

Data Center

Das RZ-Netz der Zukunft

Teil 1: Die Data Center Networking Landschaft und zukunftsorientierte Lösungen

von Dr. Franz-Joachim Kauffels

Es ist kein Geheimnis, dass sich die Änderungen in RZ-Netzen in den letzten Jahren dramatischer und anders vollziehen als früher. Das Netz der Zukunft wird vollständig automatisiert sein und seine Fähigkeiten werden weit über dem liegen, was wir heute von der Ansammlung von Kästen mit Ethernet-Schnittstellen kennen.

In diesem und folgenden Artikeln wollen wir das Thema von verschiedenen Seiten beleuchten. Die gute Nachricht ist, dass es weiterhin private RZs geben wird und dafür Netze notwendig sind. Längst nicht alles wird in die Cloud verlagert. Marktforschungsunternehmen sagen sogar voraus,



dass der Enterprise Data Center Markt in den nächsten Jahren sogar wieder deutlich wachsen wird.

Die schlechte Nachricht ist, dass es kaum mehr allgemein gültige Wahrheiten gibt. RZs und die Anforderungen an sie haben sich dramatisch entwickelt und werden dies auch weiterhin tun. Dabei werden Probleme und Lösungen aber immer individueller. Auch was die RZ-Netze betrifft, werden wir die Komfort-Zone leider verlassen müssen.

weiter auf Seite 7

Cloud Computing

IEEE 802.11ah – Ein Treiber für das Internet-of-Things?

von Dr. rer. nat. Johannes Dams

In der Vergangenheit kam nicht nur hier im ComConsult Netzwerk Insider immer wieder das Thema Internet-of-Things (IoT) auf, auch in der Praxis werden immer mehr Anwendungen relevant, die grob in die Kategorie IoT eingruppiert werden können. Neben den üblicherweise genutzten Technologien, wie WLAN, Bluetooth etc. ziehen nun die IEEE und die Wi-Fi Alliance mit Standards

und Zertifizierungen für ein IoT-WLAN nach. Aber: Welche technischen Merkmale bieten neue Standards, wie IEEE 802.11ah bzw. Wi-Fi HaLow? Für welche WLAN-Betreiber und welche Anwendungen kann die Nutzung sinnvoll sein? Kann sich der neue Standard durchsetzen? Und wird das IoT-WLAN ein Treiber für neue Internet-of-Things-Anwendungen und -Endgeräte?

Auch wenn der Begriff Internet-of-Things sich immer mehr durchgesetzt, ist eine klare Abgrenzung von anderen WLAN- oder Netzwerk-Anwendungen häufig nicht ganz einfach. Dennoch haben Diskussionen des IoT einige klare Konzepte möglicher zugrundeliegender Architekturen und so auch der damit einhergehenden Begrifflichkeiten ergeben.

weiter auf Seite 17

Geleit

Netzwerk-Switches: welche Rolle spielt Hardware noch?

auf Seite 2

Standpunkt

Sicherheitsrisiko Container?

auf Seite 15

Aktueller Kongress

ComConsult Netzwerk-Forum 2017

ab Seite 4

Aktuelle Sonderveranstaltung

Implementierung von IPv6 – Erkenntnisse und Erfahrungen

auf Seite 16

Geleit

Netzwerk-Switches: welche Rolle spielt Hardware noch?

Netzwerk-Switches waren und sind sehr teuer. Es gab Zeiten, da konnte man für den Preis eines voll ausgestatteten Switches auch in vielen Städten locker ein Einfamilienhaus in guter Lage kaufen.

Warum ist das so? Ist es das ungebremste Begehren der Hersteller sich an uns zu bereichern? Wäre das so einfach, hätte längst ein Hersteller den Markt auf der Preisbasis aufgerollt. Bisher waren Preisunterschiede zwischen den Anbietern zwar signifikant, aber immer noch in ähnlichen Preisregionen.

Was macht also einen Netzwerk-Switch so teuer?

Die Antwort ist einfach. Seit mehr als 30 Jahren wollen wir mehr Leistung als Standard-Hardware hergibt. Für viele Jahre bis vielleicht vor 10 oder 15 Jahren war der Bedarf so signifikant höher als die verfügbare Leistung, dass sich neue Switch-Produkte mit neuen Port-Technologien auch zum 10fachen Port-Preis der Alttechnologie verkaufen ließen. In der Regel würde dann der Preis innerhalb von 3 bis 4 Jahren auf den 3-fachen Port-Preis fallen. Da wir häufig mit einer neuen Generation eine Verzehnfachung der Leistung bekamen, war der dreifache Preis für die 10-fache Leistung auch scheinbar ein Schnäppchen (wenn man mal vom absoluten Preis der Switches absieht).

Wie haben die Hersteller das Problem gelöst, dass es keine verfügbare Standard-Hardware gab?

Nun, genau die Entwicklung von Spezial-ASICs mit Spezial-Leistungsprozessoren für die Software ist das Fundament der Existenz unserer führenden Hersteller. Und da man immer am Rand des Möglichen entwickelte, konnte so auch ein solider Marktvorsprung mit proprietärer Technik erreicht werden. Dabei liegen bei der Bewertung von Switch-Produkten die Tücken im Detail. Ein naheliegendes Ziel ist es, dass jeder Port blockadefrei in Line-Rate übertragen kann. Dieses Ziel ist allerdings technisch gesehen von fragwürdiger Natur, maximal kann es als Minimal-Ziel gelten. Historisch gesehen hat ein Switch die bis dahin dominanten Medienzugangsverfahren "ersetzt". Und speziell die "Ablösung" von CSMA/CD Hubs durch Switches hat scheinbar



einen wesentlichen Mangel von Ethernet beseitigt. Dies ist das Kollisionsverhalten des Verfahrens unter hoher Last. Auch wenn dazu viel Unsinn veröffentlicht worden ist wie zum Beispiel die 30%-Regel, so konnte man bei genauer Kenntnis des Verfahrens im Labor nicht unbedingt praxisnahe - Betriebs-situationen nachstellen, in denen ein Ethernet kollabierte. Der Switch löst dieses Problem auf den ersten Blick, indem er im Full-Duplex-Betrieb Kollisionen auf den Kabeln ausschließt. Dummerweise schafft er aber ein neues Problem. Dies ist die mögliche und auch leicht zu erreichende Überlastung eines Ausgangsports. Wenn eben Datenströme von 10 Eingängen denselben Ausgang ansprechen, kann dieser das bei angenommener identischer Datenrate nicht leisten. Da die heute eingesetzten Switches überwiegend Store-and-Foreward machen, also jedes zu transportierende Paket einmal in einem Puffer speichern bevor es weitergegeben wird, führt eine Überlastung des Ausgangsports zu einem Puffer-Überlauf und Pakete gehen real verloren. Seit Jahren versucht man dieses Problem durch geeignete Flusskontrollverfahren auf Layer-2 zwischen den Switches zu beherrschen, aber an dem Grundproblem Puffer-Management und Auslegung ändert das nichts. Und an dieser Stelle können sich Switches erheblich unterscheiden. Und speziell dieser Unterschied, obwohl er für den Endverbraucher kaum wahrnehmbar ist, kann extrem teuer sein und macht einen signifikanten Teil der Kosten aus. Gleiches gilt für die Modularisierung von Switches, die von Hause aus unter dem Problem leidet, dass man die zukünftig

verfügbaren Einschübe nicht kennt und demzufolge die Weiterleitung auf eine hypothetische zukünftige Leistung auslegen muss. Wird diese Leistungsgrenze erreicht, reduziert sich der modulare Switch zu einem Haufen Schrott, es sei denn man kauft wie zum Beispiel im Falle Ciscos eine neue Supervisor-Engine. Aus heutiger Sicht ist diese Form von Modularität ein fragwürdiges und in vielen Fällen unwirtschaftliches Konzept. In jedem Fall wird man aber eine Schnittstellen-Modularität mit der Anpassung an verschiedene Medien benötigen.

Aber diese ganze Betrachtung ist eigentlich Schnee von gestern. Kaum ein Kunde im Markt braucht heute für einen einzelnen Datenstrom zwischen Sender und Empfänger, nennen sie das von mir aus einen Flow, mehr als 10 Gigabit Leistung. Die meisten Speichersysteme sind weit davon entfernt diese Leistung auszufüllen, im Spitzenbereich werden dann eben mehrere 10 Gigabit-Schnittstellen eingesetzt. Mit SSD-Speichern mag sich das in Richtung des Bedarfs für 25 oder 50 Megabit ändern, das bleibt abzuwarten. Auf der Serverseite haben die Hersteller ausgelöst durch eine zunehmende Zahl von Prozessor-Kernen in Kombination mit Virtualisierung den Sprung auf 40 Gigabit vollzogen, mit den neuen Standards werden dann daraus 25 oder 50 werden, der 40 Gigabit-Standard war immer eine Krücke und wir sagen seit Jahren vorher, dass er nicht überleben wird und jede Investition in diese Richtung fragwürdig ist.

Nun muss ein Netzwerk ja nicht nur einen Flow, also eine Verbindung zwischen Sender und Empfänger unterstützen, sondern ganz viele davon. Deshalb sind Netzwerke hierarchisch aufgebaut und der sogenannte Core muss diese Summenleistung verkraften können. Bei der Frage nach der Summenleistung kommen wir wieder zu den Kosten zurück. Wenn ich die 10-fache Leistung pro Port mit dem 3-fachen Preis abdecken kann, dann ist das eine einfache Rechnung, die zugleich den Verkabelungsaufwand senkt.

Aber genau diese Entwicklung nähert sich dem Ende. Mit der 100 Gigabit-Schnittstelle haben wir genügend Leistung, um über eine geringe Zahl von Ports jede Aggregation problemlos abdecken zu können. Tatsächlich sind vie-

Netzwerk-Switches: welche Rolle spielt Hardware noch?

le Kunden nach wie vor in der Lage mit Kosten-optimalen 10 Gigabit-Schnittstellen aggregierten zu können. Anders formuliert: mit einer zunehmenden Marktdurchdringung mit 100 Gigabit kommt dieser Markt in der Hardware an seinem Ende an. Vermutlich werden wir in 10 Jahren hier noch irgendeinen Sprung bekommen, es gibt ja die Weiterentwicklung für 400 Gigabit und mehr im Providermarkt, aber das ist so weit weg, dass es heute nicht interessiert.

Parallel lösen wir uns immer mehr von der Denkweise, dass wir die nächst schnellere Technik einsetzen, wenn im Core ein Port überlastet wird. Das Netzwerk-Design geht hier klar in Richtung Skalierung durch Parallelisierung. Unternehmen wie Facebook basieren darauf ihr Netzwerk-Design, das auf extrem hohe Summenlasten ausgelegt ist, seit Jahren. In Zukunft werden wir also einen Core sehen, der aus einer flexiblen Zahl von 100 Gigabit-Verbindungen besteht. Es mag Ausnahmen im HPC-Bereich geben, in denen man versucht im Netzwerk Busleitung zu erreichen, aber die sind eben Ausnahmen.

Mit dem Ende des Rennens um die nächste Datenrate sind die Hersteller nicht mehr in der Lage mit Spezial-Chips Alleinstellungsmerkmale zu erarbeiten. Im Gegenteil. Die relative Stagnation der Bandbreiten hat den Markt geöffnet für Chip-Hersteller, die heute fast alle Bandbreiten abdecken ohne dabei selber als Switch-Hersteller aufzutreten. Man ist heute in der Lage einen sehr leistungsfähigen Switch zu bauen ohne einen einzigen Chip selber entwickeln zu müssen.

Damit kommen wir zur zentralen Frage: wird mit 100 Gbit-Portleistung eine Schwelle in der Entwicklung von Switch-Systemen erreicht, ab der Hardware austauschbar wird? Dies würde ohne Frage einher gehen mit einem drastischen Verfall der Preise.

Die Antwort auf diese Frage ist nicht so einfach wie es scheint. Wir beobachten seit Jahren eine Verschiebung der angebotenen Leistung in die Software. Und zunehmend erreichen die Hersteller ihre Alleinstellungsmerkmale nicht mehr aus der Hardware, sondern aus der Software. Gleichzeitig spielen sich im Markt merkwürdige Entwicklungen ab, die von einem neutralen Standpunkt aus kaum zu verstehen sind. So brauchen wir dringend Service-orientierte Netzwerke, um den Bedarf, der aus Virtualisierungsarchitekturen entsteht, abdecken zu können. Aber die offenen Standards, die dies optimal ermöglichen würden, werden von den Anwendern ignoriert. Speziell SPB ist ein

wirklich guter Standard und es ist nicht zu verstehen, dass er sich nicht durchsetzt. Stattdessen etablieren sich Tunnel-Krücken im Markt im Rahmen der normativen Kraft des Faktischen, die aus der Richtung der Hypervisor-Hersteller kommen. Das hat ohne Frage Gründe und die Integration von Netzwerk-Lösungen in die Virtualisierung auf der Basis von Network Function Virtualisation ist einer davon. Aber es erklärt in keiner Weise, warum die verfügbaren guten offenen Standards ignoriert werden. Es scheint so, dass viele Anwender die Abhängigkeit vom Hersteller nicht gerne verlieren wollen.

Was bedeutet das nun für die Zukunft von Switch-Systemen?

Nun, im Detail werden wir das auf dem Netzwerk-Forum 2017 mit den Teilnehmern diskutieren. Aber wir hatten bereits im Vorfeld einige sehr interessante und zum Teil auch kontroverse Diskussionen mit den Herstellern. Ein Ergebnis dieser Diskussion ist, dass wir speziell Cisco eingeladen haben, die Zukunft ihrer Hardware mit den Teilnehmern zu diskutieren (das hat einen inhaltlichen Grund).

Vereinfacht kann man an dieser Stelle aber sagen, dass alle wesentlichen Anbieter davon weggehen den Switch als Einzelprodukt zu sehen, bei dem es egal

ist, wie und wo man ihn kauft. Die Hersteller sehen sich als Anbieter eines Gesamtsystems, das weit über die Grenzen eines einzelnen Switches hinaus geht. Dies bedeutet natürlich, dass wir hier wieder über Software sprechen müssen. Aber es ist eine Software, die eng mit der spezifischen Leistung der Switch-Systeme verbunden ist.

Es gibt ihn also weiterhin, den Netzwerk-Switch. Aber als Teil einer Gesamtarchitektur. Und zur großen Freude der Kunden muss nun nicht nur die Leistung eines Switches bewertet werden, sondern eine komplexe Architektur.

Dies wird eine der wesentlichen Diskussionen des Netzwerk Forums 2017 werden. Und wir haben Sprecher dazu eingeladen, die diese Diskussion in einem interessanten Mix mit den Teilnehmern führen werden. Dazu gehört zum ersten Mal auch VMware, da wir davon überzeugt sind, dass man Gesamt-Architekturen nicht ohne die Hypervisor-Hersteller diskutieren kann.

Das wird aus meiner Sicht eines der interessantesten Foren der letzten 10 Jahre. Ich hoffe, dass Sie da sein werden und sich an der Diskussion beteiligen.

Ihr Dr. Jürgen Suppan

Kongress

ComConsult Netzwerk Forum 2017 27.03. - 30.03.2017 in Köln

Das ComConsult Netzwerk-Forum 2017 stellt die vier momentan dominantesten Netzwerk-Themen in den Mittelpunkt der Veranstaltung:

Am **ersten Tag** analysieren wir die Auswirkungen aktueller Anwendungs-Architekturen auf die schnelle Bereitstellung, die Gestaltung und die Leistung von Netzwerken. Anwendungs-Architekturen werden immer dynamischer und in Kombination mit der Forderung nach einer sehr schnellen Bereitstellung von Kapazitäten ergibt sich eine komplexe Orchestrierungs-Aufgabe. Die Dynamik ergibt sich dabei nicht nur beim Start einer Mikroservice-Architektur, sondern auch bei Lastveränderungen im laufenden Betrieb. Am **zweiten Tag** stellen wir uns den aktuellen Veränderungen im Netzwerkdesign in Kombination mit der Frage, wie wir in einer immer komplexeren Situation zu einem optimalen Betrieb kommen können. Am **dritten Tag** diskutieren wir die neuesten WLAN-Standards und zum Abschluss des Tages die Frage, wie eine umfassende Sicherheits-Lösung unter Berücksichtigung der Cloud aussehen kann. Der **vierte Tag** des ComConsult Netzwerk Forums widmet sich traditionell einem Schwerpunktthema, welches wir gemeinsam mit Ihnen intensiv beleuchten möchten. In diesem Jahr steht das Thema „Netzwerksicherheit: Bedrohungen, Herausforderungen, Trends und Best Practice“ im Fokus.

Preise: € 2.790,- netto - 4-tägige Veranstaltung mit Thementag
€ 2.390,- netto - 3-tägige Veranstaltung ohne Thementag



Buchen Sie über unsere Web-Seite

www.comconsult-akademie.de

Aktueller Kongress

ComConsult Netzwerk Forum 2017

27.03. - 30.03.17 in Köln

Die ComConsult Akademie veranstaltet vom 27.03. bis 30.03.2017 ihren Kongress "ComConsult Netzwerk Forum 2017" in Köln.

Die Architektur und die Nutzung von Netzwerken befindet sich weiterhin in einem Umbruch. Das wirft einige typische und gleichzeitig sehr kontroverse Fragen auf:

- Die Zukunft der Switch-Hardware: gibt es überhaupt noch Unterschiede, welche Strategien verfolgen die Hersteller, nachdem der Kampf um die Bandbreiten - fast - vorbei ist?
- Der Einfluss von NSX/VXlan auf die Netzwerke: die Rolle des Hypervisors in zukünftigen Netzen, was gehört wohin?
- Private Clouds werden kommen, aber wie sieht das Netzwerk dafür aus und was muss es können?
- Campus Design: Schnee von gestern oder mehr aktuell denn je?
- Wireless: WLAN unter Druck, wie sieht die Zukunft aus?
- Sicherheit aus der Cloud: ist das die Zukunft oder wie sieht eine bessere lokale Lösung aus?

Diese Fragen stellen praktisch das Design von Netzwerken wie wir sie kennen in Frage. Ein gutes Beispiel ist die Nutzung von Spine-Leaf-Architekturen als Layer 3-Lösung im Rechenzentrum mit einer Verlagerung des gesamten Layer 2-Bereichs in den Hypervisor (als eine mögliche Variante). Die sich sofort daraus ergebende Frage ist, welche Hilfsmittel wir brauchen um ein Netzwerk noch als Ganzes planen und betreiben zu können.

Gleichzeitig ist der Wettkampf der Bandbreiten - fast - vorbei. Mit 25/50 und 100 Giga-

bit findet in Kürze das Wettrennen um die schnellste Bandbreite sein vorläufiges Ende. Was bedeutet das für die eingesetzte Hardware, wird es überhaupt noch Unterschiede geben? Wie können die Hersteller darauf reagieren, um zu überleben? Wir haben Cisco speziell eingeladen ihre Vision von der Zukunft ihrer Switch-Hardware vorzustellen. Aber auch andere wesentliche Hersteller sind vertreten und werden an der Diskussion teilnehmen.

Das führt sofort zu weiteren Fragen:

- wie kommen wir zu einem schlüssigen Gesamtkonzept aus physikalischem Netzwerk und Virtualisierung?
- wie sieht die Rollenverteilung zwischen Hardware und Software in Zukunft aus?
- welchen Stellenwert wird die schnelle Bereitstellung von virtuellen Netzwerken bekommen?
- wie weit sind Netzwerke in einzelne austauschbare Komponenten zerlegbar, gibt es einen Trend zu Netzwerken als Gesamt-Architektur?
- wir brauchen mehr Intelligenz in Netzwerken, aber wo soll die herkommen? Was ist aus SDN geworden und wie reagieren die Hersteller auf den Bedarf ein Netzwerk als Service-Maschine zu betrachten?

Alle diese Fragen sind die Basis des Netzwerk-Forums 2017. Um darauf im Detail antworten zu können haben wir folgende Struktur gewählt:

- Tag 1 befasst sich mit den Anforderungen und dem zukünftigen Bedarf. Wir gehen speziell auf die Themen Private Cloud, NSX/VXlan, SDDC, von den Hardware Komponenten zum Gesamtkonzept ein.

Wir freuen uns speziell über die Bereitschaft eines Anwenders seine Erfahrungen in diesem Bereich zu präsentieren.

- Tag 2 analysiert die aktuellen Veränderungen im Netzwerk-Design, auch unter Berücksichtigung der neuen Anforderungen. Wir stellen speziell die Frage, wo das Campus-Design steht und welche Rolle Software Defined in Zukunft im Netzwerk spielen wird.
- Tag 3 ist unser Wireless und Security Tag. In beiden Bereichen sehen wir große Veränderungen kommen. Das WLAN wie wir es kennen kommt unter Druck. Wie weit kann es überleben und wofür setzen wir es in Zukunft ein? Dies wird beendet mit einer Analyse des Stands der Technik im Bereich Sicherheit. Hier sehen wir eine zunehmende Bedrohung alter Konzepte durch Sicherheit aus der Cloud. Wie funktioniert das und was stellen wir dem lokal als Antwort gegenüber?

Wie immer wird unser Netzwerk Forum 2017 um einen speziellen Vertiefungstag ergänzt, der aufgrund seiner hohen Bedeutung auch separat gebucht werden kann. Hier gehen wir in diesem Jahr detailliert auf Netzwerksicherheit ein. Wir glauben, dass dies immer mehr zu einem zentralen Baustein der Netzwerk-Gestaltung wird. Und es wird ein untrennbarer Teil eines Gesamtdesigns. Dies wirft viele kritische Fragen auf, die wir diskutieren und beantworten.

Dies ist unsere Top-Netzwerk Veranstaltung des Jahres 2017. Wie immer trifft sich hier die Branche, um aktuelle und kontroverse Entwicklungen zu analysieren und zu diskutieren.

Sichern Sie sich rechtzeitig einen Platz auf dieser einmaligen Veranstaltung.


Anmeldung an kundenservice@comconsult-research.de

ComConsult Netzwerk Forum 2017

Ich buche den Kongress
ComConsult Netzwerk Forum 2017
 27.03. – 30.03.17 in Köln

- zum Preis von € 2.790,-- netto (4 Tage)
 zum Preis von € 2.390,-- netto (3 Tage)

Bitte buchen Sie mir ein Hotelzimmer

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

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

Programmübersicht ComConsult Netzwerk Forum 2017

Montag 27.03.17**Anwendungs-Architekturen und Kommunikation im RZ**

9:30 Uhr
60 Minuten

Netzwerke zukunftssicher positionieren: welche Anforderungen generiert die IT der Zukunft?
Ergebnisse einer Analyse von ComConsult Research

*Dr. Jürgen Suppan,
ComConsult Reserarch GmbH*

10:30 Uhr
60 Minuten

Underlay / Overlay-Design für RZ-Netze

- Underlay Design
- VXLAN als De-facto-Standard für Overlay Data Plane
- Overlay Control Plane: Varianten
- BGP als De-facto-Standard für Overlay Control Plane
- Teufel im Detail: redundante Anbindung von Servern

*Dr. Behrooz Moayeri,
ComConsult Beratung und Planung GmbH*

11:30 Uhr Kaffeepause

12:00 Uhr
45 Minuten

Das Software-Defined Data Center - Der Paradigmenwechsel in der IT

- Was bedeutet „Software-Defined“?
- NFV statt OpenFlow: Die Virtualisierung des Netzwerks
- Virtualisierung von Sicherheitsfunktionen
- Unterstützung von Anwendungen: Die Anwendung definiert ihre Umgebung
- Integration von Cloud- und Fog-Computing
- SDDC = Private Cloud?
- Wie ändern sich Berufsbilder?

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

12:45 Uhr Mittagspause

14:15 Uhr
45 Minuten

Sind echte Router und Switches nicht mehr gut genug? Brauchen Netzwerker die Virtualisierung wirklich?

- Software Defined Everything: das Ende der Netzwerk-Abteilung?
- Server-, Speicher-, Firewall- und Netzwerk-Virtualisierung und ihre Integration: was bedeutet das eigentlich
- Die Rolle des Netzwerk- und Security-Spezialisten in der Zukunft
- Aktuelle Entwicklung und Planung von Datacenter-Lösungen der Zukunft

Gerd Pflüger, VMware Global Inc.

15:00 Uhr
45 Minuten

Private Cloud für die Berliner Verwaltung

*Axel Freiberg, Frank Dornheim,
IT-Dienstleistungszentrum Berlin*

15:45 Uhr Kaffeepause

16:15 Uhr
45 Minuten

Analytics im Netzwerk

- Welche Daten können erfasst werden?
- Was kann damit erreicht werden?

Markus Harbeck, Cisco Systems GmbH

17:00 Uhr
45 Minuten

Netzwerk-Gestaltung in und mit der Cloud

- Wie werden Netzwerke in und mit der Cloud gestaltet? • Welche Alternativen gibt es?
- Gibt es Funktions-Nachteile?
- Projektbericht: was haben wir gelernt?

Markus Schaub, ComConsult Study.tv

ab 18:00 Uhr Happy Hour**Dienstag, 28.03.17****Netzwerk-Design und Optimierung des Betriebs**

9:00 Uhr
60 Minuten

Modernes Campus Design

- Warum Verfahren wie STP, RSTP und LACP unzureichend sind (Neue Anwendungen in bekannten Protokollen, warum Echtzeit zunehmend unsere Netze dominiert)
- Vorteile moderner Designs mit TRILL, SPB und MC-LAG (Funktionsweise der Verfahren, Standardisierung)
- Warum QoS auch im LAN zu einem Thema wird (Designaspekte bei der QoS Umsetzung)
- Was spricht für ein Design das IP bis in den Accessbereich nutzt?

Markus Geller, ComConsult Research GmbH

10:00 Uhr
60 Minuten

Software-Defined WAN

- Active/Active-Nutzung des privaten WAN und des Internet • Nutzung physischer und virtueller CPE-Komponenten
- Zero-Touch Provisioning
- Erfahrungen aus Ausschreibungen

*Dr. Behrooz Moayeri,
ComConsult Beratung und Planung GmbH*

11:00 Uhr Kaffeepause

11:30 Uhr
60 Minuten

Software Defined - wie entwickelt sich die Technologie in den nächsten Jahren

- Netzwerk Automatisierung und Orchestrierung, wo stehen wir heute
- Automatisierung ohne SDN, Comeback der Fabrics • Künstliche Intelligenz und Netze – das Comeback von „SDN“?
- Intent based Networking: Der Weg von Analytics und ITOA zur Automatischen Netzsteuerung
- Big Data hält Einzug in die Netzsteuerung: Machine Learning als Control Plane des Netzes

*Dipl.-Ing. Markus Nispel,
Extreme Networks GmbH*

12:30 Uhr Mittagspause

14:00 Uhr
45 Minuten

Ethernet und Photonics: neue Entwicklungen für das RZ

- Neue Anforderungen durch Cloud-Dynamik und exponentielle Technologien
- 25,50,100, 200 und 400 GbEthernet und mögliche Alternativen
- Gibt es überhaupt noch Unterschiede in der Switch-Hardware?
- Silicon Photonics: Durchbruch nach schwierigerem Start • Konsequenzen für Betreiber privater RZ-Infrastrukturen

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

14:45 Uhr
45 Minuten

Die Zukunft der Hardware

Markus Harbeck, Cisco Systems GmbH

15:30 Uhr Kaffeepause

16:00 Uhr
45 Minuten

IPv6: Projekterfahrung nutzen!

- Erfahrungen aus Kundenprojekten und der Stand von IPv6
- Klare Tendenzen und Treiber für IPv6 beim Kunden
- Ein klassisches Beispiel für die IPv6-Einführung im Mittelstand: ComConsult Beratung und Planung
- Erfahrungen Nutzen und Herausforderungen der Zukunft erkennen

*Dr. Johannes Dams,
ComConsult Beratung und Planung GmbH*

Programmübersicht ComConsult Netzwerk Forum 2017

**Mittwoch 29.03.17
WLAN und Security**

9:00 Uhr **5G: Infrastruktur der Disruptiven Digitalisierung**
60 Minuten

- Anforderungen durch Disruption, IoT und neue Arbeitsmodelle • Grundlegende Technologien
- Ergebnisse der ersten größeren Testumgebungen
- Von LTE zu 5G: Weg der Standardisierung
Dr. Franz-Joachim Kauffels, Technologie- und Industrie-Analyst

10:00 Uhr **Enterprise WLANs - ein Sammelbecken aus Zukunft und Altlasten**
60 Minuten

- Erfahrungsbericht: Anforderungen und Fallstricke aus der Praxis
- In welche Richtung entwickelt sich WLAN weiter?
- Stand der Dinge bei 802.11ax und 11ay
- Der Dual-Band AP – eigentlich ein Auslaufmodell!
- Sind Gäste-WLANs noch zeitgemäß?
- Wie sehen zukunftssträngige WLAN-Konzepte aus?
Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

11:00 Uhr Kaffeepause

11:30 Uhr **Neue Architektur zum Betrieb moderner WLANs**
60 Minuten

- Betrieb mit komplett virtualisierte Controllern möglich • Hochverfügbarkeit, Hitless Failover bei Controller Ausfall
- Zentrale Steuerung der RF Umgebung für besten Datendurchsatz
- Multi-Tenant-Betrieb, Einsatz in Umgebungen mit verschiedenen Unternehmen oder Sicherheitsstufen • Überwachung in Echtzeit: welche Information gibt es, wie kann sie an andere Systeme weitergegeben werden
Reinhard Lichte, Aruba - a Hewlett Packard Enterprise Company

12:30 Uhr Mittagspause

14:00 Uhr **Sicherheit aus der Cloud: Vorteile und Herausforderungen**
45 Minuten
Dipl.-Inform. Claus Vaupel, Zscaler Germany GmbH

14:45 Uhr **Informationssicherheit in und aus der Cloud**
45 Minuten

- Herausforderung sicheres Cloud Computing in Public Cloud, (virtual) Private Cloud und Hybrid Cloud
- Integration Private Cloud und Provider Cloud
- Standardisierte und zertifizierte Cloud-Sicherheit
- Virtuelle Sicherheits-Gateways und virtuelle Internet DMZ in der Cloud: Mehr als ein Trend!
- Management von WLAN und LAN-Komponenten aus der Cloud
- Rolle der Cloud bei der Abwehr von Distributed Denial of Service (DDoS)
- Data Loss Prevention in der Cloud
- Abwehr zielgerichteter Angriffe durch Cloud-Dienste
Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

15:30 Uhr Kaffeepause

16:00 Uhr **Bessere Netzanbindung, bessere Funktechnik - wozu das alles?**
45 Minuten

- Mobilität am Arbeitsplatz 2021
- Netzanbindung mobiler Endgeräte
- Sichere Kommunikation für mobile Clients
Dipl.-Ing. Dominik Zöller, ComConsult Beratung und Planung GmbH

16:45 Uhr Ende der 3-tägigen Veranstaltung

Donnerstag 30.03.17 - Netzwerksicherheit: Bedrohungen, Herausforderungen, Trends und Best Practice

9:00 Uhr **Abwehr zielgerichteter Angriffe**
90 Minuten

- Angriffsmethoden und Werkzeugkasten
- Notwendigkeit system- und anwendungsübergreifender Strategien
- Erkennung von Symptomen
- Sandboxing
- Protokollierung, 2nd Generation SIEM und Big Data
- Bedeutung eines Information Security System für die Abwehr zielgerichteter Angriffe
- Systematisches Schwachstellenmanagement, Behandlung von Sicherheitsvorfällen
- Vulnerability Scanning: Techniken und Werkzeuge
- Sensibilisierung der Nutzer und Administratoren
- Demonstration

10:30 Uhr Kaffeepause

11:00 Uhr **NAC in der Praxis**
90 Minuten

- Warum IEEE 802.1X immer noch ein Alptraum sein kann
- Best Practice NAC: Wie NAC erfolgreich umgesetzt und betrieben werden kann
- Der Teufel steckt im Detail: Wo sich die Hersteller unterscheiden
- Projektbeispiele
- Typische Fehler in der Praxis
- Evolution von NAC: Von Advanced Monitoring über Profiling bis hin zur Abwehr zielgerichteter Angriffe

12:30 Uhr Mittagspause

13:30 Uhr **Zonenkonzepte als Standardinstrument zur Absicherung der IT**
120 Minuten

- Warum Zonenkonzepte zu einem Standardinstrument geworden sind
- Best Practice für den Aufbau von Zonen
- Zonen im Campusbereich und NAC
- Zonen im Rechenzentrum, zwischen Rechenzentren und über WAN
- Zonen in der Cloud, zwischen Private Cloud und Provider Cloud
- Zonen in der virtualisierten Welt: Wie sehen Zonenkonzepte für Network Overlays aus?
- Virtualisierte Firewalls, Hypervisor-Integration von Firewalls • Welche Zonen braucht man?
- Staging-Umgebungen: Trennung von Entwicklung/Test und produktiver Umgebung
- Zonenkonzepte in der Industrial IT
- Prozesse für den Betrieb einer Zonenarchitektur
- Notwendigkeit der Trennung von Managementverkehr und produktivem / funktionalen Verkehr
- Sichere Administration und Überwachung braucht ein eigenes Zonenkonzept
- Management von Systemen über Management-Ports, Lights-out Management oder über produktive Interfaces
- Entkopplung administrativer Zugriffe durch Sprungserver, Terminal Server, virtuelle Admin-Clients • Protokollierung administrativer Zugriffe
- Storage und Datensicherung
- Projektbeispiele
Dr. Simon Hoff, Dipl.-Math. Simon Oberem, Dipl.-Inform. Daniel Prinzen, Sebastian Wefers, ComConsult Beratung und Planung GmbH

15:30 Uhr Ende der 4-tägigen Veranstaltung

Data Center

Das RZ-Netz der Zukunft

Teil 1: Die Data Center Networking Landschaft und zukunftsorientierte Lösungen

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.

In diesem Teil betrachten wir generelle wichtige Tendenzen und ihren aktuellen und zukünftigen Einfluss auf die Gestalt der privaten RZ-Netze. Im nächsten Teil kommen wir zu wichtigen Entwicklungen bei der Switch-Hardware und einem faszinierenden Anwendungsbeispiel für die Migration auf eine 100G-Umgebung einschließlich eines sehr spannenden architekturellen Ansatzes.

Bei näherer Betrachtung gibt es trotz aller verwirrenden Einflüsse eine Reihe von Entwicklungen, die eindeutig in die gleiche Richtung zeigen. So z.B. die Vernetzung mit 25/50/100 GbE. Was für ein Unternehmen wie z.B. LinkedIn ausreicht, sollte auch für den normalen Betreiber eines privaten RZs eine Obergrenze darstellen. Kann man vielleicht demnächst einfach Bare Metal Switch Hardware beim ODM kaufen statt beim etablierten Markenhersteller? Gerne, es kann aber sein, dass man dann 10.000 Stunden oder mehr für die Entwicklung der Software benötigt.

Um dies alles systematischer (wenn auch ohne wirklichen Abschluss) diskutieren zu können, muss man weiter ausholen. Die Darstellung gliedert sich in vier wesentliche Abschnitte, zwei in jedem Teil.

Zunächst betrachten wir alle heute wesentlichen Einflussfaktoren auf die Data Center Networking Landschaft nochmal in einem zusammenfassenden Überblick. Schon dabei sieht man, dass sich in Zukunft Anforderungen und Lösungen bei unterschiedlichen Betreibern sehr unterschiedlich entwickeln werden.

Im zweiten Abschnitt gehen wir auf Themen ein, die man auch vielleicht als Sonderthemen bewerten kann, die aber wesentliche Schlaglichter auf die allgemeine

Entwicklung werfen. Wir sehen uns an einem Beispiel eine Entwicklung bei einem Content Provider an, die letztlich zu einer SDN-Lösung führt. Dann schauen wir auf die Notwendigkeit guter Anbindungen an das Internet, wenn man tatsächlich viel mit Clouds arbeitet und beleuchten die Rolle von Colocation Providern. Man kann aus diesen Themen eine Reihe von Erkenntnissen gewinnen.

Der dritte Abschnitt (im Teil 2) widmet sich der Entwicklung der Switches für 25/50 und 100 GbE. Es wird erklärt, wie sie aufgebaut sind und warum man sie konstruktiv nicht mit den bisherigen 10/40-Switches vergleichen kann. Natürlich blicken wir hier auch auf die wichtigsten Switch-Chips und einige Produkte bekannter Hersteller, allerdings nicht im Sinne eines Marktüberblicks.

Recht selten bekommt man einen so tiefen Einblick in die Eigenentwicklung eines Betreibers wie bei LinkedIn. Wir können zeigen, wie das Netzwerk grundsätzlich organisiert ist und berichten über Motivationen, Probleme, Lösungen und Vorzüge bei der Schaffung einer eigenen 100G Switching Plattform auf Bare Metal. Wirk-

lich spannend ist eher die Gesamtarchitektur, die nach Ansicht des Autors auch auf kleinere Unternehmen und Organisationen übertragbar ist und mit hoher Wahrscheinlichkeit eine neue Basisarchitektur für RZ-Netze manifestiert.

1. Die Data Center Networking Landschaft

Mittlerweile ist die Netzwerk-Schicht eine der fortschrittlichsten Infrastruktur-Komponenten im RZ geworden. Die Zeiten, in denen einfache Routen festgelegt und damit recht übersichtliche Verkehrsmuster unterstützt wurden, sind vorbei. Heute erzeugt man Kontext-abhängige Policies um Informationen, Nutzer, Anwendungen und sogar ganze Cloud Infrastruktur-Komponenten. Es gibt Automatisierung in dieser Netzwerk-Schicht und in der nächsten SDN-Generation werden Daten- und Control-Plane vollständig abstrahiert.

Die Aufgabe von Administratoren in der heutigen Zeit ist die Schaffung einer im Vergleich zu früher viel intelligenteren Netzwerk-Schicht. Diese „neue“ Netzwerk-Schicht kann mit den meisten fortgeschrittenen Geschäftsmodellen und IT-Anfor-

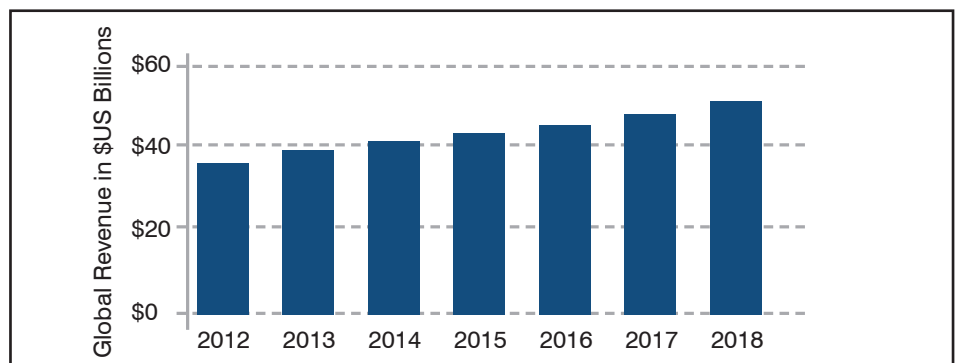


Abbildung 1: Umsatz mit 1G/10G/40G/100G Networking Ports

Quelle: Infonetics Research

Das RZ-Netz der Zukunft - Teil 1: Die Data Center Networking Landschaft und zukunftsorientierte Lösungen

derungen Schritt halten. In einem kürzlich erschienenen Weltweiten Enterprise Networking Report (<http://www.idc.com/getdoc.jsp?containerId=US40211616>) hat IDC herausgearbeitet, dass Virtualisierung nach wie vor einen bedeutenden Einfluss auf das Enterprise Netz haben wird. IDC erwartet, dass all diese Faktoren bisher noch nie da gewesene Anforderungen an Skalierbarkeit, Programmierbarkeit, Agilität, analytische Möglichkeiten und Management-Möglichkeiten von Enterprise Networks haben werden. Für 2016 hatte IDC das Wachstum des Umsatzes mit Enterprise Network Komponenten um 3,5% auf 41,1 Mrd US\$ vorausgesagt. Hier fehlt zur letztlichen Bestätigung noch das vierte Quartal 2016, aber im Großen und Ganzen stimmt das. (siehe Abbildung 1)

Wir werden die Technologie von 25/50/100G im RZ im zweiten Teil dieses Artikels genau besprechen. Sehen wir uns aber schon als Vorgeschmack in Abbildung 2 an, mit welcher Dynamik diese Entwicklung verlaufen wird.

Die wesentlichen Transformations-Faktoren der „3rd Platform“ (Cloud, Mobility, Big Data and Social Business) sind neben IoT und Robotics die wesentlichen Treiber, die uns sicher in den nächsten Jahren noch erhalten bleiben und in ihrem Einfluss sozusagen täglich zunehmen. Ganz besonders wichtig erscheint es, dass die neuen Systeme die Art und Weise ändern, wie Unternehmen „Go-To-Market“-Strategien angehen und wo die Netze der nächsten Generation eine besondere Rolle spielen.

In verschiedenen Darstellungen der letzten Jahre haben wir solche Änderungen und die SDN-Landschaft definiert. Wir

haben uns Technologien und Angebote wie NSX, ACI und auch offene Systeme angesehen. In diesem Artikel möchte ich aber nochmals einen Schritt zurücktreten und einen zusammenhängenden Blick auf die vier Bereiche des Data Center Networkings werfen, die das moderne Business beeinflussen:

- Traditionelles Data Center Networking
- Software-defined Networking SDN
- Network Functions Virtualization NFV
- White/bride Box Networking
- Cloud Networking

Alle diese Möglichkeiten stehen heute in der ein oder anderen Weise zur Verfügung, man kann sie kaufen, in Betrieb nehmen, einsetzen oder Systeme und Dienste mieten. Die wirklich spannende Frage ist doch, zu welchen Anwendungsfällen welche Systeme passen und wie sie in das Bild des RZs bzw. RZ-Netzes passen.

Mit Sicherheit wird es keine Universal-Lösung geben, die in allen Fällen passt. Wir müssen uns leider weitest gehend von recht bequemen Planungs-Mantras verabschieden. Die meisten Unternehmen werden mehrere Technologien gleichzeitig benutzen müssen, um mit den Anforderungen aus den Anwendungen und den Märkten zurecht zu kommen.

1.1 Das traditionelle RZ-Networking

Das traditionelle RZ-Networking hat in den letzten 30 Jahren erhebliche Weiterentwicklungen erfahren. Hersteller wie Cisco (Nyse: CSCO), Arista (Nasdaq: ANET), HPE (Nyse: HPQ), Extreme Networks (Nasdaq: EXTR), Juniper (JNPR) oder Mellanox (Nasdaq: MLNX) sowie weitere, die wir hier aus Platzgründen

nicht nennen können, entwickeln immer weiter integrierte Netzwerk-Systeme für das RZ. Es geht hier nicht darum, die einzelnen Angebote vollständig zu nennen oder gar zu werten, es ist vielmehr wichtig, die übergreifenden Möglichkeiten und die strategischen Ansätze der Hersteller zu verstehen. Cisco setzt schlicht und ergreifend auf die Tatsache, dass man das gesamte Netzwerk und die Fabric Backplane mit ihren Systemen aufbauen kann. Hier gibt es zwar auch die Orientierung an Standards, aber seien wir ehrlich, den größten Nutzen und eine massive funktionale Entfaltung bekommt man nur dann, wenn man ein komplettes Cisco-Ökosystem betreibt. Arbeitet man aber mit kleineren Büros, vielen Zweigstellen oder insgesamt wenigen Benutzern, kann es wirklich nützlich sein, auch zu anderen Anbietern zu schauen. HPE oder auch Dell (privat) sind z.B. dafür bekannt, sinnvolle und stabile Lösungen zu attraktiven Preisen zu liefern. Ein anderer Fall entsteht dann, wenn man wirklich richtig massive Netzwerk-Leistung im RZ vielleicht sogar in Richtung HPC benötigt. Da lohnt sicher ein Blick auf die Angebote von Juniper, Arista und besonders Mellanox. Alle drei Hersteller können Systeme liefern, die fast schon an die Grenze des wirtschaftlich Machbaren in der Hochleistungskommunikation gehen. Mellanox hat zudem den konstruktiven Vorzug, dass der Hersteller zwar „Ethernet“-Switches anbietet, die allen Normen entsprechen, in ihrem Kern aber InfiniBand-Switch Chips haben, die nach außen hin die Ethernet-Schnittstellen auf dieser konstruktiv erheblich besseren Basis bereitstellen. Trotz oder grade wegen dieser konstruktiven Unterschiede sind traditionelle RZ-Netzwerk-Technologien sehr leistungsfähig in den Use-Cases, die sie unterstützen. Wünscht man sich z.B. Konvergenz, sollte man genau hinsehen, welches Netzwerk-Angebot das technisch am gründlichsten unterstützt. In Zukunft wird „Traditionelles Networking“ noch intelligenter und vor allem noch deutlich leistungsvoller. Die Architekturen haben, wenn man genau hinschaut, die Grenzen des RZs vielfach schon überschritten. Spätestens ab 100 G ist es nur noch ein Unterschied im optischen Transceiver, ob eine Verbindung 100 m oder 40 km überbrückt. Wir besprechen die technischen Einzelheiten im zweiten Teil des Artikels.

Konsequenzen für private RZs und ihre Netze: das traditionelle RZ-Networking ist weiterhin die Basis für den wirtschaftlichen und leistungsfähigen Betrieb der IT-Infrastruktur. In vielen RZs gibt es Anwendungen, die schon seit Jahrzehnten irgendeine Funktion haben und auch

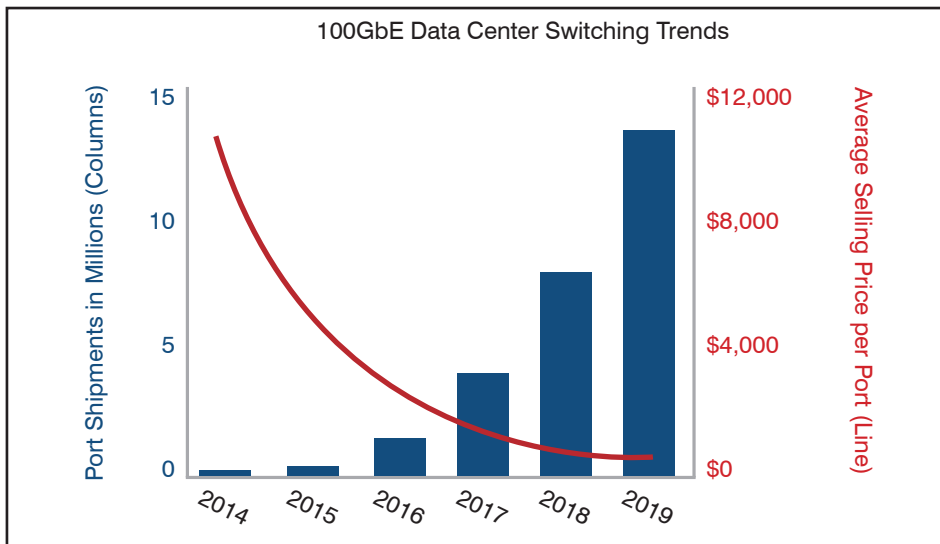


Abbildung 2: 100 GbE Data Center Switching Trends

Quelle: Crehan Research

Das RZ-Netz der Zukunft - Teil 1: Die Data Center Networking Landschaft und zukunftsorientierte Lösungen

weiterhin unverzichtbar sind. Das können durchaus Tausende sein. Es wird nicht möglich sein, sie alle in eine Cloud-Lösung zu überführen. Um arbeiten zu können, benötigen sie vielleicht Kommunikationsschnittstellen älterer Bauart. Die eigentlich völlig aufgeblähten Protokollstacks der Vergangenheit werden nicht so schnell verschwinden, vor allem nicht vollständig. Eine passende Lösung für ein RZ-Netz ist also immer ein Spagat zwischen Tradition und Zukunft. Das macht es auch so schwierig, generelle Lösungsrezepte anzugeben, denn jede Ausgangslage ist individuell. Wichtig ist es, für die Zukunft Netzwerk-Architekturen, Hardware und Software zu finden, die mit den Komponenten zusammenarbeiten, die noch die älteren Systeme unterstützen müssen, aber dennoch die Ausrichtung auf eine modernere Zukunft nicht verbauen. Deshalb hält der Autor auch nach über 30 Jahren daran fest, dass nur standardisierte und offene Lösungen in diesem Umfeld einen dauerhaften Platz verdienen. Im nächsten Teil dieses Artikels konkretisieren wir die Technik und eine mögliche besonders günstige Grundstruktur.

1.2 Software Defined Networking SDN

SDN ist für viele Organisationen, die versuchen, mehr Intelligenz in ihr Netz zu bringen, eine großartige Technologie. Hier gibt es einige grundsätzliche Überlegungen. Anbieter wie Cisco (mit ACI) oder Arista (mit EOS) haben SDN erheblich dadurch gefördert, dass sie es aus der Experimentier- und Bastel-Ecke herausgeholt und nahtlos in ihre Hardware und Software integriert haben. Wir haben ja schon in diesem Medium mehrfach dargestellt, dass SDN nur dann richtig funktionieren kann, wenn auch die Hardware und zwar auch auf der Chip Ebene entsprechend vorgerüstet ist und z.B. Flows direkt in Hardware unterstützt werden können. Auf dieser Grundlage haben Hersteller wie VMware (mit NSX) die SDN-Kontrolle in das gesamte Virtualisierungs-Ökosystem integriert. Schließlich gibt es noch die Open Source und OpenSDN-Anbieter wie Cumulus Networks (privat), Plexxi (privat) oder BigSwitch (privat). Sie schaffen leistungsfähige Netzwerk-Overlays und Integrationstechnologien für viele Anwendungen. Alleine in diesem Szenario ergeben sich drei grundsätzliche Alternativen, mit denen man arbeiten kann. Hat man bereits in RZ-Technologien z.B. von Cisco und Arista investiert, macht es wahrscheinlich ziemlich viel Sinn, mit diesen Technologien weiter zu arbeiten. Die Integration von was auch immer wird ganz gut funktionieren, man hat eine kürzere Lernkurve und man kann bestehende Investi-

tionen weitest gehend schützen. Die Arbeit mit SDN auf der Hypervisor-Ebene macht besonders dann Sinn, wenn man die Virtualisierung bereits in einem hohen Maß vorangetrieben hat und den Verkehr zwischen und mit den VMs besser kontrollieren möchte. SDN in diesem Kontext liefert zwar nicht immer den besten Blick auf die physikalische Netzwerk-Ebene (es ist ja grade der Sinn, mit den dazu gehörigen Tunnelprotokollen das physikalische Netzwerk so gut wie möglich zu verdecken) wird aber sicherlich eine große Hilfe bei der Organisation und Kontrolle der verteilten VM Architektur sein. Natürlich gibt es auch hier Bedenken, was Kompatibilität und Weiterentwicklung anbetrifft. Neben VMware (Nasdaq:VMW) sind mindestens Microsoft (Nyse: MSFT) und Red Hat (Nyse: RHT) seit Jahren ernst zu nehmende Anbieter von Virtualisierungssystemen. Kern einer jeden Netzwerk-Virtualisierung ist ein Tunnelprotokoll. Mit VXLAN gibt es zwar einen Industrie-Standard dafür, aber Switch-Chip-Hersteller wie Broadcom (Nasdaq: AVGO) müssen zu eigenen generischen Überformaten greifen, um die Funktion abzusichern. Es gibt auch Leistungsbedenken, denn die Protokolle des physikalischen Netzes müssen durch Tunnel-

End Punkte (TEPs) terminiert und in die virtuelle Umgebung überführt werden. Nicht immer werden diese TEPS wie bei bestimmten Broadcom Chips per Hardware unterstützt. Das alles hat zwar Cisco nicht daran gehindert, in den meisten Netzwerk-Segmenten Marktführer zu werden, aber es gibt auch immer die durchaus wohl begründete Tendenz, sich nicht vollständig von einem Hersteller abhängig zu machen. Weiter in die Vergangenheit zurückblickend gab es ja mit 3Com und Nortel selig massive Abflüge, und auch heute ist der absteigende Ast prominent besetzt. Statistisch mehr Kopfschmerzen bereiten allerdings die gegenseitigen Aufkäufe, wo man nie sicher weiß, was aus den Systemen des Targets werden wird. Grade in 2016 gab es ja eine regelrechte Kaufwelle für WLAN-Anbieter, was die Vielfalt des Angebots deutlich eingeschränkt hat. Dem entsprechend ist es ein aufkommender Trend, mit offenen SDN-Lösungen zu arbeiten. Hier sind vor allem jedes Unternehmen vorne, die schon in der Vergangenheit aus gutem Grund Bindungen an Hersteller gescheut haben wie der Teufel das Weihwasser, z.B. Service Provider. Möchte man eine eigene kundenspezifische Netzwerk-Lösung haben, kann

Kongress

ComConsult Netzwerk Forum 2017 27.03. - 30.03.2017 in Köln

Das ComConsult Netzwerk-Forum 2017 stellt die vier momentan dominantesten Netzwerk-Themen in den Mittelpunkt der Veranstaltung: Anwendungs-Architekturen und Kommunikation im Rechenzentrum, Netzwerk-Design und Optimierung des Betriebs, WLAN-Design und die Herausforderungen neuer Standards, Netzwerk-Sicherheit in einem Cloud-Umfeld.

Der optionale vierte Tag des ComConsult Netzwerk Forums widmet sich traditionell einem Schwerpunktthema, welches wir gemeinsam mit Ihnen intensiv beleuchten möchten. In diesem Jahr steht der „Netzwerksicherheit: Bedrohungen, Herausforderungen, Trends und Best Practice“ im Fokus.

Wie in jedem Jahr so wird auch 2017 das ComConsult Netzwerk-Forum der Treffpunkt der Branche sein. Top-Referenten, die Analyse der neuesten Entwicklungen, praxisnahe Empfehlungen, mehr Sicherheit für Ihre Entscheidungen und viele, viele Diskussionen prägen diese Veranstaltung. Versäumen Sie nicht sich rechtzeitig einen Platz zu sichern.

Top-Referenten, die Analyse der neuesten Entwicklungen, praxisnahe Empfehlungen, mehr Sicherheit für Ihre Entscheidungen und viele, viele Diskussionen prägen diese Veranstaltung.

Preise: € 2.790,- netto - 4-tägige Veranstaltung mit Thementag
€ 2.390,- netto - 3-tägige Veranstaltung ohne Thementag



Buchen Sie über unsere Web-Seite

www.comconsult-akademie.de

Das RZ-Netz der Zukunft - Teil 1: Die Data Center Networking Landschaft und zukunftsorientierte Lösungen

die Zusammenarbeit mit Anbietern offener Lösungen zu sinnvollen Ergebnissen führen. Man sollte aber nicht vergessen, dass man sich hier schnell auf absolutes Neuland begibt und immer eine etwas längere Lernkurve benötigt. Wir haben gleich ein sehr schönes Beispiel dafür.

Konsequenzen für private RZs und ihre Netze: die Diskussion über SDN gibt es schon viele Jahre. Bis jetzt ist die Industrie den Nachweis schuldig geblieben, dass SDN auch für RZ-Netze durchschnittlicher Unternehmen und Organisationen einen nachvollziehbaren Nutzen bringt. Bei Providern und Hyperscalern sieht das ganz anders aus. Blickt man aber genauer auf die veröffentlichten Anwendungsbeispiele, steckt meist noch viel Eigenentwicklung in ihnen. Das können „normale“ RZ-Betreiber nicht leisten. Wichtig erscheint es aber in diesem Zusammenhang, in der Zukunft wirklich ausschließlich Hardware einzusetzen, die eine mögliche SDN-Lösung zu einem späteren Zeitpunkt nicht behindert. Das dies möglich ist, sehen wir bei Cisco. Nur ein vergleichsweise übersichtlicher Teil der Kunden der neueren Switch-Generationen nutzt wirklich ACI. Die anderen „fahren“ mit der Weiterentwicklung der älteren Betriebssysteme. Das wird sich im Laufe der Zeit sicherlich verschieben. Aber eben über einen längeren Zeitraum. Der zweite Abschnitt dieses Artikels zeigt genauer, wie SDN bei einem Provider genutzt werden kann und wie das aufgebaut wurde. Man sieht sofort, dass Vieles nicht wirklich auf die Verhältnisse „normaler“ Betreiber übertragbar ist.

Es ist eigentlich schwierig, einer Industrie, die mit langen Abschreibungszyklen arbeitet, irgendeine Art von Revolution nahe zu bringen, aber beim Networking gibt es gleich zwei: **SDN und NFV**. Beide stellen revolutionäre Entwicklungen dar und der Erfolg des Versuchs, wirklich positive Änderungen herbeizuführen, könnte davon abhängen, beide harmonisch zu implementieren, so dass sie sich gegenseitig unterstützen. Können wir die „Harmoniepunkte“ identifizieren, gewinnen wir Erkenntnisse über das Netz der Zukunft.

1.3 Network Functions Virtualization NFV

NFV wird zwar gerne in einem Atemzug mit SDN genannt (und hängt auch damit zusammen), ist aber eigentlich eine zunächst eigenständige Initiative, Netzwerk-Funktionen, die bisher von proprietärer, spezialisierter Hardware realisiert werden, zu virtualisieren und auf diese Weise ihre Implementierung in den Rahmen eines handelsüblichen General-

Purpose Servers zu stellen. Wenn es erfolgreich ist, reduziert das Konzept die Menge proprietärer Hardware, die für die Etablierung und den Betrieb von Netzwerk-Funktionen und – Dienstleistungen benötigt wird. Das Ziel ist es, Netzwerk-Funktionen, die von spezieller Hardware wie Router, Firewalls, Load Balancer oder anderen Spezialgeräten zu entkoppeln und Netzwerk-Services aufzubauen, die auf Virtuellen Maschinen (VMs) laufen. Sobald die Netzwerk-Funktionen unter der Kontrolle eines Hypervisors stehen, können die Services, die bisher spezielle Hardware gebraucht haben, z.B. auf einem Standard X86-System realisiert werden. Dieses Konzept ist vor allem von Bedeutung, wenn es Netzwerk Administratoren erlaubt, Dienstleistungs-Ketten aufzubauen, ohne spezielle Hardware einbeziehen zu müssen. Da im Rahmen eines geeigneten Virtualisierungskonzeptes Server-Leistung durch Software hinzugefügt werden kann, gibt es keine Notwendigkeit mehr dafür, Leistungen in einem RZ zu überprovisionieren. Ein gutes VM-Konzept erlaubt eine wesentlich bessere Granularität als jede Spezial-Hardware. Braucht z.B. eine Anwendung auf einer VM mehr Bandbreite, kann der Administrator diese VM auf einen anderen Server verlagern, der mehr physikalische Bandbreite hat, oder eine weitere VM auf dem ursprünglichen Server definieren, die einen Teil der Last übernimmt. Zusätzlich werden mit jedem Konzept der Server-Virtualisierung sozusagen „natürlich“ hervorragende Möglichkeiten zur Realisierung eines unterbrechungsfreien Betriebs bereitgestellt, die weit über das hinausgehen, was man

z.B. mit einer Verdopplung einer Spezial-Hardware erreichen könnte. Eigentlich reduziert dies CapEx und OpEx deutlich. Man muss aber auch erwähnen, dass die Wirtschaftlichkeit von NFV-Konzepten vielfach durch ein wirklich unerschämtes Kostenmodell für die Virtualisierungssoftware zunichte gemacht werden kann. Das muss man im Einzelfall natürlich vorher genau prüfen. Generell trägt NFV die Möglichkeit in sich, die Agilität einer IT-Abteilung z.B. bei sich ändernden Geschäftszielen oder Anforderungen an Netzwerk-Dienste deutlich zu verbessern, was ebenfalls einen Mehrwert darstellt.

Wie hängen NFV und SDN zusammen? NFV ist ein ganz anderes Konzept als SDN, aber sie ergänzen sich prima. Wenn SDN auf einer NFV-Infrastruktur läuft, forwardet SDN die Datenpakete von einem Netzwerk-Gerät zu einem anderen, während die Kontroll-Funktionen für das Netzwerk-Routing auf einer VM laufen, die z.B. in einem Server in einem Rack implementiert ist, um nur ein Beispiel zu nennen. SDN ist aus zwei ziemlich unterschiedlichen Problemen der Netzwerk-Industrie entstanden. Aufbau und Verwaltung großer IP/Ethernet-Netze wurden angesichts der adaptiven Natur von Packet Forwarding für beide Protokolle zunehmend komplex. Man hat gehofft, Traffic Management und die Effizienz des Betriebs zu verbessern, wenn man eine zentrale Kontrolle über das Forwarding hat. Frühe Beispiele von Anwendern wie Google haben diese Annahme bestätigt. Der zweite gravierende Problemkreis ist durch das Cloud Computing entstanden. Hier erzeugt man ein neues

Seminar

RZ-Kopplung: Georedundanz für Rechenzentren am 13.03.2017 in Berlin

Die gestiegene Bedeutung von zentralen IT-Systemen für Unternehmen und gesetzliche Vorgaben erfordern geo-redundante Standorte von Rechenzentren. Für die Bereitstellung und den Betrieb der Rechenzentrums-Kopplung wird besonderes Know-how und strategische Planung benötigt. In diesem Seminar werden die aktuellsten Technologien und Anforderungen vorgestellt und ein optimales Gesamtkonzept beschrieben.

Das Seminar wendet sich an Planer und Betreiber von Rechenzentren, die sich mit der Notwendigkeit konfrontiert sehen, ihre RZ-Infrastrukturen über mehrere Kilometer oder gar die Grenzen von Regionen hinweg zu koppeln.

Referent: Dr. Behrooz Moayeri

Preis: € 1.090,- netto



Buchen Sie über unsere Web-Seite

www.comconsult-akademie.de

Das RZ-Netz der Zukunft - Teil 1: Die Data Center Networking Landschaft und zukunftsorientierte Lösungen

Modell für die Entfaltung von Anwendungen, bei dem sich Teilnehmer öffentliche Rechenzentren „teilen“, ohne in irgendeiner Weise zu interferieren und Applikationen in flexiblen Ressource Pools bereitgestellt werden müssen, ohne die Kontrolle über Leistung und Sicherheit zu verlieren. Es ist kein Wunder, dass sich angesichts dieser Vorgaben gleich drei SDN-Modelle entwickelt haben. Eines basiert auf einer zentralisierten Kontrolle mit OpenFlow Controllern, ein anderes hängt davon ab, SDN zu verwenden, um mit Hilfe von Netzwerk-Overlays Netzwerk-Virtualisierung aufzubauen und zu verwalten und das Dritte ist ein verteiltes Modell, bei dem eine höhere Software-Schicht mit dem Netzwerk und seinen existierenden Protokollen kommuniziert. Netzwerk Funktions Virtualisierung NFV ist eigentlich eine Initiative der Carrier, um teure Spezial-Hardware loszuwerden und die Funktionen auf normalen Servern implementieren zu können. In einem grundsätzlichen White Paper (https://portal.etsi.org/NFV/NFV_White_Paper.pdf) wurde ein Pool Virtueller Funktionen, ein Pool von Betriebsmitteln und ein Kompositions/Orchestrierungs-Prozess definiert, der beide miteinander verbindet (siehe Abbildung 3). Das White Paper ist jedem Interessenten ans Herz zu legen. Man sieht, dass sich NFV und SDN überlappen, aber SDN keine Untermenge von NFV ist und umgekehrt. Wo schneiden sie sich nun und wie wird die Interaktion zwischen ihnen die Weiterentwicklung beider Ideen beeinflussen? Da gibt es viele Möglichkeiten. NFV könnte z.B. die zentralen Kontroll-Funktionen von SDN als virtuelle Funktionen implementieren, so dass also z.B. OpenFlow Switches von NFV-Software gesteuert werden können. Firewalls und Load-Balancing Anwendungen sind ebenfalls lohnende Ziele für NFV, da sie eine SDN-ähnliche Trennung von Forwarding und Kontrolle haben. NFV kann auch zentrale Kontrolle und Verwaltung von Netzen realisieren, die mit höheren Protokollen wie BGP und MPLS arbeiten oder aber auch Konfiguration und Management von Optischen Übertragungsressourcen (DWDM) definieren. Letztlich kann man auch sagen, dass NFV ein Modell für virtuelle Funktionen darstellt, die in einer Cloud gehostet werden. Jede Sammlung virtueller Funktionen, die einen nutzbaren Service bereitstellen, kann als „Kunde“ einer NFV Infrastruktur betrachtet werden. Diese „Multi-Tenant“ Einflüsse bewegen NFV in Richtung eines Netzwerk-Modells mit Software-Overlay. Und da kommt SDN ins Spiel. Ein solches Modell, welches aus Tunneln und vSwitches besteht, hindert virtuelle Funktionen daran, unglücklich oder absichtlich zu interagieren und bildet eine Brücke zu aktuellen virtuellen Netzwerk-Schnittstellen im Cloud Compu-

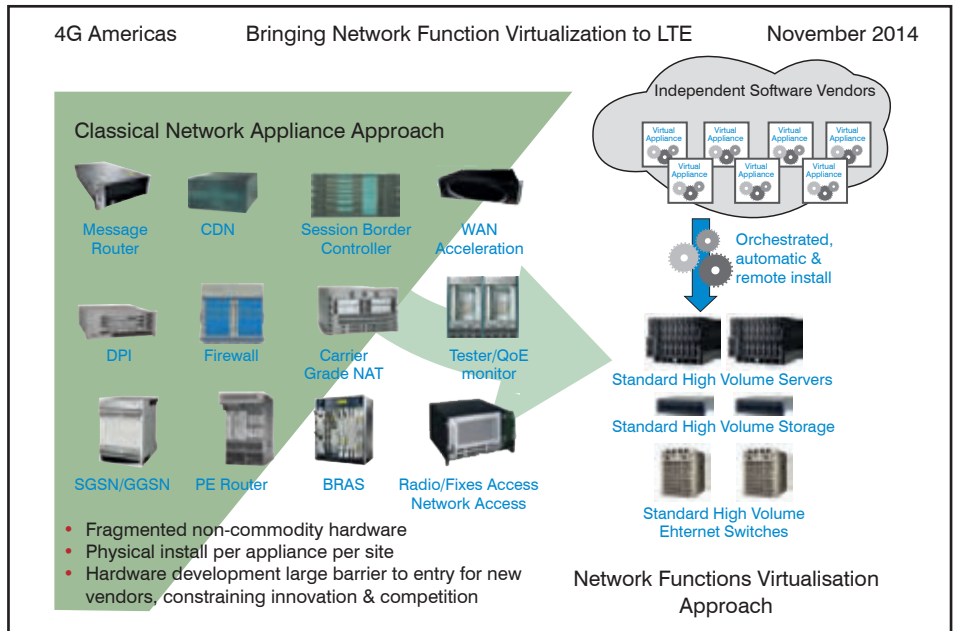


Abbildung 3: Vision für NFV

Quelle: ETSI

ting wie Neutron von OpenStack (früherer Name Quantum). (siehe Abbilung 4)

Kommt das Ganze nun auch voran? Provider haben schnell gelernt, dass die Entwicklung und Integration virtueller Netzwerk Funktionen in die heute existierenden Multi-Vendor Umgebungen zu neuen Herausforderungen hinsichtlich der Interoperabilität führen. Daher haben führende Hersteller für Systeme der Optischen Kommunikation (im Fernbereich) wie Cisco, Ericsson, Huawei und Nokia im Januar 2017 ein „Memorandum of Understanding“ zur Schaffung der so genannten „Network Functions Virtualization Interoperability Testing Initiative“ (NFV-ITI) unterschrieben, die dazu dient, die Probleme mit NFV Entwicklungen und Cloud Transformation innerhalb von Multi-Vendor-Netzen zu lösen. Die Mitglieder von

NFV-ITI kooperieren bei der Unterstützung von Interoperabilität von NFV-Elementen in spezifischen Kundensituationen, um kommerzielle Implementierungen zu beschleunigen. Es gibt zwar schon eine Anzahl anderer Initiativen in dieser Richtung, die haben bis jetzt aber kaum gezündet. NFV-ITI arbeitet eng mit der ETSI NFV Spezifikation Group und dem OPNFV-Projekt zusammen.

Konsequenzen für private RZs und ihre Netze: NFV ist sehr spannend. Abgesehen von den möglichen Kosteneinsparungen ist die Möglichkeit, Flexibilität und Zuverlässigkeit der Implementierungen von Netzwerkfunktionen im Rahmen geeigneter Virtualisierungskonzepte deutlich zu steigern eine der wesentlichsten Verbesserungen der letzten Jahre. Was zunächst den Providern durchschlagenden Erfolg

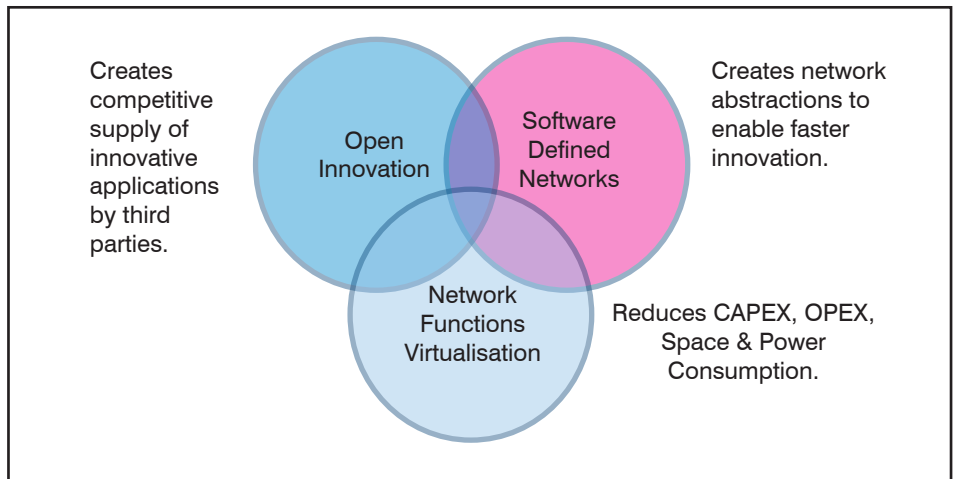


Abbildung 4: Verhältnis zwischen SDN und NFV

Quelle: ETSI

Das RZ-Netz der Zukunft - Teil 1: Die Data Center Networking Landschaft und zukunftsorientierte Lösungen

bringt, lässt sich auch durchaus herunter skalieren. Probleme mit heterogenen Lieferanten gibt es eher selten. In der aktuellen Diskussion fällt auf, dass die für die systematische Umsetzung notwendigen Tunnelkonzepte bei vielen Anwendern überhaupt nicht auf Gegenliebe stoßen. Rein technisch ist das unbegründet, weil es sehr leistungsfähige Unterstützung aus der Hardware geben kann, wenn man die richtigen Chips wählt. Natürlich möchte man seine Abhängigkeit, sagen wir mal von Cisco, nicht noch durch eine Abhängigkeit von sagen wir mal VMware erweitern. Man würde ja damit Regen, Traufe und alte Badewanne zusammen montieren. Ich sehe hier aber keine wirkliche Beharrung im Markt, in absehbarer Zeit werden sich Alternativen entwickeln, mit denen wir gut leben können. Darüber wird ausführlich zu diskutieren sein.

1.4 White/Brite Box Networking

Ein wirklich starker Trend bei größeren RZs und Service Providern ist White/Brite Box Networking. Was ist der Unterschied zwischen White und Brite? Eine White Box ist eine Hardware-Komponente, die im Kern die enthaltene Hardware zur Nutzung bereitstellt. Ein Beispiel dafür wäre ein QuantaMesh Switch. Der Quanta (Other OTC: QUCPY) T1048-LB9 z.B. ist ein Bare Metal Switch mit dem Standard Broadcom Trident Chipsatz. Für knapp 2.500 US\$ kommt er mit 48 1G Ports, 10G nachrüstbar. Steuerung mit Puppet, Chef, CFE-Engine, Integration in NSX und Open Stack und ein bisschen Management Software. Für 8000,- US\$ gibt es einen 32-Port 40GbE-Switch mit dem Trident II. Beide arbeiten mit Cumulus Linux. Brite Box Networking steht einfach für gebrandete White Boxes, wenn man z.B. Cumulus Linux mit einem solchen Switch zusammenpackt und ein Schildchen von Dell, HPE oder SuperMicro draufklebt. Diese Bewegung darf man nicht unterschätzen. Gardner erwartet, dass 2018 das „nicht-traditionelle Switching“ für mehr als 10% der global ausgelieferten Data Center Ports verantwortlich sein wird, 2013 waren es unter 4%. Es ist aber nicht zu erwarten, dass White / Brite Box Networking ein wirklich allgemeiner Trend sein wird. Aktuell ist es in der Realität auf große Service Provider, Cloud Hosts und Organisationen, die kundenspezifische Hyperscale-Lösungen kreieren, beschränkt. Wer mit derartigen Systemen arbeiten möchte, weil der Anwendungsfall dafür günstig ist, muss vor allem sicherstellen, dass der Support funktioniert. Außerdem wird auch Personal mit spezialisierten Kenntnissen benötigt.

Wir werden im zweiten Teil sehr ausführlich auf die Technik eingehen und das Thema nochmals aufgreifen. Daher an

dieser Stelle keine „Konsequenzen“.

1.5 Cloud Networking

Mittlerweile hat sich ein großes, breit angelegtes Universum aus Cloud-Lösungen ergeben und die Vernetzung spielt dabei eine sehr wichtige Rolle. Cloud Networking ist eine wichtige Aufgabe für Unternehmen und Organisationen, die ihre Rechenzentren in Richtung eines Cloud-Ökosystems erweitern wollen. Es gibt eine Vielzahl von Plattformen, die dabei helfen sollen, Netzwerk-Komponenten des Rechenzentrums sozusagen in die Cloud zu „verlängern“. Nehmen wir als Beispiel ein offenes Produkt, OpenStack Neutron. Neutron erzeugt eine „Network-as-a-Service“ Umgebung, die eine Schnittstelle zwischen den Netzwerk-Geräten im RZ und denjenigen, die von anderen OpenStack-Dienstleistungen und -Ressourcen verwaltet werden. Versucht man, das RZ in Richtung einer Cloud zu erweitern und dann die eigene Cloud mit anderen Cloud-Diensten und Hosts zu verbinden, kann es durchaus sinnvoll sein, mit OpenStack als übergreifende Management-Lösung zu arbeiten. So könnte man z.B. eine mehrschichtige Architektur zur Bereitstellung von Anwendungen oder eigene, weiter entwickelte Netzwerk-Services aufbauen, die sich in das OpenStack Ökosystem einfügen. Auch wenn man vielleicht nie damit arbeiten darf, lohnt sich ein Besuch auf der Website <https://platform9.com/support/networking-with-openstack-neutron-basic-concepts/> und bei mehr Interesse <http://de.slideshare.net/mestery/openstack-neutron-tutorial>

Nach dem, was ich in den letzten Jahren gehört habe, könnte Neutron wirklich ganz oben auf der Wunschliste eines jeden Netzwerk-Nerds stehen. Allerdings wird es heute zunächst von Providern benutzt, weil man genau damit eine sehr granulare Kontrolle und sehr leistungsfähige Werkzeuge zur Customization von Netzwerk-Funktionen und -Diensten bekommt. Es vereinfacht das Management und die Integration in komplexe Cloud-Umgebungen.

Konsequenzen für private RZs und ihre Netze: Unternehmen und Organisationen werden auch in den nächsten Jahren immer mehr Daten durch die Netzwerk-Schicht ihres RZs leiten. Mit immer dichterer Virtualisierung und der erhöhten Akzeptanz von Cloud Lösungen wachsen die Abhängigkeiten von der Netzwerk-Schicht immer weiter, genauso, wie die Anforderungen an ihre Leistung, Zuverlässigkeit, Sicherheit und Wirtschaftlichkeit. Rohit Mehra, Vize-Präsident für Netzwerk-Infrastrukturen bei IDC, formuliert es so: „Das Netzwerk wird ein immer bedeuten-

deres strategisches Element vieler Business-Strategien und in vielen Fällen ist es das Rückgrat, was die Weiterentwicklung der Unternehmen stützt. In 2016 sehen wir, dass sich dies weiter verfestigt, weil Entscheider der Unternehmens-IT neue Technologien suchen, die eine höhere Effizienz haben, indem sie das Physikalische zum Virtuellen entwickeln, APIs bewegen und bessere Wege zur Einbindung von Kunden schaffen, wodurch sie den Wert bereits existierender Netzwerk-Installationen steigern.“

2. Lösungen außerhalb privater RZs von Unternehmen und Organisationen

Im ersten Abschnitt haben wir unterschiedliche Facetten des RZ-Networkings subsummiert. Dabei konnte man sehen, dass die neueren Techniken heute offensichtlich eher in komplexeren Umgebungen als „normalen RZs“ eingesetzt werden. Ganz klar benötigt man dafür Personal mit einem überdurchschnittlichen Ausbildungsstand. Der normale Netzwerk-Administrator wäre damit aktuell eher überfordert, abgesehen von anderen Problemen wie der Sicherstellung von Support und den sicher nicht geringen Kosten. Dennoch lohnt es sich wirklich, einen Blick darauf zu werfen, was man heute schon erreichen kann und welche Erkenntnisse man mitnehmen konnte. Denn wie immer, werden sich komplexere Technologien mit der Zeit sozusagen „nach unten“ durchschütteln, mal mehr, mal weniger. Prosaisch formuliert zieht genau dieser Prozess eine Art „konzeptionelle Reinigung“ mit sich. Er ist ein Filter, in dem alles hängen bleibt, was doch nicht so nützlich wie gedacht oder aus anderen Gründen ungeeignet ist.

Die Betreiber von Hyperscale-Rechenzentren haben schon seit längerer Zeit herausgefunden, dass die beste Methode, dem Netz mehr Flexibilität zu verleihen, in der Trennung von Daten- und Kontrollebene besteht. Die beste Methode, relativ zügig zu einem weitestgehend automatisierten Betrieb zu kommen, ist offensichtlich, Hersteller-spezifische Software herauszuwerfen und sie durch Linux-basierte Betriebssysteme und Tools zu ersetzen, wobei man zusätzlich von der Macht der weitreichenden Erfahrungen mit derartigen Entwicklungsumgebungen profitieren kann. Ein gangbarer Weg zur Reduzierung der Kosten scheint es zu sein, die nach eigenen Spezifika im Auftrag gebauten Custom White Boxes mehr wie Server und weniger wie Switches zu betreiben.

Telcos wiederum haben erkannt, dass die einzige sichere Methode, den sich dynamisch und dramatisch ändernden

Das RZ-Netz der Zukunft - Teil 1: Die Data Center Networking Landschaft und zukunftsorientierte Lösungen

Bedarfen des Marktes auch in Zukunft nachzukommen, darin besteht, Netze aufzubauen, die permanent dynamisch per Software rekonfiguriert werden können. Das wird besonders klar, wenn man sich den Übergang von 4G/LTE via LTE Advanced zu 5G anschaut. Natürlich gibt es mehr mögliche Stationen pro Flächeneinheit und deutlich mehr mögliche Leistung pro nutzender Subscriber-Station, spannend ist aber vor allem das enorme Spektrum der Anschlussalternativen. Ein Wärmehäuser an einer Heizung muss vielleicht einmal pro Tag ein paar Bits versenden und bewegt sich dabei hoffentlich eher wenig. Millionen andere Nutzer möchten mit Gigabit-Tempo Videos streamen oder laden und schließlich kommen in den nächsten Jahren ja auch noch die gesamten Systeme von Smart Cities bis zu den autonomen Fahrzeugen hinzu. Außerdem haben Provider herausgefunden, dass große Marktchancen darin liegen, Funktionen, die üblicherweise an Hardware-Boxen gebunden sind, als Software-Services zu vermarkten. Content Provider wie Netflix wären ohne Telcos arbeitsunfähig. Die Telcos werden sich das nicht mehr lange anschauen und versuchen, als Gesamtanbieter aufzutreten. Die Absicht von AT&T (Nyse:T), Time Warner (Nyse: TWX) zu kaufen, ist nur der erste dickere Stein einer Lawine. Allerdings könnte das auch anders herum funktionieren, Disney (Nyse:DIS) hätte genug Geld für ein paar kleinere Provider. Je stärker die bisherigen TV-Kabelnetze unter Druck kommen, desto stärker wird diese Bewegung. Wie auch immer kann man dies alles mit der bisherigen starren hierarchischen Struktur nicht bewerkstelligen. Hier benötigt man eine andere Art flexibles Netzwerk mit vollständig virtualisierten Ressourcen. Auch wenn man noch so viele sehr teure neue Seekabel legt, wird man nicht umhinkommen, die Übertragungskapazität sinnvoll zu verwalten. Spätestens, wenn man auf die vielen neuen menschlichen und maschinellen Benutzer und deren Wunsch nach flexiblen Diensten mit dynamischer Provisionierung blickt, wird klar, dass am Ende nur die vollständige Automatisierung mit möglichst wenig notwendigen menschlichen Administratoren sein kann. Sie wären schlicht zu langsam.

Hyperscaler und Telcos wissen also schon, wie sie vorgehen wollen. Die spannende Frage ist: was passiert eigentlich mit und in privaten Rechenzentren? Können wir auch hier einen gangbaren Weg zu einem Redesign finden, der auch diesen RZs den Weg in die Zukunft ebnet? Es wird einen Weg geben, aber er wird nicht für alle gleich aussehen (einfach weil auch die Anforderungen unterschiedlich

sind) und in jedem Fall zu heftigen Diskussionen führen.

Dazu ist es hilfreich, sich zwei aktuelle Entwicklungen anzusehen. Zum einen blicken wir einmal tiefer in die Entwicklung eines wirklich sehr großen Provider-Netzes. Zum anderen kommen wir auf die spannende Frage, wie Unternehmen in Zukunft auf Cloud-Lösungen zugreifen können. Reicht die Anbindung über das Internet wirklich?

2.1 CORD für Telcos: ein LINUX-Projekt mit Rückendeckung durch Google

Nach Volumen sind die Telco Provider vermutlich der größte Verbraucher von Computing Power. In den vergangenen Jahren haben die Telcos dieser Welt Ingenieure und Entwickler fast schon verzweifelt darum angefleht, eine richtige Cloud zu bauen, die für ihre Zwecke gut funktioniert: eine, die aufgestellt, provisioniert und betrieben werden kann wie ein normales Rechenzentrum. Nur deutlich größer. Sind wir doch mal ehrlich: eine Idee wie SDN oder ein Standard wie Open Flow oder gar eine quasi proprietäre Tunnel-Lösung (einer definiert, fünf nicken begeistert) sind ja für sich gesehen ganz nett, aber zunächst kann man damit keinen verschimmelten Cent verdienen. Nein, man benötigt eine komplette Architektur, die dann solche Komponenten enthält, aber insgesamt auch zu arbeitsfähigen Produkten führt. Vor Kurzem wurde eine solche Architektur von ihren Schöpfern als „Bereit für die Tests auf Herz und Nieren“

gekennzeichnet. Die bislang als „Central Office Re-architected as a Data Center“ bezeichnete Architektur wurde offiziell CORD-Projekt getauft und steht unter der Aufsicht der Linux-Foundation. Einer der Vorteile von CORD ist seine Installation als Open Source Projekt mit eigenem Board, eigener Überwachung, eigenem Steuerungsteam und passender Community. Im Open Networking Lab (onlab.us) wird CORD vorangetrieben und das Potential der Plattform erkundet und erweitert.

Letztlich ist CORD eine Spezifikation für gewöhnliche Commodity Server in Central Offices von Providern. Sie umfasst Architektur und Anordnung von Server Racks sowie der Access Racks, die mit ihnen in Zusammenhang stehen. Weiterhin gibt es eine Software-Plattform, die auf Servern, die die Telcos bereits haben, laufen kann, aber auch auf solchen, die jetzt und in Zukunft gekauft werden. Der Wechsel zu einer unterstützenden Infrastruktur für Virtuelle Netzwerk-Funktionen (VNFs, die „Anwendungen als ein Service“ (AaaS) der Telco-Welt) würde viel zu teuer, wenn man dafür komplett neue Hardware benötigen würde. Telcos müssen ihre bestehenden Geräte soweit sie noch nützlich sind, behalten können und neue nach den Anforderungen der dynamisch wachsenden anschaffen, um die Kunden auch mit neuen Diensten richtig bedienen zu können. Guru Parulkar, der Executive Director des Open Networking Lab sagt dazu: „Sieht man sich ein typisches Central Office über die Jahre an, kann es durchaus vorkommen, dass es da-

Seminar

TCP/IP-Netze erfolgreich betreiben 13.03. - 15.03.2017 in Aachen

IP ist die Grundlage jeglicher Rechnerkommunikation. Neben IPv4 gewinnt IPv6 zunehmend an Bedeutung. Für den erfolgreichen Betrieb von IP Netzen ist es unabdingbar beide Protokolle zu verstehen und zu beherrschen. Die Protokolle TCP und UDP bilden die Basis jeder Anwendungskommunikation. Der Kurs vermittelt praxisnah das notwendige Wissen und grundsätzliche Kenntnisse über Routingprotokolle DHCP und DNS.

Wer ein Netzwerk erfolgreich betreiben will, muss die notwendigen Voraussetzungen dafür schaffen. Dafür muss man die Grundlagen beherrschen und typische Anwendungen und Fehler kennen. In diesem Seminar werden die erforderlichen Kenntnisse für den Betrieb eines IP-Netzes praxisnah vermittelt.

Referent: Markus Schaub
Preis: € 1.890,- netto



Buchen Sie über unsere Web-Seite

www.comconsult-akademie.de

Das RZ-Netz der Zukunft - Teil 1: Die Data Center Networking Landschaft und zukunftsorientierte Lösungen

rin 300 unterschiedliche Typen proprietärer Geräte gibt. Das bedeutet, dass Central Offices signifikante CapEx und OpEx für Provider darstellen. Deren Mangel an Programmierbarkeit führt zu einem Mangel an Innovation und neuen Diensten. Und genau das möchten die Service Provider ändern.“

OpenStack hat in Rechenzentren bereits in Teilen etwas in der Art getan, was Provider möchten. CORD nutzt OpenStack mit Docker Containern und den Open Source SDN-Controller ONOS, dessen Entwicklung ebenfalls unter Leitung von Parulkar steht. Sinn der Plattform ist es letztlich, Server mit unterschiedlichen Spezifikationen gleichartiger aussehen zu lassen und somit die VNFs einigermaßen einheitlich implementieren zu können. AT&T (Nyse:T), Verizon (Nyse: VZ), China Unicom und Korea's SK Telecom gehören zu den Gründungsinteressenten, ein wichtiger Hersteller in diesem Zusammenhang ist Huawei. Nach Ayush Sharma, dem Vizepräsidenten von Huawei, kann man das Problem folgendermaßen charakterisieren: „Wenn man solche RZ-ähnlichen Netze mit den Methoden aus der Welt der RZs aufbauen möchte, stößt man schnell auf das Problem, dass es in konventionellen Netzen keine Orchestrierung gibt. Die benötigt man aber, wenn man solche funktionalen Elemente realisieren möchte.“

In den letzten Monaten hat Google erfolgreich versucht, seine Container-Entwicklungen in Richtung des Open Source Orchestrators Kubernetes zu bewegen. Der kommerzielle OpenStack Anbieter Mirantis arbeitet mit Google und Intel daran, die bisherige OpenStack Entwicklungs- und Management-Komponente Fuel durch Kubernetes zu ersetzen. Google ist der CORD-Entwicklung mittlerweile beigetreten.

Die Grundzüge der Spezifikation und viele interessante Einzelheiten sind unter opencord.org zu finden. Das Herz der Architektur ist eine Fabric mit Leaf/Spine-Elementen, die WhiteBox Server und Appliances nutzt, die die VNFs beherbergen, die ihrerseits mit OpenFlow verknüpft sind. Parulkar ist auch einer der Väter von OpenFlow. Im Gegensatz zum typischen RZ in Unternehmen nutzen die Central Offices „Access Racks“, sozusagen eine funktionale Stufe über den Server Racks. Ein Central Office kann rund 10.000 Festnetz Benutzer, die über irgendeine Festnetz-Technik kommen, dazu etwa 10.000 Mobil-Nutzer, die über einen Backhaul kommen und noch ein paar Dutzend Enterprise-Kunden, die über ein Metro-Netz kommen, bedienen. Das wäre der allgemeine Ansatz. In Deutschland baut die Deutsche Telekom ja erfolgreich ein „All-IP“-Netz auf, welches letztlich die

Schnittstelle zu den Diensten auf einer anderen Ebene vereinfacht. Dies nur als Hinweis. Interessant ist, dass CORD auch an einer kompakten „Light“-Version (M-CORD Light) arbeitet, bei der direkt ein ganzes kompaktes Rack mit aller Software für 10 bis 20.000 US\$ ausgeliefert werden kann, ein sehr günstiger Preis gemessen an den Gesamtkosten der zellularen Mobilfunktechnik. (<https://wiki.opencord.org/display/CORD/Mobile+CORD>)

Aktuell betreibt AT&T in den USA rund 4700 Central Offices und arbeitet bereits jetzt erfolgreich mit einer CORD-Version.

2.2 Das Enterprise Netz der nächsten Generation braucht hohe Anbindungsqualität

Man erwartet von der Enterprise-IT heute, dass sie deutlichen Mehrwert generiert, während Kunden, Partner und Mitarbeiter Zugriff zu Anwendungen und Services zu jeder beliebigen Zeit von jeder beliebigen Stelle und mit jedem beliebigen Endgerät (in Grenzen) haben möchten. Um diese Forderungen erfüllen zu können, reicht es nicht mehr, das Corporate Netzwerk auf die eigenen Mitarbeiter zu beschränken. Es muss mit der Welt der Service-Provider verbunden werden, die diese ganzen hoffentlich gewinnbringenden Anwendungen für Kunden in der ganzen Welt bereitstellen, während die Mitarbeiter rund um die Uhr reibungslosen Zugriff auf Partner und Kunden haben.

Equinix ist ein „Colocation-Gigant“ aus Redwood, Cal., und möchte, dass die nächste Generation von RZ-Verbindungen am Besten in seinen RZs stattfindet. Interconnection als Service anzubieten, ist an sich schon ein gutes Geschäft. Equinix (Nasdaq: EQIX) ist damit aber noch nicht zufrieden und sieht Colocation als Basis für die Bereitstellung von RZ-Fläche, Stromversorgung und Kühlung weltweit an. Eine neue Studie der Marktforschungsfirma „Execute Now“ (die von Equinix gesponsert wurde) kommt zu dem (wenig überraschenden) Ergebnis, dass sich Entscheidungsträger weltweit immer mehr der Tatsache bewusst werden, dass sie eine leistungsfähige Verbindung zu einem weltweiten Ökosystem benötigen und somit die Nachfrage nach Interconnection-Diensten steigt. Es gibt noch mehr Studien in dieser Richtung mit ähnlichen Ergebnissen. Letztlich erweist sich die Vermutung, dass Geschäftsmodelle nicht mehr isoliert betrachtet werden können, sondern als verknüpft und gegenseitig abhängig gesehen werden müssen, als immer härteres Faktum. Das ist ja an sich nichts Neues, die Finanzwelt hängt schon eine gefühlte Ewigkeit in dieser Weise zusammen.

Wo könnten nun Probleme liegen? Die meisten dieser neuen hoffentlich gewinnbringenden Anwendungen laufen in Rechenzentren entsprechender Cloud Provider wie Amazon Web Services AWS (Nasdaq: AMZN), Microsoft (Nyse: MSFT) Azure oder IBM (Nyse: IBM) SoftLayer. Die Botschaften von Amazon sind klar: sie möchten nicht nur neue, sondern auch ältere Anwendungen in ihrer Cloud bedienen. AWS hat hierbei durchaus Erfolg. General Electric (Nyse: GE) und Capital One z.B. konsolidieren beide ihre Rechenzentren und bewegen die meisten Daten und Anwendungen in die Cloud. Die neue Online-Banking Lösung von Capital One basiert vollständig auf AWS.

Unternehmen und Organisationen beklagen schlechte Leistung sowie mangelhafte Zuverlässigkeit und Sicherheit, wenn sie die Cloud-Dienstleistungen über das allgemeine Internet nutzen. Das ist der Punkt, an dem Equinix und andere Provider in dieser Richtung (z.B. Digital Realty (Nasdaq: DLR), AT&T, Level3 (Nasdaq: LVL3), NTT (Nyse ADS: DCM), Orange (Nyse ADS: ORAN) oder Verizon (Nasdaq: VZ)) auf den Plan treten. Sie liefern private Netzwerk-Konnektivität zu Public Clouds. Das ist letztlich eine übersichtliche Menge von Dienstleistungen, von denen Equinix sagt, dass sie das am stärksten wachsende Segment ist. Wenn die Footprints von Unternehmens-RZs sinken, weil mehr und mehr Leistungen durch die Cloud erbracht werden, könnte man sich fragen, ob das letztlich auch eine negative Auswirkung auf das Colocation Volumen hat. Das Gegenteil ist der Fall. Viele Unternehmen, die bislang keinen guten Zugriff auf Web-Services hatten, überlegen sich aktuell, diesen zu verbessern. Derartige Leistungen sind auch in Deutschland verfügbar. Kurz nachdem Amazon sein neues RZ in Frankfurt angekündigt hatte <http://www.datacenterknowledge.com/archives/2014/10/23/aws-launches-cloud-data-center-in-germany/> hat auch Equinix die Verfügbarkeit entsprechender Colocation-Services in seinem Frankfurter RZ in Aussicht gestellt.

Enterprise-Kunden werden die Architektur ihrer Anbindung nach einem ganzen Bündel von Kriterien auswählen, allen voran den Business-Zielen und der bislang existierenden Netzwerk-Architektur. Der eigentliche indirekt sichtbare Gewinn besteht aber darin, dass eine einzige gut gemachte Anbindung nicht nur einen Cloud Service erschließen kann, sondern direkt ein ganzes Bündel neuer Möglichkeiten, die in Zukunft sicher nicht weniger, sondern mehr werden.

Fortsetzung folgt...

Standpunkt

Sicherheitsrisiko Container?

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.

Container-Techniken der Bauart Docker und Co. haben sich erstaunlich schnell in unseren Rechenzentren etabliert. Dies ist aber eigentlich nicht überraschend, denn mit Containern wird eine wichtige Lücke zwischen der Bereitstellung von (virtuellen) Servern und Anwendungen auf einem Betriebssystem geschlossen. Nicht der komplette Rechner wird samt Betriebssystem sondern lediglich die Anwendung und die hierzu unbedingt notwendigen Teile der Betriebssystemschnittstellen werden in Form eines sogenannten Containers virtualisiert. Auf diese Weise ergibt sich eine höchst interessante schlanke Alternative bzw. Ergänzung zu virtuellen Maschinen, die mit deutlich weniger Overhead entscheidende Vorteile liefert, nämlich die schnelle und flexible Bereitstellung von Anwendungen. Entwicklung, Test und Produktivsetzung vereinfachen sich mit Container-Techniken erheblich. Mit der Container-Technik erhalten wir also eine weitere Virtualisierungsebene in unserer Infrastruktur, die wir aus dem Blickwinkel der Informationssicherheit bewerten müssen.

Ein unmittelbarer Sicherheitsgewinn beim Einsatz von Containern besteht auf den ersten Blick in der Isolation von Anwendungen durch unterschiedliche Container. Jedoch muss dem Nutzer hier bewusst sein, dass diese Isolation auf einem gewöhnlichen Betriebssystem abläuft und die Sicherheit bei Containern daher stark von den Berechtigungen für den Zugriff auf Systemressourcen abhängt. Im Vergleich zur Trennung von Anwendungsinstanzen durch eine Virtualisierung über einen Hypervisor ist die Stärke der Isolation bei Containern deutlich geringer und liefert entsprechend zunächst ein geringeres Sicherheitsniveau. Container-Lösungen und das zugrundeliegende Betriebssystem müssen also zielgerichtet zusätzlich gehärtet werden, um diese Schwäche auszugleichen und dies hat gewisse Grenzen, wenn man keine Einbußen im Komfort haben möchte. Eine Grundregel ist dabei natürlich den Basis-Images aus den öffentlichen Repositories zu misstrauen und Images nur von vertrauenswürdigen Quel-



len zu installieren. Die umzusetzenden Härtingsmaßnahmen beinhalten dann im Wesentlichen die Kontrolle und Einschränkung von Rechten, die die Container-Lösung selbst und die als Container gekapselten Anwendungen haben. Dabei ist durchaus ergänzend zu empfehlen, auch weitergehende Sicherheitsinstrumente in Betracht zu ziehen, wie z.B. AppArmor unter Linux. Außerdem darf der Nutzer nicht durch den vermeintlichen Schutz durch den Container leichtsinnig werden und die Absicherung der Anwendung selbst vernachlässigen. Zu Docker gibt es ein provokati-

ves Statement hierzu: „Docker is about running random code downloaded from the Internet and running it as root.“

Die Absicherung und sichere Nutzung einer Container-Lösung ist also durchaus mit Aufwand verbunden. Es ist daher nicht überraschend, dass auch hybride Ansätze verfolgt werden, welche versuchen den Komfort einer Container-Lösung mit der Stärke der Isolation eines Hypervisor zu verbinden. Ein Beispiel ist Microsoft Hyper-V Container. Die grundsätzliche Idee ist dabei einfach: Jeder Container wird durch eine speziell für die Container-Lösung gestaltete, schlanke VM gekapselt.

Auch wenn auf der einen Seite Container-Lösungen erhebliche Sicherheitsrisiken bergen, es gibt aber auch ein sehr interessantes Potential für die Informationssicherheit, wie man sehr schön im Bereich Server-less Computing und Amazon sieht: Bei AWS Lambda handelt es sich um eine Ausführungs-umgebung in der Cloud für Python-, Java- oder C#-Funktionen. AWS Lambda startet für eine Funktion eines Kunden einfach einen neuen Container und zerstört ihn nach Aufruf. Für einen Angreifer wird es nun schwer, denn ein kompromittierter Container „lebt“ nur wenige Millisekunden.

Seminar

Information Security Management mit ISO 27001 und BSI-Grundschutz 03. - 05.04.2017 in Bonn

Angemessene Sicherheit mit optimalem Aufwand: geht das? Die Antwort liegt in der Nutzung bewährter Standards und Lösungen bei gleichzeitiger Erfüllung von Compliance-Richtlinien. Anders formuliert: Das Rad muss nicht von jedem Unternehmen neu erfunden werden. Dieses Seminar stellt den Aufbau und die nachhaltige Umsetzung eines standardisierten und zertifizierbaren Information Security Management System (ISMS) auf Basis von ISO 27001 und BSI IT-Grundschutz vor. Es wird dabei aufgezeigt, wie eine praxisgerechte Sicherheitslösung mit optimalem Aufwand erreicht werden kann.

Dieses Seminar bereitet angehende Sicherheitsbeauftragte, Mitarbeiter im Bereich Informationssicherheit und interne Revisoren auf ihre Aufgaben vor.

Referenten: Dr. Simon Hoff, Dipl.-Math. Simon Oberem
Preis: € 1.890,- netto



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

Aktuelle Sonderveranstaltung

Implementierung von IPv6 – Erkenntnisse und Erfahrungen

22.05.2017 in Bonn

Die ComConsult Akademie veranstaltet am 22.05.2017 ihre Sonderveranstaltung "Implementierung von IPv6 – Erkenntnisse und Erfahrungen" in Bonn.

IPv6 Projekte sind angelaufen. IPv6 existiert nicht mehr nur in Forschungsumgebungen, bei den Providern und in Testnetzen von Unternehmen. Immer mehr Firmen haben mit der Migration begonnen, von DAX 30 bis Mittelständler, von Finanzinstituten bis zur Fertigung. Nicht nur der Internet-Auftritt, der Provider-Anschluss und die Homeoffice VPNs werden migriert. Auch in den Unternehmen selbst hat die Migration begonnen. Profitieren Sie in dieser Sonderveranstaltung von den Erfahrungen, die bei laufenden Projekten gesammelt wurden.

Inhalte

Adresskonzept

- Welche Alternativen stehen zur Verfügung
- Was sind die Vor- und Nachteile
- ULA, PI oder PA: wie sich unsere Kunden entscheiden

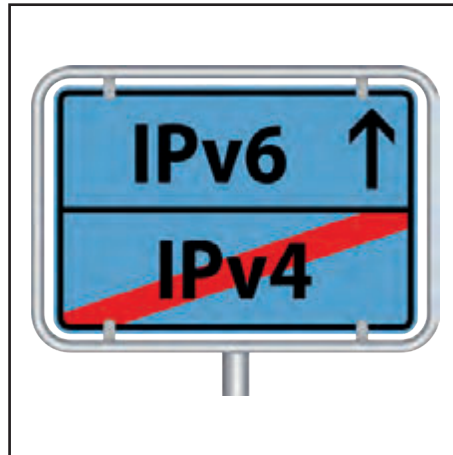
Zuweisung von IPv6 Adressen

- Welche Verfahren stehen zur Verfügung
- Wie integriert man Komponenten, die kein DHCPv6 unterstützen

LAN-Architektur

- Redundanzverfahren: VRRP, HSRP
- Routing von IPv6

Umgang mit QoS bei IPv6



- Wie weit sind die Hersteller
- Was funktioniert herstellerübergreifend und was nicht

Migration der Internetpräsenz

Migration von Anwendungen und Appliances

Externe Anbindungen

- WAN
- Internet-Provider
- Internet-VPN
- Partnerunternehmen

First-Hop-Security

Organisation eines IPv6 Rollouts

- Planung des Vorgehens, was muss wann entschieden werden
- Welche Abteilungen sind in welcher

Projektphase gefordert

- Wo existiert Schulungsbedarf

Einführung von IPv6 im Dual-Stack-Betrieb bei der ComConsult Beratung und Planung GmbH

- Logischer Netzaufbau
- IPv6-Kompatibilität von Hard- und Software
- Bekannte Probleme
- IPv6-Adressbeschaffung (LIR, sponsoring LIR?, Global Unicast oder Unique Local?)
- IPv6-Adresskonzept
- Zonenkonzept
- Übergangsmechanismen (Dual Stack, Tunnelmechanismen, NAT64)
- Testumgebung: Erkenntnisse, Hürden, Lösungen
- Dokumentation
- Einführung Dual-Stack-Betrieb

In diesem Seminar lernen Sie

- Welche Entscheidungen wann getroffen werden müssen
- Welche Komponenten im Netzwerk in welcher Reihenfolge migriert werden
- Wie man ein IPv6 Projekt planerisch und organisatorisch umsetzt
- Worauf – Stand heute – in Multivendor-Umgebungen zu achten ist
- Wie man die IPv6 Migration in den Lifecycle von Hard- und Software integriert
- Warum ein Migrationsprojekt nicht so teuer ist, wie viele annehmen
- Wo mit Schwierigkeiten zu rechnen ist und wo nicht

Anmeldung an kundenservice@comconsult-research.de

Sonderveranstaltung: Implementierung von IPv6 – Erkenntnisse und Erfahrungen

Ich buche die Sonderveranstaltung
Implementierung von IPv6 – Erkenntnisse und Erfahrungen
 22.05.2017 in Bonn

zum Preis von € 1.090,-- netto

Bitte buchen Sie mir ein Hotelzimmer

Vorname

Nachname

Firma

Telefon/Fax

Straße

PLZ, Ort

eMail

Unterschrift



Buchen Sie über unsere Web-Seite

www.comconsult-akademie.de

Cloud Computing

IEEE 802.11ah – Ein Treiber für das Internet-of-Things?

Fortsetzung von Seite 1



Dr. rer. nat. Johannes Dams hat in den vergangenen Jahren zahlreiche wissenschaftliche Artikel im Bereich der theoretischen Informatik mit Bezug zu Algorithmen für Funknetzwerke veröffentlicht. Seit 2015 ist er als Berater bei der ComConsult Beratung und Planung GmbH im Competence Center Netze tätig. Der Fokus liegt hier unter anderem auf der Konzeption und Planung in den Bereichen WLAN, IPv6 und weiteren Aspekten aktiver Netzwerktechnik.

Zuletzt wurden zahlreiche Aspekte des Internet-of-Things recht ausführlich hier im Insider von Petra Borowka-Gatzweiler in ihrer Reihe „Internet of Things – die vierte industrielle Revolution“ (ComConsult Insider vom Juli, August und Dezember 2016) diskutiert und besprochen. Einige grundlegenden Aspekte möchte ich im Folgenden anhand des angekündigten „IoT-WLAN“-Standards aus technischer Sicht beleuchten.

Auch wenn sich IoT scheinbar Schritt für Schritt immer weiterverbreitet, blieb der große Boom aber bisher aus. Das Thema als solches scheint immer noch am Rande mit anderen Entwicklungen mit zu laufen ohne sich selbstständig und selbstbewusst als eigenständiger Aspekt im Netzwerk durchzusetzen. Vielmehr schleichen sich die möglichen IoT-Anwendungen langsam in den Betriebsalltag von WLAN-Betreibern und Nutzern. Die Implementierung basiert dabei aber nur teilweise auf speziellen IoT-Technologien. Meist finden sich die Anwendungen im regulären 2,4- und 5-GHz-WLAN oder nutzen Bluetooth, Zigbee und ähnliches. Dies kann sich durch passende neue Standards und Technologien ändern.

Nun hat Anfang des vergangenen Jahres (Januar 2016) die Wi-Fi Alliance die „Wi-Fi HaLow“ Zertifizierung angekündigt. Auch wenn es von Seiten der Wi-Fi Alliance keine offizielle Erläuterung des Namens gibt, wird sich das „Low“ sicherlich auf Low-Power oder Lower Frequencies beziehen. Die Wortschöpfung „HaLow“ klingt im Englischen genau wie das Wort „halo“ (Heiligenschein oder Strahlenkranz) und bietet damit wohl den gewünschten Marketing-Effekt. Tatsächlich rückte die Wi-Fi Alliance mit dieser Ankündigung wieder einmal das Internet der Dinge (Internet of Thing – IoT) in den Fokus und wurde auf breiter Fläche in den entsprechenden Medien diskutiert.

Damit werden direkt einige Fragen aufgeworfen: Stellt „Wi-Fi HaLow“ bzw. IEEE 802.11ah, der der Zertifizierung zugrundeliegende Standard, also jetzt den Durchbruch für IoT-Anwendungen dar? Und was versteht man hierbei überhaupt als eine IoT-Anwendung?

Für die Definition des Internet-of-Things oder des Internet-of-Everything, wie es manchmal hochtrabend genannt wird, spielt vor allem die Anzahl und die Art der Endgeräte eine Rolle. Auch wenn es keine abschließende und einheitliche Definition für IoT gibt, basiert der Begriff doch immer auf dem klaren Anstieg der Anzahl ans Netzwerk (und unter Umständen auch ans Internet) angebundener Endgeräte und darauf, dass diese allgegenwärtig und beispielsweise mit Sensoren bestückt sind.

Die Entwicklung hin zum Internet-of-Things hat sicherlich schon vor einigen Jahren angefangen und von vielen un bemerkt in den letzten Jahren an Fahrt aufgenommen. Dabei umfasst diese Entwicklung verschiedenste Anwendungen und Geräte. Im Heimbereich sind dies beispielsweise Kühlschränke, die selbstständig Lebensmittelbestellungen über das Internet ermöglichen, oder auch Temperatur-Sensoren, die das Heizverhalten regeln, und viele weitere Teile der Heimautomation von Rolladen-Steuerungen bis zu Lampen und Lichtschaltern.

So haben sich verschiedenste Anwendungen in den letzten Jahren ins WLAN oder in Bluetooth- oder auch Zigbee-Netze gedrängt, die in den Bereich IoT fallen können. Auch im Industrie- und Produktionsumfeld finden sich immer mehr solche Anwendungen. Hier lassen sich Abrufknöpfe in der Logistik, Schrauber mit Drehmomentmessern und vieles weiteres aufzählen. Diese Anwendungen lassen sich häufig dadurch von anderen WLAN-Nut-

zern abgrenzen, dass sie vergleichsweise geringe Datenmengen senden und häufig besonders energieeffizient arbeiten.

Viele der so bereits genutzten IoT-Anwendungen sind durchaus im WLAN oder mit Bluetooth gut angebunden und es ist nicht unbedingt zu erwarten, dass hier plötzlich flächendeckend ein neuer Standard Einzug hält. Insbesondere mit bereits existierenden (und teilweise konkurrierenden) Funkstandards scheint die nötige Technologie bereits zu existieren. Aber genau an dieser Stelle setzt IEEE 802.11ah an. Kann sich ein solcher Standard unter diesen Vorzeichen überhaupt durchsetzen?

Der Standard bietet im Vergleich zum traditionellen 2,4- oder 5GHz-WLAN aufgrund des gewählten 900MHz-Frequenzbereich eine höhere Reichweite mit deutlich geringerem Stromverbrauch. Es lassen sich also vor allem neue Geräte, deren Bandbreitenbedarf nicht allzu hoch ist, auf einer großen Fläche anbinden. Aber reicht dieses Argument für eine Verbreitung und Nutzung aus?

Bevor wir die technischen Aspekte betrachten sei erwähnt, dass der IEEE 802.11ah-Standard zum aktuellen Zeitpunkt (Dezember 2016 / Januar 2017) noch nicht verabschiedet ist und damit alle Details vorläufig sind (eine offizielle Veröffentlichung wurde ursprünglich für 2016 erwartet). IEEE 802.11ah hat es also noch nicht in den aktuellen WLAN Standard IEEE 802.11-2016 geschafft (siehe hierzu auch den Artikel von Dr. Wetzlar im Januar Insider 2017). Trotzdem sollen im Folgenden einige Teile der technischen Spezifikation betrachtet werden und mögliche Chancen für den Standard im Industrieumfeld betrachtet und diskutiert werden. Es sei aber schon angemerkt, dass das tatsächliche Ausmaß und die Relevanz von Wi-Fi HaLow heute noch nicht

IEEE 802.11ah – Ein Treiber für das Internet-of-Things?

abzuschätzen sind solange es keine passenden Endgeräte und Access Points auf dem Markt gibt.

Technische Details zu IEEE 802.11ah

Grundsätzlich ist ein Hauptbestandteil und auch ein Hauptgrund für die Nutzung von IEEE 802.11ah als Funkstandard die Implementierung im Spektrum bei ungefähr 900 MHz. Die Dämpfung ist in diesem Bereich deutlich geringer und Funkwellen erreichen auch bei geringerer Sendeleistung deutlich größere Reichweiten als im 2,4GHz- oder im 5GHz-Band. Außerdem ist das entsprechende Spektrum häufig nicht so stark belegt, was zu weniger Interferenz führt und somit eine effizientere Nutzung ermöglicht.

Dies nutzt in vergleichbarer Art und Weise auch 802.11af aus, der ebenfalls im Sub-GHz-Bereich (bis ca. 700 MHz) arbeitet. Dieser zielt im Gegensatz zu IEEE 802.11ah aber nicht auf das Internet-of-Things und die entsprechend hohe Endgeräteanzahl ab. Stattdessen wird der Hauptnutzen hier darin gesehen, dass freie Bereiche im Fernsehspektrum genutzt werden können (sogenannte TV-Whitespaces).

Insgesamt sind viele der Technologien des IEEE 802.11ah-Standards aus IEEE 802.11ac entliehen. Man hat also das Rad nicht neu erfunden, aber zusätzlich dabei auf geringen Energiebedarf und eine besonders hohe Anzahl an Endgeräten pro Access Point geachtet. Um die Wi-Fi Alliance zu zitieren: „Wi-Fi HaLow operates in frequency bands below one gigahertz, offering longer range, lower power connectivity to Wi-Fi CERTIFIED™ products“ (Wi-Fi Alliance, 2016).

Das fasst die technischen Features eines „Wi-Fi HaLow“-Netzes schon recht gut zusammen: Es werden Reichweiten bis zu 1 km versprochen mit mehr als 8191 Endgeräten in einer hierarchischen Struktur und einem Power-Saving-Modus, bei dem Endgeräte ihre Funkkomponente für einige Zeit ausschalten können. An dieser Stelle sollte man die Argumente für HaLow, die im vorangegangenen Satz erwähnt sind, nicht zu schnell übergehen: Das ist einerseits die hohe unterstützte Anzahl von Endgeräten und andererseits der geringe Energiebedarf. Über 8.000 Endgeräte in einer Zelle sind schon eine Hausnummer. Bei derart großen Zellen und einem Anwendungsszenario im IoT ist das (und auch der Power-Saving-Modus) aber vielleicht schon fast ein Muss. Andere WLAN-Standards unterstützen hier deutlich weniger Endgeräte (z.B. 2007 verschiedene Association Identifier).

Außerdem wurden viele weitere Details optimiert und angepasst. So wurde das immer wieder (auch hier im Insider oder beim Netzwerkforum) heiß diskutierte DCF-System (Distributed Coordination Function) des WLAN-Standards IEEE 802.11 angepasst, um mit der erhöhten Anzahl an Endgeräten mithalten zu können. Da dennoch die Grundprinzipien beibehalten wurden, bleibt aber (leider) weiterhin Raum für Diskussionen.

Ein deutlicher Nachteil des verwendeten 900MHz-Frequenzbereichs ist, dass sich die internationale Regulierung noch stärker unterscheidet, als das bereits im 2,4- oder 5GHz-Band der Fall ist. Eine einheitliche globale Kanalplanung in Konzernen zu etablieren wird also praktisch unmöglich.

Mit den unterschiedlichen Vorgaben für maximale Sendestärke und freie Frequenzen im Sub-GHz-Band ergeben sich somit auch unterschiedliche Reichweiten und Datenraten. Besonders die erlaubten Sendestärken liegen mit Werten zwischen 10 mW und 1 W weit auseinander und sorgen damit dafür, dass auch der Nutzen der HaLow-Technologie variiert. Es bleibt also zu hinterfragen, ob global die oben versprochenen Reichweiten überhaupt realistisch erreichbar sind.

Selbst bei der idealisierten Freiraumausbreitung auf Abbildung 1 (deren Vorlage ich einem der Insider-Artikel von Herrn Dr. Wetzlar entliehen habe) ist zu sehen, dass die Sendestärke einen deutlichen Einfluss auf die Reichweite hat. Für Europa mit der maximalen Sendestärke von 25 mW EIRP bedeutet dies, dass bei gleicher

Empfangsstärke immerhin noch doppelt so weite Übertragungen, wie im 2,4GHz-WLAN (50 mW EIRP) erreicht werden.

Tatsächlich vernachlässigt diese Darstellung nicht nur die über die Freiraumausbreitung hinausgehenden Verluste, sondern auch die Tatsache, dass Funkempfänger eine unterschiedliche Sensibilität aufweisen. Die Grafik zielt lediglich auf die im Standard definierten Werte ab, die Empfänger mindestens erfüllen müssen. Für den WLAN-Praktiker ist also ganz klar ersichtlich, dass die hier erreichten Entfernungen rein theoretische Werte sind. Dennoch lässt sich so bereits ein Gefühl für die mögliche Zellgröße vermitteln.

Es sei hier natürlich außerdem angemerkt, dass der IEEE 802.11ah-Standard bessere Grenzwerte für die minimale Empfangsempfindlichkeit definiert als noch bei den älteren WLAN-Standards. Bei diesen wurde der Standard schon längst von der Realität überholt und die meisten Funkadapter übererfüllen die entsprechenden Vorgaben.

Diese idealisierte Darstellung reicht natürlich bei weitem nicht, um in realistischen Büro- oder Produktionsumgebungen eine Abschätzung abzugeben. Schließlich unterscheidet sich auch die Dämpfung durch Wände und Gegenstände abhängig von der Frequenz, wie in Abbildung 2 dargestellt.

In dieser Auflistung sind anstelle der 5GHz-Dämpfungswerte, Werte für 6,5 GHz zu finden. Dennoch geben diese ei-

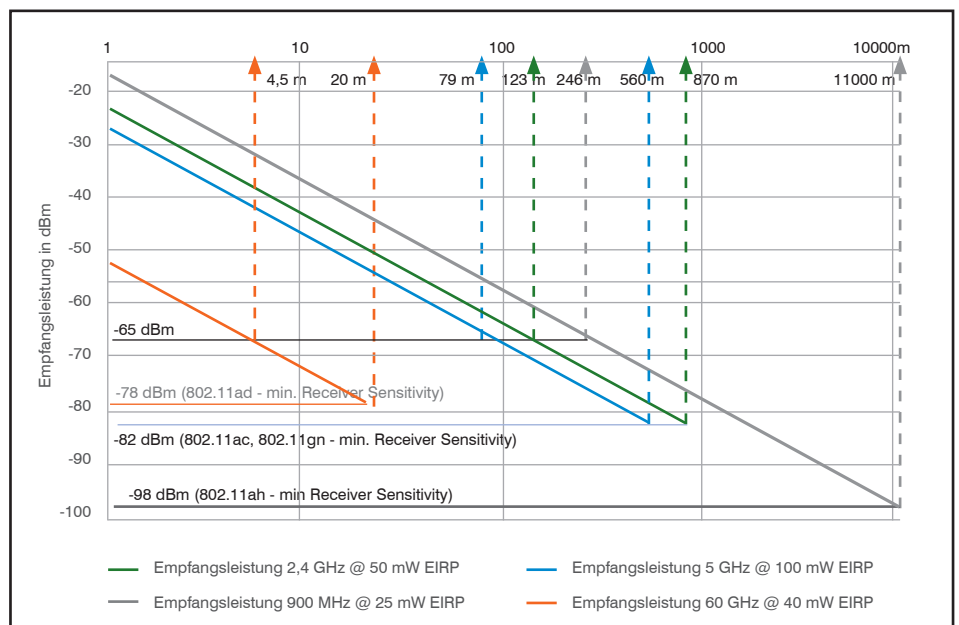


Abbildung 1: Freiraumausbreitung für verschiedene WLAN-Standards

IEEE 802.11ah – Ein Treiber für das Internet-of-Things?

nen Eindruck, wie sich die Dämpfung verhält und lassen ebenfalls Rückschlüsse darauf zu, dass die 5-GHz-Dämpfung durchaus vergleichbar ist. Ganz klar ersichtlich ist, dass die Dämpfung im 900-MHz-Bereich materialabhängig deutlich niedriger als im 2,4-GHz-Bereich ist.

Eine Reduktion der Dämpfung von 18 dB auf 3 dB beispielweise bewirkt, dass das Funksignal einen Faktor $2^5 = 32$ weniger Verlust erleidet. Das Signal dringt also deutlich besser durch Materialien und erlaubt somit auch größere Funkzellen. Dieser Effekt gleicht auch die geringere erlaubte Sendestärke EIRP (in Europa) aus.

Auch wenn die Reichweite und die unterstützte Anzahl der Endgeräte eines der Hauptargumente für ein IoT-WLAN sein werden, müssen auch weitere Bestandteile des Standards betrachtet werden. Dies betrifft insbesondere die zur Verfügung stehenden Datenraten und Kanäle.

Dem Standard zu Grunde liegen Kanalbreiten von 1, 2, 4, 8 oder 16 MHz. De facto sind in Europa aber nur 1 und 2 MHz breite Kanäle umsetzbar und praktisch wird man meist bei nur 1 MHz bleiben. Andernfalls wären lediglich zwei Kanäle nutzbar. Es bleibt also zu hoffen, dass weitere Kanäle für die Nutzung freigegeben werden (siehe z.B. ETSI-Vorschlag TR 103 245).

Wie in Abbildung 3 ersichtlich, unterscheiden sich die Frequenzen und deren mögliche Nutzung im 900-MHz-Band international recht deutlich. Dies wird mittelfristig sicherlich die Einführung von IEEE 802.11ah insbesondere in großen globalen Unternehmen behindern. Ein einheit-

Material	900 MHz	2,4 GHz	6,5 GHz
Beton	9 dB	18 dB	> 30 dB
Kalkstein	3 dB	9 dB	> 30 dB
Hochlochziegel	3 dB	18 dB	27 dB
Kiefernholz	3 dB	18 dB	> 30 dB
Angenommene Wandstärke: 24 cm			

Abbildung 2: Beispiel-Dämpfungswerte

Quelle: http://kaiserslautern.net/themen_und_projekte/elektrosmog/absicherung

licher Frequenzplan ist hier nicht mehr möglich.

Gemäß Standard ergeben sich damit (für Europa) unter Idealbedingungen Brutto-Datenraten von bis zu 8,67 Mbit/s pro Spatial Stream (Short Guard Interval und MCS 8). Bei bis zu 4 Spatial Streams wären es also immerhin ca. 35 Mbit/s. Bei den erhofften großen Reichweiten wird man hier aber deutliche Abstriche machen müssen. Die kleinste spezifizierte Datenrate beträgt 150 kBit/s und sollte für Anwendungen im HaLow-WLAN beachtet werden (siehe Seok).

Auswirkung von IEEE 802.11ah

Angesichts der oben stehenden Beschreibung des Standards und der Einschränkungen für Europa kann man auf die Idee kommen, dass Wi-Fi HaLow kaum relevant werden wird. Besonders dort, wo in Produktionshallen bereits flächendeckendes WLAN vorhanden ist, kann der Nutzen einer zusätzlichen Technik auf den ersten Blick recht nüchtern bewertet werden: Wer braucht schon ein weiteres WLAN mit weiterem Aufwand?

Dennoch bietet der neue Standard einige wichtige Punkte, die auch bei einer eingeschränkten (europäischen) Reichweite den Ausschlag für eine IEEE 802.11ah-Implementierung geben können. Hierbei sind die Nutzer und Planer vor allem auf die endgültige und schlüssige Umsetzung der Hersteller angewiesen. Die Frage ist in Zukunft also: Werden die Hersteller alle benötigten Datenraten, Reichweiten und auch eine Integration in bisherige typische WLAN-Geräte umsetzen und unterstützen? Inwieweit IEEE 802.11ah also ein Nischenprodukt wird oder ob namhafte Hersteller den Standard in Zukunft voranbringen wird sich noch zeigen.

Prinzipiell zielt HaLow (insbesondere in Europa) auf Endgeräte mit geringem Bandbreitenbedarf ab, die in entsprechend großer Anzahl auf durchaus großen Flächen eingesetzt werden. In diesem Bereich kann somit ein WLAN geboten und unter Umständen Abdeckungslücken des herkömmlichen WLANs geschlossen werden.

Durch die Nutzung eines weiteren Frequenzbands können solche Endgeräte aus dem herkömmlichen WLAN verbannt

Vergleich der Funkpartner (IEEE 802.11ah)					
	Europa	USA	China	Korea	Japan
Frequenzband	863 - 868,6 MHz	902 - 928 MHz	755 - 787 MHz	917 - 923,5 MHz	915,9 - 928,1 MHz
Kanäle					
1 MHz	5	26	32	6	11
2 MHz	2	13	4	3	-
4 MHz	-	6	2	1	-
8 MHz	-	3	1	-	-
16 MHz	-	1	-	-	-
Max. Sendeleistung (EIRP)	25 mW	1W	5 mW oder 10 mW	3 mW oder 10 mW	1 mW, 20 mW oder 250 mW + 3 dBi Antennengewinn

Abbildung 3: Vergleich des vorläufigen IEEE 802.11ah Standards

Quelle: http://www.comsocscs.org/docs/IEEE%20ComSoc_11ah_Opportunity_v6_0715.pdf
http://www.comsocscs.org/docs/802-11ah-overview-comm_soc_r1.pdf
http://www.arib.or.jp/english/html/overview/doc/5-STD-T108v1_0-E2.pdf

IEEE 802.11ah – Ein Treiber für das Internet-of-Things?

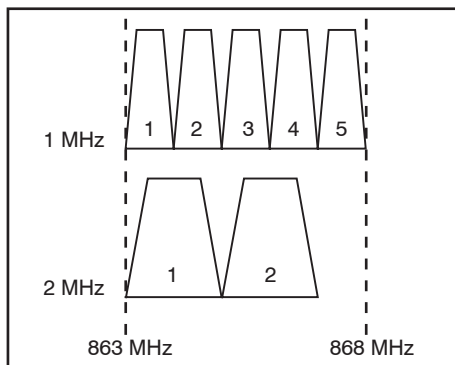


Abbildung 4: IEEE 802.11ah Kanäle in Europa (Aust, 2014)

werden und somit Übertragungsbandbreite für andere Endgeräte mit höherem Bedarf freigemacht werden. Dies schließt sich ganz klar dem von Dr. Wetzlar bei der Wireless Sonderveranstaltung im vergangenen Dezember und beim letzten Netzwerkforum vertretenen Vorschlag an: Das WLAN sollte nur mit Geräten belastet werden, die dieses wirklich benötigen. Folglich können nicht nur Gastgeräte ins Mobilfunknetz ausweichen, sondern Geräte, die mit geringer Bandbreite auskommen, ins HaLow-WLAN platziert werden. HaLow bietet sich aus meiner Sicht also besonders für solche Geräte mit geringem Übertragungsraten an.

Bei den typischen Produktionsumgebungen denkt man hier recht schnell an Abruf-Knöpfe für Logistikanwendungen. Aber auch weitere Geräte, wie verschiedenste Sensoren und Geräte der Überwachungsinfrastruktur können unter Umständen niedrige Anforderungen haben und sich somit für IEEE 802.11ah eignen.

Ein weiterer nicht zu unterschätzender Aspekt ist im Endeffekt die Sparsamkeit von IEEE 802.11ah. Endgeräte, die bereits auf energiesparenden Batteriebetrieb ausgelegt sind, erhalten hiermit Zugang zu einem (relativ) leistungsfähigen Kommunikationsmedium. Abbildung 5 zeigt das Ergebnis einer Studie, bei der die Batterieleistung eines IEEE 802.11ah WLANs für verschiedene Anwendungen simuliert wurde. Hier ist deutlich sichtbar, dass somit auf Low-Cost-Low-Energie-Geräte gesetzt werden kann und damit auch entsprechende mobile langfristig nutzbare Anwendungen möglich werden. Selbst wenn einige Annahmen dieser Studie möglicherweise von der genauen Implementierung abhängen, lässt sich das Potential von IEEE 802.11ah im Bereich des Batteriebetriebs hier nur schwer leugnen.

So wie auch immer mehr Anwendungen ins WLAN drängen, die in der Vergangenheit keine Rolle spielten, wird es vielleicht

auch einem IoT-WLAN gehen. Neue Anwendungen im Freien oder in Hallen mit entsprechender Deckenhöhe und dem entsprechenden Freiraum können sich ergeben. Hier lässt sich eine Implementierung von IEEE 802.11ah mit deutlich weniger Access Points als für herkömmliches WLAN erreichen. Im Endeffekt kann das IEEE 802.11ah-WLAN zur zusätzlichen Abdeckung und für zusätzliches Spektrum neuer Anwendungen dienen.

Alle diese Szenarien und Aspekte setzen aber grundsätzlich voraus, dass Endgeräte und Access Points diesen neuen Standard unterstützen. Es lässt sich also nur abwarten, wie sich der Markt entwickelt und ob die großen WLAN-Hersteller entsprechende Produkte anbieten werden. Analysten prophezeien hier bereits, dass die einzige Chance für Wi-Fi HaLow darin liegt, dass Tri-Band-Geräte (für WLAN im Sub-GHz- und im 2,4-GHz- und 5-GHz-Band) auf den Markt kommen (Nichols, 2015).

Relevanz für den WLAN-Betrieb

Falls der Standard sich aber tatsächlich durchsetzt, stellt sich vor der Einführung von IEEE 802.11ah also die Frage, ob die IT und der WLAN-Betrieb an dieser Stelle ein Umdenken braucht. Können hier klare Vorteile durch Wi-Fi HaLow identifiziert und implementiert werden? Endgültig lässt sich dies natürlich erst beantworten, wenn passende Produkte angeboten werden. Dennoch soll im Folgenden ein erster kurzer Abriss gegebene werden.

Auch wenn bereits erste Produzenten erfolgreich Chipsätze testen und Ergebnisse loben (z.B. Newracom oder PCS), sind noch keine endgültigen Produkte der bekannten WLAN- und Komponenten-Hersteller angekündigt. Trotzdem kann man die Fragen, ob ein Umdenken nötig ist und ob sich klare Vorteile ergeben, aus meiner Sicht mit hoher Wahrscheinlichkeit beide bejahen.

Für bestimmte Anwendungen und besonders in bestimmten Umgebungen

ist schon jetzt ein potentieller Nutzen erkennbar, indem das bisherige WLAN entlastet und eine breitere Abdeckung erreicht wird. Da ein stabileres 2,4GHz- oder 5GHz-WLAN auch anderen Anwendungen zu Gute kommt, kann und sollten die Auswirkungen einer Verlagerung von Spezialanwendungen in andere Frequenzbänder nicht vernachlässigt werden.

Ein Umdenken ist hierbei auf mehreren Ebenen von Nöten. Einerseits betrifft dies den Einsatz von Anwendungen in Frequenzbändern mit sehr unterschiedlichen Übertragungscharakteristiken. Es ist durchaus zu erwarten, dass ein und dasselbe Endgerät (situationsabhängig) verschiedene Verfahren und WLAN-Technologien nutzt. Andererseits sind nicht nur die Anwendungen und Endgeräte zu beachten, sondern auch die Planung eines solchen WLANs.

Bei der Planung eines WLANs spielen in einem noch größeren Maße, als bisher bei der Abwägung und Planung von 2,4GHz/5GHz-Mischumgebungen, die Fähigkeiten und die Anforderungen der Endgeräte eine Rolle. Datenratenanforderungen, Energiebedarf, Mobilität und die Größe der abzudeckenden Fläche sind hier Kriterien für den Einsatz von IEEE 802.11ah. In diesen Punkten bietet HaLow Vor- und Nachteile, die in eine Planung einfließen müssen. Auch der Einfluss der Umgebung (z.B. durch Produktionsmaschinen, Wände etc.) auf die Planung im Rahmen von Simulationen oder Ausleuchtungsmessungen ist anders und zeigt deutliche Unterschiede zur bisherigen WLAN-Planung. Die WLAN-Planung als solches wird also keinesfalls einfacher.

Wenn bei einem Mischbetrieb von 2,4 GHz und 5 GHz die Zellplanung noch gut durch eine passende Wahl der Sendestärken oder durch Abschalten eines Frequenzbands auf bestimmten Access Points vereinheitlicht werden konnte, ist dies mit 900MHz deutlich schwieriger möglich. Auch bei der deutlich gerin-

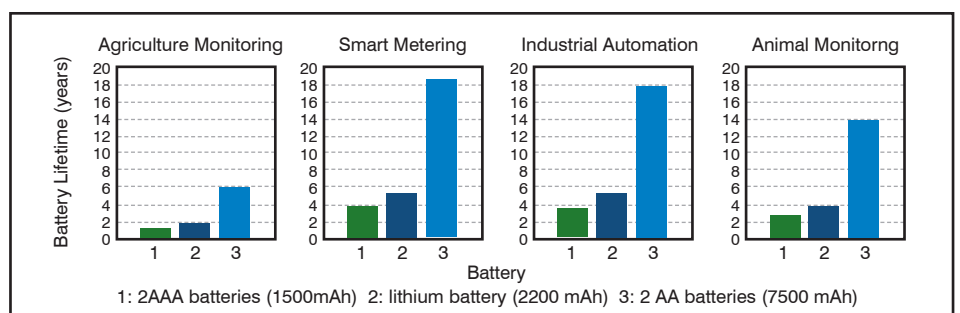


Abbildung 5: Simulierte Lebensdauer von batteriebetriebenen Endgeräten mit 802.11ah
Quelle: <https://arxiv.org/pdf/1402.4675.pdf>, <http://arxiv.org/pdf/1512.03576v1.pdf>

IEEE 802.11ah – Ein Treiber für das Internet-of-Things?

geren Dämpfung stellen insbesondere Produktionsumgebungen mit Maschinen neue Herausforderungen dar. Abdeckungslücken können durch eine (wegen der größeren Zellen) reduzierte Access-Point-Anzahl schwieriger ausgeglichen werden und fallen somit stärker ins Gewicht. Starke Veränderungen im Umfeld, z.B. bei Umbauten, können hier deutlich mehr negative Ergebnisse hervorbringen.

Fazit

Insgesamt lässt sich also festhalten, dass Wi-Fi HaLow alias IEEE 802.11ah im Laufe der nächsten Jahre bestimmt immer mal wieder ein Thema (auch hier im Netzwerk Insider) sein wird. Sobald die Standardisierung abgeschlossen ist und erste Produkte auf den Markt kommen, die auch für Industrieumgebungen und -Anwendungen geeignet sind, müssen insbesondere individuelle Analysen ange stellt werden, um das Potential und die Möglichkeiten abzugrenzen und herauszuarbeiten.

Für eine endgültige Beurteilung scheint es zum aktuellen Zeitpunkt noch zu früh zu sein. Die Chancen, die diese Technologie bietet, lassen sich im Moment noch nicht pauschal abschätzen. Gerade in der Anfangsphase wird man hier Anwendungsfälle sehr individuell bewerten müssen, da in den meisten Fällen ja bereits konkurrierende WLANs flächendeckend verfügbar sind.

Der Nutzen einer solchen Technologie hängt also von vielen Details ab, die durch die bisherige WLAN-Implementierung und die physikalische Umgebung sowie die genutzten Anwendungen bestimmt sind. Dennoch ist klar, dass IEEE 802.11ah das Potential bietet auch (oder gerade) im Industrieumfeld Anwendungsfelder zu finden. Hierzu wird bei der Planung und Implementierung durch das 900MHz-Band und durch neue Anwendungen ein Umdenken nötig werden.

Insgesamt lässt sich also feststellen, dass man als WLAN-Planer und -Betreiber im industriellen Umfeld mittelfristig nicht umher kommt, weitere Funktechnologien zu betrachten und für ein funktionierendes WLAN zu nutzen. Der Nutzen von IEEE 802.11ah alias Wi-Fi HaLow ist aber davon bestimmt, ob und wann entsprechende Chipsätze verfügbar werden. Ob hier Chancen genutzt werden können hängt vor allem von strategischen Entscheidungen der Hersteller ab. **Das heißt für WLAN-Betreiber: Noch abwarten, Tee trinken und die Augen offenhalten.**

Weiterführende Literatur

Aust, S. (2014). Advanced Wireless Local Area. Von <http://www.es.ewi.tudelft.nl/phd-theses/2014-Aust.pdf> abgerufen

Maier, F. (21.. Juli 2015). Die Kommunikation der Dinge. (Heise.de) Von <https://www.heise.de/ct/artikel/Die-Kommunikation-der-Dinge-2627817.html> abgerufen

Newracom. (3.. Juni 2016). Pressemitteilung. Von <https://www.design-reuse.com/news/39952/newracom-wi-fi-halow-ieee-802-11ah.html> abgerufen

Nichols, S. (21.. Oktober 2015). IoT's sub-GHz 802.11ah Wi-Fi will be dead on arrival, warn analysts. (The Register) Von http://www.theregister.co.uk/2015/10/21/questionable_future_subghz_wifi abgerufen

Palma Ceia Semidesign. (28.. Juni 2016). Pressemitteilung. Von <http://www.pcsemi.com/pr20160628-80211ah-haylo> abgerufen

Sartain, J. (23.. Mai 2016). Hello HaLow: Your guide to the Wi-Fi Alliance's new IoT spec. (NetworkWorld) Von <http://www.networkworld.com/article/3072961/internet-of-things/hello-halow-your-guide-to-the-wi-fi-alliance-s-new-iot-spec.html> abgerufen

Seok, Y. (kein Datum). IEEE Standardsuniversity - IEEE 802.11ah. Von <http://www.standardsuniversity.org/e-magazine/august-2016-volume-6/ieee-802-11ah-wi-fi-900-mhz-license-exempt-band-iot-application/> abgerufen

Stefan Aust, R. V. (2012). IEEE 802.11ah: Advantages in standards and further challenges for sub 1 GHz Wi-Fi. IEEE International Conference on Communications (ICC), Ottawa, 6885 - 6889.

Wi-Fi Alliance. (4.. Januar 2016). Pressemitteilung. Von <https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-low-power-long-range-wi-fi-halow> abgerufen

Kongress**ComConsult Netzwerk Forum 2017
27.03. - 30.03.2017 in Köln**

Das ComConsult Netzwerk-Forum 2017 stellt die vier momentan dominantesten Netzwerk-Themen in den Mittelpunkt der Veranstaltung: Anwendungs-Architekturen und Kommunikation im Rechenzentrum, Netzwerk-Design und Optimierung des Betriebs, WLAN-Design und die Herausforderungen neuer Standards, Netzwerk-Sicherheit in einem Cloud-Umfeld.

Am ersten Tag analysieren wir die Auswirkungen aktueller Anwendungs-Architekturen auf die schnelle Bereitstellung, die Gestaltung und die Leistung von Netzwerken. Anwendungs-Architekturen werden immer dynamischer und in Kombination mit der Forderung nach einer sehr schnellen Bereitstellung von Kapazitäten ergibt sich eine komplexe Orchestrierungs-Aufgabe. Die Dynamik ergibt sich dabei nicht nur beim Start einer Mikroservice-Architektur, sondern auch bei Lastveränderungen im laufenden Betrieb.

Am zweiten Tag stellen wir uns den aktuellen Veränderungen im Netzwerkdesign in Kombination mit der Frage, wie wir in einer immer komplexeren Situation zu einem optimalen Betrieb kommen können.

Am dritten Tag diskutieren wir die neuesten WLAN-Standards und zum Abschluss des Tages die Frage, wie eine umfassende Sicherheits-Lösung unter Berücksichtigung der Cloud aussehen kann.

Der vierte Tag des ComConsult Netzwerk Forums widmet sich traditionell einem Schwerpunktthema, welches wir gemeinsam mit Ihnen intensiv beleuchten möchten. In diesem Jahr steht das Thema „Netzwerksicherheit: Bedrohungen, Herausforderungen, Trends und Best Practice“ im Fokus.

Preise: € 2.790,- netto - 4-tägige Veranstaltung mit Thementag
€ 2.390,- netto - 3-tägige Veranstaltung ohne Thementag



Buchen Sie über unsere Web-Seite

www.comconsult-akademie.de

ComConsult Veranstaltungskalender

Lokale Netze für Einsteiger, 13.02. bis 17.02.2017 in Aachen**Garantietermin**

Dieses Seminar vermittelt kompakt und intensiv innerhalb von 5 Tagen die Grundprinzipien des Aufbaus und der Arbeitsweise Lokaler Netzwerke. Der Intensiv-Kurs vermittelt die notwendigen theoretischen Hintergrundkenntnisse, vermittelt den praktischen Aufbau, den Betrieb eines LANs und vertieft die Kenntnisse durch umfangreiche, gruppenbasierende Übungsbeispiele. Ausgehend von einer Darstellung von Themen der Verkabelung und Übertragungsprotokolle wird die Arbeitsweise von Switch-Systemen, drahtloser Technik, den darauf aufsetzenden Verfahren und der Anbindung von PCs und Servern systematisch erklärt.

Preis: € 2.490,-- *

IP-Wissen für TK-Mitarbeiter, 20.02. bis 21.02.2017 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 Grundlagen schnell verstehen. Es werden die wichtigsten VoIP-spezifischen Aspekte vorgestellt und unter praxisrelevanten Gesichtspunkten beleuchtet. Die Themen erstrecken sich von IP und LAN-Grundlagen hin zu praxisrelevanten Themen wie QoS, Jitter und Bandbreiten-Fragen. Ziel ist es dem IP-Unkundigen die wichtigsten Grundlagen der Netzwerktechnik kompakt und praxisnah zu vermitteln.

Preis: € 1.590,-- *

RZ-Kopplung: Georedundanz für Rechenzentren, 13.03.2017 in Berlin**Rabattaktion %**

Die gestiegene Bedeutung von zentralen IT-Systemen für Unternehmen und gesetzliche Vorgaben erfordern geo-redundante Standorte von Rechenzentren. Für die Bereitstellung und den Betrieb der Rechenzentrums-Kopplung wird besonderes Know-how und strategische Planung benötigt. In diesem Seminar werden die aktuellsten Technologien und Anforderungen vorgestellt und ein optimales Gesamtkonzept beschrieben.

Preis: € 1.090,-- *

Aufbau und Management von Internet-DMZ und internen Sicherheitszonen, 13.03. bis 15.03.2017 in Berlin

Die IT-Sicherheit für die Internet DMZ und internen Sicherheitszonen werden in diesem Seminar von Experten aus der Praxis vorgestellt und anschaulich erklärt. Verschiedene IT-Architekturen und Konzepte werden analysiert und auf ihre Praxistauglichkeit untersucht. Die Umsetzung anhand konkrete Projektbeispiele runden die Schulung ab.

Preis: € 1.890,-- *

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen, 13.03. bis 15.03.2017 in Köln**Garantietermin**

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,-- *

Netzzugangskontrolle: Technik, Planung und Betrieb, 13.03. bis 15.03.2017 in Berlin

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

Preis: € 1.890,-- *

TCP/IP-Netze erfolgreich betreiben, 13.03. bis 15.03.2017 in Aachen**Rabattaktion %**

IP ist die Grundlage jeden Netzes. Die Protokolle TCP und UDP bilden die Basis jeder Anwendungskommunikation. Es werden zudem Kenntnisse über Routingprotokolle, DHCP, DNS benötigt. Dieses Seminar vermittelt praxisnah das notwendige Wissen.

Preis: € 1.890,-- *

Vertragsgestaltung und rechtssichere Organisation von Cloud Services für Nichtjuristen, 03.04. bis 04.04.2017 in Bonn**Rabattaktion %**

Dieses Seminar erklärt, wie Sie die Auslagerung Ihrer Private Cloud vertraglich absichern und warum Sie das unbedingt machen sollten.

Preis: € 1.590,-- *

Virtualisierungstechnologien in der Analyse, 03.04. bis 04.04.2017 in Bonn

Im Zuge stetig zunehmender Konsolidierung ist Virtualisierung längst zum Standard in jedem Rechenzentrum geworden. Doch der Blick hinter die Kulissen offenbart einen rapide wachsenden Komplexitätsgrad, dessen Beherrschung ein tieferes Verständnis dieser Technologie erfordert. In diesem Seminar werden die Zusammenhänge zwischen Server, Netzwerk und Storage im Umfeld der Virtualisierung analysiert.

Preis: € 1.590,-- *

Kommunikation über Private WAN und Internet, 03.04. - 04.04.2017 in Bonn

Dieses Seminar vermittelt die Erfahrungen aus den jüngsten Projekten mit dem Fokus Konzeption und Ausschreibung von WANs. Teilnehmer dieses Seminars profitieren von langjährigen Erfahrungen der Vortragenden im WAN-Bereich, kombiniert mit dem großen Erfahrungsschatz von ComConsult bei der Lösung von Problemen und der Lokalisierung von Fehlern in standortübergreifenden Netzen. Ferner werden Erfahrungen bei der Gestaltung sinnvoller Service Level Agreements (SLA) im WAN-Betrieb in diesem Seminar vermittelt.

Preis: € 1.590,-- *

Zertifizierungen

ComConsult Certified Network Engineer

Lokale Netze für Einsteiger

13.02. - 17.02.17 in Aachen
08.05. - 12.05.17 in Aachen
18.09. - 22.09.17 in Aachen

TCP/IP-Netze erfolgreich betreiben

13.03. - 15.03.17 in Aachen
29.05. - 31.05.17 in Aachen
09.10. - 11.10.17 in Bremen

Internetworking

03.04. - 07.04.17 in Aachen
19.06. - 23.06.17 in Göttingen
13.11. - 17.11.17 in Aachen

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

ComConsult Certified Trouble Shooter

Trouble Shooting in vernetzten Infrastrukturen

02.05. - 05.05.17 in Aachen
26.09. - 29.09.17 in Aachen

Trouble Shooting für Netzwerk-Anwendungen

27.06. - 30.06.17 in Aachen
07.11. - 10.11.17 in Aachen

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

ComConsult Certified Voice Engineer

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen

13.03. - 15.03.17 in Köln
15.05. - 17.05.17 in Düsseldorf
16.10. - 18.10.17 in Frankfurt

Session Initiation Protocol Basis-Technologie der IP-Telefonie

05.04. - 07.04.17 in Bonn
29.05. - 31.05.17 in Frankfurt
08.11. - 10.11.17 in Stuttgart

Umfassende Absicherung von Voice over IP und Unified Communications

08.05. - 10.05.17 in Frankfurt
10.07. - 12.07.17 in Düsseldorf

Optionales Einsteiger-Seminar:

IP-Wissen für TK-Mitarbeiter
20.02. - 21.02.17 in Bonn
02.05. - 03.05.17 in Düsseldorf
18.09. - 19.09.17 in Düsseldorf

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

Basis-Paket: Beinhaltet die drei Basis-Seminare

Grundpreis: € 5.100,--* statt € 5.670,--*

Optionales Einsteigerseminar: Aufpreis € 1.190,--* statt € 1.590,--*

* alle ausgewiesenen Preise sind netto-Preise

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: kundenservice@comconsult-research.de
<http://www.comconsult-research.de>

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

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

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