung voneinander und wollen letztlich die Abhängigkeit von spezifischen Hersteller-Lösungen verringern. Ganz große Anwender wie Google verwenden dies schon heute. Wie steht es aber mit der Übertragbarkeit auf kleinere, mehr konventionelle Umgebungen? Ergeben sich Vorteile und wenn ja, in welchem Zeitraum oder ist das Ganze nur ein neuer Hype?

Neue Switch-ASICs. Die in 2010 begonnene Technologiewende hin zu hoch integrierten, höchst leistungsfähigen speicherbasierten Switch-ASICs materialisiert sich jetzt in einem wahren Produkt-Tsunami und wird mit Sicherheit zu völlig neuen Produkten der Hersteller von Netzwerk-Komponenten führen. Aber es gibt unterschiedliche Grund-Typen dieser ICs. Was ist wirklich zukunfts-sicher? Viele neue ICs begnügen sich

nicht mit L2-Switching, sondern haben darüber hinaus zusätzliche Fähigkeiten auf L3 und L4. Was bedeutet das für Netze und wo liegt demnächst die Grenze zwischen physikalischen Komponenten und Netzwerk-Steuerung?

Basistechnologie. 10 Gb Ethernet ist heute der Minimal-Standard im RZ und Produkte für 40 GbE sind weithin verfügbar. Mit ihnen eng verbunden sind Techniken zur Steigerung der Zuverlässigkeit von Ethernet zum Zwecke der Integration von Speicherkommunikation und IPC. Was bedeutet das für Komponenten und Verkabelung und wann müssen wir mit 100 GbE in der Praxis rechnen?

Neue Wireless-Technologien. Nach dem jahrelangen Stillstand mit IEEE 802.11n kommen jetzt mit 11ac und 11ad gleich zwei neue Standards, die Gigabit-Leistung versprechen. Aber: halten sie das auch? Was bedeuten Gigabit-WLAN-Zellen für die Infrastruktur wie Controller, Leitungen und Switches? Mit LTE gibt es auch ein sehr leistungsfähiges neues Angebot für Mobilfunk auf der Providerseite. Lohnen sich private WLAN-Infrastrukturen angesichts LTE überhaupt noch?

Neue WAN-Technologien. Die Umstellung auf Ethernet-basierte WAN-Dienste ist zäh und im Zweifel greift man immer noch gerne auf SONET zurück, welches jetzt schon über 25 Jahre alt ist. Wird sich das durch Carrier Ethernet 2.0 und veränderte Übertragungstechnologien mit erheblicher Kanalverdichtung ändern?

Neue Strukturverfahren. Seit Jahren sprechen wir über eine Ablösung von Spanning Tree wenigstens im RZ. Die alternativen Verfahren TRILL und PLSB sind längst in der Produktreife. Aber, wie weit ist das Ganze wirklich? Kann es uns schon heute den versprochenen Nutzen bringen oder kommt vielleicht noch eine weitere Alternative auf?

Data Center Fabrics. Im letzten Jahr haben praktisch alle Komponenten-Hersteller versucht, sehr teure proprietäre Spezial-Lösungen für das RZ auf den Markt zu bringen und sind damit weitestgehend gescheitert. Was lassen sie sich als nächstes einfallen?

Winterschule 2012

VM-Kommunikation. Dynamische virtualisierte Umgebungen, die z.B. kooperierende Web-Anwendungen unterstützen, benötigen leistungsfähige VM-Kommunikation. Leider verwechseln viele immer noch IPC und I/O. Dadurch sind selbst völlig neue Vorschläge wie VEB und VEPA nicht zielführend. Cloud-

Provider benutzen eine andere Technologie und diese ist jetzt auch auf normale Umgebungen übertragbar. Wie sehen RDMA, RoCE und OFED aus und was leisten sie?

Die Winterschule 2012 der ComConsult Akademie bringt Sie auf den neuesten

Stand der Diskussionen. Erfahrene Spezialisten analysieren Technologien, Verfahren und Entwicklungen und helfen Ihnen dabei, Schlussfolgerungen für die Entwicklung der eigenen Netze zu erarbeiten. Verpassen Sie diese Gelegenheit nicht und rüsten Sie sich jetzt für aktuelle Anforderungen und Fragestellungen!

Frühbucherphase bis zum 31.10.2012

Für Besucher unserer bisherigen Seminare bzw. für die Teilnehmer am VIP-Verteiler bieten wir Ihnen exklusiv eine Vorbuchungsphase für die "Winterschule 2012 - Intensiv-Update auf den neuesten Stand der Netzwerktechnik" bis zum 31.10.2012 für eine rabattierte Teilnahmegebühr an.

Winterschule 2012 - Intensiv-Update auf den neuesten Stand der Netzwerktechnik
zum Preis bei Buchung bis 31.10.2012 von :

03.12. - 07.12.12 - 5-tägigen Veranstaltung € 2.290,-- netto

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

Fax-Antwort an ComConsult 02408/955-399

Anmeldung Winterschule 2012 - Intensiv-Update auf den neuesten Stand der Netzwerktechnik

Ich buche das Intensiv-Seminar
Winterschule 2012

vom 03.12. - 07.12.12 in Aachen
zum Preis von € 2.290,-- netto*
*gültig bis zum 31.10.2012

Bitte reservieren Sie mir ein Zimmer

vom _____ bis _____ 12

Vorname


Nachname

Firma

Telefon/Fax

Straße

PLZ, Ort

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

eMail

Unterschrift

Sonderveranstaltung

Sonderveranstaltung Wireless Networking

Die ComConsult Akademie veranstaltet vom 29.11. - 30.11.12 Sonderveranstaltung „Wireless Networking“ in Köln.

Die Sonderveranstaltung Wireless Networking greift die aktuellsten Entwicklungen im Bereich der drahtlosen Kommunikationstechnik auf. Sie ist die zentrale Veranstaltung des Jahres 2012 zur drahtlosen Kommunikation. Sie ist für jeden Entscheider, IT-Architekten, Planer und Betreiber in diesem Bereich ein absolutes Muss. Hier trifft sich die Branche.

Die Zukunft der Kommunikation mit Clients ist drahtlos, d.h. WLAN, UMTS/LTE und Co. werden das klassische Kabel für die Client-Anbindung zur Nischenlösung machen. Folgende Entwicklungen deuten darauf hin, dass wir dabei vor einem wesentlichen Umbruch stehen:

Geschäftskritische Anwendungen

- In Office, Logistik, Retail, Produktion und Automatisierungstechnik werden immer häufiger auch geschäftskritische Anwendungen drahtlos genutzt, was leistungsfähige, sichere und hoch verfügbare Wireless-Infrastrukturen erzwingt.
- Die Erwartungshaltung des Anwenders ist dabei: Maximale Mobilität ohne spürbare Leistungseinbuße im Vergleich zur kabelbasierten Anbindung.

Dies erfordert zunächst Gigabit-Leistungen auf der Luftschnittstelle. Konsequenzen sind neue drahtlose Übertragungstechniken im WLAN, die sich mit IEEE 802.11ac und IEEE 802.11ad abzeichnen sowie entsprechende Verfahren für LTE.

Das Controller-basierte WLAN-Design muss der kommenden höheren Leistung

bei der Funkübertragung gerecht werden. Hier werden wir verstärkt eine Integration von Controller-Design und Switching-Infrastruktur erleben. Neben proprietären Techniken sind insbesondere bereits erste Ansätze sichtbar ein Controller-basiertes WLAN-Design im Rahmen von Software Defined Networking (SDN), z.B. auf Basis von OpenFlow, zu realisieren.

Die Nutzung von WLAN für geschäftskritische Anwendungen bedingt in vielen Fällen auch eine angemessene Überwachung. Bei 2,4 GHz ist durch die Vielzahl unterschiedlicher sich gegenseitig beeinflussenden Übertragungstechniken insbesondere eine systemübergreifende Messtechnik sinnvoll. In diesem Zusammenhang muss auch eine Neuregulierung des 2,4-GHz-Bereichs beachtet werden, die sich mit einer Neuauflage von ETSI EN 300 328 im Juni 2012 materialisiert hat und die speziell Auswirkungen auf drahtlose Techniken in Automatisierungsbereichen hat.

Neue Endgeräte-Typen und Nutzungsformen der IT

- Die Nutzung mobiler Endgeräte wie Smartphones und Tablets in Unternehmen und Behörden steigt exponentiell. Der traditionelle PC hat immer mehr ausgedient. Insbesondere das App-Konzept in den Betriebssystemen für Smartphones und Tablets (primär iOS und Android) lässt die Grenzen zwischen einem lokalen WLAN-basierten Zugang und dem Zugang per Mobilfunk immer mehr verwischen.
- Innovation in der IT findet im Consumer-Bereich statt und damit drängen Consumer-Techniken automatisch verstärkt in die Enterprise-IT. Mit Bring Your Own De-

vice (BYOD) materialisiert sich zusätzlich der Wunsch private Endgeräte im Unternehmensnetz für Zugriff und Verarbeitung von dienstlichen Daten einzusetzen. Daneben ist es immer häufiger notwendig auch für Fremdgeräte einen drahtlosen Zugang zur Infrastruktur (z.B. für Wartungszwecke) zu schaffen. Hierbei besteht im schlimmsten Fall keinerlei Einfluss mehr auf die Konfiguration eines Endgeräts.

Damit der Zugriff von unsicheren Endgeräten auf Unternehmensdaten auf eine sichere Weise erfolgen kann müssen spezifische Konzepte umgesetzt werden, die neben Mobile Device Management (MDM), Sandboxing und Container-Apps auch Virtualisierung und Server-based Computing umfassen.

Diese Entwicklungen haben unmittelbare Konsequenzen für drahtlose Übertragungstechniken, Kommunikationsprotokolle und Netzarchitekturen, die wir in einer zweitägigen Sonderveranstaltung erörtern wollen:

- Gigabit WLAN und andere neue WLAN-Standards
- Neuregulierung der WLAN-Frequenzen bei 2,4 GHz und bei 5 GHz
- IPv6 und WLAN
- Betrieb und Trouble Shooting von WLAN
- Cisco CleanAir-Technologie, was steckt dahinter?
- Neue Entwicklungen im Controller-basierten WLAN-Design
- WLAN in der Shop Floor IT
- Konkurrenz zu WLAN durch LTE
- Anbindung von Smart Phones und Tablets an die Infrastruktur

Fax-Antwort an ComConsult 02408/955-399


Anmeldung Wireless Networking

Ich buche die Sonderveranstaltung **Wireless Networking**

vom 29.11. - 30.11.12 in Köln
zum Preis von € 1.690,- netto

Bitte reservieren Sie mir ein Zimmer

vom _____ bis _____ 12

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

Vorname _____

Nachname _____

Firma _____

Telefon/Fax _____

Straße _____

PLZ, Ort _____

eMail _____

Unterschrift _____

Programmübersicht - Sonderveranstaltung Wireless Networking

Donnerstag, den 29.11.2012

9:30 bis 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 Bring Your Own Device (BYOD) und die Konsequenzen für drahtlose Anbindungen an die IT

Dr. Franz-Joachim Kauffels, freier Unternehmensberater

10:30 bis 11:00 Uhr

Im Dschungel von IEEE 802.11

- Die Neuauflage des Standards IEEE 802.11 von 2012 - Welche Änderungen sind relevant?
- WLANs im Straßenverkehr: Wireless Access in Vehicular Environments mit IEEE 802.11p
- Rapid Roaming mit IEEE 802.11r: Mehr als ein Papiertiger?
- Mesh Networking mit IEEE 802.11s: Wird es tatsächlich in Enterprise-WLANs verwendet und wenn ja, wie?
- IEEE 802.11v: Endlich ein Standard für das WLAN-Management!

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

11:00 - 11:30 Uhr Kaffeepause

11:30 bis 12:30 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 realistisch sind
- Auswirkungen auf Ausleuchtung und WLAN-Planung bzw. WLAN-Migration
- Was leisten die verfügbaren Vorstandardprodukte 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
- Mischbetrieb von IEEE 802.11n/ac/ad
- Langfristige Konsequenzen für das kabelbasierte LAN und die Tertiärverkabelung

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

12:30 bis 13:15 Uhr

Neuregulierung der WLAN-Frequenzen

- Die Regulierung der 5-GHz-Frequenzen in Europa, ständiger Veränderung unterworfen
- DFS und TPC, was steckt dahinter?
- DFS, DFS-2, DFS-3, welche Techniken verbergen sich hinter diesen Begriffen?
- Neuauflage von ETSI EN 300 328 im Juni 2012: 2,4 GHz ist doch etabliert, wozu eine Neuauflage?

- Listen before Talk für 2,4 GHz und die Folgen für Funktechniken bei 2,4 GHz in der Automatisierung
- Wie reagieren die Hersteller?
- Was muss der Anwender beachten?

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

13:15 bis 14:15 Uhr Mittagspause

14:15 bis 15:15 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

15:15 bis 15:45 Uhr Kaffeepause

15:45 bis 16:30 Uhr

Industrietaugliches WLAN mit Multifrequenz, Redundanz und SeamlessRoaming

- Anwendungsbereiche für WLANs in der Industrie
- Spezielle Anforderungen in industriellen Umgebungen
- Frequenzbänder und die besondere Bedeutung des 5-GHz-Bereichs
- Welche Rolle spielt hier der zukünftige Standard 802.11ac
- Roaming im industriellen Umfeld
- Warum IT-Sicherheit für Industrial WLAN leichter gesagt als getan ist
- Integration in Industrial Ethernet
- PROFINET und Co.: Umgang mit Echtzeitanforderungen
- Einsatz von speziellen Antennen, zB Leckwellenleitern
- Beispiele aus der Industrie

Heinrich Merz, ads-tec GmbH

16:30 bis 17:00 Uhr

IPv6 und WLAN

- WLAN ist doch eine Layer-2-Technik, was kümmert es IPv6?
- Controller-based-WLAN und IPv6
- Was muss bei der Produktauswahl beachtet werden?

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

17:00 bis 17:30 Uhr

Hersteller-Vortrag

Ab 18:00 Uhr Get Together

Freitag, den 30.11.2012

9:00 bis 9:45 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

9:45 bis 10:30 Uhr

Cisco CleanAir-Technologie, was steckt dahinter?

- Herausforderung systemübergreifende Überwachung der Luftschnittstelle
- Der Trick: Einbau eines Spektrumanalysators in den Access Point
- Management der Luftschnittstelle im Cisco WLAN
- Erkennung von Fremdsystemen bei 2,4 GHz: Möglichkeiten und Grenzen
- Mehrwert durch Cisco CleanAir für die WLAN-Kommunikation bei 2,4 GHz und 5 GHz • Projektbeispiele

Christian Gauer, Cisco Systems GmbH

10:30 bis 11:00 Uhr Kaffeepause

11:00 bis 11:45 Uhr

WLAN-Sicherheit 2012

- Ist WPA2 Enterprise mit IEEE 802.1X und CCMP (AES) noch sicher?
- Fallstricke bei PEAP mit EAP-MSCHAPv2: Was kann man in Theorie und Praxis (CloudCracker) 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

11:45 bis 13:15 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

Dr. Franz-Joachim Kauffels, freier Unternehmensberater

13:15 bis 14:15 Uhr Mittagspause

14:15 bis 15:15 Uhr

Anbindung von Smart Phones und Tablets an die Infrastruktur

- 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

15:30 Uhr Ende der Veranstaltung

Zweitthema

UCC gehört ins Internet!

Fortsetzung von Seite 1



Dominik Zöller ist seit 2006 Berater bei der ComConsult Beratung und Planung. Während seines Studiums konzentrierte er sich bereits auf moderne Kommunikationsnetze und Betriebssysteme. Zu seinen Spezialgebieten gehören jetzt u.a. die Konzeption und Ausschreibung professioneller Unified-Communications- und Kollaborations-Systeme sowie Microsoft-Lösungen.

Bald drehen sich die Überlegungen um viele verschiedene Kommunikationskanäle, ihre Integration in das Arbeitsumfeld der Anwender und die hieraus zu generierenden Mehrwerte. Das TK-Projekt wird zum UCC-Projekt. Aus Infrastruktur-Überlegungen werden Prozessbetrachtungen.

Denn Unified Communications & Collaboration hat sich längst von einem Thema der Infrastrukturkonvergenz zu einer Plattform für Anwender und Geschäftsprozesse fortentwickelt: die Rede ist heute von Communications Enabled Business Processes oder eben User-centric Communications. User-centric Communications spricht dabei:

- ungehinderte Kommunikation zwischen Mitarbeitern, Partnern, Zulieferern und Kunden,
- freie Wahl des Kommunikationskanals vor und während der Kommunikation,
- tiefe Integration in die Applikationswelt und somit die Geschäftsprozesse,
- bessere Erreichbarkeit aller Kommunikationsteilnehmer, sowie orts- und geräteunabhängige Kommunikation und Zusammenarbeit.

Doch was muss gewährleistet sein, damit diese Versprechen eingelöst werden können?

These 1: UCC kennt keine Unternehmensgrenzen

Will man effektiv Prozesse vereinfachen und beschleunigen, so müssen alle Teilnehmer am Prozess Zugriff auf die Plattform erhalten, die den Prozess technisch abbildet. Was das bedeutet, kann man sich anhand der Telefonie vergegenwärtigen: Niemand plant eine TK-Lösung, die nur die Telefonie von Mitarbeitern einer Abteilung untereinander ermöglicht. Die PBX stellt immer die Kommunikation zwischen allen Mitarbeitern eines Un-

ternehmens her. Und ebenso soll das für UCC-Lösungen gelten. Alle Kommunikationsteilnehmer im Unternehmen sollen auf derselben UCC-Plattform aufsetzen. Nur so ist eine medienbruchfreie Kommunikation und Zusammenarbeit möglich.

Aber hier liegt bereits der erste Denkfehler: so wie man früher die PBX – Private Branch Exchange! – als internes Kommunikationssystem angesehen hat, betrachtet man UCC ebenfalls als unternehmensinterne Plattform. Doch das ist falsch. Die Telefonanlage war immer die Verlängerung des öffentlichen Telefonnetzes in das Unternehmen hinein. Der Grund: man benötigte eine Möglichkeit, hunderte und tausende von Kupferdoppeladern an das öffentliche Netz anzukoppeln. Natürlich ermöglichte die TK-Anlage auch gebührenfreie interne Kommunikation und bot zusätzliche Leistungsmerkmale – aber das kompensiert nur Defizite des öffentlichen Telefonnetzes. Im Kern war und ist die PBX der verlängerte Arm des öffentlichen Telefonnetzes – einer standardisierten, globalen Infrastruktur für Sprachkommunikation. Und ohne dieses öffentliche Telefonnetz wären viele Prozesse im Unternehmen undenkbar. Denn die Prozessbeteiligten sind in der absoluten Minderheit innerhalb des Unternehmens angesiedelt. Neben den Mitarbeitern sind Geschäftspartner, Zulieferer und – nicht zuletzt – Kunden involviert. Will man die Mehrwerte von UCC über die gesamte Prozesskette realisieren, muss der Zugriff ALLER auf UCC-Dienste möglich sein. Eine UCC-Lösung an das Telefonnetz zu koppeln ist nur eine unzureichende Krücke, die den Verlust von Leistungsmerkmalen bedeutet und die Dienstvielfalt von UCC auf Sprache beschränkt. Einzig ein weltweites, dienstneutrales Datennetz kann ein geeignetes Interconnect über die Unternehmensgrenzen hinweg bieten.

These 2: UCC lebt vom einfachen Zugriff

Damit UCC seine Wirkung entfalten kann, müssen die Kommunikationskanäle jedem Teilnehmer einfach zugänglich sein. Ein gutes Beispiel sind raumgebundene Videokonferenzlösungen. Die Auslastung vieler derartiger Systeme ist nahe Null. Die Problematik: gerade hochqualitative Systeme, wie z.B. Telepräsenz-Lösungen, werden für einen sehr exklusiven Nutzerkreis eingeführt, der schon aufgrund seiner geringen Teilnehmerzahl nicht für eine angemessene Auslastung der Systeme sorgen kann. Selbst wenn der Teilnehmerkreis nicht auf das Management beschränkt ist, sorgt die Verortung auf der sprichwörtlichen „Chef-Etage“ für Berührungssängste und mangelnde Akzeptanz. Zudem ist die Buchung entweder zu kompliziert oder ohne Zugriff auf das Unternehmensnetz nicht möglich. In dem Moment, wo Videokonferenzsysteme frei zugänglich in regulären Besprechungsräumen verbaut und über ein global zugängliches Buchungssystem von autorisierten Nutzern mit wenigen Klicks reserviert werden können, steigt die Auslastung sprunghaft an.

Doch auch hier sind rein unternehmensinterne Systeme wieder schlechter gestellt. Beschränkt sich die Interkonnektivität auf drei, zehn oder gar zwanzig Telepräsenzsysteme innerhalb des Unternehmens mangelt es oft an Anwendungsfällen für den durchschnittlichen Benutzer. Er muss überlegen, ob das Telepräsenzsystem wirklich das geeignete Kommunikationsmedium ist. Sobald ein externer Kommunikationspartner an Bord ist, kann das Telepräsenzsystem nicht genutzt werden. Das lässt viele Anwender direkt zu einer einfacheren Alternative greifen – zum Beispiel einem öffentlichen Webconferencing- oder Desktopvideo-Dienst. Ob das immer das optimale Kommunikati-

UCC gehört ins Internet!

onsmedium ist, darf in Frage gestellt werden. Wie unter Punkt eins bereits diskutiert, braucht es also ein Datennetz, das die Systeme an Standorten in- und außerhalb des Unternehmens miteinander verbindet. Das gilt aber nicht nur für Medienstrom und Signalisierung. Will man einfache Nutzbarkeit erzielen, muss die Buchungsplattform auch externe Raumsysteme einbeziehen können. Das heißt, dass diese mit ihrer öffentlichen Adresse im Buchungssystem registriert oder bei Anfrage durch den Gesprächspartner im Buchungssystem hinterlegt werden können. Ein globales Adressverzeichnis und ein einfaches Adressformat unterstützen hierbei. Unabdingbar ist aber ein gemeinsames Kommunikationsnetz, das für den Austausch dieser Daten geeignet ist.

These 3: Perimeterschutz verhindert globale Kommunikationslösungen

Wir halten fest: UCC benötigt ein weltweites Netz, das für interne wie externe Teilnehmer zugänglich ist, und neben den diversen Medienströmen und der Signalisierung auch Dienste wie Adressbücher und Buchungssysteme miteinander koppeln kann. Innerhalb eines privaten Weitverkehrsnetzes ohne jegliche Sicherheitseinrichtungen ist das leicht vorstellbar. Wer allerdings einmal die Firewall-Regeln für den externen Zugriff auf eine UCC-Lösung konfigurieren musste, der weiß: sollen alle Dienste intern wie extern erreichbar sein, ist das ein kompliziertes Unterfangen, das im Ergebnis zu einer Firewall führt, die alle möglichen Arten von Traffic von und zu allen möglichen Zielen zulässt. Will man zumindest die zulässigen Quellen und Ziele einschränken, so steigt die Komplexität der Regelwerke linear zu deren Anzahl. Tut man dies nicht, wird der Gedanke des Perimeterschutzes ad absurdum geführt. Denn de facto öffnet man vielfältigste Einfallstore für Angreifer.

Angesichts dieser Problematik muss man sich die Frage stellen, was durch den Perimeterschutz erreicht werden soll. IT-Sicherheit hat im Kern zwei Ziele:

- Sicherung der Vertraulichkeit und Integrität von Informationen
- Sicherung der Verfügbarkeit von IT-Diensten

Zu beidem trägt ein effektiver Perimeterschutz wesentlich bei. Aber nur unter der Annahme, dass der Angreifer sich außerhalb des Firmennetzes befindet. Glaubt man diversen Studien zur IT-Sicherheit, so geht die größte Gefahr für die Integrität und Sicherheit der IT-Infrastruktur nicht von externen Angreifern aus, sondern von Innentätern. Von Racheakten frustrierter Mitarbeiter bis hin zur Wirtschafts-

spionage – hat der Angreifer autorisierten Zugriff auf Netz und Systeme, nutzt der beste Perimeterschutz nichts. Versagen andere Sicherheitssysteme, wie z.B. der Malware-Schutz, so wird der externe Angreifer via Trojaner zum Innentäter. Und überhaupt: in Zeiten höchster Mobilität befindet sich ein großer Teil der Mitarbeiter schon längst nicht mehr „im“ Unternehmensnetz, sondern wird künstlich und mit hohem Aufwand via VPN in dieses zurückgeholt. Unter diesen Voraussetzungen den Perimeterschutz als Allheilmittel zu betrachten ist kurzsichtig.

Das bedeutet nicht, dass man seine lokalen Netze – oder gar Rechenzentren und produktionskritische Infrastrukturen – schutzlos preisgeben sollte. Die Sicherheit in Zeiten hochkomplexer IT-Systeme muss aber neu gedacht werden. Weg vom Perimeterschutz, hin zum Inhaltsschutz. Auf UCC-Dienste bezogen bedeutet das, dass die Verschlüsselung von Medienströmen und Signalisierung Pflicht sein muss. Andernfalls endet die Integrität der Kommunikation nicht erst beim Übergang in das öffentliche Telefonnetz, sondern schon im lokalen Netzwerk. Die Verfügbarkeit der Dienste darf nicht durch eine Trennung in inneres und äußeres Netz, sondern muss durch mehrfach redundante Auslegung der Systeme, geeignete Lastbalancierung und intelligente Angriffserkennung an Netzübergängen und Clients stattfinden. Was diese Mechanismen angeht, hinkt die Infrastruktur der meisten Unternehmen denen eines einfachen Webhosters hinterher. Und der Netzübergang wird allzu oft zum Sin-

gle Point of Failure. Was aber nützt hochverfügbare interne Kommunikation, wenn die externe Kommunikation – und damit der Geschäftsprozess – unterbrochen ist? Wie der renommierte Sicherheitsexperte Dan Kaminsky einmal treffend bemerkte, ist Mehrwert das, was in Abwesenheit eines Angreifers erzielt werden kann. Den Mehrwert von UCC einem althergebrachten Sicherheitsverständnis von „drinnen und draußen“ zu opfern ist mit Sicherheit falsch. Und was unterscheidet – geeignete Sicherheitsmechanismen vorausgesetzt – noch das „innere“ vom „äußeren“ Netz, dem Internet?

These 4: UCC braucht öffentlich zugängliche, standardisierte Plattformen

Mit dem Internet steht die größte, standardbasierte Routingplattform aller Zeiten zur Verfügung. Mit den Bordmitteln des Internet ist es problemlos möglich, Punkt-zu-Punkt-Beziehungen zwischen Unternehmenslösungen für Unified Communications aufzubauen. Jedoch mangelt es an der Möglichkeit, solche „Föderationen“ für alle Kommunikationsmedien gleichermaßen aufzubauen. Auch sind diese Föderationen in den vielen Fällen auf Systeme desselben Herstellers begrenzt. Das gewichtigste Argument gegen Föderationen ist aber, dass man aus zwei Inselösungen nur eine neue, größere Inselösung schafft. Man kann durchaus alle Unternehmenslösungen, mit denen man Kommunikationsbeziehungen pflegt, via Föderation ankoppeln. Doch der administrative Aufwand für das einzelne Unternehmen steigt linear mit der Anzahl der Föderationspartner. Und alle anderen bleiben

Kongress

ComConsult TK-, UC- und Videokonferenzforum 2012 19.11. - 22.11.12 in Düsseldorf

Dieses hochaktuelle Forum analysiert aktuelle Trends, neue Technologien und Produkt-/Hersteller-Strategien im Bereich TK, UC und Videokonferenztechnik. Die Kernthemen sind: wie viel UC braucht TK; zukunftsweisende Client-Strategien; User Centric Communications; der Kunde, das unbekannte UC-Wesen; Videokonferenztechnik der Zukunft.

Moderation: Dipl.-Inform. Petra Borowka-Gatzweiler, Dominik Zöller

Kosten: 4-tägige Veranstaltung inkl. Intensiv-Tag	€ 2.490,- netto
3-tägige Veranstaltung ohne Intensiv-Tag	€ 2.090,- netto
Nur Intensiv-Tag	€ 990,- netto



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

UCC gehört ins Internet!

wieder einmal außen vor, bzw. werden nur über Einzelkanäle wie das Telefonnetz oder eine Instant-Messaging-Föderation eingebunden. Diesen Aufwand kann kein Unternehmen auf Dauer tragen.

Doch was ist die Alternative? Das zeigt – wieder einmal – das gute alte öffentliche Telefonnetz. Es ist ein Verbund aus Vermittlungsstellen der verschiedenen Provider, die folgendes bieten:

- eine standardisierte Kunden-Schnittstelle
- ein einheitliches, menschenlesbares Adressierungsformat
- Interkonnektivität zu allen Teilnehmern (auch anderer Anbieter!) weltweit

Einzig die Beschränkung auf Sprachdienste und die viel zu oft noch leitungsvermittelte letzte Meile machen das Telefonnetz für UCC ungeeignet. Die eben angesprochenen öffentlichen Instant Messaging Dienste, wie z.B. ICQ, AIM oder Skype zeigen, wie eine solche Plattform in Zeiten von UCC aussehen kann. Privatnutzer (wenige „Nebenstellen“!) registrieren sich beim Betreiber und beziehen den Dienst mit allen Leistungsmerkmalen aus der öffentlichen Plattform. Als Nebenprodukt entsteht ein plattformweites Teilnehmerverzeichnis. Große Installationen werden per Föderation („Anlagenanschluss“?) angekoppelt und ergänzen das öffentliche Dienstangebot ggf. um zusätzliche Funktionen.

Damit aus solchen Plattformen eine mögliche UCC-Plattform wird, müssen die oben genannten Punkte erfüllt werden. Als Schnittstelle für die Signalisierung bietet sich hier natürlich der SIP(S)-Standard an. Er ist hinreichend standardisiert, trotzdem erweiterbar und liefert ein einfaches, menschenlesbares Adressierungsformat gleich mit. Und ist zoeller@comconsult.com nicht viel intuitiver, als +492408951161!? Für Sprach- und Videodatenströme sind mit (S)RTP und den diversen G.XYZ Codecs ebenfalls hinreichende Standards vorhanden. Nur müssen diese Dienste auch standardkonform von den Plattformbetreibern umgesetzt werden. So könnten Privatnutzer, lokale Unternehmenslösungen und mobile Teilnehmer gleichermaßen mit Kommunikationsdiensten bedient werden. Das Interconnect zu anderen Betreibern – und damit zu allen anderen Teilnehmern – fehlt bislang, zumeist aus falsch verstandenen wirtschaftlichen Interessen. Die Plattform, die diese Punkte als erstes löst, wird das öffentliche Telefonnetz überflüssig machen. Für die großen Carrier ist es höchste Zeit zu handeln und ihre SIP-Trunking-Angebote von reinen Voice- zu UCC-Trunks zu erweitern.

These 5: UCC ist längst im Internet!

Die Föderation mit öffentlichen Instant Messaging Diensten zeigt: UCC ist längst im Internet! Zudem nutzen viele Unternehmen längst die Vorteile von Internetdiensten – oft ohne es zu wissen! Ein Beispiel ist die Integration von öffentlichen Social Media Plattformen. Ob als Kommunikationskanal und Datenquelle im Contact Center, als Globales Adressbuch via Plug-In für MS Outlook oder als App auf dem Mobilien Endgerät – öffentliche soziale Medien werden intensiv im Alltag der Mitarbeiter genutzt. Ein weiteres Beispiel ist die Nutzung von zwar kostenpflichtigen, aber dennoch öffentlichen Webconferencing-Diensten. Der Erfolg von WebEx und artverwandten Diensten beruht einzig und allein auf ihrer ständigen und allgegenwärtigen Verfügbarkeit – via Internet. In Zukunft werden internetbasierte Cloud-Dienste für Kommunikation – Unified Communications as a Service – stark an Bedeutung gewinnen. Ob als globales Adressbuch oder als Videokonferenzdienst aus der Cloud – genutzt werden sie schon heute.

Fazit

Ohne das Internet gäbe es kein Internet Protocol, ohne IP gäbe es kein UCC. Doch die globalen Kommunikationsplattformen, die im Schutz der wohlgeheuten Unternehmensnetze entstanden sind, brauchen Interkonnektivität. Andernfalls bleibt der größte Mehrwert dieser Systeme – die nahtlose Kommunikation über den gesamten Geschäftsprozess hinweg –

auf der Strecke. Und sind die Systeme für den Anwender nicht orts- und geräteunabhängig verfügbar, wird er sich Alternativen suchen. Ob die Schlussfolgerung nun lauten muss, dass alle Daten in die Public Cloud verlagert und die gesamte Unternehmenskommunikation über das Internet abgewickelt werden sollte, muss sicherlich – gerade unter Sicherheitsgesichtspunkten – diskutiert werden. Aber nichts spricht gegen den Aufbau einer unternehmensinternen Lösung, die über eine standardisierte und gut vernetzte, und öffentlich zugängliche UCC-Plattform in Kommunikation zur Außenwelt steht. Voraussetzung ist dabei immer, dass geeignete Sicherheitsmechanismen zum Einsatz kommen – weg vom Perimeterschutz, hin zum Schutz der transportierten Inhalte. Einzig: es mangelt an Angeboten – während die großen Carrier SIP-Trunking immer noch als Alternative zum ISDN-Anlagenanschluss betrachten, sind die öffentlichen UCaaS-Dienste untereinander noch nicht hinreichend vernetzt, geschweige denn standardkonform. Heute schon auf die Vernetzung über öffentliche UCC-Angebote zu setzen, ist ein mutiges und schwieriges Unterfangen. Zukünftig den Mehrwert, den das Internet für UCC bietet, nicht auszuschöpfen, ist hingegen fahrlässig.

UCC und das Internet – das Spannungsfeld zwischen komplexen Architekturen, vertraulicher Kommunikation und erzielbaren Mehrwerten ist auch in diesem Jahr das Thema auf dem ComConsult TK-, UC- und Videokonferenzforum.

Report

Unified Communications: Cisco versus Microsoft Juni 2012 - 310 Seiten



Dieser Report analysiert die bestehenden UC-Lösungen von Cisco und Microsoft auf dem Stand der neuesten Releases und stellt die spannende Frage, wer die bessere Lösung hat. Auch die erkennbaren Weiterentwicklungen werden dabei berücksichtigt. Der Report bewertet nicht nur die rein technische Funktionalität, sondern gibt auch Einschätzungen zum strategischen und wirtschaftlichen Einsatz und zur Zukunftssicherheit der Produkte ab. Eine derartige Gegenüberstellung der UC-Lösungen dieser beiden Hersteller ist im Markt einzigartig, sie bietet eine detaillierte und kontroverse Gegenüberstellung.

Autorin: Dipl.-Inform. Petra Borowka-Gatzweiler
Preis: € 398,- netto



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

Aktuelle Veranstaltungen

Internetworking: optimales Netzwerk-Design mit Switching und Routing, 22.10. - 26.10.12 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

IT-Projektmanagement Kompaktseminar, 22.10. - 24.10.12 in Hamburg

Ein Projekt stellt an einen Projektleiter hohe Anforderungen. In diesem Kurs vervollständigen Sie praxisnah Ihre Kenntnisse aus der gesamten Bandbreite des Projektmanagements: Der Kurs umfasst sowohl Administratives, wie Planen und Überwachen des Projekts, als auch Softskills, wie Moderation von Projektsitzungen und Präsentation von Information. Denn die in der Regel nur „lose“ unterstellten Projektmitarbeiter müssen überzeugend auf Basis einer strukturierten Planung geführt werden. Und jede Chance, sich und sein Projekt erfolgreich zu präsentieren, ist zu nutzen! Preis: € 1.890,- netto

Rechenzentrumsdesign - Technologien neuester Stand, 22.10. - 24.10.12 in Hamburg

Das 3-tägige Seminar „Rechenzentrumsdesign – Technologien neuester Stand“ fokussiert sich auf aktuelle Technologien und Trends im Rechenzentrumsfeld. Sie lernen von der Verkabelung über die Stromversorgung, die Klimatisierung und den Schrankaufbau, wie ein ausfallsicheres und energieeffizientes Rechenzentrum heute strukturiert wird. An den Tagen zur aktiven Netztechnik lernen Sie, welche Mechanismen für Redundanz, Lastverteilung und Standort-übergreifende Hochverfügbarkeit in aktuellen RZ-Planungen zu berücksichtigen sind und 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: € 1.890,- netto

Trouble Shooting in vernetzten Infrastrukturen, 23.10. - 26.10.12 in Aachen

Dieses Seminar vermittelt, welche Methoden und Werkzeuge die Basis für eine erfolgreiche Fehlersuche sind. Es zeigt typische Fehler, erklärt deren Erscheinungsformen im laufenden Betrieb und trainiert ihre systematische Diagnose und die zielgerichtete Beseitigung. Dabei wird das für eine erfolgreiche Analyse erforderliche Hintergrundwissen vermittelt und mit praktischen Übungen und Fallbeispielen in einem Trainings-Netzwerk kombiniert. Die Teilnehmer werden durch dieses kombinierte Training in die Lage versetzt, das Gelernte sofort in der Praxis umzusetzen. Als Protokoll-Analysator-Software kommt Wireshark zum Einsatz. Einer Verwendung selbst mitgebrachter Analyse-Software, mit deren Bedienung der Teilnehmer vertraut ist, steht nichts im Wege. Preis: € 2.290,- netto

Mobile Device Management - Betrieb von mobilen Endgeräte-Flotten, 25.10.12 in Bonn

Dieses Seminar analysiert den Trend zur Mobilisierung der Unternehmens-IT. Es werden Konzepte und technische Maßnahmen zum Umgang mit diesem Sachverhalt aufgezeigt. Es werden verfügbare technische Lösungen vorgestellt und Strategien für den Betrieb dieser Lösungen erarbeitet. Preis: € 990,- netto

Storage: Planung moderner Speicher-Lösungen, 25.10. - 26.10.12 in Bonn

Dieses 2-tägige Seminar konzentriert sich auf Fragestellungen, die bei der Planung und dem Betrieb von Speicherumgebungen entstehen. In der Anforderungsanalyse werden die möglichen Einsatzszenarien wie etwa Datenbanken und virtuelle Umgebungen differenziert betrachtet. Zu diesen Anforderungen werden Lösungsansätze entwickelt, die sowohl heutige als auch zukünftige Technologien berücksichtigen. Die Kombination aus strategischen Überlegungen und technischen Maßnahmen bilden eine Leitlinie, welche Aspekte in welcher Form bei der Planung einer modernen Speicherinfrastruktur zu berücksichtigen sind. Preis: € 1.590,- netto

Wireless LAN professionell, 29.10. - 31.10.12 in Stuttgart

Dieses Seminar vermittelt den aktuellen Stand der WLAN-Technik und zeigt die in der Praxis verwendeten Methoden für Aufbau, LAN-Integration, Betrieb und Optimierung von WLANs im Enterprise-Bereich auf. Die verschiedenen WLAN-Varianten werden analysiert, Markt- und Produktsituation werden bewertet, und Empfehlungen für eine optimale Auswahl werden gegeben. Preis: € 1.890,- netto

WAN: Aktuelle Technologie und Erfahrungen aus Ausschreibungen, 29.10. - 30.10.12 in Stuttgart

Das Programm des Seminars „WAN: Neue Verfahren und Erfahrungen aus Ausschreibungen“ 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 standortübergreifenden 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

Zertifizierungen

ComConsult Certified Network Engineer

Lokale Netze

12.11. - 16.11.12 in Aachen
 21.01. - 25.01.13 in Aachen
 22.04. - 26.04.13 in Aachen
 09.09. - 13.09.13 in Aachen
 25.11. - 29.11.13 in Aachen

TCP/IP intensiv und kompakt

18.02. - 22.02.13 in Stuttgart
 13.05. - 17.05.13 in Bonn
 07.10. - 11.10.13 in Stuttgart

Internetworking

22.10. - 26.10.12 in Aachen
 11.03. - 15.03.13 in Aachen
 17.06. - 21.06.13 in Aachen
 14.10. - 18.10.13 in Aachen

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

ComConsult Certified Trouble Shooter

Trouble Shooting in vernetzten Infrastrukturen

23.10. - 26.10.12 in Aachen
 05.02. - 08.02.13 in Aachen
 11.06. - 14.06.13 in Aachen
 24.09. - 27.09.13 in Aachen

Trouble Shooting für Netzwerk-Anwendungen

04.12. - 07.12.12 in Aachen
 12.03. - 15.03.13 in Aachen
 09.07. - 12.07.13 in Aachen
 05.11. - 08.11.13 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

26.11. - 28.11.12 in Bonn
 25.02. - 27.02.13 in Köln
 03.06. - 05.06.13 in Bonn
 16.09. - 18.09.13 in Berlin
 02.12. - 04.12.13 in Bonn

Session Initiation Protocol Basis-Technologie der IP-Telefonie

29.10. - 31.10.12 in Bonn
 18.03. - 20.03.13 in Berlin
 24.06. - 26.06.13 in Köln
 07.10. - 09.10.13 in Stuttgart

Umfassende Absicherung von Voice over IP und Unified Communications

11.04. - 12.04.13 in Bonn
 18.07. - 19.07.13 in Bonn
 04.11. - 05.11.13 in Bonn

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

18.02. - 19.02.13 in Stuttgart
 13.05. - 14.05.13 in Bonn
 30.09. - 01.10.13 in Düsseldorf

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

ComConsult Certified Service Catalogue Manager

Servicialisierung - Leitkonzept für verlässliche Service-Erbringung

18.03. - 19.03.13 in Berlin

Service-Identifizierung - Von Service-Begriff bis Service-Konsumentennutzen

22.04. - 23.04.13 in Düsseldorf

Service-Offertierung - Von Service-Spezifizierung bis Service-Katalogisierung

11.06. - 12.06.13 in Aachen

Paketpreis für alle drei Seminare € 4.290,-- netto (Einzelpreise: je € 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
 Erscheinungsweise: Monatlich,
 12 Ausgaben im Jahr

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

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