ComConsult Research
Der Netzwerk Insider
Dezember 2012
Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

Werden SDN und OpenFlow herkömmliche Netzwerke verdrängen?
Teil 2

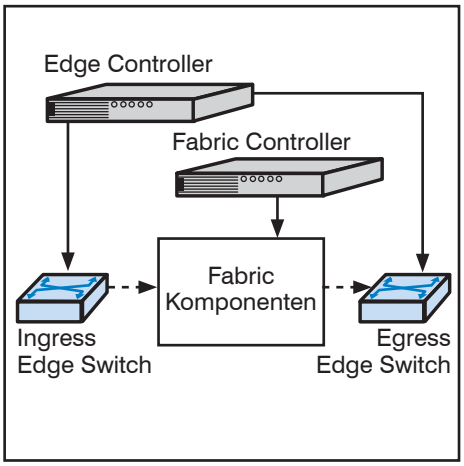
von Dipl.-Inform. Petra Borowka-Gatzweiler

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

Im Folgenden lesen Sie die Fortsetzung des Artikels aus der Ausgabe Oktober 2012)

2.3 Der OpenFlow Channel

Der OpenFlow Kanal (Channel) ist das Interface, das jeden OpenFlow Switch mit einem Controller verbindet. Durch dieses Interface konfiguriert und managt er den Switch, erhält Meldungen vom Switch und sendet Pakete zum Switch. Zwar ist das Interface zwischen Datenbearbeitung und dem OpenFlow Kanal implementierungsspezifisch, jedoch müssen alle Nachrichten, die über den OpenFlow Kanal laufen, konform zum OpenFlow Protokoll formatiert sein. Typischerweise wird der OpenFlow Kanal mit TLS verschlüsselt, er darf jedoch auch direkt über TCP implementiert sein.



weiter auf Seite 8

Zweitthema

Voice, Video und UC ... ein Erfahrungsbericht

von Dr. Krystian Wencel

Voice over IP (VoIP), Video und Unified Communications waren und sind seit Jahren ein großer Migrationstrend des Kommunikationsmarktes. Aussagen wie „... nicht ob, sondern wann ...“ suggerieren vielen Kunden, dass sie eigentlich schon spät dran sind, diese Technologien zu nutzen.

Doch wer trifft diese oder ähnliche Aussagen und wie zuverlässig sind diese „Marktmeinungen“ für den Kunden? Zum einen sind es die Hersteller, die durch Innovation ihrer Produkte gezwungen sind, ihre Marktanteile zu verteidigen bzw. auszubauen. Die Innovatoren unter ihnen fordern heraus, indem sie Bewährtes in Frage stellen. Die Herausgeforderten warten häufig ab, doch dieses Abwarten kostet sie den gnadenlosen Verlust von technologischem Vorsprung und Marktanteilen.

Umsatzgetrieben preisen die Hersteller zahlreiche Vorteile und werben mit Alleinstellungsmerkmalen ihrer Produkte und deren Leistungsmerkmalen (LM). Gestützt durch die großen internationalen Consultingfirmen und Analystenhäuser versprechen sie die Reduzierung von Total Cost of Ownership (TCO), kurze Amortisationszeiten (ROI) und überzeugen so manchen CIO, eine Migration zu initiieren.

weiter auf Seite 21

Geleit

Switches, Router, Firewalls, WLAN: wird alles Software?

ab Seite 2

Standpunkt

Der Rundumschlag: Pauschale Verschlüsselung in WAN/MAN/LAN

ab Seite 19

Aktueller Kongress

Netzwerk-Redesign Forum 2012

ab Seite 4

Neues Seminar

Die Führungskraft in IT und Telekommunikation

auf Seite 6

Zum Geleit

Switches, Router, Firewalls, WLAN: wird alles Software?

Netzwerke stehen in den nächsten drei Jahren vor dem größten Umbruch der letzten 20 Jahre. Die traditionellen Anbieter stellen sich neu auf und bereiten sich auf eine völlig veränderte Marktsituation vor. So hat Brocade gerade die Übernahme von Vyatta angekündigt, Cisco die von Meraki und VMware hat Nicira zum spektakulären Preis von 1,26 Milliarden USD gekauft und Intel droht mit seinen Fulcrum-Produkten der Branche mit dem Einstieg in einen neuen Markt.

Im Kern geht es um drei eigentlich separate Entwicklungen, die sich aber in der faktischen Umsetzung vereinigen und so den Marktdruck erst produzieren:

- Die Zeit der Hardware im Netzwerk-Bereich ist vorbei. Software wird die Zukunft in weiten Bereichen bestimmen. Das verändert nicht nur die Produkte, sondern auch die Betriebsmodelle.

- Cloud Computing erfordert eine neue Form und einen neuen Typ von Netzwerk, um in der Cloud verteilte Ressourcen für Kunden zu einem virtuellen Netzwerk zusammen fassen zu können.

- Mobile Endgeräte explodieren in Anzahl und Nutzungsformen. Der traditionelle Desktop wird in fünf Jahren nicht mehr existieren. Dies erfordert neue Infrastrukturen, die bereits jetzt auf der Herstellerseite entstehen und in 2013 in den Markt gebracht werden.

Wird alles Software? Darunter können wir drei unterschiedliche Megatrends ansiedeln:

- Das extrem schnell wachsende Angebot an virtuellen Appliances wie Switches, Router, Firewalls, IDS/IPS und Load Balancer. Diese spielen sowohl eine tragende Rolle für alle Virtualisierungs- und Cloud-Lösungen, sind aber auch unabhängig davon sehr ernst zu nehmen.

- Der zunehmende Übergang von Hersteller-spezifischen ASICs hin zu Standard ASICs, so dass Hersteller ihre Alleinstellungsmerkmale in der Software suchen.

- Der Trend zur zentralen Kontrolle und Konfiguration von Netzwerken durch Software. Weg von der bisherigen verteilten Autonomie und hin zu einer zentralen Kontrolle.

Aus Sicht des Preis-Leistungs-Verhältnisses ist der Trend zu virtuellen Appliances verbunden mit einem erheblichen Einsparungs-Potenzial in der Beschaffung und im Betrieb (die Hersteller werben in ihren Beispiel-Rechnungen mit bis zu 70% und die Rechnungen sind durchaus plausibel). Die Frage, die sich natürlich aufdrängt, ist, ob eine Lösung auf der Basis einer virtuellen Maschine wirklich mit einer Spezial-Hardware verglichen werden kann. Dazu folgende Anmerkungen:

- Auch bei den Herstellern von Routern setzt sich Standard-Hardware schon seit längerer Zeit durch. In dem nett designten Gehäuse wird also häufig eine „normale“ Hardware-Architektur stecken.

- Der Schlüssel zur Leistung liegt im eingesetzten Betriebssystem und dem direkten Zugriff auf die Hardware inklusive der Netzwerk-Schnittstellen. Aus diesem Grund wird man auch bei einer virtuellen Appliance ein spezielles Betriebssystem mit hoher Realzeit-Leistung brauchen, das dann natürlich die virtuelle Umgebung unterstützen muss. Vyatta ist ein typisches Beispiel für eine solche Lösung.

- Virtualisierungs-Lösungen erreichen heute über 95% der Rechenleistung von nicht-virtualisierten Servern. Es gibt Unterschiede in der Latenz im Netzwerk-Zugriff und beim Jitter. Cisco gibt für sein UCS eine Latenz zwischen virtueller Maschine und Top-of-Rack-Switch von 1,6 usek an, das wird für die meisten Router- und Firewall-Lösungen mehr als ausreichend sein.

- Generell gilt für eine virtuelle Appliance: wenn wenige Verbindungen die Leistungs-Kriterien erfüllen, dann skaliert die gesamte Lösung. Im Bereich von Virtualisierung strebt man nicht den Mega-Server mit Top-Leistung, sondern Parallelisierung von Leistung an. Wenn eine virtuelle Appliance also nur 5000 VPN-Tunnel anstelle von 10.000 kann, dann arbeitet man eben mit mehreren Appliances. Gleiches gilt für den Gesamtdurchsatz, der für eine einzelne Appliance sicher unter den Tera-Bit-Werten der Top-Router liegt. Da sich Appliances aber nahezu unendlich parallelisieren lassen, ist ihre Gesamtleistung in jedem Fall nicht zu unterschätzen.

Interessant wird die Frage „Hardware kontra Software“ bei Hochleistungsgeräten wie Layer-2-Switches. Auch hier hat sich im Bereich der Software viel getan. Noch vor zwei Jahren haben wir den Softswitch im Hypervisor der typischen Virtualisierungs-Lösungen als möglichen Engpass angesehen und nach Lösungen zur Umgehung dieses Soft-Switches gesucht. Inzwischen haben die Softswitches eine sehr hohe Leistung erreicht und kombiniert mit den verschiedenen Varianten der Leistungs-Steigerung hat dies dazu geführt, dass im Virtualisierungs-Bereich die Zukunft eher in der Software als in der Hardware liegt. Einer der Gründe dafür ist die Flexibilität von Software im Vergleich zu Hardware-Lösungen. Ein gutes Beispiel ist hier die von Nicira entwickelte OpenvSwitch-Lösung und das Nicira-eigene Overlay-Produkt, das eine Form von Netzwerk-Virtualisierung in Kombination mit einem (für diese Lösung nicht unbedingt erforderlichen) SDN-Controller schafft. Software-Entwicklungen sind flexibler und schneller als Hardware-Entwicklungen. Und gerade bei der Schaffung von Mehrwerten kann das eine Rolle spielen. Aber natürlich hat Software auch ihre Nachteile, zum Beispiel im Bereich des Nachweises ihrer Fehlerfreiheit (was eben nur sehr bedingt geht).

Jetzt ist klar, dass das Beispiel Softswitch in dem Sinne hinkt, als dass ein Softswitch bei aller Leistungssteigerung nie die Leistung eines modernen Hardware-L2-Switches erreichen wird. Ist hier also das Ende der Software und der sichere Hafen der Hardware erreicht? Wir haben im Markt einen starken Trend weg von Hersteller-spezifischen ASICs hin zu Standards-ASICs, die dann natürlich von allen Herstellern eingesetzt werden.

Switches, Router, Firewalls, WLAN: wird alles Software?

Im Endeffekt kann ein Hersteller mit seinem eigenen ASIC kaum noch einen Leistungsvorsprung gegenüber einem Standard-ASIC schaffen, zum Teil ist sogar das Gegenteil der Fall. Was bleibt den Herstellern übrig? Die Schaffung von Alleinstellungsmerkmalen in der Software. Ein Mittelweg liegt in den programmierbaren ASICs, die in den nächsten Jahren eine hohe Marktbedeutung erlangen werden. Ein normaler ASIC ist einfach nicht flexibel genug, um den Herausforderungen der schnellen Entwicklungen im Netzwerk-Bereich gerecht zu werden. Ein gutes Beispiel ist die Entwicklung von TRILL/SPB in den letzten Jahren.

Die Vollendung der Reduzierung der Hardware-Abhängigkeit liegt in der Reinform des Software-Defined Networking in Kombination mit Open Flow als Protokoll, um spezielle Flow Tabellen in Standard-Switchen zu füllen. Hiermit wird die Intelligenz komplett in den zentralen Controller verlagert und der Switch wird auf die Ausführbarkeit von Flow-Tabellen reduziert. Auch wenn diese Reinform noch sehr weit von der Umsetzung entfernt ist (es fehlen sowohl ein guter Controller, als auch ein passendes Betriebssystem, als auch die notwendigen Funktionsmodule auf dem Controller), so existiert doch inzwischen die Hardware, um diese Vision möglich zu machen.

Die zunehmende Anzahl von Netzwerk-Komponenten und deren geografische Verteilung stellt für viele Unternehmen die Frage des zukünftigen Betriebs und der Konfiguration. Auch unabhängig von SDN besteht der Bedarf nach einer Standort-Übergreifenden Zentralisierung der Steuerung. Damit wären wir beim Beispiel Meraki angekommen. Meraki hat für seine Komponenten eine Cloud-basierende Konfigurations-Lösung entwickelt, die über VPNs mit den einzelnen Komponenten verbunden ist und extrem gut skaliert. Die Lösung ist offenbar so überzeugend, dass Cisco Meraki gekauft hat. In dieser Form von Betrieb und Konfiguration liegt ein Teil der Zukunft von Netzwerken.

Dies sind nur einige Beispiele aus den vielen Paradigma-Änderungen, die wir im Moment beobachten. Die Zeit der Hardware nähert sich dem Ende, die Zeit der Software ist im Kommen. Natürlich musste auch die Hardware bisher mit Software betrieben werden, aber die genannten Beispiele belegen, wie sich hier die Schwerpunkte verschieben.

Dies ist eines unserer zentralen Diskussions-Themen für das ComConsult Netzwerk-Redesign Forum 2013. Und es ist nicht frei von Kontroversen und Kritikpunkten. Aus diesem Grund laden wir zum Forum eine Reihe von führenden Experten zu einer Diskussion ein, um die Frage „Zentrale Steuerung kontra traditionelle verteilte Autonomie“ zu diskutieren. Mit Sicherheit wird dieses Forum eines der spannendsten der letzten Jahre.

Ihr
Dr. Jürgen Suppan

Netzwerk-Redesign Forum 2013:
Switches, Router, Firewalls, WLAN: wird alles Software?
15. - 17.04.13 und Intensiv-Tag 18.04.12 in Bad Neuenahr

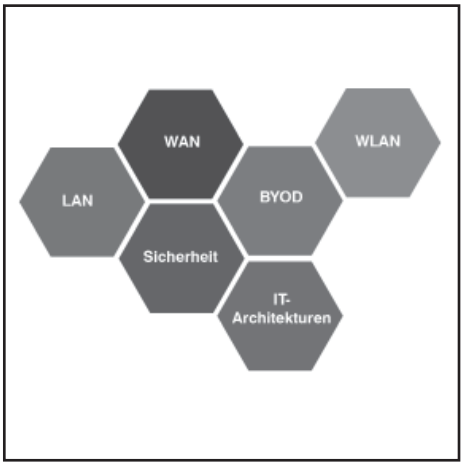
Die ComConsult Akademie veranstaltet vom 15.04. - 17.04.13 ihr "Netzwerk-Redesign Forum 2013" in Bad Neuenahr.

Netzwerke stehen in den nächsten drei Jahren vor dem größten Umbruch der letzten 20 Jahre. Dabei beobachten wir zurzeit vier Megatrends, die sich gegenseitig ergänzen:

- Das extrem schnell wachsende Angebot an virtuellen Appliances wie Switches, Router, Firewalls, IDS/IPS und Load Balancer mit hohen Leistungswerten und einem deutlich besseren Preis/Leistungs-Verhältnis.
- Virtualisierung und Cloud-Technologien generieren neue Architekturen und Betriebsformen, die auch für Unternehmen, die nicht die Cloud nutzen, Auswirkungen haben.
- Der Trend zur zentralen Kontrolle und Konfiguration von Netzwerken durch Software Defined Networking und Cloud Management: weg von der bisherigen verteilten Autonomie und hin zu einer zentralen Kontrolle.
- Mobile Endgeräte explodieren in Anzahl und Nutzungsformen. Ihre Integration erfordert weitreichende Infrastrukturen in allen Bereichen vom WLAN über Routing bis hin zur Sicherheit.

Das ComConsult Netzwerk Redesign Forum stellt diesen Umbruch der Netzwerk-Technologien in den Mittelpunkt der Veranstaltung und analysiert diesen Trend in sechs Themenblöcken:

Block 1: Switches, Router, Firewalls, WLANs: wird alles Software?
Spezial-Hardware und Hersteller-spezifische ASICs haben den Weg in die Gigabit Netzwerke geebnet. Doch die Zeit der Spezial-Hardware ist vorbei. Virtuelle Appliances wie Router und Firewalls (Beispiel Vyatta) auf der Basis moderner Server-Hardware bedrängt traditionelle Produkte. Im Bereich der Highend-Switches lassen Standard ASICs die Hardware-Unterschiede zwischen den Herstellern immer weiter verschwimmen, die



Hersteller drängen mit Macht in die Software, auch um Alleinstellungsmerkmale zu erzielen. Parallel bringen Software Defined Networking und Cloud-based-Management neue Architekturen und Betriebsformen, die den Betriebsaufwand senken und die Betriebssicherheit erhöhen. Wir analysieren für Sie, wo die Software-Reise hingeht und wie sich der Markt in den nächsten Jahren verändern wird.

Block 2: WLAN 2013 bis 2015: Gigabit, aber wie und wofür?
IEEE 802.11ac und 11ad werden den Markt in den nächsten 5 Jahren nachhaltig verändern. Dabei wirft gerade 11ad mit seinen kleinen Zellstrukturen viele Fragen zu einer sinnvollen Nutzung auf. Die Zahl der Teilnehmer in Funknetzen wird explodieren und die heutigen WLAN-Architekturen mit Controllern müssen in Frage gestellt werden. Die zunehmende Zahl der Access Points wird völlig neue Management- und Betriebskonzepte erfordern. SDN und Cloud-based Management gehört hier die Zukunft. Die Übernahme von Meraki durch Cisco ist das beste Beispiel dafür. Wir analysieren für Sie, wie WLAN-Technik in Zukunft aussieht und welchen Herausforderungen wir uns stellen müssen.

Block 3: IPv6: Tunnel ins Nichts: Migration, aber wo anfangen?
Auch wenn die Provider und einige Hersteller bei IPv6 peinlich versagen, der Zug ist nicht mehr aufzuhalten, die Anzahl der Projekte schnellt nach oben. Damit steht die Frage der stufenweisen Migration auch angesichts der starken Zunahme mobiler Endgeräte wieder im Vordergrund. Für die meisten Unternehmen wird kein Weg am zeitweisen Parallelbetrieb vorbei gehen. Aber wie und was tun, wenn Dual-Stack nicht geht? Und wie ausgereift sind die verfügbaren Tunnel-Technologien? Und welche Rolle spielen Spezialbereiche wie SIP? Wir analysieren für Sie wie die optimale Migration aussieht und welchen Reifegrad Tunnel-Verfahren für den Parallelbetrieb erreicht haben.

Block 4: Mobile Endgeräte: Das Ende des Desktops? Wie sieht unsere Zukunft aus?
Smartphones, Tablets und Laptops halten Einzug in die Unternehmen und verdrängen traditionelle Endgeräte. Dabei entstehen gleichzeitig viele neue Nutzungsformen, und neue Anwendergruppen müssen integriert werden. Wie ist mit dem extremen Mengengerüst umzugehen und was steht uns in den nächsten Jahren bevor? Wir analysieren für Sie, welche Rolle mobile Endgeräte für Ihre Infrastrukturen spielen werden und worauf Sie vorbereitet sein müssen.

Block 5: Verkabelung am Arbeitsplatz: alles neu, alles anders?
Und wieder einmal stehen Kabel im Brennpunkt. Zum Teil, weil Kunden noch alte Vierdraht-Verkabelungen betreiben, zum Teil, weil speziell IEEE 802.11ad die Frage nach der Integration vieler neuer Access-Points aufwirft. Verschwindet die Endgeräte-Verkabelung in den Büros und werden Mini-Access-Points der Standard? Wie werden diese verkabelt, wenn Datenströme von mehr als ein Gigabit anfallen? Führt der Bedarf nach Datenraten jenseits der 1 Gigabit für die Access Points zu einer Wiederbelebung des Themas „Glasfaser zum Arbeitsplatz“? Wir analysieren für Sie, wie die Zukunft der Tertiär-Verkabelung inklusive der Infrastrukturen für WLANs aussieht.

Block 6: Sicherheit: Software, Virtualisierung und Mobilität: hat die traditionelle Sicherheit ausgedient?
Der Trend zur Virtualisierung im Rechen-

zentrum und hin zu virtuellen Appliances in Kombination mit der Explosion mobiler Endgeräte hat direkte Auswirkungen auf alle Sicherheits-Konzepte. Wir analysieren für Sie, wo die bisherige Technik an ihre Grenzen stößt und wie zukünftige Lösungen aussehen können.

Streitthema/Podiums-Diskussion: Was ist besser: Zentrale Software-Steuerung oder traditionelle verteilte Autonomie?
Podiumsdiskussion mit eingeladenen Spezialisten zum aktuell heißesten Thema der Branche, das wie kein anderes das Gesicht der Netzwerke verändern kann.
Selten gab es so viele Neuerungen in so kurzer Zeit. Nie zuvor mussten sich alle Hersteller innerhalb weniger Jahre neu positionieren, und nie zuvor wurden bestehende Marktstrukturen und Marktanteile so intensiv in Frage gestellt wie jetzt. Anbieter wie Brocade und HP wittern ihre Chance, endlich in den Markt von Cisco eindringen zu können. Marktfremde Anbieter wie Intel und VMware sehen in Netzwerken mittlerweile ein Allgemeingut, das nicht mehr den Spezial-Anbietern überlassen werden muss. Cisco wiederum setzt seinerseits Zeichen für die Zukunft mit spektakulären Übernahmen. Es wird richtig spannend.

Das ComConsult Netzwerk_Redesign Forum 2013 ist der perfekte Kongress zu einem optimalen Zeitpunkt, um sich über diese hochspannenden Entwicklungen zu informieren. Wie in jedem Jahr so trifft sich auch in 2013 hier die Branche, um die heißesten Trends mit Top-Spezialisten zu diskutieren.

Frühbucherphase bis zum 31.12.2012

Für Besucher unserer bisherigen Kongresse bzw. für die Teilnehmer am VIP-Verteiler bieten wir Ihnen exklusiv eine Vorbuchungsphase für das Netzwerk-Redesign Forum 2013 bis zum 31.12.2012 für eine rabattierte Teilnahmegebühr an. Die Buchung innerhalb der Frühbucherphase ist verbindlich, kann aber jederzeit auf einen anderen Mitarbeiter Ihres Unternehmens übertragen werden.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
ComConsult Netzwerk-Redesign Forum 2013

Ich buche den Kongress
ComConsult Netzwerk-Redesign

Kongress mit Intensiv-Tag
☐ vom 15.04. - 18.04.13 in Bad Neuenahr
zum Preis € 2.290,-- netto*

Kongress ohne Intensiv-Tag
☐ vom 15.04. - 17.04.13 in Bad Neuenahr
zum Preis € 2.090,-- netto*

Ich buche nur den **Intensiv-Tag**
☐ am 18.04.13 in Bad Neuenahr
zum Preis € 790,-- netto*

***gültig bis zum 31.12.2012**

☐ Bitte reservieren Sie mir ein Zimmer

vom _____ bis_____ 13

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

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

Neues Seminar

Die Führungskraft in IT und Telekommunikation

Werkzeuge zur Mitarbeiterführung effektiv und stressfrei nutzen

Die ComConsult Akademie veranstaltet vom 08.04. - 09.04.13 ihr neues Seminar "Die Führungskraft in IT und Telekommunikation" in Aachen.

Die Führungskraft in der IT oder Telekommunikation steht unter Strom – und zwar an vielen Spannungsfeldern: zum einen wird man mit hohen Zielvorgaben konfrontiert und zum anderen verlangen Mitarbeiter Aufmerksamkeit für ihre Bedürfnisse. So kostet nicht nur manch schwieriger Mitarbeiter viel Energie, auch müssen die oft zahlreich eingesetzten Externen koordiniert – also geführt werden.

Eine weitere Herausforderung beim Führen im Bereich IT/Telekommunikation ist der zunehmende Einsatz technischer Medien und Plattformen zur Verteilung der Aufgaben und zum gegenseitigen Austausch von Informationen. Hier gilt es, auch mit Blick auf Organisation und Kommunikation (= Management) den optimalen Nutzen für sich und alle Mitarbeiter zu erzielen.

Sie erhalten einen Überblick über Best Practices in Mitarbeiterführung in den Bereichen IT und Telekommunikation. Die vorgestellten Führungsaufgaben und Werkzeuge, die sich an dem Modell von F. Malik orientieren, können Sie in Ihrem beruflichen Umfeld uneingeschränkt einsetzen.

Dieses Seminar richtet sich in den Bereichen IT und Telekommunikation an Führungskräfte aller Ebenen, auch Projektleiter und Mitarbeiter, die sich auf eine Führungsaufgabe vorbereiten.

In diesem Seminar lernen Sie
- wie gute Führung in IT/Telekommunikation funktioniert
- welche Aufgaben eine Führungskraft in IT/Telekommunikation hat
- welche Werkzeuge (Tool-Box) eine Führungskraft in IT/Telekommunikation zur Verfügung stehen
- wie Sie als Führungskraft hiermit erfolgreich sind

Der Referent Dr. Ralf Hillemacher ist Inhaber der Unternehmensberatung Hillemacher Consulting, war 12 Jahre Aufsichtsratsvorsitzender des IT-Unternehmens FirstAttribute AG und ist in Industrie und Verwaltung ein gefragter Referent und Management-Trainer.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Die Führungskraft in IT und Telekommunikation

Ich buche das Seminar

Die Führungskraft in IT und Telekommunikation

☐ vom 8.04. - 09.04.13 in Aachen
zum Preis von € 1.590,-- netto

☐ Bitte reservieren Sie mir ein Zimmer

vom _____ bis_____ 13

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

_____ Vorname

_____ Nachname

_____ Firma

_____ Telefon/Fax

_____ Straße

_____ PLZ,Ort

_____ eMail

_____ Unterschrift

ComConsult-Study.tv

Foto-Spezial im Dezember bei ComConsult-Study.tv

Nicht nur unterm Weihnachtsbaum werden Fotos geschossen. Auch im Unternehmen wird immer wieder Bildmaterial benötigt, sei es für Marketing oder PR Zwecke, sei es für Präsentationen, interne Dokumente oder Firmenfeiern. Sind wir ehrlich: lässt man dafür keinen Fotografen kommen oder hat das Glück einen ambitionierten Hobbyfotografen in der Abteilung zu haben, ist kaum eines der Fotos nachher verwertbar. In diesen beiden Videos erläutert Ulrike Häßler die Grundlagen der digitalen Fotographie. Sie erklärt, was gute Fotos ausmacht und stellt für verschiedene Situationen einfache Rezepte vor diese zu machen.

Monitore kalibrieren und profilieren
Referentin: **Dipl.-Inform. Ulrike Häßler**
Zeit: 00:29:08
Einzelpreis: 39,00 € netto
Im Abo: kostenlos

Die korrekte Farbwiedergabe von Monitoren ist für die Erstellung von Präsentationen, von Werbematerial oder für die Bearbeitung von Fotos von entscheidender Bedeutung. Aber häufig liegen Erwartungen und Ergebnisse weit auseinander. Woran liegt das?

Fotografieren für PR und Marketing
Referentin: **Dipl.-Inform. Ulrike Häßler**
Zeit: 03:39:13 gesamt
Einzelpreis: 59,00 € netto
Im Abo: kostenlos

Fotografieren im Unternehmen generiert besondere Herausforderungen. Sei es auf einer Veranstaltung, beim Besuch von Gästen oder bei Personen-Aufnahmen. Lernen Sie in diesem Video-Seminar die bewährten Rezepte erfolgreicher Fotografen für dieses Umfeld kennen. Lernen Sie wie Sie sicher und schnell überzeugende Fotos für Ihre Website, Ihre Marketing-Unterlagen oder andere Werbemittel erzeugen können.

Das Bundle dieser zwei Videos kostet nur € 69,--* netto
*Statt regulärer Preis € 98,-- netto. Dieses Angebot gilt nur im Dezember 2012.

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

Schwerpunktthema

Werden SDN und OpenFlow herkömmliche Netzwerke verdrängen?

Teil 2

Fortsetzung von Seite 1

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

Für die Controller ← → Switch Kommunikation gibt es drei Nachrichtentypen:

- Controller-Switch-Messages, die der Controller initiiert
- Asynchrone Messages, die der Switch initiiert
- Symmetrische Messages vom Controller zum Switch und entsprechende Rückantwort, z.B. Hellos, Echo/Reply oder ähnliche

Controller - Switch Nachrichten
Controller - Switch Nachrichten initiiert immer der Controller, der Switch sendet gegebenenfalls eine Antwort. Es gibt verschiedene Nachrichtentypen: Der Feature-Request fragt Funktionen eines Switches ab, üblicherweise beim Verbindungsaufbau des OpenFlow Channels. Der Switch muss den Feature Request beantworten. Die Configuration Nachricht fragt Konfigurations-Parameter vom Switch ab oder setzt diese neu fest. Die Read-State Nachricht liest verschiedene Informationen vom Switch aus wie aktuelle Konfiguration, Statistiken und Features/ Funktionen. Die Modify-State Nachricht betrifft die OpenFlow Tabellen und fügt Flow- oder Gruppen-Einträge hinzu, löscht oder ändert vorhandene Einträge.

Den Packet-out Befehl nutzt der Controller, um den Switch Pakete auf einen bestimmten Switch-Port senden zu lassen, die er vorher mit Packet-in Nachrichten vom Controller (als Kopie) erhalten hat. Die Packet-out Nachrichten enthalten hierfür die Paket-Referenz oder die Puffer-Referenz für das Paket, das der Switch puffert, bis er die Controller-Direktive empfängt. Die Packet-Out Nachricht enthält zusätzlich die Aktionen, die der Switch für dieses Paket ausführen soll. Eine "leere" Aktions-Liste führt zum Verwerfen des Pakets. Den Barrier-Request nutzt der Controller, um bei Nachrichten, die zueinander Abhängigkeiten haben, entsprechende Zwischenantworten vom Switch zu erhalten.

Der Role-Request kommt zum Einsatz, wenn es für einen Switch mehrere Controller gibt und einer von diesen die Rolle des OpenFlow Kanals zu diesem Switch festlegen will (zum Beispiel auf "gleichwertig", Master oder Slave). Die Asynchrone-Konfigurations-Nachricht nutzt ein Controller, um zusätzliche Filter auf die asynchronen Nachrichten zu setzen, die er auf seinem OpenFlow Kanal erhalten will, oder um diese Filter abzufragen. Auch dieser Nachrichtentyp kommt zum Einsatz, wenn mehrere Controller im Spiel sind.

Asynchrone Nachrichten
Switches können eigeninitiativ Nachrichten zum Controller senden, zum Beispiel bei Erhalt bestimmter Pakete, bei Zustands-Änderungen oder Fehlermeldungen; aber auch alle Pakete, mit denen ein Switch nichts anfangen kann oder die keinen Match auf einen Flow Eintrag haben.

Packet-in Nachrichten stehen hier natürlich an erster Stelle: Für alle Pakete, die der OpenFlow Switch aufgrund von Flow Einträgen oder aufgrund des "Table-Miss Flow Eintrags" an den reservierten Port "Controller" sendet, nutzt er Packet-in Nachrichten. Ein Packet-in kann als Output Aktion von einem Flow Eintrag ausgelöst werden oder kann in der Switch-Konfiguration spezifiziert sein. Üblicherweise wird der Switch das Paket so lange puffern, bis er vom Controller eine Antwort erhält, was mit dem Paket geschehen soll. Das hat den Vorteil, dass er nicht das gesamte Paket zum Controller senden muss sondern nur einen Teil des Headers (Default = 128 Byte) zuzüglich einer Puffer-ID als Referenz zum Wiederauffinden des Paketes durch den Switch, wenn die Controller-Antwort eintrifft und der OpenFlow Switch die endgültige Paketbearbeitung durchführen muss.

Flow-Removed Nachrichten sind eine Rückantwort an den Controller, der zuvor eine Modify-State Nachricht mit einem Delete Request gesendet hat. Port-Status Nachrichten informieren den Controller über eine Änderung an einem Switchport. Der Switch sendet Port-Status Nachrichten, wenn sich die Portkonfiguration (zum Beispiel Shut Down) oder der Port-Status ändert (zum Beispiel Link Down).

Symmetrische Nachrichten
Symmetrische Nachrichten sendet entweder der Controller oder der Switch in beliebiger Richtung, ohne vorherige Anforderung von der Gegenseite. Hello Nachrichten tauschen der Switch und der Controller beim Verbindungsaufbau aus. Echo Requests implementieren den alive Mechanismus und werden wahlweise vom Switch oder vom Controller gesendet, die Gegenseite muss sie mit einem Echo Reply beantworten. Echo Requests müssen jedoch nicht nur für die "Up and running"-Prüfung genutzt werden, sie können auch zur Delaymessung oder Bandbreitenmessung eingesetzt werden.

Experimeter Nachrichten sind eine standardisierter Möglichkeit für OpenFlow Switches, um zusätzliche OpenFlow Nachrichtentypen zu nutzen. Hierdurch erhalten die Hersteller - oder auch die Standardisierer - Möglichkeiten für zukünftige OpenFlow Weiterentwicklungen, die nicht alle Produkte unterstützen müssen, können oder sollen.

Nachrichten-Bearbeitung
Das OpenFlow Protokoll nutzt zwar einen zuverlässigen Protokolldienst für Übermittlung und Bearbeitung, aber es stellt NICHT automatisch einen Quittungsme-

Werden SDN und OpenFlow herkömmliche Netzwerke verdrängen? - Teil 2

chanismus (ACK) oder eine geordnete Reihenfolge bei der Übermittlung der Pakete sicher. Auch der Totalausfall der physischen Controller = Switch Verbindung wird zuerst einmal nicht abgedeckt.

Switches müssen eine Controller-Nachricht vollständig bearbeiten. Gelingt ihnen das nicht, müssen sie eine Fehlermeldung zurücksenden. Bei Packet-out Nachrichten bedeutet dies jedoch nicht, dass das Paket auch noch im Switch vorhanden sein muss, es kann nämlich schon aufgrund von Pufferüberläufen verworfen worden sein, bevor die Packet-out Antwort des Controllers beim Switch eintrifft. In diesem Fall bearbeitet der Switch die Packet-out Nachricht vollständig, hat das Paket zuvor mit "silently drop" verworfen, und er muss hierüber nicht zwingend eine Meldung an den Controller senden.

Natürlich müssen Switches alle asynchronen Nachrichten über Status-Änderungen an den Controller senden, damit die Controller-Sicht auf den Switch deckungsgleich mit dem tatsächlichen Switch-Status ist. Solche Nachrichten können jedoch durch eine Asynchronous-Configuration am Controller ausgefiltert werden. Zusätzlich können Bedingungen, die eine OpenFlow Zustandsänderung auslösen würden, schon vorher am Switch ausgefiltert werden: beispielsweise kann ein Paket, das auf einem Port empfangen wird, für den eine Weiterleitung zum Controller konfiguriert ist, schon vorher aufgrund eines Pufferüberlaufs verworfen werden, so dass alle Output Aktionen, die dieses Paket getriggert hätte, unterbleiben.

Um Denial-of-Service Attacken gegen den OpenFlow Controller zu vermeiden, empfiehlt die OpenFlow Spezifikation den Herstellern, eine Ratenlimitierung zu implementieren, die jedoch in der OpenFlow Spezifikation selbst "out of scope" ist.

Die Reihenfolge von OpenFlow Nachrichten und deren Bearbeitung kann durch Barrier-Nachrichten erzwungen werden. Fehlen solche Barrier-Nachrichten, kann der Switch die Bearbeitungs-Reihenfolge beliebig ändern, um seine eigene Leistung zu optimieren. Insbesondere darf der Switch Flow Einträge in einer anderen Reihenfolge einfügen, als der Controller die Flow-Mod-Nachrichten gesendet hat.

Die OpenFlow Channel Verbindungen

Typischerweise handhabt ein OpenFlow Controller viele OpenFlow Kanäle, nämlich zu jedem Switch einen. Es ist jedoch immer der Switch, der die Verbindung zum Controller initiiert. Der Verbindungs-Aufbau läuft wie üblich über die IP-Adresse des Controllers, die im Switch konfiguriert wurde. OpenFlow nutzt den TCP Port

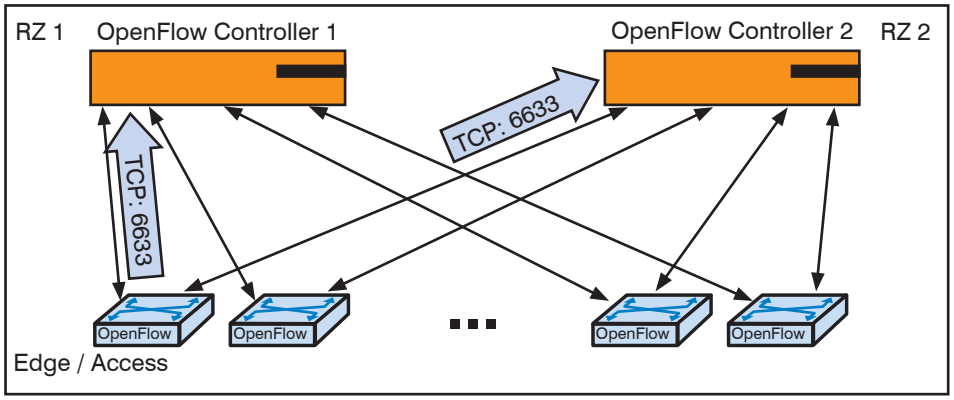


Abbildung 2.11: OpenFlow Kanäle zwischen Controllern und Switches

6633 für TLS-Verbindungen. Ein OpenFlow Switch kann eine Verbindung zu einem singulären Controller oder aber mehrere OpenFlow Verbindungen zu redundanten Controllern halten. Zu einem einzelnen Controller hält der Switch aber immer nur einen einzelnen OpenFlow Kanal (siehe Abbildung 2.11).

Der OpenFlow Controller managt den Switch im Regelfall remote über eine TCP/IP Infrastruktur, die in der OpenFlow Spezifikation als gegeben betrachtet und nicht näher spezifiziert wird. Dies kann zum Beispiel als Inband- oder OOB-Management implementiert sein.

Bei Nutzung von TLS authentizieren sich der Switch und der Controller gegenseitig durch Austausch der Zertifikate und eines standort-spezifischen Privaten Schlüssels. Jeder Switch muss daher mit zwei Zertifikaten konfigurierbar sein, eines für die Authentisierung des Controllers und eines für seine eigene Authentisierung gegen den Controller.

Mehrere Controller

Hält der Switch Verbindungen zu mehr als einem Controller, so erhöht dies natürlich die Verfügbarkeit des OpenFlow Netzwerks, da OpenFlow auch weiterlaufen kann, wenn einer der Controller ausgefallen ist. Ein Failover zwischen zwei hot standby Controllern ist komplett herstellerspezifisch implementiert und in der OpenFlow Spezifikation out of scope. So sind alle entsprechend schnellen Schaltverfahren und auch active-active Konfigurationen (Load Balancing) heutiger Hersteller-Lösungen möglich. Auch zum Thema Virtualisierung der Controller (lauffähig als VM) äußert sich die OpenFlow Spezifikation nicht weiter.

Wurde der Switch so konfiguriert, dass er OpenFlow Verbindungen zu mehreren Controllern hält, so muss er weitestmöglich versuchen, alle diese Verbindungen stets parallel aufrechtzuerhalten. Sendet einer der Controller einen Request an den Switch, so muss die resultierende Antwort oder Fehlermeldung natürlich über genau denselben OpenFlow Kanal zurück gesendet werden. Muss der Switch eine asynchrone Nachricht an mehrere Controller senden, so kopiert er sie entsprechend.

Die Default-Rolle aller Controller ist "Equal". In dieser Rolle hat ein Controller konfigurierenden Zugriff und erhält

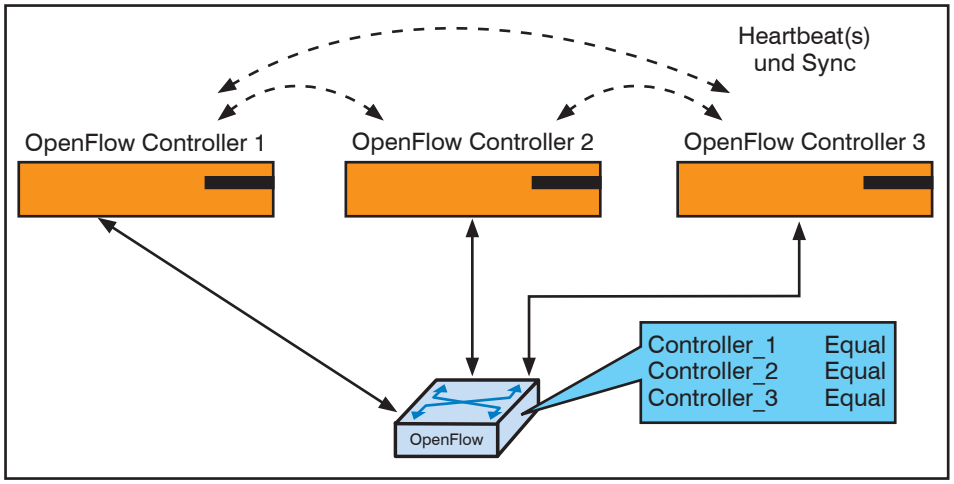


Abbildung 2.12: Mehrere OpenFlow Controller mit der Rolle "Equal"

Werden SDN und OpenFlow herkömmliche Netzwerke verdrängen? - Teil 2

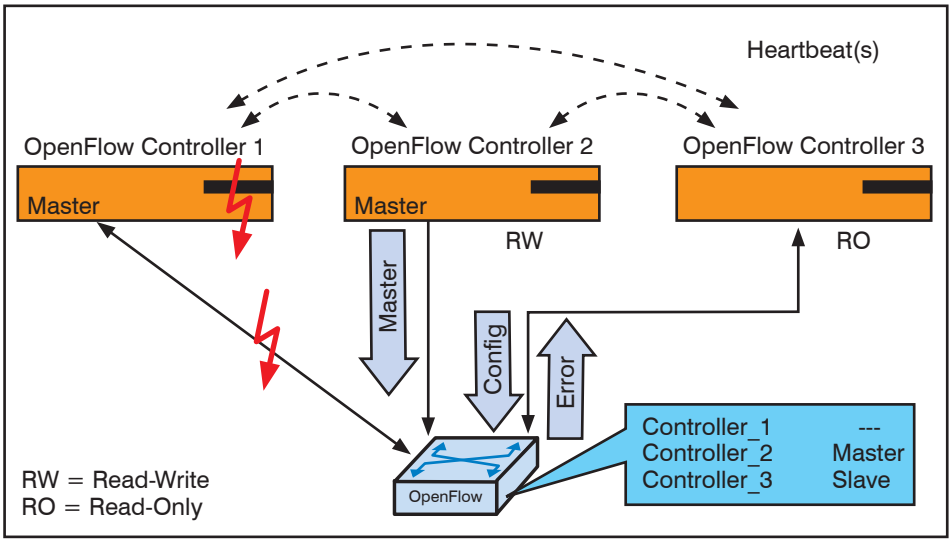


Abbildung 2.13: OpenFlow Controller Failover und Rollenwechsel von Slave auf Master

alle asynchronen Nachrichten (siehe Abbildung 2.12). Ein Controller kann seine Rolle in "Slave" ändern, dann hat er nur Read-Only Zugriff auf den Switch (bei active-standby Redundanz-Konfigurationen) und erhält auch keine asynchronen Nachrichten mit Ausnahme von Portstatus-Nachrichten. Versucht ein Slave-Controller einen konfigurierenden Zugriff auf einen Switch, so erhält er eine Fehlermeldung zurück. Haben mehrere Controller die Rolle "Equal", so müssten diese sich natürlich über getätigte Konfigurationen gegenseitig informieren. Eine solche Synchronisierung wird definitiv nicht vom Switch durchgeführt, und Controller-Controller Synchronisierung ist in der aktuellen OpenFlow Version out of scope.

Das Gegenstück zur Slave-Rolle ist die "Master" Rolle, die ein Controller beim Switch anmelden kann, mit der er den vollen Zugriff auf den Switch hat und gleichzeitig der einzige Controller mit diesem Zugriff ist. Der Switch muss dann in jedem Fall sicherstellen, dass alle anderen Controller die Slave Rolle haben. Hierfür ändert er ohne Benachrichtigung der betroffenen Controller die Rolle der anderen Controller auf "Slave" – im Regelfall sind diese dann nicht mehr erreichbar. Ein Slave Controller hat nur lesenden (RO), keinen konfigurierenden (RW) Zugriff auf den Switch. Versucht ein Slave Controller einen konfigurierenden Zugriff, so erhält er eine Fehlermeldung vom Switch zurück (wie in Abbildung 2.13 dargestellt).

2.4 OpenFlow und andere Overlay-Technologien

OpenFlow ist eine Overlay Technologie, bei der der zentrale Controller mit Hilfe des Kontrollkanals (TLS/TCP/IP-Enkapsulierung der Kontrollpakete) Netzwerk-Komponenten steuert und so logische Strukturen auf der Basis des physikalischen Netzwerks implementieren kann.

Insbesondere zur Lösung des VLAN-Problems (max. 4096 eindeutige VLANs) im Ost-West-Verkehr als auch des Mandantenproblems gibt es weitere Overlay-Technologien beziehungsweise Tunneltechniken, die sich aktuell im Markt etablieren wollen oder dies schon getan haben.

Hierzu zählen
- VXLAN (Virtual eXtended LAN)
- NVGRE (Network Virtualization using Generic Routing Encapsulation)
- STT (Stateless Transport Tunneling)
- LISP (Locator/ID Separation Protocol, IETF LISP WG Draft 24, Nov. 2012; ursprünglich Cisco)
- GRE (Generic Routing Encapsulation)
- MPLS (Multi-Protocol Label Switching)
- PBB (Provider Backbone Bridging)
- SPBM (Shortest Path Bridging MAC)
- CAPWAP (Control and Provisioning of Wireless Access Points) oder proprietäre Alternativen im WLAN Bereich

Brocade und Nicira definieren diese Overlay Technologien zum Beispiel als "SDN für die Data Plane".

Wie geht OpenFlow mit der Integration solcher Overlay-Technologien um? Wenn sie die OpenFlow Spezifikation v1.3 lesen, gar nicht. Nehmen wir das Beispiel VXLAN: Laut VMware ist VXLAN irgendwo zwischen dem Hypervisor und dem vSwitch angesiedelt. Wenn wir OpenFlow mit dem vSwitch assoziieren, ist VXLAN außen vor und der Administrator muss VXLAN über das Hypervisor Management zusätzlich zu OpenFlow konfigurieren. Nehmen wir die Definition von Nicira, werden Virtualisierungs-Overlays "along the network edge, generally within the vswitch" implementiert. Insofern kann ein Virtualisierungs-Overlay über eine OpenFlow Controller Anwendung implementiert sein, muss aber nicht: Der vSwitch kann das Overlay-Netz auch ohne OpenFlow implementieren.

Betrachten wir VXLAN aus der Paket-Sicht, so ist es ein UDP/IP Paket mit einer well-known Portnummer (auch wenn die von IANA noch festzulegen ist). Da der OpenFlow Controller im Switch sowohl Weiterleitungs-Regeln auf der Basis von TCP/UDP Portnummern und IP-Adressen als auch Regeln zur Paket-Manipulation (wie das Einfügen eines VXLAN Headers) konfigurieren könnte, könnte ein OpenFlow Controller eine Anwendung haben, die die Arbeitsweise von VXLAN nachbildet. Diese Anwendung ist jedoch im OpenFlow Standard keinesfalls spezifiziert.

Gleichartig verhält es sich mit allen anderen oben genannten Overlay Technologien bis auf PBB, SPBM und allenfalls CAPWAP, diese sind eindeutig Layer-2 Technologien. Aber auch sie sind in der OpenFlow Spezifikation v1.3 nicht speziell berücksichtigt.

2.5 Versions-Unterschiede

Viele Hersteller unterstützen mit ihren Produkten erst die Version 1.0.0 oder 1.1.0, während aktuell schon die Version 1.3.1 verabschiedet ist (September 2012).

Das bedeutet: Alle Produkte, die nur Version 1.0 unterstützen, leisten die später erarbeiteten Erweiterungen nicht.

Einige wesentliche Versionsunterschiede sind im Nachfolgenden zusammengefasst (siehe auch Teil 1 dieses Themas zur Beschreibung der Features).

Version 1.1.0

Die OpenFlow Version 1.1.0 (Februar 2011) brachte das Pipeline Processing, Version 1.0.0 geht noch von einer singulären Flow Tabelle im Switch aus. Daher: vergessen Sie im Wesentlichen alle Produkte, die v1.0.0 unterstützen, die arbeiten mit deutlich eingeschränkten Bordmitteln. Auch die Gruppentabellen entstanden in v1.1.0, ebenso wie Ein- und Ausfügen von VLAN Tags und MPLS Tags, zusätzlich das Konzept "Virtueller Port". Die Handhabung eines Controller-Ausfalls wurde vereinfacht: Der Switch arbeitet entweder mit seiner aktuellen Flow Tabelle einfach weiter oder fällt zurück in seine Standard-Arbeitsweise (d.h. klassisches Ethernet Switching ohne Controller).

Version 1.2.0

Version 1.2.0 brachte die flexible Paket-Match-Struktur OXM (OpenFlow Exten-

Werden SDN und OpenFlow herkömmliche Netzwerke verdrängen? - Teil 2

sible Match) auf der Basis von TLV (Type Length Vektoren), vorher war diese statisch. Die Rewrite-Möglichkeiten des Paket-Headers, die Inhalte der "Packet-In" Nachrichten und die Fehlermeldungen wurden erweitert. Anfängliche IPv6 Unterstützung kam hinzu. Parsing Vorschriften für die Paketbearbeitung wurden aus der Spezifikation herausgenommen. Der Einsatz mehrerer Controller für Fehlertoleranz sowie die nötigen Mechanismen zur Änderung von Controller-Rollen (Equal, Master, Slave) wurden neu spezifiziert.

Version 1.3.0
Version 1.3.0 brachte erweiterte Capability Negotiation und verbesserte Möglichkeiten, die Flow-Tabellenfunktionen zu beschreiben. Das Statistik Framework wurde durch das "Multipart" Framework ersetzt und kann jetzt sowohl zur Festlegung von Statistiken als auch Tabellen-Funktionen genutzt werden. Per Flow Messungen für Statistiken sind neu, ebenso die Festlegung einer Messdauer / eines Messintervalls. Die Paketbearbeitung bei einem "Table Miss" (ein Paket hat keinen Match) wurde erweitert: Vorher gab es drei Flags für 3 Miss-Bearbeitungsvarianten, jetzt kann ein Table-Miss Flow Eintrag beliebige Aktionen festlegen. Matches auf Extension Header ließen sich bis v1.2.0 sich nicht konfigurieren. Ab Version 1.3.0 sind Matches auf gängige IPv6 Extension Header unterstützt:

- Hop-by-Hop
- Router
- Fragmentation
- Destination Options
- Authentication
- Encryptid Security Payload
- No Next Header
- Extension Header Out of preferred Order
- Unexpected Extension Header

Weitere neue Funktionen sind: Separate Event Filter im Switch je Controller-Verbindung, MPLS BoS Bit Matches (Bottom of Stack) und PBB Tagging. Die strikte Reihenfolge von Tags wurde aufgehoben (bis v1.2.0 stand z.B. der MPLS Shim Header immer hinter allen VLAN Tags). Die Tag-Reihenfolge wird jetzt durch die Reihenfolge der Tagging Operationen bestimmt.

2.6 Zielsetzungen von OpenFlow

Nachdem nun die Funktionen und Arbeitsweise von OpenFlow (grob!) beschrieben wurden, können wir uns darum kümmern, welche Zielsetzungen die Treiber dieser Technologie mit OpenFlow erreichen wollen. Wie so oft haben verschiedene Hersteller und Provider hier verschiedenste Zielsetzungen im Auge. Nachfolgend wird der Versuch unternommen, diese zusammenzufassen.

OpenFlow als eine / erste SDN Instanzierung hat dieselbe Zielsetzung wie SDN (Zitat aus Teil 1): "OpenFlow will den bislang proprietären Control Plane Konzepten ein Ende bereiten: Die Control Plane wird aus den Netzkomponenten auf eine zentrale Steuerungs-Elemente ausgelagert. Hierdurch wird sie für den Betreiber (mittels remote Software Clients) zugreifbar und programmierbar".

Die Väter von OpenFlow hatten die Idee, völlig neue Netze, vielleicht sogar völlig neue Protokoll-Alternativen zu IP und gängigen Routing Verfahren zu entwickeln: Was wäre, wenn wir Forwarding Verfahren von Grund auf neu definieren könnten? Und das programmieren wir jetzt mal - versuchsweise.

Hierfür definiert OpenFlow Dienst-Primitive, die von einer externen Applikation (Software) genutzt werden können, um die Forwarding Plane des Netzwerks zu programmieren (ONF).

OpenFlow soll die Netztopologie (= Interfaces, Verbindungen, Peers) von der Kontrolle (=Lernen, Forwarding Decision) entkoppeln (SDN Wiki).

OpenFlow soll die Netzwerk-Virtualisierung vom Controller-Design entkoppeln und somit eine separate Weiterentwicklung von beiden Bereichen ermöglichen (Flowvisor / Sherwood, Casado, McKeown).

Die Zielsetzung von OpenFlow ist NICHT die Skalierung der Netzwerk Fabric, sondern: Security / NAC, TE, LB, Virtualisierung, Service Interposition, Zustandsmanipulation am Edge, parallel zu den traditionellen Protokollen im Core (Network Heresy).

In typischen Mandanten-Umgebungen haben wir 20-80 VMs je Host. Dies führt zu einer höheren Anzahl Hosts als in traditionellen Rechenzentren, sehr großen MAC-Adresstabellen und einer sehr hohen Anzahl Policies. Hieraus resultieren teure Switches. Eine Lösung könnte so aussehen: Die VM-MAC Adressen werden vor dem Netzwerk verborgen, im Netzwerk ist nur noch die Host-MAC Adresse sichtbar. Wie lassen sich die VM-MAC Adressen verbergen? Mit Edge Provisionierung. Also mit SDN/OpenFlow (Nicira).

SDN/OpenFlow bietet die Möglichkeit eines Single Point of Management für Switches, vSwitches, WLAN Komponenten, es soll Top-Level Entscheidungen aus einer ganzheitlichen Sicht und Gesamt-Monitoring von Verkehrslasten ermöglichen. OpenFlow ist somit eine OpenSource Option für die Control Plane. (Network Computing).

Insbesondere kann OpenFlow die Möglichkeit bieten, vSwitches und Hardware Switches einem einheitlichen Management zuzuführen.

OpenFlow ist "Cisco gegen der Rest der Welt" - oder anders herum: der Rest der Welt gegen Cisco (Netzwerk Guru Mike Fratto).

2.7 Offene Fragen und Probleme mit OpenFlow

Führt uns das zentrale Controller-Konzept von SDN zurück in die SNA-Ära, in der wir zur Netzwerksteuerung zentrale Front End Prozessoren hatten? Dann muss es sich die Frage stellen lassen: Woran ist SNA gescheitert? Ist Zentralität eine dauerhafte Lösung? Oder ist einfach entsprechend der allgemeinen Pendel-Theorie (zentral-dezentral, thin-fat, Layer2-Layer3 etc.) die Zeit wieder mal reif für einen Schwenk von

völliger Dezentralität in die extreme Gegenrichtung?

Die dezentrale Control Plane aktueller Netzwerke hat eine Robustheit erreicht und seit Jahren bewiesen, die eine zentrale Control Plane noch nachweisen muss. Mathematisch betrachtet stellt eine zentrale Komponente in jedem Fall ein höheres Fehler-Risiko dar als viele dezentrale, selbst wenn sie gedoppelt und HA ist. Was ja die Ursache für die Entwicklung heutiger dezentraler Designs war. Solange Netzkomponenten unabhängig von komplexen Edge Policies arbeiten, bieten sie ein hohes Maß an Hochverfügbarkeit und hitless Failover für den 24x7x365 Betrieb. LACP, OSPF und BGP erfüllen die Anforderungen vieler geschäftskritischer Anwendungen. Wo ist dann die Motivation, sie zu ersetzen? Ist es tatsächlich angebracht, zugunsten von Traffic Flow Optimierung Kompromisse in der Verfügbarkeit zu machen? Diese Überlegungen deuten darauf hin, dass uns zumindest eine hybride Lösung für lange Zeit erhalten bleiben wird. Was wiederum den Mehrwert der OpenFlow Lösung erkennbar schmälert.

Ein offensichtliches Hindernis für die allgemeine Marktakzeptanz ist die sehr kleine Kunden-/Anwendergruppe, die von den Problemen, die OpenFlow lösen will, überhaupt betroffen ist: Mega-Provider. Für wen sonst lohnt sich der Aufwand, Netze mit komplexer Edge Provisionierung und einfachem Core völlig neu zu designen? OpenFlow benötigt ein Inhaus-Team, um das neue Design zu programmieren. Welches Unternehmen will sich das leisten?

Aktuell ist nicht erkennbar, dass der Einsatz von OpenFlow tatsächlich zur Entwicklung der gewünschten einfachen Hardware führt. Dies liegt unter anderem auch daran, dass SDN/OpenFlow keine klare Trennung / Unterscheidung der Host-Netz-Schnittstelle und Paket-Switch-Schnittstelle spezifiziert: OpenFlow koppelt Host Anforderungen nach wie vor an das Netzwerk Core Verhalten (siehe hierzu auch 2.8 "Weiterentwicklung zu SDN Fabrics).

Wenn jede OpenFlow Match/Aktions-Funktionalität an jedem Host Interface (vSwitch) gewünscht ist, wird daraus ein massiver Trend zu allgemein reduzierter Funktionalität getrieben. Es ist fraglich, ob dies dem breiten Einsatzspektrum von Switches Unternehmens-Netzwerken dient.

Die meisten Hersteller unterstützen aktuell Version 1.0.0 oder maximal 1.1.0. Die aktuelle Spezifikation ist bereits Version 1.3.1. Bei dem aktuell sehr schnellen Release-Zyklus von etwa 6 Monaten sind jede Menge Inkompatibilitäten zwischen verfügbaren Produkten zu erwarten.

OpenFlow (und ebenso Open Virtual Switch) muss die "out-of-scope" Lücken in der bisherigen Spezifikation mit Leben füllen:

- Hardware-Anforderungen für Enkapsulierung Feature Umfang für OpenFlow und Open Virtual Switch
- Kompatibilität zu non-OF Netzen
- Troubleshooting Tools
- Zuverlässigkeit und Fehlertoleranz
- Skalierung und Leistung der Controller

Solange OpenFlow eine Overlay Technologie bleibt, müssen zwei Netze gemanagt werden, die sich gegenseitig in keiner Weise sehen, muss der Betreiber Troubleshooting Tools für zwei Netze vorhalten, Fehler-Analyse innerhalb und außerhalb der Tunnel leisten. OpenFlow kann nicht auf die Basis-Switch-Konfiguration zugreifen, wie zum Beispiel ein Reboot durchführen, den Low Power Transmission Modus aktivieren oder die propagierte SSID wechseln. Somit bleibt weiterhin eine 2-Level Konfiguration (OpenFlow plus Hardware-Management) erforderlich. All dies bedeutet aktuell eher Mehr- als Minderaufwand. Wer erbringt die Konsistenzprüfung zwischen Overlay und physischer Netztopologie – kann dies ein automatisiertes Konfigurationstool leisten?

Und wie steht es mit der Hersteller-Abhängigkeit? Die einzelnen Steuerungs-Aktionen sind zwar definiert, die Anwendungen des Controllers und seine Bedienoberfläche jedoch nicht. Ein Betreiber, der sich jahrelang an die Arbeitsweise und Features der Anwendungen seines Controllers gewöhnt hat, muss wieder neu lernen, wenn er auf einen anderen Controller umsteigen will. Daher wird zumindest eine Abhängigkeit vom Controller entstehen.

Kommen wir zu einigen technischeren Problemen: Fluten skaliert linear, das Prinzip "Controller-Benachrichtigung und zurück an den Edge" skaliert deutlich schlechter und ist schon beim alten Spanning Tree schief gegangen. Das Update Delay wird steigen, da Updates vom Controller seriell an alle Switches gesendet werden müssen. Die Control Plane arbeitet als Inband Signalisierung, das heißt wenn das physische Netzwerk ein Problem hat, funktioniert auch die Signalisierung nicht mehr. Die Schaltzeit bereichnet sich typischerweise wie folgt: Netzwerk Failover plus Neuberechnung im Controller. Somit ist die OpenFlow Schaltzeit immer länger als eine Standard-L2/L3 Schaltzeit.

2.8 Alternativen zu OpenFlow?

OpenFlow ist nicht der erste Versuch einer ausgelagerten und standardisierten Control Plane. Es hat schon vorher andere Initiativen und Protokolle wie ALTO, Netconf oder Junipers PCE (Path Computation Element) gegeben, die in die Richtung "Auslagerung der Control Plane" zielen.

Die Netconf Arbeitsgruppe der IETF hat versucht, ein generisches XML-basiertes Device-Management zu etablieren, um die Schwächen von SNMP zu heilen. Hierbei hat die Firma Juniper ihr JUNOS XML API zur Verfügung gestellt. Aus der Arbeitsgruppe ist im Dezember 2006 als Hauptstandard der RFC 4741 erwachsen. Der Inhalt wird im RFC Überblick wie folgt dargestellt: "The Network Configuration Protocol (NETCONF) defined in this document provides mechanisms to install, manipulate, and delete the configuration of network devices." Hat er sich im Markt durchgesetzt? Nein.

Viele verteilte Anwendungen wie File Sharing, Echtzeit-Kommunikation, Live und On-demand Media Streaming übertragen oft sehr hohe Datenmengen, suchen sich jedoch aus einer Menge möglicher Peers einen zufälligen anstelle eines optimalen Peers aus. Die ALTO Arbeitsgruppe der IETF (Application-Layer Traffic Optimization) erarbeitet seit 2008 eine Dienstspezifikation, wie verteilte Applikationen den Weg zu ihrem Peer besser als zufallsgesteuert auswählen können, und hat hier Anfangs-Input von Ciscos Network Positioning System (NPS) erhalten. Der Auswahlalgorithmus nutzt mehrere Faktoren wie Bandbreite, minimaler Cross-Domain-Verkehr, kostengünstigster Weg zum Nutzer/Client o.ä. Die Standardisierung will Anforderungen wie die von BitTorrent, trackerless P2P oder auch CDN und Auswahlverfahren für Spiegelung berücksichtigen. Der RFC ist aktuell im Draft-Stadium (Draft-13, November 2012) und noch nicht verabschiedet. Nach vier Jahren lässt sich auch hier das Fazit ziehen, dass eine generische Auslagerung von Netzwerk-Steuerungsaufgaben offensichtlich nicht zu einem schnellen Konsens führt.

3. Weiterentwicklung von SDN zu SDN Fabrics

Im Sinne von SDN lässt sich die Netzwerkinfrastruktur in zwei Komponenten unterteilen: die unterliegende Hardware und die Software, die das Gesamtverhalten des Netzwerks kontrolliert. Für die Hardware werden folgende Ideal-Eigenschaften gefordert:

- einfach, das heißt mit niedrigen Kosten für Produktion und Betrieb

Werden SDN und OpenFlow herkömmliche Netzwerke verdrängen? - Teil 2

- herstellerneutral, so dass die Nutzer leicht von einem Hersteller auf einen anderen migrieren können

- zukunftssicher durch Einsatz einer Hardware, die weitestmöglich an zukünftige Erweiterungen und Neuerungen angepasst werden kann

Die ideale Kontrollsoftware auf der anderen Seite soll so flexibel sein, dass sie die Vielfalt aktueller Anforderungen wie Isolierung/Mandanten, Virtualisierung, Verkehrssteuerung (TE, LB) und Zugangskontrolle (NAC) unterstützen kann und darüber hinaus für zukünftig auftretende Anforderungen erweiterbar ist.

Einige Väter von SDN und OpenFlow, allen voran Scott Shenker (Berkely Universität) und Martin Casado (Nicira/VMware), kritisieren, dass die SDN-Gemeinde sich zwar tiefgehend mit einem sauberen SDN-Architekturdesign auseinandergesetzt habe, nicht jedoch mit dem Design der Netzwerkinfrastruktur. Dieses wird durch Netzwerk-Anforderungen und Netzwerk-Schnittstellen geprägt.

Woher kommen die Netzwerk-Anforderungen? Von Hosts, respektive deren Nutzern, und von den Netzwerk-Betreibern. Die Hosts wollen im Prinzip einfach nur, dass sich die Pakete von A nach B bewegen, möglicherweise unter Einhaltung bestimmter QoS-Anforderungen aus der Natur der Anwendung heraus. Die Netzwerk-Operatoren haben ein breiteres Anforderungs-Spektrum wie Isolierung, Virtualisierung, Verkehrssteuerung und Zugangskontrolle, die gegebenenfalls für die Hosts nicht sichtbar sind.

Welche Schnittstellen müssen für die Erfüllung der Anforderungen berücksichtigt werden?

- Zuerst das Host-Netzwerk Interface: hier informiert der Host das Netzwerk über seine Anforderungen, die sich typischerweise im Paketheader in Form von Adressen, DS und CoS Bits wiederfinden. In manchen Designs gibt es jedoch noch höherwertige Interfaces, um Dienst-Anforderungen zu spezifizieren (z.B. IntServ).

- Als zweites das Betreiber-Netzwerk Interface: über diese Schnittstelle teilen die Netzwerk-Operatoren dem Netzwerk ihre Anforderungen mit, heute typischerweise per Konfiguration jeder einzelnen Netzkomponente. Hier hat SDN ein programmatisches Interface (materialisiert in OpenFlow) eingeführt.

- Als drittes das Paket-Switch Interface: dieses legt fest, wie sich das Paket selbst dem Switch gegenüber identifiziert. Um ein Paket weiterzuleiten, nutzt ein Layer-3 Switch einige Felder des Headers als Index für seine Forwarding Tabelle. Das dritte Interface kümmert sich um diese Index-Parameter.

Im originären Internet Design gab es im Wesentlichen keine Betreiber-Anforderungen, die Betreiber waren zufrieden, wenn das Netzwerk schlichtweg die Pakete von der Quelle zum Ziel transportiert hat. Jeder Router hat mittels Paket Header die Host-Anforderungen eigenständig interpretiert und die hierfür erforderliche Weiterleitung durchgeführt. Somit waren das Host-Netzwerk und Paket-Switch Interface identisch, den Bedarf für ein Betreiber-Netzwerk Interface gab es nicht.

MPLS hat eine Unterscheidung zwischen Netzwerk Edge (Edge Router) und Netzwerk Core (Core Router) eingeführt: Edge Router untersuchen den Header des ankommenden Pakets (dem die Host-Anforderungen zu entnehmen sind) und tragen dann einen Label ins Paket ein. Die Label-basierten Forwarding Tabellen der Core Router werden nicht nur für Forwarding Informationen genutzt, sondern setzen auch die Betreiber-Anforderungen (VPN-Tunnel oder Traffic Engineering) um. Die Labels haben jedoch nur im MPLS Core eine Bedeutung und sind völlig unabhängig von jedem Host Protokoll (zum Beispiel IPv4, IPv6). Das Host-Netzwerk Interface ist weiter IP, während das Paket-Switch Interface der MPLS Label ist. Somit unterscheidet MPLS das Host-Netzwerk und das Paket-Switch Interface, kennt aber generell kein Operator-Netzwerk Interface.

Im Gegensatz zu MPLS fokussiert sich SDN auf die Control Plane und spezifiziert eine vollwertige programmatische Betreiber-Netzwerk Schnittstelle, die die Umsetzung der vielfältigen Betreiber-Anforderungen ermöglichen soll, ohne Änderungen der unterliegenden Netzwerkbereiche zu erfordern. SDN erreicht diese Flexibilität durch eine Entkopplung der Control Plane von der Data Plane Topologie, bei der das Weiterleitungs-Modell der Control Plane keine Nachbildung der Weiterleitung auf der Data Plane sein muss. OpenFlow als die aktuelle Umsetzung des SDN Design hat dabei aber das Problem, dass es keine Unterscheidung zwischen Host-Netzwerk und Paket-Switch Schnittstelle kennt: Nach wie vor muss jeder Switch immer noch den Host Header interpretieren.

Das führt aus Sicht von Casado/Shenker zu drei Problemen:

- Erstens wird das Versprechen einfacher Hardware nicht erfüllt, da der Switch in der Praxis Lookups über Hunderte von Bits im Header durchführen muss. Zum Vergleich: MPLS Lookups gehen nur über einige 10 Bits.

- Zweitens erbringt OpenFlow nicht die volle Flexibilität, da die Match-Felder und die hierfür unterstützten Aktionen zu eingeschränkt sind. Eine Erweiterung muss nach dem heutigen OpenFlow Paradigma in jedem einzelnen Switch implementiert werden – was wiederum das Zünglein an der Waage eher in Richtung Einfachheit und somit reduzierter Funktionalität ausschlägen lässt.

- Drittens bindet OpenFlow die Host Anforderungen unnötig an das Verhalten des Netzwerk Core. Ein Wechsel im Netzwerk Protokoll (z.B. von IPv4 auf IPv6) erzwingt eine Änderung im Match Verhalten beziehungsweise der Matching Funktionalität (das Matching erfolgt auf andere Header Felder), was

Werden SDN und OpenFlow herkömmliche Netzwerke verdrängen? - Teil 2

wiederum ein verändertes Paket-Matching bis in den Core hinein nach sich zieht.

Um diese Problempunkte zu beseitigen, schlagen Casado/Shenker eine Erweiterung der SDN Architektur um eine Netzwerk-Fabric Komponente vor. Das Netzwerk-Design kennt dann drei Komponententypen: Hosts, die als Quelle und Ziel von Paketen agieren; Edge Switches als Ingress und Egress Komponenten; und die Netzwerk-Fabric im Core. Edge und Fabric werden durch (logisch) getrennte Controller gesteuert, den Edge Controller und den Fabric Controller. Der Edge Controller handhabt das Operator-Netzwerk Interface und ist für die Bereitstellung komplexer Netzdienste zuständig (Virtualisierung, Mandanten, NAC, TE, LB, etc.). Der Ingress Edge Switch handhabt zusammen mit dem Edge Controller das Host-Netzwerk Interface. Der Fabric Controller und die Fabric Switches handhaben das Paket-Switch Interface. Die Paketbearbeitung funktioniert dann wie folgt: Der Quell-Host sendet ein Paket zu einem Edge Switch, der die entsprechenden Netzwerk-Dienste bereitstellt, das Paket dann durch die Fabric hindurch an den Egress Switch sendet, der es zum Zielhost weiterleitet oder idealerweise direkt am Ziel-Host abgibt (siehe hierzu auch Abbildung 3.1).

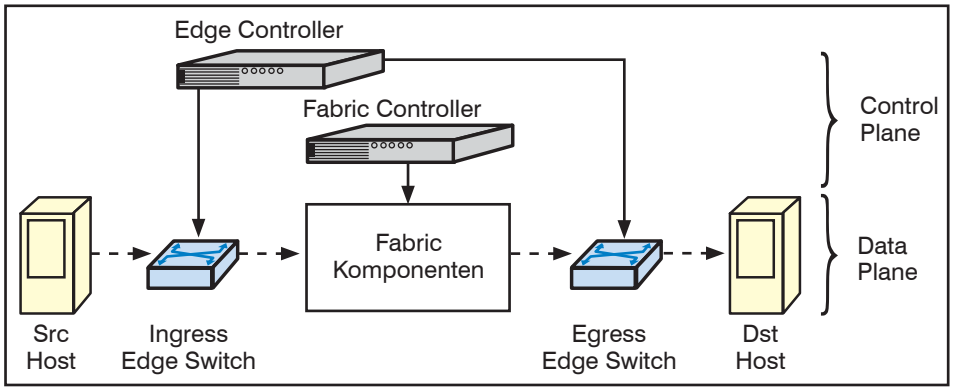


Abbildung 3.1: Erweitertes SDN Konzept mit Edge und Fabric Controller

Fabric Konzepte sind eine etablierte Technologie und wenn die neue SDN-Konzeptintelligenz am Netzwerk Edge umgesetzt wird, wird der Core hiervon entlastet und ist so einfach wie möglich betreibbar. Auch im "non-OpenFlow" LAN Bereich sind Trends erkennbar, die eine intelligente Edge Provisionierung durch die Access Switches und einen möglichst simplen Core favorisieren (z.B. Enterasys OneFabric, Cisco WLAN/Ethernet Access Strategie).

SDN Fabric

Zu den Kernfunktionen einer SDN Fabric gehört das Fabric-interne optimierte Forwarding. Um das Fabric Forwarding weitestgehend von der Edge Provisionierung zu entkoppeln, sollte am Edge ein minimaler Satz von Weiterleitungs-Primitiven bereitgestellt werden, ohne irgendwelche Fabric-internen Forwarding Mechanismen nach außen, das heißt am Edge sichtbar zu machen. Insbesondere sollen externe / Edge Adressen nicht für die Fabric-interne Weiterleitungs-Entscheidung herangezogen werden. Das ermöglicht einerseits eine Vereinfachung der Fabric Komponen-

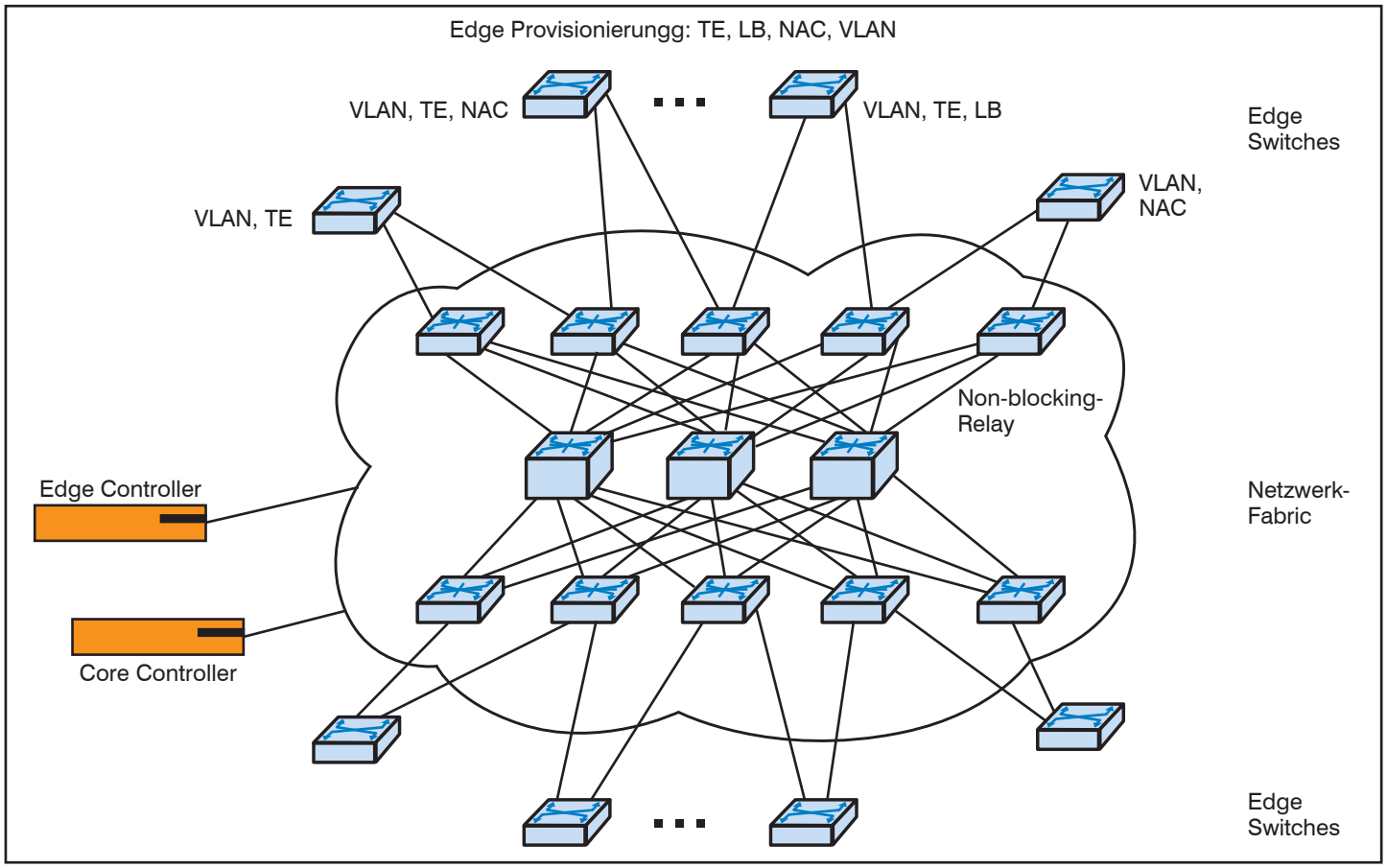


Abbildung 3.2: SDN Edge Provisionierung und Fabric Konzept

Werden SDN und OpenFlow herkömmliche Netzwerke verdrängen? - Teil 2

ten, andererseits entkoppelt es die Weiterentwicklung des Edge-Bereiches von der Fabric-Weiterentwicklung.

Eine weitere Kernfunktion ist die Entkopplung der Control Plane des Netzwerk-Edge und der Netzwerk-Fabric, da beide unterschiedliche Aufgaben handhaben. Die Fabric ist für die schnelle, möglichst blockierungsfreie Weiterleitung zuständig, der Edge ist für die Provisionierung komplexer Dienste (VMotion, TE, LB, NAC etc.) zuständig, wie in Abbildung 3.2 dargestellt.

Auch in kommerziellen Chassis-Geräten ist übrigens das Fabric Modell wiederzufinden: Die Line-Karten haben die Funktions-Intelligenz im Sinn einer Edge-Provisionierung, die interne Switching Matrix ist eine relativ dumme aber extrem leistungsfähige Forwarding-Infrastruktur. Das Management-Modul respektive "die CPU" (Supervisor, Controller oder wie sie auch bei verschiedenen Herstellern heißen mögen) ist Edge und Fabric Controller in einem.

Eine gute Fabric muss eine beliebige Anzahl intelligenter Edges unterstützen können und umgekehrt. Sie muss im Prinzip beliebige Edge Designs mit verschiedenen Adress-Schemas, NAC- und TE-Policies unterstützen. Umgekehrt kann dann jedes Edge Design von der Hochleistungs-Fabric profitieren, da das Edge Design völlig unabhängig davon ist, wie die Fabric intern arbeitet. Die Fabric muss Punkt-zu-Punkt-Kommunikation, Punkt-zu-Multipunkt-Kommunikation und für den Überlastfall ein Priorisierungs-Konzept zum Verwerfen von Paketen unterstützen. Diese drei Dienst-Primitive sind nach Casasdo/Shenker ausreichend. In diesem Sinne sehen sie zwei Optionen für Adressierung und Forwarding in einer Fabric:

- MPLS-ähnliche Beschränkung von Netzwerk-Adressen auf opaque Labels sowie Beschränkung der Forwarding-Aktionen auf forward, push, pop und swap; dies könnte mit mehreren Control Planes sowohl Path-basierte als auch Ziel-basierte Provisionierung ermöglichen

- Beschränkung der Forwarding-Aktionen auf "Destination Address Lookup per longest Prefix Match" und ECMP-basierte Weiterleitung; dies ist wenig geeignet für die Bereitstellung eines Ende-zu-Ende Weges (Path-Provisionierung), führt aber zu einer einfacheren Control Plane und höhere Skalierbarkeit

Die eigentliche Komplexität und Krux der Edge/Fabric Architektur liegt darin, den komplexen Edge Kontext auf Netzwerk-Adressen oder Wege (Paths) zu mappen, also festzulegen, welche "Fabric-Netzwerkadresse" oder welchen Label ein bestimmtes Paket erhält. Soll heißen: Irgendwie "im Netzwerk" entschieden werden, welche Fabric-interne Netzwerkadresse zu nutzen ist. Hierfür kommen Translations- oder Enkapsulierungs-Verfahren in Frage, wobei Enkapsulierung der umfassendere Ansatz ist. Und hier sind wir wieder bei der Fülle der möglichen Overlay-Technologien SPBM, MPLS, VXLAN, STT und Konsorten angekommen.

Prinzipiell soll eine SDN Fabric die gleichen Vorteile wie SDN als Ganzes bieten: Die Reduzierung auf simples Forwarding soll einfache und kostengünstige Switch-Implementierungen ermöglichen, klar und eindeutig definierte und standardisierte Fabric Schnittstellen sollen zur Herstellerunabhängigkeit führen, das heißt Edge und Fabric beliebig kombinierbar und austauschbar machen. Soweit die Theorie. Leider ist das Stand heute nicht der Fall und auch noch nicht in Sicht. Weder Chassis-Fabrics noch Netzwerk-Fabrics (mit wenigen Ausnahmen) arbeiten mit standardisierten Interfaces, etablieren sich aber auch ohne OpenFlow im Markt. Somit widerspricht OpenFlow dem Marktinteresse der Komponenten-Hersteller.

Die Chance auf eine standardisierte Edge Provisionierung ist niedrig. Welchen Mehrwert kann dann ein neues Overlay Protokoll und eine Standardisierung der Edge-Fabric Schnittstelle bringen? Und ist eine SDN Fabric Welt mit hochkomplexer Edge Provisionierung und einer Fabric, deren Innenleben opaque ist, wirklich so viel besser handhabbar als konventionelle Netze mit Edge Provisionierung und einem auf Layer-2/Layer-3 reduzierten Core? Warten wir es gelassen ab.

4. Einige Einsatzszenarien und Hersteller-Konzepte

OpenStack
OpenStack ist ein OpenSource IaaS Cloud Computing Projekt von Rackspace Cloud und NASA. Aktuell haben sich mehr als 150 Unternehmen angeschlossen, unter anderem AMD, Intel, Canonical, SUSE Linux, Red Hat, Cisco, Dell, HP, IBM und Yahoo. OpenStack hat zum Ziel, jeder Organisation zu ermöglichen, Cloud Computing Dienste auf der Basis von Standard Hardware zu implementieren und zu vermarkten.

OpenStack ist in die Module "compute", "storage", "networking" und "dashboard" gegliedert (siehe Abbildung 4.1). Das Networking Modul ist ein skalierbares API, das der Administrator als Plugin für Netzwerkmanagement und IP Adressen nutzen kann. Es unterstützt OpenFlow für Mandanten-Konfiguration in hochskalierende Umgebungen.

Open Virtual Switch (OVS)
OVS ist ein Layer-2 vSwitch, der auf Basis Apache 2.0 lizensiert wird. Das Design wurde mit Programmierschnittstellen für massive Netzwerk-Aotomatisierung optimiert. Ähnlich wie VMwares vNetwork Distributed vSwitch oder der Nexux 1000v von Cisco kann der Switch virtuell über mehrere Server verteilt werden. Der OVS

Werden SDN und OpenFlow herkömmliche Netzwerke verdrängen? - Teil 2

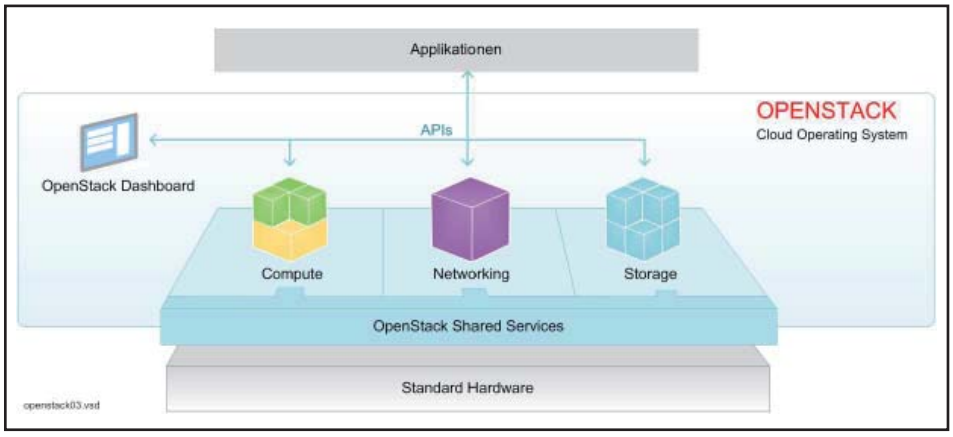


Abbildung 4.1: OpenStack Quelle: openstack.org

ed Virtual Network Infrastructure. Ein virtuelles Netzwerk ist so definiert, dass es alle VMs verbindet, die zusammen in einem Layer-2 Verbund sein sollen, im gezeigten Beispiel aus Abbildung 4.3 die grünen, gelben und roten VMs (1). Jeglicher VM-Verkehr wird in L2 over L3 Tunnel enkapsuliert und so von der physischen Infrastruktur entkoppelt. Unterstützte Tunnelverfahren sind GRE, NVGRE, VXLAN und CAPWAP. Die Tunnel-Topologie kann beliebig vermascht sein (2), die vSwitches können Zehntausende Tunnel unterstützen. Netzwerk-Dienste, die am Edge beziehungsweise am ersten vSwitch provisioniert werden, sind L2, L3 und ACL Lookups (3). Der Übergang zwischen virtualisiertem und traditionellem Netzwerk ist ein Gate-

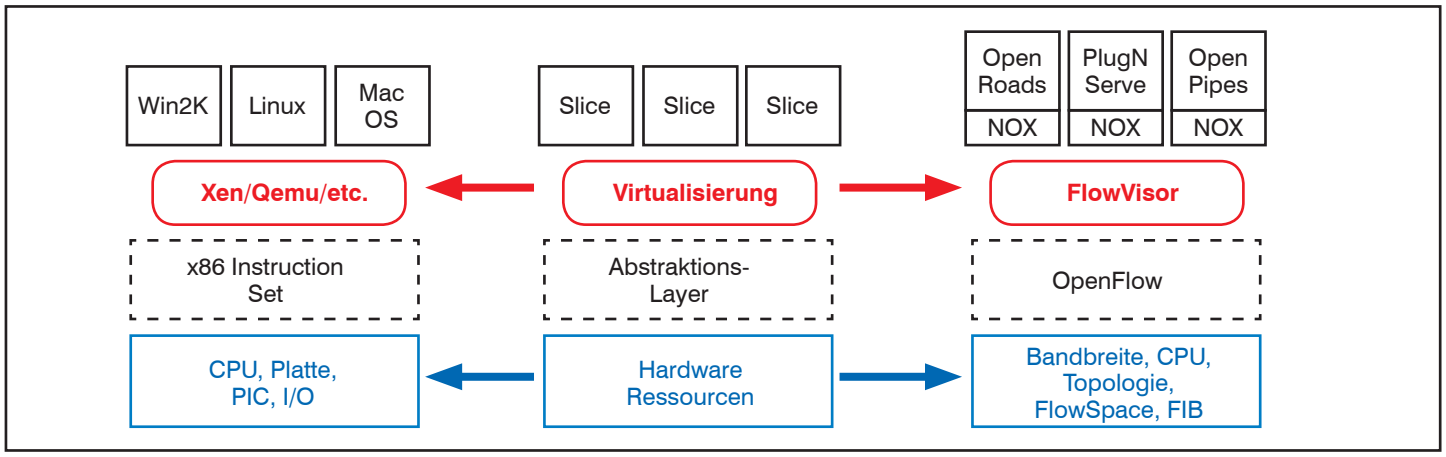


Abbildung 4.2: FlowVisor für Netzwerk-Virtualisierung

unterstützt sowohl OpenFlow mit Pipeline Processing für automatisiertes Management als auch traditionelle Management Protokolle wie NetFlow, sFlow oder GRE-getunneltes Mirroring. QoS Funktionen sind Queueing und Traffic Shaping, Sicherheits-Funktionen sind VLAN Isolierung und Filtersetzung, Layer-2 Verfahren sind Spanning Tree (802.1-1998!) und LACP und VLAN Tagging / Trunking.

OVS unterstützt IPv6 und die Tunnelverfahren Ethernet over GRE, CAPWAP, IPsec, GRE over IPsec. Linux Bridging und NIC Bonding mit Source MAC LB, Active Backup oder Layer-4 Hash sind möglich.

FlowVisor
FlowVisor ist eine Implementierung von OpenFlow zur Durchführung von Netzwerk Experimenten in einem Produktiv-Netzwerk, die an der Stanford Universität in Zusammenarbeit mit Nicira und der Deutschen Telekom entwickelt wurde. Ähnlich wie bei der Servervirtualisierung ist der FlowVisor eine Netzwerk-Virtualisierungs-Schicht, die systemtechnisch zwischen dem Betriebssystem und der Hardware sitzt (wie in Abbildung 4.2 dargestellt). Netzwerktechnisch ist der FlowVisor zwischen dem Controller und den Switches angesiedelt. Dies können vSwitches oder Hardware Switches sein.

FlowVisor virtualisiert das Netzwerk, indem ein definiertes Subset aus allen Flows das klassische Switch Forwarding umgeht und mit OpenFlow gesteuert wird. Dieses Subset heißt Flowspace oder auch Slice (ein kleines Stück aus dem großen Traffic-Kuchen). FlowVisor kann mehrere Gast OpenFlow Controller hosten, ein Gast Controller steuert jeweils einen Flowspace. So lassen sich verschiedene OpenFlow Anwendungen programmieren. OpenRoads, PlugNServe und OpenPipes beispielsweise sind Gast Controller, die auf NOX programmiert wurden.

Nicira Network Virtualization Platform (NVP)
Niciras NVP ist eine weitere Lösung zur Netzwerk-Virtualisierung. Der Controller ist der NVP, die OpenFlow-fähigen Switches sind OVS Switches.

Nicira nennt das Konzept DVNI, Distributway, das die Standard-Verfahren in Richtung traditionelles Netzwerk unterstützt (4). Die unterliegenden Hardware Switches agieren als simple Layer-2 Fabric; werden hier Multipath Verfahren genutzt (TRILL, SPBM), können auch alle Wege parallel aktiv sein (5). Der Controller handhabt die Zustandsinformationen des Netzwerk Edge und hat ein API für Provisionierung, Konfiguration und Monitoring (6).

Die Anwendungen zur Netzwerk-Steuerung sind dann zum Beispiel in der Bedienoberläche als Menüpunkte auswählbar (siehe Abbildung 4.4):

- Custom Network Services
- WAN Optimierung
- Load Balancer
- L3 Routing
- Firewall
- Monitor
- QoS
- Mandanten und Port Isolierung
- L2 Switch

Weitere Produkte und Aktivitäten
Sicher kann eine Unterstützung von OpenFlow durch die Founding Members

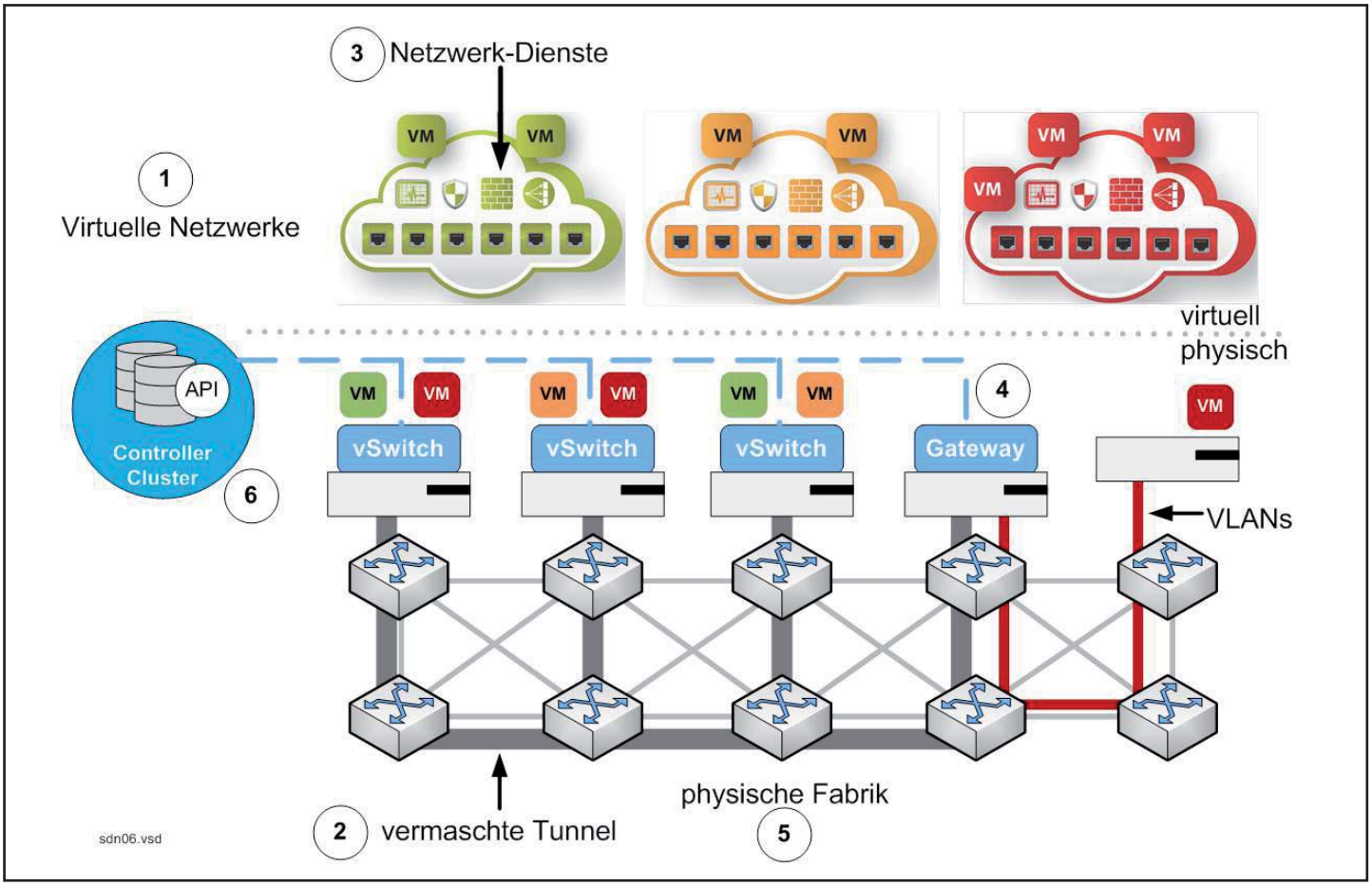


Abbildung 4.3: Nicira DVNI

erwartet werden. Welches non-founding Mitglied SDN tatsächlich aktiv unterstützen wird oder aber nur die Konkurrenz beäugen möchte, bleibt jedoch abzuwarten. Juniper hat sich schon wieder abgesetzt (was im Angesicht von QFabric nicht wirklich überrascht), und auch Arista traut der Skalierbarkeit von OpenFlow nicht wirklich über den Weg.

Auf der Interop 2011 haben 15 Hersteller (BigSwitch, Broadcom, Brocade, Citrix, Dell, Extreme, Fulcrum, HP, IBM, Juniper, Marvell, NEC, Netgear, NetOptics, Pronto Systems) eine OpenFlow Demo gezeigt, die Aufmerksamkeit erzeugt hat.

Der Stanford Controller kann 500 Flows pro Sekunde bearbeiten (Kommentar von Arista: Die Netze unserer Kunden haben 1 Mio. Flows pro Sekunde). Aber: Bei OpenFlow müssen die Pakete im Regelfall ja auch nicht durch den Controller. Und: BigSwitch ist schon auf dem Weg, einen leistungsfähigeren Controller zu entwickeln. Genesis hat in ihrem Data Center zwei NEC Controller als Redundanzlösung, die immerhin 2.500 VMs unterstützen.

BigSwitch entwickelt ein Mandanten-Modell für OpenFlow, das aus beliebigen Ports von beliebigen OpenFlow Switches einen virtuellen Switch generieren kann. Extreme hat einen OpenFlow Software-Agenten in seinem XOS System, der im Testbetrieb mit NEC und Big Switch Controllern gefahren wurde.

Cisco ist mit ONE (Open Network Environment) und OnePK (One Platform Kit) auf den Hype-Zug aufgesprungen. Wieviel OpenFlow und wie viele proprietären Erweiterungen die angekündigten Produkte bei Verfügbarkeit haben werden, bleibt abzuwarten. Eingebunden werden sollen zuerst ISR G2, ASR 1000, später Catalyst 3750-X und Nexus 1000v Switches. Implementiert wird OpenFlow 1.0.0.

Extreme Networks unterstützt auf ihren Access Switches OpenFlow Version 1.0.0 zusammen mit dem BigSwitch Controller.

IBM hat seit Dezember 2011 den G8264 von Blade Network Technologies als OpenFlow Switch.

HP fährt OpenFlow auf den 3500, 5400/8200 und 6600 Switches (was ist mit der 3com / A-Produktlinie??).

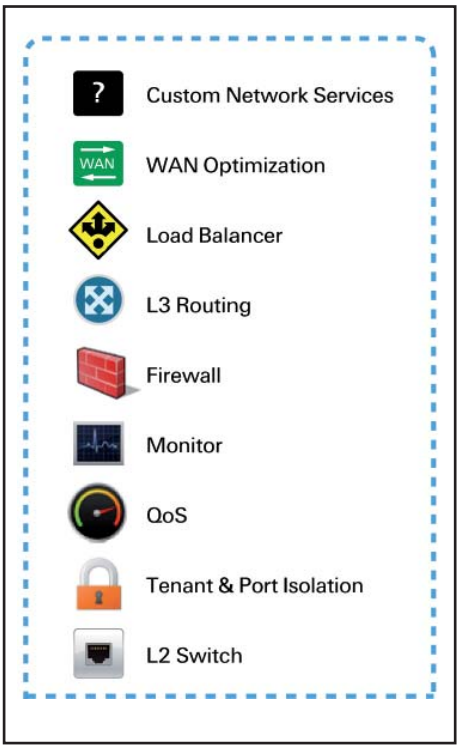


Abbildung 4.4: NVP Anwendungs-Menü
Quelle: Nicira

NEC hat mit dem PF5240Switch auf der Interop 2011 den "Best of" gewonnen, im Dezember 2011 kam der PF5820 mit integriertem Controller.

Im Internet2 kommen NEC Switches mit OpenFlow zum Einsatz.

5. Fazit: Ist OpenFlow eine Revolution, Evolution oder Hype?

Wenn wir Netzwerk-Technologie in Zeitalter einteilen, lässt sich 1974 bis 1994 als das Zeitalter von IBM, 1992 bis 2012 als das Zeitalter von Cisco charakterisieren. Läutet nun SDN mit völlig frei programmierbaren standard-baisierten Netzwerk-Komponenten seit 2010 ein neues Zeitalter ein? Setzt sich das neue Netzwerk aus Billig-vSwitches, Billig-Hardware-Switches (mit Silicum von Broadcomm und Fulcrum), einem mega-intelligenten Controller-Cluster und völlig neuen Traffic Engineering sowie völlig neuen Fehlerumschaltungen zusammen? Falls ja, so wird dies sicherlich noch eine Weile dauern.

So, wie es sich aktuell abzeichnet, wird OpenFlow parallel zur proprietären Switch-Software im Hybrid-Modus laufen und komplementär agieren. In diesem Fall muss die Switch Architektur beziehungsweise das Switch Design sowohl für lokale Kontrolle als auch für einen Steuerzugriff durch Controller ausgelegt sein. Das bedeutet für hohe Leistung: neue Hardware. Aktuellen Broadcom Chipsätzen fehlt zum Beispiel der eine oder anderen Action Modifier, den OpenFlow erfordert.

Das bedeutet: Marktinteresse ist da, allein der Funktionsumfang von OpenFlow ist noch sehr limitiert und es fehlen auf breiter Ebene Chipsätze, die die neueste Spezifikation implementieren.

Wo sind kurz- bis mittelfristig erreichbare Mehrwerte durch OpenFlow erkennbar? Mit OpenFlow könnte das Netzwerk-Team Einblick in die Virtualisierungs-Umgebung erhalten und Möglichkeiten der dynamischen Netz-Provisionierung gewinnen. Selbst wenn OpenFlow nichts weiter eine gemeinsame Control Plane für alle vSwitches dieser Welt bringt, wäre ja schon ein erkennbarer Mehrwert erreicht. Eine Steigerungsstufe wäre OpenFlow als Management für alle proprietären vSwitches, OpenSource vSwitches (OVS) sowie alle OpenStack Komponenten. Die Steigerungsstufe wäre ein gemeinsames Management für vSwitches, Hardware Switches und WLAN Komponenten.

Ein sinnvoller Trend könnte der vereinfachte Core Betrieb in Kombination mit intelligenterer Edge Provisionierung werden, auch hier wieder mit dem Blick darauf, dass der Netzwerk-Edge gegebenenfalls ein vSwitch im Host ist. Aber brauchen wir dafür zwingend OpenFlow?

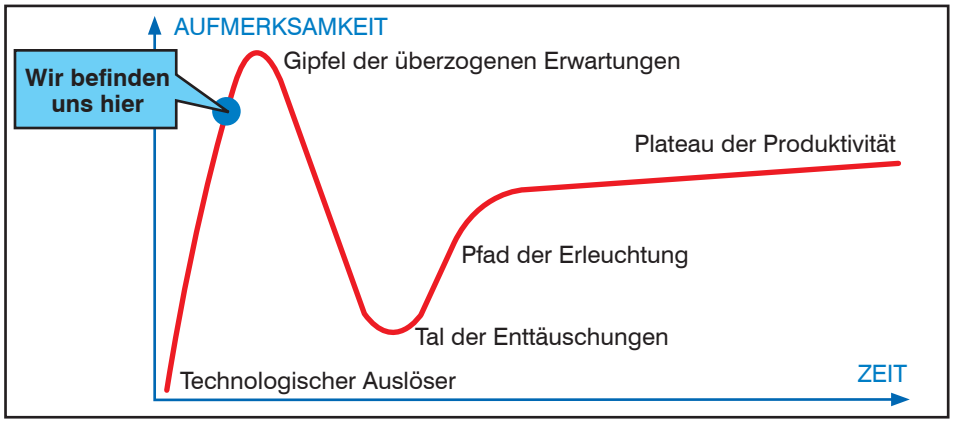


Abbildung 5.1: SDN / OpenFlow Hype Cycle

SDN und OpenFlow bewegen sich im Gartner Hype Cycle sicher noch vor dem Erwartungs-Peak (siehe Abbildung 5.1). Daher dürfen wir getrost erwarten, dass wir in den Jahren 2013 und 2014 ins Tal der Enttäuschungen plumpsen, bevor der Markt sich gegebenenfalls aufmacht zum Pfad der Erleuchtung und zu einer sinnvollen Konsolidierung.

Abkürzungen

ACK	Acknowledgement
ACL	
ALTO	Application-Layer Traffic Optimization
API	Application Programming Interface
BGP	Border Gateway Protocol
BoS	Bottom of Stack
CAPWAP	Control and Provisioning of Wireless Access Points
CDN	Content Delivery Network
CoS	Class of Service
CPU	Central Processing Unit
DS	Differentiated Services
DVNI	Distributed Virtual Network Infrastructure
ECMP	Equal Cost Multipath
GRE	Generic Routing Encapsulation
IANA	Internet Assigned Numbers Authority
ID	Identifikator
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPsec	IP Security
JUNOS	Juniper Operating System
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
LB	Load Balancing
LISP	Locator/ID Separation Protocol
MAC	Media Access Control
MPLS	Multi Protocol Label Switching
MPLS	Multi-Protocol Label Switching
NAC	Network Access Control
NASA	National Aeronautics and Space Administration
NIC	Network Interface Card
NPS	Network Positioning System
NVGRE	Network Virtualization using Generic Routing Encapsulation
NVP	Network Virtualization Platform (Nicira)
OF	OpenFlow
ONF	Open Networking Foundation
OOB	Out-Of-Band
OSPF	Open Shortest Path First
OVS	Open Virtual Switch
OXM	OpenFlow Extensible Match
P2P	Punkt-zu-Punkt, Peer-to-Peer
PBB	Provider Backbone Bridging
PCE	Path Computation Element
QoS	Quality of Service
RFC	Request for Comment
RO	Read-Only
RW	Read-Write
SDN	Software-Defined Networking
SNA	Systems Network Architecture
SPBM	Shortest Path Bridging MAC
SSID	Service Set Identifier
STT	Stateless Transport Tunneling
TCP	Transmission Control Protocol
TE	Traffic Engineering
TLS	Transport Layer Security
TLV	Type Length Vector
TRILL	Transparent Interconnection of Lots of Links
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VM	Virtual Machine
VPN	Virtual Private Network
VXLAN	Virtual Extensible LAN
XML	Extended Markup Language

Literatur

- ONF: OpenFlow Switch Specification 1.3.1, September 2012
- ONF: OF-CONFIG 1.1 OpenFlow Management and Configuration Protocol

Standpunkt Sicherheit

Der Rundumschlag: Pauschale Verschlüsselung in WAN/MAN/LAN

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

Wenn Daten mit hohem (oder sogar sehr hohem) Schutzbedarf hinsichtlich Vertraulichkeit bzw. Integrität in Netzen übertragen werden sollen, hat die Informationssicherheit schon immer zunächst unterschieden, ob es sich hier um ein Netz in einem vertrauenswürdigen Bereich handelt oder nicht. Im letzteren Fall fordert die Informationssicherheit unabhängig vom Typ des Netzes reflexartig fast immer den Einsatz von Verschlüsselung.

Als Konsequenz sind bei entsprechendem Schutzbedarf Daten zu verschlüsseln, sobald sie z.B. das geschützte LAN und das Rechenzentrum einer Unternehmung verlassen. Dies gilt dann nicht nur im WAN (z.B. MPLS), sondern sogar auch bei der Verbindung zwischen Standorten / Rechenzentren per Dark Fiber bzw. Dense Wavelength Division Multiplexing (DWDM). Hier genügt bereits die Machbarkeit eines Lauschangriffs, auch wenn er bei DWDM mit erheblichem Aufwand verbunden ist.[1]

Sofern nur eine Hub-and-Spoke-Kommunikation vorliegt, kann man sich im klassischen WAN noch mit einem eigenbetriebenen IPsec VPN oder mit proprietären Kryptoboxen behelfen. Spätestens bei VoIP und UC wäre aber oft ein vollvermaschtes VPN notwendig, was für IPsec eine quadratische Komplexität für den Aufbau der Security Associations oder den Einsatz trickreicher Mechanismen (z.B. Gruppenschlüssel gemäß RFC3547) nach sich zieht. Hier springen gerade bei MPLS die Provider ein und bieten oft die Möglichkeit eines verschlüsselten MPLS-VPN als (natürlich teurere) Dienstleistung an. Sofern man als Kunde hier nicht die Kontrolle über das Schlüsselmaterial hat, muss man dabei natürlich dem Provider trauen.

Ist eine Glasfaserstrecke zu verschlüsseln, kommen IPsec-basierte VPNs schnell an die Grenzen ihrer Leistungsfähigkeit und

bei einer Verbindung zwischen Rechenzentren sind neben einer Verschlüsselungsleistung von mehr als 10 Gbit/s auch Layer-2-Verbindungen zu unterstützen. Hierzu gibt es mit IEEE 802.1AE MACsec (z.B. im Cisco Nexus 7000) und mit Layer-2-Kryptoboxen zwar Lösungen, die leistungsfähig genug sind, sich auch für Carrier-Ethernet eignen, jedoch auch entsprechend teuer sind.

Die IT könnte bei diesen aufwendigen Techniken geneigt sein, den „schwarzen Peter“ vom Netz zu denjenigen Anwendungen zu schieben, die den hohen Schutzbedarf auch mitbringen. Falls im WAN – zumindest für alle kritischen Anwendungen – konsequent mit per HTTPS geschützten Web Applikationen oder mit anderen durch eine Verschlüsselung zusätzlich abgesicherten Techniken des Server-based Computing (Terminal Server, Virtual Desktop Infrastructure, VDI) gearbeitet würde, mag dies auch gelingen. Die Praxis sieht jedoch meist anders aus und die Folge wäre dann höchstwahrscheinlich ein Zoo von verschiedensten, heterogenen Lösungen, der in Summe nicht nur bei den Investitionen, sondern insbesondere im Betrieb einen nicht mehr überschaubaren Aufwand verursacht.

Also bleibt es doch beim Netz und der Forderung hier bei entsprechendem Schutzbedarf zu verschlüsseln. Um die ewige Diskussion der Schutzbedarfsfeststellung zu beenden, gibt es nicht wenige IT-Abteilungen, die sogar über eine pauschale Verschlüsselung aller Daten zumindest im WAN nachdenken.

Interessanterweise werden ähnliche Anforderungen auch an die Absicherung der Kommunikation im LAN gestellt. Dies hat durchaus damit zu tun, dass die Arbeitsannahme, dass ein LAN eine geschützte, vertrauenswürdige Umgebung sei, immer häufiger in Frage zu stellen ist. Unterschiedlichste Nutzer- und Gerätegruppen auf allen denkbaren Sicherheitsniveaus teilen sich hier eine gemeinsame LAN-Infrastruktur. In dieser Situation sind

[1] Siehe „Kurzstudie zu Gefährdungen und Maßnahmen beim Einsatz von DWDM“ vom Bundesamt für Sicherheit in der Informationstechnik (BSI), verfügbar unter https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/hilfmi/doku/doku.html

Standpunkt Sicherheit

die Forderungen nach einer Netzzugangskontrolle und dem Aufbau einer mandantenfähigen LAN-Infrastruktur schnell gestellt. LANs, deren Netzzugang mit IEEE 802.1X abgesichert wird, sind tatsächlich immer häufiger anzutreffen und auch der Einsatz von Virtual Routing and Forwarding (VRF) zur Trennung der Gruppen (Mandanten) ist in der Praxis zu finden. Der Aufwand für den Betrieb solcher Lösungen ist jedoch meist erheblich, und VRF bzw. VLAN müssen außerdem mit der Vorhaltung leben, dass hier nur eine logische Trennung der Netze auf Layer 3 und Layer 2 stattfindet.

Wenn nun ein LAN immer weniger vertrauenswürdig ist (im Extremfall wird eine LAN-Infrastruktur wie Strom aus der Steckdose durch einen Provider bereitgestellt), könnte bei hohem Schutzbedarf von Daten (hinsichtlich der Vertraulichkeit oder Integrität) die oben diskutierte Forderung nach Verschlüsselung daher eins zu eins auf das LAN übertragen werden.

Die Standards hierzu haben wir mit MACsec und mit IEEE 802.1X-2010 bereits, d.h. es ist grundsätzlich möglich, konsequent über MACsec vom Client über LAN/MAN/WAN bis hin zum Server die gesamte Übertragung im Netz zu verschlüsseln. Wir haben aber ein Problem mit der Verfügbarkeit entsprechender Produkte. Lediglich Cisco bietet Switches mit MACsec und eine entsprechende Client-Software an. Außerdem ist bei Cisco eine durchgängige Nutzung von MACsec erst seit kurzem möglich. Trotzdem ist diese Technik als hochinteressant einzustufen und wir werden 2013 tatsächlich erste Netze sehen, die konsequent mit MACsec verschlüsseln. Dass dies ein (kalkuliertes) Abenteuer darstellt und eine solche Technik mit Bedacht und schrittweise eingeführt werden muss, ist klar. Erfahrungen im Netzbetrieb, insbesondere im Trouble Shooting müssen hier erst noch gewonnen werden. Ob sich diese Technik durchsetzen wird und auch andere Hersteller MACsec unterstützen werden, kann auch noch nicht gesagt werden.

Es wird in den nächsten Jahren daher auch weiterhin mit den bewährten Mitteln des Aufbaus mandantenfähiger Netze und der Absicherung kritischer Daten mit VPN-Techniken gearbeitet werden müssen.

Interne Absicherung der IT-Infrastruktur

28.01. - 30.01.13 in Bonn

Die ComConsult Akademie veranstaltet vom 28.01. - 30.01.13 ihr Seminar "Interne Absicherung der IT-Infrastruktur" in Bonn.

Bedingt durch Netzkonvergenz, Mobilität und Virtualisierung hat die interne Absicherung der IT-Infrastruktur in den letzten Jahren enorm an Bedeutung gewonnen. Heterogene Nutzergruppen mit unterschiedlichstem Sicherheitsniveau teilen sich eine gemeinsame IP-basierte Infrastruktur und in vielen Fällen ist der Aufbau sicherer, mandantenfähiger Netze notwendig. Dieses Seminar identifiziert die wesentlichen Gefahrenbereiche und zeigt effiziente und wirtschaftliche Maßnahmen zur Umsetzung einer erfolgreichen Lösung auf. Alle wichtigen Bausteine zur Absicherung von LAN, WAN, Endgeräten, RZ-Bereichen, Servern und SAN werden detailliert erklärt und anhand konkreter Projektbeispiele wird der Weg zu einer erfolgreichen Sicherheits-Lösung aufgezeigt.

In diesem Seminar lernen Sie

- wie aktuell die wichtigsten internen Bedrohungen aussehen und wie diese systematisch zu kategorisieren sind
- welche Kernbausteine zur internen IT-Sicherheit sich aus der Bedrohungslage ergeben
- welche Maßnahmen die IT-Grundschutz-Kataloge des BSI für die interne IT-Sicherheit vorsehen und wie sie umgesetzt werden können
- wie Firewalls und Intrusion-Prevention-Systeme im LAN zum Aufbau von Sicherheitszonen genutzt werden können
- wie mandantenfähige LANs aufgebaut werden mit welchen Techniken eine Netzzugangskontrolle realisiert werden kann
- welche Sicherheitsaspekte im Netzmanagement zu beachten sind
- wie sich die Server-Virtualisierung auf Sicherheitskonzepte auswirkt und welche Sicherheitsmaßnahmen notwendig sind
- wie SANs in der Absicherung berücksichtigt werden müssen
- welche Sicherheitsmaßnahmen auf Ebene der Netzdienste und des Betriebssystems relevant sind
- wie VoIP und Unified Communications abgesichert werden können welche Sicherheitsmechanismen bei WLANs eingesetzt werden

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Ich buche das Seminar

Interne Absicherung der IT-Infrastruktur

☐ vom 28.01. - 30.01.13 in Bonn
zum Preis von € 1.890,-- netto

☐ Bitte reservieren Sie mir ein Zimmer

vom _____ bis_____ 13

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

_____ Vorname

_____ Nachname

_____ Firma

_____ Telefon/Fax

_____ Straße

_____ PLZ,Ort

_____ eMail

_____ Unterschrift

Zweitthema

Voice, Video und UC ... ein Erfahrungs-bericht

Fortsetzung von Seite 1

Dr. Krystian Wencel war in den 90iger Jahren als zertifizierter Trainer für Netzwerk-Betriebssysteme und Netzwerktechnologien im LAN/WAN-Umfeld tätig. Seit 2001 war er Senior Consultant bei Siemens und langjähriger Projektleiter mit den Beratungsschwerpunkten LAN/WAN-Technologien, Design, Planung und Migration konvergenter Multiservice-Netzwerke, Infrastrukturen für VoIP, Video und UC, Sicherheit und Virtualisierung.
Kontakt: krystian.wencel@kabelmail.de

Aber ist es wirklich so? Nein, es bestehen große Zweifel … und es gibt zahlreiche Gegenargumente:

1. Eine Aussage zur TCO-Reduzierung setzt überhaupt erst einmal voraus, dass ein Unternehmen die tatsächlichen TCO seiner bisherigen Kommunikationstechnik kennt, was bei TDM-basierten Alt-PBX und/oder IP-PBX-Systemen die absolut seltene Ausnahme ist und Kosten über Cost Center verteilt wurden bzw. immer noch werden. Doch ohne den direkten Kostenvergleich ist von einer Reduzierung kaum zu reden, zumal immer beliebter werdende Flatrates auch im Unternehmensumfeld eine Kostenermittlung nach dem Verursacherprinzip unwahrscheinlich bzw. unmöglich machen. Ferner werden vergleichbare Annahmen bzw. Kriterien für eine solche Kostenerhebung nicht publiziert und je moderner eine Technologie wie Video, UC oder BYOD auch ist, umso weniger Daten liegen vor.

2. Auch beim ROI sind die Versprechungen mit Vorsicht zu genießen, denn TDM- und IP-Technologien sind ja nun nicht gerade verwandte Verfahren, die durch eigenständige Gremien wie ITU bzw. IETF vertreten werden. Die Migration auf IP bedeutet aber schlagartig die notwendige Nutzung von zusätzlichen IT-Basis-Diensten, wie DNS und DHCP, die in der klassischen Telefonie gar nicht benötigt wurden. Allein die Verdopplung bis Vervielfachung der IP-Adressen in BYOD-Umgebungen, neue Netzsegmentierungen von Broadcast-Domänen, zusätzliche IP-bedingte Sicherheitsanforderungen und Berechtigungen durch Verzeichnisdienste, die Provisionierung, Softwareverteilung und andere IT-Dienste, die TDM nicht kannte, bedeuten u.U. erhebliche Mehrkosten, an die die meisten Kunden weder gedacht noch sie budgetiert haben, machen eine ROI-Betrachtung illusorisch.

3. TDM-Telefone kommen mit weniger als 2 Watt Leistung aus, was bei IP-Endgeräten nicht zu erreichen ist. Gehobene Endgeräte mit Gigabit-Ethernet-Port und großem Farbdisplay und einem Leistungsbedarf von mehr als 15 Watt zwingen sogar zu neuen „erweiterten“ PoE- Switchen (Power over Ethernet Extended). Sie bedeuten erhebliche Folgeinvestitionen, die nicht vorgesehen waren. Begrenzte Raumkapazitäten verhindern häufig den Ausbau der Etagenverteiler bzw. die Integration einer unterbrechungsfreien Stromversorgung mit notwendiger Klimatisierung.

4. Die hohen Anforderungen an die Sicherheit zwingen zum Einsatz neuer Geräte, wie z.B. dem von Session Border Controllern (SBC) oder dem Austausch bestehender Firewalls.

Die Liste ließe sich mit weiteren gravierenden Fakten fortsetzen, so dass von einer Reduzierung der TCO und schnellem ROI gar nicht die Rede sein kann. Ganz zu schweigen von der Notwendigkeit eines Redesigns der IT-Prozesse im Unternehmen, die nahezu in jeder Migration, in Planungsrichtlinien oder im technischen Designkurs immer noch ausgeklammert werden.

Berücksichtigt man die über Jahre gewachsene und forcierte vertikale Strukturierung der Organisationen mit getrennten Hoheitsbereichen für Server, Betriebssystem, Applikationen, Netzwerk, Sicherheit und klassischer Telefonie, dann kann man die Komplexität nur erahnen. Wo früher die Fraktion der „Teleföner“ ihre Anlagen autark geplant, realisiert und betrieben haben, müssen jetzt in monatelanger Zusammenarbeit mehrere Teams koordiniert werden, was die Flexibilität der Organisation extrem herausfordert. Kommen dann noch moderne Blade-Server mit integriertem Switch, d.h. mit integrierten Netzwerk- und Sicherheitsfunktionen und Virtualisierung von Diensten zum Einsatz, dann sind innerhalb der alten Organisationsstrukturen die Hoheitsbereiche und Verantwortlichkeiten kaum noch zuzuordnen.

Erinnert man sich an die Studienberichte zum erfolgreichen Projektmanagement von Gartner, Accenture oder des Bitkom-Verbandes, wonach 30 bis 70% aller Projekte scheitern, d.h. die Ziele hinsichtlich Zeit, Kosten und Qualität nicht erreichen, dann lassen sich das Risikopotential, die negativen Auswirkungen auf den Projektplan und eine Kostenexplosion nur erahnen.

In der Vorbereitung auf die Migration von TDM nach IP spielt eine zweite Gruppe eine entscheidende Rolle; die Beratungsunternehmen und Ingenieurbüros. Sicher geben sie mit ihrem technologischen Know-how und der umfangreichen eigenen Projekterfahrung vielen Kunden eine sehr wertvolle Hilfe bei der Bewältigung der Komplexität der Migration, aber ihre Beratungsleistung ist zunehmend differenziert zu bewerten.

Die Marktführer sind nahezu vollends durch einen wissenschaftlichen Anspruch stark technologiegetrieben. Sie differenzieren die Hersteller durch den Vergleich von Produktleistungsmerkmalen. Häufig bekommen nur die neuesten Entwicklungen gute Noten, während durchaus bewährte Technologien und Produkte mal schnell degradiert werden. Sicher, wir wollen alle die neuesten Technologien nutzen, doch neu bedeutet nicht zwangsläufig „reif“. Erinnern wir uns an die innovative aber Bluescreen geprägte „Reife“ einer Windows NT 4 Version.

Ferner sind die Mitarbeiter der Marktführer hoch qualifizierte Spezialisten mit umfangreichen Zertifizierungen. Aber leider sind gerade diese Zertifizierungen ein Hindernis für eine objektive Bewertung. Wer sich selbst hoher Zertifizierungen rühmen kann, weiß, wie schwer es ist, objektiv zu sein. Unbewusst neigt man dazu, sein „geballtes und wohlgemerkt herstellerspezifisches und zertifiziertes Wissen“ gegen die Wettbewerber einzusetzen.

Doch was nutzt einem Kunden das modernste IP-basierte Produkt mit SIP-Leistungsmerkmalen, wenn er die dafür notwendige Infrastruktur nicht besitzt oder nur mit größtem Investitionsaufwand schaffen kann. Wir dürfen nicht vergessen, dass weltweit agierende Unternehmen zum Teil an Standorten vertreten sind, die weder die Bandbreiten noch die Verfügbarkeit oder die notwendige Zuverlässigkeit geeigneter Netzwerkinfrastrukturen besitzen; ganz zu schweigen von u.U. sehr bürokratischen und restriktiven nationalen Regularien.

Die Vernachlässigung dieser Aspekte ist häufig der Albtraum für Kunden und Lieferanten und zwingt zu erheblichen Zugeständnissen in Kompatibilität und Funktionalität, so dass die im Labor gewonnenen hohen Produktbewertungen an den Hürden der Praxis scheitern.

Ein weiterer hinderlicher Aspekt ist die Ausschreibung von Migrationen. Hier sind mehrere nachteilige Einflüsse zu beobachten.

1. In zahlreichen kleineren Beratungsunternehmen und Ingenieurbüros haben viele „ehemalige Teleföner“ eine neue Perspektive erhalten, was einerseits sehr zu begrüßen ist, aber leider bringen sie nicht das notwendige Know-how hinsichtlich der IP-Netzwerke, IT-Services, Sicherheit und IT-Betrieb mit; mit der gravierenden Folge: Die Ausschreibung ist sehr stark auf die Abfrage von Telefonie-Leistungsmerkmalen fokussiert, um nicht zu sagen begrenzt und klammert die Integration von UC, BYOD-Umgebungen o.a. aus.. Die Komplexität solcher Projekte findet somit nicht einmal ansatzweise eine adäquate Berücksichtigung bzw. es wird alte Technik für dutzende Amtsköpfe ausgeschrieben, obwohl Kunden hochmoderne redundante MPLS-Netzwerke besitzen.

2. Viele kleinere Beratungsunternehmen haben auch nicht die finanziellen Mittel, um in die teure Ausbildung und Zertifizierung ihrer Mitarbeiter zu investieren, so dass erst die Beantwortung der Ausschreibung durch mehrere Bieter das notwendige Know-how liefert. Das wird schnell deutlich, wenn man sich anschaut, welche der sogenannten A-Kriterien zur Bewertung der Bieter priorisiert werden, die eigentlich für das Geschäft des Kunden und den täglichen IT-Betrieb absolut irrelevant sind. Folgt man den Bewertungskriterien einer üblichen Ausschreibung, stellt man fest, dass die letzten 3 Bieter einer „Short List“ sich nur marginal im Punktebereich von 83 bis 87% differenzieren. Das ist so, als ob man sich als Kunde für die Premiummarke dreier Autohersteller entscheiden müsste.

3. Weil die Erstellung von Ausschreibungsunterlagen eine z.T. sehr kostspielige Angelegenheit für alle Beteiligten ist, wird gern auf Mustervorlagen von Herstellern zugegriffen. Diese wettbewerbshemmende Vorgehensweise führt dazu, dass der Herstellername, ohne ihn zu nennen, unverkennbar in jedem Absatz wiederzuerkennen ist und wichtige A-Kriterien herstellerspezifisch dominant auftreten. Typisch bei derartigen Ausschreibungen ist, dass die Anzahl der Bieter sehr gering ist, obwohl es ein halbes Dutzend erstklassiger Marktteilnehmer gibt.

Bewertet man diese immer noch üblichen Vergabeverfahren, wo letztendlich auf Grund der geringen technologischen Unterschiede nur noch der marktübliche Portpreis über die Projektvergabe entscheidet, dann muss man den Sinn dieser kostspieligen Ausschreibungen und Teststellungen der Vergangenheit absolut in Frage stellen.

Eine besondere Rolle aus der Sicht der Beratung kommt dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zu. Das BSI ist eine politische Institution und muss in dieser Rolle alle erdenklichen Risiken benennen und Empfehlungen zu ihrer Beseitigung geben. Mangelndes Know-how auf Kunden- oder Beraterseite macht aus diesem empfehlenden Charakter allzu häufig einen „zwingend notwendig zu erfüllenden Standard“, der besonders im Behördenumfeld fast schon als „Gesetz“ mit fatalen Folgen für den Kunden angesehen wird. So werden z.B. die Schicht-2-Protokolle CDP und LLDP als unsicher eingestuft, was absolut richtig ist und die notwendige Definition von Sicherheitsregelwerken unterstreicht. Doch sind Bedrohungsszenarien, Gegenmaßnahmen und Restrisiken keine Sache einzelner Protokolle, sondern sind immer aus wirtschaftlicher und funktionaler Sicht der notwendigen Infrastruktur und Dienste dahinter zu bewerten. Um es einfach zu sagen – sie kosten Geld, unter Umständen viel Geld.

Zum Beispiel leiten einige „Beratungsunternehmen“ oder interne IT-Abteilungen aus BSI-konformen Sicherheitsanalysen unsinnige Schlussfolgerungen und Empfehlungen ab, diese Protokolle abzuschalten. Das ARP-Protokoll ist auch unsicher und so mag der Leser selbst entscheiden, wie damit zu verfahren ist.

Bleibt die Rolle der Kunden selbst. Hier stellt sich, ohne die Integrität des Kunden zu verletzen, ein breites Spektrum dar: Von exzellent aufgestellt mit erfahrenen und leistungsstarken IT-Abteilungen, ausgereiften Prozessen und angepasster Organisation bis hin zu wenig entwickelter und klar überforderter IT-Organisation.

Aber auch gut aufgestellte Kunden besitzen keine klare Kommunikationsstrategie, so dass die Unterschätzung der Projektkomplexität, falsche Erwartungen, die vernachlässigte Integration in IT-Basisdienste und die damit unzureichende Budgetierung vorprogrammiert sind. Projekte ohne das Schlüsselelement „Kommunikationsstrategie“ scheitern in diesen Organisationen regelmäßig.

Eine weitere Begleiterscheinung ist die halbherzige Migration, bei der weite Teile der historisch gewachsenen Infrastruktur z.T. gar nicht migriert werden können (Industrieanlagen, Gebäude unter Denkmalschutz, fehlende Infrastruktur und/oder Bandbreiten) und schon zu Beginn des Projektes das Risiko multiplizieren.

Einige Beispiele sollen fragliche Extremforderungen verdeutlichen:

- Call Admission Control Zero, d.h. nur die reine Signalisierung soll über das IP Netzwerk geroutet werden, während die Sprache über das PSTN geführt wird.
- Unterstützung von weit entlegenen analogen a/b Endgeräten (> 400 Meter)
- Unterstützung für Geräte mit Impuls-Wahlverfahren
- DECT-Integration großer Installationen

Aus der Sicht der Hersteller muss man eindeutig sagen: Diese Anforderungen sind technologisch eindeutig erfüllbar und werden in Angeboten natürlich schnell als Alleinstellungsmerkmale vermarktet, doch um welchen Preis von Komplexität, Stabilität, Verfügbarkeit und Managebarkeit?

Die fehlende Kommunikationsstrategie im Unternehmen behindert somit auf lange Sicht die Umsetzung moderner Technologien.

Sicher gibt es „gute Argumente“ für eine Abwärts-Kompatibilität oder den Investitionsschutz und kostengünstige Flat-Rates sind der Treiber für CAC 0, aber eine potenzielle Integration von UC und der flexible Einsatz von sozialen Plattformen oder von BYOD-Architekturen wird dadurch nicht gefördert.

Wenn also bei einer Migration so viele Risiken wirksam sind, was ist dann die bessere, alternative Vorgehensweise?

Dabei muss zunächst die Dreiecksbeziehung Kunde–Berater–Hersteller neu bewertet werden.

Der Kunde muss höchste Priorität auf eine umfassende Kommunikationsstrategie legen, die Teil seiner Geschäftsstrategie ist und die Anforderungen an die Wertschöpfung widerspiegelt, d.h. es sind die Fragen zu beantworten:

- „Wie soll die moderne Kommunikationsinfrastruktur das heutige und vordergründig das zukünftige Geschäft stützen und/oder entwickeln?“
- „Welche Komplexität und welche Auswirkungen auf die Infrastruktur sind zu erwarten?“
- „Welche bisherige Infrastruktur kann ohne Verlust an Wertschöpfung abgelöst werden und welche nicht?“
- „Welche IT-Dienste sind ebenfalls betroffen und welche Auswirkungen hat das auf ein zu planendes Budget?“
- „Welche Auswirkungen hat diese Strategie auf die bestehende Organisationsstruktur?“

Die Antworten auf diese Fragen werden eines ganz sicher schnell zeigen, dass sie durch einzelne Telefonieleistungsmerkmale nicht zu geben sind. Die Migration auf eine neue Infrastruktur kann nur wertschöpfungsorientiert erfolgen.

Damit es keine Missverständnisse gibt, sage ich es deutlich: Die Abfrage von Leistungsmerkmalen ist notwendig, aber sie darf nicht das alles entscheidende Primat für einen Projektauftrag sein.

Die zweite Gruppe, die der Beratungshäuser/Ingenieurbüros, muss verstärkt in ihre Ausbildung investieren, weil es neben Voice /Video und UC wohl kaum einen komplexeren IT-Dienst gibt. Die Komplexität liegt darin begründet, dass hier nicht das klassische Client-Server-Prinzip mit einem Kommunikations-Protokoll und -Port vorliegt, sondern ein vielschichtiges Multiclient-Multiserver-Prinzip, das gleichzeitig eine Vielzahl von Protokollen (SIP, SDP, TLS, RTP, RTCP, …) mit dynamischer Portzuweisung nutzt. Die Nutzung von Telefon- bzw. Videokonferenzen mit mehreren Teilnehmern und Dokumenten-Sharing lässt die Komplexität und die vermaschten Kommunikationsbeziehungen nur erahnen. Insbesondere die dynamische Portzuweisung und die immense Bedeutung von Network Address Translation (NAT) in Filialkonzepten sowie die Implementierung von Sprachverschlüsselung stellt eine immense Herausforderung an das Know-how der Beratungsunternehmen dar. Neben dem technologischen Aspekt muss die intensive Auseinandersetzung mit dem Kerngeschäft des Kunden die zweite tragende Säule einer geschäftsorientierten Kommunikationsberatung bilden.

Auch die Hersteller müssen umdenken und viel intensiver ihre Architekturen zu einer ganzheitlichen wertschöpfenden Lösung ausbauen. Der noch gegenwärtig starke Fokus auf einzelne Leistungsmerkmale bzw. die Besessenheit, auch noch die letzte Kundenanforderung nach einem LM der alten TDM-Welt in SIP abzubilden, muss abgelöst werden durch die Entwicklung von Architekturen, die bedingungslos geschäftsfördernd, offen und betreiberfreundlich sind. Der Siegeszug der Smartphones macht deutlich, dass nicht ihre begrenzten Telefonieleistungsmerkmale ihren Erfolg begründen, sondern ihre ungeheure Flexibilität, Voice, Video und UC mit Mini-Apps zu integrieren. Damit stellen sie nicht nur klassische Mobiltelefone, sondern mehr und mehr auch den Einsatz hochwertiger Festnetz-Endgeräte völlig in Frage.

Da die heutige Kunden–Berater–Hersteller-Beziehung durch isoliertes Handeln geprägt ist und die Anforderungen moderner Kommunikationsstrategien nur mangelhaft bedient werden, stellt sich die Frage:

„Was sind dann die verlässlichen Kriterien für eine zukunftsweisende VoIP/UC-Migration? Wie sollen sich Beratungshäuser aufstellen und Angebote bewerten bzw. wie sollen Hersteller ihre Produkte anbieten, wenn der Vergleich von Produkten und ihrer Leistungsmerkmale nicht mehr DER Maßstab sind?“

Die Antwort lässt sich grundsätzlich nur aus den Anforderungen des Geschäftsmodells des Kunden an die Kommunikation und seiner Auswirkungen auf die Geschäftskontinuität ableiten.

Die Geschäftskontinuität ist das einzige objektive und relevante Kriterium, das universelle Gültigkeit besitzt und aus dem sich trotz Kundenindividualität eine zugeschnittene Lösung für die Wertschöpfung ableiten lässt.

Wir sprechen auch von einer IT-basierten Wertschöpfung und sie macht ganz deutlich:

Es geht nicht um einzelne Produkte, unterstützte Protokolle oder Leistungsmerkmale; es geht um komplexe wertschöpfende Lösungen.

Aber was charakterisiert eine Lösung? Versuchen wir, eine Definition zu geben:

„Eine Lösung ist eine abgegrenzte Produktumgebung, bestehend aus Hardware, Software und Diensten, deren Komponenten einen lösungsorientierten, aufeinander abgestimmten Reifegrad besitzen; Komponenten, die durch eindeutig definierte Schnittstellen interagieren, um die geforderten Geschäftsanforderungen des Kunden zu erfüllen.“

Was zunächst abstrakt klingt wird klarer, wenn man nach Analogien sucht und gerade die klassischen Ingenieurwissenschaften wie der Brückenbau sind ein exzellentes Beispiel für moderne Lösungen und ihre Grundprinzipien besitzen interessanterweise auch für IT-Projekte Gültigkeit.

Ein geniales Bauwerk wie das „Viaduc De

Abbildung 1: Schlüsselleistungsindikatoren

Millau“ in Frankreich stellt mit seinen Komponenten wie Pfeilern unterschiedlicher Höhe, Stahlträgern und –seilen optimaler Tragfähigkeit, also Komponenten mit einem aufeinander abgestimmten Reifegrad, die perfekte Lösung dar. Die Architektur dieser Schrägseilbrücke mit optimierten Auffahrten von und zu den Autobahnen (Topologie und Schnittstellen) erfüllt die Geschäftsanforderung; zwei durch ein unwegsames Tal getrennte Punkte wirtschaftlich miteinander zu verbinden.

Das Bauwerk repräsentiert anschaulich auch die für IT-Projekte so wichtigen Schlüsselleistungsindikatoren, die in Abbildung 1 zu sehen sind. Ihre Vollständigkeit kann jederzeit verfeinert werden.

Bezogen auf Voice/UC-Projekte kann man wichtige Schlussfolgerungen ziehen:

1. Das wirtschaftliche Geschäftsziel bzw. seine Wertschöpfung legt die Anforderung an die Infrastruktur fest und nur die besondere Architektur, ihre Topologie, ihre Verfügbarkeit, ihre Leistungsfähigkeit, Skalierung, Managebarkeit und Sicherheit machen die Basis für die Einzigartigkeit der Lösung aus. Erst wenn diese adäquate Infrastruktur vorhanden ist, können weitere Services (Outsourcing oder ITIL-basierte Managed Services) realisiert werden.

2. Diese Kriterien sind als Schlüsselleistungsindikatoren anzusehen und können nach Anforderung, wie am Beispiel der Sicherheit, beliebig detailliert und als messbare Erfolgsfaktoren für die Projektziele und zur Prozesskontrolle eingesetzt werden.

3. Die Umsetzung eines abgestimmten Reifegrades für alle Lösungskomponenten innerhalb der definierten Architektur und Topologie gewährleistet deren optimales Zusammenspiel und ist somit von entscheidender Bedeutung für den Projekterfolg. Wird der Reifegrad für eine Komponente nicht erfüllt, degradiert sie die Lösung als Ganzes.

4. Erst der Austausch einzelner Leistungsmerkmale durch allgemeingültige Leistungsindikatoren ermöglicht die optimale Erfüllung der Geschäftsanforderungen.

5. Leistungsindikatoren gestatten die eindeutige Definition eines Services pro Port und ermöglichen so ein transparentes abgestuftes Portpreismodell, was ideal dem Sinn einer Cloud Computing Umgebung entspricht. Ein transparentes Portpreismodell könnte eine teure und leistungsmerkmalorientierte klassische Ausschreibung ablösen.

6. Mit dem OSI-Modell besitzen wir ein Rahmenwerk für den Bau und Betrieb einer IT-Infrastruktur; und hält man sich an seine Elemente, so wird kein Detail vergessen und man bleibt im geplanten Projektbudget. Mit der Schicht eins, der physikalischen Infrastruktur, schaffen wir die Basis und enden mit der Präsentationsschicht bei der Sicherheit und dem IT-Management. Abstrahiert man auf eine imaginäre Schicht 8, so kann man selbst Prozesse und den Umbau der Organisation einschließen.

7. Die Summe aller erfüllten Kriterien macht die Einmaligkeit einer kundenspezifischen Lösung aus und sichert die Geschäftswertschöpfung.

Kehren wir zum „Geschäftsmodell der Brücke“ zurück. Schnell wird deutlich: Niemand würde eine Brücke befahren, deren Leistungsindikatoren Verfügbarkeit, Zuverlässigkeit, Skalierung, Sicherheit, Überwachung und Notfallpläne etc. nicht gewährleistet sind. Hier akzeptieren wir mit absoluter Selbstverständlichkeit, dass diese Kriterien untrennbar miteinander gekoppelt bzw. abgestimmt sind und dass sie auch eingehalten werden. In der IT aber ignorieren wir das eine oder andere Kriterium mal schnell. Unternehmen schreiben die modernste SIP-Kommunikation aus, sind aber oft wenig gewillt, eine geeignete Infrastruktur zu bauen und verzichten aus Kostengründen auf Reifegrade, auf dringend notwendige Sicherheit, Services und Compliance.

Was bedeutet nun abgestimmter oder optimaler Reifegrad einer Lösung?

Abbildung 2 soll eine Vorstellung geben: Der Reifegrad einer Lösung bedeutet hier nicht die generelle Bereitstellung eines Leistungsmerkmals, ihrer Anzahl, eines Protokolls oder einer einzelnen Komponente, sondern es bedeutet die Bereitstellung einer notwendigen und verzahnten Infrastruktur mit der geforderten Skalierung, Verfügbarkeit, Performance, Managebarkeit, Provisionierung, Sicherheit bis hin zu einem Backup und Desaster Recovery für alle Komponenten. Ein nahezu identischer Reifegrad soll durch die geraden horizon-

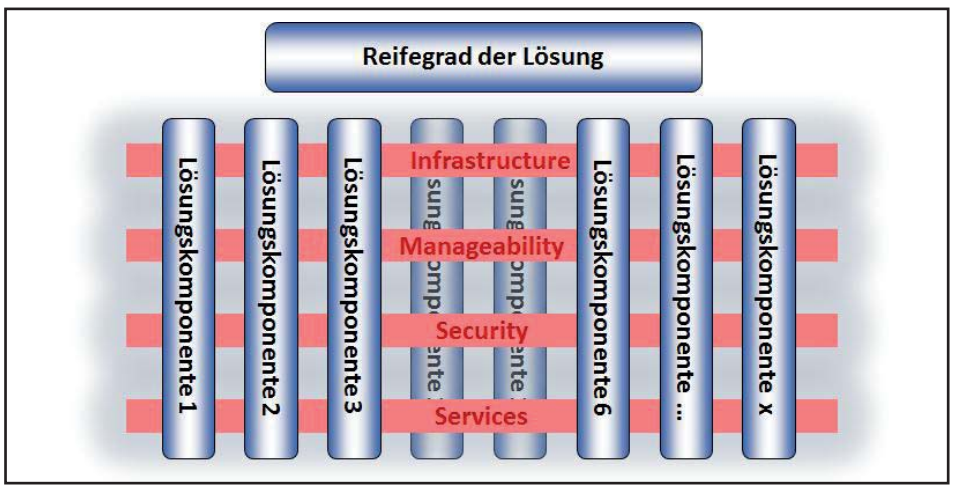


Abbildung 2: Reifegrad einer Lösung

talen Balken dargestellt werden, während ein zickzackförmiger Balken für sehr unterschiedliche Reifegrade stehen würde.

Übertragen auf eine Voice-, Video- und UC-Architektur heißt das, die Komponenten Softswitch, UC-, Media-Server, Voice-Mail-, Conferencing-Server etc. stehen in einer engen Relation zueinander und sie benötigen einen aufeinander abgestimmten Reifegrad der Leistungsparameter. Jede dieser Komponenten muss sich in ein ganzheitliches Konzept von Managebarkeit, Sicherheit und Services integrieren lassen und einheitliche Kriterien erfüllen. Bewertet man Angebote der Hersteller unter dem Aspekt des Reifegrades, so wird man z.T. sehr zackige Balken feststellen.

So macht es absolut keinen Sinn, Softswitche auf Kapazitäten von mehreren 10.000 Nutzern zu „überskalieren“, wenn andere Komponenten der „Lösung“ dramatisch „unterskalieren“ und es macht ebenso wenig Sinn, die Implementierung z.B. eines Protokolls wie 802.1x zur Zugriffssicherung von Endgeräten hervorzuheben, wenn die notwendige skalierbare, managebare Infrastruktur für RADIUS, die PKI, die Zertifikats-Provisionierung und der Zertifikatslebenszyklus vernachlässigt werden. Auch ist die häufige Kundenforderung, SIP-kompatible Endgeräte von Dritt-Herstellern einzusetzen, zwar nachvollziehbar, aber dennoch aus Kostengründen absolut kontraproduktiv, weil Sicherheit, Managebarkeit, Provisionierung, Softwareverteilung nicht mehr gewährleistet sind, d.h. ein sichtlich vorhandener hoher Reifegrad eines abgestimmten Endgerätes wird sogar gezielt zerstört und degradiert die Lösungsorientiertheit und Wertschöpfung.

Besonders anschaulich ist der Reifegrad bei der Skalierung und der Mandantenfähigkeit. Er führt schnell zu einem nicht vorhergesehenen Serverwildwuchs für schlecht skalierende und nicht mandantenfähige Dienste, schlechter Service-Performance, der Notwendigkeit, die Verfügbarkeit kritischer Dienste z.B. durch Clustertechniken und/oder Virtualisierung auszudehnen. Die Folge ist ein unüberschaubares, kompliziertes und komplexeres Zusammenspiel der Komponenten mit kritischen Fail-over-Szenarien, sehr kostenintensiver Fehlersuche und intransparentem Management.

Wichtig ist ebenso die Berücksichtigung der ergänzenden Dienste. Dazu ein Beispiel: Die Skalierung der Telefonie auf 100.000 Nutzer ist ohne große Anstrengungen möglich, aber gleichzeitig für 100.000 Endgeräte die zertifikatsbasierte 802.1x Portsicherheit umzusetzen, ist nicht nur kostspielig, sondern auch eine sehr stolze technische Herausforderung.

Gelegentlich tritt ein konträres Verhalten der Leistungsindikatoren auf. Die vielseitig geforderte Sprachverschlüsselung durch Anwendung von TLS und SRTP verkompliziert bzw. behindert das Management und Monitoring von Diensten. Ein Brechen der Verschlüsselung für Monitoringzwecke ist aber aus Compliance-Gründen nicht zulässig. Diese beiden Beispiele aus dem Sicherheitsbereich zeigen auch, dass sie zwar BSI-konform sind, aber extreme Herausforderungen generieren.

Die Betrachtung und Anwendung des lösungsorientierten Reifegrades hat einen weiteren wesentlichen Vorteil: Sie ist ebenso auf neue Dienste wie Cloud Computing, Virtualisierung, die Integration von sozialen Netzen, BYOD- und zukünftige Architekturen anwendbar.

Wieder sind es die Hersteller, die mit der Integration dieser Dienste und Geräte in ihre Voice, Video bzw. UC-Umgebungen werben und die Beratungshäuser, die diesen Trend als Mega-Innovation preisen, doch niemand trifft Aussagen zur notwendigen Infrastruktur, Skalierung, Managebarkeit oder Sicherheit.

Die Kunden, getrieben von blendenden Leistungsmerkmalen, haben derweil Angst, einen Hype zu verpassen.

Besinnt man sich aber auf den Reifegrad und die oben genannten Leistungskriterien stellt man schnell fest:

- So genial diese Entwicklung auch ist, sie ist zum gegenwärtigen Zeitpunkt unreif.
- Ihre Wertschöpfung ist kaum bzw. nicht nachgewiesen.
- Private, geschäftliche und Kundendaten werden vermischt, wodurch ein erhebliches rechtliches Risiko entsteht.
- Rechtezuweisung, Sicherheit, Provisionierung, Support u.v.a.m. sind heute völlig offen.

Ein wirklich lösungsorientierter Ansatz mit hohem Reifegrad würde entstehen, wenn eine komplette Voice/UC- Infrastruktur inklusive aller zusätzlichen Dienste als festskaliertes Modul angeboten werden würde. Hierbei spielen Referenzarchitekturen eine große Rolle, weil erst sie standardisierte Lösungen ermöglichen. Aus der Notwendigkeit heraus, Kosten zu sparen, versuchen sich einige Hersteller in dieser Entwicklung. Leider nur mit mäßigem Erfolg, denn die Standardisierung erfolgt vertikal, also produktorientiert und nicht horizontal, lösungsorientiert. Diese Diskrepanz ließe sich nur durch die Definition von Richtlinien (Policy) für die Produktentwicklung und die Integration von Voice/UC-Komponenten erreichen.

Bedauerlicherweise verfolgen nur wenige Kunden einen policybasierten Ansatz für die Beschreibung ihrer IT-Lösungen, doch der Vorteil ist bestechend. Sie definieren die Policy für einen Dienst an einem Port, wie er bereitzustellen ist und bedienen sich genau der oben genannten Leistungsindikatoren. Mit welcher Hardware und Software oder von welchem Hersteller der Dienst realisiert wird, ist dann zweitrangig, aber in jedem Fall erfüllt eine solche Policy die erforderliche Herstellerunabhängigkeit, die Geschäftstauglichkeit und nicht zuletzt die Compliance. Diese Vorgehensweise wäre auch der Garant für die Geschäftswertschöpfung durch Innovation und die schrittweise Ablösung musealer Technologien.

Die Umsetzung der oben genannten Kriterien in einer Entwicklungsrichtlinie wäre auch ein großer Fortschritt für die Hersteller selbst, so dass ausgehend von einer modularen Skalierung von z.B. 10.000 Nutzer-Ports eine optimale Skalierung für alle Komponenten umsetzbar wäre und hierarchische Architekturen ermöglichen würde. Eine solch modulare Infrastruktur ließe sich als Service aus der Box mit geringstem Aufwand konfektionieren und verkaufen und stellte eine echte Referenzarchitektur dar.

Zum Verständnis einer hierarchischen Architektur kann wieder das Brückenmodell herangezogen werden. Kein Architekt käme auf die Idee, eine zweite Brücke direkt parallel zur ersten zu bauen, um die Skalierung, sprich den Verkehrsdurchsatz, zu erhöhen. Eine zweite Brücke wird immer in gehörigem Abstand zur ersten gebaut, damit sich Verkehrsströme entkoppeln lassen und nicht die Zufahrtstrassen zum Nadelöhr werden. Was ist also der Unterschied zwischen einer Brücke und einer IT-Umgebung für Voice/Video und UC? Aus Sicht der oben beschriebenen Kriterien absolut keiner; wir müssen nur den Mut entwickeln, die jahrhundertealte Tradition der Ingenieurwissenschaften auf die IT anzuwenden.

Wir stehen heute an der Schwelle zur industrialisierten IT und das Cloud-Computing ist das Synonym für diese Entwicklung. Wir überlassen zunehmend private Daten des Unternehmens, der Kunden und der eigenen Person, eigentlich unsere gesamte persönliche und unternehmerische Identität einer „privaten“ und öffentlichen Cloud; also lassen Sie uns ohne Abstriche die gleichen bewährten industriellen Kriterien anwenden.

ComConsult Veranstaltungskalender

Aktuelle Veranstaltungen

Lokale Netze für Einsteiger, 21.01. - 25.01.13 in Aachen

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

Preis: € 2.490,-- netto

Interne Absicherung der IT-Infrastruktur, 28.01. - 30.01.13 in Bonn

Bedingt durch Netzkonvergenz, Mobilität und Virtualisierung hat die interne Absicherung der IT-Infrastruktur in den letzten Jahren enorm an Bedeutung gewonnen. Heterogene Nutzergruppen mit unterschiedlichstem Sicherheitsniveau teilen sich eine gemeinsame IP-basierte Infrastruktur und in vielen Fällen ist der Aufbau sicherer, mandantenfähiger Netze notwendig. Dieses Seminar identifiziert die wesentlichen Gefahrenbereiche und zeigt effiziente und wirtschaftliche Maßnahmen zur Umsetzung einer erfolgreichen Lösung auf. Alle wichtigen Bausteine zur Absicherung von LAN, WAN, Endgeräten, RZ-Bereichen, Servern und SAN werden detailliert erklärt und anhand konkreter Projektbeispiele wird der Weg zu einer erfolgreichen Sicherheits-Lösung aufgezeigt.

Preis: € 1.890,-- netto

RZ-RZ-Kopplung - alles nur eine Frage der Bandbreite?, 04.02.13 in Düsseldorf

Immer mehr Unternehmen sehen sich derzeit damit konfrontiert, ihre Rechenzentrumsdienstleistungen über entfernte Standorte redundant anzubieten. Neben den entsprechenden Vorgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI) für Desaster Recovery Konzepte fordert auch die Kundenseite entsprechende Service Level Agreements zur Hochverfügbarkeit ihrer Dienste und Daten ein. In diesem Seminar werden die aktuellen Techniken vorgestellt, technisch erläutert und für die richtige strategische Entscheidung zu einem Gesamtkonzept zusammengeführt.

Preis: € 990,-- netto

Netzzugangskontrolle: Technik, Planung und Betrieb, 04.02. - 06.02.13 in Düsseldorf

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

Trouble Shooting in vernetzten Infrastrukturen, 05.02. - 08.02.13 in Aachen

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

Preis: € 2.290,-- netto

Bring Your Own Device, 18.02.13 in Bonn

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

Preis: € 990,-- netto

TCP/IP intensiv und kompakt, 18.02. - 22.02.13 in Stuttgart

LAN-, WLAN- und WAN-Netzwerke sind heutzutage IP-Netze, und ein Verzicht auf Nutzung des IP-basierten Internet undenkbar. Auch für früher nur mit herstellerspezifischen Protokollen in Verbindung gebrachte Anwendungsgebiete wie Telefonie oder Produktionsumgebungen gibt es mittlerweile geeignete IP-basierte Lösungen. Hersteller und Dienstanbieter versuchen den Eindruck zu vermitteln, die Nutzung sei kinderleicht, fast schon plug and play - man trägt ein paar Adressen ein (wenn überhaupt), und es kann losgehen. Falsch!

Preis: € 2.490,-- netto

IP-Wissen für TK-Mitarbeiter, 18.02. - 19.02.13 in Stuttgart

Dieses Seminar vermittelt kompakt und effizient das IP-Wissen, das TK-Mitarbeiter ohne Vorkenntnisse zur Planung und zum Betrieb von IP-basierten Telefonie-Lösungen benötigen. Alle Seminarinhalte werden von einem Referenten mit hoher Praxiserfahrung betreut. Ziel ist dabei bewusst, statt einer umfassenden Theorieschulung gezielt die Aspekte vorzustellen und unter Praxis-relevanten Gesichtspunkten zu beleuchten, die erfahrungsgemäß aus Sicht einer IP-basierten Telefonielösung wichtig sind.

Preis: € 1.590,-- netto

Recht und Datenschutz bei Einführung von Voice over IP, 18.02. - 19.02.13 in Stuttgart

Durch die Einführung von Voice over IP ergeben sich zahlreiche neue Funktionen einer Telefonanlage und eine wesentlich bessere Zusammenarbeit von TK- mit CRM- und anderen IT-Systemen. Gleichzeitig lassen sich auf diese Weise erhebliche Kostensenkungen durch gemeinsame Nutzung der IT-Infrastruktur mit der TK erzielen. Dabei entstehen jedoch zahlreiche Gefahren in Bezug auf Datenschutz und Datensicherheit der Mitarbeiter. Bei Überwachungsfunktionen sollten Geschäftsführung und Mitarbeiter bzw. Betriebs- oder Personalrat offen Vor- und Nachteile bestimmter Funktionen diskutieren und abstimmen.

Preis: € 1.590,-- netto

IPv6: Planung, Migration und Betrieb, 25.02. - 27.02.13 in Köln

In diesem Seminar erfahren Sie, wo sich mit einer IPv6-Einführung etwas ändert, und wie Migrationsphase und Betriebsalltag aussehen.

Preis: € 1.590,-- netto

Zertifizierungen

ComConsult Certified Network Engineer

Lokale Netze
21.01. - 25.01.13 in Aachen
22.04. - 26.04.13 in Aachen
09.09. - 13.09.13 in Aachen
25.11. - 29.11.13 in Aachen

TCP/IP intensiv und kompakt
18.02. - 22.02.13 in Stuttgart
13.05. - 17.05.13 in Bonn
07.10. - 11.10.13 in Stuttgart

Internetworking
11.03. - 15.03.13 in Aachen
17.06. - 21.06.13 in Aachen
14.10. - 18.10.13 in Aachen

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

ComConsult Certified Trouble Shooter

Trouble Shooting in vernetzten Infrastrukturen
05.02. - 08.02.13 in Aachen
11.06. - 14.06.13 in Aachen
24.09. - 27.09.13 in Aachen

Trouble Shooting für Netzwerk-Anwendungen
12.03. - 15.03.13 in Aachen
09.07. - 12.07.13 in Aachen
05.11. - 08.11.13 in Aachen

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

ComConsult Certified Voice Engineer

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen
25.02. - 27.02.13 in Köln
03.06. - 05.06.13 in Bonn
16.09. - 18.09.13 in Berlin
02.12. - 04.12.13 in Bonn

Session Initiation Protocol Basis-Technologie der IP-Telefonie
18.03. - 20.03.13 in Berlin
24.06. - 26.06.13 in Köln
07.10. - 09.10.13 in Stuttgart

Umfassende Absicherung von Voice over IP und Unified Communications
11.04. - 12.04.13 in Bonn
18.07. - 19.07.13 in Bonn
04.11. - 05.11.13 in Bonn

Optionales Einsteiger-Seminar: IP-Wissen für TK-Mitarbeiter
18.02. - 19.02.13 in Stuttgart
13.05. - 14.05.13 in Bonn
30.09. - 01.10.13 in Düsseldorf

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

ComConsult Certified Service Catalogue Manager

Servicialisierung - Leitkonzept für verlässliche Service-Erbringung
18.03. - 19.03.13 in Berlin

Service-Identifizierung - Von Service-Begriff bis Service-Konsumentennutzen
22.04. - 23.04.13 in Düsseldorf

Service-Offerierung - Von Service-Spezifizierung bis Service-Katalogisierung
11.06. - 12.06.13 in Aachen

Paketpreis für alle drei Seminare € 4.290,-- netto (Einzelpreise: je € 1.590,-- netto)

Impressum

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

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

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

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