ComConsult Research

Der Netzwerk Insider

Februar 15

Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

Neue Ethernet Datenraten

von Dr. Franz-Joachim Kauffels

Bei der Weiterentwicklung der Übertragungssysteme in Netzen gibt es heute zwei Schwerpunkte, an denen dringend um Lösungen gerungen wird: die Infrastruktur für die nächste Generation von 11ac WLAN-Access Points und ein passendes RZ-Design für neue Server, die mehr als 10 GbE für eine vernünftige Anbindung benötigen. Bei den WLANs kommen wir bald an den Punkt, wo eine Anbindung der 11ac APs mit 1 GbE nicht mehr ausreichend ist, weil die zweite Produktwelle dieser APs mehr Leistung hat. Aber: 10 GbE ist zu teuer und zu leistungsfähig.

Wir benötigen angepasste Lösungen zwischen diesen Raten, die auch auf bestehender Campus-Verkabelung laufen. Im RZ ist die Gemengelage bei den 40 GbE-Anschlüssen unübersichtlich. Optimal und problemangepasst ist hier aktuell gar nichts. Kann hier die neue 25/50 GbE-Initiative helfen? In jedem Fall ist klar: es gibt eine neue Generation höchst leistungsfähiger 25/40/50/100 GbE Switch-ASICs, die die heute erhältlichen Lösungen deutlich in den Schatten stellt.

weiter auf Seite 7

Zweitthema

Warum Private Cloud? Und wie?

von Dr. Behrooz Moayeri

Wenn die Cloud-Diskussion in der unternehmensinternen IT etwas bewegt hat, dann – zumindest in Deutschland – in Richtung Private Clouds. Private Clouds sind die angemessene Antwort der in Druck geratenen IT-Organisationen auf Vorhaltungen, die öffentlichen Anbieter machen alles besser und billiger. Dieser Beitrag geht auf die Daseinsberechtigung von Private Clouds und Ansätze für deren Aufbau und Betrieb ein.

Warum nicht die Public Cloud?

Der unternehmensinternen IT wird oft vorgeworfen, ihr gehe es nur um einen Bestandsschutz. Sie denke nicht wirtschaftlich und wolle nur ihre Bastionen verteidigen, lautet ein häufiger Spruch. Gepaart mit der Absicht, sich auf das Kerngeschäft zu konzentrieren, dienen solche Sprüche dazu, der internen IT Kompetenzen zu entziehen. Die öffentlichen Anbieter sollen es richten. Die private IT dient dabei als Vorbild. Der Verbraucher zahlt meistens keinen Cent für den E-Mail-Dienst, für zunehmenden Speicherplatz, für Kommunikationsdienste usw. Und wenn er mal ein paar Funktionen mehr haben will als die kostenlosen, bekommt er sie für den sprichwörtlichen Appel und n Ei. Warum soll dies also nicht für die IT-Belange des Unternehmens versucht werden? Das Unternehmen könne dabei massiv das IT-Budget reduzieren und sich auf sein Kerngeschäft konzentrieren.

weiter auf Seite 21

Geleit

IEEE 802.11ac WLAN Wave 2: viele Fragezeichen und Risiken hinter Gigabit WLAN

auf Seite 2

Aktueller Kongress

ComConsult Netzwerk- und IT-Infrastruktur Forum 2015

ab Seite 4

Standpunkt

Neue Sicherheitsarchitekturen mit Software-Defined Security

auf Seite 18

Neue Seminare

Crashkurs IT-Recht für Nichtjuristen
IT-Sicherheit in der industriellen Fertigung und der Shop Floor IT

ab Seite 19

Zum Geleit

IEEE 802.11ac WLAN Wave 2: viele Fragezeichen und Risiken hinter Gigabit WLAN

Endlich sind sie da, die lange erwarteten Wave 2 Lösungen für 802.11ac. Die erste Produkt-Generation war doch in den gebotenen Leistungen sehr eingeschränkt und setzte die Möglichkeiten des Standards nur teilweise um. Mit den neuen Wave 2 Chips, die gerade in Las Vegas auf der CES vorgestellt wurden, gibt es mehr Leistung und auch mehr Funktionalität. Damit steht die Tür offen für wirkliche Gigabit-WLAN-Lösungen. Oder auch nicht, denn es gibt viele Fragezeichen mit erheblichen Auswirkungen auf die Planung und spätere Nutzung.

Wer geglaubt hat, dass das alles noch Zeit hat, der wurde am 20. Januar eines besseren belehrt als Cisco seine neuen Switches zur Versorgung von Wave 2 Access Points angekündigt hat. Und es ist keine Frage, dass die Konkurrenz bald folgen wird.

Warum beobachten wir diese Hektik im Markt? Nun erst einmal muss festgestellt werden, dass Wave 1-Produkte weit von den Versprechungen eines Gigabit-WLAN entfernt waren. In der Regel kamen sie der Gigabit-Grenze selbst auf kurzen Funk-Entfernungen nicht einmal nahe. Auf der anderen Seite haben fast alle neuen mobilen Endgeräte inzwischen den 802.11ac-Standard implementiert, allerdings bisher mit den Funktionen von Wave 1, also zum Beispiel ohne die Unterstützung von MU-MIMO. Trotzdem hat das den Bedarf erzeugt, auf der Seite der Access Points diesen Standard auch zu unterstützen. Gleichzeitig gibt es eine zunehmende Anzahl von Nutzungssituationen, in denen wir an die Grenzen der bisherigen Technologie stoßen. Beispiele dafür sind Konferenzbereiche in Hotels, Flughäfen, Krankenhäuser und Fertigungsbereiche oder Warenhäuser mit vielen Client-Systemen.

Bei der Betrachtung des Wortes “Gigabit” muss unter Berücksichtigung typischer Bedarfssituationen beachtet werden, dass wir die Kapazität einer WLAN-Zelle unter ganz verschiedenen Gesichtspunkten bewerten können:

- Eine Sichtweise ist, die Kapazität mit der maximal erreichbaren Bandbreite durch einen Teilnehmer gleichzusetzen. Das Problem dabei ist, dass eine wirklich hohe Bandbreite nur auf so kurzen Entfernungen erreicht werden kann,

dass dies als bedeutungslos für die Praxis angesehen werden kann. In keinem Fall wird dabei die Gigabit-Grenze erreicht. Außerdem gibt es kaum mobile Clients, die mehr als einen Stream unterstützen, wodurch Gigabit gar unerreichbar wird.

- Eine andere Sichtweise ist es, die Kapazität aus der Sichte einer typischen Nutzungssituation mit der Zahl gleichzeitig zu versorgender Teilnehmer gleichzusetzen. Also zum Beispiel könnte es ein Planungsziel sein, in einem Kongress-Raum oder einem Flughafen mit einem Access-Point gleichzeitig maximal 50 bis 100 mobile Teilnehmer zu versorgen. Diese Anzahl ist etwas willkürlich gewählt, basiert aber auf der Annahme, dass im wesentlichen Email-Kommunikation und einfache Web-Anwendungen zu unterstützen sind und nicht die Absicht besteht, ein perfektes Video-Erlebnis mit YouTube oder Netflix für eine große Anzahl von Teilnehmern zu erreichen. Da für Email oder einfaches Browsing zum Beispiel mit der Salesforce-App nur eine sehr geringe Bandbreite von weniger als einem Mbit/s benötigt wird, könnte man die Erwartung haben, dass ein so genanntes Gigabit-WLAN dies ja wohl erfüllen würde

Leider stoßen wir in der Umsetzung solcher Szenarien wie der eines Konferenz-Raumes oder eines Terminals in einem Flughafen auf einige Tücken der heute genutzten WLAN-Technik. So nimmt die verfügbare Bandbreite in einer Zelle verursacht durch das Medienzugangsverfahren mit einer zunehmenden Teilnehmerzahl stark ab. Faktisch kann es dabei sein, dass nur noch 200 Mbit/s oder sogar weniger zur Verfügung stehen. Gegenüber der Situation mit nur einem perfekten Teilnehmer kann es dabei zu Einbußen von 50% und deutlich mehr kommen. Gleichzeitig müssen wir uns der Frage stellen, welche Einflussfaktoren von Endgeräten ausgehen, die nach älteren WLAN-Standards kommunizieren. Wer die Gigabit im WLAN wirklich erreichen will, der sollte die Zelle nur für 11ac-Teilnehmer auslegen und keine anderen WLAN-Standards erlauben. Dies bedeutet, dass der Access-Point mehrere Radio-Teile für parallel angebotene WLAN-Verfahren haben muss, damit auch die alten Standards abgedeckt werden können (was wiederum neue Probleme in der Gestaltung der Zelle aufwirft). Was wiederum sofort zu einer Frequenzfrage führt.

Die Frequenzplanung ist eine der großen Herausforderungen der Zukunft. Die 160 MHz-Kanalbandbreite können wir für die meisten Praxissituationen getrost abschreiben, sie blockiert zu viele Frequenzen. Aber auch bei einer 80 MHz-Planung ist zu beachten, dass wir einen Trend zu immer kleineren Zellen haben. In der Praxis wird mit weiter fallenden Preisen für Access Points die Zahl der Access Points fast nur noch durch die Kosten und Umsetzbarkeit der Verkabelung bestimmt (und die Verfügbarkeit einer ausreichenden Menge an Ports am versorgenden Switch). Es kann als sicher angesehen werden, dass wir in wenigen Jahren mit eher kleinen als großen Zellen arbeiten. Das hat aber seine Tücken. Funkwellen neigen nicht dazu an der Grenze einer geplanten Zelle einfach zu verschwinden. So haben wir Überlappungen zwischen Zellen, die manchmal im Sinne eines Handovers für sich bewegende Teilnehmer erforderlich sind, aber auch manchmal ohne Absicht entstehen und zu erheblichen Problemen führen können (bitte lesen Sie den Artikel von Dr. Wetzlar im letzten Netzwerk Insider). Dabei sind auch 3-dimensionale Szenarien zu berücksichtigen.

Betrachten wir weiterhin die Betriebserfahrungen aus Projekten wie Hotels, Flughäfen und Krankenhäusern, dann müssen wir natürlich feststellen, dass unser Planungswunsch einer möglichst professionellen Nutzung durch die Teilnehmer nicht immer der Realität entspricht. So müs-

IEEE 802.11ac WLAN Wave 2: viele Fragezeichen und Risiken hinter Gigabit WLAN

sen wir damit leben, dass Teilnehmer auf ihren schönen großen neuen Smartphones begeistert Videos konsumieren oder in großem Stil mit Dropbox oder ähnlichen Diensten synchronisieren. Was für Teilnehmer, die gerade ein Flugzeug verlassen haben oder nach einer Reise im Hotel-Foyer ihr Gerät einschalten, durchaus mit einem erheblichen Datenstrom gleichgesetzt werden kann (ich bin einer der Schrecken der WLAN-Betreiber am Flughafen Singapur. Ich arbeite mit Adobe Lightroom und synchronisiere meine Foto-Bibliotheken mit Dropbox. Die Katalog- und Preview-Dateien sind dabei erheblich. Um die Freude der Betreiber zu erhöhen nutze ich gleichzeitig mobile Videokonferenz von meinem iPad aus). Wir müssen uns also der Frage stellen wie wir damit umgehen. Und die einzig sinnvolle Lösung ist Traffic-Shaping (mit der Ausnahme von Singapur natürlich). Wir müssen den bekannten Verursachern von Bandbreitenverbrauch schlicht Grenzen setzen. Und gleichzeitig müssen wir den realen Verbrauch permanent überwachen und diese Traffic-Shaping-Parameter permanent der Realität anpassen. Dies setzt auch voraus, dass wir ein Monitoring-System betreiben, dass die einzelnen Anwendungen überhaupt erkennen kann. Dabei müssen wir uns mit einer Reihe von Schlüsselfragen auseinander setzen. Eine davon ist, wie wir in Zukunft mobile Videokonferenzen behandeln. Produkte wie VSee greifen sich was sie bekommen können. Während ein Flughafen vielleicht nach einer einfachen Lösung sucht und die Bandbreite pro Teilnehmer generell begrenzt, kann das in vielen anderen Szenarien nicht gemacht werden. Ich kann eine Begrenzung dann nur Applikations-abhängig umsetzen.

Das Thema Monitoring wird nach aller Voraussicht eines der zentralen Themen der nächsten Jahre werden. Zum einen haben wir immer mehr Access Points und zum anderen sind die Nutzungssituationen überaus dynamisch. Wir müssen die Parameter unseres WLAN-Netzes dementsprechend kontinuierlich der Realität anpassen.

Das Ganze geht dann auch sofort in Sicherheitsfragen über. Je mehr Teilnehmer wir im WLAN haben, desto mehr müssen wir uns der Frage stellen, welche Rolle das WLAN in unserem Sicherheitskonstrukt spielt. Dies steht in einem direkten Zusammenhang mit dem Monitoring. Und tatsächlich geht es eine ganze Stufe weiter. Wir gehen im Moment davon aus, dass virtuelle Appliances und SDN gerade in diesem Umfeld eine stark zunehmende Bedeutung haben werden.

Damit sind wir bei dem letzten Punkt dieses Geleits, das wie immer nicht den Anspruch erhebt vollständig zu sein. Was passiert eigentlich, wenn eine WLAN-Zelle tatsächlich trotz aller technischen Irrungen und Wirrungen auf der Funkseite die Gigabit-Grenze überschreitet? Nehmen wir zum Spaß mal an, dass MU-MIMO tatsächlich funktioniert (woran wir erhebliche Zweifel haben). Ein Access Point wird im Moment mit einer Gigabit-Ethernet-Verbindung versorgt. Dies reicht dann nicht mehr aus. Die nächste Stufe wären dann nach aktuellen Standards 10 Gigabit. Aber dies würde nicht nur eine andere Qualität von Kabel erfordern, sondern auch Probleme mit PoE erzeugen. Was ist also zu tun? Die Anbindung von Access Points mit Gigabit-Ethernet ist in keinem Fall Zukunfts-tauglich.

Dies hat auch die Branche erkannt. Und wie sie dem in dieser Ausgabe enthaltenen Artikel von Dr. Kauffels entnehmen können, sind neue Ethernet-Bandbreiten im Kommen. Das spannende an diesen neuen Bandbreiten ist, dass sie technologisch auf bereits verfügbaren Lösungen aufsetzen, also schnellstens umgesetzt werden könnten. Und dazu gehören 2,5 und 5 Gigabit, die gezielt so ausgelegt sind, dass sie auf Cat 5E arbeiten und auch PoE unterstützen. Diese Standards sind bisher nicht verabschiedet. Tatsächlich gibt es auch zwei Interessen-Gruppen, die sich hier nicht einig sind. In der NBase-T Allianz haben wir Aquantia, Cisco, Intel, Qualcomm und Ruckus. In der Konkurrenz-Allianz MGBase-T ist wiederum Broadcom vertreten, die einer der wesentlichen Lieferanten der entsprechenden Chips sind. Tatsächlich sollte man also in dieser Situation meinen, dass wir bis zur endgültigen Verabschiedung abwarten müssen.

Dem ist nun nicht so. Am 20. Januar hat Cisco seine neuen Catalyst 3560-CX und 2960-CX angekündigt. Diese unterstützen bereits die neuen Bandbreiten. Damit setzt Cisco den Markt erheblich unter Druck. Im Endeffekt muss sich Broadcom nun entscheiden, ob sie sich dem Druck beugen oder weiterhin einen anderen Weg gehen wollen.

Sie sehen also, dass der ganze WLAN-Markt erheblich in Bewegung ist. Es gibt weitere signifikante Entwicklungen, die den Rahmen des Geleits sprengen würden. Aber seien Sie versichert, hier wird in den nächsten Monaten und Jahren noch einiges passieren. Genug jedenfalls, um dieser Entwicklung auf den Zahn zu fühlen.

Wir werden unsere Analysen zur Entwicklung von Gigabit WLAN auf dem ComConsult Netzwerk- und IT-Infrastruktur-Forum 2015 vorstellen. Zusammen mit den anderen sehr weit reichenden Entwicklungen, die den Netzwerk Markt im Moment treffen, ist das ComConsult Netzwerk- und IT-Infrastruktur-Forum 2015 damit die richtige Veranstaltung zur richtigen Zeit.

Ihr
Dr. Jürgen Suppan

Aktueller Kongress

ComConsult Netzwerk- und IT-Infrastruktur Forum 2015

20.04. - 22.04.15 in Königswinter

Das ComConsult Netzwerk- und IT-Infrastruktur-Forum 2015 stellt die drei momentan dominanten Netzwerk-Themen in den Mittelpunkt der Veranstaltung:

- Netzwerke und Infrastrukturen im Rechenzentrum
- Netzwerk-Planung und Design
- Betrieb, Verfügbarkeit und Wirtschaftlichkeit von Netzwerken

Dabei beobachten wir in allen drei Bereichen herausragende Entwicklungen, die sowohl die Leistung als auch die Wirtschaftlichkeit von Netzwerken in den nächsten Jahren stark beeinflussen werden. Drei Beispiele aus dem Programm des Forums sollen das verdeutlichen.

Im Rechenzentrum führen die Anforderungen von Virtualisierung, dem Aufbau von Private Clouds und der performanten Integration von Speicher-Systemen dazu, dass wir unsere bisherigen Architekturen mehr und mehr in Frage stellen. Statt dessen drängen neue Themen in die Diskussion:

- die Rolle von Software-Switches in den Architekturen und als Teil von Lösungen wie VMware NSX
- die Rolle von virtuellen Appliances, um ganze Anwendungsbereiche über mehrere Server hinweg mobil zu gestalten und zwischen Standorten verlagern zu können (wesentlicher Teil für Notfall-Szenarien, das ging so bisher nicht)
- SDN gewinnt in diesem Umfeld rapide an Bedeutung, zwar nicht wie ursprünglich als Technologie vorgestellt, sondern mehr als Speziallösung zur Steuerung von Software-Switches und virtuellen Appliances, aber dafür hat es in diesem Bereich den Status einer unreifen Technologie längst verlassen

Im Bereich Netzwerk Design dominiert die Kombination aus einer besseren Anpassung von Netzwerken an den Bedarf und nach flexibleren Lösungen. So sehen wir:

- neue Ethernet-Bandbreiten, die auf den ersten Blick überraschen, aber bei näherer Analyse sehr viel Sinn machen
- neue Design-Konzepte zur Verbesserung von Skalierung und Provisionierung, zum Beispiel als Edge/Core-Design
- die erste große Welle der IPv6-Projekte

Im Bereich Betrieb geht es sehr viel um die Optimierung bekannter Technologien und die dynamische Anpassung an einen sich permanent verändernden Bedarf:

- im Bereich WLAN haben wir zwar mit 802.11ac eine neue Technologie und müssen Planung und Design daran anpassen. Aber die eigentlichen Anforderungen liegen in vielen Projekten mehr und mehr im Betrieb. Und Bandbreiten-Management in Kombination mit Sicherheits-Aspekten und einer Integration in ein sehr leistungsfähiges Monitoring sind hier die Schlüssel-Funktionen
- wir haben im Betrieb ein zunehmendes Problem mit der Komplexität des Netzwerk-Aufbaus und der daraus resultierenden Destabilisierung des Netzwerks an sich. Eine der wesentlichen Ursachen für die Destabilisierung liegt in der Explosion der Anzahl von Middleboxes im Netzwerk (Firewalls, IDS, Load Balancer, …). Wir beobachten eine zunehmende Zahl von Netzwerken, die im Core mehr MiddleBox-Systeme als Switches haben
- das Thema Sicherheit nimmt noch weiter an Bedeutung zu. In den Projekten ist es in vielen Fällen inzwischen das Thema Nummer 1 für die Gestaltung des Betriebs. Das Problem liegt hier nicht in der Auswahl einer Lösung, sondern in der Gestaltung der Lösung in einer Form, dass sie mit überschaubarem Aufwand betrieben werden kann.

Der Netzwerk-Markt ist in Bewegung wie diese Beispiele zeigen. Das ComConsult Netzwerk- und IT-Infrastruktur-Forum 2015 ist das richtige Forum zur richtigen Zeit. Wir analysieren für Sie:

- was passiert im Rechenzentrum und wie können Sie Ihr Netzwerk darauf optimal vorbereiten
- wie verändert sich Netzwerk-Design und wie können Sie die Vorteile zu Ihren Gunsten nutzen ohne das gesamte Netzwerk ablösen zu müssen
- wie können Sie die Komplexität des Netzwerkes im Betrieb reduzieren und dabei gleichzeitig besser werden

Wie in jedem Jahr hat auch dieses Forum einen Vertiefungstag, in diesem Jahr dreht er sich komplett um IPv6 und die aktuellen Projekterfahrungen in diesem Bereich.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

ComConsult Netzwerk- und IT-Infrastruktur Forum 2015

Ich buche den Kongress
ComConsult Netzwerk- und IT-Infrastruktur Forum 2015

☐ vom 20.04. - 22.04.15 in Königswinter zum Preis € 2.390,-- netto

☐ vom 20.04. - 21.04.15 in Königswinter zum Preis € 1.990,-- netto

☐ am 22.04.15 in Königswinter zum Preis € 990,-- netto

Zum Kongressportal
www.comconsult-research.de

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

Programmübersicht ComConsult Netzwerk- und IT-Infrastruktur Forum 2015

Montag, 20.04.2015

9:30 - 10:15 Uhr
Keynote: Netzwerk- und IT-Infrastruktur-Trends 2015: wohin geht der Weg?
- Bedarfsanalyse
- Die Top 5 Zukunfts-Technologien in der Bewertung von ComConsult Research
- Investitions-Alternativen im Vergleich

Dr. Jürgen Suppan, ComConsult Research Ltd.

Netzwerke und Infrastrukturen im Rechenzentrum

10:15 - 11:00 Uhr
Das tatsächliche Potential von SDN
- Wo steht SDN heute?
- SDN ist nicht gleich SDN - eine Klarstellung
- Was macht SDN denn so attraktiv?
- Anwendungsbeispiele mit SDN, die traditionell nicht oder nur mit hohem Aufwand umsetzbar sind
- Empfehlungen

Dipl.-Ing. Markus Nispel, Extreme Networks GmbH

11:00 - 11:30 Uhr Kaffeepause in der Ausstellung

11:30 - 12:15 Uhr
Neue Lösungsansätze für RZ-Netze
- Unterschiede zu klassischen Netzwerktechnologien
- Was ist der Kern von SDN?
- OpenFlow-SDN vs. Netzwerkvirtualisierung
- NV und SDN als Bausteine für das Software-Defined Datacenter von VMware (NSX)
- Wo bleiben die Anwendungen: Cisco ACI und QoS im Rechenzentrum

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

12:15 - 13:00 Uhr
Private Clouds und die Auswirkung auf IT-Infrastrukturen
- Was eine Private Cloud als solche qualifiziert
- Software-Defined Data Center: Voraussetzung für die Cloud
- Virtualisierte Server als Kernbestandteil
- Elemente einer modernen Speicherstrategie
- Das passende RZ-Zonenkonzept zur Cloud
- Organisatorische Herausforderungen

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

13:00 - 14:15 Uhr Mittagspause

14:15 - 15:00 Uhr
Application Centric Infrastructure: Die Basis für eine Policy-Definierte RZ, LAN und WAN-Infrastruktur
- ACI als Basis für die Policy-Definierte RZ-Infrastruktur (Bausteine der ACI-Architektur, Grundlage für Automation im RZ, Policy-Modell: wie Anwendungen abgesichert werden können)
- Wie APIC-EM den LAN- und WAN-Betriebsprozess optimiert (Vorteile der Controller gemanagten Infrastruktur, Abstraktion als Basis für Automatisierung, QoS, ACL, Richtlinien auf der Basis abstrahierter Topologie, die Rolle des Controllers)

Dipl.-Inform. Matthias Wessendorf, Markus Harbeck, Cisco Systems GmbH

Netzwerk-Planung und Design

15:00 - 15:45 Uhr
Neue Datenraten für Ethernet
- 2,5GbE und 5GbE zur Unterstützung flächendeckender WLAN-Inrastrukturen
- 25GbE und 50GbE als skalierbare Alternative zum unseligen 40GbE
- Die neue Generation der 25/50/100G Switch ASICS wie Broadcom Tomahawk
- 40G am Scheideweg: kommt 40 GBASE-T oder doch nicht?

Dr. Franz-Joachim Kauffels, unabhängiger Unternehmensberater

15:45 - 16:15 Uhr Kaffeepause in der Ausstellung

16:15 - 17:00 Uhr
IPv6: Wo wir stehen, was wir noch brauchen
- Aktueller Stand bei Unternehmen, Providern und Herstellern
- Mit welchen Schwierigkeiten müssen Unternehmen rechnen?
- Welche ungeklärten Problemfelder müssen noch angegangen werden?

Markus Schaub, ComConsult-Study.tv

17:00 - 17:45 Uhr
The New IP – welche Rolle wird NFV in heutigen Netzen spielen?
- Warum Software und wie sehen typische Lösungen aus?
- Vergleich mit Hardware-Lösungen: Vor- und Nachteile
- Kosten-Vergleich: wie viel Geld lässt sich sparen
- Einsatz-Szenerien und Empfehlungen

Christopher Feussner, Brocade Communications GmbH

ab 18:00 Uhr Happy Hour

Dienstag, 21.04.2015

9:00 - 9:45 Uhr
Neue Designkonzepte im Vergleich: Verbesserung von Skalierung und Provisionierung
- Trennung in Edge und Core / Backbone
- Erhöhte Skalierbarkeit
- Verbesserte Provisionierung (Virtualisierung, Quality of Service, Zugangskontrolle/NAC, Mobilität)
- Anforderungen für den Edge: RZ, Access
- Anforderungen für den Core: RZ, Campus
- Technologien: Tunnelverfahren und Markierung
- Migrations-Aufwand
- Multivendor-Unterstützung
- Einheitlichkeit für Campus, RZ und Access

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

Betrieb, Verfügbarkeit und Wirtschaftlichkeit von Netzwerken

9:45 - 10:30 Uhr
WLAN-Netzwerke mit 802.11ac: Methoden zur Bandbreiten-Optimierung und zuverlässigen Versorgung mobiler Teilnehmer
- Analyse: wie viel Bandbreite hat 11ac wirklich und wo liegen Probleme
- Warum Bandbreiten-Management erforderlich ist
- Einfache Prioritäten-Schemata versagen, wie kann eine intelligente und adaptive Lösung genau auf den Bedarf zugeschnitten werden
- Wahl eines optimierten 802.11 ac Channel Design
- Intelligente Steuerung der Clients um optimale Bandbreite für die gesamte WLAN Infrastruktur zu gewährleisten.

Reinhard Lichte, Aruba Networks GmbH

10:30 - 11:00 Uhr Kaffeepause in der Ausstellung

Programmübersicht ComConsult Netzwerk- und IT-Infrastruktur Forum 2015

Dienstag, 21.04.2015

11:00 - 11:45 Uhr
Quality of Service im WLAN: Grenzen und Möglichkeiten der Technologie
- QoS auf der Luftschnittstelle: IEEE 802.11e und WiFi Multimedia (WMM)
- Übertragungs-Kapazität, der Schlüssel für hohe Dienstegüte: Wie plant man leistungsfähige WLAN?
- Multi-User MIMO wird verfügbar, nützt es der QoS?
- QoS zum „Nulltarif", wie funktionieren Anwendungs-sensitive WLANs?
- Software Defined Networking (SDN), ein alternativer Ansatz zur Umsetzung von QoS

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

11:45 - 12:30 Uhr
Problematik und Zukunft von Middleboxes
- Firewalls, IPS, Proxies, Load Balancer, WAN-Optimierer & Co.: warum sie immer mehr Aufwand verursachen
- Ist SDN die Zukunft für Middleboxes?
- Bestehende vielversprechende Ansätze

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

12:30 - 14:00 Uhr Mittagspause

14:00 - 14:45 Uhr
Neue Herausforderungen für die Netzwerksicherheit
- Abwehr von Lauschangriffen und Advanced Persistent Threats: Anforderungen an die Netzwerk-sicherheit und resultierende Sicherheitsarchitekturen
- Netzzugangskontrolle, Verschlüsselung auf Ebene des Netzwerks, Zonenkonzepte: Aufwand vs. Sicherheitsgewinn
- Virtualisierung und Vertikal integrierte Systeme: Evolution zu Plattform-integrierten Sicherheitskomponenten
- SDN, ACI und Co.: Notwendigkeit Anwendungs-zentrierter Sicherheitskonzepte im modernen RZ

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

14:45 - 15:30 Uhr
Vom klassischen Infrastruktur Monitoring zum Ende zu Ende Business Applikations Monitoring
- Proaktive Überwachung und Root-Cause Analyse von Applikationsproblemen
- Überwachung der Business Transaktionen auf dem Weg durch die IT Infrastruktur
- Business Impact Analyse
- End Benutzer Monitoring
- Applikations und Datenbank Decodierung (L2-L7 Decodierung)
- Automatische Erkennung von Anomalien

Peter Rehle, ICS GmbH

15:30 - 16:15 Uhr
Technologien, die die nächsten Jahre beeinflussen werden und unsere Netzwerke und Infrastrukturen verändern werden
- Die Top-Technologien der nächsten Jahre
- Auswirkung auf Infrastrukturen
- Empfehlungen für die Vorbereitung, Planung und Investition sowie die zukünftige Nutzung

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

16:15 Uhr Abschließende Kaffeepause

Mittwoch, 22.04.2015

IPv6 Migration: Projekterfahrungen und -empfehlungen
- Organisation eines IPv6 Rollouts (Planung des Vorgehens, was muss wann entschieden werden, welche Abteilungen sind in welcher Projektphase gefordert, wo existiert Schulungsbedarf)
- Adresskonzept (Welche Alternativen stehen zur Verfügung, was sind die Vor- und Nachteile)
- Zuweisung von IPv6 Adressen (Welche Verfahren stehen zur Verfügung, wie integriert man Komponenten, die kein DHCPv6 unterstützen)
- Anforderungen an Netzwerk- und Infrastrukturkomponenten (Erstellung von Anforderungsprofilen für einzelne Komponenten, Testdurchführung, ausgewählte Testergebnisse)
- LAN-Archtitektur (Redundanzverfahren: VRRP, HSRP, Routing von IPv6, Umgang mit QoS bei IPv6)
- Migration der Internetpräsenz
- Migration von Anwendungen und Appliances
- Erstellung eines Anforderungskataloges für die Anschaffung von Hard- und Software
- Externe Anbindungen (WAN, Internet, Internet-VPN, Externe Partnerunternehmen)
- Security (Ergebnisse von Proxy-Tests, Firewalls & IDS, First-Hop-Security)

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH
Markus Schaub, ComConsult Study.tv

10:30 - 11:00 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause
15:30 Uhr Ende der Veranstaltung

Schwerpunktthema

Neue Ethernet Datenraten

Fortsetzung von Seite 1

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

Ethernet ist nun schon deutlich über 40 Jahre alt. Kein wirkliches Alter für eine Riesen-Schildkröte, aber außerordentlich beachtlich für eine Informations-Technologie, wo doch schon ein zwei Jahre altes Gerät im Verdacht steht, sich demnächst spontan zu zerlegen. Auf fast schon wundersame Weise hat es Ethernet geschafft, sich mit bezogen auf den Zeitraum eigentlich recht wenigen gravierenden Änderungen (wie z.B. der Entwicklung vom Shared Medium zum Switching) eher in den Stand einer Commodity, eines grundsätzlichen Versorgungssystems, hochzuarbeiten. Systeme zur Wasser- und Stromversorgung haben trotz aller zwischenzeitlichen technischen Neuerungen den erheblichen Charme, dem Nutzer gegenüber immer in der gleichen Form zu erscheinen, lediglich mit Unterschieden in der Leistung.

Und das ist auch das Geheimnis von Ethernet. Nicht die rohen Datenraten oder die teilweise verwegenen Zusatzprotokolle wie FCoE, sondern schlicht und ergreifend das Paketformat und die grundsätzliche Verarbeitung sind der Kern des Erfolges.

In den vergangenen Jahrzehnten hatten wir uns daran gewöhnt, dass es ab und an einen Leistungssprung um den Faktor 10 zu grob den dreifachen Kosten der aktuell bestehenden Leistungsstufe gab, also von 10 MbE auf Fast Ethernet, von Fast auf Gigabit Ethernet und von Gigabit auf 10 Gigabit Ethernet. Durch den Standard zu 40 und 100 GbE gab es in diesem System eine Unterbrechung. Anlass war, dass die Provider vor einigen Jahren gerne eine 40G-Technologie haben wollten und 100G ohnehin technisch noch außer Reichweite war. An privaten RZ-Netzen ging diese Diskussion ebenso vorbei wie die Weiterentwicklung der optischen Übertragungstechnik am Standard selbst.

Deshalb stehen wir heute in einer erneuten Diskussion um neue, andere Ethernet Datenraten. Aber nicht nur im Bereich zwischen 10 GbE und 100 GbE gibt es erhebliche Bewegungen, sondern auch im Access Bereich zwischen 1 GbE und 10 GbE. Durch die neue Generation WLANs mit IEEE 802.11 ac sind Access Points entstanden, die mehr als 1 GbE für ihren Anschluss benötigen. 10 GbE wäre für die Anbindung dieser APs aber viel zu teuer.

In diesem Artikel betrachten wir diese sehr neuen Entwicklungen nach dem aktuellen Stand dessen, was wir bereits darüber wissen. Wichtig ist dabei, dass es keinerlei fundamentale technische Probleme gibt, was bedeutet, dass die jetzt vorgeschlagenen Alternativen den Markt viel schneller erreichen können als im Rahmen einer länglichen herkömmlichen Standardisierung.

Bevor wir aber auf die einzelnen Alternativen eingehen, möchte ich einige Bemerkungen zur Struktur moderner Switch-ASICs machen, die für das Verständnis der Entwicklungen wesentlich sind.

1. Das Multi-Lane Konzept als Grundlage

Für die Konstruktion von Switch-ASICs, aber auch für die Implementierung vieler begleitender Funktionen wie Sicherheitsprüfungen oder Zähler oder Flow-Funktionen ist das Multi-Lane Konzept eine lebenswichtige Grundlage. Wir kennen seit Jahrzehnten Moore´s Law, das besagt, dass sich die Anzahl der auf einer Chipfläche verfügbaren Transistorfunktionen alle 18 bis 24 Monate verdoppelt. Darauf können wir uns auch in den nächsten Jahren verlassen. Allerdings steht nirgendwo, dass die immer kleiner werdenden Transistoren immer schneller werden. Es gibt unterschiedliche VLSI-Herstellungsprozesse. Der preisgünstige CMOS-Prozess, der seit vielen Jahren die Basis für alle Entwicklungen ist, führt zu Schaltungen, die sich mit höchstens rund 3 GHz takten lassen. Natürlich gibt es auch erheblich schnellere Techniken, die aber alle deutlich geringere Integrationsgrade und höhere Kosten nach sich ziehen. Deren Einsatz wird auf das absolut notwendige Minimum beschränkt.

Bei Prozessoren führt das einfach zu mehr Cores über die Zeit und ohne ein Betriebskonzept wie die Virtualisierung hätten alle Prozessor-Hersteller große Probleme, die vielen Cores noch sinnvoll zu nutzen. Bei Speicher ist es einfach nett, immer mehr Kapazität auf immer kleinere Flächen zu bringen, wobei jetzt aktuell ja auch die dritte Dimension erklimmt wird, was zu weiteren Optimierungen führt.

Aber seit dem Schritt von 1 GbE auf 10 GbE führen die beschriebenen Fakten zur Notwendigkeit, den Datenstrom zu Beginn eines Schaltkreises auseinander zu nehmen und am Ende wieder zusammen zu setzen, denn für die meisten Aufgaben einer Schaltung, die den Datenstrom manipulieren soll, muss anschaulich gesprochen die Schaltung schneller sein als der Datenstrom. Bei 10 GbE hat das dazu geführt, dass vier Lanes zu je 2,5 Gbit/s vorgesehen wurden, in die der Datenstrom zur Bearbeitung zerlegt wurde. Damit konnte man Schaltkreise verwenden, die im Bereich zwischen 2,6 ... 3,0 GHz getaktet wurden, wie es der preisgünstige CMOS-Prozess verlangt.

Im Standard IEEE 802.3 ba für 40 und 100 GbE wurde dieses Konzept verallgemeinert. Nach außen sehen wir z.B. bei 40(100) GBASE-SR die Möglichkeit, 40

Neue Ethernet Datenraten

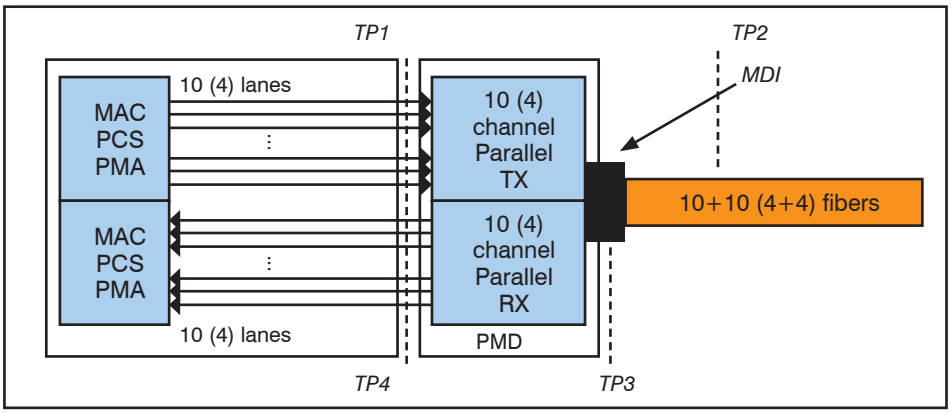


Abbildung 1: Konstruktion von 100 (40) GBASE-SR 10 (4)

definieren, in die die Lanes die Daten parallel ablegen können bzw. aus ihnen wieder aufnehmen. Der eigentliche Switching-Vorgang bewegt die Daten ja gar nicht, sondern ordnet nur den durch die Menge der zu einem Input-Port gehörenden Speicherzellen einen passenden Output-Port zu, das ist aber keine Manipulation mit Daten, sondern mit Adressen der Speicherzellen.

Es ist vielleicht dem einen oder anderen Leser aufgefallen, dass die aktuelle Generation der 40 G-Ethernet-Switches im Großen und Ganzen die gleiche L2-Switch-Latenz hat wie ihre 10G-Vorgänger. Solange nur geswitcht wird, ist es

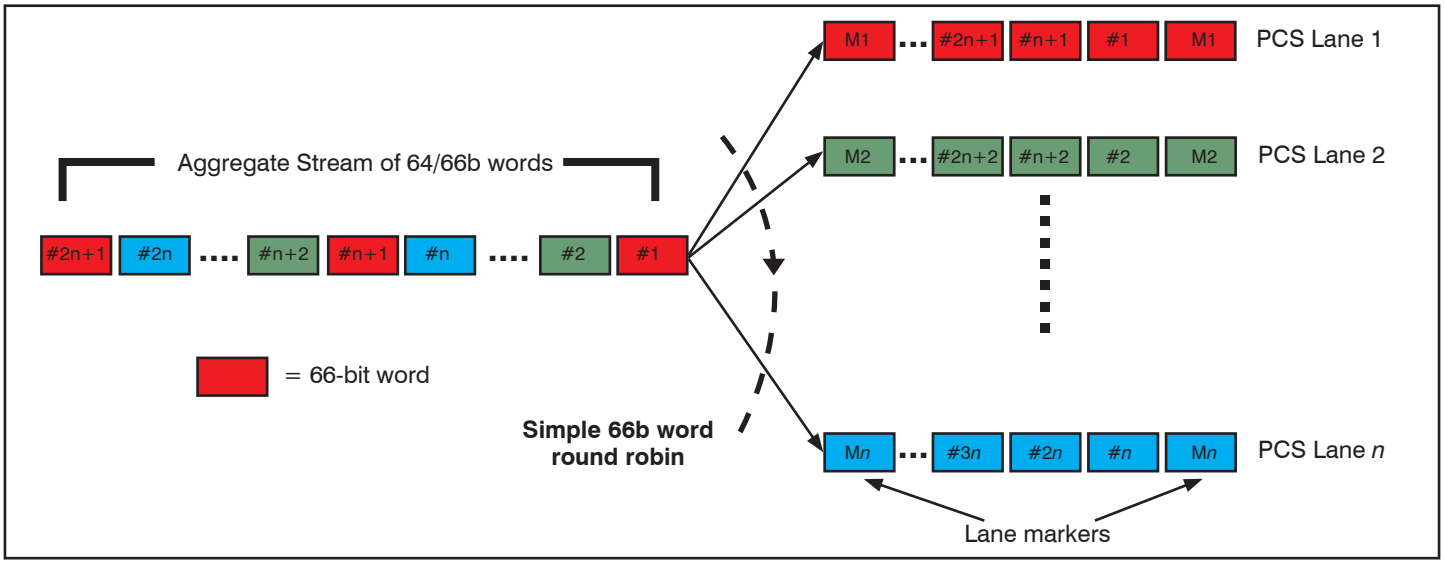


Abbildung 2: IEEE 802.3 ba PCS Lane Distribution Konzept

GbE auf vier und 100 GbE auf 10 Fasern zu implementieren. (siehe Abbildung 1)

Nach innen gibt es aber weitere Differenzierungen mit dem PCS (Physical Coding Sublayer) Distribution Konzept, welches einen Strom aus 64/66b-Worten durch Einfügung von Markern in praktisch beliebig viele Lanes zerlegen kann. (siehe Abbildung 2)

Hat man jetzt in einem Schaltkreis durch die konsequente Anwendung eines Bibliothekskonzeptes mit Modulen hinreichend viele parallele Schaltungen, ist es überhaupt kein Problem, z.B. einen 40 GbE Datenstrom in 16 Lanes á 2,5 Gbps zu zerlegen und diese Lanes dann in den entsprechenden Modulen weiter zu verarbeiten.

Die Einrichtungen zur Zerlegung und zum Wiederzusammenbau von Datenströmen heißen SerDes (Serialisierer/Deserialisierer). Bei der aktuellen Generation von Switch-ASICs kommt dann noch praktischerweise hinzu, dass diese mit Speichermanipulation arbeiten. Für die Implementierung eines Switching-Vorgangs muss man nur Speicherbereiche gleichgültig, ob 4 Lanes (für 10G) oder 16 Lanes (für 40G) parallel bearbeitet werden. Unterschiede gibt es natürlich bei der Bearbeitung von L3 oder noch

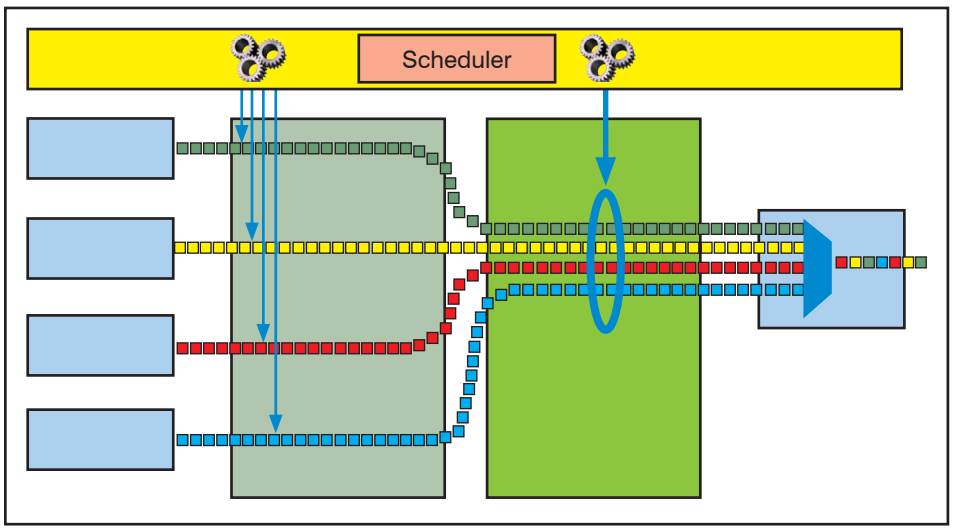


Abbildung 3: Zusatzfunktion Rate Conversion

höheren Funktionen, das hängt dann davon ab, wie viel Rechenleistung in Form paralleler Prozessoren im Switch Chip steckt.

Die aktuelle Switch-Generation auf der Basis von 40 G Switch-ASICs wie Broadcom Trident II ® oder Mellanox Switch-X ® ist deshalb auch großzügig hinsichtlich der Konfiguration. Ein Switch mit z.B. 48 40 GbE-Ports kann im Extrem auch so konfiguriert werden, dass er 192 10 GbE Ports hat. Und es kann sinnvolle Mischungen geben, wie z.B. 16 40 GbE Ports und 128 10 GbE Ports. Natürlich beherrschen die Switches dann Rate Conversion. (siehe Abbildung 3)

Die in diesem Abschnitt dargestellten Randbedingungen bilden das Umfeld für folgende Neuentwicklungen:

- Ethernet Access mit 2,5 und 5 Gbit/s
- 25 und 50 GbE für das RZ

Ethernet Access mit 2,5 und 5 Gbit/s. kann unmittelbar auf Basis sehr preiswerter 10 GbE-Switch-Chips implementiert werden. 25 und 50 GbE ergeben sich durch die bereits existierenden 100 G-Switch-ASICs. Diese haben einen sehr interessanten neuen technologischen Ansatz, den wir weiter unten vorstellen.

Was wird mit 40 GbE? Naja, das Schicksal dieser Datenrate kann man schon bei den Providern ablesen: sie haben zwar in diesem Jahr ein paar Prozent 40 G-Switches installiert, gehen aber jetzt sofort Richtung 100 G. Nach Ansicht von Marktforschern wird 40 G hier nicht mehr weiter ausgebaut. (siehe Abbildung 4)

Im RZ erwarte ich unterschiedliche Entwicklungen. Mega-RZs (wie Google, Amazon ...) sehen konstruktiv 25 und 50 G für die Serveranbindung vor, bei privaten RZs wird es entscheidend sein, ob z.B. mit 40 GBASE-T endlich eine für die Bedarfe eines RZs geeignete PHY-Variante auf den Markt kommt oder ob es bei den aktuellen Verwerfungen mit deutlich zu teuren Techniken bleibt.

2. Next Generation Enterprise BASE-T Access

Der Titel des im November 2014 bei IEEE 802.3 angeregten Call for Interest sagt direkt, worum es geht: Bereitstellung kostenoptimierter Verbindungen in Ethernet Access Netzen mit Datenraten zwischen 1 und 10 Gbit/s unter Nutzung strukturierter UTP-Verkabelungen. Es sollen neue MAC-Datenraten und PHY-Schnittstellen definiert werden, die sich unmittelbar aus der 10 GBASE-T PHY-

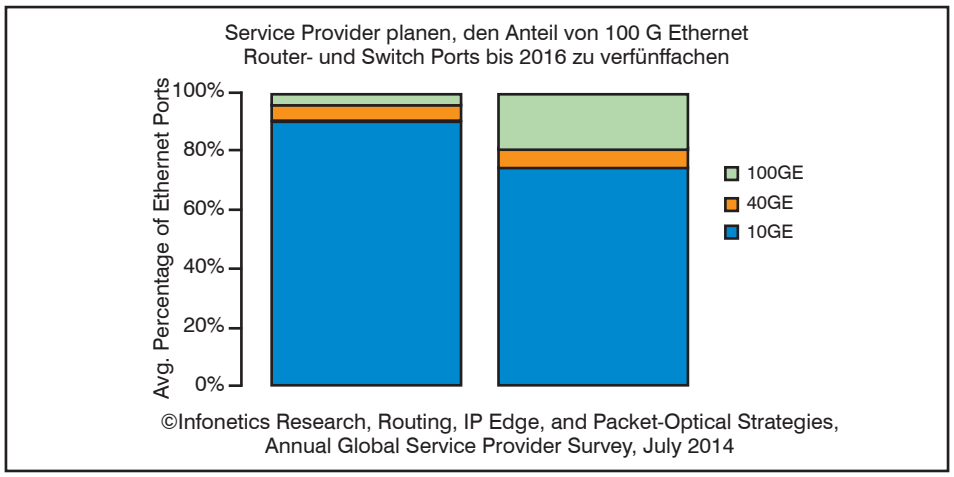


Abbildung 4: Service Provider planen ...

Technologie ergeben und die Datenraten über installierte strukturierte Verkabelung (z.B. 100 m über Cat 5e oder besser) optimieren.

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

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

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

Das wird aber nicht so bleiben, denn die „Wave 2"-Produkte befinden sich bereits in der Entwicklung. Sie werden dann auch 160 MHz-Kanäle, Multi-User MIMO und bis zu vier Spacial Streams haben.

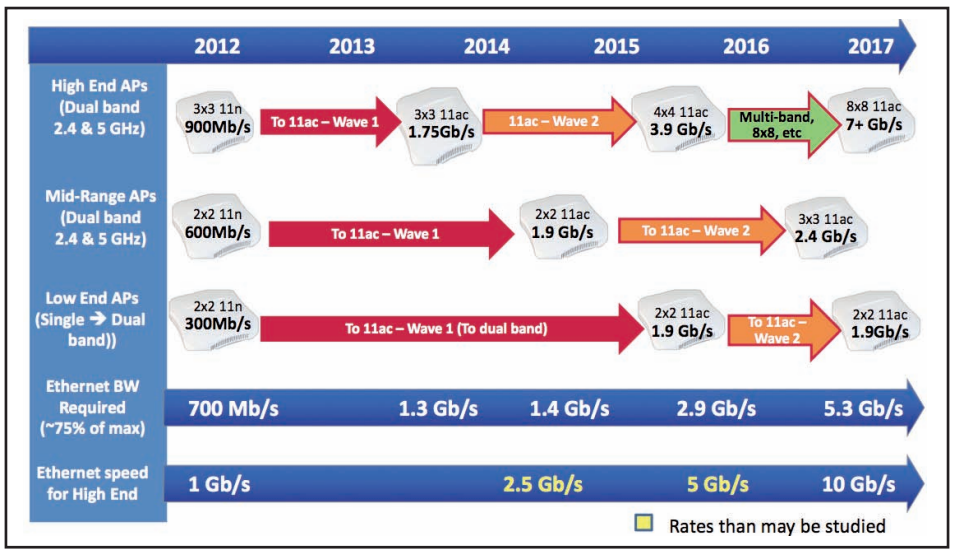


Abbildung 5: 802.11ac Enterprise AP Segmente und Trends

Eigentlich sind nur diese für eine wirkliche Leistungssteigerung verantwortlich, denn die 160 MHz-Kanäle kann man im Rahmen einer flächendeckenden WLAN-Planung nicht brauchen, weil man mindestens drei unterschiedliche Kanäle für ein störungsarmes 2D-Muster benötigt, womit es bei 80 MHz-Kanälen bleibt. Das MU-MIMO ist, wie ich mehrfach beschrieben habe, ein Verfahren, welches es ermöglicht, einen Teil der MIMO-Kanäle nur auf eine einzige Station zu konzentrieren, die damit deutlich mehr individuelle Leistung bekommt, was aber zu Lasten der anderen Stationen geht. Die Leistung einer Zelle wird dadurch also nicht erhöht, sondern nur anders verteilt.

Bei der CFI-Sitzung der IEEE war man der Ansicht, dass die Wave 2-Produkte innerhalb der nächsten 12 Monate zu Leistungsanforderungen im Bereich von 2 GbE für einen AP und innerhalb von 24 bis 36 Monaten zu Anforderungen im Bereich von 4 GbE für einen AP führen werden. Die Abbildung 5 zeigt eine weiter differenzierte Sicht.

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

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

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

Man kann jetzt schon konstatieren, dass 11ac den Markt schneller erobern wird als damals 11n. Wir haben schon nach 5 Quartalen der Auslieferung von Wave 1-Produkten einen Anteil von 21 % erreicht. Die Wave 2-Produkte werden bei geeigneter Planung den Unternehmen deutlich mehr Leistung bringen können als dies heute mit 11n möglich ist, auch wenn nach wie vor das DCF-Verfahren die Systeme ungünstig beeinflusst und in unnötiger Weise in der Leistungsentfaltung behindert. Noch wichtiger ist, dass die Akzeptanz von 11 ac bei den Endgeräten (Smartphones, Tablets, Notebooks, ...) fast schon als enorm bezeichnet werden kann. Innerhalb eines Zeitraums von weniger als fünf Jahren werden daher alle Endgeräte 11ac unterstützen, viele davon mit mehreren parallelen Spatial Streams.
Das Einzige, was dem Erfolg noch im Weg steht, ist die Anbindungsproblematik. Hier muss eine pragmatische, preiswerte Lösung auf den Tisch.

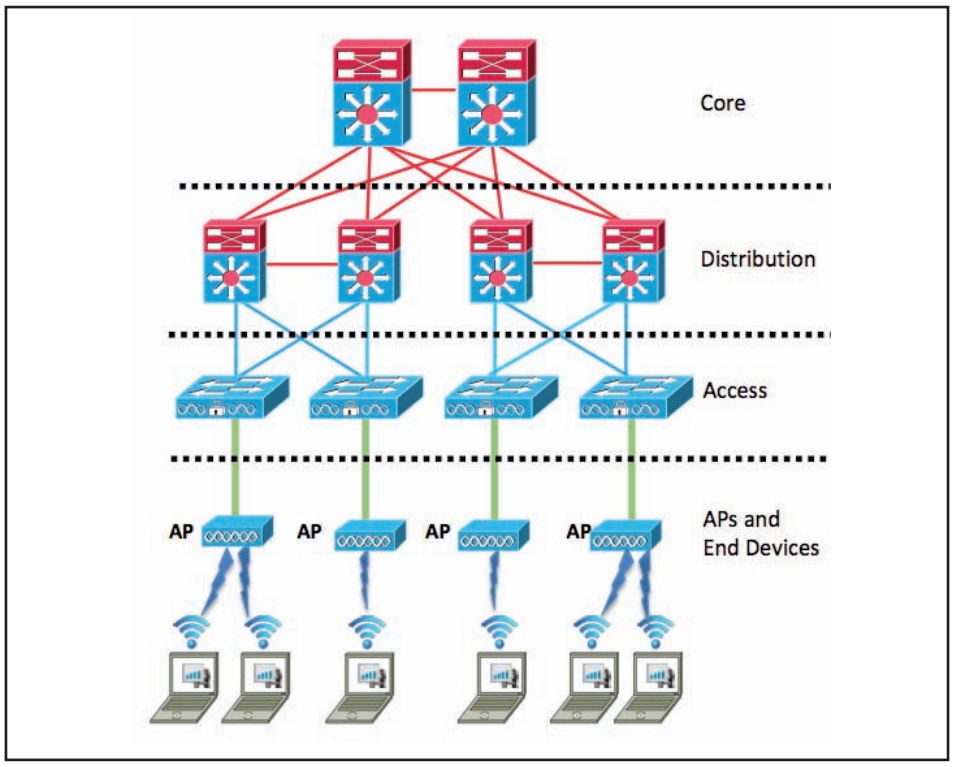
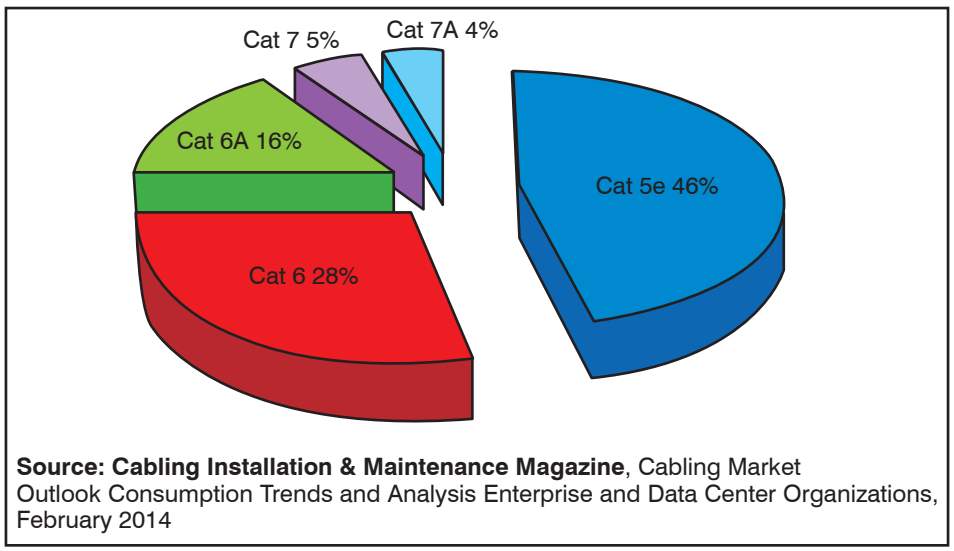


Abbildung 6: Struktur eines Campus-Netzes Quelle: IEEE 802 CFI

Noch schnellere WLANs sind allerdings zunächst nicht zu befürchten. Die im Mai 2014 neu gegründete Gruppe 802.11ax High Efficiency WLAN (HEW) gibt als Zieldatum das erste Halbjahr 2019 an.

Campus-Netze werden üblicherweise in einem dreilagigen Design aufgebaut, welches sich im Gegensatz zum RZ bewährt hat und auch in Zukunft kaum ändern wird (siehe Abbildung 6). Es geht bei diesem CFI ausschließlich um die „grünen“ Verbindungen zu den APs.

Für solche Initiativen ist es immer besonders spannend, welche Kabel denn nun in



Source: Cabling Installation & Maintenance Magazine, Cabling Market Outlook Consumption Trends and Analysis Enterprise and Data Center Organizations, February 2014

Abbildung 7: Kabeltypen in Campus-Netzen

der Realität verlegt wurden. Weltweit liegen hier Cat. 5 und 6-Verkabelungen vorne. (siehe Abbildung 7)

Nach vielen Gesprächen mit Kunden von ComConsult bin ich der Auffassung, dass die Verkabelung bei diesen statistisch in Richtung der qualitativ besseren Varianten verschoben sein wird, was sich sicher eher günstig auswirkt.

Ein Problem, das schon seit einiger Zeit heftig diskutiert wird, ist die Stromversorgung der Access Points. Bei den heutigen 1 GbE Access Switches ist man die bequeme PoE-Versorgung gewohnt. Für 10 GBASE-T ist aber überhaupt kein PoE definiert. Das liegt hauptsächlich daran, dass die Funktion von 10 GBASE-T durch eine Reihe aufeinander gestapelter nachrichtentechnischer Tricks realisiert wird. Ein Kabel, wie z.B. vom Typ 6A, ist nicht für die Übertragung von Strom-Leistung ausgelegt. Überträgt man dennoch wie heute üblich Versorgungsstrom auf solchen Leitungen, verändern sich ihre physikalischen Parameter. Sie werden z.B. bis zu 10 Grad wärmer, was durch die hohe Verlustleistung sofort einleuchtet. Das fällt aber nicht weiter auf, weil man eben heute nur 1 GBASE-T überträgt, ein vergleichsweise unempfindliches Signal. Es wird aber sicher möglich sein, einen Kompromiss mit Übertragungsraten von 2,5 oder 5 Gbit/s. bei gleichzeitiger Nutzung von PoE über solche Leitungen zu erzielen.

Wie sieht es mit der technischen Machbarkeit aus? Nun, die Industrie hat in den vergangenen Jahren schon mehrere Schnittstellen gezeigt, die zwischen 1 und 10 GbE liegen, also funktionieren wird es. Es gibt allerdings zwei mögliche Alternativen: Ausbau der 1 GbE PCS für schnellere Datenraten oder Nutzung einer 10 GbE 66/64 PCS, die man lediglich langsamer laufen lässt.

Generell muss man sagen, dass die „langsamere“ 10 GbE PCS die bessere Lösung ist. Für die 10 GBASE-T-Schnittstelle liegt eine große Menge von Erfahrungen, Berechnungen und Versuchen im Zusammenhang mit aktuellen Kabeltypen vor. Die 10-wertige Codierung (PAM 10) bei 10 GBASE-T führt zu einer besseren Ausnutzung des zur Verfügung stehenden Übertragungsfensters auf dem Kabel. 1000 BASE-T benötigt für die Übertragung eines Gigabits pro Sekunde aufgrund der fünfwertigen Codierung eine Bandbreite von 62,5 MHz. Würde man auf dieser Grundlage eine Übertragung von 2,5 Gbps implementieren, müsste man eine Bandbreite von 156,25 MHz bereitstellen. Leitet man die 2,5 GbE von 10 GBASE-T ab, kommt man dank der dichteren Codierung mit einer Bandbreite von 100 MHz aus. Und das macht z.B. einen deutlichen Unterschied bei der Nutzung von Cat 5e-Kabel, das ja bei einer Länge von maximal 100m im Rahmen einer strukturierten Verkabelung bis 100 MHz spezifiziert ist. Ein 5 GbE-System würde auf Basis einer verlangsamten 10 GBASE-T-Schnittstelle eine Bandbreite von 200 MHz benötigen und käme somit durchaus mit normalem Cat.6-Kabel aus. Und es geht ja bei solchen Überlegungen nicht nur um Kabel, sondern auch um Stecker und Patchfelder. Die Abbildung 8 zeigt nochmals die Zusammenhänge.

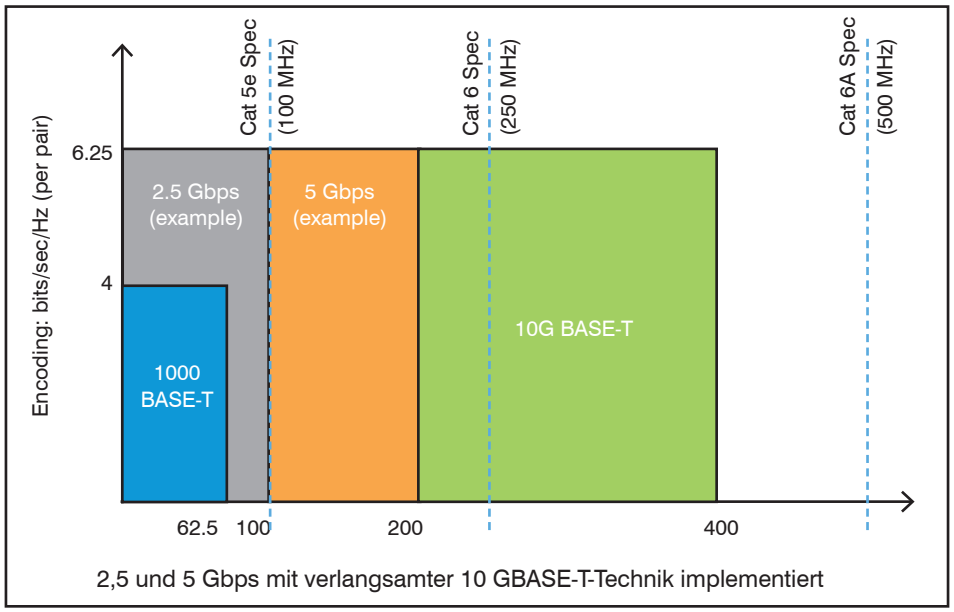


Abbildung 8: Frequenzbereiche für unterschiedliche PHYs

Blickt man auf die Darstellungen zum Multi-Lane-Konzept zurück, sieht man auch, dass die Nutzung einer verlangsamten 10 GBASE-T-Schnittstelle einfach mit nur einer oder zwei 2,5 Gbps-Lanes eine „natürliche“ Wahl ist.

Eine solche Lösung würde bei 2,5 Gbps sofort mit allen existierenden 5e, 6 und 6A-Verkabelungen funktionieren. Für 5 GbE auf dieser Basis können bei schlechteren Kabeln Längenbeschränkungen unter 100m für 5e eintreten. Üblicherweise haben die Hersteller aber Systeme geliefert, die die Spezifikationen der Standards teilweise weit übertroffen haben. Speziell in Deutschland können wir von einer günstigen Situation ausgehen.

Übrigens ist das alles nicht neu: schon 2003 wurde bei der Standardisierung von 10 GBASE-T über langsamere Datenraten gesprochen, allerdings eher aus Not,

weil man noch keine erweiterte Kabelspezifikation hatte, siehe (POW03).

Schließlich sollte man folgende Punkte nicht vergessen:

- Die Switch-Chips für 10 GbE sind mittlerweile recht preiswert geworden. Verteilt man die Ports so, dass man z.B. aus einem 10 GbE Port vier 2,5 GbE Ports macht, kommt man auf einen nur noch zweistelligen Portpreis.

- Die wesentlichen Kosten liegen in der Verkabelung. Wenn man also die bisher nur für die Anbindung von Endgeräten gedachte Verkabelung weitest gehend für die 11ac Access Points nutzen kann, entstehen erhebliche Kostenvorteile. Vor allem wird man bei fallender Zahl fest verkabelter Endgeräte irgendwann in das Problem laufen, die bestehende Verkabelung „beschäftigen“ zu wollen, damit diese Investition nicht unnütz herumliegt.

- Energy Efficient Ethernet ist für 1 und 10 GBASE-T verfügbar. Bei modernen Chips ist es eine serienmäßige Funktion, die natürlich auch für abgeleitete Datenraten zur Verfügung steht.

Noch ausstehend ist lediglich die Technik für PoE. Hier ergeben sich aber Möglichkeiten durch eine intelligentere Nutzung der einzelnen Drähte als bisher, z.B. mit PoE über vier statt bisher zwei Paare, siehe dazu Abbildung 9.

Die erste Sitzung der entsprechenden Interessengruppe ist im Januar 2015. Allerdings sollten sie auch nicht trödeln. Ein Hersteller wie Cisco könnte wegen der bereits komplett bestehenden Technologie im Handumdrehen entsprechende Lösungen für die eigenen Access Points auf den Markt bringen.

3. 100 G Switching

Mitte des Jahres 2014 hat sich mit der „25 Gigabit Alliance“ eine Interessengruppe gebildet, die 25 GbE und 50 GbE vor allem für den Serveranschluss voranbringen wollen.

Dies wird aber nur verständlich vor dem Hintergrund der neuen Technologien für 100 G-Switching, so dass wir zunächst den Blick auf dieses Thema lenken.

Es muss jedem Leser eigentlich intuitiv klar sein, dass die 40 GbE-Switch ASICs wie der Mellanox Switch X ® oder der Trident II ® von Broadcom eigentlich eine bereits veraltete Technologiegruppe repräsentieren. Es gibt sie prinzipiell schon seit drei oder vier Jahren, man hat damit

- Bei gleicher Last ist die Stromeinspeisung über 4 Paare effizienter als die über 2 Paare
- Mögliche höhere Leistung
- Mögliche Unterstützung von Po10GBASE-T
- Bewahrung der Rückwärtskompatibilität mit Clause 33

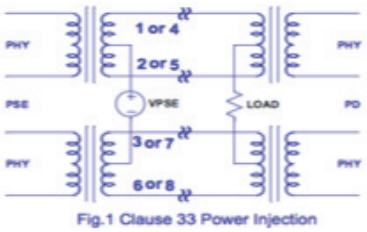


Fig.1 Clause 33 Power Injection

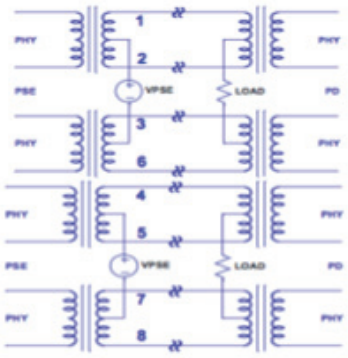


Fig.2 4-pair Power Injection

Abbildung 9: PoE über 4 Paare

gearbeitet und es gab bereits eine Reihe von Generationen. Außerdem hat man mit den Intel FM 7000 oder den Carrier Ethernet Switch Chips von Broadcom oder Marvell Erfahrungen damit gesammelt, was geschieht, wenn man höherwertige Funktionen von L3 und L4 bis hin zur automatischen Generierung von Tunnel Endpunkten implementiert. Diese Chips sind die Grundlage der aktuellen Generation von 40 GbE-Switches bis hin zu den 56 GbE Infiniband-Modellen von Mellanox.

Wie schon erwähnt, legen die Provider keinen großen Wert mehr auf 40 G. Für den Ausbau der Netze, vor allem vor dem Hintergrund von LTE, müssen stärkere Mittel her. Also gibt es schon seit einiger Zeit von führenden Herstellern passende 100 G-Switches, wie z.B. Cisco CRX-1, Juniper T-, MX-, EX-Reihen oder Arista 7500 E, letzterer ist durchaus auch für die Anwendung in Rechenzentren gedacht.

Sieht man aber genauer hin, ist das Design der Switches völlig anders als bei den monolithischen 40 G Switch ASICs. Aktuelle 100 G Switches arbeiten mit einem Kern für das Switching und Ingress bzw. Egress Modulen, die den Kern umgeben und all die Funktionen bereitstellen, die für die Manipulation der Datenpakete benutzt werden. Das hat den enormen Vorteil, dass man den Kern auf maximale L2-Leistung optimieren kann und bei der Gestaltung der Randmodule eine sehr hohe Flexibilität walten lassen kann. Grade in einer Provider-Umgebung kann es geerbte Schnittstellen geben, die man beim besten Willen nicht in ein Gesamt-Design einbringen kann. Die neuen Nexus 9000 Switches von Cisco arbeiten mit einem geteilten Design, aktuell aber noch bei 40G.

Abbildung 10 zeigt das Basisdesign, in diesem Fall mit einem Clos-Netz als Kern. Das Clos-Netz hat ja den Vorteil, dass

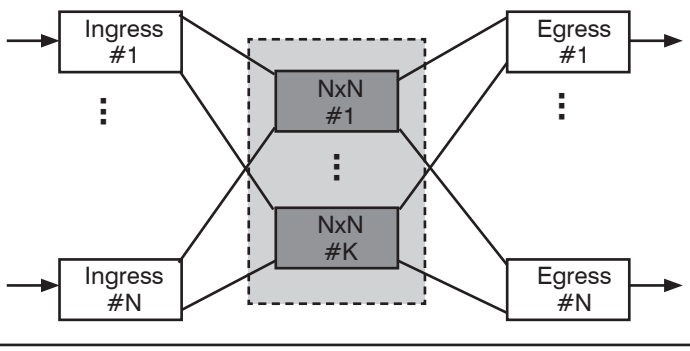


Abbildung 10: 100G-Switch Basis-Struktur

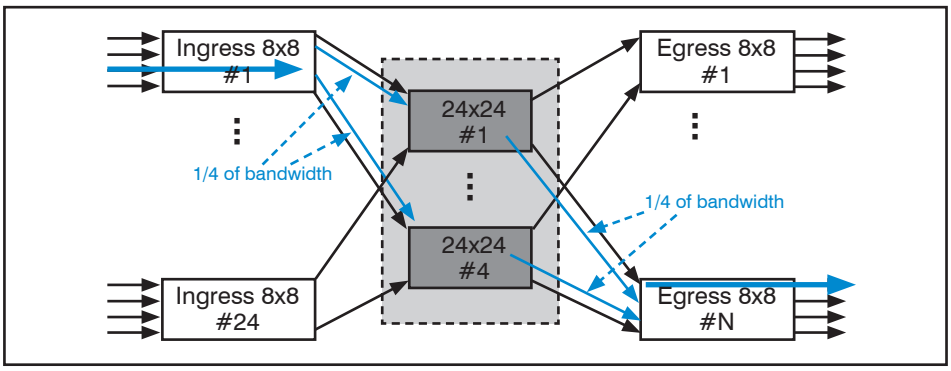


Abbildung 11: DUNE Clos Netzwerk mit dynamischem Routing

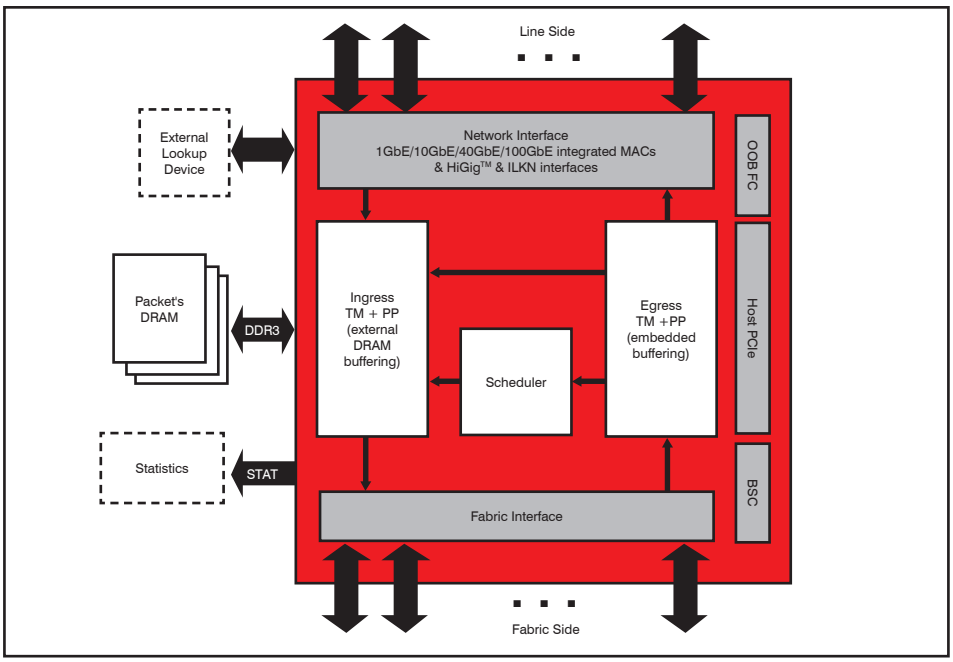


Abbildung 12: Broadcom BCM 88650 200 G Line Modul Quelle: Broadcom

man ein einmal bestehendes Switching-Basis-Element rekursiv wiederverwenden kann, wobei die Stufenzahl nur logarithmisch steigt.
Das Design geht zurück auf Arbeiten der Firma Dune, die von Broadcom gekauft wurde. Die wesentliche Leistungssteigerung eines Mehrstufen-Mehrfach-Verbindungsnetzwerkes nach Clos geschieht durch dynamisches Routing, welches es ermöglicht, einen Datenstrom auch in parallelen Wegen durch den Switching-Kern zu führen (siehe Abbildung 11). Das harmonisiert natürlich optimal mit dem Multi-Lane-Konzept und erlaubt einen praktisch beliebige Parallelisierung des Kerns, durchaus auch in der Größenordnung von 10, 20 oder 40 parallelen Lanes.
Was wir jetzt noch brauchen, ist ein passendes Line Modul. Das gibt es auch schon seit ein paar Monaten, wir zeigen in Bild 12 direkt das 200 G-Modul, was man ja für Vollduplex braucht. Es besitzt eine sehr flexible Netzwerk-Schnittstelle für verschiedene Datenraten, auf der anderen Seite natürlich ein passendes Fabric Interface und dazwischen wenig überraschend Puffer und Scheduler sowie Schnittstellen zu externen Funktonseinheiten. Für 100 G-Switches ist es natürlich wichtig, viel Speicher bereitstellen zu können und der gehört rein strategisch nicht direkt auf das Modul, weil man ihn dann nicht flexibel genug gestalten kann. Da ist eine DDR3-Schnittstelle nach außen schon besser. Ein weiterer Punkt ist die mögliche Anbindung von Prozessorleistung für die unterschiedlichsten Zwecke mit dem Host PCIe-Interface.

Man sieht also ganz klar die Tendenz dieses Herstellers, den bisherigen Kunden eher die Elemente eines Bausatzes für einen 100 G-Switch als ein fertiges Design zu liefern. Das ändert sich jetzt aber: mit dem Tomahawk bietet Broadcom einen monolithischen Switch ASIC für 25/50 und 100 GbE an, der die Nachfolgegeneration des Trident einläutet.

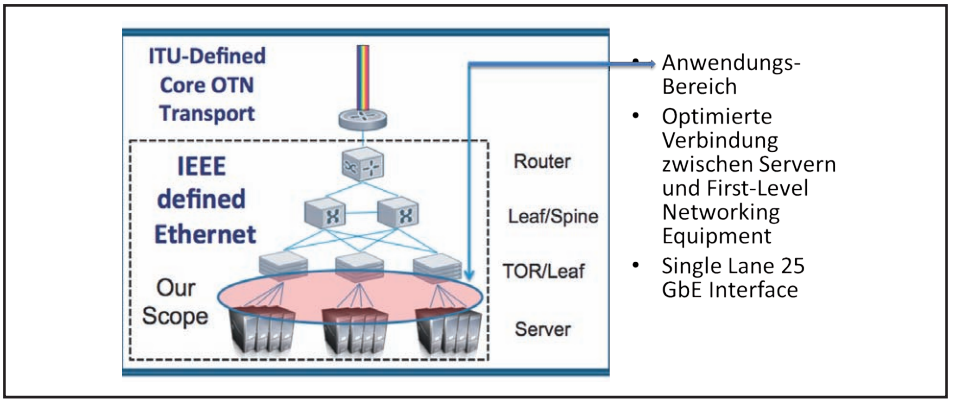


Abbildung 13: Anwendungsbereich für 25 GbE

4. 25 und 50 GbE

Vor einigen Monaten hat sich das „25 Gigabit Ethernet Consortium“ gebildet, www.25gethernet.org. Die Initiatoren Google, Microsoft, Arista, Broadcom und Mellanox wollen mit dieser Industrie-Vereinigung innerhalb von IEEE 802 die Entwicklung eines Standards für 25 und 50 GbE vorantreiben. Unterstützer sind Hersteller wie Brocade, Cisco, Dell, Qlogic, Cadence und weitere.

Ansatz ist hier die Optimierung und Erhöhung der Effizienz des Anschlusses von Servern durch die unmittelbare Nutzung der Lane-Technologie in harmonischer Teilung von 100 G mit 25 G Single Lanes. Primäre Anwendungsbereiche sind Web-Scale Rechenzentren und Cloud Service Provider. Es geht hauptsächlich um die Verbindungen zwischen Servern und der ersten Stufe des Netzwerks. (siehe auch Abbildung 13)

Was sind nun technische Gründe für 25 G?

Zunächst greift man die aktuelle Anschlussproblematik auf. Primäres Ziel der Arbeitsgruppe sind Techniken für den Anschluss von Servern an ToR-Switches, also

zunächst kurze Strecken. Bei 40 G gibt es ja dafür den Twinax-Standard 40 GBASE-CX mit einer maximalen Übertragungsdistanz von 7m. Aber, muss es 40 G sein?

Intel x86 CPUs verbessern sich in I/O-Funktionalität und Geschwindigkeit. Hier ist 10 GbE nicht mehr schnell genug. Natürlich könnte man auf die Idee kommen, Link Aggregierung zu nutzen. Für einen Server-Block würde alleine die Aufrüstung von 10 auf 20 GbE doppelt so viele notwendige Ports in den ToR-Switches, doppelt so viele Stecker und NICs und doppelt so viele Leitungen bedeuten, ganz abgesehen von der Notwendigkeit, in die Uplinks ebenfalls mehr Leistung zu geben, um die Überbuchung nicht zu übertreiben. Wie gesagt, bei einem oder zwei Servern kann man das machen, aber nicht in einer Server Farm z.B. eines Cloud Providers. Prozessoren der nächsten Generation der Intel „Grantley“ CPUs werden im dritten Quartal 2014 ausgeliefert und Server, die mit ihnen ausgestattet sind, kommen mit 10 GbE nicht mehr aus. Die versteckten Kosten einer Lösung mit Link Aggregierung sind auch bei sehr günstigen 10 GbE Portpreisen viel zu hoch, weil eine Verdopplung der Ethernet Switches ja auch entsprechende Kosten in Platz- und Strombedarf sowie in der Kühlung nach sich zieht.

Eine 40 GbE-Lösung für diesen Zweck ist aber völlig übertrieben. Hier würde man für sehr viel Geld Überkapazitäten aufbauen, die man in den nächsten 1 oder 2 Jahren nicht benötigt.

Die aktuellen 40 GbE-Switch-ASICs sind überdies in 2 bis 3 Jahren, wenn die größere Menge der Intel E7-Prozessoren über die Netze hereinbricht, bereits 5 bis 6 Jahre alt! Sie zerfallen dann noch nicht spontan zu Staub, sollten sie aber besser, denn es gibt schon länger 100 GbE Switch-ASICs, die ersten werden sogar bereits verbaut. Im letzten Abschnitt hatten wir die Entwicklung ja bereits dargestellt. Mellanox hat vor wenigen Wochen mit dem Switch X-3 ® einen 100 G Infiniband Switch-ASIC vorgestellt. Es gibt keinen Grund, warum er nicht genau wie seine Vorgänger Ethernet einfach nachmachen kann. Und auf den Tomahawk von Broadcom kommen wir noch.

Von den vielen möglichen Varianten bei 100 G greifen wir jetzt die heraus, die für das RZ am besten brauchbar ist, nämlich mit 4 Lanes zu je 25 Gbit/s. über Fiber oder Kupfer. Einsteckbare Transceiver Module mit kompakten Form Faktoren, wie dem C-Form Faktor (SFP/CFP) haben vier VCSELs, die jeweils mit 25 Gbit/s. arbeiten. Für jede Lane braucht man ein SerDes-Chipset.

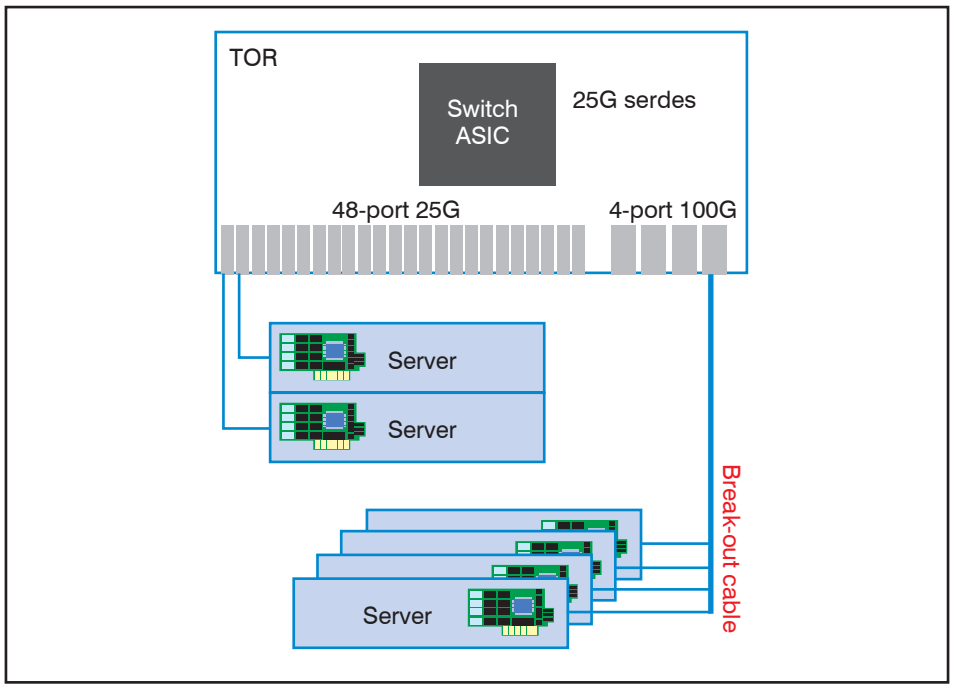


Abbildung 14: 25 GbE Anschluss

In Abbildung 14 sehen wir, dass der ToR-Switch auf einer 100 G Switching Architektur basiert und somit 100 G und 25 G-Ports unterstützt. Die Topologie ist ganz ähnlich wie bei 10 oder 40 GbE. Man kann 25 GbE Ports einzeln mit SFP28 oder mit einem QUAD 25 Gb/s QSFP28 Breakout implementieren. Das optimiert Ports und Bandbreite in der ToR Steckerfläche und unterstützt höhere Dichte in den Racks.

Der 25 GbE-Standard wird die gleiche physikalische Chipstruktur wie eine einzelne 25 Gbit/s Lane haben. Das vereinfacht den Herstellungsprozess, es müssen nur einige kleinere Änderungen in der Vorwärts-Fehlerkontrolle und dem Lane-Alignment gemacht werden. Die Herstellungskosten sind aber geringer als für 40 GbE.

Und damit sind wir beim wesentlichen Faktor: den Kosten. 25 GbE wird einen ordentlichen Leistungsgewinn gegenüber 10 GbE haben, dabei aber die geringsten Kosten aller möglichen anderen Alternativen aufweisen. Anshul Sadana, Senior Vize-Präsident bei Arista Networks erwartet für die erste Generation von 25 GbE die 2,5-fache Leistung zum 1,5-fachen Preis gegenüber 10 GbE. In der zweiten Generation werden seiner Ansicht nach die Preise für 10 GbE und 25 GbE gleich sein, wobei 25 GbE eben die 2,5 fache Leistung hat. Das entspricht eher dem alten Ethernet-Versprechen bei Generationen-Übergängen. Bei 100 M auf 1 G und 1 G auf 10 G wurde mittelfristig immer die zehnfache Leistung zum dreifachen Preis erreicht. Die Mehrleistung kann ohne Erhöhung der Betriebskosten gefahren werden, weil sich die Anzahl der Komponenten ja nicht erhöht.

Das 25 Gigabit Ethernet Consortium wurde gegründet, um die Arbeit von IEEE zu beschleunigen, die ja, wie wir wissen, notorisch langsam sind und viel zu oft von der Realität überholt werden. Das Consortium steht in einer Reihe mit der Ethernet Alliance, dem Metro Ethernet Forum oder auch WiFi, die ja alle dafür gesorgt haben, dass aus den IEEE-Ansätzen irgendwann etwas Funktionsfähiges wurde.

Google und Microsoft sind wichtige Schwergewichte in der 25 GbE-Gruppe. Von Arista ist bekannt, dass sie sowohl Google als auch Microsoft mit Technologie einschließlich der Mellanox-Adapter versorgen. Der Standard wird keine Verkabelungssysteme definieren, sondern die Hersteller entscheiden, was sie unterstützen wollen. Aus Kostengründen werden das zunächst primär Twinax-Kabel sein, da kann man sich auch noch die optischen Transceiver sparen, aber optische Verbindungen sind natürlich nicht ausgeschlossen. Hier kann man sich bestehender 10G-Technik bedienen. Hinreichend leistungsfähige VCSELs und PINs in den Transceivern vorausgesetzt, kann man durchaus die alte Milchmädchenrechnung bei Fasern über das Bandbreite/Reichweite Verhältnis anwenden: eine 10G Lösung, die mit einer Faser/Steckerkombi über 100 m funktioniert, wird mit der gleichen Faser über bis zu 40m auch 25 G übertragen können.

Ohne hier jetzt tiefer zu gehen: durch die Integration optischer Elemente „funktioniert“ Moore´s Law auch bei der Elektronik hinter optischen Übertragungssystemen. Die Erwartung, dass ein 25G-Transceiver in 2 Jahren nicht mehr kostet als ein 10 G-Transceiver ist völlig berechtigt. Der 10 G-Transceiver sinkt allerdings nicht mehr im Preis, wenn er nicht weiter mit multiplen Strukturen wachsen kann.

Bei der Entwicklung des Standards zu 40 und 100 GbE gab es ja schon um 2005 größere Diskussionen hinsichtlich 40 und 25 GbE. Damals hat sich IEEE für die 40 GbE-Variante entschieden, die ganz klar durch den Bedarf von Providern für Fernstrecken gekennzeichnet ist und ja dort auch zu respektablen Lösungen geführt hat. Die Provider arbeiten jetzt an der flächigen Einführung von 100 G oder mehr. Das Aufkommen von Cloud Service Providern hat aber gegenüber damals die Landschaft für den Einsatz von Ethernet-Varianten mit mehr als 10 GbE innerhalb von RZs massiv verändert. Hier möchte man unkomplizierte Hochgeschwindigkeitskommunikation zu günstigen Preisen.

Auch wenn wir das in diesen Medien kaum verfolgen, die wirklichen technischen Fortschritte gab es bei 100 G, sowohl in der Übertragungstechnik als auch beim Switching. Eine erhöhte Produktion integrierter VCSELs und anderer optischer Komponenten führt zu günstigen Preisen. Es ist durchaus eine sehr nahe liegende Idee, auf dem Weg von 10 G zu 100 G im RZ keine artfremde Technologie zu verwenden, sondern bereits vorliegende, erfolgreiche Elemente der 100 G-Technologie in anderer Weise zu verwenden. So kommt man natürlich auch sehr einfach zu 50 G, auch wenn es momentan nicht benötigt wird.

5. In Deckung: Tomahawk kommt

Broadcom nennt seine Switch-Chips gerne nach US-Kampf-Flugkörpern. Tomahawk kann man sich aber auch besser merken als den offiziellen Namen BCM 56960 Strata XGS® für die mit dem Tomahawk Switch-ASIC gebauten 100 G-Switches. Tomahawk ist der Nachfolger des Trident II und setzt selbst für den erfahrenen Chip-Fan neue Maßstäbe. Schon jetzt ist der Hersteller mit seinen Trident und Dune ASIC-Familien ein dominanter Anbieter auf diesem Sektor. Es gibt aber einen harten Wettbewerb mit Firmen wie Intel oder Marvell und die Tendenz mancher Netzwerk-Komponenten Hersteller wie Cisco oder HP, Switch-ASICs selbst herzustellen. Außerdem gibt es auch neue Chip-Maker wie XPliant, die mit ihrer

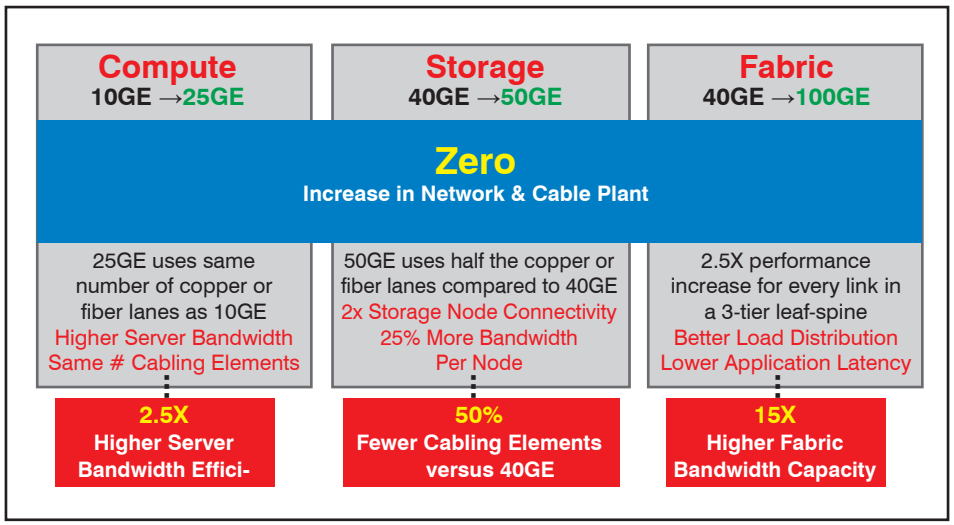


Abbildung 15: Verbesserungen durch 25/50/100 G Quelle: Broadcom

CNX-Familie von Switch ASICs plötzlich aus dem Nichts aufgetaucht sind und im Markt für 25 und 100 G mitmischen. Die aktuelle Anforderung von Betreibern von Hyperscale-RZs ist schlicht und ergreifend kostengünstiges schnelleres Networking für ihre Abertausende Server. Mit der 25GbE Alliance haben diese Anwender zusammen mit dem Netzwerk-Hersteller Arista den Willen gezeigt, zur Not selbst einen Standard zu formulieren, wenn IEEE dazu unfähig sein sollte.

Bei diesen Anwendern ist es eigentlich schon längst klar, dass die immer höheren Core-Zahlen bei Prozessoren und auf Servern basierenden Speicher-Arrays die 10 GbE-Ports, die zu den Servern führen, schnell überlasten. Bei großen Rechenzentren, Unternehmen, Hyperscale-Konstrukten und Cloud Service Providern macht das Netzwerk rund 10 bis 15% der Gesamtkosten aus. Daher suchen sie alle ein besseres Preis/Leistungsverhältnis als bisher. Ein 25 GbE-Port wird zu Beginn im Vergleich zu einem 10 GbE-Port das 1,5-fache kosten, die 2,5-fache Bandbreite haben, nur die Hälfte Strom verbrauchen und so eine höhere Portdichte ermöglichen. Es ist auch schon das Problem aufgetreten, dass Unternehmen nicht so viele Geräte an ein Netz bringen konnten, wie sie eigentlich vorhatten. Kunden möchten Netzwerk-weite Analyse-Funktionen, um das Verhalten ihres Netzes besser zu verstehen, damit die Congestion im Netz keine Anwendungen abmurkst. Es nützt gar nichts, wenn man alle Rechen- und Speicherkapazität der Welt hat, aber nicht genügend Bandbreite für moderne, hochgradig verteilte Workloads bereitsteht. Die Idee hinter den ganzen Initiativen ist, nach wie vor nur rund 10 bis 15% des Gesamtbudgets für das

Netz auszugeben, dafür aber einen überproportionalen positiven Effekt auf die Anwendungen zu bekommen.

Tomahawk wurde entworfen, um genau diese Problembereiche abzudecken. Der Trident Chip hat maximal 128 SerDes-Schaltungen, die auf 10 GHz laufen und die man zu (bis zu 128) 10 GbE- oder (bis zu 32) 40 GbE-Switch-Ports (oder gemischt) konfigurieren kann. Der Tomahawk hat ein neues SerDes, welches mit 25 GHz getaktet ist und welches man dann zu 25, 50 oder 100 GbE Switch-Ports konfigurieren kann. Das neue SerDes mit dem Namen „Long Reach“ ist hinsichtlich Bandbreite, Skalierbarkeit und geringer Latenz optimiert. Der Tomahawk-Chip kann eine Ende-zu-Ende-Latenz zwischen zwei Ports von 400 ns garantieren und hat 680 Mb für das Puffern von Paketen.

Im Gegensatz zu den weiter oben beschriebenen 100 G Switch-Konfigurationen ist der Tomahawk ein einzelner monolithischer Chip mit über 7 Milliarden Transistoren. Damit schlägt er sogar den neuen 18-Core Xeon ® E5 2600 v3 Prozessor Intel, der „nur“ 5,57 Milliarden Transistoren besitzt. Noch vor zehn Jahren brauchte Broadcom neun Chips, um einen 8-Port 10 GbE-Switch zu bauen. Das ist Moore´s Law! Der Tomahawk-ASIC kann bis zu 3,2 Tb/sec im Vollduplex schalten, knapp dreimal so viel wie der Trident II mit seinen 1,28 Tb/sec. Wichtig ist auch, dass sich Switches, die mit dem neuen Tomahawk ausgestattet sind, nahtlos in die bestehende Verkabelungs-Infrastruktur einfügen und dennoch erhebliche Leistungssteigerungen für Links zu Servern und Speichern sowie über Fabrics hinweg erzeugen. Die Abbildung 15 fasst die Unterschiede zwischen 10/40G und 25/50/100G-Lösungen zusammen.

Die so genannte „God Box“-Version eines Tomahawk-Switches ist ein Gerät mit 32 100 GbE-Ports. Damit kann man natürlich auch bestehende dreistufige Leaf/Spine-Konfigurationen, die auf 10 und 40 GbE basieren, zum großen Teil oder sogar komplett ablösen. Es ist allerdings immer die Frage, ob sich das lohnt, weil die „God Box“ mindestens zu Beginn nicht grade ein Schnäppchen sein wird. Andere Konfigurationen wären 64 Ports zu 40 oder 50 Gbit/s oder 128 Ports zu 25 Gbit/s oder eben auch praktische Mischungen. Der Chip unterstützt neben vielen anderen Protokollen auch RoCE und RoCE v2, die Remote Direct Memeory Access Technologie aus InfiniBand, die ja damit auf Converged Ethernet portiert wurde. Vor über zwei Jahren hatte ich schon einmal einen Artikel über die hervorragende Eignung dieser Protokolle für die Implementierung hochdynamischer virtueller Umgebungen geschrieben und bis heute gibt es weit und breit kein Verfahren, das die VM-Migration wirkungsvoller unterstützt. Nachdem Broadcom ja schon früher einen Chip herausgebracht hat, der Tunnel-Protokolle direkt implementiert, ist es nicht verwunderlich, dass der Tomahawk VXLAN und NVGRE unterstützt, natürlich aber auch MPLS und SPB. Der Tomahawk ASIC ist seit Q4/14 in den OEM-Laboren und sicherlich auch bei dem einen oder anderen besonders interessierten Großanwender.

Der Software-Stack, der mit den Tomahawk-Chips kommt, umfasst die sog. „Broadview“-Instrumentierung, die die Pakete nachverfolgt und den Paketfluss in und um die Fabric herum sichtbar macht. Die Software besitzt verschiedene eingebaute Analyse-Routinen für Congestion und Hashing, Monitore für Load Balancing und die Erkennung von „Elefanten“ (unregelmäßig auftretende große Datenmengen, die andere Flows unterbrechen können), Puffer-Zuständen, Timing und aktuellen Leistungsreserven in der Fabric. Wenn Broadview die Vorgänge im Netzwerk beobachtet und analysiert, ist die FlexGS-Engine in der Software die Stelle, die diese Daten hernimmt und den Verkehrsfluss über die Datenebene optimiert. Das ist ein automatisches Traffic Shaping, was nach Aussage des Herstellers dabei hilft, aus dem Netz eine optimale Leistung zu beziehen.

Je schneller Switch-ASICs werden, umso wichtiger sind derartige Automatismen. Das ist genau die Art von Software, die Google & Co für ihre White Box-Netze geschrieben haben, als in dieser Richtung kommerziell noch nichts kommerziell verfügbar war. Die Broadcom Software hat verschiedene Anbindungsmöglichkeiten an SDN-Stacks, zu Cloud Controllern wie OpenStack, Automationstools wie Chef und Puppet und natürlich den Netzwerk-Betriebssystemen, die auf der Broadcom Switch Produktlinie laufen. Es ist für uns nicht möglich abzuschätzen, wie lange die Umarbeitung einer bisherigen Trident-Betriebssoftware auf den Tomahawk dauert. Allerdings sollten die Hersteller von Adapterkarten eiligst an 25G-Varianten gehen.

6. Konsequenzen

Die Konsequenzen für den ersten Teil des Artikels sind unstrittig und sehr angenehm. Die 2,5 und 5 GbE-Varianten sind letztlich Kosmetik-Creme für die Stirnfalten der geplagten WLAN-Planer, die bislang annehmen mussten, im schlimmsten Falle eine durchgängige 10 GbE-Versorgung für die WLAN-APs vornehmen zu müssen. Es gab aber auch einige Experten, die die Möglichkeiten von 11ac überbewertet haben. Das Ganze hat sich beruhigt und es wird im passenden Zeitraum, wenn die APs der zweiten Produktwelle kommen, passende Lösungen geben, die überwiegend auf der bisherigen Endgeräteverkabelung laufen. Es bleibt dann eigentlich nur noch die Frage, ob man das Ganze nach einem IEEE-Standard aufbaut oder die Lösung nimmt, die der Hersteller der APs mit anbietet, sofern er das macht.

Bei den 25 und 50 GbE Varianten müssen wir eigentlich abwarten, ob tatsächlich auch Produkte für normale Betreiber zu interessanten Preisen angeboten werden oder nicht. Die Lage bei 40 GbE ist nicht grade prickelnd für die Betreiber von privaten RZs, weil es bis zum heutigen Tage keine wirklich passende Alternative für das physikalische Übertragungssystem gibt. 40 GBASE-SR4 leistet eigentlich zu viel, ist damit zu teuer und überdies technisch veraltet, die MPO-Verkabelung ist eine Katastrophe und 40 GBASE-T ist noch nicht fertig. Das werde ich in einem anderen Artikel behandeln.

Aber leider ist es nicht so einfach. Die Bewertung einer möglichen Lösung hängt nämlich maßgeblich vom generellen Konstruktionskonzept des RZ-Netzes ab.

RZ-Netze mit ToR-Switches benötigen nur sehr kurze Verbindungen zwischen Servern und dem ToR-Switch, so dass hier die bestehenden Kupfervarianten ausreichen. Der Nachteil ist, dass die ToR-Switches ja selbst wieder irgendwo angeschlossen werden müssen und dann haben wir recht viele längere Verbindungen. Für dichte Umgebungen mit starken und/oder vielen Servern ist das Konzept der 25/50/100-Switches auf Basis z.B. eines Tomahawk unstrittig erheblich besser als die Variante 10/40/100.

RZ-Netze mit EoR- oder MoR-Switches, die also auf ToR-Switches verzichten, brauchen die Unterstützung längerer Distanzen, z.B. 15, 20 oder 30 m. Genau dafür wäre 40 GBASE-T optimal. Die 25/50-Fraktion möchte bestehende Verkabelungen benutzen (das wird ja offen gesagt). Bei kurzen Strecken ist das kein Problem, bei längeren Distanzen, wie sie in einem EoR- oder MoR-Design auftreten, schon. Die 25/50 Alliance möchte die ToR-Switches verbilligen, am billigsten sind aber gar keine ToR-Switches. Persönlich hält der Autor das ToR-Design für ein Relikt aus einer Zeit, als es nicht anders ging. Die Hyperscale-Betreiber wechseln ihre Geräte systematisch und schnell aus. Der Betreiber eines privaten RZ-Netzes wird längere Betriebszeiten wünschen. Dafür benötigt

man ein entsprechend stabiles Design.

RZ-Netze mit Disaggregation z.B. nach der Intel Rack Scale Architektur mit kooperierenden Processing-Feldern benötigen weder ToR- noch EoR- oder MoR-Switches, weil deren Funktionen direkt von den in die Prozessoren integrierten Switching Fabrics erledigt werden. Dieses Konzept aus dem HPC-Bereich kommt früher oder später auch zu „normalen" RZs. Dann sind normale 25, 40 und 50 GbE-Switches ohnehin gleichermaßen Elektronikschrott.

Ganz fein raus sind natürlich all jene, die heute und auch in einem oder zwei Jahren keine Engpässe durch 10 GbE haben, einfach weil ihre Anwendungen noch bescheiden genug sind und auf Servern laufen, die sich bei der I/O-Performance zurückhalten, denn in der Zukunft liegen durchaus erhebliche Unsicherheiten hinsichtlich möglicher Kommunikations-Architekturen im RZ.

Der Tomahawk wird „irgendwann" in diesem Jahr in den Verkauf kommen, aber ich schätze, es ist dann nicht der einzige Kandidat. Etwa für den gleichen Zeitraum hat XPliant seine neuen Chips in Aussicht gestellt, Mellanox wird auch nicht länger benötigen, um dem bestehenden 100 G InfiniBand-Switch ASIC auch Ethernet beizubringen und es wird sicherlich noch der eine oder andere Hersteller zusätzlich aus dem Unterholz springen und neue 25/40/50/100 Switch-ASICs vorstellen. Die einzige Ausnahme, die ich hier erwarte, ist Intel. Zum einen hat Intel eine enge Zusammenarbeit mit Mellanox, das sieht man an den Xeon-Phi®-Systemen für HPC, zum anderen, möchte ja Intel den Prozessoren selbst Switching-Fähigkeiten geben, so dass im Rahmen der Rack Scale Architektur Switches herkömmlicher Bauart überflüssig werden.

Statt aber über zu viele Alternativen zu klagen, möchte ich zum Ende besonders herausstellen, dass es noch zu keiner Zeit eine so große Vielfalt an Ethernet-Schnittstellen bzw. Datenraten gegeben hat, die der aufmerksame Betreiber zu genau dem System zusammenstellen kann, was am besten zu ihm passt. Die Zeiten der breiten Verkündigung allgemeiner Wahrheiten sind effektiv vorbei, was zählt sind Information und Flexibilität vor dem Hintergrund des Entwurfs möglichst optimaler Lösungen.

Literatur

(POW03) Powell, Scott „Feasibility Study on High Speed Transmission over UTP Cables, IEEE Meeting July 2003, http://www.ieee802.org/3/10GBT/public/jul03/powell_2_0703.pdf

Standpunkt

Neue Sicherheitsarchitekturen mit Software-Defined Security

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

Die Informationssicherheit ist seit Jahren von einem scheinbar ehernen Prinzip geprägt: Der strikten Trennung zwischen innen (der vertrauenswürdigen eigenen IT-Infrastruktur) und außen (den fremden „bösen“ Netzen) mit einer Schutzhülle um die zu schützende IT herum: dem sogenannten Perimeter. Die bewährten Elemente der Perimetersicherheit waren daher seit langem die Kontrolle des Kommunikationsverkehrs und der Kommunikationsinhalte, die über den Perimeter fließen, sowie die Entkopplung der Kommunikation, um direkte Zugriffe vom unsicheren auf den sicheren Bereich zu vermeiden.

Das funktioniert solange die Kommunikationsbeziehungen, die Anwendungspalette und die Komplexität der Anwendungen überschaubar sind. Die Agilität der modernen Anwendungsentwicklung führt jedoch zu immer größerer Vielfalt, immer kürzeren Produktzyklen und insgesamt zu einer Vielzahl von Schnittstellen über die fast unüberschaubare Kommunikationsmuster möglich sind. Mit dieser Entwicklung steigen automatisch auch die Angriffsmöglichkeiten entsprechend deutlich an und damit die Anforderungen an die Flexibilität und Intelligenz der Sicherheitsfunktionen am Perimeter.

Gleichzeitig verwischt die Grenze zwischen innen und außen durch mobile Nutzer, heterogene Nutzergruppen, Outsourcing und Cloud Computing. In der Vergangenheit erstreckte sich der Perimeter auf wenige Außenanbindungen, zum Internet und z.B. zu Partnern. Inzwischen müssen oft WAN-Übergänge zu anderen Standorten, Systeme bei Providern oder in einer Cloud abgesichert werden und auch innerhalb der eigenen Infrastruktur werden immer häufiger Sicherheitszonen geschaffen, um z.B. kritische Systeme oder Systeme von denen eine besondere Bedrohung ausgeht (z.B. fremdbetriebene Systeme) abzuschotten.

Als Ergebnis materialisieren sich an immer mehr Netzübergängen immer leistungsfähigere Firewalls, die mit immer komplexeren und intelligenten Regelwerken und Policies versuchen der Lage Herr zu werden. Damit entsteht mit traditionellen Sicherheitsarchitekturen ein kaum noch verwaltbarer Moloch an Sicherheitskomponenten, der den Spagat zwischen der Abwehr immer anspruchsvollerer Bedrohungen (d.h. sich dynamisch ändernde höchst komplexe Regelwerke, Policies und Signaturen) und den extrem hohen Anforderungen an Betriebsstabilität und Performance schaffen muss.

Software-Defined Networking (SDN) bietet nun eine Plattform, auf dessen Basis durch eine Trennung von Policy-Verwaltung und -Enforcement neue, standardisierte Sicherheitsarchitekturen geschaffen werden können, mit denen diesen Herausforderungen begegnet werden kann:

- Die notwendige Intelligenz zur Abwehr von Bedrohungen (insbesondere von Angriffen) und zur system- und anwendungsübergreifender Analyse von Kommunikations- und Verhaltensmustern wird auf zentrale Controller, d.h. auf wenige Punkte mit hoher Rechenleistung, konzentriert. Neben komplexen Policies können diese Security Controller eine Vielzahl von externen und internen Kommunikationsbeziehungen bedienen und auf verschiedenste Informationsquellen (z.B. Datenbanken mit neuesten Verhaltensmustern zur Angriffserkennung) zurückgreifen.

- Die Durchsetzung von Policies erfolgt (quasi als Türsteher im Netz) auf dezentralen Enforcement Points, die dynamisch zielgerichtet von den Controllern mit der für die lokale Lage eines Enforcement Points zu einem gegebenen Zeitpunkt erforderlichen Entscheidungslogik versorgt werden. Enforcement Points können SDN-Netzkomponenten aber auch Virtualisierungs-Hosts oder Server sein. Dies ermöglicht auch neue Zonenkonzepte, bei denen Sicherheitszonen nicht mehr zwingend eine spezifische Netzsegmentierung erfordern. Da die Enforcement Points nur noch über einen Bruchteil der Intelligenz der Controller verfügen müssen, ist auch eine wirtschaftlich tragbare Unterstützung von hohen Durchsatzraten jenseits der 10 Gbit/s möglich.

- Durch gesicherte VPN-Tunnel zwischen Enforcement Points kann schließlich ein sicheres virtuelles Overlay-Netz geschaffen werden, das eine flexible Provisionierung von End Points (z.B. VMs) und deren Mobilität im Netz zu unterstützt.

Entsprechende Konzepte sind im Laufe des letzten Jahres beispielsweise von der Cloud Security Alliance (CSA) im Rahmen der Software Defined Perimeter (SDP) Working Group erarbeitet worden[1]. Seitens der Hersteller (z.B. Check Point mit Software-Defined Protection [2] oder der Security Controller von Intel[3]) materialisieren sich bereits erste Produkte, die solche Konzepte umsetzen.

Sicherheitskomponenten werden künftig also nicht nur stärker in Virtualisierungslösungen, sondern auch in SDN-Konzepte integriert werden. Dabei zeigt sich bereits jetzt, dass Sicherheitsarchitekturen unmittelbar von SDN profitieren und sich mit Software-Defined Security dringend benötigte eigene, spezifische Standards für die Informationssicherheit etablieren.

[1] Siehe https://cloudsecurityalliance.org/research/sdp/

[2] Siehe http://www.checkpoint.com/sdp/ebook/files/assets/common/downloads/Software-defined%20Protection.pdf

[3] Siehe http://www.intelsecurity.com/solutions/intel-security-controller.html

Neues Seminar

Crashkurs IT-Recht für Nichtjuristen

23.04.15 in Bonn

Die ComConsult Akademie veranstaltet am 23.04.15 ihr neues Seminar "Crashkurs IT-Recht für Nichtjuristen" in Bonn.

Die dritte IT-Revolution hat begonnen. Geschäftsleben, Produktionsprozesse und Freizeitverhalten stehen vor einer umfassenden informationstechnologischen Vernetzung. IT und TK wachsen zusammen. Damit eröffnen sich neue unternehmerische Möglichkeiten. Zugleich nimmt die rechtliche Durchdringung und Komplexität in der Netzwirtschaft stark zu. Zivilrecht, öffentliches Recht, gewerbliche Schutzrechte und Strafrecht sind bedeutende Leitplanken für die rechtssichere und optimale IT-Lösung. Ohne Kenntnis der rechtlichen Einflussfaktoren können IT-Projekte nicht sinnvoll geplant und durchgeführt werden. Das Seminar soll einen griffigen Überblick der wichtigsten rechtlichen Grundlagen und Anforderungen bieten:

- Recht der Informations- und Kommunikationstechnologie (ITK) im Überblick (B2B, B2C, B2A)
- Lieferung/Bereitstellung von Hard- und Software, ITK-Dienstleistungen, Strukturierung komplexer Projekte
- Der Internet-System-Vertrag, Domainverträge
- Der öffentliche IT-Auftrag (EVB-Muster)
- Elektronischer Geschäftsverkehr
- Rechtliche Querbezüge: AGB-Kontrolle, Datensicherheit und Datenschutz, Compliance, Kartellrecht, Strafrecht
- Sanierung von IT-Verträgen im Krisenfall
- Trends in der IT-Industrie: rechtliche Herausforderungen (z.B. Digital Health, Intelligente Maschinen, Internet of Things, Computing Everywhere)
- Rechtsschutz und Konfliktlösung im Falle von Streitigkeiten
- Fälle, Muster und Praxisbeispiele

Diese Veranstaltung wendet sich an IT-Leiter, Compliance-Beauftragte und Geschäftsführer, die sich kompakte und praktische Grundkenntnisse zu den rechtlichen Eckpunkten des IT-Projektes verschaffen wollen. Die Inhalte sind insbesondere an Nichtjuristen gerichtet, die sich nicht alltäglich mit rechtlichen Fragestellungen befassen und eine Grundorientierung suchen. In dem Seminar werden auch Praxisfälle erörtert.

Das Seminar wird geführt von Rechtsanwalt Dr. Jan Byok. Er ist seit mehr als 20 Jahren Rechtsanwalt in Düsseldorf und Partner der internationalen Wirtschaftskanzlei Bird&Bird LLP. Sein Fokus liegt in den Gebieten des öffentlichen Vergabe-, Vertrags- und Preisrechts, des ITK-Rechts, des Wettbewerbs- und Kartellrechts und in der juristischen Projektsteuerung. Dr. Byok hat zahlreiche komplexe Technologieprojekte bei der bundesweiten Einführung des BOS-Digitalfunks, der elektronischen Gesundheitskarte, der Umstellung des öffentlichen Rechnungswesens, der Einführung von e-procurement-Systemen, dem Abschluss von Providerverträgen, in der Beschaffung von Hard- und Software und bei IT-Outsourcings erfolgreich umgesetzt. Er veröffentlicht regelmäßig Beiträge in juristischen Fachzeitschriften und Wirtschaftsmagazinen. In den einschlägigen Bewertungsveröffentlichungen rangiert er seit mehr als 15 Jahren als bundesweit führender Rechtsanwalt in seinen Spezialgebieten (zuletzt JUVE Handbuch 2014/2015, Wirtschaftskanzleien; The Legal 500 2014; WirtschaftsWoche Top-Kanzlei-Rankings 2014; Handelsblatt in Kooperation mit Best Lawyers ® 2014 (vgl. Ausgabe vom 10. Juni 2014, S. 14-17).

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Ich buche das Seminar
Crashkurs IT-Recht für Nichtjuristen

☐ am 23.04.15 in Bonn
zum Preis € 1.090,-- netto

☐ Bitte buchen Sie mir ein Hotelzimmer

vom_____ bis_____15

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

_____ Vorname

_____ Nachname

_____ Firma

_____ Telefon/Fax

_____ Straße

_____ PLZ,Ort

_____ eMail

_____ Unterschrift

Neues Seminar

IT-Sicherheit in der industriellen Fertigung und der Shop Floor IT 27.04.15 in Düsseldorf

Die ComConsult Akademie veranstaltet am 27.04.15 ihr neues Seminar "IT-Sicherheit in der industriellen Fertigung und der Shop Floor IT" in Düsseldorf.

Der Trend des Einsatzes von Standard-IT in der industriellen Fertigung, speziell in der Automatisierungstechnik verbunden mit der Konvergenz zu IP-basierter Vernetzung der Komponenten und Nutzung von Standard-Protokollen erzwingt konsequente Sicherheitsmaßnahmen.

Grundsätzlich vererben sich zunächst alle Gefährdungen der Standard-IT mit allen Konsequenzen auf die IT in der industriellen Fertigung und im Shop-Floor-Bereich. Sicherheitsvorfälle haben hier in der Vergangenheit nicht selten zu Produktionsausfällen geführt und es sind auch Vorfälle denkbar, bei denen Menschen in Gefahr sind. Die bewusste Manipulation von Steuerungen durch einen speziellen Virus ist beispielsweise seit geraumer Zeit kein Science Fiction mehr.

Der Schutz vor schadenstiftender Software muss mindestens die Qualität aufweisen, die im Office-IT-Bereich möglich ist. Wenn hierzu PCs in Maschinen und Steuerungen nicht angemessen gehärtet und mit einem soliden Virenschutz und Patch-Management gesichert werden können, muss mit anderen Mitteln ein vergleichbarer Schutz geschaffen werden. Hier müssen dann Maßnahmen der

Netztrennung kritischer Bereiche in Verbindung mit Firewall- und Intrusion-Prevention-Techniken greifen. Dies macht deutlich, dass für die IT in der industriellen Fertigung umfassende Sicherheitskonzepte notwendig sind.
Eine ähnliche Situation findet man auch in anderen Bereichen. Zu nennen sind hier beispielsweise die moderne Gebäudetechnik, die Medizintechnik aber auch der Aufbau von Anlagen in Forschung und Entwicklung, z.B. Prüfstände.

Die Sonderveranstaltung dient als Ideengeber und Diskussionsforum für die Absicherung von IT-Systemen in der industriellen Fertigung und im Shop-Floor-Bereich.

Berater mit jahrelanger Projektpraxis vermitteln auf dieser Veranstaltung ihre Erfahrungen in folgenden Bereichen:

- Anatomie bekannter Sicherheitsvorfälle und was daraus gelernt werden kann
- Aufbau von sicheren Netzen und Zonenkonzepte für die Trennung von Netzen der industriellen Fertigung
- Sichere Anbindung an Campus-Netze
- Einsatz von Firewall-Techniken und Intrusion Prevention
- Virenschutz und Patch-Management
- Unterstützung von Sicherheitsmaßnahmen auf Ebene der Anlagen durch den Anlagenbauer
- Anwendung von Sicherheitsstandards und Integration in die Sicherheitsprozesse
- Sicherer Betrieb und Überwachung der IT in der industriellen Fertigung und im Shop-Floor-Bereich
- Sichere Administration, speziell Administration durch Fremdfirmen

Die Sonderveranstaltung analysiert die Gefährdungslage und stellt zielgerichtet Sicherheitskonzepte aus der Projektpraxis vor. Dabei wird auch aufgezeigt, welche Elemente für den sicheren Betrieb der IT in der industriellen Fertigung und im Shop-Floor-Bereich notwendig sind und wie durch die Integration in Sicherheitsprozesse und andere IT-Prozesse eine nachhaltige Informationssicherheit geschaffen werden kann.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Ich buche das Seminar
IT-Sicherheit in der industriellen Fertigung und der Shop Floor IT

☐ am 27.04.15 in Düsseldorf
zum Preis € 990,-- netto

☐ Bitte buchen Sie mir ein Hotelzimmer

vom_____ bis_____15

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

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

Zweitthema

Warum Private Cloud? Und wie?

Fortsetzung von Seite 1

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

Sicher hat es in den letzten Jahrzehnten Fehlentwicklungen der Unternehmens-IT gegeben. Die IT hat sich in vielen Unternehmen verselbständigt. Die Anzahl der internen und externen IT-Mitarbeiter vieler Unternehmen steht oft in einem Missverhältnis zur Gesamtgröße der Unternehmen. Das IT-Budget verschlingt häufig einen zu großen Teil der Ressourcen der Firma.

Aber rechtfertigen solche Fehlentwicklungen das Verfallen ins andere Extrem? Ist die reflexartige Verlagerung der IT-Kompetenzen zu öffentlichen Anbietern die angemessene Reaktion auf eine nicht optimierte interne IT?

Sicher bieten Public Clouds Vorteile. Manche Dinge funktionieren am besten in der Public Cloud. Man denke etwa an die sehr schnell realisierbare unternehmensübergreifende Kooperation in Public Clouds. Web- und Videokonferenzen, Datenaustausch und Collaboration über Unternehmensgrenzen hinweg sind in Public Clouds meistens unkomplizierter zu nutzen. Ein Startup-Unternehmen kann sicher den eigenen IT-Bedarf in der Public Cloud viel schneller decken als wenn es von Anfang an versuchen würde, eine selbstbetriebene IT aufzubauen. Aber gilt das für alle IT-Anwendungen aller Unternehmen?

Neben den Sicherheitsbedenken, die meistens gegen die Public Clouds geltend gemacht werden, und zusätzlich zu den häufig diskutierten rechtlichen Problemen mit Public Clouds gibt es auch andere Gründe, eine eigene IT den öffentlichen Angeboten vorzuziehen. Hier gibt es eine Analogie zu anderen Bereichen. Stellen Sie sich ein Unternehmen vor, das den eigenen Fuhrpark gänzlich abschafft. Die Mitarbeiter könnten ja öffentliche Angebote nutzen: Züge, Busse, Taxis. Weg mit den teuren Dienstwagen! Diese seien in Deutschland ohnehin nur steuersparende Privilegien. Nun stellen Sie sich den Monteur vor, der um sieben Uhr früh auf der Baustelle sein muss. Er müsste einiges von seiner Freizeit opfern, wenn er keinen Dienstwagen nutzen könnte. Oder denken Sie an einen Vertriebsmitarbeiter, der an einem Tag vier Kunden in seinem Zuständigkeitsgebiet besuchen muss. Er wird ohne Dienstwagen an Effizienz einbüßen.

Ja, es kann für einige Unternehmen sinnvoll sein, auf Dienst-PKW zu verzichten. Aber jedes Unternehmen unterscheidet sich von anderen. In seinem eigenen Unternehmen hält der Autor (der als Teilhaber die Dienstwagen mit bezahlen muss) die unternehmenseigenen PKW für sinnvoll.

Es gibt bei der Nutzung von Public Clouds zu viele Nachteile und Unklarheiten, als dass Public Clouds als Allheilmittel gelten könnten. Ein Beispiel ist der Umgang mit den Daten des Unternehmens bei Beendigung des Vertragsverhältnisses. Kein Unternehmen wird ein Vertragsverhältnis eingehen wollen, ohne den Ausstieg aus dem Vertrag nicht vorher zu regeln. Dies bedeutet, dass jedes Unternehmen wissen muss, wie es bei Beendigung des Vertragsverhältnisses in den Besitz seiner Daten kommt. Die Beendigung des Vertrages kann fristgerecht oder aus wichtigem Grund vor Ablauf der Vertragszeit erfolgen. Am besten sollte der Kunde eines öffentlichen Cloud-Betreibers immer im Besitz aller seiner Daten sein, um auch jederzeit aus dem Vertrag aussteigen zu können. Das Format der Daten muss den Kunden befähigen, diese Daten sofort nach dem Verlassen einer Public Cloud in einer anderen Cloud, privat oder öffentlich, nutzen zu können. Ob und wie diese Daten dem Kunden zur Verfügung gestellt werden, ist im Vertragsverhältnis zu klären. Über diese Frage diskutieren und verhandeln die Public Cloud Provider nicht gern. Oft ist in deren Szenario der Ausstieg aus deren Cloud gar nicht vorgesehen.

Die Ausstiegsmodalitäten sind nur ein Beispiel für die Unwägbarkeiten bei der Nutzung von Public Clouds. Diese und andere Unwägbarkeiten, und nicht etwa die angebliche Rückständigkeit deutscher Unternehmen, sind meistens der Grund, weshalb viele Unternehmen den Public Clouds eher skeptisch gegenüberstehen.

Andererseits liegen die Vorteile von Clouds auf der Hand:

- Nutzung von Synergien durch gemeinsame Nutzung derselben Infrastruktur (siehe Abbildung 1)
- Schnelle Skalierbarkeit
- Nutzbarkeit überall und standardbasierend
- Nutzungsabhängige Abrechnung
- Einfache Einrichtung von Diensten und Applikationen

Einige dieser Vorteile wie zum Beispiel Synergieeffekte werden durch die fortgeschrittene Virtualisierung in der Unternehmens-IT bereits genutzt. Andere Cloud-Merkmale wie zum Beispiel die einfache Einrichtung von Diensten und Applikationen sind in den Unternehmen unterschiedlich ausgeprägt. Gerade der einfachen Einrichtung und somit der schnellen Reaktion der IT auf Geschäftsanforderungen stehen oft viele Hindernisse im Weg.

Private Cloud oder virtuelle Private Cloud?

Öffentliche Cloud-Anbieter kennen die Bedenken der Unternehmen gegen Public Clouds und reagieren mittlerweile darauf. Sie versuchen, ihre Dienste auch den Unternehmen schmackhaft zu machen.

Warum Private Cloud? Und wie?

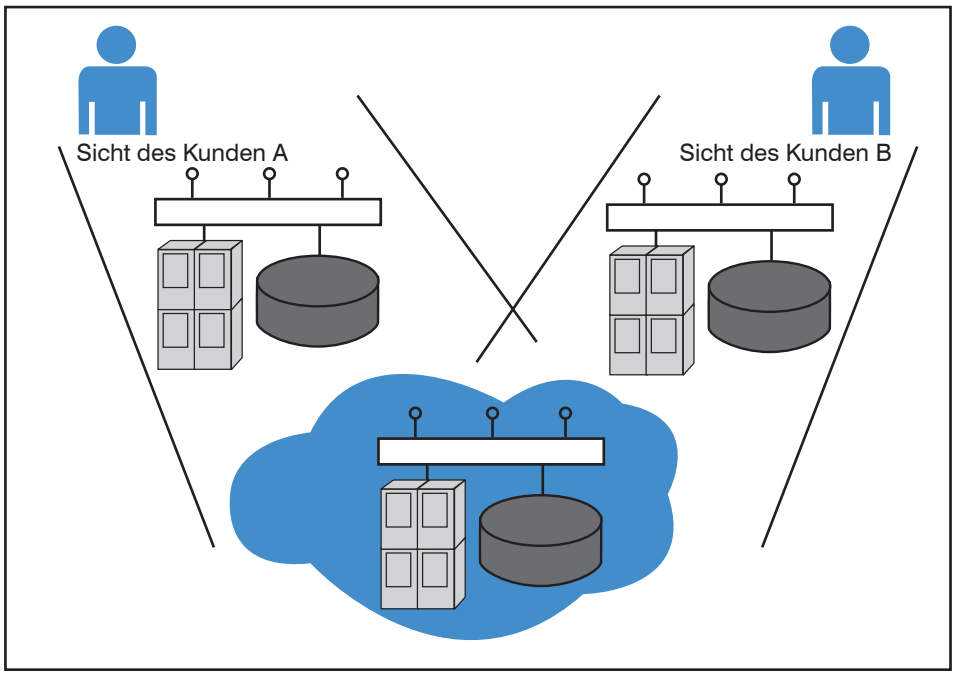


Abbildung 1: Gemeinsame Nutzung einer Cloud

Neulich wurde der Autor gefragt, was er von einer virtuellen Private Cloud halte. Da sich der Autor bei der Begriffsbestimmung an standardisierten und providerunabhängigen Termini orientiert, die zum Beispiel in einem Dokument des US-amerikanischen National Institute of Standards and Technology (NIST)[1] vorkommen, schlug er dort nach. Leider taucht der Begriff „Virtual Private Cloud“ in den Cloud-Definitionen von NIST gar nicht auf.

Das Nachschauen bei Amazon[2] war erfolgreicher. Bei Amazon heißt es:

„Amazon Virtual Private Cloud (Amazon VPC) ermöglicht die Bereitstellung eines logisch isolierten Bereichs der Amazon Web Services (AWS)-Cloud, in dem Sie AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk ausführen können. Sie haben die vollständige Kontrolle über Ihre virtuelle Netzwerkumgebung, u. a. bei der Auswahl Ihres eigenen IP-Adressbereichs, dem Erstellen von Subnetzen und der Konfiguration von Routing-Tabellen und Netzwerk-Gateways.“

Im Kern geht es also darum, dass in der öffentlichen Cloud der Amazon Web Services (AWS) der Kunde einen virtuellen Netzbereich bekommt. Im Sinne der NIST-Definition weist Amazon VPC also Elemente von Infrastructure as a Service (IaaS) auf. Ohne Amazon VPC entspricht AWS nämlich eher dem Modell Platform as a Service (PaaS). Ein AWS-Kunde hat keine Kontrolle über Netze, Server, Betriebssysteme oder Speicher in der Cloud. Er nutzt die Web Services als Plattform.

Während sich darüber streiten ließe, in welche der drei NIST-Kategorien SaaS, PaaS oder IaaS das eine oder andere Amazon-Angebot gehört, ist die Definition von Public und Private Cloud bei NIST sehr eindeutig (siehe Abbildung 2). Eine Private Cloud wird von einer Organisation exklusiv genutzt. Dagegen steht eine Public Cloud jedem offen. Jeder kann Services von der Amazon-Cloud beziehen. Dazu gehört AWS, aber auch VPC. Die Tatsache, dass bei VPC der Kunde die Kontrolle über die virtuelle Netzumgebung erhält, ändert nichts daran, dass es sich um keine Private Cloud, sondern um eine Public Cloud handelt.

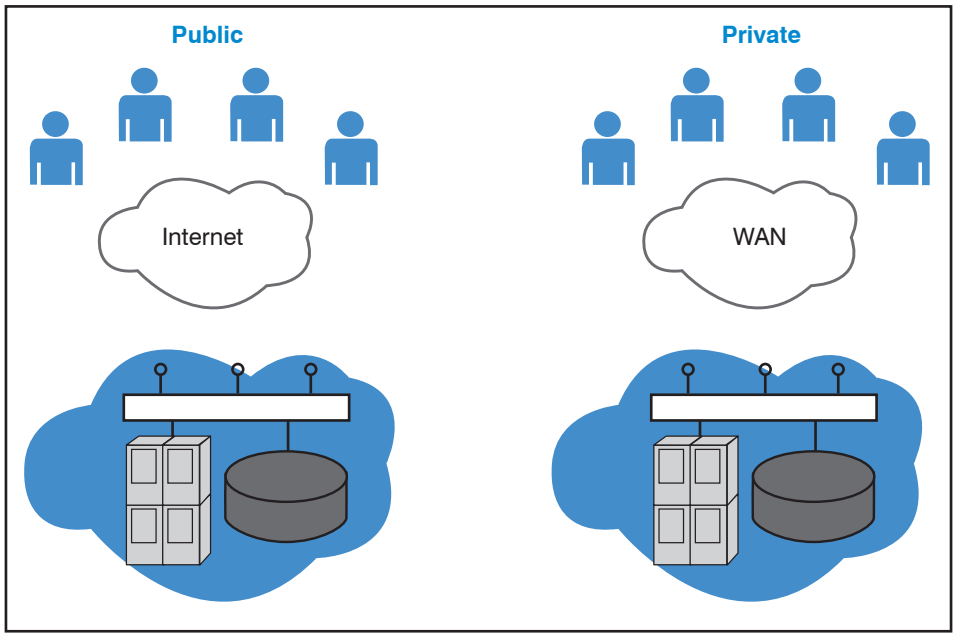


Abbildung 2: Public und Private Cloud

Versuchen wir, an den Begriffen im NIST-Dokument festzuhalten: Wenn die Befähigung des Kunden, Teile der Infrastruktur selbst zu konfigurieren, aus einer öffentlichen eine private Cloud machen würde, gäbe es für NIST keine Veranlassung, die Variante IaaS auch für Public Clouds zu definieren. Mit anderen Worten: Amazon VPC ist keine Private Cloud im Sinne der NIST-Definition, sondern weist einfach Elemente von IaaS in einer Public Cloud auf.

Warum verwendet der Provider dann den Begriff der Virtual Private Cloud? Weil er um die Befindlichkeiten und Bedenken im Zusammenhang mit Public Clouds weiß und diese umgehen will. Hier geht der Provider davon aus, dass er mit dem Attribut „privat“ punktet. Die Bevorzugung von Private Clouds durch die Unternehmen ist also auch bis zu den Anbietern öffentlicher Clouds vorgedrungen.

Es ist also davon auszugehen, dass sich immer mehr Unternehmen damit befassen, wie sie ihre eigene IT in Richtung einer Private Cloud entwickeln.

Virtualisierung ist das A und O

Cloud Computing ist kein von anderen Entwicklungen in der IT losgelöster Trend. Lange bevor der Begriff der Cloud die Runden machte, gab es schon Ansätze und Lösungen, auf die eine Cloud aufsetzt. Der wichtigste dieser Ansätze ist die Virtualisierung.

Warum Private Cloud? Und wie?

Virtualisierung hat es in der IT schon immer gegeben. Als in den 1940er Jahren der damalige IBM-Präsident Thomas Watson meinte, weltweit gäbe es den Markt für circa fünf Computer, ging er sicher davon aus, dass jeder dieser Computer einer Vielzahl von Kunden zur Verfügung stehen müsse. Etwa dreißig Jahre später entwickelte seine Firma das Konzept logischer Partitionen (LPAR), das bis heute die Basis der Aufteilung eines IBM-Rechners in verschiedene virtuelle Computer ist. Dieses Konzept wurde zunächst auf dem Mainframe umgesetzt und fand ca. zwanzig Jahre später den Weg in die AIX-Rechner von IBM.

Damals, also in den 1990er Jahren, boten die Intel-Prozessoren, die in PCs verbaut wurden, sowie die eher sparsame Ausstattung von PCs mit Arbeitsspeicher nicht genügend Spielraum für die virtuelle Aufteilung eines PCs. Interessanterweise waren die Beweggründe für die Implementierung virtueller Maschinen auf der Basis von PCs anders gelagert. Gegen Ende der 1990er Jahre ging es eher darum, dass virtuelle Maschinen die sehr lästigen Abhängigkeiten zwischen Software und Hardware von PCs beseitigten. Ein Spielprogramm oder irgendeine andere Software sollte auf jedem PC laufen, unabhängig davon, mit welcher Hardware der PC ausgestattet ist. Virtualisierung ist eine Abstraktionsmethode. Sie schafft eine gemeinsame virtuelle Basis, dort wo es keine gemeinsame physikalische Basis gibt.

Folgerichtig war das erste Produkt von VMware, einer Firma, die Virtualisierung zu ihrem Kerngeschäft machte, Software für eine Workstation. Virtualisierung für Server kam später dazu.

Aber virtuelle Maschinen auf x86-Basis sind jünger als manch anderes Verfahren, das heute zum festen Werkzeugkasten der Virtualisierung gehört. Virtual Local Area Networks (VLANs) sind ca. 20 Jahre alt. Auch die Virtualisierung im Speicherbereich war schon Gang und Gäbe, als die x86-Virtualisierung noch in den Kinderschuhen steckte.

x86-Virtualisierung (Abbildung 3) kam später als Netz- und Speichervirtualisierung, entwickelte aber eine Dynamik, die VLANs und Speichervirtualisierung überholte. Insbesondere als es möglich wurde, x-86-Server als physikalische Basis verschiedener Virtueller Maschinen (VMs) zu nutzen, kam für die x86-Virtualisierung in Unternehmen der Durchbruch. Der Autor kann sich noch gut daran erinnern, dass vor gar nicht so langer Zeit, nämlich um die Jahrtausendwende, die Rechenzentren vieler Unternehmen durch die explodierende Zahl der eingesetzten physikalischen Server aus allen Nähten platzten. Ein Unternehmen ist beim Autor noch in guter Erinnerung. Die ca. 1.000 Mitarbeiter des Unternehmens waren damals nicht so zahlreich wie die Server im RZ des Unternehmens. Das Unternehmen hatte mehr Server als PCs.

Die x86-Virtualisierung war die Erlösung aus dem merkwürdigen Zustand, dass die aggregierten Ressourcen der Vielzahl der Rechner nur zu einem geringen Prozentsatz genutzt wurden. Trotzdem brauchte man die Vielzahl der Rechner, weil es aus verschiedenen Gründen nicht möglich war, verschiedene Anwendungen auf der Basis desselben Rechners zu betreiben.

Die x86-Virtualisierung löste also ein dringendes Problem in den Rechenzentren, genauso wie vorher die Speichervirtualisierung geholfen hatte, den zentralen Speicher zu konsolidieren und vielen Anwendungen gleichzeitig zur Verfügung zu stellen, und genauso wie VLANs die gemeinsame Nutzung desselben physikalischen Netzes durch eine Mehrzahl von logisch getrennten Umgebungen erlaubte.

Gemeinsam bilden die Virtualisierungstechniken bei Prozessoren, Speichern und Netzen das A und O für die wichtigste Eigenschaft von Clouds, nämlich Synergien durch die gemeinsame Nutzung derselben Infrastruktur.

Cloud =
Virtualisierung + Automatisierung

Während die Virtualisierung in den meisten Unternehmen etabliert und intensiv in Nutzung ist, ist es mit anderen wichtigen Cloud-Eigenschaften in der IT von Unternehmen nicht weit her. Insbesondere die Selbstbedienung, die bei NIST als eine der fünf Cloud-Eigenschaften genannt wird, ist in den meisten Unternehmen nicht umgesetzt.

Wie definiert NIST die Selbstbedienung in einer Cloud? So: „Ein Verbraucher kann unilateral Computing-Ressourcen wie Serverzeit und vernetzten Speicher nach Bedarf automatisch und ohne Intervention des Personals beim Service Provider belegen."

Davon ist die Unternehmens-IT meist weit entfernt. Das hat verschiedene Gründe, auf die wir in diesem Beitrag noch zurückkommen.

Aber zunächst zu den drei anderen Eigenschaften von Clouds, nämlich:

- Schnelle Skalierbarkeit
- Nutzbarkeit überall und standardbasierend
- Nutzungsabhängige Abrechnung

Was die schnelle Skalierbarkeit betrifft, steht sie im direkten Verhältnis zur Größe einer Umgebung. Je mehr Nutzer eine Infrastruktur hat, desto mehr kann der Betreiber der Infrastruktur in Reserven investieren, die eine schnelle Skalierbarkeit ermöglichen. In anderen Worten: Einen Teil der Synergievorteile muss der Betreiber in diese Reserven reinvestieren. Das erhöht die Chance, dem Zustand gemäß NIST-Definition näher zu kommen, in dem

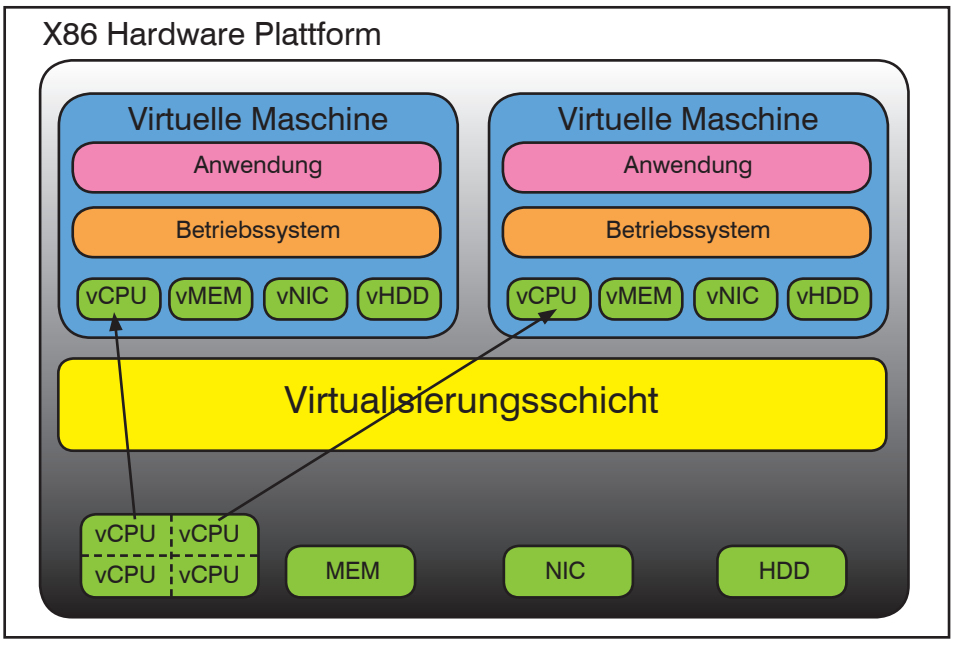


Abbildung 3: x86-Virtualisierung

jedem einzelnen Nutzer die Ressourcen in der Cloud als unendlich vorkommen. In einer Umgebung mit insgesamt 10 TB Arbeitsspeicher für 1000 VMs fällt es leichter, einer VM statt 10 GB eben 20 GB Arbeitsspeicher zur Verfügung zu stellen als in einer Umgebung mit 100 GB Speicher für 10 VMs.

Clouds überall und für Standardwerkzeuge wie Browser, Smartphones und Tablets nutzbar zu machen, hat zwei Komponenten: die Erreichbarkeit der Cloud-Ressourcen über das Netz und die Umstellung von Applikationen derart, dass sie möglichst keine proprietäre Client-Software mehr benötigen. Die erste Komponente ist in vielen Unternehmen bereits Realität. Ob über IPsec-VPNs, SSL-VPNs oder ganz einfach über das Internet: Jede Cloud kann über das allgegenwärtige weltweite Netz erreichbar gemacht werden. Wenn das nicht oder nur eingeschränkt gemacht wird, hat es meist Sicherheitsgründe. An der Technik scheitert es nicht.

Die zweite Komponente, nämlich die Software-Komponente, ist schwieriger zu realisieren. Applikationen sind oft auf die Bedürfnisse des Unternehmens zugeschnitten. Je wichtiger eine IT-Anwendung im Arbeitsablauf ist, desto größer ist die Wahrscheinlichkeit, dass viel Aufwand und Geld in die unternehmensspezifische Anpassung der Applikation geflossen ist. Eine solche Anwendung wirft man nicht einfach über Bord, weil sie nicht mehr schick ist. Solche Applikationen sind oft langlebig. Sie überleben häufig mehrere Generationen von Infrastrukturen. Empfehlungen für die Entwicklung von neuen Applikationen auszusprechen würde den Rahmen dieses Beitrages sprengen. Der allgemeine Hinweis, eine neue Applikation soll Browser-basierend nutzbar sein, reicht meistens nicht aus.

Die nutzungsabhängige Abrechnung ist für die meisten Unternehmen nicht die wichtigste Cloud-Eigenschaft, die man dringend anstreben sollte. Sie ist auch nicht Cloud-spezifisch. Seitdem der Autor die Unternehmen in IT-Themen berät, ist er mit der Diskussion in Unternehmen vertraut, ob sich die nutzungsabhängige Abrechnung lohnt. Sie diszipliniert und motiviert zum sparsamen Umgang mit Ressourcen. Aber viele Erfahrungen belegen, dass der Aufwand dafür durch die dadurch erreichbare Optimierung nicht immer gerechtfertigt ist.

So bleiben als die zwei wichtigsten Cloud-Eigenschaften, die insbesondere die für die IT-Infrastruktur in Unternehmen zuständigen Instanzen interessieren, die Virtualisierung und die Automatisierung. So lässt sich die (sicher vereinfachte) Formel aufstellen, dass eine Cloud durch Virtualisierung und Automatisierung zu erreichen ist.

Rechenzentren haben in den letzten Jahren in Sachen Virtualisierung große Fortschritte gemacht. Die Automatisierung, die den Schlüssel zur Wettbewerbsfähigkeit der internen IT im Vergleich mit Public Clouds bildet, lässt meistens noch zu wünschen übrig. Nach wie vor können die Kritiker der Unternehmens-IT in den meisten Firmen behaupten, die Unternehmens-IT könne sich in Sachen unkomplizierte, schnelle und automatische Selbstbedienung mit Public Clouds nicht messen. Hier der Leidensweg durch Anträge, Bewilligungen und Kompetenz-Silos, dort die Einrichtung von Diensten mit ein paar Mausklicks und Online-Formularen. Oft bleibt die (meist naiv gestellte) Frage im Raum: Warum braucht unsere Unternehmens-IT so lange für etwas, was ich bei Amazon, Google und Co. binnen Minuten bekomme?

Ist die Selbstbedienung erwünscht?

Im Januar 2015 sorgte ein Betrugsfall in einer westdeutschen Stadt für Aufregung. Die Stadtverwaltung hat einen Vertrag mit einem Mobilfunkprovider. Im Rahmen dieses Vertrages können über das Online-Portal des Providers Einzelverträge für Mobilfunk abgeschlossen und Leistungen dazu bezogen werden. Zu diesen Leistungen gehört auch die Lieferung stark subventionierter Endgeräte bei Abschluss von Einzelverträgen mit einer Mindestdauer.

Der Provider hat irgendwann festgestellt, dass tausende Einzelverträge überhaupt nicht zum Telefonieren benutzt worden sind. Nur die subventionierten Endgeräte wurden im Rahmen dieser Verträge bezogen. Es stelle sich dann heraus, dass Mitarbeiter einer städtischen Gesellschaft mit Berechtigung zur Online-Bestellung über den Mobilfunkvertrag die Einzelverträge für die Bestellung (und vermutlich Weiterverkauf) subventionierter Endgeräte missbraucht haben. Neben der strafrechtlichen Verfolgung des Falles zogen die Stadtverantwortlichen die Konsequenz, dass fortan jede Bestellung vom Geschäftsführer der zuständigen städtischen Gesellschaft abzuzeichnen sei.

Bei der Lektüre der Berichte über diesen Fall kam die Situation dem Autor durchaus bekannt vor. Der Autor und seine Kolleginnen und Kollegen haben an mehreren Mobilfunkausschreibungen mitgewirkt, in denen die Selbstbedienung über ein Online-Portal ganz oben auf der Wunschliste des Auftraggebers stand. Dies war häufig dem Umstand geschuldet, dass der Aufwand für Bestellungen, Reklamationen, Lieferungen usw. im Zusammenhang mit Mobilfunkendgeräten der ausschreibenden Organisation über den Kopf gewachsen war und die Verantwortlichen diesen Aufwand minimieren wollten. Ein Online-Portal ist etwas ganz Praktisches. Es arbeitet Tag und Nacht, auch am Wochenende. Es arbeitet automatisch. Es kommt ohne lästige Call-Center-Warteschleifen aus. Wer hat noch nie aufgeatmet, als ein Service endlich auch online bestellbar geworden ist?

Komfort kann aber auch Missbrauch Tür und Tor öffnen, wie der neuerliche Betrugsfall zeigt. Der peinliche Fall zwingt die Verantwortlichen, einen Schritt zurückzugehen und den Komfort einzuschränken. Keine Selbstbedienung mehr. Das

Smartphone gibt es erst nach Abzeichnung des Berechtigten, der jetzt mit gutem Grund die Aufgabe nicht weiter delegiert. Wahrscheinlich stapeln sich bei ihm demnächst die Handy-Anträge.

Das Formularwesen innerhalb von Unternehmen hat seine Daseinsberechtigung. Der Autor kann sich an die Startup-Zeit von ComConsult erinnern, als man bei Lieferanten eine Bestellung aufgeben konnte, wenn man etwas brauchte. Kein böswilliger Missbrauch, sondern die unkoordinierte Belastung des Budgets für Beschaffungen hat dem Schlaraffenland für Besteller sehr bald ein Ende bereitet. Anträge für Bestellungen mit Platz für die Unterschrift einer mit Prokura ausgestatteten Person gehörten zu den ersten bei ComConsult eingeführten Formularen.

Das entscheidende Hindernis auf dem Weg zur Selbstbedienung in der IT ist der Umstand, dass Unternehmen die Kontrolle über Ausgaben für Ressourcen behalten wollen. Nun belastet die Bestellung eines Smartphones das Budget des Unternehmens sofort und unmittelbar, im Gegensatz zur Einrichtung einer VM, die vielleicht Ressourcen belegt, die „eh da“ sind. Wird die unkontrollierte VM-Einrichtung aber zum Usus, müssen Hardware-Ressourcen sicher früher und häufiger nachgerüstet werden als bei einer kontrollierten und restriktiven Einrichtung. Kaum ein Unternehmen wird daher jedem Endanwender die Berechtigung erteilen, in der Private Cloud alles technisch Mögliche auch zu tun.

Deshalb ist die von NIST als Cloud-Eigenschaft aufgeführte Selbstbedienung innerhalb der Unternehmen in Automatisierung zu übersetzen. Automatisierung bedeutet nicht Selbstbedienung für alle, sondern Optimierung der Abläufe. Die Einrichtung eines Dienstes in der Private Cloud wird wegen der erforderlichen internen Kontrolle immer länger dauern als in der Public Cloud.

One-Stop Provisioning

Der Autor zieht im Zusammenhang mit Private Cloud den Begriff „One-Stop Provisioning“ der von NIST so formulierten Selbstbedienung vor. One-Stop Provisioning bedeutet, dass dank Automatisierung die Einrichtung eines neuen Dienstes oder einer neuen Applikation möglichst von einer einzigen berechtigten Instanz durchführbar ist und nicht mehr aus vielen Schritten besteht, für die verschiedene Technikbereiche zuständig sind.

Nun kann sofort der Einwand kommen, dass die arbeitsteilige Organisation in der IT nicht von ungefähr komme und genau wie das formalisierte Bestellwesen ihre Berechtigung habe. Ein Storage-Experte versteht nun mal viel von Speicher und nicht unbedingt von Netz. Und umgekehrt. Ein Serverexperte kann am besten überblicken, was eine neue Anforderung für die Serverfarm bedeutet. Und da für Dienste und Applikationen nun einmal Server, Speicher und Netz erforderlich sind, sind alle Experten involviert. Ein Totschlagargument gegen One-Stop Provisioning.

Hier können aber Tools einer modernen Umgebung aus dem Dilemma helfen. Diese Tools sollten jedem, der ein gesundes Allgemeinwissen über die IT-Umgebung hat, vor Augen führen, wie es mit der Ressourcenauslastung in den verschiedenen Infrastrukturbereichen Computing, Storage und Netz steht. Mit diesen Tools sollte es nicht mehr Experten vorbehalten bleiben zu beurteilen, ob eine Serverfarm eine weitere VM mit bestimmten Merkmalen und Ausstattungskennzahlen verkraftet. Noch besser, die Tools sollten die Machbarkeit selbst überprüfen.

Die Idee hinter One-Stop Provisining ist, dass jegliche Einrichtung von Diensten und Applikationen in einer Private Cloud Software-basierend und mithilfe von Tools erfolgen kann, deren Bedienung möglichst kein Expertenwissen in bestimmten Teilgebieten der Infrastruktur voraussetzt. Der Schritt hierzu, ausgehend von spartenspezifischen Tools für jedes Teilgebiet, ist nicht zu unterschätzen. Genauso wie die IT innerhalb von Unternehmen arbeitsteilig organisiert ist, haben sich Hersteller spezialisiert. Ein Netzhersteller ist meistens kein Speicherhersteller. Jeder Hersteller hat sich in den letzten Jahrzehnten auf die Marktsegmente konzentriert, deren Technologien er am besten beherrscht. Ein Hersteller liefert Produkte in einem bestimmten Teilgebiet. Ein guter Hersteller liefert zudem die Werkzeuge, mit denen seine Produkte in ihrem speziellen Teilgebiet betreibbar und beherrschbar gemacht werden. Diese Werkzeuge werden auch Element Manager genannt. Sie helfen, Teile (Elemente) einer IT zu managen. Manchmal scheitern die Hersteller schon an dieser Aufgabe. Sie liefern Produkte, die vielleicht gut funktionieren, und vernachlässigen das Management. Und nun sollen Tools eingesetzt werden, die nicht nur einen Teilbereich der IT managen, sondern sogar aktiv in alle Teilbereiche eingreifen und diese für einen neuen Dienst, eine neue Applikation konfigurieren? Ist das nicht ein aussichtsloses Unterfangen?

Wo sollen die Tools herkommen?

Noch bevor die Diskussion um Private Clouds losging, befassten sich einige Projekte, die der Autor kennen lernte, mit „RZ-Automatisierung“. Die Vorstellung über das Ziel solcher Projekte war, eine Software Suite zu finden, mit der ein komplexes RZ, bestehend aus Produkten verschiedener Hersteller in den Bereichen Server, Speicher und Netz, betrieben werden kann. Der Anspruch ging über die Findung eines klassischen „Umbrella Manager“ hinaus. Letzteres wird meistens als Synonym für eine Überwachungskonsole verwendet. Einige Firmen haben sich seit den 1980er Jahren auf die Entwicklung zentraler Managementkonsolen spezialisiert. Trotz der Verwendung des standardisierten Simple Network Management Protocol (SNMP) war und ist bei der Vielfalt von Produkten, die in der IT zum Einsatz kommen, selbst die passive Überwachung eine komplexe Aufgabe. Und dann kam zur reinen Überwachung das aktive Eingreifen hinzu. Kein Wunder, dass die Projekte zur RZ-Automatisierung nicht sehr erfolgreich waren.

Es ist immer problematisch, wenn ein Hersteller ein Werkzeug liefern muss, das Produkte mehrerer anderer Hersteller kontrollieren und beherrschen soll. Erfahrungsgemäß hinkt der eine den anderen Herstellern immer hinterher. Jede neue Entwicklung und Änderung bei der Vielzahl der Produkte kann Entwicklungs- und Änderungsbedarf beim Management-Produkt nach sich ziehen.

Besser wäre, Produkte von vornherein so zu entwickeln, dass sie zur Management Suite passen. Auch wenn Wettbewerb immer gut ist, könnte man sich manchmal wünschen, eine Management Suite würde sich im Markt durchsetzen, und alle Hersteller würden sich fortan daran orientieren. Diese Situation gibt es aber nicht. Es gibt kein den Markt beherrschendes Tool für die RZ-Automatisierung, an dem sich alle Hersteller orientieren.

Die nicht so positiven Erfahrungen mit den Versuchen, RZ-Automatisierung in einer heterogenen Umgebung zu realisieren, geben Anlass zu der Überlegung, die Aufgabenstellung zu überdenken. Warum ist der Ansatz gescheitert? Er ist gescheitert, weil das Ziel, eine heterogene Umgebung bestehend aus ganz verschiedenen Produkten mehrerer Hersteller in verschiedenen Teilgebieten mit einer Software Suite zu betreiben, zu hoch gesteckt war.

Die Aufgabenstellung zu überdenken kann zum Beispiel bedeuten, auf verschiedene Werkzeuge zurückzugreifen. Dann muss eben das Personal, das für die Einrichtung von Diensten und Applikationen in der Cloud zuständig ist, ver-

schiedene Werkzeuge bedienen und beherrschen. Solche Multitalente mag es geben. Sie sind aber nicht die Regel. Die Produkte und die dazu gehörenden Tools sind doch zu verschieden und zu breit gestreut, um in Personalunion beherrscht werden zu können.

Ein anderer Weg wäre erfolgsversprechender. Dieser Weg wurde in der IT schon oft eingeschlagen. Es ist der Weg der Abstraktion.

In diesem Fall bedeutet Abstraktion die Umgehung der Abhängigkeiten von der Hardware. Die die Automatisierung im RZ erschwerende Vielfalt ist eine Vielfalt der Hardware. Man hat die LAN Switches, die Server, die Storage-Komponenten. Das Abstrahieren von dieser Hardware ist über Virtualisierung möglich. Dabei wird im Zuge der Einrichtung von Applikationen und Diensten gar nicht mehr in die Hardware eingegriffen, damit kein Beherrschen der Konfiguration verschiedener Hardware-Produkte erforderlich wird. In diesem Modell ist die Hardware am besten statisch, oder zumindest weitaus statischer, als dass sie mit jeder Neueinrichtung eines Dienstes oder einer Applikation verändert werden müsste. Das Modell entkoppelt die häufigsten Einrichtungsaufgaben von der Hardware und sieht sie in Software vor.

Dies bedeutet nicht, dass die Hardware nie verändert, erweitert oder angepasst werden muss. Nur sollten solche Hardware-Änderungen nicht annähernd so häufig erforderlich werden wie Änderungen auf der abstrahierten Software-Ebene. Nichtsdestotrotz müssen die Hardware-Ressourcen der ständigen Überwachung unterliegen. Hardware-Ressourcen sind zu erweitern, wenn sie ausgeschöpft sind bzw. die erforderliche Wachstumsreserve nicht bieten. Dies gilt für die Übertragungsleistung im Netz, die Prozessorlast auf Servern, die Auslastung von Arbeitsspeicher, die I/O-Leistung und die Kapazität von Massenspeicher. Ein solches Performance Management ist die Grundvoraussetzung für eine andere Cloud-Eigenschaft, nämlich für die schnelle Skalierbarkeit und die jedem Benutzer unendlich vorkommenden Cloud-Ressourcen.

Wenn die Einrichtung von Diensten und Applikationen mit möglichst keinen Änderungen auf der Hardware-Ebene verbunden sein soll, sind die damit einhergehenden Änderungen eben auf einer abstrahierten Ebene durchzuführen. Diese abstrahierte Ebene ordnet den Applikationen und Diensten auf Software-Basis Ressourcen zu. Die darüber bereit zu stellenden Ressourcen umfassen wieder Netz, Storage und Server.

Software Defined Storage

Ein Beispiel für die Verlagerung der Einrichtungs- und Managementaufgaben auf die Software-Ebene ist Software Defined Storage (SDS). Zum Beispiel verwendet VMware diesen Begriff für mittels Software eingerichteten und bereitgestellten Speicher. Dabei wird im Zuge der Konfiguration einer VM auch der zugehörige Speicherbereich angelegt.

Ein Bestandteil von VMware vSphere ist das Storage Policy Based Management (SPBM). Anhand von Richtlinien (Policies) werden die von den VMs benötigten Storage Services den VMs zugeordnet.

Die heute verfügbare Virtualisierung des Speichers auf der Hypervisorebene heißt bei VMware Virtual SAN. Um einen Virtual SAN Cluster bilden zu können, muss die vSphere-Umgebung mindestens aus drei Hosts bestehen. Jeder Host muss mindestens mit einem Plattencontroller, einer Platte und einem Flash Drive ausgestattet sein. Die Vernetzung des Speichers erfolgt über Ethernet-Adapter der Hosts. VMware empfiehlt dabei die Verwendung von 10Gigabit-Ethernet-Adaptern.

Beim Anlegen eines Virtual SAN kann entweder der automatische oder der manuelle Modus gewählt werden. Beim automatischen Modus durchforstet Virtual SAN alle Hosts der vSphere-Umgebung nach Speichereinheiten, die dem Virtual SAN hinzugefügt werden können. Beim manuellen Modus werden die Speichergeräte manuell hinzugefügt.

Analog zur Speicherverwaltung auf Hardware-basierenden Speichersystemen erfolgt die Konfiguration von VSAN über Disk Groups.

Wenn Funktionen wie Replikation und Deduplizierung auf der Hypervisorebene wahrgenommen werden, kann die Speicherhardware selbst aus relativ einfachen Bausteinen bestehen, zum Beispiel dem Direct Attached Storage (DAS) der Hosts. (siehe Abbildung 4)

Software Defined Network und Netzvirtualisierung

Das Netz gehört auch zu den Ressourcen, die in einer Cloud eingerichtet werden müssen. Auch beim Netz lässt sich mittlerweile die Bereitstellung von Ressourcen Software-gesteuert durchführen. Viele Hersteller haben sich daher das Software Defined Network (SDN) auf die Fahne geschrieben, wobei ganz unterschiedliche Ansätze darunter verstanden werden.

Neben den SDN-Varianten, die nur auf die Software-gestützte Einrichtung von Netzen fokussiert sind, gibt es auch Ansätze, die SDN in den Kontext eines Software Defined Data Center (SDDC) einordnen. Diese Ansätze folgen der Einsicht, dass vor allem in Clouds eine ganzheitliche Betrachtung aller Ressourcen erforderlich ist. Die Effizienz der Bereitstellung von Diensten und Applikationen in der Cloud kann nicht wesentlich verbessert werden, wenn jeder

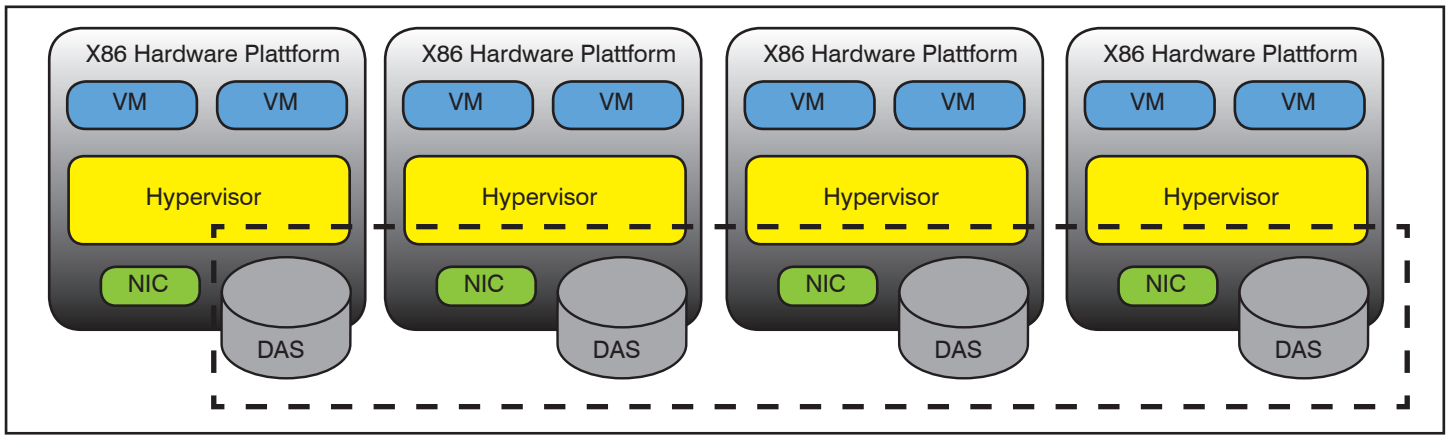


Abbildung 4: Virtualisierung von Direct Attached Storage (DAS)

Ressourcenbereich isoliert betrachtet wird. Daher nennt Cisco den eigenen Ansatz Application Centric Infrastructure (ACI) und nicht etwa Application Centric Network. Schon seit einigen Jahren existieren sogenannte Vertikal integrierte Systeme (ViS) mit Cisco-Produkten. Ein ViS ist eine Anordnung von Server-, Speicher- und Netzkomponenten, die aufeinander abgestimmt sind. Das ViS stellt dabei alle Ressourcen zur Verfügung, die für eine Applikation benötigt werden. Wird eine Software hinzugefügt, mit der Anwendungen im ViS eingerichtet werden können, kann das One-Stop Provisioning in einem ViS realisiert werden.

Beispiele für ViS mit Server- und Netzkomponenten von Cisco sind Vblock mit Speicher von EMC und FlexPod mit Speicher von NetApp. Beide Ansätze gibt es jetzt auch mit Cisco ACI. Bei ACI bringt Cisco die eigene Netzexpertise ein. Netzkomponenten wie Nexus 9000 und der Cisco Application Policy Infrastructure Controller (APIC) sind die beiden Kernkomponenten von Cisco ACI. Cisco ACI basiert auf dynamisch konfigurierbarer Netzhardware, zum Beispiel Nexus 9000. Der Controller, nämlich APIC, übernimmt dabei die Aufgabe der dynamischen Konfiguration des Netzes nach den Anforderungen der Applikationen, also der VMs. Ein einfaches Beispiel ist die VLAN-Zuordnung einer VM. Diese VLAN-Zuordnung gehört zum Profil der VM. Jede Verlagerung einer VM zieht die Anwendung des VM-Profils auf das physikalische Netz nach sich. Wird die VM zu einem Host verlagert, muss der Netzport, der für den Host verwendet wird, für das Profil der VM konfiguriert werden. Zum Beispiel muss das VLAN, zu dem die VM gehört, auf dem Netzport eingerichtet werden, mit dem der Host verbunden ist.

Es gehört zum Kerngeschäft von Netzherstellern wie Cisco, Netzkomponenten zu verkaufen. Daher ist es nicht weiter verwunderlich, wenn Cisco einen Ansatz verfolgt, in dem die eigenen Netzkomponenten eine zentrale Rolle spielen.

Dagegen ist die Vermarktung von Netzkomponenten kein Geschäft für Software-Hersteller, die Virtualisierungslösungen anbieten. Deshalb verfolgt VMware einen Ansatz, bei dem die Hardware keine zentrale Rolle mehr spielt. VMware ist einer der wenigen Hersteller, die sich in diesem Zusammenhang gegen SDN positionieren. Wörtlich heißt es bei VMware[3]:

„Im Gegensatz zu Software-Defined Networking (SDN), bei dem die Hardware die treibende Kraft bleibt, entkoppelt die Technologie von VMware die Netzressourcen wirklich von der zugrundeliegenden Hardware."

Statt SDN spricht VMware im Zusammenhang mit dem Software Defined Data Center von Netzvirtualisierung. Die VMware-Plattform dazu ist NSX. Da bei NSX sämtliche Netzstrukturen und Netzmechanismen in Software realisiert werden, kann NSX auf der Basis jeder Netzhardware realisiert werden. Die Netzhardware übernimmt dabei nur die reine Übertragung von Paketen. Netzstrukturen und -dienste, die sich dynamisch den Anforderungen der Applikationen anpassen, werden ausschließlich in Software implementiert, die in den Hypervisor integriert ist.

Organisatorische Herausforderungen

Unabhängig davon, nach welchem der hier genannten Ansätze eine Private Cloud technisch implementiert wird, sind bei der Realisierung der Cloud organisatorische Herausforderungen zu bewältigen.

Eine dieser Herausforderungen ist die Art und Weise, wie die Ressourcen in einer Cloud finanziert werden. Die Unternehmens-IT agiert bisher häufig nach Bedarf. Eine Infrastruktur wird dabei meistens projektorientiert auf- oder ausgebaut. Oft wird das Projekt aus den Mitteln finanziert, die zum Beispiel im Zuge der Einführung einer neuen Applikation bereitgestellt werden.

Dieses Modell widerspricht dem Cloud-Ansatz. Eine Cloud lebt von Synergieeffekten. Nur durch Nutzung von Synergien zwischen verschiedenen Nutzern kann eine Cloud die Skalierbarkeit und Flexibilität bieten, von der in Verbindung mit einer Cloud ausgegangen wird. Daher muss die Cloud aus einem Topf finanziert werden, der sich aus den Beiträgen aller Nutzer refinanziert. Die schnelle, unkomplizierte und flexible Einrichtung von Applikationen ist nur möglich, wenn andererseits der Ausbau der Cloud-Ressourcen unkompliziert und schnell erfolgen kann, wenn die vorhandenen Ressourcen nicht mehr ausreichen. Diese Entkopplung der Applikationen von den Hardware-Ressourcen muss auch organisatorisch umgesetzt werden, insbesondere bei der Finanzierung.

Eine weitere Herausforderung ist das Aufbrechen der manchmal starren Grenzen zwischen verschiedenen Zuständigkeiten für Teilbereiche der Infrastruktur. One-Stop Provisioning bedeutet, dass die Einrichtung einer neuen Applikation nicht über mehrere Instanzen geht, die für verschiedene Teile der Infrastruktur zuständig sind. Ist eine Instanz als Provisioning-Instanz festgelegt, dürfen andere nicht mehr den Anspruch erheben, bei jeder Einrichtung gefragt und eingebunden zu werden. In der neuen Organisation muss der Netzverantwortliche, wenn er die Applikationen nicht selbst einrichtet, damit leben, dass ohne sein vorheriges Wissen und Zutun Änderungen im Netz durchgeführt werden. Man könnte sich je nach technologischem Ansatz darauf verständigen, dass die im Zuge der Einrichtung von Applikationen und Diensten durchgeführten Änderungen rein virtueller Natur sein müssen. Dann bleibt jede Erweiterung oder Änderung der Hardware dem jeweiligen Hardware-Kompetenzbereich vorbehalten.

Auf dem Weg zur Private Cloud muss sich die Unternehmens-IT somit nicht nur technisch, sondern auch organisatorisch neu aufstellen. Aber die Vorteile der Private Cloud sind diese Mühe wert.

Literatur

[1] The NIST Definition of Cloud Computing, September 2011

[2] http://aws.amazon.com/de/vpc/

[3] http://www.vmware.com/software-defined-datacenter/networking-security.html

ComConsult Veranstaltungskalender

IP-Wissen für TK-Mitarbeiter, 23.02. - 24.02.15 in Bonn

Garantietermin

Dieses Seminar vermittelt TK-Mitarbeitern ohne Vorkenntnisse im Bereich LAN und IP das erforderliche Wissen zur Planung und zum Betrieb von VoIP-Lösungen. Die Inhalte sind so gegliedert, dass Sie die Grundlangen schnell verstehen. Es werden die wichtigsten VoIP spezifischen Aspekte vorgestellt und unter Praxis-relevanten Gesichtspunkten beleuchtet. Die Themen erstrecken sich von IP und LAN Grundlagen hin zu Praxis relevanten Themen wie QoS, Jitter und Bandbreiten Fragen. Ziel ist es dem IP-Unkundigen die wichtigen Grundlagen der Netzwerk Technik kompakt und praxisnah zu vermitteln. Preis: € 1.590,-- netto

Lokale Netze für Einsteiger, 02.03. - 06.03.15 in Aachen

Garantietermin

Dieses Seminar vermittelt kompakt und intensiv innerhalb von 5 Tagen die Grundprinzipien des Aufbaus und der Arbeitsweise Lokaler Netzwerke. Dabei werden sowohl die notwendigen theoretischen Hintergrundkenntnisse vermittelt als auch der praktische Aufbau und der Betrieb eines LANs erläutert. Ausgehend von einer Darstellung von Themen der Verkabelung und der grundlegenden Übertragungsprotokolle werden die wichtigen Zusammenhänge zwischen der Arbeitsweise von Switch-Systemen, den darauf aufsetzenden Verfahren und der Anbindung von PCs und Servern systematisch erklärt. Preis: € 2.490,-- netto

Sicherheitsmanagement mit BSI-Grundschutzmethodik/ ISO 27001, 02.03. - 04.03.15 in Düsseldorf

Garantietermin

IT-Sicherheit konform ISO 27001 und BSI Grundschutzkatalog - klingt kompliziert? Ist es auch. Gerade angehende IT-Sicherheitsexperten fühlen sich schnell überfordert! In diesem Seminar gehen Experten aus der Praxis deshalb nicht nur auf die Theorie, sondern auf die Praxis und den Betrieb ein. Preis: € 1.890,-- netto

RZ-RZ-Kopplung - alles nur eine Frage der Bandbreite?, 09.03.15 in Bonn

Garantietermin

Rechenzentren in entfernten Standorten zu betreiben erfordert sich mit IT-Sicherheit, Desaster Recovery, Service Level Agreements und Hochverfügbarkeit auseinander zu setzen. Dabei sind zum Teil Vorgaben bspw. vom BSI zu beachten. In dieser Schulung werden die aktuellen Techniken erläutert und für die richtige strategische Entscheidung zu einem Gesamtkonzept zusammengeführt.
Preis: € 990,-- netto

Die neue EU-Datenschutzgrundverordnung, 09.03.15 in Bonn

Garantietermin

2015 wird ein neues einheitliches Datenschutzrecht in der Europäischen Union in Kraft treten. Die Verordnung ist noch nicht endgültig verabschiedet, aber die wichtigsten Regelungen sind bereits jetzt weitgehend klar. So wird es gravierende Änderungen bei der Verarbeitung von sensiblen Daten und bei der grenzüberschreitenden Datenverarbeitung geben. Informieren Sie sich frühzeitig über die geplanten Regelungen, damit Sie bei Inkrafttreten der Richtlinie wissen, was auf Ihr Unternehmen zukommt. Preis: € 990,-- netto

Das mobile Unternehmen, 09.03. - 10.03.15 in Hamburg

Dieses 2-tägige Seminar gibt Ihnen einen umfassenden Überblick über Einsatzmöglichkeiten, Risiken und Chancen sowie Anforderungen und Auswirkungen mobiler Technologien im Unternehmen. Es werden die grundlegenden Veränderungen in Arbeitsweise und Arbeitsausstattung aufgezeigt, die die steigende Mobilität mit sich bringt und die Auswirkungen auf den IT-Betrieb, die Infrastruktur und das Management von mobilen Geräten diskutiert. Zum einen werden mögliche Gefährdungen aufgezeigt, die sich durch die zunehmende Konsumerisierung und den damit verbundenen Anstieg von privat genutzten Geräten entstehen. Zum anderen werden aber auch Möglichkeiten und Chancen, die mobile Applikationen und die lückenlose Vernetzung im „Internet of Things“ bieten, erläutert. Preis: € 1.590,-- netto

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen, 09.03. - 11.03.15 in Hamburg

Dieses Seminar vermittelt alle notwendigen Projektschritte zu einer erfolgreichen Umsetzung von VoIP Projekten. Diese erstrecken sich über die Einsatz- und Migrations-Szenarien, die einsetzbaren Basis-Technologien und Komponenten und die erweiterten TK-Anwendungen wie IVR, UM oder UC. Es werden Bewertungskriterien für eine TK-Lösung und eine Übersicht über den bestehenden TK-Markt mit allen etablierten Hersteller vorgestellt. Preis: € 1.890,-- netto

Interne Absicherung der IT-Infrastruktur, 09.03. - 10.03.15 in Hamburg

In diesem Seminar lernen Sie wie man die Sicherheit von LAN, WAN, Endgeräten, RZ-Bereichen, Servern und SAN erreicht. Konkrete Beispiele aus der Praxis zeigen den Weg zu einer erfolgreichen IT-Sicherheits-Lösung. Preis: € 1.590,-- netto

WAN: Konzept, Planung und Ausschreibung, 09.03. - 10.03.15 in Hamburg

Garantietermin

Seminar über die erfolgreiche Konzeption, Planung und Betrieb von WAN-Netzwerken. Lernen Sie wie Sie mit modernsten T echnologien und erprobten Architekturen wirtschaftliche, verfügbare und leistungsfähige WAN-Lösungen aufbauen können. Erfahren Sie wie Sie sinnvoll SLAs für die Praxis aufsetzen können, die auch im Tagesbetrieb standhalten. Mit vielen Tipps und Tricks aus der Praxis.
Preis: € 1.590,-- netto

Wireless LAN professionell, 09.03. - 11.03.15 in Hamburg

Lernen Sie in diesem Seminar wie Sie eine WLAN-Lösung zukunftsorientiert und investitionssicher für die verschiedensten Endgerätetypen und Dichten aufbauen. Lernen Sie wie Sie Verfügbarkeit und Bandbreite optimieren. Verbessern Sie Ihr WLAN mit den verschiedensten Struktur-Elementen vom Access-Point bis zum WLAN-Controller. Erfahren Sie worin sich Produkte und Technologien führender Anbieter unterscheiden. Berücksichtigen Sie die neusten Entwicklungen zur Gestaltung einer WLAN-Lösung, die langfristig tragfähig und wirtschaftlich ist. Lernen Sie Vor- und Nachteile aller aktuellen Technologien kennen und vermeiden Sie Planungs-Fehler. Preis: € 1.890,-- netto

Zertifizierungen

ComConsult Certified Network Engineer

Lokale Netze
02.03. - 06.03.15 in Aachen
18.05. - 22.05.15 in Aachen
28.09. - 02.10.15 in Aachen

TCP/IP-Netze erfolgreich betreiben
13.04. - 15.04.15 in Düsseldorf
15.06. - 17.06.15 in Nürnberg
09.11. - 11.11.15 in Köln

Internetworking
23.03. - 27.03.15 in Aachen
08.06. - 12.06.15 in Aachen
19.10. - 23.10.15 in Aachen

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

ComConsult Certified Trouble Shooter

Trouble Shooting in vernetzten Infrastrukturen
05.05. - 08.05.15 in Aachen
27.10. - 30.10.15 in Aachen

Trouble Shooting für Netzwerk-Anwendungen
09.06. - 12.06.15 in Aachen
17.11. - 20.11.15 in Aachen

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

ComConsult Certified Voice Engineer

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen
09.03. - 11.03.15 in Hamburg
04.05. - 06.05.15 in Bonn
28.09. - 30.09.15 in Köln

Session Initiation Protocol Basis-Technologie der IP-Telefonie
13.04. - 15.04.15 in Düsseldorf
15.06. - 17.06.15 in Nürnberg
09.11. - 11.11.15 in Köln

Umfassende Absicherung von Voice over IP und Unified Communications
23.03. - 24.03.15 in Berlin
08.06. - 09.06.15 in Stuttgart
19.10. - 20.10.15 in Bonn

Optionales Einsteiger-Seminar: IP-Wissen für TK-Mitarbeiter
23.02. - 24.02.15 in Bonn
27.04. - 28.04.15 in Nürnberg
14.09. - 15.09.15 in Bonn

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

Basis-Paket: Beinhaltet die drei Basis-Seminare
Grundpreis: € 4.840,-- netto statt € 5.370,-- netto
Optionales Einsteigerseminar: Aufpreis € 1.190,-- netto statt € 1.590,-- netto

Impressum

Verlag:
ComConsult Research Ltd.
64 Johns Rd
Christchurch 8051
GST Number 84-302-181
Registration number 1260709
German Hotline of ComConsult-Research:
02408-955300

E-Mail: insider@comconsult-akademie.de
http://www.comconsult-research.de

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

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