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-

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

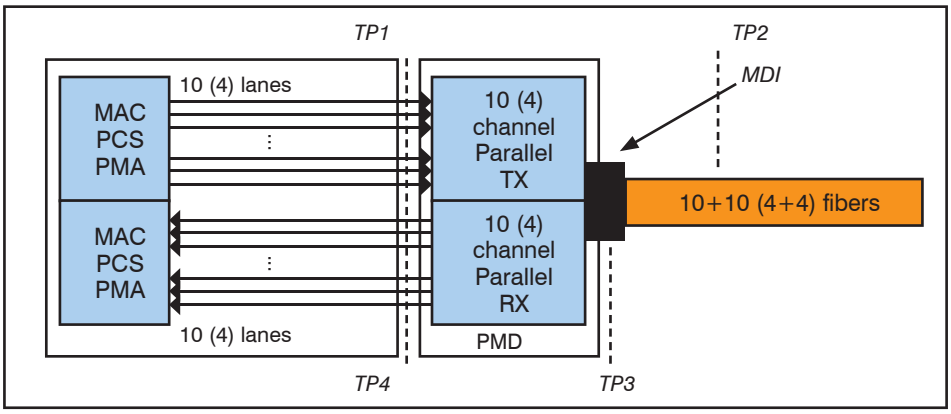

Abbildung 1: Konstruktion von 100 (40) GBASE-SR 10 (4)

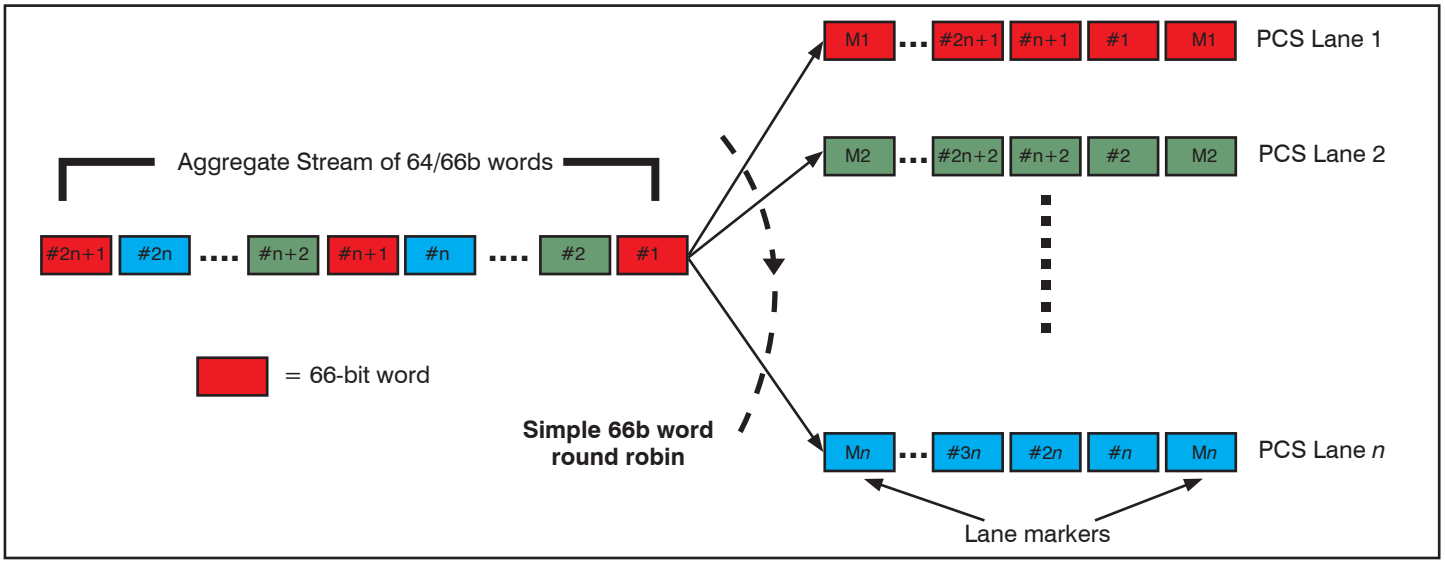

Abbildung 2: IEEE 802.3 ba PCS Lane Distribution Konzept

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 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 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

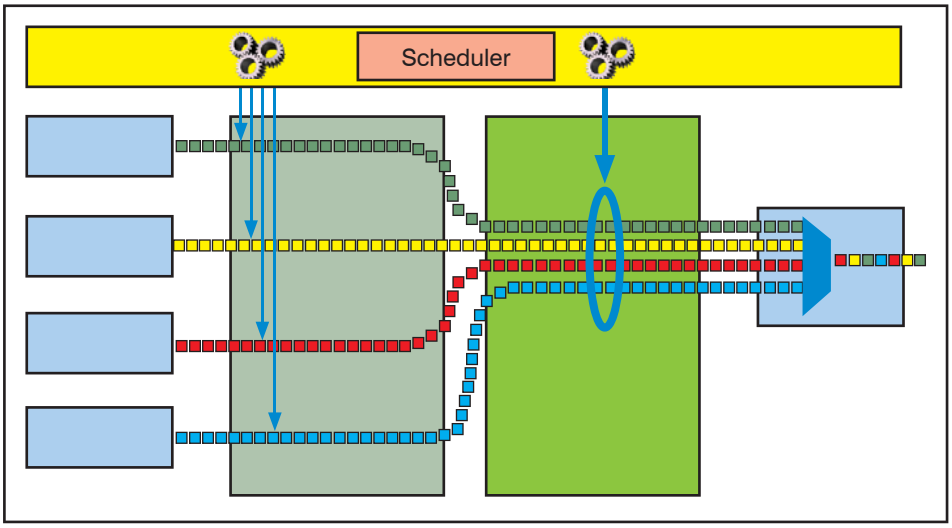

Abbildung 3: Zusatzfunktion Rate Conversion

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?

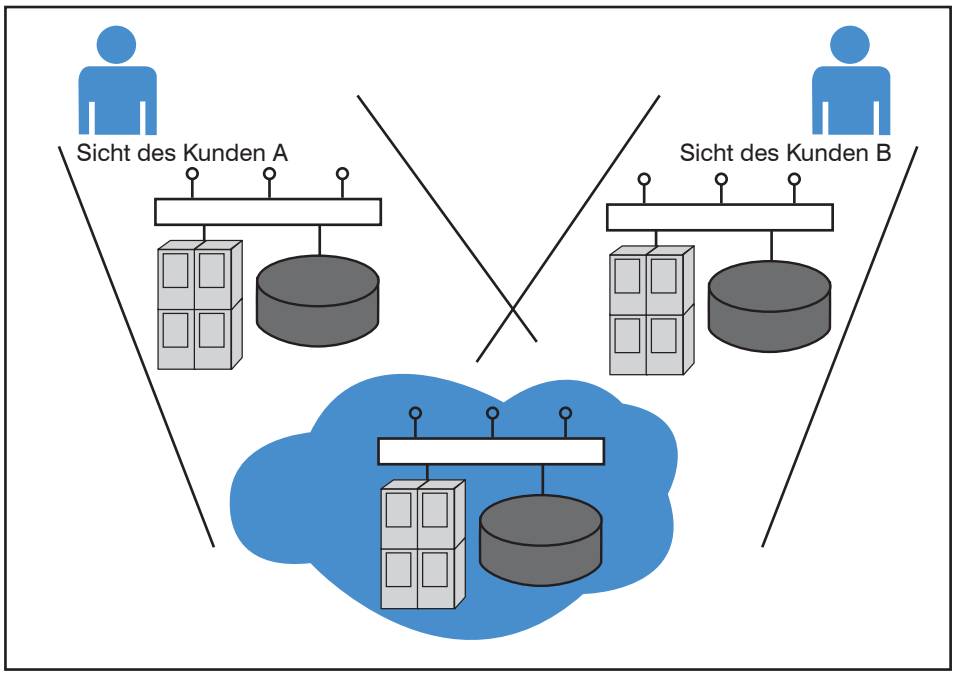

Abbildung 1: Gemeinsame Nutzung einer Cloud

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.

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.

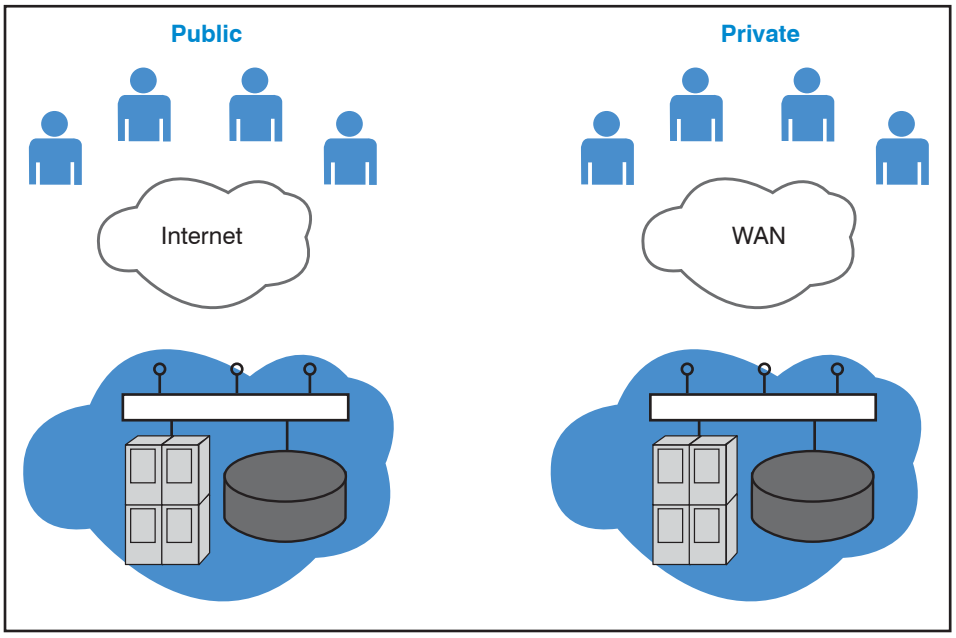

Abbildung 2: Public und Private Cloud