ComConsult Research

Der Netzwerk Insider

Juni 15

Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

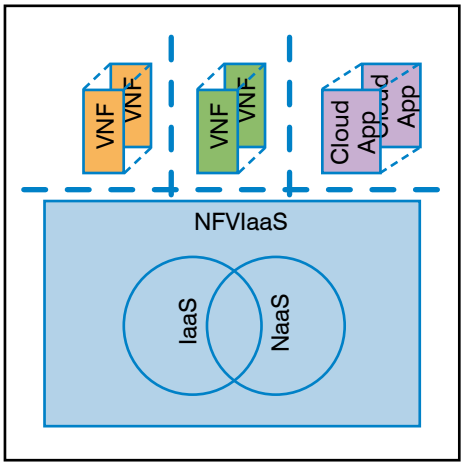
SDN, NFV, OpenFlow und Virtualisierungs-Protokolle – Zusammenhänge, Perspektiven, Marktrelevanz - Teil 3

von Dipl.-Inform. Petra Borowka-Gatzweiler

2.2 NFV und SDN

Teilweise werden NFV und SDN als komplementär bezeichnet, teilweise wird NFV als Untermenge von SDN betrachtet – das kommt auf die jeweilige Brille an. Sieht man SDN im weiteren Sinne als Softwaretechnologie in Netzwerken, dann ist NFV eine SDN-Ausprägung.

Sieht man SDN im engeren Sinne konform zu ONF, dann ist es komplementär zu NFV: SDN trennt Control und Data Plane im Netzwerk, das heißt es entkoppelt die Kontrolle von der Hardware und schafft einen zentralen Kontroll- und Orchestrierungspunkt mit zentraler Sicht auf das verteilte Netzwerk mit all seinen unterschiedlichen Komponenten. NFV richtet sich auf die Optimierung der Netzwerkdienste selbst, indem es die Netzwerk-Funktion von der Hardware entkoppelt, wobei typischerweise höherwertige Funktionen als Layer-2/3 im Fokus stehen (DHCP, DNS, Caching, Firewall, Load Balancer etc.).



In diesem Sinn lässt sich jede Technologie alleine einsetzen, aber eine Kombination von SDN und NFV ist ebenfalls möglich und verspricht Synergien: SDN leistet dann die Netzwerk-Automatisierung, insbesondere Policy Management und Traffic Engineering, und NFV optimiert höherwertige Ende-zu-Ende Netzdienste.

weiter auf Seite 6

Zweitthema

Konsequenzen von Moore´s Law für die Arbeitswelt und die Gestaltung von Netzen und Systemen in den nächsten Jahren

von Dr. Franz-Joachim Kauffels

Wir feiern in diesem Jahr den 50. Geburtstag von „Moore´s Law“, der Beobachtung und Prognose von Gordon Moore, dass sich die Anzahl von Transistoren in einem Chip wenigstens alle 24 Monate verdoppelt. Es ist für die nächsten Jahre nicht abzusehen, dass sich an dieser Tendenz grundsätzlich etwas ändern wird. Was bedeutet das aber für die „Millenium-Generation“, die jetzt langsam beginnt, in die Arbeitswelt einzutreten? Die Antwort auf diese Frage gibt eine Reihe von wichtigen, konkreten Hinweisen darauf, wie sich Unternehmen angesichts des aktuellen Wandels positionieren müssen. In jedem Fall wird es keine für alle gültigen IT-Architekturen und -Lösungen geben.

Vor fünfzig Jahren hat Dr. Gordon Moore die schnelle Rate der Leistungsverbesserung von Halbleiter-Chips systematisch bestimmen wollen und hat rückblickend betrachtet den Herzschlag der modernen Welt entdeckt. Es ist ein sich immer weiter beschleunigender Rhythmus, den auch diejenigen spüren, die im digitalen Zeitalter geboren wurden, oft ohne seinen Ursprung zu kennen.

weiter auf Seite 24

Geleit

BND-Affäre: das Ende der Email?

auf Seite 2

Aktuelle Veranstaltung

Sommerschule 2015 - Intensiv-Update auf den neuesten Stand der Netzwerktechnik

ab Seite 4

Standpunkt

Herrschaft der Maschinen

auf Seite 20

Aktuelle Sonderveranstaltung

IT-Kommunikation im Umfeld von Fertigung und Automation

ab Seite 21

Zum Geleit

BND-Affäre: das Ende der Email?

Die BND-Affäre unterstreicht wieder einmal, dass wir öffentlichen Vermittlungseinrichtungen nicht trauen können. Dies gilt offenbar nicht nur für die Technik, sondern auch für mindestens eine Bundesbehörde. Die offenkundige Mitwirkung an Industriespionage sucht in der Geschichte der Bundesrepublik seines gleichen. Nicht nur, dass keinerlei Bereitschaft gezeigt wird, die Sicherheit im Internet für Unternehmen in Europa zu fördern (es ist ja kein wirkliches technisches Problem eine sichere Email- oder Kommunikations-Lösung zu schaffen), hier wird aktiv gegen die Interessen von deutschen Unternehmen gearbeitet. Das Argument, dass die Offenheit und Abhörbarkeit benötigt wird, um kriminellen Aktivitäten auf die Spur zu kommen, ist dabei so an den Haaren herbeigezogen, dass es schon peinlich ist. Jeder organisierte Kriminelle wird mittlerweile mitbekommen haben, dass Kommunikation über das Internet abgehört wird und eine entsprechende Lösung gefunden haben. Da die Politik keinerlei Bereitschaft zeigt, hier Abhilfe zu schaffen (was natürlich zur Frage führt, warum das so ist), stellt sich umgekehrt die Frage was deutsche Unternehmen unternehmen können, um sich zu schützen.

Dies ist natürlich auch direkt mit der Frage verbunden, ob die durch den BND durchgeführte Industrie-Spionage eine andere Qualität hat als “normale” Industriespionage. Anders gefragt, reichen dieselben Schutzmechanismen aus, die wir sowieso zum Einsatz bringen oder gibt es angesichts dieser Entwicklung einen erhöhten Schutzbedarf? Der Unterschied liegt maximal darin, dass Bundesbehörden ggf. einen leichteren Zugang zu zentralen Kommunikations-Infrastrukturen haben (siehe das Beispiel des Abhörens von Seekabeln durch die Briten). Aber im Kern verdeutlicht die Abhöraffäre nur das Grundprinzip, dass öffentliche Kommunikations-Infrastrukturen als nicht vertrauenswürdig anzusehen sind. Die anderen Elemente einer Sicherheits-Strategie, die die interne Sicherheit und zum Beispiel Zonenkonzepte betreffen, sind hiervon nicht berührt.

Im Moment gibt es mindestens zwei typische Kommunikationsdienste, die über öffentliche Vermittlungseinrichtungen laufen und häufig nicht verschlüsselt sind:

- Sprach- und Videokommunikation
- Email

Zumindest für Gespräche und Video-

konferenzen innerhalb der Unternehmen, auch wenn sie über das Internet führen, sind Verschlüsselungs-Lösungen verfügbar und sollten sowieso generell eingesetzt werden. Für Videokonferenzen mit Externen gibt es auch entsprechende Lösungen oder man greift zu Peer-to-Peer-Lösungen, die nur zwischen den Endteilnehmern in verschlüsselter Form ablaufen. Das bekannteste Beispiel ist hier VSee, das auch die Zulassung der amerikanischen Gesundheits-Behörden für die Nutzung im medizinischen Dienst hat (also zum Beispiel zur Kommunikation zwischen Ärzten). Generell muss man erwarten, dass auch solche verschlüsselten Lösungen gezielt angegriffen werden könnten, aber der Aufwand wird sehr hoch sein und der Zugang zu Dienst-Providern wird in der Regel einen Gerichtsbeschluss erfordern (sofern die Angreifer sich nicht andere Backdoor-Mechanismen bei den jeweiligen Providern geschaffen haben).

Damit sind wir bei der Frage, wie wir in Zukunft mit der Email als Kommunikations-Dienst umgehen wollen. Neben ausgewählten Bundesbehörden ist die Email sowieso ein kritischer Dienst, der auch anderen Angreifern immer wieder Gelegenheit bietet, Trojaner und andere Abhör- und Sabotage-Instrumente im Unternehmen zu platzieren. Da die Verschlüsselung von Email bis heute nicht so umgesetzt werden kann, dass man von einer eleganten Nutzung sprechen kann, steht die Frage nach der Vermeidung von Email und der Nutzung anderer Dienste im Raum.

Aus meiner Sicht liegt es zumindest nahe folgende Alternativen zu evaluieren:

- Aufbau von internen Kommunikations- und Kollaborations-Portalen, keinerlei interne Kommunikation mehr über Email
- Aufbau von zentralen Datei-Diensten, wahlweise als Cloud-Lösung mit privatem Schlüssel-Management oder als eigen-gehostete Lösung (siehe box.net)

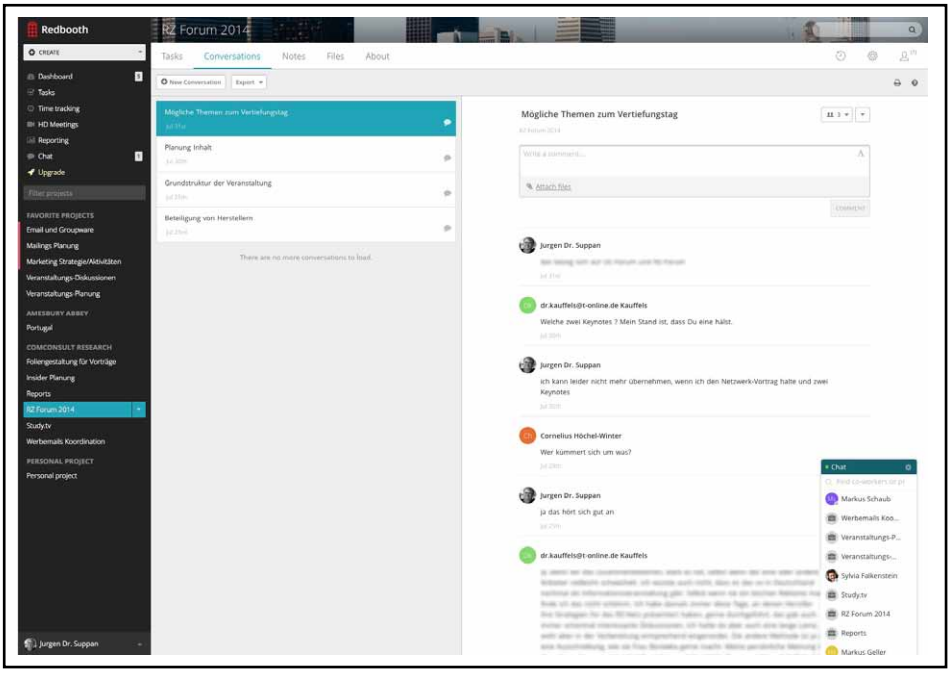


Abbildung 1: Einsatz eines Kollaborations-Portals bei ComConsult mit Integration Externer, hier zur Vorbereitung des UC-Forums 2014

BND-Affäre: das Ende der Email?

- Datei-Austausch mit Dritten über diesen Datei-Dienst in genau kontrollierter Form

Speziell der Aufbau von Kommunikations- und Kollaborations-Portalen hat diverse Zusatz-Vorteile. Kommunikation kann Projekt-bezogener mit integriertem Task-Management abgewickelt werden, Teilnehmer können auch im Nachhinein zu einer Kommunikation hinzu kommen und alle für eine Kommunikation benötigten Dokumente können mit in die Plattform integriert werden (entweder direkt oder über Link-Integrationen mit entsprechenden Plattformen wie box.net). Zum Teil können Kommunikationsdienste mit Portalen gebündelt werden, so zum Beispiel bei Redbooth und Zoom.

Anschließender Standpunkt:

- Email als Dienst sollte so weit wie möglich vermieden werden

- Generell sollte nur verschlüsselt kommuniziert werden, auch wenn dies gerade wenn eine Entschlüsselung auf Servern erfolgt, nur eine bedingte Sicherheit ist

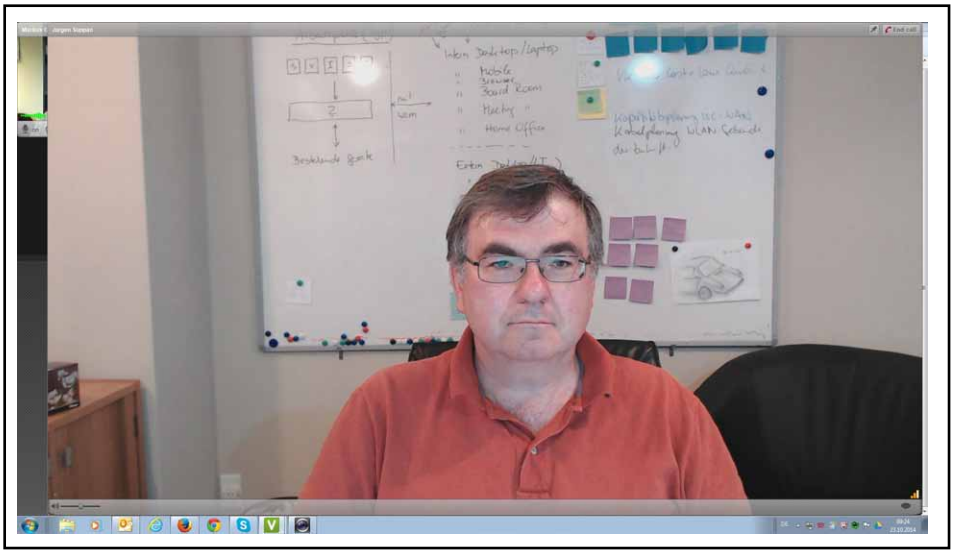


Abbildung 2: Einsatz von VSee bei ComConsult Research

- Innerhalb eines Unternehmens bieten Kommunikations- und Kollaborationsportale deutlich mehr Funktionalität und sollten evaluiert werden

- Es gibt ein Angebot für sichere Kommunikation im Markt, das ebenfalls evaluiert werden sollte, VSee ist ein Beispiel hierfür

- Wer heute noch Dateien über unverschlüsselte Emails übertragt ist selber schuld

Ihr Dr. Jürgen Suppan

Sonderveranstaltung

Voice und Video im WAN - 22.06.15 in Köln

All-IP, B2B, B2C und Daten kämpfen um die Kapazität, wie kann das beherrscht werden?

Wie kann die Übertragung von Sprache und Video im WAN optimiert werden ohne andere Anwendungen zu gefährden? Wie gehen wir mit einem immer größeren Anteil und vor allem der Integration von Video in wesentliche Geschäftsprozesse um? Neue Kollaborations-Lösungen erhöhen zudem den Druck auf die Infrastrukturen. Verkehrslasten werden dabei immer dynamischer und einfache statische Regeln wie traditionelles QoS stoßen an ihre Grenzen.

Die Sonderveranstaltung beleuchtet den Status Quo, die Zukunftsaussichten, mögliche Optionen und eventuellen Investitionsbedarf für den sicheren Betrieb aller Anwendungen.

Diese Sonderveranstaltung greift dieses drängende Problem auf und analysiert:
- wie können Sprache und Video optimiert werden ohne andere Anwendungen zu gefährden
- wie gehen wir mit einem immer höheren Anteil speziell von Video in zentralen Geschäftsprozessen und speziell auch in der Kommunikation mit Kunden um
- wie können wir die extreme Dynamik der Verkehrslasten beherrschen
- wie können wir eine ausreichende Qualität gerade in sensitiven Nutzungen für Video sicher stellen
- welche Parameter stehen uns zur Verfügung, um die notwendige Optimierung durchzuführen
- welche Dimensionierung des WAN ist in Zukunft erforderlich
- wie können Betriebsprobleme erkannt, bearbeitet und eingeschränkt werden

Referenten: Dipl.-Ing. Martin Egerter, Dipl.-Math. Leonie Herden, Dipl.-Ing. Dominik Zöller
Preis: € 990,-- netto

Buchen Sie über unsere Web-Seite

www.comconsult-akademie.de

Aktuelles Seminar

Sommerschule 2015 - Intensiv-Update auf den neuesten Stand der Netzwerktechnik

22.06. - 26.06.15 in Aachen

Die Sommerschule 2015 bringt Sie in 5 Intensiv-Tagen auf den letzten Stand der Netzwerk-, Kommunikations- und Infrastruktur-Technik.
Wir analysieren für Sie:

- Wie verändern sich IT-Architekturen?
- Welche neuen Technologie-Ansätze gibt es bei Netzwerken?
- Welche Auswirkungen hat das auf Netzwerke, Kommunikations-Technik und Infrastrukturen in der täglichen Praxis?
- Welche Änderungen und Investitionen sind auf Ihrer Seite in der nächsten Zeit erforderlich?

Programmübersicht Sommerschule 2015

Montag, der 22.06.15 - IT-Architekturen und Auswirkungen auf auf LAN und WAN

IT-Architekturen sind geprägt von Endgeräten, die lokale Anwendungen ausführen und auf Applikationen auf Server zugreifen. Im Moment ändert sich hier alles. Unser Verständnis von Endgerät, Betriebssystem und Server muss auf den Prüfstand. Ohne Zweifel wird unsere IT-Landschaft in fünf Jahren dramatisch anders aussehen als heute. Und Netzwerke haben die zentrale, tragende Rolle für diese Entwicklung. Wir analysieren wo es hingeht und wie Netzwerke aussehen müssen, um diesen Weg zu unterstützen.

9:30 - 17:00 Uhr
Wir analysieren für Sie:

- Wie ändert sich IT und welche Auswirkungen hat das auf Infrastrukturen?
- Was passiert auf der Netzwerk-Seite, um diesen Anforderungen zu entsprechen?
- Welche neuen Technologien müssen speziell bei den Planungen für die nächsten Jahre beachtet werden?

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

Das WAN gewinnt mit den Entwicklungen im IT-Architektur-Bereich immer mehr an Bedeutung. Gleichzeitig entstehen Nutzungssituationen, die wirtschaftlich nicht immer abgedeckt werden können.

Wir analysieren für Sie:

- Welchen Stellenwert haben aktuelle WAN-Technologie für eine moderne IT
- Internet versus WAN: was ist besser?
- Ist Mobilfunk die Zukunft? Taugt es als Ersatz für terrestrische Leitungen?
- Anforderungen von Voice und Video: B2B und B2C puschen den Video-Anteil in bisher unerreichte Höhen, wie kann das WAN damit umgehen?
- QoS im WAN: unlösbarer Widerspruch oder wie weit gehen die vorhandenen Lösungen?

Dr.-Ing. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

11:00 - 11:15 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause
15:00 - 15:15 Uhr Kaffeepause
ab 19:00 Uhr Happy Hour

Dienstag, der 23.06.15 - LAN-Technologien: aktuelle Entwicklungen

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

9:00 - 17:00 Uhr
Sie lernen in diesem Themenblock:

- Welche neuen LAN-Technologien gibt es, welche Konsequenzen hat das?
- Netzwerk-Design mit 10/40/100 Gigabit, wie sehen Anforderungen und Planungs-Ansätze aus?
- Fabric-Konzepte verdrängen traditionelle Architekturen: was leisten sie und wie können sie sinnvoll eingesetzt werden?
- Edge/Core-Architekturen mit neuen Formen von Label-Switching: ist hier die Zukunft?
- Quo Vadis VLAN-Technik: werden VLANs durch Edge-Provisioning und Overlays verdrängt?

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

10:30 - 10:45 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause
15:00 - 15:15 Uhr Kaffeepause

Mittwoch, der 24.06.15 - Sicherheit / Unified Communications: wo stehen wir?

Sicherheit in der IT wird zum dominierenden Thema der nächsten Jahre. Aber hier geht es nicht um hochfliegende Träume, sondern um ein solides Fundament aus Basis-Sicherheits-Funktionen. Dies ist das Thema des Bereichs Sicherheit in der Sommerschule:

9:00 - 12:30 Uhr

- Sicherheit im LAN: neueste Entwicklungen
- Sicherheit und mobile Endgeräte: haben wir noch eine Chance unsere Sicherheit zu retten?
- Sicherheit und UC: immer offener und immer sicherer, ist das ein unlösbarer Widerspruch?

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

UC-Projekte haben in den letzten Jahren deutlich an Komplexität gewonnen. Zwar haben sich die Produkte weiter entwickelt, doch gleichzeitig hat sich ein neues Verständnis von Kommunikation mit einer gleichzeitigen Verschiebung der Funktionsbereiche ergeben. Moderne Browser beinhalten heutzutage die komplette Funktionalität eines UC-Clients für Sprache und Video und generieren die Frage nach der Zukunft des Telefons.

14:00 - 17:00 Uhr
In diesem Themenblock lernen Sie:

- Wo steht UC heute?
- Wie sieht die Zukunft des Clients aus?
- Wird das Telefon als Endgerät verdrängt?
- Was kommt nach ISDN?
- UC und Kollaboration: Gibt es überhaupt noch eine Abgrenzung? Wie sieht die Zukunft aus?
- Welche Rolle werden Produkte wie Cisco Project Square oder Unify Circuit für den Markt haben?
- Was bedeutet diese Entwicklung für Infrastrukturen?

Dipl.-Inform. Petra Borwoka-Gatzweiler, Planungsbüro UBN
Markus Geller, ComConsult Research GmbH

10:30 - 10:45 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause
15:00 - 15:15 Uhr Kaffeepause

Programmübersicht Sommerschule 2015

Donnerstag, der 25.06.15 - WLAN und Mobilfunk / IPv6: aktueller Stand bei Unternehmen

Mit der rasanten Zunahme mobiler Endgeräte bekommt der Zugang dieser Geräte zu den Unternehmens-Infrastrukturen eine zentrale Bedeutung. In Zukunft werden deutlich mehr Endgeräte diesen Zugang wählen als die Kabel-basierte Alternative. Denkt man einen Schritt weiter zum Internet of Everything, dann wird die zukünftige strategische Bedeutung des Zugangs über WLAN und Mobilfunk deutlich. Sowohl die schiere Anzahl der Teilnehmer als auch der damit verbundene Schutz- und Kontrollbedarf machen Änderungen an der Netzwerk-Infrastruktur erforderlich.

9:00 - 12:30 Uhr
In diesem Themenblock lernen Sie:
- Welche Optionen Ihnen das moderne WLAN bietet
- Wie sich Mobilfunk-Alternativen demgegenüber positionieren

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

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.

14:00 - 17:00 Uhr
In diesem Themenblock lernen Sie:
- Welche Entscheidungen wann getroffen werden müssen
- Wie man ein IPv6 Projekt planerisch und organisatorisch umsetzt
- 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
- Wie man die Internet-Präsenz schrittweise migriert
- Worauf bei Software und Appliances in Bezug auf IPv6 zu achten ist

Markus Schaub, ComConsult Study.tv

10:30 - 10:45 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause
15:00 - 15:15 Uhr Kaffeepause

Freitag, der 26.06.15 - Rechenzentren: neue Arten von Infrastrukturen gefordert

Rechenzentren sind von allen Seiten unter Druck:
- Die Cloud generiert einen direkten Kostenvergleich und puscht das Thema Wirtschaftlichkeit im RZ noch weiter als bisher
- Infrastrukturen für mobile Endgeräte erfordern den Aufbau einer private Cloud und setzen neue Anforderungen an Infrastrukturen
- Server- und Speicher-Konsolidierungen gehen permanent weiter, neue Perspektiven entstehen und stellen alle traditionellen Ansätze in Frage
- Virtualisierung geht in die nächste Runde, leistet noch mehr, stellt aber auch immer mehr und immer schwierigere Anforderungen an die Infrastrukturen

Angesichts dieser Entwicklungen brauchen Rechenzentren eine neue und Zukunftsorientierte Infrastruktur-Strategie.

9:00 - 15:30 Uhr
Sie lernen in diesem Themenblock:
- Was passiert im RZ, welche neuen Anforderungen entstehen?
- Wo stehen Server und Speicher?
- Welche Anforderungen generiert Virtualisierung?
- Dienstneutralität im Netzwerk: geht das noch im RZ der Zukunft? Ist Ethernet nach wie vor DIE Technologie, auf der alles basiert?
- Was ist ein Software-defined Data Center? „Nur“ eine Provider-Technologie oder auch eine Chance für Unternehmen? Und wie realisert man es?

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

10:30 - 10:45 Uhr Kaffeepause
13:00 - 14:00 Uhr Mittagspause
15:30 Uhr Ende der Veranstaltung

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Sommerschule 2015 - Intensiv-Update auf den neuesten Stand der Netzwerktechnik

Ich buche das Intensiv-Seminar
Sommerschule 2015

☐ vom 22.06. - 26.06.15 in Aachen
zum Preis € 2.490,-- netto

Zur Anmeldung
www.comconsult-akademie.de

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

Schwerpunktthema

SDN, NFV, OpenFlow und Virtualisierungs-Protokolle – Zusammenhänge, Perspektiven, Marktrelevanz (Teil 3)

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

Fortsetzung von Seite 1

Beide Technologien haben erkennbare Gemeinsamkeiten, die bei einer Kombination von NFV und SDN zu Synergien führen können:

- Verschiebung von Funktionalität aus der Hardware in die Software
- Nutzung von Standard-Hardware
- Nutzung offener APIs
- Effiziente Unterstützung von Orchestrierung, Virtualisierung und Automatisierung
- Fokussierung auf Cloud Umgebungen

Indem SDN einerseits die Netzkontrolle von der Hardware löst und zu einer netzweiten Sicht auf das Gesamtnetz bündelt, andererseits Netzressourcen abstrahiert und (vor)programmierte Kontrolle implementiert, passt es gut in das NFV Paradigma: SDN kann eine wichtige Rolle in der Orchestrierung der NFV Infrastruktur Ressourcen spielen, indem es hier Konfiguration und Provisionierung von Konnektivität, Bandbreite, Sicherheit und anderen Policy-Bereichen leistet.

NFV erschafft eine sehr dynamische, mandantenfähige Netzwerkumgebung, in der VNFs und ihre Konnektivität häufig die Lokation ändern, um der aktuellen Verkehrslast gerecht zu werden. Die Programmierbarkeit, die SDN auf der Netzwerkseite bereitstellt, lässt sich hierfür gut einsetzen. Der SDN Controller kann die Automatisierung komplexer NFV Forwarding Graphen und Service-Ketten (Service Chaining) unterstützen. Innerhalb der NFV Architektur kann der SDN Controller als Netzwerk Controller im Architekturblock NFVI seinen Platz finden. Dann wäre SDN eine Untermenge von NFV (was die SDN-Bäcker sicher nicht so gerne sehen). In der NFV Bewegung wird jedoch äußerst großer Wert darauf gelegt, dass ein SDN Controller auf keinen Fall eine wesentliche Vergrößerung von Overhead, Jitter, Latenzzeit usw. und auch keine Verschlechterung von Verfügbarkeit oder Robustheit verursachen darf. Somit ist die SDN-Einsetzbarkeit mit deutlichen Restriktionen belegt.

Andersherum aufgezogen, könnte SDN auch von NFV-Konzepten wie virtualisierte Infrastruktur Manager profitieren: Ein SDN Controller – vorausgesetzt, er ist auf einer VM lauffähig – könnte Teil einer Service-Kette sein und sich selbst im Verbund mit anderen VNF als virtualisierte Netzwerkfunktion präsentieren, um so von der Dynamik und Elastizität profitieren, die NFV mit sich bringt.

Fazit: Je nach Sichtweise und Implementierung können SDN und NFV komplementär sein, kann NFV Teil von SDN sein oder kann SDN Teil von NFV sein.

Was den geneigten Leser jetzt sicher sehr viel weiter bringt. Aber wie sagt der Schweizer dazu: Ist so, weil ist so.

2.3 NFV Einsatz-Szenarien

Im Dokument "NFV 001: NFV; Use Cases" hat die ETSI Arbeitsgruppe eine Reihe Einsatz-Szenarien spezifiziert, die aus ihrer Sicht im Fokus von NFV stehen und die aktuelle Ausrichtung der NFV-Entwicklung verdeutlichen:

- Infrastruktur als Dienstleistung (IaaS)
- Virtuelle Netzwerk-Funktion als Dienstleistung (VNFaaS)
- Virtuelle Netzwerk-Plattform als Dienstleistung (VNPaaS)
- VNF Forwarding Graphen
- Virtualisierung des Mobilfunk Core Netzwerks und des IMS
- Virtualisierung der Mobilfunk-Basisstation
- Virtualisierung der Home Umgebung
- Virtualisierung von CDNs (vCDN)
- Virtualisierung der Netzwerk-Funktionen für den Festnetz-Zugang (Last Mile / DSL)

Nachfolgend beschreiben wir einige dieser Einsatzszenarien exemplarisch.

Beispiel 1: NFV für Infrastructure as a Service (NFVIaaS)

Viele Cloud Provider bieten zusätzlich zu den bekannten Netzwerk-Diensten Rechen-Dienste (Computing Services) an, sind also zusätzlich zum ISP auch CSP. Solche Cloud-Rechen-Dienste erfordern physische Rechner, Netzwerk- und Speicher-Ressourcen, hierzu gibt es zum Beispiel die ITU-T Empfehlungen Y.3510 (05-2013) und Y.3501 (05/2013). Ressourcen Pools sind ja auch ein essentielles Cloud Computing Merkmal in der NIST Definition. Gleichermaßen sind Ressourcen Pools eine Charakteristik der NFV Infrastruktur. Somit passt beides sehr gut zusammen: Der gemeinsame Wunsch ist es, Rechner-, Netzwerk- und Speicher-Ressourcen so in Pools zusammenzufassen, dass ein Service Provider möglichst einfach sowohl Cloud Computing als auch Netzwerk-Dienste bereitstellen und erbringen kann.

Die benötigten physischen Rechner-, Netzwerk- und Speicher-Ressourcen werden im NFV Modell als Compute, Hypervisor und Netzwerk-Domäne innerhalb der NFV Infrastruktur bezeichnet. Im

SDN, NFV, OpenFlow und Virtualisierungs-Protokolle - Teil 3

Cloud Computing Modell werden diese Ressourcen als Elemente dargestellt, die IaaS oder NaaS als Cloud-Dienst unterstützen.

Die Rechner-Knoten (Hosts) der NFV Infrastruktur werden in NFVI-PoPs stehen. Dies können zentrale Standorte, Außengelände, spezielle PoDs sein, oder aber die Ressourcen können in andere Netze sowie mobile Infrastrukturen eingebettet sein. Der tatsächliche physische Standort ist weitestgehend unabhängig vom Cloud Dienst, aber viele Netzwerk-Dienste haben eine gewisse Abhängigkeit von der konkreten Lokation / dem geografischen Standort. Das Konzept des Ressourcen-Pools beinhaltet selbstverständlich auch Mandantenfähigkeit: derselbe Ressourcen-Pool unterstützt verschiedene Anwendungen von verschiedenen administrativen Zonen oder sicherheitstechnischen Schutz-Zonen. Eine Übersicht zeigt Abbildung 2.7.

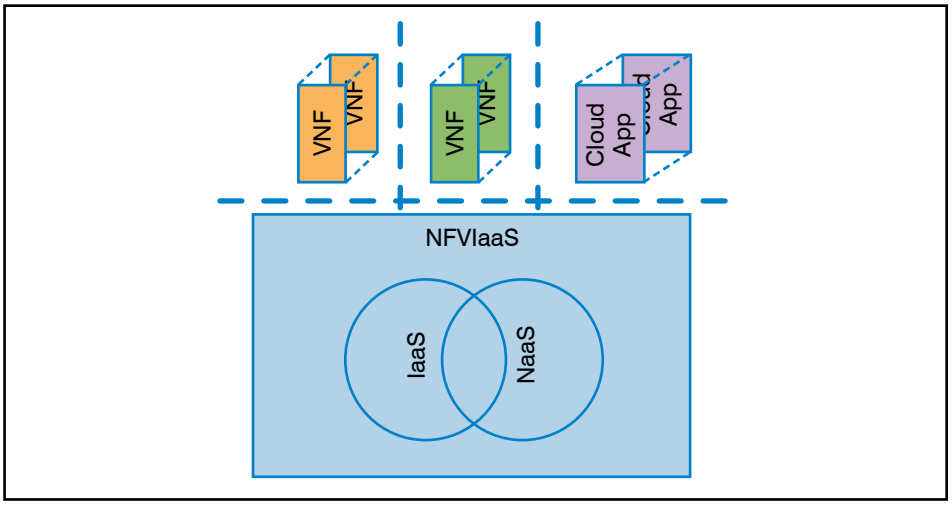


Abbildung 2.7: NFVIaaS mit Mandanten-Unterstützung

Das NFVIaaS-Modell unterstützt auch die Verschachtelung von Providern und Cloud Diensten: Ein Service Provider B betreibt VNF Instanzen in der NFVI/Cloud Infrastruktur eines anderen Service Providers A – hierzu existiert dann eine entsprechende Dienstvereinbarung zwischen beiden Providern.

Der parallele Einsatz und Betrieb von virtualisierten und nicht-virtualisierten Netzwerk-Funktionen ist nach wie vor möglich, hier erwartet die ETSI keine Seiteneffekte oder besondere Probleme. Gleiches gilt für die Koexistenz von VNFs verschiedener Service Provider innerhalb einer gemeinsamen NFV Infrastruktur (NFVI). Die Isolierungs-Mechanismen zwischen den Ressourcen können gleicherweise Mandanten oder verschiedene Service Provider handhaben.

NFVIaas: Probleme, offene Punkte

NFVIaaS soll einem Service Provider X ermöglichen, dem Endkunden Dienste anzubieten, diese zu leisten und auch in Rechnung zu stellen – dabei soll er unterschiedliche NFVIs nutzen können, die zu verschiedenen administrativen Domänen gehören. Dies erfordert ein sehr genaues Monitoring und Reporting für alle entsprechenden Statuswerte der Ressourcen, die dem Provider X als VNF Instanzen bereitgestellt wurden. Die SLA-Parameter, die ein Provider mit seinen Kunden vereinbart hat, müssen in einer NFVIaaS zwischen verschiedenen Providern unterstützt und übermittelt werden.

Die Lösungs-Idee ist hier folgende: Management und Orchestrierung von VNF Instanzen in einer Netzwerk-Service-Instanz sollte durch einen VNF Forwarding Graph auch dann möglich sein, wenn die VNF Instanz auf der NFV Infrastruktur eines anderen Service Providers läuft. Für die Orchestrierung der VNF Instanzen in solchen Umgebungen sind angemessene Authentisierungs- und Autorisierungs-Verfahren erforderlich. Betriebserfahrungen hierzu liegen bisher allerdings kaum vor.

Beispiel 2: VNF as a Service (VNFaaS)

Aktuell betreiben Unternehmen am Perimeter eines Außenstandortes eine ganze Reihe von Diensten. Abgesehen davon, dass dedizierte standalone Appliances je Dienst unflexibel, schlecht installierbar und aufwändig zu betreiben sind, sind die Kosten für diese Appliances dem Controlling ein Dorn im Auge. In einigen Implementierungen leistet ein integrierter Access Router die gewünschten Dienste, dieser hat jedoch häufig einen eingeschränkten Funktionsumfang. Für flexibles Wachstum hinsichtlich Funktionalität und Skalierbarkeit bietet sich eine Auslagerung dieser Dienste in die Cloud an. Anvisierte Dienste, die sich in der Cloud mit NFV virtualisieren lassen, sind aus ETSI-Sicht:

- AR – Enterprise Access Router
- E-CPE – Enterprise CPE
- PE – Provider Edge Router
- FW – Enterprise Firewall
- NG-FW – Enterprise NextGen Firewall
- WOC – Enterprise WAN optimization Controller
- DPI – Deep Packet Inspection (Appliance oder Funktion)
- IPS – Intrusion Prevention System und andere Sicherheits-Appliances
- Network Performance Monitoring

So wird der AR zu einem vAR, das E-CPE zum vE-CPE (siehe Abbildung 2.8). der PE zu einem vPE und der FW zum vFW virtualisiert. Ein vPE beispielsweise sollte die Data Plane und Control Plane unabhängig voneinander skalieren können, um mittlere bis äußerst große Forwarding Tabellen sowie die dazu korrespondierende noch deutlich größere Anzahl von Flows zu unterstützen… Hierbei gilt für den Enterprise Bereich im Vergleich zum Home Bereich: Der Enterprise Bereich erfordert eine signifikant niedrigere Anzahl von VNFs, jedoch jede davon mit erheblich größerer Anzahl von Flows und Leistungs-Anforderungen als der Home Bereich.

Anforderungen von VNFaaS

Aber schon die für den Enterprise Bereich erforderliche, absolut betrachtet hohe Anzahl an virtualisierten Enterprise Appliances muss in der NFV Infrastruktur auf einer limitierten Anzahl von CPUs / COTS Rechnern integriert werden. Je höher die Enterprise-Bedarfe nach Bandbreite steigen, desto höhere Bandbreite je CPU werden sie anfordern. Heutige CPUs sind für das erwartete Bandbreiten-Wachstum definitiv noch nicht ausgelegt.

Die Frage, warum für Netzwerk-Core Komponenten heute noch keine NFV-fähige Lösung von COTS-Herstellern vermarktet wird, hat sich damit selbst beantwortet: Diese Geräte erfordern eine derartige Leistung, dass sie zur Zeit einfach nicht virtualisiert und auf beliebige NFV Infrastrukturen und COTS CPUs verteilt werde können.

Ein weiterer potenzieller Problembereich ist die Erwartungshaltung, dass sowohl der Enterprise Betreiber als auch der Provider sich die Verantwortung für das Management der vPE und vE-CPE teilen. So erwartet der Enterprise Betreiber zum Beispiel, dass er seine CPE Komponenten konfigurieren und Software Upgrades durchführen kann, wann immer gera-

SDN, NFV, OpenFlow und Virtualisierungs-Protokolle - Teil 3

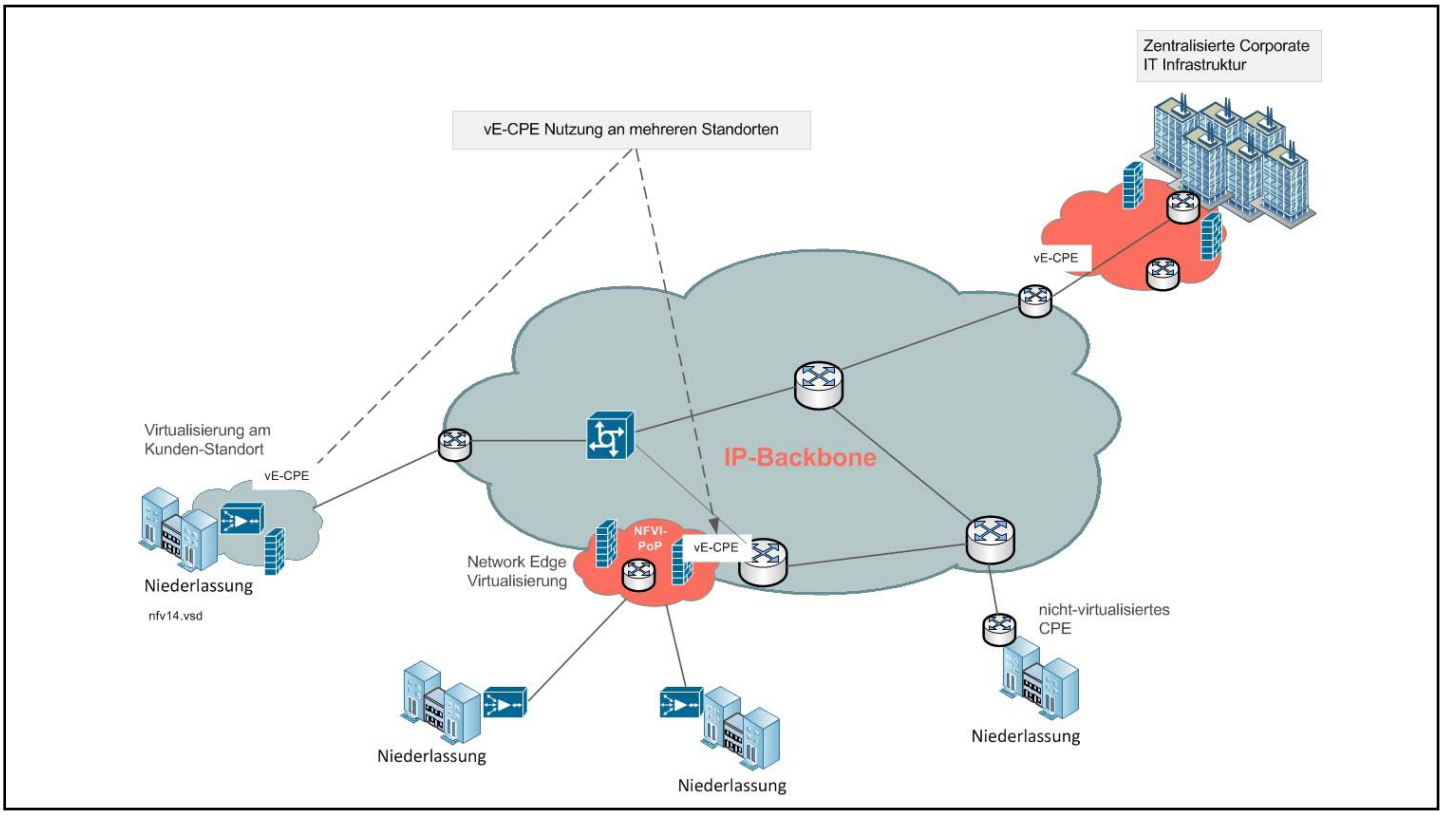


Abbildung 2.8: vE-CPE Standort-Beispiele

de der Bedarf dazu besteht – auch dann, wenn sie als virtualisierter Dienst bereitgestellt werden.

Zudem entsteht ein neuer Single Point of Failure: Konfiguration und Management sind nicht mehr möglich, wenn der Netzwerk-Zugang zum Service- / Virtualisierungs-Provider nicht mehr funktioniert! Wie soll die Service-Kontinuität aufrechterhalten werden, wenn der Access Link nicht zur Verfügung steht? Hier liegen für NFV Provider ernsthafte Herausforderungen, deren valide Lösungen im Betrieb nachgewiesen werden muss.

Will man eine SDN-Architektur nutzen, und ein zentraler Controller steuert vPE oder vE-CPE, ist auch der Controller und Controller-Zugang lebenswichtig und gilt es, hier einen SPoF zu vermeiden.

Sichere Mandanten-Isolierung ist für die Ausdehnung eines Enterprise LAN in das Betreiber-Netzwerk eines Cloud-Anbieters ein sine-qua-non. Darüber hinaus muss das Thema gelöst werden: Wie werden Enterprise Daten und Konfigurationsdateien geschützt?

Es müssen Metriken für die VNF-Nutzung, das Accounting und die Parameter der mit dem Kunden vereinbarten SLAs entwickelt werden. Solche Metriken gibt es heute bestenfalls ansatzweise.

VNFaaS: Probleme, offene Punkte

Es ist leicht vorstellbar, dass über die Summe aller Endkunden hinweg eine schlichtweg riesige Menge an virtualisierten Geräten / Appliances entstehen wird, die von der NFV Infrastruktur für den gesamten Enterprise Edge Bereich unterstützt werden müssen.

Für weitere Beispiele sei auf das ETSI-Dokument ETSI GS NFV 001 v1.1.1: "Network Function Virtualisation (NFV); Use Cases" verwiesen.

3. Marktrelevanz und Fazit

Aktuell besteht die Erwartungshaltung, dass SDN und NFV zu den dramatischsten Technologie-Änderungen im Netzwerkbereich gehören werden. Sie führen zu signifikanten Änderungen in Design, Deployment, Betrieb sowie zukünftigen Netzwerk- und Rechenkomponenten. Marktforscher wie Gigaom Research gehen davon aus, dass diese beiden Technologien in den nächsten fünf bis zehn Jahren über Erfolg oder Scheitern von Dienstanbietern und Betreibern entscheiden können.

Kernaussagen einer Umfrage von Gigaom Research (300 Enterprises, 300 Service Provider) 2013/2014 ergaben:

- Bei den Unternehmen, die sich dafür entschieden haben, sind die erhofften Umsetzungszeiträume durchaus ehrgeizig, die Erwartungen in den zu erreichenden Mehrwert sind hoch. Die Umsetzungs-Zeitachse wird überwiegend bei ein bis zwei Jahren gesehen.

- Sicherheit ist immer noch eine der großen Herausforderungen, egal ob mit oder ohne SDN. Auch hier erhofft man sich Lösungsfortschritte durch SDN und NFV.

- Vorrangige kurzfristige Verbesserungen beim Ausrollen von SDN und NFV erhoffen sich die Betreiber durch den Einsatz von OpenSource Lösungen. Investitions-Optimierung, effizientere Auslastung und verbesserte Service Level werden als mittelfristiges Potenzial betrachtet.

- Im Providerbereich war das erste Ziel für SDN und NFV Anwendungen mit großem Abstand das Rechenzentrum, im reinen Enterprise Umfeld hat das WAN jedoch noch Vorrang vor dem Rechenzentrum.

- SDN / NFV für WLAN Netzwerke hat Vorrang vor verkabelten Netzwerken.

- Der Wunsch nach Industrie-Standards steht sehr weit oben auf der Wunsch-Liste, dennoch suchen die Betreiber

SDN, NFV, OpenFlow und Virtualisierungs-Protokolle - Teil 3

nicht nach einer "Low-Feature-Common-Denominator"-Lösung, sondern erwarten durchaus auch von standardbasierten Produkten einen hohen Funktionsumfang. Sie wollen Basis-Interoperabilität mit dem High-End Funktionsumfang von proprietären Lösungen Ihres Netzwerk-Ausstatters kombinieren.

- Open Source Lösungen erhalten deutlich den Vorzug bei den Betreibern, allerdings suchen sie einen kommerziellen Dienstleister für den Support für die Open Source Lösungen.

- Allerdings stellen ebendiese Open Source Lösungen auch die größten Hindernisse für eine Implementierung dar, insbesondere aufgrund von Sicherheits- und Zuverlässigkeits-Bedenken. Die aktuell aufgesetzten Open Source Projekte versuchen, diesen Bedenken entgegenzuwirken.

- Ein weiteres Hindernis (und das ist nun wirklich nicht neu) sind die zu tätigenden Investitionen in neue Hardware und Software.

- Inkonsistente Funktionalität über verschiedene Lösungen hinweg stellen immerhin für 24,5% der Befragten ein wesentliches Hindernis dar.

Beispiele für Hersteller, die bereits jetzt ein SDN Produkt-Portfolio haben oder von denen dies in naher Zukunft zu erwarten ist, sind (Quelle: The 2015 Guide to SDN and NFV, Jim Metzler e.a.; Webtorials)

- Merchant Silicon / Chip Hersteller: Broadcom, Intel, Marvell, Mellanox

- Mega Data Center Betreiber: Yahoo, Google, Facebook

- Server-Virtualisierungs-Hersteller: Citrix, Microsoft, VMware

- Telekom Service Provider: AT&T, Deutsche Telekom, NTT, Pertino, Verizon

- Anbieter für Telekom Service Provider Infrastrukturen: ADVA Optical Networking, Ciena, Cyan, Infinera, ZTE Corporation

- Switch Hersteller: Alcatel-Lucent, Cisco, Dell, Extreme Networks, HP, Meru Networks, NEC, PICA8

- Hersteller von Produkten für Netzwerk- und Service-Monitoring, Management und Automatisierung: EMC, CA, Netscout, QualiSystems

- Netzwerk Servcie Provider: A10, Citrix, Cisco, Embrane, Extreme Networks, HP, NEC, Radware, Riverbed

- Test-Equipment Hersteller, Test-Dienstleister: Qualisystems, InCNTRE, Ixia, Spirent

Beispiele für Hersteller, die bereits jetzt ein NFV Produkt-Portfolio haben oder von denen dies in naher Zukunft zu erwarten ist, sind (Quelle: The 2015 Guide to SDN and NFV, Jim Metzler e.a.; Webtorials)

- Telekom Service Provider: AT&T, CableLabs, France Telecom S. A., Telefonica S.A., NTT

- Merchant Silicon / Chip Hersteller: Broadcom, Freescale Semiconductor, Intel, Marvell

- Hersteller von Netzwerk-Komponenten und elektronischen Komponenten: ADTRAN Europe, Cisco, Ericsson, Huawei Technologies Inc. (UK), IBM Europe, Spidercloud Wireless Inc.

- Hersteller, die virtualisierten Netzwerk Service und Cloud Service Lösungen anbieten: Allot Communications Systems, Mavenir Systems, NetNumber, Virtela Technology Services

- NFVI Provider: 6Wind, BTI Systems, Wind River

- Hersteller für Orchestrierungs-Software: Anuta Networks, Cadzow Communications, CENX

- Hersteller von Produkten für Netzwerk-Monitoring, Management und OSS / BSS: Netscout, Amdocs Software Systems, Comptel Corporation, Comverse Network Systems Europe B.V., EMC, Metra Tech Corp.

- Hypervisor Hersteller: Citrix, Oracle, Virtual Open Systems

- Test-Equipment Hersteller, Test-Dienstleister: EANTC, JDSU Deutschland, QualiSystems, Spirent Communications, Tektronix, Yokogawa Europe

Die Übersichten lassen erkennen, dass die Hersteller-Klassen für SDN und NFV durchaus Ähnlichkeiten aufweisen. Beide Bereiche ergänzen und/oder überschneiden sich ja auch massiv.

Beispiele für Hersteller von SDN / NFV Controllern sind:

- SDN: Big Switch Networks, Cisco, HP, NEC, Netsocket, Nuage, OpenDaylight Consortium, VMware/Nicira

- NFV: Adara Networks, ConteXtream, NEC

Fazit: Schlussfolgerungen

Sind SDN / NFV ein Hype oder sind sie gekommen um zu bleiben? Falls Letzteres zutrifft, welche relevanten Folgerungen ergeben sich insgesamt für den SDN / NFV Markt und Netzwerk Betreiber? Welche Verbreitung haben die Technologien aktuell? Welcher Handlungsbedarf entsteht wann? Welche Bereiche sind die größten Push-Faktoren für SDN / NFV?

SDN

- Der Bekanntheitsgrad des Themas SDN hat sich im letzten Jahr deutlich gesteigert.

- Die Nutzung von SDN in Produktionsnetzen sollte Ende 2015 einen signifikanten Nutzen bringen können.

- Zwei hauptsächliche Hinderungsgründe sind Bedenken, wie sich SDN in die existierende restliche Infrastruktur integrieren lässt und das Fehlen eines zwingenden Business Case.

- IT Organisationen sind hochgradig skeptisch, dass sie Netzwerk-Virtualisierung im Rechenzentrum implementieren können, ohne irgendwo doch noch dedizierte Hardware zu nutzen.

- OpenFlow ist nur bei sehr wenigen Unternehmen zum Einsatz gekommen.

- Viele Unternehmen sind unschlüssig, ob sich das SDN Fabric-Modell oder das Overlay-Modell durchsetzen wird.

- Nur wenige Unternehmen glauben, dass SDN dazu beitragen wird, CAPEX Kosten einzusparen oder die Komplexität zu verringern. (!)

- Der SDN Fokus der nächsten zwei Jahre liegt im Rechenzentrum und im WAN.

- Es gibt einen gewissen Optimismus unter den Netzwerk-Unternehmen, dass SDN sich in den nächsten 3 Jahren besser etablieren wird und sogar Common Sense Status erhalten wird.

NFV

- Die Bekanntheit von NFV hinkt SDN deutlich hinterher.

- Diejenigen, die sich mit NFV beschäftigen, halten es jedoch nicht für eine reine Provider-Technologie, sondern sehen auch Einsatzszenarien im Enterprise Umfeld.

SDN, NFV, OpenFlow und Virtualisierungs-Protokolle - Teil 3

- Der Haupttreiber für Interesse an NFV ist die erhoffte Zeiteinsparung, um neue Dienste auszurollen.

- Die drei Haupthindernisse für NFV sind:
  - Bedenken hinsichtlich der tatsächlichen Ende-zu-Ende Provisionierung
  - das Fehlen eines zwingenden Business Case
  - fehlende Produktreife aktueller Produkte

- Viele IT-Organisationen glauben jedoch, dass NFV in einigen Jahren in relevantem Umfang Einsatz finden wird.

- Zwar gibt es erkennbares Interesse an den ETSI-Standards und Einsatzszenarien, mit großem Abstand wird jedoch NFV Infrastructure as a Service als der interessanteste Fall eingestuft.

- Die meisten IT-Organisationen glauben, dass selbst nach einem erfolgreichen PoC ein immenser Aufwand erforderlich ist, um NFV auf breiter Ebene in der Produktion zu implementieren.

SDN und NFV

- Die meisten Unternehmen halten SDN und NFV für komplementäre Technologien, die "irgendwie" zusammenhängen.

- Die große Mehrheit der Unternehmen hat keine gut durchdachte Strategie, wie die Orchestrierung von SDN und NFV implementiert werden soll.

- SDN und NFV bieten Management Verbesserungen auf der einen, jedoch Sicherheits-Herausforderungen auf der anderen Seite.

- SDN und NFV wird durchaus das Potenzial zugetraut, IT Organisationen zu ermöglichen, ihre Umgebung dynamisch zu ändern, um SLAs gerecht zu werden.

- Applikationen und Dienste müssen Ende-zu-Ende eingerichtet werden (können).

- Physische und virtuelle Umgebungen sollen unabhängig voneinander eingerichtet werden können; dabei sollen Netzwerk-Management Organisationen jedoch die Möglichkeit haben, beide Management-Datasets zu korrelieren und zu konsolidieren, insbesondere soll operationeller Einblick in die Ende-zu-Ende Dienstqualität gegeben sein.

- SDN und NFV sowie die fortschreitende Adoption von software-basierter IT Funktionalität werden die Struktur von IT-Organisationen sowie die IT-Arbeitsplätze nachhaltig verändern.

SDN und NFV sind Technologien, die gekommen sind um zu bleiben. Direkter Handlungsbedarf besteht gegebenenfalls für Evaluierungen und die Erarbeitung einer Strategie, insbesondere im Bereich NAC, Monitoring, zentrale Provisionierung und Orchestrierung.

Noch ist jedoch unsicher, in welchem Umfang, wie schnell und wie dauerhaft einzelne Lösungen sich im Markt etablieren werden.

Industrie-Standards haben bestenfalls den Status einer "Generation eineinhalb bis zwei".

4. Die Welt der Overlay Protokolle für SDN und NFV

Konkrete SDN/NFV-Implementierungen verwenden verschiedenste Overlay Protokolle zur Enkapsulierung des Kontroll- und Datenverkehrs. OpenFlow wurde im Insider bereits ausführlich behandelt, daher verweisen wir an dieser Stelle auf das Insider-Archiv.

Im RZ-Umfeld sind aktuell diverse Ansätze zu finden, teilweise aus konkurrierenden Hersteller-Umgebungen getrieben:

- VXLAN
- IETF NVO3
- VXLAN GPE
- NVGRE
- GENEVE
- LISP
- NSH

4.1 VXLAN: Virtual eXtensible LANs

VXLAN wurde als das VMware Overlay in RZ-Umgebungen bekannt und hat aktuell den größten Marktanteil an Overlay-Verfahren im RZ-Umfeld. Für das Protokoll gibt es einen verabschiedeten IETF Standard (RFC 7348 aus 2014), damit ist es eine Stufe weiter als die anderen Overlay-Verfahren (sieht man einmal von OpenFlow ab).

VXLAN ist ein Protokoll, das die Verbindung von Layer-2 Domänen über eine unterliegende Layer-3 Infrastruktur (Campus Netz; die Vision: Internet, Corporate WAN) hinweg ermöglicht, wodurch es sich für die Migration von VMs, zum Beispiel mit vMotion eignet. Insbesondere gelten die nachfolgenden Verhaltensmerkmale:

- Die Kommunikation ist innerhalb der Layer-2 Domäne transparent möglich

- Verschiedene Layer-2 Domänen können voneinander isoliert werden

- Die IP Kontext kann bei Migration auf einen anderen Host mitgenommen werden

- Georedundanz wird (theoretisch) unterstützt

Die Autoren von VXLAN sind VMware, Red Hat, Citrix, Arista, Brocade und Cisco – und wer fehlt? Tja, Microsoft steht leider auf der anderen Seite. Damit gilt: Wenn Sie VXLAN in Hyper-V Umgebungen einsetzen wollen, haben Sie leider NICHT gewonnen…

Wesentliche Ziele von VXLAN sind die Erhöhung der Skalierbarkeit im Vergleich zur IEEE 802.1Q VLAN Technologie (16 Mio. VXLANs / Layer-2 Domänen) sowie die Vergrößerung der Layer-2 Domänen-Ausdehnung über mehrere Standorte hinweg (geo-redundante RZ's).

Um die Layer-2 domänen-interne und -übergreifende Kommunikation zu gewährleisten, hat VXLAN einige technische Anforderungen:

- Multicast Unterstützung: IGMP, PIM

SDN, NFV, OpenFlow und Virtualisierungs-Protokolle - Teil 3

(SM, DM, BIDIR)
- Layer-3 Routing: OSPF, BGP, IS-IS
- gegebenenfalls entsprechende IPv6-fähige Versionen obiger Protokolle

VXLAN ist ein Tunnel-/Enkapsulierungs-Verfahren (fällt dem Entwickler nichts mehr ein, so muss es halt ein Tunnel sein). So genannte VTEPs (Virtual Tunnel End Points) sorgen als Tunnel-Endpunkte am vSwitch für die host- und RZ-übergreifende Layer-2-interne Verbindung der ansonsten "getrennten" Layer-2 Domänen (siehe Abbildung 4.1). Hierfür hat im Regelfall jeder Hypervisor respektive vSwitch einen VTEP. Die VMs sind über den vSwitch an Tunnelendpunkt (VTEP) angekoppelt, jede Layer-2 Domäne erhält einen eindeutigen 24-Bit VNI (Virtual Network Identifier) als Identifikator, der den ursprünglichen 12-Bit VLAN-Tag von 4094 auf 16 Millionen Möglichkeiten vergrößert.

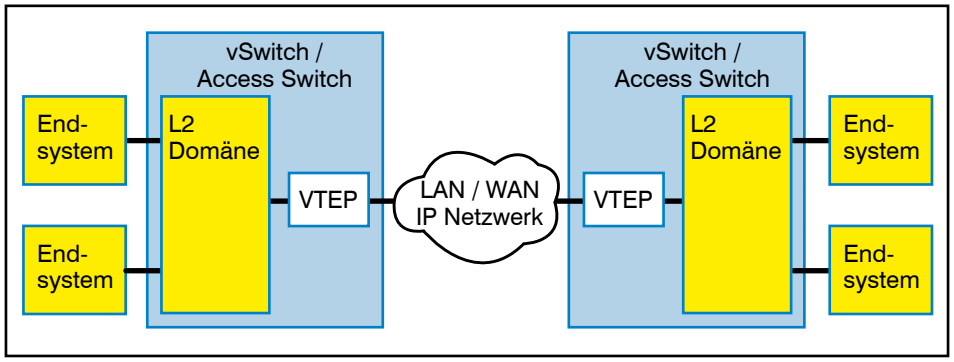


Abbildung 4.1: VXLAN Architektur-Übersicht

VMs in derselben Layer-2 Domäne, d.h. solche, die demselben VNI zugeordnet sind, können über den VTEP miteinander kommunizieren. Da ein VTEP mehrere VNIs bedienen kann und im Regelfall wird, ist der VNI als Unterscheidungs-Tag erforderlich: Er wird in den VXLAN-Header eingetragen, um als eindeutige Kennung über die VTEP Tunnel netzwerkweit Konnektivität zwischen den ihm zugeordneten VMs zu ermöglichen. Für unterschiedliche VNIs können überlappende IP-Adressen verwendet werden, die Eindeutigkeit wird durch VNI + VTEP-IP Adresse hergestellt. Auf diese Weise ist ein Mandantenkonzept denkbar, in dem ein einzelner Mandant intern überlappende IP-Adressen und VLAN-Tags nutzen kann, die auch von anderen Mandanten genutzt werden. Somit müssen VLANs und IP-Adressen nur noch innerhalb eines vSwitches eindeutig sein. Was jedoch dazu führt, dass die VLAN-Zuordnung und IP-Adresse einer VM nichts mehr darüber aussagt, ob diese mit einer anderen VM kommunizieren kann, die demselben VLAN zugeordnet ist!

Abbildung 4.2 zeigt Hosts aus den zwei verschiedenen Layer-2 Domänen 128.0.100/16 (grün) und 192.0.100/24 (gelb). Eine Verbindungs-Funktionalität ist a priori nur innerhalb der gelben und innerhalb der grünen VMs gegeben. Will VM2 mit VM3 oder VM8 kommunizieren, so benötigt sie hierfür die zuvor beschriebene Routing Instanz (Default Router).

Die Enkapsulierung erfolgt über Ethernet bzw. beliebiges MAC-Protokoll, IP, UDP mit der well-known Portnummer 0x4789 und dem VXLAN Header, an den sich dann die "innere Payload" beginnend mit einem weiteren MAC-Header anschließt. Die FCS wird (wie bei allen anderen vergleichbaren Protokollen auch) jedoch nur einmal berechnet, nämlich über das gesamte Frame. Insgesamt ist der zusätzliche Paket-Overhead bei VXLAN 50 Byte (bei Ethernet Nutzung) bzw. inklusive äußerem VLAN Header 54 Byte lang (siehe Abbildung 4.3). Eine Übersicht des eigentlichen, 8 Byte langen VXLAN-Headers zeigt Abbildung 4.4. Hierbei wird das I-Flag für valide VNIs auf I=1 gesetzt; der UDP Source Port nutzt das Intervall 49152

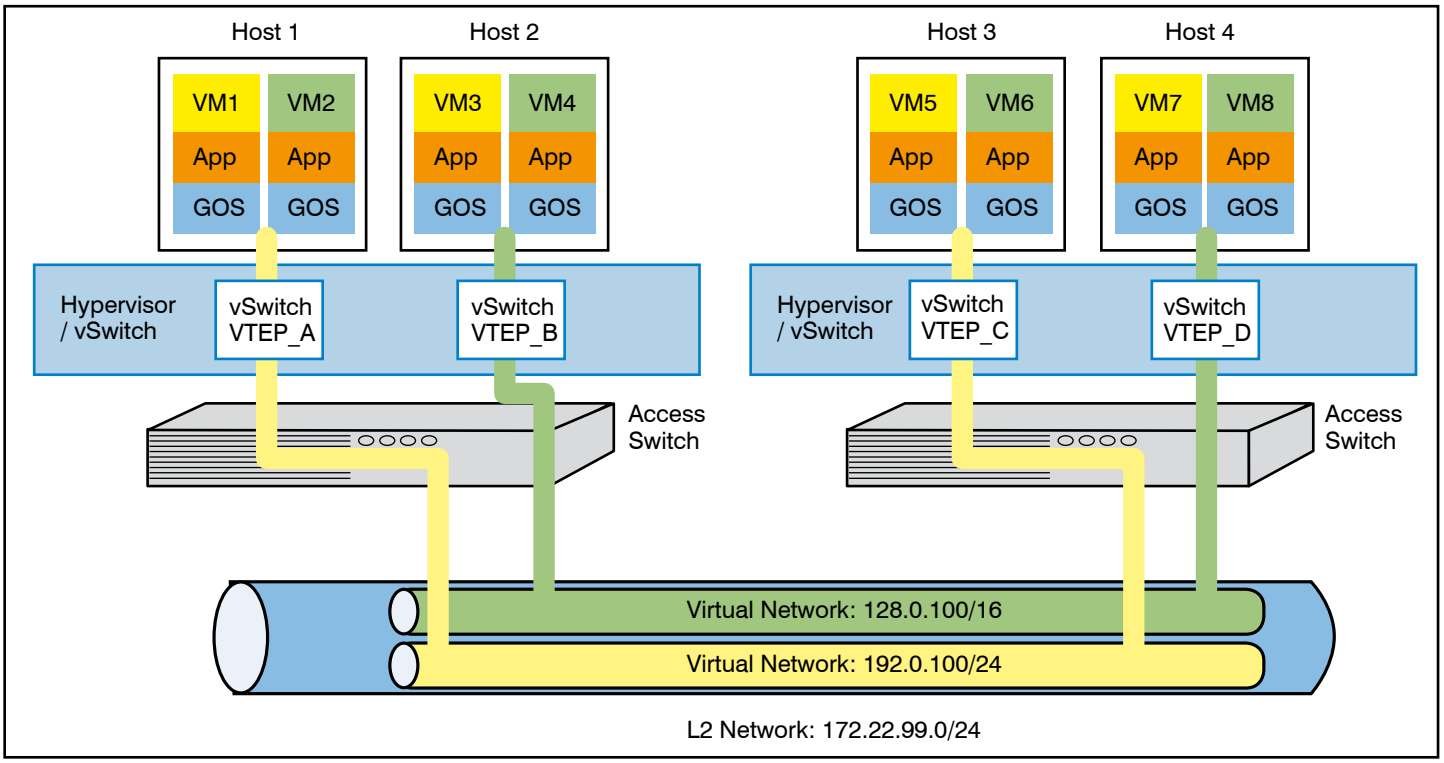


Abbildung 4.2: VXLAN Übersicht: Trennung von Layer-2 Domänen

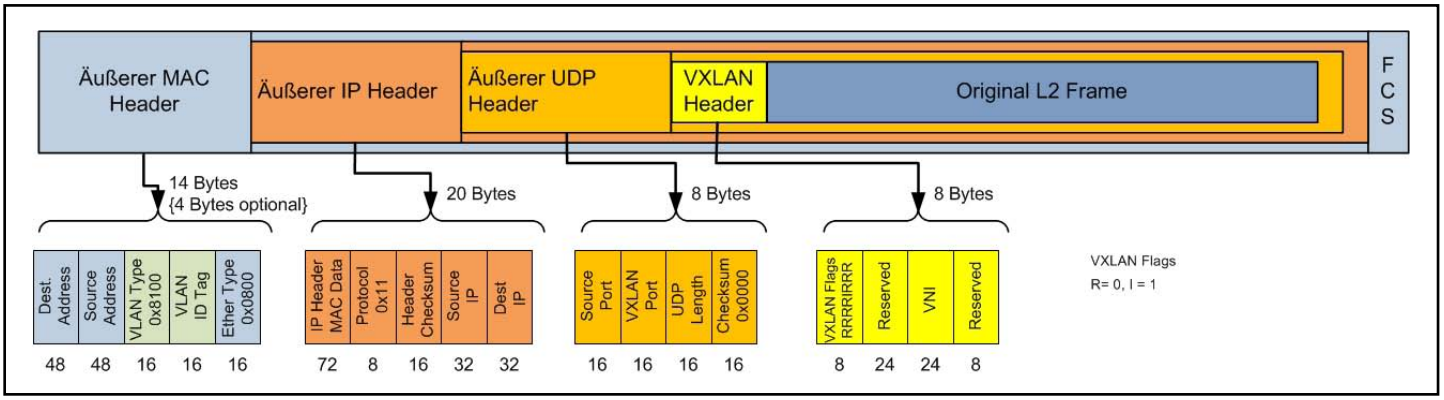


Abbildung 4.3: Gesamtheader der VXLAN Enkapsulierung

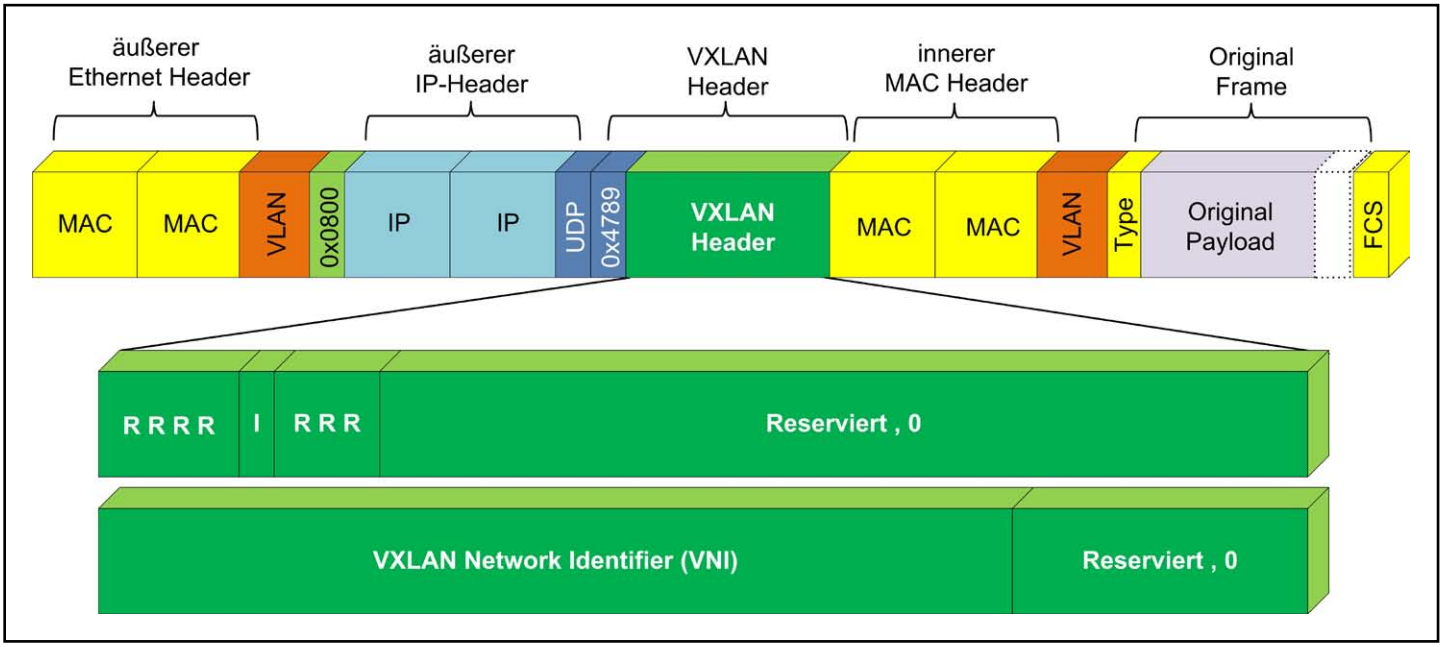


Abbildung 4.4: VXLAN Header der VXLAN Enkapsulierung

– 65535, wobei die konkrete Portnummer mittels 5-Tupel Hash (MAC-Dest, MAC-Src, IP-Dest, IP-Src, Portnummer) über die Header des inneren Ethernet Frames berechnet wird. Lastverteilung über parallele Wege kann mittels OSPF ECMP erfolgen, wobei die Flow-basierte Verteilung mittels Hash über den UDP Source Port (d.h. Hash über den 5-Tupel) erfolgen kann. Für zukünftige Erweiterungen sind eine Reihe reservierte Bits vorgesehen.

Cisco nutzt beispielsweise einige dieser Bits aktuell in seiner ACI Architektur (genauer gesagt VXLAN GPE, das weiter unten beschrieben wird), um Monitoring Werte zu übertragen, aus denen dann die Network Health Parameter berechnet werden können.

Der Virtuelle Tunnel Endpunkt (VTEP) baut Mapping Tabellen auf, die für jede VM die jeweilige MAC-Adresse der VM, die zugehörige VNI-Kennung, zugehörige IP MC-Gruppe und den zugehörigen (am anderen Ende liegenden) VTEP enthalten. In der Praxis heißt das: Es ist ein Management-Tool für die Verwaltung der Mapping Tabellen erforderlich! Ein Datenpaket (Ethernet Payload) wird dann am "Ingress" VTEP enkapsuliert und mittels IP-Adresse an den "Egress" VTEP adressiert.

An dieser Stelle taucht die Frage auf: Was passiert mit BUM-Traffic (Broadcast, Unknown, Multicast)? Sofern eine Ziel-Adresse nicht in der Mapping Tabelle gefunden wird oder ein Broadcast/Multicast anliegt, muss innerhalb der Layer-2 Domäne geflutet werden, das typische Beispiel ist der ARP-Request. Da VXLAN Pakete über eine IP-geroutete Infrastruktur übertragen werden, lässt sich hier kein MAC-Broadcast oder -Multicast verwenden. Daher ist das Fluten über IP Multicast realisiert: Jedem VNI wird eine IP Multicast-Adresse zugeordnet, im Netzwerk muss zur Freude (oder auch nicht) des Betreibers Multicast Routing implementiert werden, üblicherweise PIM SM oder auch PIM BIDIR (beispielsweise bei Cisco). Die Zuordnung mehrerer VNI zur selben MC-Adresse wäre auch möglich, bedeutet aber erhöhten Flutungs-Overhead und weniger Lasteffizienz. Eine Übersicht zum Multicast-Transport zeigt Abbildung 4.5.

Wie kommt man aus der VXLAN-Welt in die "normale" oder eine andere Welt? VTEPs können zusätzlich zum Forwarding eine Gateway-Funktion zur Verbindung von VXLAN Teilnetzen mit VLAN Teilnetzen implementieren.

Soll eine Layer-2 übergreifende Kommunikation stattfinden, muss der Weg wie allgemein üblich über eine Routing Instanz laufen – die VM spricht hierfür wie gehabt ihren Default Router an, ein Beispiel zeigt Abbildung 4.6.

Problem ist nun, dass beim Wandern ei-

ner VM in einen anderen Standort der Default Router nicht mitwandert, die VM jedoch weiterhin genau diesen bisherigen Default Router anspricht. Hierdurch entstehen so genannte Routing Trombones, wie in Abbildung 4.7 dargestellt ist. Was die tatsächliche Eignung von VXLAN für georedundante Netzwerk-Designs deutlich in Frage stellt – besser gesagt zu der Feststellung führen muss, dass diese Eignung zwar auf der Liste der VXLAN-Ziele steht, de facto jedoch nicht gegeben ist (Dies ist bei vergleichbaren Protokollen wie NVGRE ebenfalls so!).

Abschließend ist eine Bewertung von VXLAN in Tabelle 4.1 zusammengefasst.

4.2 VXLAN GPE: Generic Protocol Extension for VXLAN

VXLAN GPE (IETF Draft04, Feb. 2015) wird in der IETF-Arbeitsgruppe NVO3 als VXLAN-Erweiterung spezifiziert. Autoren sind Broadcom, Cisco, Huawei, Intel, Marvell und Microsoft (!). Letzteres kann zu der Vermutung führen, dass Microsoft seinen Kleinkrieg gegen VXLAN aufgibt und sich von NVGRE weg dieser erweiterten VXLAN-Variante zuwenden könnte.

VXLAN GPE ist eine Konkretisierung und Erweiterung von VXLAN für spezielle Einsatzszenarien, insbesondere auch Service Chaining und OAM. Diese Erweiterung ist keine Header-Erweiterung, sondern nutzt einige reservierte Bits des bestehenden VXLAN Headers. Den erweitert genutzten VXLAN-Header von VXLaN GPE zeigt Abbildung 4.8. Im ersten Byte wurden eine Version (Ver = 00) sowie zwei neue Bitflags eingefügt, P=1 für das spezifizierte Next Protocol und O für OAM (O=1 für OAM-Paket, O=0 für Datenpaket).

Ist P=1, wird der Wert für das nachfolgende Protokoll in Byte 3 eingetragen, aktuell spezifiziert sind

- 0x01 = IPv4
- 0x02 = IPv6
- 0x03 = Ethernet
- 0x04 = NSH

Die Bewertung von VXLAN GPE ist in Tabelle 4.2 zusammengefasst.

4.3 NVGRE: Network Virtualization using Generic Routing Encapsulation

NVGRE ist das Microsoft "Konkurrenz-Protokoll" zu VXLAN und wird von Microsoft spezifiziert (IETF Draft08, Mai 2015). Zwar gibt es eine Reihe weiterer Netzwerk- und Peripherie-Hersteller, die NVGRE ebenfalls unterstützen, jedoch ist es ziemlich weit weg von einem de facto Standard.

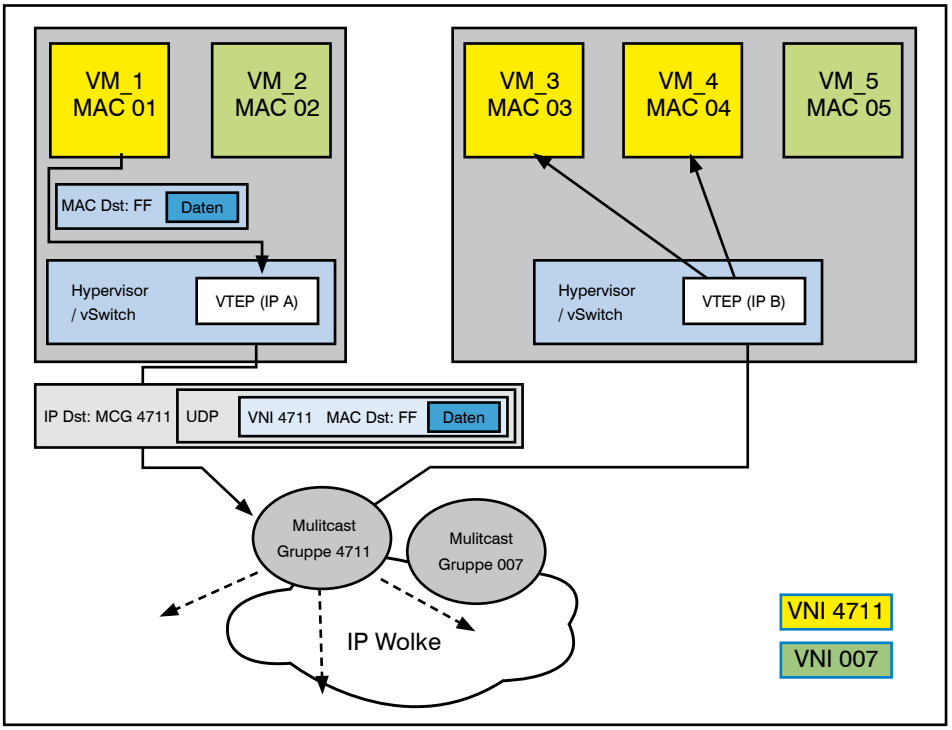


Abbildung 4.5: Fluten des BUM-Verkehrs mittels IP-Multicast

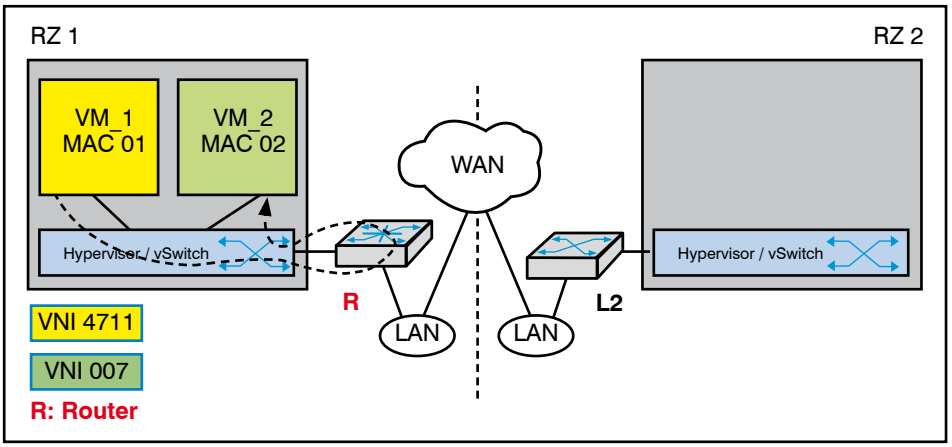


Abbildung 4.6: Geroutete Verbindung bei VXLAN

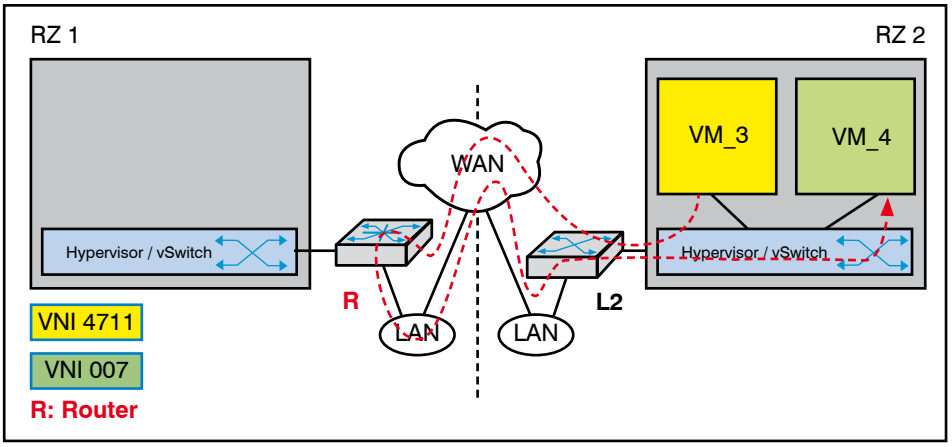


Abbildung 4.7: Routing Trombone bei VXLAN

SDN, NFV, OpenFlow und Virtualisierungs-Protokolle - Teil 3

Funktion, Skalierbarkeit	VXLAN	
Skalierung: Anzahl virtueller Netze	24 Bit VNI = 16 Mio.: limitiert durch PIM Multicast Skalierung	☺
Netzwerk Reichweite (Durchmesser)	Reichweite von PIM Multicast Gruppen (WAN; Internet ?)	☹
Einsatzbereich	DC	☹
Trennung RZ-Netz / Anwendungs-Ebene	Host	☹
Spezifikation der Control Plane	Nein	☹
Zusatzkomponenten	Nein	☺
Unterstützung dynamischer VM-Migration	Begrenzt	😐
Mandantenfähigkeit	Ja	☺
Enkapsulierung	IP / UDP / VXLAN Header	😐
Multicast Anforderungen	PIM (SM, DM, oder BIDIR); Anzahl unterstützter MC Gruppen definiert Anzahl virtueller Netze	☹
Routing Unterstützung	Jeder Router oder L3-Switch, der mit VMware vShield, vEdge zusammen arbeitet, jedes VTEP-fähige Gateway	☹
Routing Unterstützung im Tunnelendpunkt	Nicht gefordert	☹
optimiertes Routing im Transportnetz	Ja	☺
Multipath / Lastverteilung im Transportnetz	OSPF ECMP, Hash für UDP Source Port ("innere Eth Header", z.B. MAC, IP, Port-Nr), Intervall = 49152-65535	☺
TE im Transportnetz	Nein	☹
QoS-Unterstützung	nur in den inneren Headern	☹
MAC Adresstabelle	Anzahl der **VTEP** MAC Adressen ist an die Switch MAC Tabellengröße gebunden	☺
Hardware Parsing	Ja, 5-Tupel (IP-S / IP-D / L4-P / L4-S / L4-D), jedoch ohne VXLAN Header	😐
Standardisierung	RFC 7348, Informational	☺
Hersteller-Unterstützung (Autoren)	Arista, Broadcom, Cisco, Citrix, Cumulus, RedHat, VMware	😐
Produktkategorien	Layer-2/3 Switch, vSwitch, Router, Appliance, Tester, NIC, Orchestrator	
Produktstatus	Verbreitet	☺
		-1

Tabelle 4.1: Bewertung von VXLAN

NVGRE ist das Overlay-Protokoll, das in Hyper-V Umgebungen genutzt werden muss, da VXLAN aus naheliegenden Gründen derzeit nicht unterstützt wird (zählt VMware doch zu den Erzfeinden von Microsoft).

NVGRE ermöglicht, wie VXLAN auch, die Verbindung von Layer-2 Domänen über eine unterliegende geroutete Layer-3 Infrastruktur (Internet, Corporate WAN) hinweg. VM Migration wird daher mit den gleichen Zielen unterstützt wie bei VXLAN:

- Die Kommunikation innerhalb der Layer-2 Domäne ist transparent
- Der IP Kontext kann bei Migration auf einen anderen Host mitgenommen werden
- Georedundanz wird theoretisch unterstützt
- Einsatzbereich sind alle Hyper-V Umgebungen

Auch hier geht es um eine Erhöhung der Skalierbarkeit mittels 24-Bit Identifikator VSID (Virtuelle Subnetz ID; 16 Mio. Layer-2 Domänen) und Vergrößerung der Ausdehnung (georedundante RZs). Die Enkapsulierung erfolgt anstatt über IP/UDP über IP mit Next Protocol = 0x2F sowie daran anschließend einen GRE-Header. Einen inneren VLAN-Header gibt es nicht (siehe Abbildung 4.9). Da die Enkapsulierung nicht den 5-Tupel (MAC-Dst/Src, IP-Dst/Src, Portnummer) nutzt, muss die Hardware wiederum für NVGRE ertüchtigt werden, was im Einzelfall für entsprechende Netzkomponenten nachzuprüfen ist.

Da die Protokolle VXLAN und NVGRE "im Wesentlichen" gleichartig arbeiten und lediglich eine unterschiedliche Enkapsulierung nutzen, sind auch die Voraussetzungen gleich, die NVGRE erfordert:

- Multicast Unterstützung: IGMP, PIM (SM, DM, BIDIR)
- Layer-3 Routing: OSPF, BGP, IS-IS
- ggf. entsprechende IPv6-fähige Versionen obiger Protokolle (aktuell für NVGRE nicht definiert)

Die Bewertung von NVGRE ist in Tabelle 4.3 zusammengefasst.

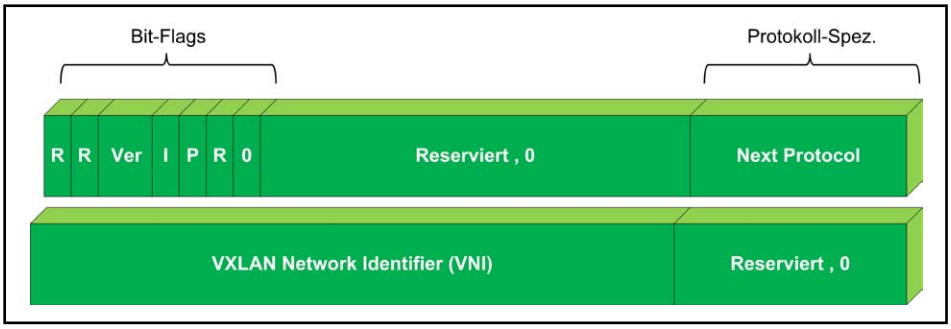


Abbildung 4.8: VXLAN Headernutzung bei VXLAN GPE

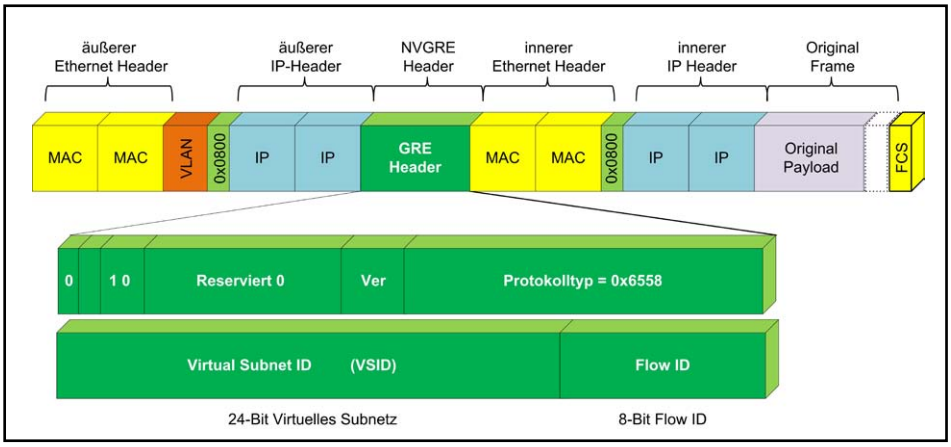


Abbildung 4.9: NVGRE Header

4.4 NVO3: Network Virtualization Overlays over Layer-3

Auch die IETF hat erkannt, dass Overlay Verfahren zur besseren Skalierung und "Loslösung der IP-Adresse vom konkreten Standort" ein relevantes Thema sind, welches nach Standardisierung verlangt. Die NVO3 Arbeitsgruppe hat sich im Mai 2012 konstitutioniert und erst einmal Dokumente zu Problem Statement (RFC 7364), Framework (RFC 7365), Sicherheits-Anforderunge, Multicast, Data Plane und Use Case produziert. Sie befasst sich mit allen Problemen und Anforderungen an mandantenfähige virtuelle Netzwerk-Infrastrukturen im Rechenzentrum. Insbesondere geht es um:

- Isolierung der Verkehrsströme virtueller Netze gegeneinander
- Wahl von MAC und IP Adressen unabhängig vom Standort und von anderen Netzen
- Positionierung und Migration von VMs unabhängig vom physischen Netzwerk
- Zu lösende Fragen sind fokussiert auf:
  - optimales IP-Routing, optimaler Default Router
  - Konflikte bei der VLAN-ID
  - maximale MTU Size

Die technologischen Elemente zur Lösung des Themas sind – wie zu erwarten – ähnlich wie bei den existierenden Overlay-Verfahren:

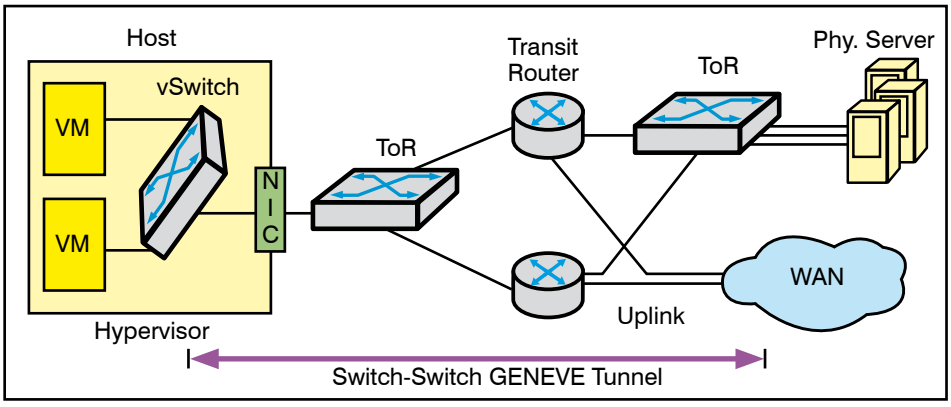


Abbildung 4.10: GENEVE Tunnel-Konzept

- Trennung der IP/MAC-Adresse von der Netzwerk-Physik
- Mapping am ersten Hop
- Enkapsulierung am Netzwerk Ingress
- Forwarding: bekanntes und robustes Routing
- Dekapsulierung am Netzwerk Egress

Die NVO3 Arbeitsgruppe hat einige Overlay-Drafts unter ihre Fittiche genommen, um sie zu "neutralisieren": GENEVE, VXLAN GPE und Generic UDP Encapsulation werden jetzt unter NVO3 weiterverfolgt. NVGRE ist bei NVO3 bisher nicht zu finden.

4.5 GENEVE: Generic Network Virtualization Encapsulation

GENEVE ist ein Konsensversuch, um VXLAN und NVGRE zusammenzuführen (Draft02, Okt. 2014; migriert in die IETF NVO3 WG zum Draft00, Mai 2015), damit über ein neutrales drittes Protokoll der Streit zwischen VXLAN und NVGRE endlich aufhören möge. Motiviert ist dieser Ansatz sicherlich auch durch Chip-Hersteller wie Broadcom, die keine Lust mehr haben, mehr und mehr Overlay-Protokolle in Hardware zu gießen und sich stattdessen lieber darauf beschränken möchten, ein gemeinsames Trägerprotokoll zu verdrahten. Zu den Herstellern, die Autoren oder Unterstützer sind, gehören Arista, Broadcom, Brocade, Cumulus Intel, Microsoft, RedHat und Vmware.

GENEVE versteht Netzwerk-Virtualisierung als Verbindungs-Infrastruktur für ein integriertes System, z.B. mit Vmware, Microsoft, Cisco und/oder KVM Virtualisierung. Tunnel-Endpunkte können flexibel vSwitches, phySwitches, Middleboxen, Appliances und Applikationen sein (siehe Abbildung 4.10).

Darüber hinaus sahen die GENEVE Bäcker den Bedarf für Metadaten-Übertragung und haben deshalb den Header flexibel, d.h. mit einer variablen Länge spezifiziert (was netterweise die vollständige Implementierung in Hardware verunmöglicht). Entsprechende Header-Optionen soll die IANA allgemein festlegen. Metadaten bei GENEVE sind:

- Input Port
- Sicherheits-Policy
- Service-basierter Kontext

Die Enkapsulierung erfolgt über Ethernet, IP (Next Prot. = 0x17) und UDP (Dest. Port = 0x6081) mit dem bemerkenswerten Portrange = 0 .. 65535 (!), wobei die MAC-Schicht nicht auf Ethernet festgelegt ist. Eine Header-Übersicht zeigt Abbildung 4.11. Auch hier finden wir den

Funktion, Skalierbarkeit	VXLAN GPE	
Skalierung: Anzahl virtueller Netze	16 Mio.: limitiert durch PIM Multicast Skalierung	☺
Netzwerk Reichweite (Durchmesser)	Reichweite von PIM MulticastGruppen (WAN; Internet ?)	☹
Einsatzbereich	DC	☹
Trennung RZ-Netz / Anwendungs-Ebene	Host	☹
Spezifikation der Control Plane	Nein	☹
Zusatzkomponenten	Nein	☺
Unterstützung dynamischer VM-Migration	Begrenzt	😐
Mandantenfähigkeit	Ja	☺
Enkapsulierung	IP / UDP / VXLAN Header	😐
Multicast Anforderungen	PIM (SM, DM, oder BIDIR); Anzahl unterstützter MC Gruppen definiert Anzahl virtueller Netze	☹
Routing Unterstützung	Jeder Router oder L3-Switch, der mit VMware vShield, vEdge zusammen arbeitet, jedes VSID-fähige Gateway	☹
Routing Unterstützung im Tunnelendpunkt	Nicht gefordert	☹
optimiertes Routing im Transportnetz	Ja	☺
Multipath / Lastverteilung im Transportnetz	OSPF ECMP, Hash für UDP Source Port (MAC, IP, Port-Nr)	☺
TE im Transportnetz	Nein	☹
QoS-Unterstützung	nur in den inneren Headern	☹
MAC Adresstabelle	Anzahl der **VTEP** MAC Adressen ist an die Switch MAC Tabellengröße gebunden	☺
Hardware Parsing	Ja, 5-Tupel (IP-S / IP-D / L4-P / L4-S / L4-D), jedoch ohne VXLAN Header	😐
Standardisierung	IETF Draft	😐
Hersteller-Unterstützung (Autoren)	Broadcom, **Cisco**, Huawei, Intel, Marvell, Microsoft	😐
Produktkategorien	Layer-2/3 Switch, vSwitch, Router, Appliance, Tester, NIC, Orchestrator	
Produktstatus	Eingeschränkt	☹
		-4

Tabelle 4.2: Bewertung von VXLAN GPE

schon bekannten 24-Bit Identifikator sowie zwei Flags O und C für OAM und Critical Options. Die eingetragene Länge gibt die Anzahl 4-Byte Worte ohne die fixen 8 Byte Tunnel an. Im Gegensatz zu NVGRE ist GENEVE für IPv4 und IPv6 definiert. Lastverteilung erfolgt über OSPF ECMP, hierfür kann der UDP Source Port mittels 5-Tupel Hash berechnet werden.

Eine Vorab-Bewertung, da GENEVE noch nicht wirklich als "fertig" zu bezeichnen ist, zeigt Tabelle 4.4.

Im nächsten Teil lesen Sie:
- LISP
- Service Chaining: NSH
- Fazit zu Overlay Protokollen

Abkürzungen, Links, Literatur

ACI	Application Centric Infrastructure (Cisco)
API	Application Programming Interface
AR	Access Router
ARP	Address Resolution Protocol
ASIC	Application Specific Integrated Circuit
BGP	Border Gateway Protocol
BUM	Broadcast, Unnown, Multicast
CAPEX	Capital Expenditure
CDN	Content Delivery Network
vCDN	virtual CDN
COTS	Commercial-Off-The-Shelf
CPU	Central Processing Unit
CPE	Customer Premises Equipment
CSP	Cloud Service Provider
DC	Data Center
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
DSL	Digital Subscriber Line
ECMP	Equal Cost Multipath
E-CPE	Enterprise Customer Premises Equipment
ETSI	European Telecommunications Standards Institute
FCS	Frame Check Sequence
FW	Firewall
GENEVE	Generic Network Virtualization Encapsulation
GRE	Generic Routing Encapsulation
aaS	Infrastructure as a Service
IANA	Internet Assigned Numbers Au-

SDN, NFV, OpenFlow und Virtualisierungs-Protokolle - Teil 3

Funktion, Skalierbarkeit	NVGRE	
Skalierung: Anzahl virtueller Netze	24 Bit VSID = 16 Mio.: limitiert durch PIM Multicast Skalierung	☺
Netzwerk Reichweite (Durchmesser)	Reichweite von PIM Multicast Gruppen (WAN; Internet ?)	☹
Einsatzbereich	DC	☹
Trennung RZ-Netz / Anwendungs-Ebene	Host	☹
Spezifikation der Control Plane	Nein	☹
Zusatzkomponenten	Nein	☺
Unterstützung dynamischer VM-Migration	Begrenzt	😐
Mandantenfähigkeit	Ja	☺
Enkapsulierung	IP / GRE Header; vielfach kein HW-Parsing	☹
Multicast Anforderungen	PIM (SM, DM, oder BIDIR); Anzahl unterstützter MC Gruppen definiert Anzahl virtueller Netze	☹
Routing Unterstützung	Jeder Router oder L3-Switch, der mit VMware vShield, vEdge zusammenarbeitet, jedes VSID-fähige Gateway	☹
Routing Unterstützung im Tunnelendpunkt	Ja	☺
optimiertes Routing im Transportnetz	Ja	☺
Multipath / Lastverteilung im Transportnetz	theoretisch ja, wenn Router Flow ID ausliest	😐
TE im Transportnetz	theoretisch: Flow ID für TE	😐
QoS-Unterstützung	Flow ID	☺
MAC Adresstabelle	Anzahl der **Tunnel** MAC Adressen ist an die Switch MAC Tabellengröße gebunden	☺
Hardware Parsing	Switches und Router müssen GRE in Hardware unterstützen	😐
Standardisierung	IETF Draft	😐
Hersteller-Unterstützung (Autoren)	Arista, Broadcom, Emulex, Google, Intel, HP, **Microsoft**	😐
Produktkategorien	Layer-2/3 Switch, vSwitch, Router, Appliance, NIC, Orchestrator	
Produktstatus	Eingeschränkt	☹
		-1

Tabelle 4.3: Bewertung von NVGRE

	thority
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPS	Intrusion Prevention System
IS-IS	Intermediate System - Intermediate System
ISP	Internet Service Provider
IT	Informations-Technologie
ITU-T	International Telecommunications Union for Telecommunication Standards
KVM	Kernel-based Virtual Machine
LAN	Local Area Network
LB	Load Balancer
LISP	Locator / ID Separation Protocol
MAC	Media Access Control
MC	Multicast
MD	Metadaten
MTU	Maximum Transmission Unit
NAC	Network Access Control
NETCONF	Network Configuration
NFV	Network Function Virtualisation
NFVI	Network Function Virtualisation Infrastructure
NFVIaaS	NFVI as a Service
NG-FW	NextGen Firewall
NIC	Network Interface Card / Coupler
NIST	National Institute of Standards and Technology
NSH	Network Services Header
NVGRE	Network Virtualization using Generic Routing Encapsulation
NVO3	Network Virtualization Overlays over Layer-3
OAM	Operation, Administration and Maintenance
OSPF	Open Shortest Path First
PC	Personal Computer
PCRF	Policy and Charging Rules Function
PE	Provider Edge
PIM	Protocol Independent Multicast
PIM BIDIR	Bidirectional PIM
PIM DM	PIM Dense Mode
PIM SM	PIM Sparse Mode
PoC	Proof of Concept
PoD	Point of Delivery
PoP	Point of Presence

Funktion, Skalierbarkeit	NVGRE	
Skalierung: Anzahl virtueller Netze	24 Bit VNI = 16 Mio.; unlimitiert durch variable Optionen	☺
Netzwerk Reichweite (Durchmesser)	abhängig von MC-Nutzung	😐
Einsatzbereich	DC	☹
Trennung RZ-Netz / Anwendungs-Ebene	Host oder Middlebox oder Access Switch	😐
Spezifikation der Control Plane	Nein	☹
Zusatzkomponenten	Nein	☺
Unterstützung dynamischer VM-Migration	Begrenzt	😐
Mandantenfähigkeit	Ja	☺
Enkapsulierung	IP / UDP / GENEVE Header	😐
Multicast Anforderungen	PIM (SM, DM, oder BIDIR); Anzahl unterstützter MC Gruppen definiert Anzahl virtueller Netze	☹
Routing Unterstützung	nicht vorgegeben	😐
Routing Unterstützung im Tunnelendpunkt	Nicht gefordert	☹
optimiertes Routing im Transportnetz	Ja	☺
Multipath / Lastverteilung im Transportnetz	OSPF ECMP, Hash für UDP Source Port (MAC, IP, Port-Nr empfohlen), Intervall = 0 - 65535 (!)	😐
TE im Transportnetz	abhängig von Underlay und Control Plane	😐
QoS-Unterstützung	abhängig von gewählter Transport Enkapsulierung (VXLAN, GRE, NVGRE, IP …	😐
MAC Adresstabelle	Anzahl der **Tunnelendpunkt** MAC Adressen ist an die Switch MAC Tabellengröße gebunden	☺
Hardware Parsing	Ja, jedoch ohne variable Optionen und ohne Geneve Header	😐
Standardisierung	IETF Draft	😐
Hersteller-Unterstützung (Autoren)	Arista, **Broadcom**, Brocade, Cumulus, Intel, Microsoft, RedHat, Vmware	😐
Produktkategorien	Layer-2/3 Switch, vSwitch, Router, Appliance, NIC, Orchestrator	
Produktstatus	Eingeschränkt	☹
		0

Tabelle 4.4: Bewertung von GENEVE

PYANG	in Python geschriebenes YANG
QoS	Quality of Service
RFC	Request For Comment
RZ	Rechenzentrum
SLA	Service Level Agreement
SPBM	Shortest Path Bridging MAC
SDN	Software-Defined Networking
ToR	Top of Rack
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VM	Virtual Machine
VNF	Virtualized Network Function
VNFaaS	VNF as a Service
VNI	Virtual Network Identifier
VSID	Virtuelle Subnetz ID
VTEP	Virtual Tunnel End Point
VXLAN	Virtual eXtensible LANs
VXLAN	GPE Generic Protocol Extension for VXLAN

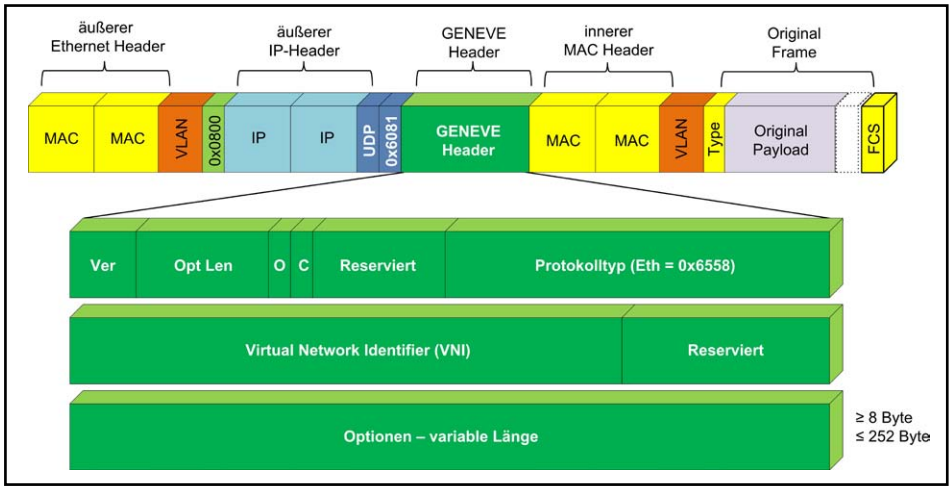


Abbildung 4.11: GENEVE Header

SDN, NFV, OpenFlow und Virtualisierungs-Protokolle - Teil 3

WAN	Wide Area Network
WG	Working Group
WOC	WAN optimization Controller
YANG	Yet Another Next Generation

Links

https://tools.ietf.org/wg/nvo3/
http://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-733127.html

Literatur

- The 2015 Guide to SDN and NFV, Jim Metzler e.a.; Webtorials
- Encapsulation Techniques: Generic Network Virtualization Encapsulation, VXLAN Generic Protocol Extension, and Network Service Header; Cisco White Paper; 10/2014

Lesen Sie auch folgende Artikel aus dem Netzwerk Insider zum Thema:

Ausgabe Oktober 2012: "Werden SDN und OpenFlow herkömmliche Netzwerke verdrängen?" von Petra Borowka-Gatzweiler

Ausgabe März 2015: " SDN, NFV, OpenFlow und Virtualisierungs-Protokolle – Zusammenhänge, Perspektiven, Marktrelevanz (Teil 1)" von Petra Borowka-Gatzweiler

Ausgabe April 2015: " SDN, NFV, OpenFlow und Virtualisierungs-Protokolle – Zusammenhänge, Perspektiven, Marktrelevanz (Teil 2)" von Petra Borowka-Gatzweiler

Außerdem finden Sie einen Online-Beitrag auf unserem Wissensportal von Herrn Höchel-Winter " VXLAN (Virtual eXtensible LAN) – VMwares neuster Draft" vom September 2011 (**http://www.comconsult-research.de/vxlan-virtual-extensible-lan-vmwares-neuster-draft/**)

Standpunkt

Herrschaft der Maschinen

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.

In der 4. Industriellen Revolution (Industrie 4.0), die wir aktuell erleben, entstehen „Cyber-Physische (Produktions-)Systeme, also Systeme aus miteinander vernetzten Geräten, Maschinen und beweglichen Gegenständen, die mittels IT und kontinuierlichem Datenaustausch – zum Beispiel über das Internet – gesteuert werden“ . Roboter werden dabei auch ihren Käfig verlassen und unmittelbar an der Seite des Menschen ihre Arbeit verrichten. Nebenbei, das Design dieser Maschinen wird so sein, dass wir – zumindest psychologisch – keine Angst haben müssen, erschlagen zu werden. Weiterhin werden autonome Fahrzeuge als Schwarmintelligenz unsere Probleme in der produktionsnahen Logistik lösen. Außerdem werden die Nutzungsmöglichkeiten von Cloud Computing in der Industrie sehr genau betrachtet. Hier geht es nicht nur um Virtualisierungstechniken in der Fertigung, sondern auch um die Verlagerung der Intelligenz für Fertigungsprozesse in eine Cloud. Hinzu kommt die Verwendung von Big Data zur Optimierung von industriellen Prozessen.

Mit geschlossenen Systemen wäre die 4. Industrielle Revolution nicht möglich. Es ist klar, dass das entscheidende Kernelement in der Industrie 4.0 die Vernetzung über IP und insbesondere über das Internet (Internet of Things, IoT) ist.

Die Offenheit durch Vernetzung (insbesondere im IoT) hat ihren Preis. Jedes System, das Kommunikationsschnittstellen hat, ist über diese Schnittstellen nun mal grundsätzlich angreifbar, wenn durch Schwachstellen oder andere Sicherheitsmängel ein missbräuchlicher Zugriff möglich ist. Da Software nur mit erheblichstem Aufwand fehlerfrei entwickelt werden kann, sich diverse Softwarefehler als Schwachstellen erweisen, die für Angriffe genutzt werden können, ist dies ein systemimmanentes Risiko für alle vernetzten Systeme. Das ist nichts Neues und in der traditionellen IT haben wir uns längst daran gewöhnt, exponierte und kritische Systeme besonders abzusichern. Dies beinhaltet Härtungsmaßnahmen (z.B. Einsatz eines Virenschutzes, Schutz von Schnittstellen durch Kommunikationskontrolle, Authentisierung und Verschlüsselung), die sys-

tematische Erfassung von Schwachstellen von Systemen (inklusive Penetration Testing) und möglichst deren Beseitigung (ggf. nur Risikoreduzierung) z.B. durch Patches.

Spätestens seit 2010 wissen wir dank Stuxnet um das Potential von zielgerichteten Angriffen und zugehöriger Schadsoftware gegen Steuerungen und anderer vernetzte Systeme in der Automatisierungs-, Prozessleittechnik und allgemein in der Industrie.

Nun könnte man denken, die Hersteller von Systemen hätten hieraus gelernt. Das scheint zumindest nicht überall der Fall zu sein. Wie SPIEGEL ONLINE im Mai berichtete, warnt die Pilotenvereinigung Cockpit vor der Gefahr, „dass Hacker in die Steuerungscomputer von Passagierflugzeugen eindringen und die Maschine zum Absturz bringen könnten“. Ein IT-Spezialist hatte auf Einfallstore in modernen Flugzeugen hingewiesen und exemplarisch demonstriert, wie sich diese Schwachstellen ausnutzen lassen.

Dass erst ein offensichtlich nicht von den Flugzeugherstellern beauftragter IT-Experte kommen muss und einen Nachweis von Schwachstellen erbringt, deutet zumindest auf ein unzureichendes Verwundbarkeits- bzw. Schwachstellenmanagement der betroffenen Flugzeughersteller hin. Der Verdacht kommt sofort auf, dass die Informationssicherheit zumindest bei manchen Flugzeugherstellern nur eine sekundäre Rolle spielt (und das im Zeitalter des IoT).

Hier kommen wir zum Kern der Industrie 4.0 und allgemein des IoT: Die Informationssicherheit muss ein integraler Bestandteil des IoT werden. Hier sind Hersteller von IT-Komponenten, Anlagenbauer und Anlagenbetreiber gleichermaßen gefordert. Jeder Mitspieler muss nachweisen, dass er die Informationssicherheit nach dem Stand der Technik im Griff hat. Dazu werden Gütesiegel benötigt, damit wir einem Produkt unmittelbar ansehen können, wie robust es hinsichtlich der Informationssicherheit ist. Hier sind die Standardisierungsgremien gefordert. Außerdem müssen Hersteller nachweisen, wie stark sie die Informationssicherheit im gesamten Lebenszyklus ihrer Produkte berücksichtigen. Dies beinhaltet auch die systematische Schwachstellensuche und -beseitigung in den eigenen Produkten. Denkbar wäre ein solcher Nachweis z.B. auf Basis der Common Criteria[3]. Schließlich muss auch der Gesetzgeber einen Beitrag leisten. Wir benötigen offensichtlich nicht nur ein IT-Sicherheitsgesetz, das sich an Betreiber kritischer Infrastrukturen richtet, wir benötigen auch ein Instrument, mit dem Informationssicherheit nachvollziehbar bei Herstellern von IoT-Systemen eingeklagt werden kann.

Denken Sie z.B. beim nächsten Flug, bei der nächsten Fahrt im Zug, Schiff oder Auto daran, dass Sie in einer vernetzten, höchst komplexen IT-Infrastruktur sitzen!

Literatur

[1] Siehe BMWi, „Industrie 4.0 und Digitale Wirtschaft“, verfügbar unter http://www.bmwi.de/DE/Themen/Industrie/industrie-4-0.html

[2] Siehe http://www.spiegel.de/netzwelt/netzpolitik/piloten-und-behoerde-warnen-vor-dem-hacking-von-flugzeugen-a-1035139.html

[3] Siehe http://www.commoncriteriaportal.org/

Sonderveranstaltung

IT-Kommunikation im Umfeld von Fertigung und Automation 17.06.15 in Bonn

Die ComConsult Akademie veranstaltet am 17.06.15 ihre neue Sonderveranstaltung "IT-Kommunikation im Umfeld von Fertigung und Automation" in Bonn.

Fertigungsnetze unterscheiden sich von Büronetzen. In Fertigungsnetzen werden eine hohe Verfügbarkeit, die Vermeidung unnötiger Bedrohungen und trotzdem hohe Flexibilität erwartet. Mit der aktuellen Technologie-Entwicklung stellt sich aber immer mehr die Frage, ob eine klare Trennung zwischen Büro und Fertigung in Zukunft erreichbar sein wird. Es stellt sich auch die Frage, ob wir nicht über genügend leistungsfähige Architekturen und Werkzeuge verfügen, um einen Grad an Schutz und Kontrolle zu etablieren, der die Kombination aus Sicherheit, Leistung und Flexibilität möglich macht.

Während über Konzepte wie Internet of Things (IoT) und Smart Home überwiegend visionär gesprochen wird, haben produzierende Unternehmen schon seit Jahren eine stark steigende Anzahl von Geräten in ihren Industrienetzen. Insofern ist für diese Firmen die vierte industrielle Revolution kein Bruch mit dem Bisherigen, sondern die konsequente Fortsetzung der dritten, nämlich der Automatisierung.

Der explosionsartige Anstieg der Zahl der Geräte in der Fertigung stellt die IT-Infrastruktur in den Hallen und im Campus vor nie dagewesene Herausforderungen. Das Netzkonzept muss in vieler Hinsicht an die neue Situation angepasst werden:

- Die steigende Anschlussdichte stellt traditionelle Netzdesigns in der Halle in Frage. Die alte Frage „Lichtwellenleiter oder Kupfer“ stellt sich neu. Mit dieser Frage sind andere verbunden, wie zum Beispiel das Verteilerkonzept, schließlich ist für abgeschottete Räume mit Klimatisierung, Zugangskontrolle, etc. in Hallen kein Platz. Auch damit verbunden ist die Auswahl der Netzkomponenten. Sind Standardkomponenten für den industriellen Einsatz ungeeignet? Wie sieht eine optimale Mischung von Standardkomponenten und Industrieswitches aus?

- Immer mehr IP-Adressen werden gebraucht. Für die größten weltweit agierenden Industrieunternehmen reicht der

vorgesehene Vorrat an privaten IPv4-Adressen nicht mehr. Network Address Translation (NAT) im internen Netz behindert viele Anwendungen. Auf der anderen Seite sind viele Lieferanten von Automatisierungssystemen noch nicht so weit, dass ihre Geräte über IPv6 statt IPv4 kommunizieren könnten. Die Industrieunternehmen brauchen zweierlei: einerseits die schnelle Lösung der jetzigen Probleme mit dem IP-Adresskonzept und andererseits den klaren Ausblick auf eine dauerhafte Lösung mit IPv6. Letzteres bedeutet fraglos eine Bringschuld seitens der Anbieter von Automatisierungslösungen. Die Kunden müssen diesen Anbietern die Anforderungen hinsichtlich der Unterstützung von IPv6 konkret vorgeben.

- Immer wieder und seit Jahren wird diskutiert, wie das passende Zonenkonzept für Industrieunternehmen aussehen soll. Nicht alle Unternehmen setzen auf die konsequente Bildung separater Sicherheitszonen für die Fertigung. Ist eine solche Trennung unumgänglich? Wenn ja, stellt sich die Frage nach den Details eines Zonenkonzeptes. Können funktional abgeschlossene Einheiten zum Beispiel in einer Halle einer Zone zugeordnet werden? Wenn ja, wie ist mit solchen Bereichen wie Logistik umzugehen?

- Die sichere Administration von Systemen in der Fertigung ist eine immer wiederkehrende Herausforderung. Die Gestaltung der Sicherheit für den administrativen Zugriff muss nicht nur internes, sondern vor allem auch externes Personal berücksichtigen. Gerade in der Automatisierung werden viele Systeme von externen Technikern gewartet.

- Handscanner und „WLAN-Schrauber“ begegnen einem schon lange in der Fertigung. Aber auch innovative Endgeräte wie Smartphones und Tablets finden Einzug in die Fertigungsnetze. Wie ist mit diesen Geräten umzugehen? Wie sieht das zugehörige Sicherheitskonzept dafür aus? Wie werden diese Geräte vernetzt?

- Wireless LAN ist seit Jahren ein wichtiger Bestandteil von Fertigungsnetzen. Mittlerweile liegen viele Erfahrungen bei der WLAN-Gestaltung in Fabrikhallen vor. Störeinflüsse von anderen Geräten beeinträchtigen hin und wieder die industriellen WLANs. Wie sind solchen Störungen zu minimieren? Welches WLAN-Design gilt als zuverlässig und robust genug, um auch in der Halle zum Einsatz zu kommen? Welche Frequenzen sollen für welche Anwendungen genutzt werden? Wie bekommt man die optimale Ausleuchtung einer Halle am besten hin?

- Ausfälle in der Fertigung kosten messbar Geld – viel Geld. Und wenn doch einmal eine Störung auftritt, muss alles ganz schnell gehen. Wer trägt die Betreiberverantwortung für welche Komponenten? Welche Tools braucht man für Betrieb und Fehlersuche in einer Fertigungsumgebung? Wie ist die passende Arbeitsteilung dazu? Wer muss zu welchen Themen geschult werden? Braucht man Experten im Schichtbetrieb oder reicht eine Bereitschaftsregelung aus

Mit der aktuellen Technologie-Entwicklung stellt sich immer mehr die Frage, ob eine klare Trennung zwischen Büro und Fertigung in Zukunft noch erreichbar sein wird. Diese Sonderveranstaltung analysiert wie Fertigungsnetzwerke auf diese Herausforderungen reagieren können und wie mit geeigneten Technologien Sicherheit, Leistung und Flexibilität gewährleistet werden kann.

Programmübersicht IT-Kommunikation im Umfeld von Fertigung und Automation

Mittwoch, den 17.06.2015

9:30 Uhr
90 Minuten

Keynote – Netzarchitekturen für die Fertigung
- Verkabelungskonzepte in der Halle: „Lichtwellenleiter oder Kupfer“?
- Die Halle ist riesig! Aber wohin mit den Verteiler?
- Welche Netzkomponenten braucht man für welchen Zweck?
- Wie sehen IP-Adresskonzepte im Fertigungsbereich aus?
- Das Internet der Dinge ist schon da: Braucht man IPv6 in der Fertigung?

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

11:00 Uhr Kaffeepause

11:15 Uhr
75 Minuten

WLAN in Fertigungsumgebungen
- Wie bekommt man die optimale Ausleuchtung einer Halle am besten hin?
- Welches WLAN-Design gilt als zuverlässig und robust genug, um auch in der Halle zum Einsatz zu kommen?
- Welche Frequenzen sollen für welche Anwendungen genutzt werden?
- An allen Ecken funkt es: Lassen sich Störungen überhaupt vermeiden?
- „Fremde“ Funkanwendungen sickern unbemerkt ein! Wie geht man damit um?

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

12:30 Uhr Mittagspause

13:30 Uhr
45 Minuten

Tablets und Smartphones im Fertigungsbereich
- Wie ist mit diesen Geräten umzugehen?
- Wie sieht das zugehörige Sicherheitskonzept dafür aus?
- Wie werden diese Geräte vernetzt?

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

14:15 Uhr
60 Minuten

IT-Sicherheit und Zonenkonzepte in der industriellen Fertigung
- Passendes Zonenkonzept für Industrieunternehmen
- Separater Sicherheitszonen für die Fertigung?
- Können funktional abgeschlossene Einheiten zum Beispiel in einer Halle einer Zone zugeordnet werden?
- Wie ist mit solchen Bereichen wie Logistik umzugehen?
- Sichere Administration von Systemen in der Fertigung
- Sicherheit für den administrativen Zugriff externer Techniker

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

15:15 Uhr Kaffeepause

15:30 Uhr
45 Minuten

Hochverfügbare und sichere industrielle Kommunikationskonzepte & Industrie 4.0

Thomas Schramm, Hirschmann Automation and Control GmbH

16:15 Uhr
45 Minuten

Netzbetrieb und Fehlersuche in Fertigungsnetzen
- Wer trägt die Betreiberverantwortung für welche Komponenten?
- Tauscht der Betriebselektriker defekte Switches oder braucht man Experten im Schichtbetrieb?
- Wer muss zu welchen Themen geschult werden?
- Welche Tools braucht man für Betrieb und Fehlersuche in einer Fertigungsumgebung und wer sollte sie nutzen können?

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

Ende der Veranstaltung 17:00 Uhr

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Ich buche die Sonderveranstaltung
IT-Kommunikation im Umfeld von Fertigung und Automation

☐ am 17.06.15 in Bonn
zum Preis von € 990,-- netto

☐ Bitte buchen Sie mir ein Hotelzimmer

vom_____ bis_____15

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

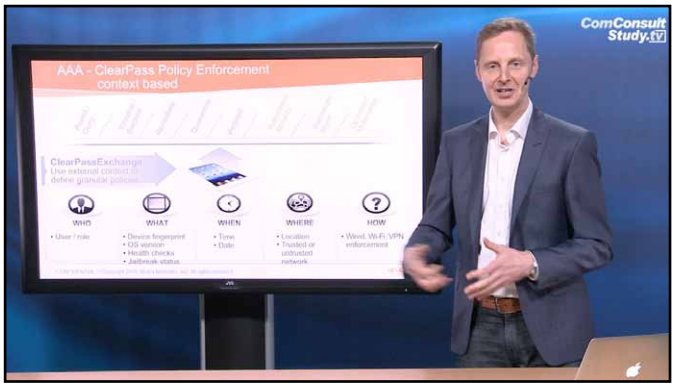
_____ Vorname	_____ Nachname
_____ Firma	_____ Telefon/Fax
_____ Straße	_____ PLZ,Ort
_____ eMail	_____ Unterschrift

ComConsult-Study.tv

Aktuelle Neuerscheinungen

ComConsult-Study.tv ist mit seiner Gründung im Jahr 2009 das jüngste Unternehmen der ComConsult-Gruppe. ComConsult-Study.tv bietet mit seinem breit gefächerten Angebot an Video-Trainingsmodulen die ideale Ergänzung zum bestehenden Portfolio der ComConsult Akademie mit ihren bewährten Präsenz-Veranstaltungen und den Produkt- und Technologie-Analysen aus dem Testlabor der ComConsult Research GmbH.

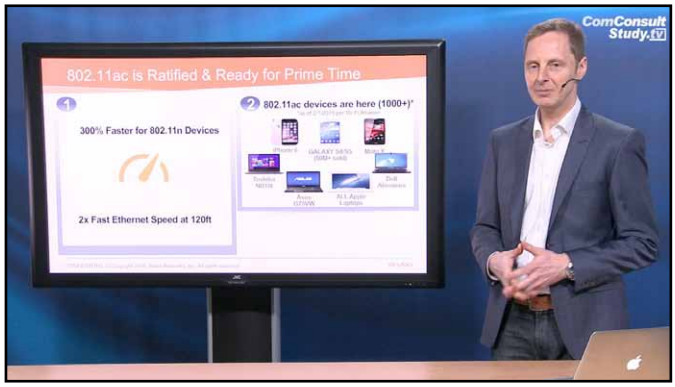
In rund 250 Videobeiträge werden IT-Techniken anschaulich vorgestellt, Trends analysiert und Prognosen zur Marktentwicklung gegeben. Neben klassischen IT-Techniken wie UC, Rechenzentrum und Sicherheit werden auch Themen behandelt, die über das reine Fachwissen hinausgehen. So gibt es Schulungen zur Präsentationstechnik, Fotografie für PR und Marketing und Empfehlungen für einen erfolgreichen Webauftritt. Monatlich kommen weitere, aktuelle Videos hinzu. Mit dem Abo bleiben Sie immer auf dem aktuellen Stand.



Network Access Control mit Clearpass

Referent: **Reinhard Lichte**
Zeit: 00:38:30
Preis: kostenlos
veröffentlicht am 29.05.2015

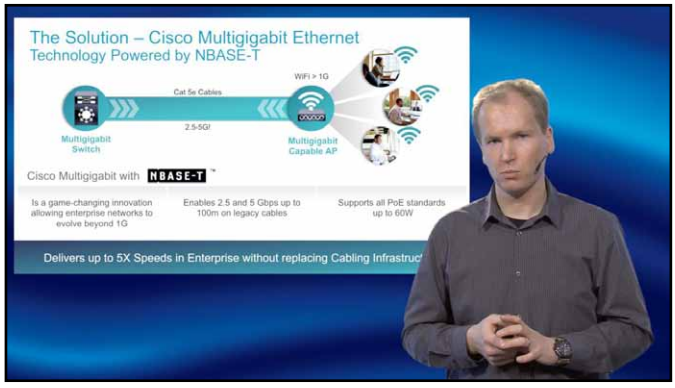
Ziel von NAC-Projekten ist die sichere Identifikation der Endgeräten und Usern. Doch darüber hinaus gilt es den aktuellen Stand der Geräte zu Qualifizieren, will man größtmögliche Sicherheit erreichen. Reinhard Lichte zeigt die Herausforderungen auf und wie diese mit Aruba Netzworks Clearpass gelöst werden können.



WLAN-Netzwerke mit 802.11ac

Referent: **Reinhard Lichte**
Zeit: 00:37:27
Einzelpreis: 49,00 € netto Im Abo: kostenlos
veröffentlicht am 29.05.2015

802.11ac ist Stand der Technik. Doch die höhere Datenrate stellt Planer auch vor neue Herausforderungen. In diesem Video werden folgende vier Problemfelder erläutert und deren Lösungen vorgestellt:
1.Umgang mit langsame WLAN-Clients
2.Planung von .11ac Netzen
3.Umgang mit "Sticky Clients" mit langsamen Datenraten
4.Bandbreitenmanagement in 802.11ac Netzen



Cisco Multigigabit Ethernet: nBase-T

Referent: **Sascha Ulfig**
Zeit: 00:15.51
Einzelpreis: 49,00 € netto Im Abo: kostenlos
veröffentlicht am 20.03.2015

Multigigabit Ethernet ist die neueste Ethernet Evolutionsstufe und erlaubt es mit Geschwindigkeiten >1Gbps über bestehende Cat5e Verkabelung zu senden. Somit wird es möglich, die Leistung der neuesten Generation von 802.11ac Access Points (wave 2 mit Datenraten von bis zu 6,8Gbps) ohne Neuverkabelung ausnutzen zu können. Neben IEEE kompatiblen Datenraten (100Mbps, 1Gbps, 10Gbps) werden erstmalig auch neue “Zwischen-Datenraten" (2,5Gbps, 5Gbps) unterstützt.

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

Zweitthema

Konsequenzen von Moore´s Law für die Arbeitswelt und die Gestaltung von Netzen und Systemen in den nächsten Jahren

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.

Fortsetzung von Seite 1

Rückwirkend betrachtet hat es seit der durch die Dampfmaschine ausgelösten industriellen Revolution nichts mehr gegeben, was insgesamt und weltumspannend größeren Einfluss auf das Leben und Arbeiten von Generationen hatte als Moore´s Law, denn ohne das hier beschriebene Wachstum in der Funktionalität wären überwiegende Teile der industrialisierten Welt völlig undenkbar. Waren diese Trends zunächst nur in der Arbeitswelt interessant, ist das letzte Jahrzehnt ja grade dadurch gekennzeichnet, dass die elektronischen Helferlein auch in unser Privatleben eingedrungen sind, mit nicht immer wünschenswerten Konsequenzen.

1. Moore´s Law wird weiterleben

Was Dr. Moore in seinem Artikel vom 19. April 1965 für das „Electronics"-Magazin beschrieben hat, war die ersten zehn Jahre danach nicht unter dem Begriff „Moores´Law" bekannt. Es war eine Feststellung, die zunächst nur innerhalb der Halbleiter-Industrie von Interesse war, bis sich zum Ende der Achtziger Jahre des letzten Jahrhunderts Implikationen dieses Entwicklungsgesetzes auf den Rest der Elektronik-Industrie auswirkten. Erst mit dem Beginn des 21. Jahrhunderts wurde die Bedeutung von Moore´s Law integraler Bestandteil einer mehr öffentlichen Diskussion. Man hatte zwar schon Jahrzehnte zuvor gesehen, wie Technologie dabei helfen kann, Menschen zum Mond und zurück zu bringen, aber ein breiteres Bewusstsein ist rückblickend ungefähr erst dann entstanden, als man erkennen musste, wie PCs ein unabdingbares Instrument zum Lernen und zum Aufbau einer Karriere wurden.

Moore´s Law hat seine außergewöhnliche Zugkraft nicht aufgrund seiner Neuartigkeit, modischer Launen oder einer starken Werbung bekommen, sondern einfach deswegen, weil es sich im letzten halben Jahrhundert als das effektivste Vorhersage-Tool für neue Chip-Generationen, technologische Innovation und sogar soziale und kulturelle Änderungen erwiesen hat. Es hat den Vorteil, dass es auch für diejenigen leicht zu merken ist, die keinerlei technologische Vorbildung haben. Es hat dies alles in einem Umfeld des Misstrauens erreicht, selbst Dr. Moore hat immer an seiner Dauerhaftigkeit gezweifelt. Es ist auch kein wirklich wissenschaftliches Maß, sondern vielmehr eine Art „Pakt" zwischen der Chip-Industrie und der Weltwirtschaft.

Gegen alle Widerstände und reguläre Vorhersagen über sein bevorstehendes Ende dauert Moore´s Law an, fördert damit Fortschritte in Industrie und Wissenschaft und sorgt sogar für neue Erfahrungen von Menschen im Rahmen einer erweiterten oder virtuellen Realität. Historisch hat sich die ursprüngliche Rate der Verdopplung der Chipleistung alle 18 Monate aktuell etwas verlangsamt, aber selbst Pessimisten werden zugeben, dass es wenigstens noch ein Jahrzehnt und wahrscheinlich sogar noch weiter „hält". Es gab in letzter Zeit eine Reihe wissenschaftlicher Durchbrüche auf Bereichen wie Transistoren auf atomarem Niveau, Nanotechnologie und biologischer Computer. Sollten diese sich im Rahmen wirtschaftlich vernünftiger Fabrikation materialisieren, wird Moore´s Law noch einige Jahrzehnte länger halten. Vielleicht wird man rückwirkend die Zeit zwischen 1960 und 2060 einmal als „Moore´s Ära" bezeichnen [MEL 15].

Und dafür sieht es gut aus. Die führenden Hersteller integrierter Schaltkreise wie Intel, TSMC, Qualcomm, Apple oder Samsung sind jetzt dabei, die angekündigten Herstellungsprozesse mit 16, 14 oder sogar 10 nm in den Fabrikationsmaßstab zu überführen. Dazu war es notwendig, eine technologische Barriere zu durchbrechen, nämlich das Drucken unterhalb der optischen Auflösung. Es gibt hier verschiedene Ansätze, die von den Herstellern unterschiedlich verfolgt werden. Der Oberbegriff für die neue Herstellungsmethode ist „Multiple Patterning" [SIV 12], [ROR 15]. Das ist prinzipiell eine Menge von Prozeduren, die es erlaubt, bestimmte lithographische Charakteristika KLEINER zu drucken, als das die Auflösung des Druckers eigentlich erlaubt. Die Auflösung der extrem teuren Drucker in der Halbleiter-Herstellung wird durch bestimmte Brechungseigenschaften des Lichtes begrenzt. Möchte man jetzt eine noch kleinere Auflösung erzielen, muss der Wafer schlicht ausgedrückt mehrfach bedruckt werden. Dafür gibt es zwei wesentliche Methoden. Eine davon ist die sog. Doppelbelichtung. Hier wird der Wafer zweimal durch den lithographischen Scanner geschickt, wobei jeweils eine andere Maske verwendet wird. Beim ersten Durchgang wird die maximale Auflösung im Rahmen der Grenzen durch die Lichtbrechung erzielt. Man kann dann Strukturen sagen wir von der „Größe" w belichten, die um sich herum freie Stellen mit der Größe L haben. Gestaltet man die photoempfindliche Schicht richtig, so kann man durch unterschiedliche Lichtempfindlichkeiten erreichen, dass $w < L$ wird, z.B. $w = 3L$.

Beim nächsten Durchgang kann man, die nötige Präzision vorausgesetzt, nochmals Strukturen der Größe w in die freien Stellen der Breite L projezieren. Das ist ja soweit ganz anschaulich. Wichtig ist vielleicht noch zu wissen, dass beim etwa vor 15 Jahren vollzogenen Übergang von 65 nm- auf 45nm- oder 32nm-Technik das Bild der integrierten Strukturen „aufgeräumt“ wurde. Die 65 nm-Strukturen waren recht verspielt und sahen in Vergrößerung eher wie ein modernes Wandgemälde aus. Der Umbruch wurde dadurch erreicht, dass man lineare oder eindimensionale Strukturen eingeführt hat, bei denen Transistoren letztlich systematisch in Linien angeordnet wurden, die Verbindungen zwischen sich hatten (siehe Abbildung 1). Diese „1D“-Struktur ermöglicht jetzt das Durchbrechen der 20 nm-Grenze und ist übrigens auch die Grundlage für die Schaffung von 3D-Schaltungen wie den 3D-SSDs. Nur zum allgemeinen Größenvergleich dient die Abbildung 2.

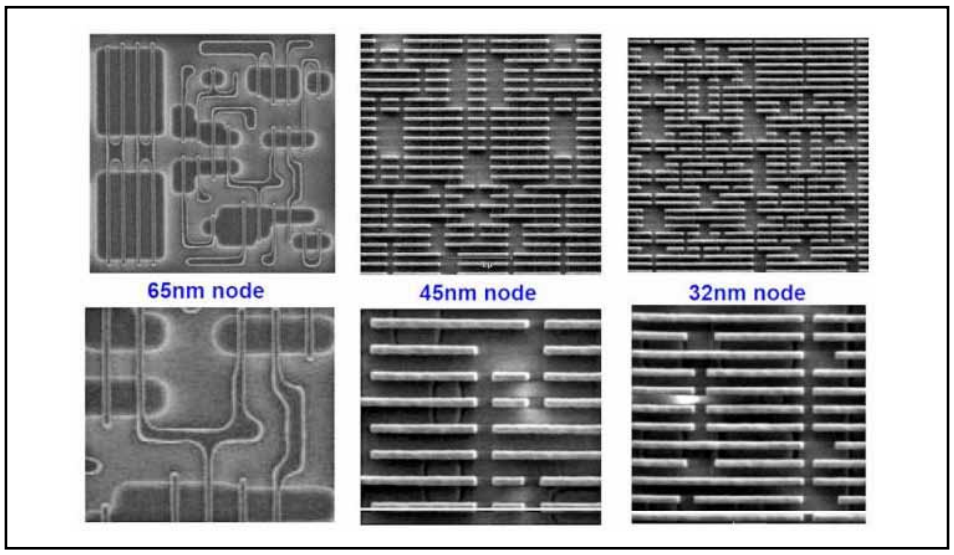


Abbildung 1: Entwicklung der Schaltkreis-Geometrie bei immer fortschrittlicheren Herstellungsprozessen
Quelle: K. Kuhn: „Variation in 45nm and Implications for 32nm and Beyond“, Keynote 2nd CMOS-Variability Conference London 2009

Möchte man das „Weiterleben“ von Moore´s Law abschätzen, sind die Betrachtungen hinsichtlich des Herstellungsprozesses wesentlich wichtiger als architekturelle Variationen. Nochmals zur Verdeutlichung: die 14 nm-Technologie ist bereits heute in jedem neuen Apple MacBook mit den „Core-M“-Prozessoren zu haben, 10 nm steht bei Intel für Ende 2015, bei TSMC für Anfang 2016 auf der Liste.

Es sei vielleicht noch bemerkt, dass Moore´s Law nicht wirklich etwas über die Kosten aussagt. Die neuen Herstellungsprozesse liegen bei rund 10 Mdr. US$, es muss also schon eine Menge Chips verkauft werden, damit sich das lohnt.

2. Auswirkungen auf kommende Generationen

Diese Vorhersagen werden enorme Auswirkungen auf die um 2000 geborene Generation haben (die deshalb auch als „Millennials“ bezeichnet werden), weil diese ab jetzt damit beginnen, in die Arbeitswelt einzutreten. Schon die Generation vor ihnen hat zu mindestens in den Industriestaaten keine Welt mehr kennengelernt, die nicht von Moore´s Law geprägt wurde. Für die Millennials gehören Internet, Soziale Netze oder Smartphones schon eher zur öffentlichen Grundversorgung wie Wasser und Strom. Sie sind eher von komplexeren Dingen fasziniert, wie Drohnen, Roboter oder 3D-Drucker, ohne zu verstehen, wie eng auch diese Entwicklungen mit Moore´s Law zusammenhängen. Sie sind an solchen langweiligen Dingen wie dessen 50. Geburtstag weder interessiert, noch ist es ihnen bewusst, aber ihre Zukunft wird mehr als die jeder vorhergehenden Generation genau davon abhängen. Ihre Karrieren werden damit stehen und fallen, wie gut sie von einer Entwicklung profitieren können, die auf einem Zusammenhang basiert, der während der Amtszeit von Lyndon B. Johnson oder Ludwig Erhard entdeckt wurde.

Allerdings: will die Arbeitswelt der Kurve von Moore´s Law folgen, kann das ein wilder Ritt werden. Die sich immer weiter verdoppelnde Gangart war schon immer brutal und in der Vergangenheit hauptsächlich verantwortlich für die Mortalitätsrate von rund 90% bei den Elektronik-Herstellern, die eigentlich als erste industrielle Gruppe von der neuen Technologie vollends abhängig waren. Heute gibt es von der Frittenbude bis zum internationalen Großkonzern kein Unternehmen mehr, welches ohne Technologie überhaupt Umsatz machen könnte, was natürlich zu unglaublichen Risiken führt, die es vorher in dieser Art nicht gab. Aber es werden eben auch neue unternehmerische Möglichkeiten im Zwei-Jahrestakt erzeugt. Während die meisten Leute noch ehrfürchtig vor den Sozialen Netzen, Smartphones und der globalen Finanzkrise von 2008 standen, ist eine neue Generation von „Digital Natives“ aufgewachsen, ohne die massive Revolution bei Halbleitern, Computern, Kommunikation und dem Internet, die insgesamt in den letzten vierzig Jahren statt gefunden hat, miterlebt zu haben. Während dieser Zeitspanne hat Moore´s Law Industrien beeinflusst und sogar transformiert, die jetzt einiges von den Millennials verlangen: sie müssen hochgradig ausgebildet sein, schnell und flexibel denken können, sowie mit Komplexität und einem sich schnell ändernden Wettbewerb umgehen, die es so vorher nicht gab.

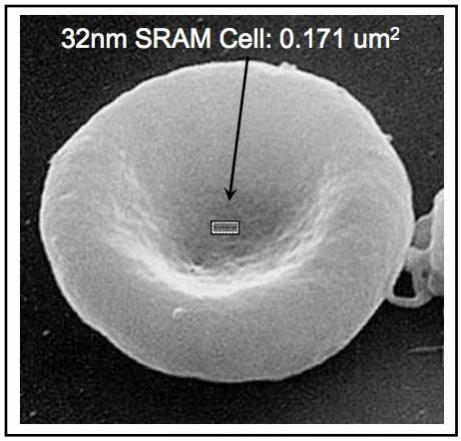


Abbildung 2: SRAM-Zelle in 32nm-Technik im Vergleich zu einem menschlichen roten Blutkörperchen
Quelle: K. Kuhn: „Variation in 45nm and Implications for 32nm and Beyond“, Keynote 2nd CMOS-Variability Conference London 2009

Man kann eigentlich jetzt schon den Beginn der Entwicklung der Tools und Plattformen für diesen neuen Wettbewerb sehen. Es gibt durchaus die Prognose, dass einige Bereiche zehnmal schneller wachsen könnten als die „heißesten“ Unternehmen heute.

Das wird dadurch geschehen, dass praktisch alles rein virtuell wird, und alles auf den Bereichen Produktentwicklung, Design, Herstellung, Marketing und Sales Force über Bord geworfen werden wird,

was betriebliche Hemmnisse erzeugt. Aufgaben, die traditionell im Haus erledigt wurden, werden zunehmend ausgelagert, auf Sites außerhalb des Unternehmens bearbeitet oder direkt an die Kunden weitergegeben. Es bedarf schon eines ausgeprägten Scharfsinns, um mit der durch Moore´s Law bedingten Geschwindigkeit immer weiter mitzuhalten. Das Problem ist, dass z.B. einmal eingeführte Dienste explosionsartig wachsen können, wenn sie Anklang finden. Abbildung 3 zeigt nur eines von vielen Beispielen.

Crowd-Sharing, Crowd-Funding, Bitcoin, Micro Venture Funding, Cloud Computing und Big Data sind frühe Versuche, bei der nächsten Phase von Moore´s Law mitzukommen. Wir sehen schon, dass der Erfolg bislang sehr unterschiedlich ist.

Wie schon zuvor wird der neue, schnellere Takt auch die Gesellschaft allgemein durchdringen. Moore´s Law hat schon immer die Miniaturisierung befördert: aus massiven Mainframe-Computern werden Smart-Watches und große, vertikal integrierte Organisationen werden von wesentlich kleineren Armeen von „Davids“ herausgefordert und in ernsthafte Schwierigkeiten gebracht.

Heute werden starre Kommando- und Kontroll-Strukturen häufig durch adaptive und kurzlebige Allianzen und Konföderationen ersetzt. Es entsteht eine in immer stärkerem Wettbewerb stehende Welt von „Frenemies“. Dieser Prozess wird auf jede Ecke der Gesellschaft übergreifen und die Zukunft in ein Gebiet verwandeln, welches auf wirklich keiner Landkarte verzeichnet ist.

Es gibt schon verschiedentlich Zweifel am Wert des heutigen Ausbildungssystems, was sicher nur bedingt dazu geeignet ist, die Millennials auf die zukünftige Welt richtig vorzubereiten. Manche glauben, dass Online-Universitäten eine Lösung für das Problem sein könnten. Die persönliche Erfahrung des Autors ist leider, dass dies alles nicht wirklich neu ist. Die Schule bereitet nicht recht auf die Universität vor, und diese kaum auf das richtige (Berufs-) Leben.

Sieht man genau hin, ist wegen Moore´s Law heute wirklich alles in Bewegung. Betrachten wir nur das Gesundheitswesen. Kliniken werden angesichts der aufkommenden Revolution beim personalisierten Gesundheits-Monitoring ihre Rolle ändern müssen. (siehe Abbildung 4)

Die Health-Apps, die auf der Apple-Watch und anderen Geräten dieser Art laufen, sind nicht nur dazu gedacht, dem stolzen Besitzer des Gerätes zum Verlassen des Sessels aufzufordern oder ihm seine gesundheitlichen Daten mitzuteilen, sondern

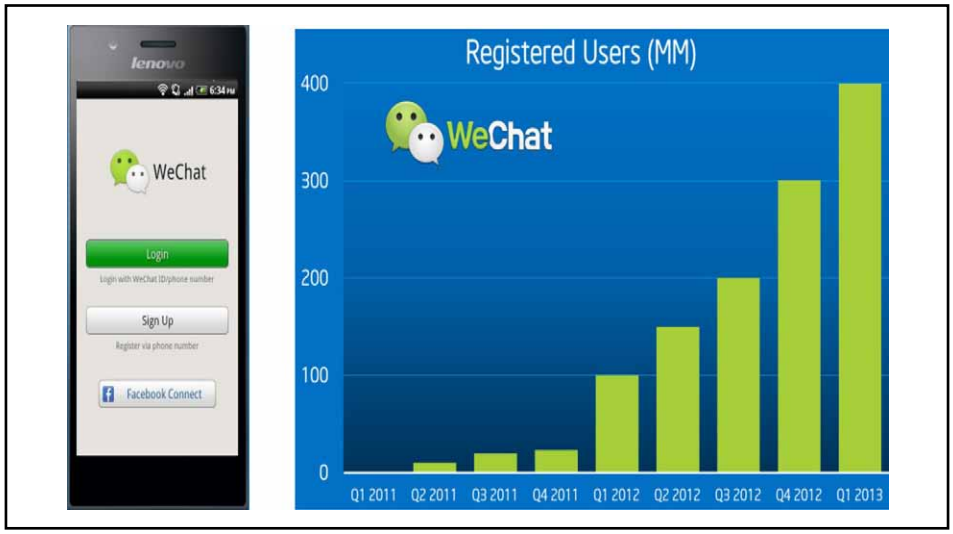


Abbildung 3: Explosionsartiges Wachstum Digitaler Dienste Quelle: Morgan Stanley

diese Daten können auch an entsprechende Auswertungsprogramme in der Cloud gehen, die ihrerseits wiederum mit Big Data in der ersten Phase zu statistischen Auswertungen, in weiteren Phasen aber auch zu Behandlungsempfehlungen kommen werden, die Ärzte und Kliniken sozusagen in einen Patienten-bezogenen Informationskreislauf einbinden. Natürlich gibt es hier wie bei jeder Entwicklung auch berechtigte Bedenken, z.B. hinsichtlich des Datenschutzes, aber es wird auch nichts von heute auf morgen geschehen. Es werden aber Prozesse in Gang gesetzt, die in Zukunft an Fahrt gewinnen werden und dann wiederum die Leistung benötigen, die ihnen durch Moore´s Law zugesichert wird.

Die Millennials stehen vor einer der größten Chancen, die eine Generation nur selten hat: sie können die Welt, in der sie leben, komplett überarbeiten. Allerdings könnte Moore´s Law auch zu ihren Lebzeiten an Bedeutung verlieren. Daher müssen sie eigentlich noch härter als ihre Vorgänger daran arbeiten, es am Leben zu halten.

3. Das Ende allgemeingültiger IT-Infrastrukturen und -Lösungen

In der geschilderten Situation ist es für Unternehmen absolut überlebenswichtig, die IT-Infrastruktur nicht nur „irgendwie“ zum Überleben zu bringen, sondern Änderungen und Entwicklungen möglichst frühzeitig aufzunehmen um letztlich auch der kommenden Generation hoch qualifizierter Mitarbeiter ein entsprechendes Arbeitsumfeld anbieten zu können. Wir haben in Deutschland schon heute einen erheblichen Fachkräftemangel, der sich angesichts der immer weiter dramatisch steigenden Anforderungen und der Unfähigkeit der Schulsysteme zu Anpassungen nicht wirklich verbessern wird. Das ist an und für sich nichts Neues, auch der Autor hat in der Schule gar nichts und im Studium kaum etwas Sinnvolles für sein Berufsleben lernen können, und das ist schon einige Jahrzehnte her. Solange Ausbildungssysteme primär auf das Abhaken von Qualifikationen ausgerichtet sind, wird das auch nichts. Aber das können wir hier kaum ausdiskutieren.

Fakt ist nur, dass sich Unternehmen frühzeitig positionieren müssen, um Fachkräften nicht den Eindruck zu vermitteln, man arbeite im Mittelalter.

Dr. Suppan [SUP 15] identifiziert folgende Spannungsfelder moderner IT-Infrastrukturen:

Abbildung 4: Giga-Trend: Wearables Quelle: Apple

- Übergang von teurer Spezialtechnik zu Massenware
- Zunehmendes Angebot spezialisierter Technologien
- Nutzungsdauer einzelner Technologien deutlich gestiegen
- Neue Technologieansätze / neue Schwerpunkte

Der Übergang von teurer Spezialtechnik zu Massenware wurde rückwirkend betrachtet eigentlich nicht so sehr durch wirkliche architekturelle Impulse aus der Hardware ausgelöst, sondern durch die Kombination von (immer leistungsfähiger werdender) Standard-Hardware und der Möglichkeit der Virtualisierung. In den 80er Jahren wurden teure Host-Systeme bei Standardaufgaben vielfach durch PC-Netze ergänzt und ersetzt. Das führte zu Legionen relativ einfacher Server. Die Entwicklung erheblich leistungsfähigerer Server in Standard-Architekturen hätte ohne Virtualisierung nicht viel genützt. Man kann Virtualisierung am Besten als betriebliches Konzept verstehen, welches die durch die im Rahmen von Moore´s Law gegebene strukturelle „Verbreiterung“ sinnvoll nutzt. Prozessor Chips haben immer mehr Prozessoren, die man aber ohne Virtualisierung überhaupt nicht brauchen könnte. Die Virtualisierung hat die einfacheren Server auf die neuen Plattformen konsolidiert. So haben sich diese Konzepte gegenseitig befruchtet und man kann durchaus davon ausgehen, dass die Virtualisierung ebenfalls dauerhafter Bestandteil der IT ist und sein wird. Heute ist man soweit, dass man z.B. auch wichtige Funktionen in Netzwerken, wie Lastverteilung oder Firewalls, nicht mehr in teurer Spezial-Hardware ausführt, sondern diese Funktionen ebenfalls in virtualisierten Standard-Umgebungen implementiert. Diese sog. Netzwerk- Funktions-Virtualisierung (NFV) führt nicht nur zu geringeren Kosten, sondern auch zu erheblich gesteigerter Funktionalität. Letztlich möchte man heute alles, was nicht aufgrund seiner Funktion notwendig in Hardware gegossen werden muss, eher in Software realisieren. Konzepte wie SDN (Software Defined Networking) führen letztlich zu modernen „Betriebssystemen“ für hinreichend standardisierte Hardware.

Das ist aber nur die eine Seite der Medallie. Neben einer sehr stark durch Hardware-Standardisierung und Virtualisierung geprägten Welt entstehen nach wie vor spezialisierte Technologien. Dazu gehören z.B. „Cloud“ oder „Big Data“. Bleiben wir bei letzterem. In den 90er Jahren hat mit der Ausbreitung des Internets auch in private Haushalte das Zeitalter des eBusiness begonnen. Heute kann jeder Privatmann grundsätzlich alles, was er für sein gesamtes Leben benötigt, im Internet bestellen. Der Erfolg des eBusiness ist um ein Vielfaches größer als von den ursprünglichen gedanklichen Vätern erträumt, die prinzipiell nur vorhatten, das Massen-Marketing durch ein auf den individuellen Kunden zugeschnittenes One-to-One-Marketing zu ersetzen und letztlich zwischen allen Beteiligten eine durchgängige Feedback-Schleife zu errichten, die zu einer höheren Kunden-Zufriedenheit führt. Durch den rasanten Erfolg wurden die Grundgedanken bis vor rund fünf Jahren kaum weiterentwickelt, bis jemand auf die „Idee“ kam, dass die Datenspur, die jeder Konsument im Laufe seines Internet-Lebens hinterlässt, eine wirkliche Fundgrube und die Summe solcher Datenspuren ein wertvolles Vermögen darstellt. Parallel zu solchen Gedanken kamen die sozialen Netze auf, die wesentlich mehr über ihre Teilnehmer preisgeben, als diesen eigentlich lieb sein kann. So sind unglaubliche Mengen von Daten entstanden, die nach neu zu entwickelnden Konzepten bearbeitet werden müssen, um sinnfällige Ergebnisse ableiten zu können: Big Data war geboren. Kurz gesagt werden extrem leistungsfähige Systeme aus dem wissenschaftlich orientierten HPC-Bereich mit Unmengen Daten gefüttert, um Ergebnisse über das Verhalten von Einzelnen, kleinen oder großen Gruppen sowie ganzen Bevölkerungen zu erhalten, die man dann wiederum z.B. für den Waren- oder Leistungsverkauf nutzen kann. Aus diesem von der Interessenlage her eigentlich trivialen „Sumpf“ haben sich aber mittlerweile ganz andere Systeme entwickelt, von denen als Beispiel die im Gesundheitswesen genannt werden können. Neue Endgeräte wie Wearables (z.B. Apple Watch) werden zu einem medizinischen Datenvolumen führen, welches es vorher so noch nie gab. Man wird neue Diagnose- und Behandlungsverfahren entwickeln können. Spannend ist aber, dass der Patient eine praktisch dauerhafte Verbindung zu den Systemen hat, die seine Gesundheit überwachen. Wir können dies hier nicht weiter fortführen, aber dieses eine Beispiel zeigt, dass sich spezialisierte Technologien entwickeln, die eben grade NICHT mit Standard-Systemen implementiert werden können.

Also brauchen wir ein weiteres Instrument, um die „normale“ IT eines „normalen“ Unternehmens mit den spezialisierten Lösungen zu verbinden. Und dieses Instrument ist ganz klar die Cloud oder allgemeiner das Cloud Computing. Netze haben dazu geführt, dass nicht jedes Unternehmen alles, was benötigt werden könnte, vor Ort hat. Das ist viel zu teuer. Es gibt unterschiedliche Ausprägungen des Cloud-Computings, die wir später weiter diskutieren, aber klar sollte sein, dass trotz aller Bedenken z.B. hinsichtlich Sicherheit und Zuverlässigkeit Cloud Computing ein Instrument ist, das jedes Unternehmen benötigt, wenn es mehr als seine Standard-Aufgaben erledigen möchte. (siehe Abbildung 5)

Man sollte eigentlich denken, dass mit zunehmendem Fortschritt Technologien in immer schnellerem Takt auftauchen und verschwinden. Aber es gibt einige Systeme, die zeigen, dass eigentlich nur die Kontinuität in bestimmten Basis-Technologien erlaubt, sozusagen an der technologischen Spitze Neuheiten einzuführen. Nehmen wir als Beispiel das Ethernet. Es hat sich als universelles Transportsystem durchgesetzt und sich über mehr als 40 Jahre immer wieder neuen Anforderungen angepasst. Es gibt ja von mir einen eigenen Artikel speziell zu diesem Thema, darum möchte ich darauf hinwei-

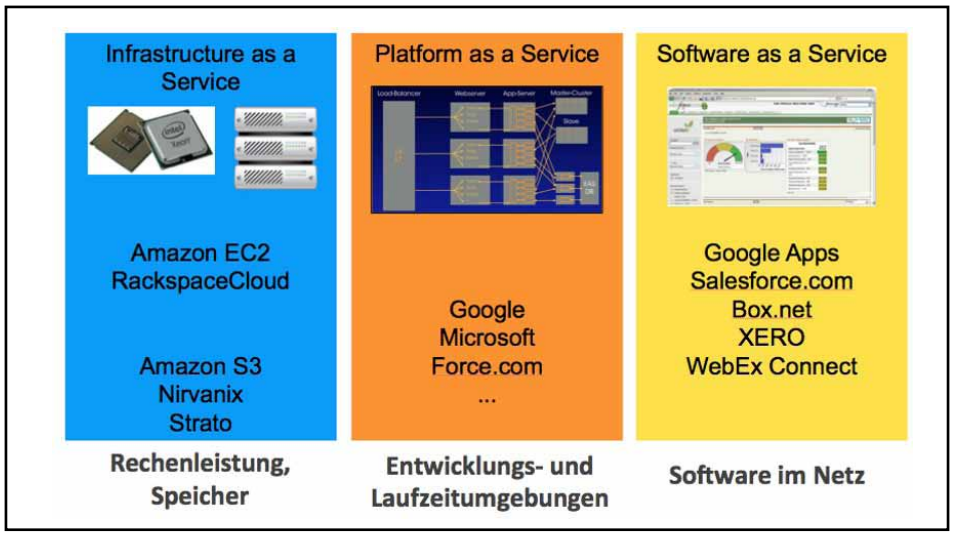


Abbildung 5: Cloud-Alternativen Quelle: Dr. Jürgen Suppan, Com Consult Research GmbH

sen, dass es nicht notwendigerweise immer die Mega-Ultra-Ausbaustufen sind, auf die es ankommt. Mobilität ist das A und O moderner Arbeitsumgebungen in Unternehmen aber auch zuhause. Unternehmen müssen in ziemlich kurzer Zeit Wireless-Grundversorgungen schaffen, die Funkzellen mit Multi-Gigabit-Leistung versorgen. Die Access Points dazu gibt es schon. Bisherige Ausbaustufen von Ethernet mit 1 GbE (kann zu wenig) oder 10 GbE (kann zu viel) passen weder zu den Anforderungen noch zur bestehenden Verkabelung. Die neuen Standards für 2,5 und 5 GbE helfen den meisten Unternehmen sicherlich mehr als singuläres Terabit-Ethernet.

Für die neuen mobilen Endgeräte und deren Nutzung haben sich im Laufe der Zeit auch neue Schnittstellen ergeben, wie z.B. die Gesten-Steuerung. Das heißt aber nicht, dass Browser verschwinden werden. Sie werden vielleicht, genau wie Ethernet, ihre Form etwas ändern und immer leistungsfähiger und flexibler werden. Aber unter „Benutzer-Zentrierung“ ist ja wohl nicht zu verstehen, dass der Benutzer durch immer neue Schnittstellen letztlich völlig verwirrt oder dauerhaft mit deren Erlernen beschäftigt wird.

Natürlich gibt es auch immer wieder neue Technologieansätze und neue Schwerpunkte. Einer der dynamischsten Bereiche ist sicherlich das Internet of Things, schon heute kommunizieren über das Internet wesentlich mehr Geräte und Maschinen als Menschen. Hier kann man alte Funktionsbereiche optimieren und neue erfinden. Der Fantasie sind praktisch keine Grenzen gesetzt. Wir behandeln dies in anderen Darstellungen, deshalb belassen wir es hier bei diesem Hinweis.

Grundsätzlich kann man aber Folgendes konstatieren: ***eine für alle gültige IT-Architektur und –Lösung gibt es nicht mehr!***

Das hat natürlich massive Implikationen von der Planung bis zur Einäscherung von IT-Systemen. Noch vor wenigen Jahren gab es Wahrheiten, die für einen überwiegenden Teil von Unternehmen planerisch nützlich und sinnvoll waren. Nach diesen haben wir die IT-Infrastruktur aufgebaut und geprägt. Derartige allgemein gültige Wahrheiten verschwinden immer mehr, an ihre Stelle tritt eine massive Flexibilisierung, bei der es am Ende so sein wird wie mit den Autos. Es ist schon heute schwierig, zwei wirklich identische sagen wir VM Golf zu finden. Jeder kann sein Auto bei der Bestellung sehr individuell gestalten und es gibt bestimmt über 100.000 Varianten. Genauso wird es der unternehmensweiten IT ergehen: das massiv flexible Angebot führt zu immer mehr Varianten, nimmt man die Software hinzu, sind es quasi unendlich viele. Und nur wenige davon werden wirklich optimal sein.

Eine mögliche Vorgehensweise - um hier zu Lösungen zu kommen - ist eine klare Strukturierung entlang von Bedarfsfaktoren und dazu passenden Lösungstechnologien.

4. Bedarfs-Faktoren

Wir können in diesem Abschnitt weder alle Bedarfs-Faktoren nennen noch ausdiskutieren. Es sollte aber sichtbar werden, wie man generell vorgehen könnte.

Der offensichtlichste ist sicher Bedarfs-Faktor 1: die Mobilität. Schon heute sind mehr Endgeräte mobil als stationär. Das ist aber nicht der Punkt. Durch die Entwicklungen vor allem in der Hardware hat eine starke Professionalisierung der mobilen Endgeräte stattgefunden. Das findet nicht nur bei Unternehmen, sondern auch bei der Privatkundschaft großen Anklang, wie der Erfolg des neuen iPhone 6+ mit dem deutlich größeren Bildschirm zeigt. Was der Unterhaltung recht ist, sollte den Unternehmen billig sein, denn die neuen Formfaktoren eröffnen auch neue Einsatzgebiete. Der Punkt „BYOD“, über den wir vor zwei oder drei Jahren heiß diskutiert haben, hat sich dadurch erledigt, dass es nicht so sehr auf die Geräte, sondern auf die Integration der mobilen Geräte in Prozesse ankommt. Wer sich noch wenig damit befasst hat, sehe sich einfach die Anwendungen an, die IBM mit Apple zusammen entwickelt und anbietet. Sie wurden für spezielle Anwendungsbereiche teilweise ganz neu entworfen und zeigen eindrucksvoll, was heute mit „passenden“ mobilen Endgeräten möglich ist. Fragen und Problembereiche, die sich hier ergeben, sind neben Anwendungen und deren Integration der wirtschaftliche Betrieb und die Qualität der Infrastruktur, mit der man das kombinierte System unterstützen möchte. Eine ganz wesentliche Rolle spielen hierbei natürlich die nutzbaren Sicherheitsarchitekturen. Hier muss sicherlich in der Zukunft angesichts der allgemeinen Bedrohungslage mehr getan werden als bisher. (siehe Abbildung 6)

Über die Bedeutung der Virtualisierung haben wir bereits gesprochen, das ist aber durchaus der zweite wichtige Bedarfsfaktor. Nach einer gewissen Einführungseuphorie stellt sich der Markt hier als etwas schwierig dar, auch weil sich die Produkte unterschiedlicher Hersteller in vielen Bereichen sehr ähneln. Rein faktisch gesehen ist Virtualisierung eine Betriebssystem-Erweiterung, aber der Hersteller VMware verkauft das ganz anders, eher als eine Art Weltwunder, für das jeder Nutzer entsprechend hohe Lizenzgebühren bezahlen muss. Es gibt durchaus das Problem, dass ganze Projekte durch diese Kosten gefährdet werden können. Am Anfang hat die Einführung der Virtualisierung zu erheblichen Verbesserungen im Betrieb geführt, weil statt der vielen kleinen einige wenige große Server genutzt werden konnten. In einer weiteren Phase sind die zusätzlichen Funktionen wie z.B. zum Lastausgleich oder zum unterbrechungsfreien Betrieb in den Vordergrund gerückt, aber hier wurden auch Grenzen offenbar, z.B. beim Wandern Virtueller Maschinen, denn die VM selbst oder ihre vektorielle Darstellung sind kein gro-

Abbildung 5: Cloud-Alternativen Quelle: Dr. Jürgen Suppan, Com Consult Research GmbH

ßes Mirakel, auch nicht bei der Übertragung, aber am Ziel einer Wanderung sollte eine VM die gleiche Umgebung wieder finden, wie auf der Maschine, wo sie gestartet ist. Das führte letztlich zu der Idee, die Speicher auch zu virtualisieren. Mittlerweile gibt es aber aufgrund neuerer technischer Entwicklungen erhebliche Zweifel daran, ob das noch so sinnfällig ist. Neue 3D-SSD-Speicher müssten, wenn man sie von den Servern trennt, mit multiplen 100 G-Netzen angefahren werden. Vergleichsweise kosten die aber noch soviel wie italienische Sportwagen, das kann sich nicht jedes Unternehmen leisten. Die sog. Konvergierten Netze haben häufig nicht funktioniert, viele Unternehmen verwenden zur Sicherheit immer noch Fibre Channel oder InifiniBand statt FCoE. Außerdem vergibt man unter Umständen Möglichkeiten bei der Einführung neuer Methoden der Arbeit auf Speichern, wie das In-Memory Computing.

Worauf es bei der Weiterentwicklung der Virtualisierung ankommt ist die Frage, wie neue Konzepte aufgenommen und integriert werden können. Ein wichtiges Ziel moderner IT-Infrastrukturen ist der weitest gehend automatisierte Betrieb. Genau das gibt den großen Cloud-RZs einen möglichen wirtschaftlichen Vorteil gegenüber privat betriebenen IT-Infrastrukturen von Unternehmen. Letztlich wird es natürlich so sein, dass Unternehmen private Clouds betreiben, die mit den öffentlichen Clouds verbunden oder vermascht werden, um genau die Dienstleistungen beziehen zu können, die man in der eigenen IT nicht wirtschaftlich darstellen kann. Damit das aber funktioniert, muss das Konzept der Virtualisierung in verschiedenen Punkten erheblich erweitert werden. Dazu gehört die automatische Inbetriebnahme virtueller Applikationen, die Unterstützung einer sicheren Private Cloud und die Unterstützung einer sicheren Öffnung zu vermaschten Cloud-Infrastrukturen.

Das alles führt zu vielen Fragen von der technischen Ausführung der mit immer höherer Leistungsdichte aufweisenden Server-Schränke, der Kommunikation innerhalb der Schränke und zwischen den Schränken, der Anordnung und Lokalisierung der Speicherkomponenten (letztlich zu solchen Ideen wie der Disaggregation im Rahmen einer spezialisierten Architektur wie der Rack Scale Architektur von Intel) und der infrastrukturellen Versorgung bis hin zu Schaffung und Ausbalancierung verschiedener Cloud-Konzepte. Natürlich alles mit höchster Sicherheit und weitest gehend automatischem Betrieb. Es hilft nichts, da müssen alle durch!

Nebenbei schon mehrfach erwähnt, ist die Sicherheit natürlich ein eigenständiger Bedarfs-Faktor. In einer derart dynamischen Phase, wie wir sie heute haben, kann durchaus ein Wildwuchs von Lösungen entstehen, der letztlich immer eine Gefahr für die Sicherheit sein kann. Ein weiterer Trend ist der Ersatz von Geräten mit Spezial-Hardware für sicherheitsrelevante Aufgaben wie Firewalls oder Load Balancer durch Software (Middleware-Boxen). Wir diskutieren ja schon lange über diesen Punkt und die Tendenz zu derartigen Lösungen hat sich stark stabilisiert. Damit entstehen aber wiederum Fragen über Fragen. Soll man Nutzer, Dienste und Komponenten vom Standpunkt der Sicherheit eher gleich behandeln oder eine Selektion durchführen? Kann man eine durch Ereignisse gesteuerte automatische Selektion einführen? Sind die oftmals an statischen Lösungen orientierten Sicherheitssysteme auch für dynamische Architekturen brauchbar? Wie gehen wir mit neuen Risiko-Faktoren um, wie sie im Rahmen der Kopplung mit einer Public Cloud aufkommen? Ist es möglich, für alle Komponenten in Hard- und Software eine übergreifende Architektur mit zentraler Steuerung zu etablieren, die die Einbindung von Sicherheitsfunktionen unterstützt? Kann man die Komplexität insgesamt senken, um die Einführung von Sicherheitsfunktionen zu begünstigen? Was, wenn die Architekturen dynamisch sind? Können neue Ansätze wie SDN hier Hilfen geben oder stellen sie eher neue Problemfelder dar?

Welches Universum an Komplikationen sich selbst durch die zunächst einmal vergleichsweise simple Einführung von Middleware-Boxen ergeben, veranschaulicht [MOA 15] sehr eindrücklich. Generell mit neuen Herausforderungen befasst sich [HOF 15].

Ein weiteres Problem bei welchem der Autor oftmals den Eindruck hat, völlig alleine zu stehen, ist die Frage nach der Zuverlässigkeit oder Authentizität von Software. Macht die Software das, was sie soll? Oder macht sie vielleicht zusätzlich mehr, was uns schaden könnte? Funktioniert sie tatsächlich immer präzise so, wie sie soll? Wenn wir Software „laden“, woher wissen wir dann, ob das genau die Software ist, die wir haben wollen oder nur eine Software, die vorgibt die gewünschte zu sein? Der Hund ist hier in der Gewohnheit begraben. Eigentlich verwenden wir in praktisch allen Bereichen Software, die zu Beginn nur ungefähr das macht, was sie soll. Früher musste man sogar bei PCs Software-Updates, die die relativ schlimmsten Fehler beheben sollten, von Hand einspielen. Da hatte man noch ein Gefühl dafür, wie viel wirklich schief geht. Heute „loadet“ alles automatisch. Ich war letztlich nur eine Stunde bei eBay und hatte wegen der Nutzung von LTE zu diesem Zweck ein kleines Programm mitlaufen, was das übertragene Datenvolumen mitprotokolliert. Mein MacBook hatte sich mal eben 1,6 GByte gezogen, von denen ich bis heute noch nicht einmal erfahren konnte, was das nun war. Was ich damit sagen will, ist, dass wir uns daran gewöhnt haben, fehlerhafte oder unvollständige Software völlig selbstverständlich zu benutzen, weil es ja meistens „gut geht“, warum auch immer.

Betrachtet man dies alles aus dem Blickwinkel der Sicherheit, kommt man schnell zu der Erkenntnis, dass Kommunikationssysteme heute gar nicht wirklich sicher gemacht werden können. Denn dazu müsste die Korrektheit der gesamten eingesetzten Software mathematisch bewiesen werden. Solche Beweise scheitern aber schon für kleine Protokolle und erfor-

dern auch eine sehr strenge Systemsicht. In [KAU 12] erkläre ich diese Problematik genauer. So oder so ist das Ergebnis frustrierend.

Nun könnte man ja sagen, dass eben rein aus der Gewohnheit der Betrieb nicht völlig astreiner Software auf der Ebene der Anwendungen überwiegend unproblematisch ist. Mit Middle-Boxes und SDN werden aber infrastrukturell sensible Funktionen ebenfalls in Software gegossen. Man könnte auch sagen, dass z.B. die Switch-Betriebssysteme der einschlägigen Hersteller auch schon seit Jahrzehnten fehlerbehaftet sind, und es trotzdem „irgendwie“ funktioniert. Ich würde aber gerne anregen, den aktuellen Umbruch als Chance zu sehen, derartige Probleme endlich gründlich zu beleuchten und hier letztlich zu wesentlichen Verbesserungen zu kommen.

Ein weiterer wichtiger Bedarfsfaktor ist eine sinnvolle und verantwortliche Nutzung der Cloud. Wir haben ja in diesem und vergleichbaren Medien schon häufig darüber diskutiert, aber es kommen ja auch immer wieder neue Bereiche dazu. Bis vor rund einem Jahr war die Welt aufgeteilt in private, hybride und öffentliche Cloud. Hier wurden Infrastrukturen, Plattformen oder Software als Service bereitgestellt. Merkmale einer Cloud-Lösung sind Abruf nach Bedarf, Self-Provisioning, Elastizität, Abstraktion, Verfügbarkeit im Netzwerk und Bezahlung nach Verbrauch.

Mittlerweile ist wenigstens die „Hosted Private Cloud“ als Betriebsmodell hinzugekommen, einfach erklärt CaaS, „Cloud as a Service“. Ein wesentlicher Einflussfaktor ist aber auch, dass die Cloud in den letzten Jahren erheblich in den Privatbereich vorgedrungen ist. Wenn Millionen Privatleute ihre Fotos, Filme und sonstigen Erinnerungen einer Public Cloud anvertrauen, wird es immer schwieriger, mit Sicherheits- und Zuverlässigkeitsproblemen bei der Nutzung von Public Cloud-Lösungen durch Unternehmen zu argumentieren. Zertifizierungen und Sicherheit bei Rechtlichen Rahmenbedingungen tun ein Übriges zur Erhöhung der Akzeptanz. Anwendungen, die auf einer Verteilung von Mobilgeräten und zentralisierten Komponenten beruhen, werden ohne Cloud-Konzept problematisch zu betreiben sein.

Der Public Cloud Markt ist in heftiger Bewegung, denn es gab einen „Shake-out“, bei dem die großen Drei Amazon, Google und Microsoft als Gewinner hervorgingen, und alle anderen, sogar Unternehmen wie IBM, sich eine Nische suchen müssen. Das ist an und für sich kein Schaden für mögliche Nutzer, denn die betreffenden Unternehmen müssen in ihren Nischen etwas besonders Attraktives anbieten, wobei es kaum mehr um den Preis gehen kann. Was können solche Nischen sein ? Nehmen wir Cognizant (Nasdaq: CTSH), die kostengünstigen Code für Finanz- und Gesundheitsanwendungen bereitstellt, der wiederum durch Customization von Spezialanbietern in diesen Bereichen genutzt werden kann. Man könnte die Leistung von CTSH auch als „Software Modules as a Service“ SMaaS bezeichnen. Die hierzulande wahrscheinlich völlig unbekannte Firma ist immerhin schon 36 Mrd. US$ wert und zeigt eindrücklich, dass der Phantasie bei Cloud-Konstruktionen keine Grenzen gesetzt sind. Ein weiterer Nischenanbieter ist Veeva Systems (NASDAQ: VEEV), die sich auf die Unterstützung von Pharma-Referenten spezialisiert haben, wobei das über einfache Vertriebsunterstützung weit hinausgeht. Letztlich baut Veeva Informationsnetze zwischen Ärzten und anderen Playern im Gesundheitswesen auf, die neben der Unterstützung bei der Einführung neuer Medikamente zu wesentlichen Verbesserungen für Patienten führen können. Auf diesem Sektor werden wir noch wirklich massive Entwicklungen sehen, das ist genau so heute noch alles Spaß wie beim IoT. Eigentlich ist nur in solchen Nischen auch Geld zu holen, und deshalb finden wir dort auch IBM. Man darf nicht vergessen, dass zu den ältesten Kunden von IBM auch sehr sicherheits-bewusste Organisationen wie z.B. das US-Militär gehören. Umfragen zeigen immer wieder, dass man vor allem IBM zutraut, sichere Lösungen zu bauen, sozusagen eine goldene Eintrittskarte für zukünftige Cloud-basierte Kombinationslösungen, wie sie z.B. mit Apple jetzt etabliert werden, um nur ein Beispiel zu nennen.

Weitere Bedarfsfaktoren liegen natürlich in optimierten Systemen für Kommunikation und Kollaboration. Darauf können wir hier aber schlicht aus Platzgründen nicht mehr eingehen.

5. Konsequenzen für private IT-Infrastrukturen

Wir können das Weiterleben von Moore´s Law für die nächsten 15 bis 20 Jahre durchaus als gesichert betrachten. Es könnte sogar sein, dass sich die bisherige Dynamik etwas verschärft. Es wird eine neue Generation von Mitarbeitern geben, die aufgrund ihrer Geburtsjahr-

gänge völlig natürlich mit allen Instrumenten umgehen, die den aktuellen Generationen noch neuartig und fremd erscheinen.

Eine für alle gültige IT-Architektur und entsprechende Lösungen aus einem Standard-Baukasten gibt es nicht mehr. Der Umbruch ist deutlich härter als der von Host-Systemen auf vernetzte PCs oder der von PC-LANs zu Internet/Intranet-Strukturen. Bei diesen historischen Übergängen hat man sich meist über einen langen Zeitraum damit beholfen, Dinge au der alten Welt in der neuen „nachzumachen“ (z.B. 3270-Emulation und Host-Kopplung im PC-Netz, Virtual Desktop im Internet/Intranet).

Das wird man auch jetzt „irgendwie“ wieder können, aber dabei vergibt man (mit u.U. enormem Aufwand) wirklich spannende Möglichkeiten, die es so vorher nicht gab, wie Mobilität, endlich Benutzer-zentrierte Endgeräte-Gestaltung und natürlich auch die effektive Nutzung praktisch beliebiger Service-Konstruktionen aus der Cloud, die letztlich zu ganz neuen Anwendungen und erheblichen Produktivitätsschüben führen können.

Das ist eine NEUE, ANDERE WELT. Hier stellen sich Fragen, die man mit Techniken der alten Welten kaum beantworten können wird. Neue technologische Ansätze wie SDN und NFV, die vielleicht heute noch als Luxus erscheinen, werden in Zukunft unabdingbar für den Betrieb der Infrastrukturen mit erheblich leistungsgesteigerter Hardware sein.

Nebenbei bemerkt: der Ausbau des Internets, wie wir ihn heute sehen, die mögliche Versorgung Hunderter Millionen privater Endkunden mit Multi-Gigabit-Leistung statt des heutigen behäbigen DSL sowie private und kommerzielle flächendeckende Multi-Gigabit-WLAN-Strukturen als Ergänzung der Mobilnetze wären schon heute ohne SDN und NFV nicht machbar.

Unternehmen müssen sich vermehrt damit auseinandersetzen, in welcher Weise und mit welchen Mechanismen sie ihre Infrastruktur für ihre Anforderungen optimieren möchten. In diesem Artikel haben wir einige Beispiele für Bedarfs-Faktoren genannt. Das war aber nicht einmal die Spitze des Eisbergs, sondern vielleicht das höchstgelegene Eishäufchen, in dem die Fahne steckt. Die Aufgabe wird sein, Anforderungen viel präziser als bisher zu formulieren. Das verlangt nicht nur ein Umdenken, sondern auch viel mehr Kooperation bisher isolierter Mitarbeiter.

Es kann ja durchaus sein, dass ein Unternehmen über Disaggregation diskutiert. Das betrifft aber mindestens alle Netzwerk-, Server- und Speicherleute, die sich bislang vielleicht kaum kennen.

Wenn man versteht, dass diese übergreifende Kooperation die eigentliche Herausforderung ist, kommt die passende Technologie wahrscheinlich ohne größere Hürden.

Es wird am Ende keine zwei gleichen Lösungen mehr geben. Henry Ford sagte: „der Kunde bekommt (für das Modell T) jede Farbe, solange sie Schwarz ist.“ Die Zeiten, in denen IBM oder Microsoft die DV in ähnlicher Weise wie Henry Ford bestimmt haben, sind endgültig vorbei. Es wird bunt!

Literatur

[HOF 15] Hoff, S.: „Neue Herausforderungen für die Netzwerk-Sicherheit“, ComConsult Netzwerk- und IT Infrastruktur-Forum Königswinter 2015

[KAU 12] Kauffels, F.-J. „Sicherheitsprobleme und – Lösungen in Netzen“Wissensportal www.comconsult-research.de, Serie Professionelle Datenkommunikation, ab Teil 49

[MEL 15] Malone, Michael S. : „Millennials Marching to the Quickening Metronome of Moore´s Law“, Intel Innovative Technology Mag.April 2015, iq.intel.com

[MOA 15] Moayeri, B. : „Problematik und Zukunft von Middleboxes“, ComConsult Netzwerk- und IT-Infrastruktur-Forum Königswinter 2015

[MOO 65] Moore, Gordon E.: „Cramming More Components onto Integrated Circuits“, Electronics, 19. April 1965, Faksimile unter http://www.cs.utexas.edu/~fussell/courses/cs352h/papers/moore.pdf

[ROR 15] Rorvic, Mordechai: „Intel: Understanding Multiple Patterning At 14 Nanometers And Below“, seekingalpha.com, May 1, 2015

[SIV 12] Sam Simakuva of Intel talks about Lithography and Patterning, Part 1 to Part 3, YouTube 16.10.2012

[SUP 15] Suppan, J: „2015: Netzwerk- und IT-Infrastruktur-Trends: wohin geht der Weg ?“ Keynote ComConsult Netzwerk- und IT-Infrastruktur-Forum Königswinter 2015

ComConsult Veranstaltungskalender

RZ-RZ-Kopplung - alles nur eine Frage der Bandbreite?, 15.06.15 in Stuttgart

Garantietermin

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

Netzzugangskontrolle: Technik, Planung und Betrieb, 15.06.-17.06.15 in Stuttgart

Garantietermin

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,-- netto

TCP/IP-Netze erfolgreich betreiben, 15.06.-17.06.15 in Nürnberg

Garantietermin

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,-- netto

Aufbau und Management von Internet-DMZ und internen Sicherheitszonen, 15.06.-16.06.15 in Stuttgart

Garantietermin

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

Preis: € 1.590,-- netto

SIP (Session Initiation Protocol) - Basis-Technologie der IP-Telefonie, 15.06.-17.06.15 in Nürnberg

Garantietermin

Ziel der Schulung ist die Erläuterung von SIP als den Schlüssel für eine offene, leistungsfähige und Kosten-optimale Kommunikations-Lösung. Es umfasst nahezu alle Dienste, die wir heute für UC benötigen: Sprache, Video, Daten und Präsenz. Lernen Sie was SIP leistet, worin sich wesentliche Hersteller-Lösungen unterscheiden und wie Sie das Beste aus beiden Welten zukunftsorientiert nach Ihrem Bedarf optimieren.

Preis: € 1.890,-- netto

WAN: Konzept, Planung und Ausschreibung, 15.06.-16.06.15 in Stuttgart

Garantietermin

Ziel der Schulung ist die Erläuterung von SIP als den Schlüssel für eine offene, leistungsfähige und Kosten-optimale Kommunikations-Lösung. Es umfasst nahezu alle Dienste, die wir heute für UC benötigen: Sprache, Video, Daten und Präsenz. Lernen Sie was SIP leistet, worin sich wesentliche Hersteller-Lösungen unterscheiden und wie Sie das Beste aus beiden Welten zukunftsorientiert nach Ihrem Bedarf optimieren.

Preis: € 1.590,-- netto

IT-Kommunikation im Umfeld von Fertigung und Automation, 17.06.15 in Bonn

Garantietermin

Mit der aktuellen Technologie-Entwicklung stellt sich immer mehr die Frage, ob eine klare Trennung zwischen Büro und Fertigung in Zukunft noch erreichbar sein wird. Diese Sonderveranstaltung analysiert wie Fertigungsnetzwerke auf diese Herausforderungen reagieren können und wie mit geeigneten Technologien Sicherheit, Leistung und Flexibilität gewährleistet werden kann.

Preis: € 990,-- netto

Das neue IT-Sicherheitsgesetz, 22.06.15 in Bonn

Garantietermin

Die Veranstaltung soll kompakte und praktische Grundkenntnisse zu den Eckpunkten des von der Bundesregierung kürzlich verabschiedeten IT-Sicherheitsgesetzes vermitteln. Die Adressaten des neuen Gesetzes müssen mit erheblichen Neuerungen in ihrem IT-Betrieb rechnen. Betroffen sind Unternehmen mit IT-Systemen, deren Ausfall gravierende Folgen für das gesellschaftliche Leben haben kann und die daher als „Betreiber kritischer Infrastrukturen“ im Sinne des Gesetzesentwurfes einzuordnen sind.

Preis: € 1.090,-- netto

Sommerschule 2015 - Intensiv-Update auf den neuesten Stand der Netzwerktechnik, 22.06. - 26.06.15 in Aachen

Garantietermin

Die Sommerschule 2015 bringt Sie in 5 Intensiv-Tagen auf den letzten Stand der Netzwerk-, Kommunikations- und Infrastruktur-Technik. Die Themen: IT-Architekturen und Auswirkungen auf LAN und WAN - LAN-Technologien: aktuelle Entwicklungen - Sicherheit - Unified Communications: wo stehen wir? - WLAN und Mobilfunk - IPv6: aktueller Stand bei Unternehmen - Rechenzentren: neue Arten von Infrastrukturen gefordert.

Preis: € 2.490,-- netto

Voice und Video im WAN, 22.06.15 in Köln

Garantietermin

Die Sonderveranstaltung zum Thema PSTN-Migration hin zu All-IP bietet top-aktuelle Informationen und Analysen mit ausgewählten Experten. Eine ausgewogene Mischung aus Analysen, Hintergrundwissen und Projekterfahrungen in Kombination mit Produktbewertungen und Diskussionen liefert das ideale Umfeld für alle Planer, Betreiber und Verantwortliche solcher Lösungen.

Preis: € 990,-- netto

IPv6 Grundlagen - SeminarPlus, 22.06.-23.06.15 in Bonn

Garantietermin

IPv6 betreiben, bedingt IPv6 verstehen. In diesem Seminar werden die Grundlagen des neuen IP Protokolles verständlich und praxisnah vermittelt. Die Schulung richtet sich gleichermaßen an Planer, Betreiber, Administratoren und Software-Entwickler.

Preis: € 1.790,-- netto

Zertifizierungen

ComConsult Certified Network Engineer

Lokale Netze
28.09. - 02.10.15 in Aachen

TCP/IP-Netze erfolgreich betreiben
15.06. - 17.06.15 in Nürnberg
11.11. - 13.11.15 in Bonn

Internetworking
19.10. - 23.10.15 in Aachen

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

ComConsult Certified Trouble Shooter

Trouble Shooting in vernetzten Infrastrukturen
27.10. - 30.10.15 in Aachen

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

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

ComConsult Certified Voice Engineer

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen
28.09. - 30.09.15 in Köln

Session Initiation Protocol Basis-Technologie der IP-Telefonie
15.06. - 17.06.15 in Nürnberg
11.11. - 13.11.15 in Bonn

Umfassende Absicherung von Voice over IP und Unified Communications
19.10. - 21.10.15 in Bonn

Optionales Einsteiger-Seminar: IP-Wissen für TK-Mitarbeiter
14.09. - 15.09.15 in Bonn

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

Basis-Paket: Beinhaltet die drei Basis-Seminare
Grundpreis: € 5.100,-- netto statt € 5.670,-- netto
Optionales Einsteigerseminar: Aufpreis € 1.190,-- netto statt € 1.590,-- netto

Impressum

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

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

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

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