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

Schwerpunktthema

Werden SDN und OpenFlow herkömmliche Netzwerke verdrängen?
Teil 2

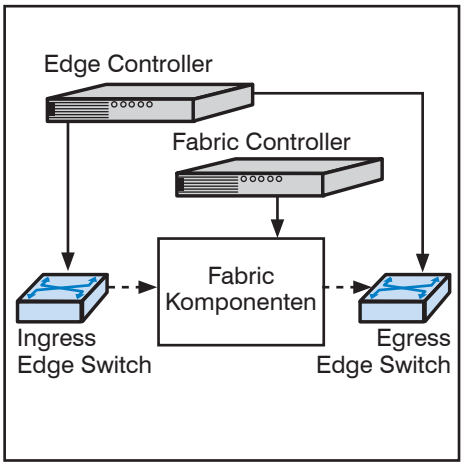
von Dipl.-Inform. Petra Borowka-Gatzweiler

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.

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

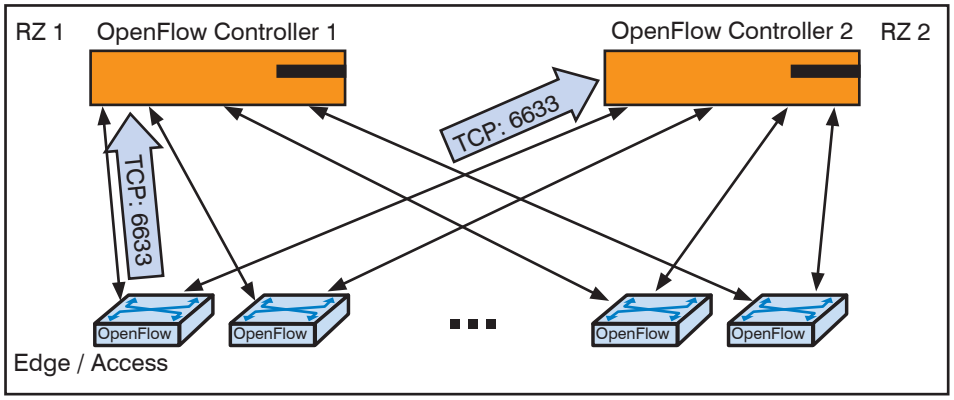


Abbildung 2.11: OpenFlow Kanäle zwischen Controllern und Switches

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

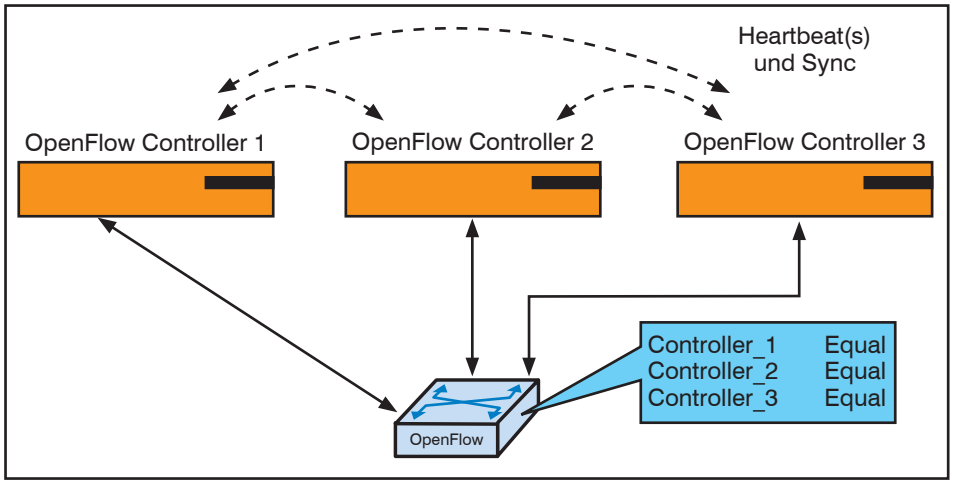


Abbildung 2.12: Mehrere OpenFlow Controller mit der Rolle "Equal"

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.