ComConsult Research

Der Netzwerk Insider

Januar 2013

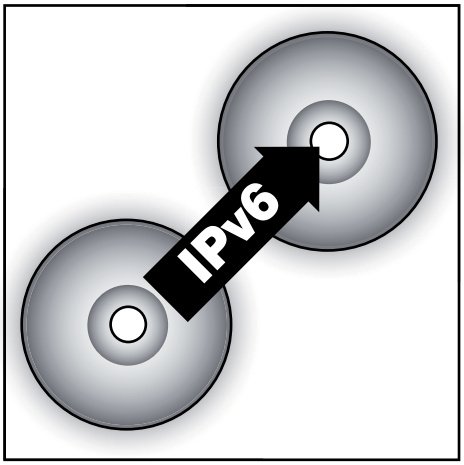
Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

IPv6 ist eine Software-Migration! Teil 1: Problemfälle

von Markus Schaub

Machen wir uns nichts vor: die Migration zu IPv6 ist kein Selbstzweck und somit auch kein rein internes Netzwerk- oder IT-Thema. Will man zu IPv6 migrieren, muss vor allem eines sichergestellt werden: unternehmenskritische Prozesse dürfen nicht gestört werden und die weniger kritischen am besten auch nicht. Perfekt verläuft eine Migration dann, wenn außerhalb der betroffenen IT-Abteilungen niemand etwas davon merkt.



Natürlich ist das ein frommer Wunsch, der unerfüllt bleiben wird. Zu groß sind die Verquickungen von IP mit allen anderen Ebenen des OSI-Modelles und auch darüber hinaus: bis in die Software hinein. Das beginnt bereits beim Dual-Stack. Die Entscheidung, ob V4 oder V6 wird nicht von irgendeinem ominösen Session-Layer und schon gar nicht vom Transport- oder Netzwerk-Layer getroffen, sondern von der Anwendung, beispielsweise dem Browser. Je nach Prozess kann es aber auch das Betriebssystem sein, das diese Entscheidung in seiner unendlichen Weisheit fällt. Und hier ist zu beachten, dass moderne Betriebssysteme den Dual-Stack per Default aktiviert haben, egal ob Windows, Linux oder OS X.

weiter auf Seite 8

Zweitthema

Multidimensionale Datenverarbeitung und die Konsequenzen für private DV-Infrastrukturen

von Dr. Franz-Joachim Kauffels

Die Indizien, dass wir vor einem massiven technologischen Umbruch stehen, der qualitativ und quantitativ der großen Evolution von der zentralen zur verteilten DV Mitte der 90er Jahre entspricht, verdichten sich mit großer Geschwindigkeit. Das neue Szenario kann man als „Multidimensionale DV“ bezeichnen. Aus der Perspektive eines Benutzers zeichnet sie sich durch Flexibilität, Mobilität und die Nutzung der modernen Endgeräte aus.

Damit das auch funktioniert, muss die leistungserbringende DV in vielen Bereichen völlig umstrukturiert werden. Provider haben das schon erkannt und in den letzten Jahren mit erheblichem Kostenaufwand umgesetzt. Betreiber privater Netze werden sich den Änderungen nicht mehr lange entziehen können. Schlüsseltechnologien der multidimensionalen DV sind skalierende Web-Applikationen, Virtualisierung, hochdichte und funktional reichhaltige Chips für Server, Speicher und Switches sowie SDN auf der Seite der Netze und Gigabit-Wireless-Techniken bei der Versorgung der Benutzer. Diese aktuell meist einzeln diskutierten Technologiebereiche sind Komponenten eines Gesamtbildes, dessen Verständnis nicht nur die zukünftige Planung erleichtert, sondern auch Fehlinvestitionen in sterbende Technik vermeiden hilft.

weiter auf Seite 16

Geleit

Wie kommunizieren wir in Zukunft?

ab Seite 2

Standpunkt

Hochfrequenz geht seltsame Wege!

ab Seite 15

Aktueller Kongress

ComConsult Netzwerk-Redesign Forum 2013

ab Seite 4

Neues Seminar

Aufbau und Management von Internet-DMZ und internen Sicherheitszonen

auf Seite 6

Zum Geleit

Wie kommunizieren wir in Zukunft?

Telefon, Video, Email: reicht das nicht aus? Oder was ist falsch mit unserer etablierten Art zu kommunizieren? Der Schlüssel zur Antwort liegt in zwei Kern-Kriterien der Unternehmens-Kommunikation:

- **Effizienz**
- **Transparenz**

Effizient kommunizieren bedeutet, mit dem kleinst möglichen Aufwand genau die richtigen Ansprechpartner zu erreichen und zu vorgegebenen Deadlines die benötigte Antwort oder Mitwirkung zu erhalten.

Transparenz bedeutet, dass alle an einem Prozess beteiligten Personen über die aktuelle Situation, die bisherigen Aktivitäten und die zukünftigen Aktivitäten des Prozesses informiert sind.

Nehmen wir Email-Kommunikation als Beispiel für ein gängiges Element der Team-Kommunikation:

- Dokumente, Grafiken, Fotos und Videos werden als Anhang an beliebige Teammitglieder verschickt.
- Es ist unklar, ob das komplette Team erreicht wurde und bei Antworten bleibt offen, ob das komplette Team eingebunden wurde.
- Startet eine Diskussion, ist der Ablauf der Diskussion je nach Email-Client kaum nachvollziehbar.
- Will ein neues Teammitglied später Diskussionen oder Ereignisse der Vergangenheit nachschlagen, ist das kaum sinnvoll möglich.
- Alle Anhänge verlieren schon mit der Versendung ihre Versions-Kontrolle. Es ist bereits nach Stunden unklar, ob diese Anhänge so noch aktuell sind oder ob längst neue Versionen existieren. Zugleich lassen sie den Speicherbedarf des Email-Systems explodieren.
- Die Suche nach Anhängen der Vergangenheit ist fehleranfällig und führt wieder zu der Frage der korrekten Version. Zudem kann die Suche je nach Email-System zeitaufwendig sein.
- Es ist völlig unklar was die Empfänger mit den Anhängen machen. Das Unternehmen verliert komplett die Kontrolle über den Ort und den Zugriff auf diese Anhänge.
- Jede Prozess-orientierte Email-Kommunikation geht in einer Flut anderer Emails unter. Zwar lässt sich dieses Problem je nach Email-System reduzieren (Tagging in Google-Mail oder effiziente Suche und Filterung in Apple-Mail

als Beispiel), aber das bleibt schon wieder der individuellen Handhabung des Empfängers vorbehalten.

Wenn es ein Beispiel für eine nicht effiziente und in keiner Weise transparente Kommunikation gibt, dann ist das Email-Kommunikation. Email wurde ursprünglich entworfen, um eine private 1-zu-1 Kommunikation umzusetzen und nicht als Basis für eine Team-Kommunikation. In den letzten Jahren wurden viele Versuche unternommen, den Umgang mit Emails effizienter zu gestalten (noch einmal der Hinweis auf Gmail), aber keiner dieser Versuche kann wirklich überzeugen. Datei-Anhänge in Emails sollten in Unternehmen schlicht verboten werden.

Schon an diesem Beispiel werden aber auch Fragen klar, die sich geradezu aufdrängen:

- Sollte die Kommunikation im Unternehmen nicht in einem geschlossenen Medium erfolgen, um dem Bedarf des Unternehmens genau gerecht zu werden?
- Sollten Dokumentenspeicher und Kommunikation nicht klar angegrenzt werden?
- Sollte jede Kommunikation im Unternehmen Prozess-orientiert erfolgen?

Die letzte Frage lässt sich natürlich mit nein beantworten. Es wird immer den Bedarf für einfache und triviale Kommunikationen geben. Allerdings ist gerade dafür Email eigentlich nicht perfekt, ein IM-Tool wäre hier besser. Umgekehrt muss aber auch die Frage gestellt werden, ob diese einfachen Tools eine geeignete Basis für wichtige Unternehmens-Prozesse sind. Interessanter wäre die Nutzung eines Tools, das neben einer Chat-Kommunikation gleichzeitig die Basis für Prozess-Kommunikation ist.

Spannend ist die Frage nach dem Dokumentenspeicher. Ein zu einem Prozess gehöriges Dokument sollte immer nur an einer Stelle existieren. Dabei sollte transparent sein:

- Dass das Dokument existiert und welchen Wert es für den Prozess hat
- Welche Teammitglieder Zugang haben
- Wer zugegriffen hat, wann zugegriffen wurde und welche Änderungen erfolgten
- In welchem Umfang das Dokument Externen zugänglich gemacht wurde

In jedem Fall sollte die Möglichkeit bestehen, alte Versionen wieder herzustellen.

Wenn man über Dokumente spricht, muss man auch über die Endgeräte sprechen, über die man auf diese Dokumente zugreift. Der Trend zu mehreren Endgeräten pro Benutzer und dabei speziell zu mobilen Endgeräten stellt die traditionelle Speicherung von Dokumenten infrage. Dokumente müssen für alle Geräte ortsneutral zugreifbar sein. Dies führt automatisch auch zu mehr Risiken im Sinne des Zugangs nicht autorisierter Personen. In letzter Konsequenz gehen die Ortsneutralität und der Einsatz mobiler Endgeräte her mit dem Bedarf des Erfassens des Zugangs zu Dateien und erfolgter Weitergaben an Externe.

Wenn aber das Dokumenten-Management im Zusammenhang mit mobilen Endgeräten sowieso die etablierte Form der Speicherung und des Zugangs infrage stellt, dann liegt es nahe, in Kombination mit der Email-Diskussion eine prozessorientierte und transparente Form der Speicherung zu erwägen.

Dies haben auch die Anbieter entsprechender Produkte erkannt. So gibt es momentan mindestens zwei Ansätze, um den Umgang mit Kommunikation in Verbindung mit Dokumenten auf eine neue Basis zu stellen:

1. Cloud-Dienste zum Dokumenten-Management mit Integration von Prozessen, Produktbeispiele wären Box und Huddle.

2. Cloud-Dienste zur Schaffung Unternehmens-interner sozialer Netzwerke (Enterprise Social Networks ESN), Produktbeispiele wären BlueKiwi und Jive. Diese Produkte lehnen sich an der durch Facebook und Google+ erfolgreich eingeführten Methode der Kommunikation an, professionalisieren sie aber und optimieren sie für den Bedarf eines Unternehmens.

Wie kommunizieren wir in Zukunft?

Der erste Ansatz wird mehr der Sichtweise gerecht, dass nicht alle Dokumente zwingend einem Prozess zugeordnet sein müssen, aber bei Bedarf zugeordnet werden können. Box selber ist dabei sehr rudimentär in sich, setzt aber auf die Ergänzung um externe Tools wie Salesforce (also Box liefert quasi den Basis-Speicher und andere Anbieter liefern die Mehrwert-Funktionen). Huddle ist eine geschlossene Lösung, die im Prinzip eine einfache Sharepoint-Installation nachbildet und Workspaces für die verschiedenen Prozesse bietet. An die Workspaces können dann die Verwaltung der Teammitglieder, Aufgabenlisten, Dokumentenfreigaben und einfache Abläufe gebunden werden.

Aus meiner Sicht ist keiner der erwähnten Dienste bisher wirklich perfekt, auch wenn namhafte Unternehmen auf der Referenzliste der Hersteller stehen. Im Endeffekt wäre die Kombination beider Ansätze in einem Produkt mit einer dynamischen und bedarfsorientierten Gestaltung der Workspaces besser. Dabei darf es aber nicht wieder so komplex wie bei Sharepoint werden. Mit Sicherheit werden wir aber gerade in diesem Bereich in den nächsten Jahren erhebliche Weiterentwicklungen sehen. Dienste wie Box entwickeln sich sehr schnell weiter und auch Microsoft hat seinen Hut in den Ring der Unternehmens-internen Sozialen Netze geworfen. In Kombination mit Sharepoint könnte daraus durchaus eine interessante Lösung entstehen, wenn gleichzeitig die völlig überzogene Komplexität von Sharepoint beseitigt wird.

Dies beantwortet aber nicht die Frage, wie wir mit Voice und Video in diesem Zusammenhang umgehen. Huddle zeigt erste Ansätze, Sprach- und Videokonferenzen zu integrieren. Von großer Bedeutung wäre es natürlich, die gesamte Kommunikations-Historie eines Projektes oder einer Person abrufen zu können und in einem Gespräch gleichzeitig Zugang zu allen erforderlichen Dokumenten zu haben. Für den Vertriebsbereich leisten dies Tools wie Salesforce natürlich, aber diese sind für normale Anwendungen viel zu komplex.

Fassen wir an dieser Stelle noch einmal zusammen:

- Wir brauchen mehr Effizienz und Transparenz in unserer Kommunikation.
- Email ist dabei der große Schwachpunkt und muss deshalb in seiner Zukunftsbedeutung generell in Frage gestellt werden.
- Mobile Endgeräte erfordern andere IT-Infrastrukturen als wir sie traditionell gewohnt sind. Speziell Dateisysteme müssen auf den neuen Bedarf zugeschnitten werden.
- Wir brauchen eine Team- und Prozessorientierung in allen wesentlichen IT-Bereichen.
- Die zukünftige Form der Kommunikation muss auch Sprache und Video sauber und transparent integrieren.

Betrachten wir auf der einen Seite den Bedarf und auf der anderen Seite die Entwicklungen im Markt, dann wird deutlich, dass sich unsere Art zu kommunizieren in den nächsten Jahren deutlich verändern wird. Dies muss als Teil eines Gesamtprozesses gesehen werden, bei dem alle Elemente der traditionellen IT auf den Prüfstand gestellt werden.

Ihr
Dr. Jürgen Suppan

Netzwerk-Redesign Forum 2013:
Switches, Router, Firewalls, WLAN: wird alles Software?
15. - 17.04.13 und Intensiv-Tag 18.04.13 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 High-end-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 Rechenzentrum 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.

Inklusive Technologie-Report

Neuerscheinung März 2013:
"RZ-Netze: die nächste Generation"

Wir stehen vor einem fundamentalen technologischen Umbruch, dessen Konsequenz in den nächsten Jahren sein wird, dass die bisherigen Netzwerkstrukturen in einem RZ völlig verschwinden und in Folge auch andere Netzwerkbereiche, allerdings in unterschiedlichem Maße, davon betroffen sein werden. Wer glaubt, sich diesem Umbruch z.B. durch hektische Hinzufügung von Funktionen zu bestehenden Netzen dauerhaft entziehen zu können, begreift nicht, was ein solcher Umbruch tatsächlich bedeutet und dass er sich mit der Zeit in eine Isolation von der allgemeinen technologischen Entwicklung begibt, die umso mehr Geld verbrennt, je länger sie dauert.

In einer solchen Phase ist es zunächst wichtig, zusammenhängend zu verstehen, was überhaupt passiert, auch wenn Produkte nur zum Teil verfügbar sind, was sich aber in diesem Jahr dramatisch ändern wird. Und genau diesem Zweck dient dieser Report.

Bis zum 28.02.13 können Sie von der Subskriptionsphase profitieren.
Teilnehmer an der 3- oder 4-tägigen Veranstaltung erhalten den Report zum Sonderpreis von nur € 298,--. netto.
Für alle anderen Teilnehmer gilt der Preis von € 338,-- netto, der ab dem 01.03.13 Gültigkeit hat.

Autor: Dr. Franz-Joachim Kauffels
Kosten: € 348,--* netto zzgl. Versandkosten (statt regulär € 398,-- netto - *Preis gültig bis zum 28.02.13)

Bestellen Sie über unsere Web-Seite **www.comconsult-research.de**

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 € 2.490,-- netto

Kongress ohne Intensiv-Tag
☐ vom 15.04. - 17.04.13 in Bad Neuenahr
zum Preis € 2.290,-- netto

Ich buche nur den **Intensiv-Tag**
☐ am 18.04.13 in Bad Neuenahr
zum Preis € 990,-- netto

☐ Bitte reservieren Sie mir ein Zimmer

vom _____ bis_____ 13

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

☐ Inklusive Technologie-Report
RZ-Netze: die nächste Generation
zum Preis von € 298,-- * netto

*Preis gültig bis zum 28.02.13 für Kongressteilnehmer an der 3- bzw. 4-tägigen Veranstaltung. Für alle anderen Teilnehmer gilt der reguläre Sonderpreis von € 338,-- netto, der ab dem 01.03.13 Gültigkeit hat.

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

Neues Seminar

Aufbau und Management von Internet-DMZ und internen Sicherheitszonen

Die ComConsult Akademie veranstaltet vom 01.07. - 03.07.13 ihr neues Seminar "Aufbau und Management von Internet-DMZ und internen Sicherheitszonen" in Bonn.

Der Aufbau und der Betrieb von einer Internet Demilitarized Zone (DMZ) für die Perimeter-Sicherheit ist zunächst von bewährten Techniken und Methoden geprägt. Die seit Jahren bestehenden Sicherheitsmechanismen der Kontrolle und Entkopplung der Kommunikation durch Firewalls, Gateways und Proxies sind auch heute selbstverständlich immer noch gültig.

Andererseits müssen für einen modernen DMZ-Aufbau der Umgang mit Server-Virtualisierung und damit verbunden die logische Trennung von Kommunikationsflüssen bei einer Netztrennung genauso berücksichtigt werden, wie die Frage der Datensicherung und der SAN/NAS-Anbindung. Ebenso wichtig ist die Notwendigkeit der Filterung der Kommunikation auf Ebene von Anwendungen, um nutzer- bzw. gruppenspezifische Anwendungszugriffe zu kontrollieren und insbesondere zur Erkennung schadenstiftender Aktivitäten.

Hier haben wir uns z.B. an Intrusion-Prevention-Systeme (IPS), Web Application

Firewalls (WAF), Session Border Controller (SBC), spezifische Security Gateways (z.B. für E-Mail oder Web-Zugriff) zwar gewöhnt, trotzdem ist der Einsatz dieser Techniken alles andere als seiteneffektfrei. Außerdem haben sich hier auch Next Generation Firewalls (NGFW) positioniert und sind entsprechend einzuschätzen.

Höchst interessant ist der Trend, diese Konzepte auch für die interne Absicherung der Kommunikation, z.B. zwischen LAN-Clients und Servern oder für den Aufbau von Sicherheitszonen im Rechenzentrum zu portieren. Dies erfordert allerdings spezifische Ansätze, um eine hohe Verfügbarkeit, einen hohen Durchsatz, eine geringe Latenz und insbesondere eine akzeptable Betriebssicherheit zu schaffen.

Außerdem trifft uns die Cloud mit Macht. Immer mehr Anwendungen und Dienste werden über eine Cloud bereitgestellt. Dies hat Auswirkungen auf DMZ-Architekturen.

Dieses Seminar analysiert die verschiedenen aktuellen technischen Konzepte und Architekturen für den Aufbau und Betrieb von Internet DMZs und internen Sicherheitszonen. Anhand konkreter Projektbeispiele wird die Umsetzung dieser Konzepte illustriert.

Dieses Seminar richtet sich an IT-Sicherheitsbeauftragte, Administratoren, Projektleiter und Verantwortliche für die Architektur, Planung, Einführung und Betrieb von Kommunikationsumgebungen.

Die Referenten Dr. Simon Hoff und Dipl.-Inform. Andreas Meder blicken auf jahrelange Projekterfahrungen in den Bereichen Informationssicherheit und Netzwerktechnik zurück und vermitteln diese Erfahrungen im Seminar.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Ich buche das Seminar

Aufbau und Management von Internet-DMZ und internen Sicherheitszonen

☐ vom 01.07. - 03.07.13 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

ComConsult-Study.tv

IT-Analysten-Spezial im Januar bei ComConsult-Study.tv

Endgeräte, Netzwerke, Rechenzentren, Cloud, SDN: wohin man auch schaut, die ganze IT-Welt scheint in Bewegung zu sein. Doch welche Trends sind real? Was ist nur Hype? Muss man jetzt reagieren, oder sollte man abwarten?
Im Januar-Spezial bieten wir Ihnen zwei Videos mit Analysen und Standpunkten von Dr. Suppan, der diesen Fragen nachgeht:

Standpunkt: Cloud-Technologien für die RZ-Automatisierung?
Referent: **Dr. Jürgen Suppan**
Zeit: 00:34:08
Einzelpreis: 49,00 € netto
Im Abo: kostenlos

Cloud-Angebote basieren auf einem extremen Grad an Automatisierung. Neue Standards machen diese Technologien für alle Unternehmen zugänglich. Dr. Suppan analysiert welche Zukunfts-Bedeutung speziell OpenStack für Unternehmen und Behörden hat.

Trend-Analyse: Endgeräte-Entwicklung und Auswirkung auf IT-Infrastrukturen
Referent: **Dr. Jürgen Suppan**
Zeit: 00:41:17
Einzelpreis: 49,00 € netto
Im Abo: kostenlos

Auf der Endgeräte-Seite erleben wir den größten und schnellsten Wandel der letzten 20 Jahre. Dieses Video analysiert die Entwicklung und die daraus resultierenden Anforderungen an IT-Infrastrukturen.

Das Bundle dieser zwei Videos kostet nur € 69,--* netto

*Statt regulärer Preis € 98,-- netto. Dieses Angebot gilt nur im Januar 2013.

Beachten Sie in diesem Zusammenhang auch das kostenlose Video:

Analyse:
Software Defined Networking SDN
Referent: **Dr. Jürgen Suppan**
Zeit: 00:36:34
Preis: kostenlos

Software Defined Networks werden momentan als die Zukunft der Netzwerke gehandelt. Geringere Kosten, mehr Flexibilität, geringere Komplexität und weniger Fehler sind die Attribute, mit denen diese Technologie beworben wird. Dr. Suppan analysiert und bewertet was hinter SDN steckt und inwieweit Unternehmen und Behörden davon betroffen sind.

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

Schwerpunktthema

IPv6 ist eine Software-Migration!

Teil 1: Problemfälle

Fortsetzung von Seite 1

Markus Schaub ist seit 2009 Leiter von ComConsult-Study.tv. Er verfügt über umfangreiche Berufserfahrung in den Bereichen Netzwerken und VoIP und ist seit mehr als 13 Jahren bei ComConsult beschäftigt. Seine Schwerpunkte liegen im Netzwerk-Design, IP-Infrastrukturdiensten und SIP, zu denen er viele Vorträge auf Kongressen hielt, erfolgreich Seminare durchführte und zahlreiche Veröffentlichungen schrieb.

Migriert man ein Netzsegment, migriert man automatisch alle daran angeschlossenen Endsysteme und Server mit einem solchen modernen Betriebssystem, sobald Router Advertisements gesendet werden. Und das nicht erst nach dem Neustart, sondern sofort. Und wer nun glaubt, der Dual-Stack würde es schon richten, wird sein blaues Wunder erleben.

Ein Beispiel, das uns selbst passiert ist: zu einer Zeit, als wir eigentlich noch gar nicht über IPv6 nachdachten, stellte unser Administrator fest, dass es seit der Einführung von Windows Server 2008 plötzlich vermehrt Warnungen in den Events gab. Dort beschwerte sich die Backupsoftware, dass andere Server nicht über IPv6 erreichbar wären. Also dachte sich unser Admin, man könne doch einfach mal IPv6 konfigurieren, damit die Event-Logs übersichtlicher würden. Dazu aktivierte er u.a. auf dem Windows DHCP Server die Router Advertisements (RA). Nun haben wir ein recht kleines Netz und mein Rechner, ein MacBook Pro, hing im selben LAN wie auch der DHCP Server. Also bekam er IPv6 RA, was zwei Konsequenzen hatte:

1. Er generierte sich eine routbare IPv6 Adresse aus dem angebotenen Präfix.

2. Er hielt den DHCP Server für einen IPv6 Router, da selbiger RA verschickte.

Das hatte nun für mich zur Folge, dass ich plötzlich auf bestimmte Webseiten fast nicht mehr zugreifen konnte: sie bauten sich zwar noch auf, aber mit einer Trägheit, die kaum noch zu überbieten war.

Was war passiert? Ganz einfach: die betroffenen Webseiten hatten sowohl IPv4 als auch IPv6 Adressen. Standardkonform versuchte mein Browser zunächst einmal, eine IPv6 Verbindung aufzubauen und dabei den DHCP Server als Router zu nutzen. Erst wenn der Browser-TCP-Timeout überschritten war, versuchte er es mit IPv4 (vgl. Abbildung 1).

Leider merkte er sich nicht, dass das nicht funktioniert und hat es für jede TCP-Sitzung aufs Neue versucht. Browser-TCP-Timeouts sind ziemlich lang und so konnte ich jedes Bild auf einer Seite einzeln begrüßen.

Dass wir mit diesem Problem nicht alleine waren, zeigt ein Bericht aus einem Google-Testlabor. Dort ist exakt dasselbe passiert.

Was dieses Beispiel zeigt, ist, dass man ohne die Software im Blick zu behalten schnell Probleme generieren kann, wenn man „gedankenlos“ einfach IPv6 einschaltet. Im Folgenden werden deshalb zunächst typische Ursachen für die Verquickung von Anwendung und IP vorgestellt und in einem zweiten Teil werden später verschiedene Lösungsmöglichkeiten vorgestellt. Denn eine einzige Lösung gibt es leider nicht.

Ursachen bei der Software

Zunächst werden die Ursachen für die Abhängigkeit von IP und Software vorgestellt. Diese Ausführung hat nicht den Anspruch vollständig zu sein, sondern soll eine Idee vermitteln, wo und welche „Stolperfallen“ einen erwarten. Dazu werden verschiedene Anwendungsarten betrachtet und der aktuelle Stand dargestellt.

Betriebssysteme

Betriebssysteme sind unmittelbar von IPv6 betroffen. Der IP Stack ist integra-

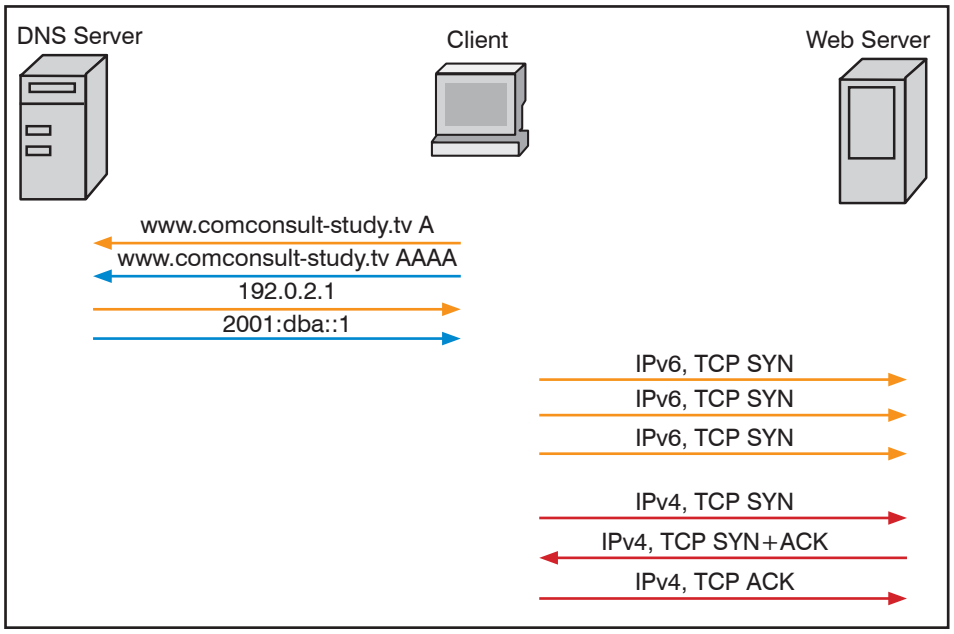


Abbildung 1: Dual-IP-Problem

IPv6 ist eine Software-Migration! - Teil 1: Problemfälle

ler Bestandteil derselben. Damit ist offensichtlich, dass jede Überlegung, ein System mit nicht IPv6 fähigem Betriebssystem zu migrieren, überflüssig ist.

Doch müssen Betriebssysteme weit mehr unterstützen als nur eine IPv6 Adressierung.

Wie Tabelle 1 zeigt, sind die meisten modernen Betriebssysteme durchaus IPv6 fähig und bei fast allen wird es auch standardmäßig mit installiert und aktiviert. Unterschiede treten bei „neueren" Standards auf, die noch nicht durchgängig implementiert wurden. Beispielsweise bei der Zuweisung eines DNS-Servers per Router Advertisement (ND RDNSS).

Was die Tabelle jedoch nicht verrät, ist ob die Systeme anschließend auch über IPv6 kommunizieren oder mit der Adresse alleine schon glücklich sind. So sieht die Zeile beim mobilen Apple-Betriebssystem iOS zunächst einmal sehr gut aus (4x ja) und man sollte annehmen, das IPv6 genutzt wird, sobald das möglich ist. Die Realität sieht aber anders aus. (siehe Abbildungen 2 und 3)

Auf Abbildung 2 sieht man sehr schön, dass das iPad sowohl IPv4 als auch IPv6 Adressen zugewiesen bekommen hat. Insbesondere hat es auch öffentliche IPv6 Adressen, so dass einer Kommunikation mit Internetserver über Version 6 nichts im Wege steht.

Die Abbildungen 2 und 3 zeigen, dass sowohl die Namensauflösung funktioniert und der Server auch per IPv6 gepingt werden kann. Ruft man den Server dann aber mit dem Safari auf und schaut anschließend, welche Verbindungen genutzt wurden, so steht dort die IPv4 Adresse des Servers, nicht die IPv6 Adresse. Safari hat also Version 6 ignoriert und Version 4 genutzt.

Man sieht an diesem Beispiel, dass das Betriebssystem selbst durchaus IPv6 unterstützt, aber noch nicht einmal System-immanente Programme (Safari) bei Standardprotokollen (HTTP) die neue IP Version benutzen. Böse formuliert könnte man nun sagen, dass die IPv6 Unterstützung in iOS nicht mehr als ein Feigenblatt ist, getreu dem Motto: „Können wir zwar, machen wir aber nicht".

Und noch etwas sieht man daran: zwar ist die Unterstützung durch das Betriebssystem unabdingbar, das alleine reicht aber nicht aus. Die Anwendungen müssen IPv6 ebenfalls unterstützen.

Anders sieht das beispielsweise aus, wenn man ein Desktopsystem desselben Herstellers nutzt. (vgl. Abbildung 6, Wireshark-Trace des Aufrufes derselben Webseite von einem OS X System mit Chrome)

OS	Version	IPv6-ready	Standard-installation	DHCPv6	ND RDNSS
AIX	4.3	ja	ja	ja	nein
Android	4.2	teils	ja	nein	nein
Fedora	13	ja	ja	ja	ja
FreeBSD	9.0	ja	ja	Addon	ja
iOS	*6.0*	ja	ja	ja	ja
Mac OS X	*10.8.2*	ja	ja	ja	ja
OpenBSD	5.1	ja	ja	Addon	nein
OpenVMS	8.3	ja	ja	nein	nein
Red Hat Enterprise Linux	6	ja	ja	ja	ja
Solaris	10	ja	ja	ja	nein
SUSE Linux Enterprise Server	11	ja	ja	ja	ja
Symbian	7.0	ja	ja	nein	nein
Ubuntu	10.10	ja	ja	Addon	ja
Windows	XP	ja	nein	Addon	nein
	VISTA	ja	ja	ja	Addon
	7	ja	ja	ja	Addon
	8	*ja*	*ja*	*ja*	*n/a*
Windows Phone	6.5	ja	ja	teils	nein
	7.5	nein	nein	nein	nein

Tabelle 1: IPv6 Unterstützung bei verschiedenen Betriebssystemen
Quelle: http://en.wikipedia.org/wiki/Comparison_of_IPv6_support_in_operating_systems
(Kursive Daten vom Autor ergänzt/aktualisiert)

Standardserversoftware

Es stellt sich somit die Frage, ob man bei „Standard-Unternehmenssoftware" davon ausgehen kann, dass sie IPv6 unterstützt. Das Bild ist in diesem Fall ähnlich uneinheitlich wie es bei Betriebssystemen ist. Eine generelle Aussage kann man heute dazu nicht treffen. Schaut man sich aber

Abbildung 2: IPv6-Adressen bei iOS 6.0

Abbildung 3: DNS bei iOS 6.0

IPv6 ist eine Software-Migration! - Teil 1: Problemfälle

Abbildung 4: Ping mit IPv6 bei iOS 6.0

Abbildung 5: HTTP-Verbindung zu Dual-IP-Server mit iOS 6.0

die Server-Software an, die meist im Internet angewendet wird, so ist IPv6 in der Regel kein Problem. Der Server aus Abbildung 6 beispielsweise ist ein Apache, der auf einem Ubuntu Linux läuft. Auf demselben Server laufen weitere typische Internet-Anwendungen (openssh, Mail-Server, etc.), die alle ohne Probleme auch per IPv6 angesteuert werden können.

Doch selbst hier gibt es kleine Stolperfallen. Ein Beispiel dafür ist mysql: unsere Webserver greifen alle auf einen zentralen Datenbankserver zu. Während die neuen Webserver bereits mit Dual-IP laufen, können die alten ausschließlich IPv4. Eines der Ziele bei der Umstellung auf einen zentralen Datenbankserver war es, dass der mysql-Dienst über das Internet nicht erreichbar sein sollte, sondern nur von den Webservern aus. Deswegen hat der Datenbank-Server eine private IPv4 Adresse und eine ULA für IPv6.

Grundsätzlich gibt es bei mysql die Möglichkeit eine „bind-address“ zu konfigurieren. Also die Adresse, auf die der Dienst hört. Andere Adressen des Servers würden von mysql ignoriert werden. Dumm nur, dass dieser Eintrag nur 1x vorgenommen werden kann und nicht eine Adresse für IPv4 und eine für IPv6. Sicher: es gibt weitere, zum Teil elegantere Methoden den Dienst vor unberechtigten Zugriffen abzusichern, die wir auch einsetzten. Nur muss man bei der Migration daran denken. Wurde diese Option bislang nämlich genutzt, so wird auch nach Einführung von IPv6 der Serverdienst nur auf die „alte“ Adresse hören.

Damit ist mysql ein Beispiel für ein Konfigurations-Problem, das bei Dual-IP auftreten kann.

Ein weiteres Beispiel aus dem Haus Oracle sind deren kommerziellen Datenbanken, die unter demselben Namen (Oracle) vermarktet werden. Auf der Webseite des Herstellers findet man ein achtseitiges Dokument mit dem Titel „Oracle Database and IPv6 – Statement of Direction“. Zieht man Deckblatt, Inhaltsverzeichnis etc. ab verbleiben vier Seiten, auf denen beschrieben wird, wie und unter welchen Voraussetzungen Oracle-Produkte IPv6 fähig sind. Dabei sind so überraschende Erkenntnisse, wie dass Oracle-Software keine Verbindungen zwischen einem IPv4-only Client und einem IPv6-only Server unterstützt.

Alles andere liest sich wie „geht alles“. Erst auf der letzten Seite kommen die Einschränkungen:

„Oracle Database 11g Release 2 supports IPv6 addressing for all features and components in single-instance mode. IPv6 support for RAC will be available in a future Database release.“

Mit anderen Worten: RAC, Clusterware und Fail Safe funktionieren noch nicht mit IPv6.

Fazit: Serversoftware

Selbst bei Internet-Serverdiensten und Software großer Anbieter kann nicht a priori von einer vollständigen IPv6 Unterstüt-

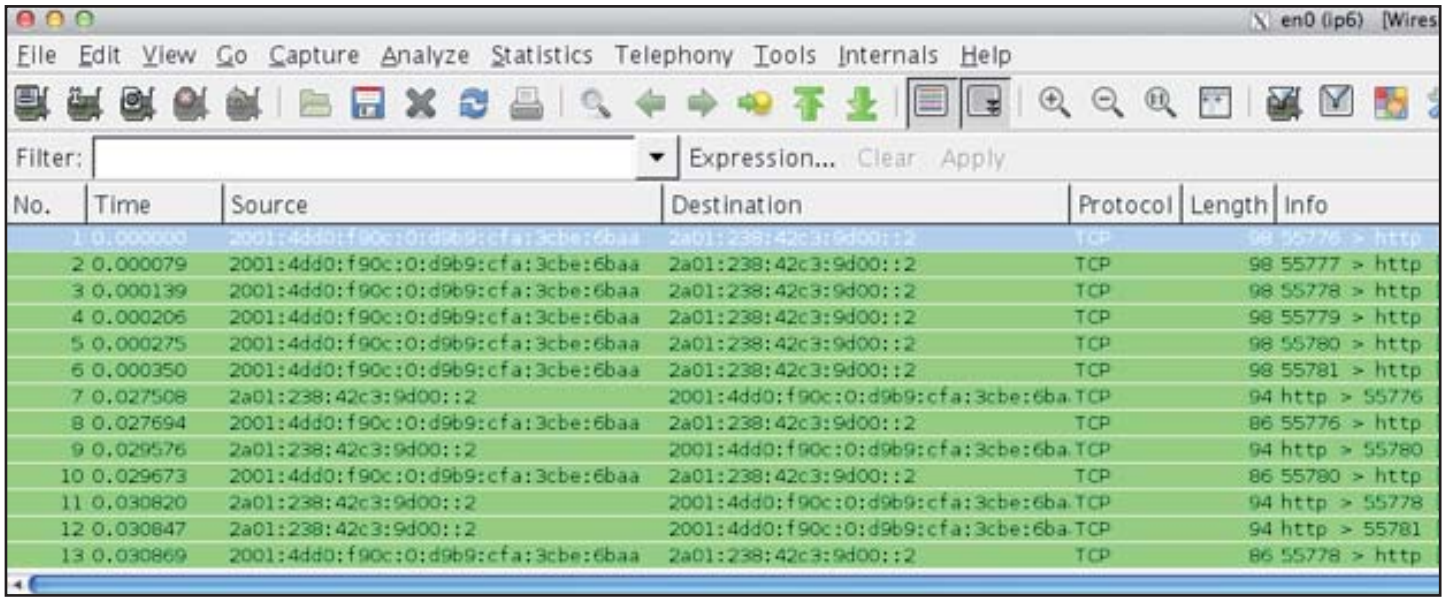


Abbildung 6: HTTP über IPv6 bei OS X + Chrome

IPv6 ist eine Software-Migration! - Teil 1: Problemfälle

```
root@db6:~# ping -n www.comconsult-study.tv
PING www.comconsult-study.tv (85.214.210.133) 56(84) bytes of data.
64 bytes from 85.214.210.133: icmp_req=1 ttl=63 time=2.24 ms
64 bytes from 85.214.210.133: icmp_req=2 ttl=63 time=2.03 ms
64 bytes from 85.214.210.133: icmp_req=3 ttl=63 time=2.06 ms
^C
--- www.comconsult-study.tv ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 2.031/2.112/2.240/0.098 ms
root@db6:~# ping6 -n www.comconsult-study.tv
PING www.comconsult-study.tv(2a01:238:42c3:9d00::2) 56 data bytes
64 bytes from 2a01:238:42c3:9d00::2: icmp_seq=1 ttl=63 time=2.11 ms
64 bytes from 2a01:238:42c3:9d00::2: icmp_seq=2 ttl=63 time=2.00 ms
64 bytes from 2a01:238:42c3:9d00::2: icmp_seq=3 ttl=63 time=1.99 ms
^C
--- www.comconsult-study.tv ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.992/2.038/2.114/0.065 ms
```

Abbildung 7: ping und ping6

zung ausgegangen werden. Jeder einzelne Fall, jede einzelne Version muss separat geprüft werden und somit führt gerade bei unternehmenskritischer Software um eigene Tests nichts vorbei.

Standardclientsoftware

Hier gilt, was auch für die Server gilt: die meisten Internetprogramme unterstützen die neue IP Version parallel zur alten. Am Beispiel des Browsers (Abbildung 6) wurde das ja schon gezeigt. Aber auch ssh, telnet etc. funktionieren. Zum Teil müssen dafür aber andere Befehle ausgeführt werden: beispielsweise heißt der Befehl zum Pingen unter Ubuntu nicht einfach „ping“ sondern „ping6“, andernfalls wird der Ping per IPv4 gesendet. (vgl. Abbildung 7)

Jedoch gibt es selbst hier Fälle, in denen IPv4 genutzt wird, obwohl IPv6 möglich wäre und zwar dann, wenn IPv6 zu langsam ist. Dafür gibt es sogar einen Standard (RFC6555: Happy Eyeballs: Success with Dual-Stack Hosts), auf den im zweiten Teil noch eingegangen wird.

Abseits dieser Standardprogramme kann man keine Aussage mehr machen. Während es Hersteller gibt, die ihre Software bereits auf Dual-IP umgestellt haben, gibt es welche, die IPv4 in fast sträflicher Weise missbrauchen, was eine Software-Migration schwierig macht.

Dazu zwei Beispiele:

1. **Nutzung alter Librarys oder „falscher“ Funktionen von Standard-Librarys**
   Dieses Problem ist bei uns selbst aufgetreten. Der Clients von ComConsult-Study.tv ist vor Version 2.0 nicht IPv6 fähig. Das ist erst aufgefallen, nachdem wir den Server auf IPv6 umgestellt haben.
   Auf meine Nachfrage, woran es gelegen hat, bekam ich von dem Entwickler folgende Antwort, die ich einfachheitshalber mal wörtlich wiedergebe:

   > „Statt sockaddr_in Strukturen mit Hilfe von inet_addr (oder auch gethostbyname/inet_aton) zusammenzubauen, nutze ich jetzt getaddrinfo. Diese liefert ein Array dessen Felder man für die Routine "socket" nutzen kann. Das hat jetzt auch noch den Vorteil, dass, wenn der Name auf mehr als eine IP-Adresse auflöst, diese alle durchprobiert werden.“

2. **Missbrauch von IP Adressen**
   Mein persönliches Highlight sind aber Programme, die IP Adressen für Dinge missbrauchen, für die IP nie gedacht war. Vorzugshalber wenn die Lizenz an die IP-Adresse gebunden ist. Solche Lizenzen haben schon in der Vergangenheit ein vollständiges IP-Redesign erfolgreich behindert und besonders spannend wird es immer dann, wenn der entsprechende Hersteller nicht mehr existiert. Dann kann man die IP-Adresse nämlich nie wieder ändern.

   Ein paar Beispiele ohne Nennung des Herstellers:

   a. „Meine XX-Lizenz wird als ungültig erkannt - was habe ich falsch gemacht? Ihre XX- Lizenz ist an unsere Vserversysteme und IP-Adressen gebunden. Versuchen Sie nachträglich Ihre IP-Adressen zu ändern und die XX-IP umzustellen, wird die Lizenz seitens des Herstellers ungültig.“

   b. „Mit dem Erwerb von XX erhalten Sie eine Lizenz für den Betrieb auf einem Server. Die Lizenz ist an eine Domain und eine Server IP gebunden und nicht übertragbar.“

   c. „Um eine abgeleitete Lizenz wieder [...] zurückzugeben, muss das Notebook unter demselben User und derselben IP-Adresse im Netz angemeldet werden“.

   Wohlgemerkt: „Notebook“, das sind die Geräte, die sich dadurch auszeichnen, dass sie sich stets im selben Netz befinden und deswegen stets dieselbe IP Adresse bekommen.

   Sollte derselbe Hersteller das auch in späteren Releases mit IPv6 so handhaben, aktivieren sie besser nicht die Security Extensions für die Bildung des Interface Anteiles. Für Notebooks macht das zwar eigentlich Sinn, wenn man das Tracking verhindern will, da die Adressen aber nur zeitlich begrenzt gültig und später auch nicht mehr reproduzierbar sind, hat man

sonst ein ernst zu nehmendes Problem: 264 Adressen, die zum Zeitpunkt der Softwareinstallation möglich waren.

Fazit: Clientsoftware

Wie bei der Serversoftware muss auch bei Clientanwendungen genau hingeschaut werden. Insbesondere darf man sich nicht auf Aussagen von Entwicklern verlassen, sie würden Standardfunktionen der Standardlibrarys verwenden und deswegen wäre alles kein Problem. Auch hier wird man um entsprechende Tests bei unternehmenskritischen Anwendungen nicht herum kommen.

P2P-Kommunikation: Protokoll-Immanente-Adressierung

Eine Besonderheit stellen Peer-2-Peer-Kommunikationen dar. Also diejenigen, bei denen Endsysteme direkt miteinander kommunizieren. Das wohl bekannteste Beispiel dafür ist VoIP, sei es nun SIP, Skype oder wie auch immer. In den meisten Fällen läuft zwar der Verbindungsaufbau über einen zentrale (öffentliche) Infrastruktur, die Daten selbst werden jedoch von Endgerät zu Endgerät gesendet. Dazu müssen beim Verbindungsaufbau die notwendigen Parameter ausgetauscht werden. Neben Medien, Codecs und Ports gehört dazu auch die Adresse, unter der ein Gerät erreichbar ist. (siehe Abbildung 8)

SIP URL Format	Erklärung
sip:donald.duck@aceme-ltd.com	Einfacher SIP URL
sip:donald@aceme-ltd.com; transport=tcp	Einfacher SIP URL mit TCP als Transport Protokoll (Default ist UDP)
sip:donald@172.16.02.54	SIP URL mit IP Adresse
sip: +49-999-12345678@ddd.de; user=phone	SIP URL mit globaler Telefonnummer
sip:sales@aceme-ltd.com;maddr=225.0.2.1;ttl=64	SIP URL mit Multicast Adresse, die den vorher spezifizierten Host Namen überschreibt. TTL steht auf 64 (0 .. 255). TTL muss bei Multicast gesetzt werden, ebenso muss UDP geutzt werden.

Abbildung 8: SIP/SDP URL Formate Quelle: Borowka-Gatzweiler, UBN Netzwerke

Bei SIP/SDP sind für die Adressierung verschiedene Varianten erlaubt, so sind neben Namen auch IP Adressen zulässig. Denn anders als Server haben Clients oft keine globalen Namen. In Unternehmen ist das theoretisch zwar anders, da Clients sowohl in einer DNS-Domain hängen als auch mit „ihrem“ Namen am DNS-Server angemeldet werden, jedoch sind diese Namen aus Sicherheitsgründen selten im globale DNS abrufbar. D.h IP Adressen tauchen auch in höheren Schichten als der Netzwerk-Schicht auf. Das macht schon bei IPv4 Probleme, da NAT-Gateways beispielsweise von Hause aus nur die Adressen im IP Header austauschen, nicht aber im SIP und SDP.

Da IPv6 eben die Ende-zu-Ende-Kommunikation wieder ermöglichen soll, sollte es also eigentlich sogar zu weniger Problemen bei P2P-Kummunikation kommen als beim Vorgänger. In der Theorie stimmt das auch, in der Praxis jedoch leider nicht: die Software muss nämlich entsprechend angepasst werden, um sicherzustellen, dass in allen genutzten Protokollen und allen vorkommenden Feldern die richtigen Daten stehen.

Dass das nicht so ohne weiteres umgestellt werden kann, zeigt ein Beispiel aus dem Hause Microsoft: obwohl in den Supportbedingungen schon seit Jahren gefordert wird, dass der Dual-Layer aktiviert ist, war der Hauseigene Kommunikationsserver Lync in der Version 2010 nicht IPv6 fähig. Erst mit der neuen Version 2013 ändert sich das.

Ein weiteres Problem, das sich aus dem Protokoll-immanten Adressaustausch ergibt, tritt bei NAT64 auf, oder wenn es ganz schlimm kommt bei NAT646, doch dazu später mehr, da davon auch andere Software betroffen ist.

Fazit: P2P-Software

P2P-Software stellt eine eigene Klasse von Kommunikationsform dar, da hier Adressen zwischen Endsystemen in höheren Schichten des OSI-Modelles ausgetauscht werden. Das muss sowohl von den Protokollen selbst als auch von der Software unterstützt werden.

Hardwareappliances

Auch Hardware ist Software! Denn in jeder Hardware, die an ein Netz angeschlossen wird, läuft irgendeine Form von Software. Gemeint sind damit Hardware-Appliances mit definierten Funktionen, die es in vielfältigster Form in Unternehmen gibt:

- Produktion
  Hierzu gehören Produktionsstraßen, Sensortechnik, Roboter, Gabelstabler, etc.
- Haussteuerung
  Beispiele sind die Gegensprechanlage, die Fahrstuhlsteuerung oder automatisch gesteuerte Rollos zur Klimakontrolle
- Überwachung
  Zunehmend basieren auch Überwachungskameras auf IP
- IT-Infrastruktur
  Beispiel dafür sind Scanner, Drucker und Access-Points (siehe Abbildung 9)

Auch in Privathaushalten gibt es zunehmend solche Geräte:

- Multimedia-Boxen
- HiFi-Geräte
- Haussteuerung
- Fernwartung

Für fast alle diese Hardware-Geräte gilt:

- Lange Laufzeiten, oftmals über 10 Jahre
- Wenig Speicher und damit kaum Möglichkeit für größere Softwareupdates
- Geringe Prozessorleistung

Abbildung 9: Produktion

IPv6 ist eine Software-Migration! - Teil 1: Problemfälle

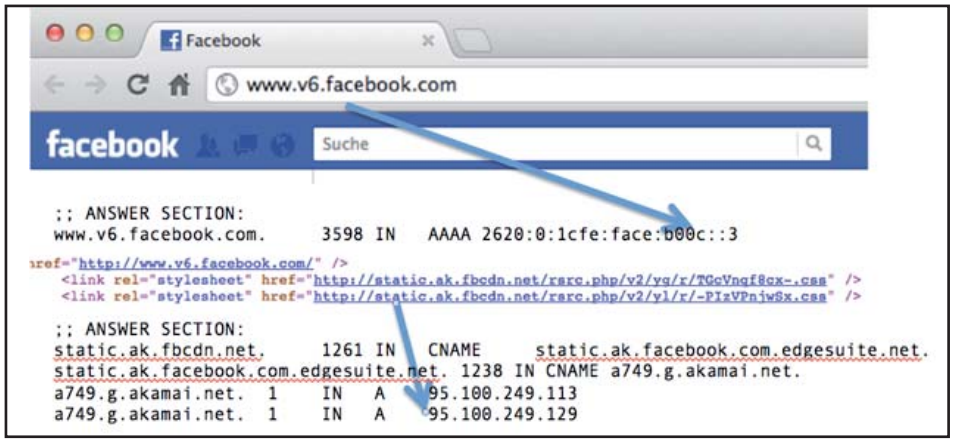


Abbildung 10: Facebooks IPv4/IPv6-Wirrwarr

Damit ergibt sich bei einer Migration zu IPv6 jedoch automatisch das Problem, dass diese Geräte außen vor bleiben müssen, da ein entsprechendes Software-Update oftmals unmöglich ist. Problematisch dabei ist, dass es sich z.B. im Falle der Produktion jedoch um unternehmenskritische Prozesse handelt.

Bei einer Migration müssen diese Bereiche also gesondert betrachtet werden und wenn möglich sogar so lange gegenüber dem neuen Protokoll abgeschirmt werden, bis sie umgestellt werden können. Das ergibt sich aus den oftmals schwachen Prozessoren, die nicht durch ein weiteres Protokoll unnötig belastet werden sollten. Denn selbst wenn das Gerät IPv6 nicht versteht, so muss es die Ethernet-Päckchen doch erst verarbeiten, bevor es das unbekannte Protokoll verwerfen kann.

Dienste: Cloud, Sozial-Networks

Dieses Kapitel hätte auch mit „Merkwürdigkeiten“ getitelt sein können, denn Cloud Dienste sind in den meisten Fällen und soziale Netzwerke in allen HTTP-Angebote, die eigentlich ohne weiteres auf IPv6 umgestellt werden können sollten. Doch gibt es immer wieder Fälle, wo die Umstellung noch nicht vollständig ist. D.h einige der beteiligten Serversysteme sind bereits umgestellt, andere nicht. Ein Beispiel der Vergangenheit war für einige Zeit Facebook.

Abbildung 10 zeigt, wie IPv6 einige Zeit bei Facebook gehandelt wurde: die Webseiten konnten über eine spezielle URL per IPv6 aufgerufen werden. Im HTML-Text standen jedoch jede Menge Querverweise zu weiteren Dateien wie Javascript und CSS, die von anderen Servern abgerufen wurden. Diese Server wiederum waren nur über IPv4 erreichbar.

Zur Ehrenrettung von Facebook und zur eigenen Schande muss allerdings gesagt werden, dass Facebook im Gegensatz zu ComConsult-Study.tv diese Übergangsphase scheinbar abgeschlossen hat: die Seiten werden heute auch bei Aufruf der „normalen“ www-URL wenn möglich per IPv6 ausgeliefert, ebenso wie alle nachzuladenden Elemente. Bei ComConsult-Study.tv wurde zwar bereits der Webserver vollständig auf Dual-IP umgestellt, nicht aber der Streaming-Server.

Eine weitere Merkwürdigkeit in diesem Zusammenhang kann man bei Microsoft Office 365 entdecken:

> „**Only A record** (no AAAA) and CNAME record **are available for creation in the DNS Manager in Microsoft Online Portal** currently. So it’s not available to create IPV6 related DNS records if you fully delegate your domain to Office 365.
>
> However, **if your domain registrar/DNS provider provides IPV6 related records creation function, then you can switch the name servers back to your domain registrar/DNS provider**, create Office 365 related DNS records then create IPv6 related records.“
>
> (Quelle: http://community.office365.com/en-us/f/148/p/19337/90433.aspx#90433)

Abbildung 11: VoIP Telefon mit nur einer IP-Adresse

Das kann man grob zusammenfassen als: IPv6 eigentlich ja, DNS AAAA eigentlich nein.

Was das Beispiel zeigt, ist allerdings nicht MS spezifisch, sondern im Umfeld von DNS geradezu archetypisch. Wir selbst haben einen neuen DNS Registrar gesucht, die Mindestbedingung war, dass AAAA, IP6 und SRV Records unterstützt werden, die Nebenbedingung war, dass die DNS-Server des Registrars selbst auch über IPv6 erreichbar sind. Es war (nahezu) unmöglich einen solchen zu finden: entweder scheiterte es an den SRV Records oder an der IPv6 Erreichbarkeit der DNS Server. Letzten Endes wurde es dann ein Provider, der alle Server-Records unterstützt, seine Server aber noch nicht auf Dual-IP umgestellt hat.

Was diese beiden Beispiele zeigen, ist ein Problem im Zusammenhang mit IPv6, das auch noch an vielen anderen Stellen zu beobachten ist: nicht der Dual-Stack, nicht das Betriebssystem und auch die eingesetzte Software behindern die Migration, sondern schlicht die Konfigurationsoberfläche. Obwohl der BIND und MS-DNS-Server problemlos AAAA und SRV Anfragen beantworten könnten, ist es auf der Oberfläche einfach noch nicht vorgesehen.

Beispiele findet man auch vielfach bei Hardware-Geräten, z. B. VoIP Telefonen wie in Abbildung 11. Für die IP-Adresse ist nur ein Feld vorgesehen und da muss man sich dann eben entscheiden. Genau genommen muss man sich im abgebildeten Fall vorher entscheiden, denn will man dort eine IPv6 Adresse eintragen, muss ein anderes Image eingespielt werden. Dazu muss allerdings gesagt werden, dass das Betriebssystem ein embedded Linux ist, also grundsätzlich Dual-IP fähig wäre.

Grundlegendes Problem

Häufig liest oder hört man, dass es die ganzen Probleme mit der Software nicht gäbe, würden die Entwickler statt auf IP-

IPv6 ist eine Software-Migration! - Teil 1: Problemfälle

Adressen auf DNS-Namen setzen. Dann bräuchte man jetzt an der Software nichts ändern, da man nur im DNS die AAAA Records nachpflegen müsste, und schon wäre die Software automatisch auf IPv6 umgestellt. Also ganz so wie bei einer Umstellung von Gigabit auf 10-Gigatit Ethernet: Netzwerkkarte austauschen, neuen Treiber einspielen, fertig.

Schön, wenn es so wäre! Leider ist es nicht so.

Das Grundproblem liegt im Alter von IP. Das Protokoll stammt aus einer Zeit vor dem OSI Modell. Somit kann es gar nicht OSI-konform sein. Stattdessen basiert es auf dem sogenannten DoD Modell. Dort setzt der Application-Layer direkt auf dem Transport Layer auf, wobei einigermaßen offen bleibt, was dieser Application-Layer eigentlich ist. Die Anwendung ist er nämlich nicht, sondern nur die Schnittstelle zwischen Anwendung und Transportschicht.

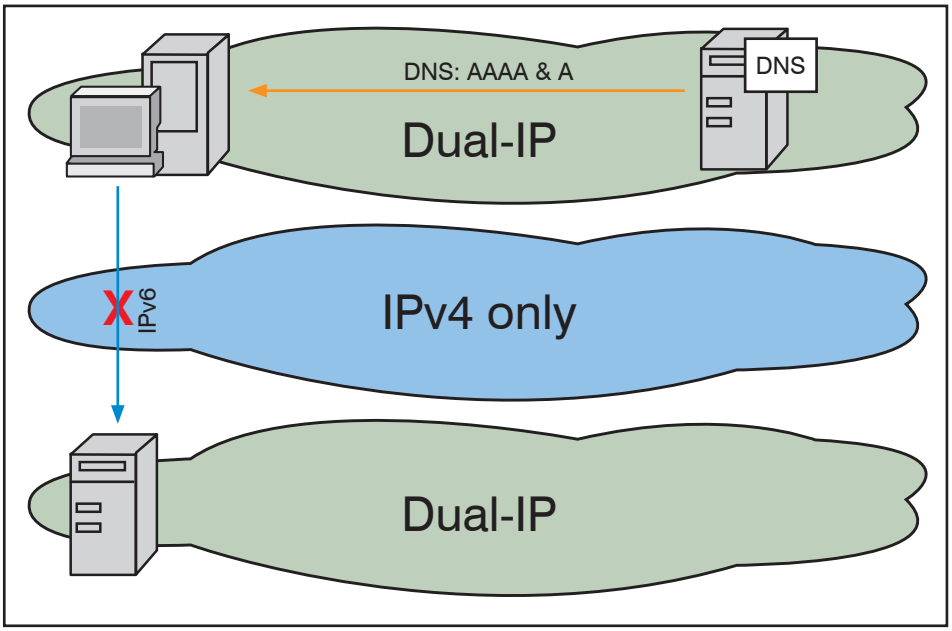


Abbildung 12: Inhomogene Netzwerk-Infrastruktur

Ganz ursprünglich gab es noch nicht mal die formale Trennung zwischen Transport- und Netzwerkschicht, wie sie heute als DoD Modell gelehrt wird: zunächst gab es TCP (inkl. IP). Erst als man erkannte, dass man für Echtzeitkommunikation auch ein weniger aufwendiges Transportprotokoll braucht, wurden die Schichten getrennt und UDP kam hinzu. Daraus erklärt sich, warum nicht eine wohldefinierte Kommunikationsschicht die Entscheidung über das Transport- und Netzwerkprotokoll trifft, sondern die Anwendung selbst. Und damit ist auch die Anwendung selbst dafür verantwortlich, die Adresse des Gesprächspartners zu ermitteln. Moderne Betriebssysteme bieten zwar eine Routine, den sogenannten Resolver an, der DNS-Namen entgegennimmt und IP Adressen zurückliefert, aber dieser Dienst muss zum einen von der Anwendung aufgerufen werden und zum anderen muss die Anwendung sagen, ob sie A oder AAAA Records erwartet.

Daraus folgt, dass die Anwendung die Entscheidung über IPv4 oder IPv6 trifft und es nicht reicht, entsprechende Stacks im Betriebssystem zu ändern.

Infrastrukturelles Problem

Unabhängig, ob die Anwendung oder das Betriebssystem die Entscheidung trifft, gibt es noch ein weiteres Problem, das gelöst werden muss: das Infrastrukturproblem.

Abbildung 12 zeigt ein Beispiel für das Infrastrukturproblem: der Client im oberen Netz und der Server im unteren haben sowohl eine IPv4 als auch eine IPv6 Adresse. Eine DNS Anfrage der Serveradresse liefert somit sowohl einen gültigen A als auch einen gültigen AAAA Record zurück. Gemäß Standard müsste nun IPv6 gegenüber IPv4 bevorzugt werden. Die Verbindung kann jedoch nicht zustande kommen, da zwischen dem Server und dem Client ein IPv4-only Transportnetz liegt.

Obwohl also beide Kommunikationspartner über beide Protokolle verfügen und obwohl grundsätzlich eine Kommunikation über IPv4 möglich wäre, würde diese entweder gar nicht oder wie im Beispiel eingangs nur sehr verzögert zustande kommen.

Diese Art infrastruktureller Probleme kann und muss man im eigenen Unternehmen vermeiden - im schlimmsten Fall durch entsprechende Tunnelmechanismen. In der weltweiten Kommunikation könnte das mittlere Netz jedoch ein durchleitender Internet-Service-Provider sein und die kann man sich nun mal nicht aussuchen.

Fazit

Es reicht nicht aus, einfach nur das Netz zu migrieren und Dual-Layer-Betriebssysteme wie Windows 7 oder 8 einzuführen, um auf IPv6 umzustellen. Vielmehr muss in späteren Phasen der Migration auch die Software überprüft und gegebenenfalls getestet werden. Aber schon bei den ersten Migrationsschritten ist Vorsicht geboten und man sollte immer ein Auge auf die Anwendungen haben: sobald Endgeräte und/oder Server Router Advertisments empfangen, beginnen sie auch damit IPv6 als Netzwerkprotokoll zu nutzen. Wenn die Infrastruktur das noch nicht vollständig hergibt, kommt es zu unvorhersehbaren und teils schwer zu analysierenden Problemen.

Im zweiten Teil werden verschiedene Lösungsmöglichkeiten vorgestellt und analysiert, welche Lösung für welchen Problemfall geeignet ist.

Abkürzungen

DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoD	Department of Defence
HTTP	Hypertext Transfer Protocol
IP	Internet Protocol
IPv4	IP Version 4
IPv6	IP Version 6
IT	Information Technology
LAN	Local Area Network
NAT	Network Address Translation
ND	Neighbor Discovery
OS	Operating System
OSI	Open Systems Interconnection
P2P	Peer-to-Peer
RA	Router Adversisement
RAC	(Oracle)Real Application Clusters
RDNSS	Recursive DNS Server
RFC	Request for Comments
SDP	Session Description Protocol
SIP	Session Initiation Protocol
ssh	Secure Shell
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
ULA	Unique Local Address
URL	Uniform Resource Locator

Standpunkt Troubleshooting

Hochfrequenz geht seltsame Wege!

Der Standpunkt Troubleshooting von Dr. Joachim Wetzlar 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.

Als „Trouble Shooter“ beschäftigt man sich mit den kuriosesten Dingen. Neulich ging es um Funkstörungen. In einer Werkhalle setzt der Kunde Handfunkgeräte ein, um das Rangieren von Fahrzeugen zu unterstützen; es handelt sich um Betriebsfunk im 2-Meter-Band. Die Verfügbarkeit der Kommunikation ist für ihn von entscheidender Bedeutung. Geht eine Nachricht verloren, kracht´s. Und seit einiger Zeit treten nun Störungen auf. Ständiges Rauschen und Knistern im Lautsprecher der Handfunken, so dass man die zwischendurch gesprochenen Meldungen kaum wahrnimmt.

Ein Ingenieurbüro für EMV-Messtechnik wurde eingeschaltet. Es identifizierte HDMI-Schnittstellen (High Definition Multimedia Interface, eine Schnittstelle für den Anschluss von PC-Monitoren) als Quelle der Störungen. Die entsprechenden PCs befanden sich in einem an die Werkhalle angrenzenden Bürobereich. Ich konnte den Effekt mit eigenem Test-Equipment nachvollziehen und war doch recht erstaunt über die Stärke der Störsignale, die von den HDMI-Kabeln abgestrahlt wurden und deren Auswirkung.

Warum sollten sich „Netzwerker“ für HDMI und Handfunkgeräte interessieren? Im Prinzip liegt doch beides außerhalb unseres Verantwortungsbereiches. Im Prinzip aber auch nicht. Denn in Form der Wireless LAN hat die Funktechnik schon lange Einzug in die Netze gehalten. Viele unserer Endgeräte sind daneben mit den Funktechniken Bluetooth, UMTS oder LTE ausgestattet. Was bedeutet das im Einzelnen?

Im vorliegenden Fall war es nützlich, dass der Kunde Kontakt zu einem Fachmann hatte, der einerseits über Erfahrung in der EMV-Messtechnik und andererseits über die dafür benötigten Geräte verfügte. Der Einsatz von Funktechnik erfordert also unbedingt das Bereithalten von Messtechnik und entsprechendem Know-how.

Darüber hinaus fördert der Einsatz von Funktechnik die Zusammenarbeit zwischen verschiedenen Bereichen und Mitarbeitern eines Unternehmens. So wenig wie sich Funkwellen von Wänden oder Grundstücksgrenzen aufhalten lassen, so wenig lassen sie sich auf den Verantwortungsbereich einer Abteilung begrenzen. Die Konsequenzen aus dieser Erkenntnis sind vielfältig.

So sollte sich jedes Unternehmen, das im eigenen Hause Funktechnik einsetzt, eine eigene kleine Regulierungsbehörde schaffen. Ein „Funkbeauftragter“ koordiniert alle Funkdienste, die im Unternehmensumfeld eingesetzt werden. Jede neue Funktechnik, die im Hause eingeführt werden soll, wird vom Funkbeauftragten bezüglich ihrer Verträglichkeit zu bestehenden Diensten bewertet, nötigenfalls im Rahmen eines Testaufbaus unter Einsatz von Messtechnik. Zweckmäßig ist es, die Anforderungen an den Einsatz von Funktechnik in einem Unternehmens-internen Standard festzuschreiben. Darin findet sich z.B. die Antwort auf die Frage, welcher Funkdienst in welchem Frequenzbereich als „Primärnutzer“ anzusehen ist und welche Konsequenzen das für die „Sekundärnutzer“ hat.

Der Funkbeauftragte eröffnet auch eine ganzheitlich Sicht auf das Thema. Eine mögliche Lösung für den eingangs geschilderten Fall wäre z.B. auch der Einsatz einer digitalen Funktechnik, die aus verschiedenen Gründen robuster gegen Störungen ist. Das ist vielleicht nicht die naheliegende Lösung, aber eine zukunftsträchtige.

Das Problem konnte hier übrigens durch den Einsatz besser geschirmter HDMI-Kabel gelöst werden. In Messreihen zeigte sich, dass sich dadurch die Abstrahlung der Störungen um den Faktor 100 (!) senken ließ. Dagegen zeigten die verbreiteten Klappferrite, die Sie als auffällige Wülste auf vielen Ihrer am Computer angeschlossenen Kabel finden, in diesem Fall überhaupt keine Wirkung.

Hochfrequenz geht eben seltsame Wege.

Zweitthema

Multidimensionale Datenverarbeitung und die Konsequenzen für private DV-Infrastrukturen

Dr. Franz-Joachim Kauffels ist Technologie- und Industrie-Analyst und Autor. Seit über 30 Jahren unabhängiger, kritischer und oft unbequemer Bestandteil der Netzwerkszene. Verfasser von über 20 Büchern in über 70 Ausgaben sowie über 2000 Artikeln, Videos und Reports.

Fortsetzung von Seite 1

In den letzten zwei Jahren sind mit zunehmender Verdichtung eine Reihe von Technologien und Szenarien aufgekommen, die jede für sich erhebliche Änderungen in der bisherigen DV-Landschaft nach sich ziehen:

Cloud: die Idee, Anwendungen und Dienstleistungen in skalierbarer und flexibler Weise ortsunabhängig zur Verfügung zu stellen. Leistungsanbieter und Nutzer können der gleichen Organisation angehören, müssen das aber nicht

BYOD: die Idee, dass ein Mitarbeiter für seine Arbeit die Endgeräte der neuen Generation (Smartphones, Tablets, ...) benutzen kann, die er auch privat benutzt.

Apps: die Idee, statt großer, schwerfälliger monolithischer Software Anwendungen im Rahmen kleiner, flexibler kooperierender Programme (Web-Applikationen) verfügbar zu machen, die, falls es notwendig ist, wiederum auf andere strukturierte Leistungen (z.B. Datenbanken) zurückgreifen können.

Virtualisierung: Nutzung abstrakter leistungserbringender Ressourcen (Prozesse als „Virtuelle Maschinen“ und abstrakte Speicherbilder) unterstützt durch eine Virtualisierungs-Infrastruktur mit zusätzlicher betriebsoptimierender Eigenleistung (High Availability, Migration).

Konsolidierung und Konzentration: wo immer möglich, werden ältere Systeme (Server, Speicher, Netze) dadurch konsolidiert, dass man neue Systeme anschafft, die einen höheren Konzentrationsgrad erreichen und damit wirtschaftlicher zu betreiben sind.

Automation: neben Konsolidierung und Konzentration ist Automation ein wesentliches Element, die neu entstehenden DV-Umgebungen nicht nur wirtschaftlich zu betreiben, sondern sie überhaupt insgesamt beherrschbar zu machen.

Es gibt aktuell eine Ansammlung von Methoden und Technologien und man sieht auch Zusammenhänge zwischen diesen einzelnen technologischen Elementen, aber eigentlich fehlt oftmals ein übergreifendes Gesamtverständnis. Dabei liegt es klar auf der Hand:

Wir stehen am Beginn eines gravierenden technologischen Wechsels, der alle Bereiche der DV um- und erfasst und letztlich zu einer multidimensionalen Datenverarbeitung führt. Dieser ist qualitativ und quantitativ dem Umbruch von zentraler DV auf verteilte dezentrale DV in den 90er Jahren vergleichbar.

Was bedeutet multidimensionale Datenverarbeitung? Ganz einfach: mehr Dimensionen!

Endgeräte: an die Stelle fest montierter PCs treten die neuen flexiblen mobilen Endgeräte. Und die gibt es nicht nur in verschiedenen Formfaktoren (Smartphone, Mini-Tablet, Tablet, Ultrabook, Notebook ...) sondern auch mit einer bunten Betriebssystem-Vielfalt (Viele Android-Versionen, iOS, neue Windows-Varianten).

Endgeräte-Anbindung: an die Stelle fest verdrahteter „User Outlets, Wall Mounted“ treten flächendeckende drahtlose Infrastrukturen (WLAN 11ac und ad, WiMax (international gesehen) und LTE sowie LTE R.10 Nachfolger).

Benutzeroberfläche: an Stelle mehr oder minder „bemühter“ Masken, die letztlich nur eine bunte Darstellungsform der grünen Zeilen auf 3270-Terminals sind und sich somit in den letzten 40 Jahren kaum weiterentwickelt haben, treten jetzt endlich Schnittstellen, die auch für Anwendungen in Unternehmen eine erweiterte Benutzererfahrung ermöglichen, wie es sie allgemein im Internet schon länger gibt.

Anwendungsunterstützung: die (kooperierenden, skalierenden) Apps werden auf eine dynamische Virtualisierungsumgebung abgebildet. Diese ist eine Weiterentwicklung der bisher vorherrschenden eher statischen Virtualisierung und wird bei Providern von Cloud-Leistung schon längst eingesetzt, sollte also im Laufe der Zeit auch für normale Unternehmen verfügbar werden.

1. Indizien eines gravierenden technologischen Umbruchs

Datenkommunikation und die bei den Kunden von ComConsult im Mittelpunkt stehende Kommunikations-Infrastruktur unterliegt einem permanenten technischen Wandel. Dieser Wandel ist immer ein Wechselspiel aus technischen Entwicklungen und Notwendigkeiten, die sich aus Anwendung und Betrieb ergeben.

Ein aktuelles, sofort einleuchtendes Beispiel ist die Endgeräteverkabelung. Hier wurden in den letzten 30 Jahren vehemente Diskussionen geführt und speziell in Deutschland in einer Mischung aus vorauseilendem Gehorsam und völlig übertriebenem Sicherheitsfanatismus massenhaft teure strukturierte Verkabelungssysteme aufgebaut, die zum Zeitpunkt ihrer Installation schon viel mehr Leistung hatten, als man jemals benötigt hat.

Mittlerweile gibt es aber mehr mobile als festgetackerte Endgeräte und in wenigen Jahren wird man den Punkt erreicht haben, wo man stationäre Endgeräte nur noch in den Fällen einsetzen wird, bei denen es eine Anwendung gibt, die einen

derart großen Bildschirm benötigt, dass man sie mit vernünftigem Aufwand mit einer Person nicht bewegen kann. Das wäre z.B. bei Konstruktion und Simulation der Fall. Man kann eigentlich nur noch Diskussionen darüber führen, ob das in 2, 3 oder 5 Jahren eintritt.

Diese Situation ist für den Betreiber direkt mindestens dreifach misslich. Erstens kann er die Investition in die bisherige strukturierte Verkabelung abschreiben, zweitens muss er in großem Umfang Geräte zur flächendeckenden funktechnischen Versorgung anschaffen und drittens sein bisheriges Sicherheitskonzept völlig überarbeiten und anpassen.

Das LAN-Switching ist ein weiteres instruktives Beispiel. Schon zu Beginn der 80er Jahre hat die Firma Kalpana einen Ethernet-Switch vorgestellt. Aber es mussten noch einige Dinge passieren und ca. 6 bis 10 Jahre vergehen, ehe bei den Betreibern der Leidensdruck so groß wurde, dass sie auch tatsächlich LAN-Switches in größerem Umfang eingesetzt haben, weil es auf den wechselseitig ausgeschlossen zu benutzenden Ethernet-Segmenten einfach zu eng wurde. Dann hat man aber sofort gesehen, dass man für größere Strukturen übergreifende (Routing-) Protokolle benötigt. Darin war Cisco Systems bereits erfahren und wurde letztlich der große Gewinner der ganzen LAN-Switching-Welle.

Ein Technologiewechsel verläuft meist kontinuierlich, aber ab und an gibt es einen erheblichen „Sprung“. Dieser Sprung ist dadurch zu charakterisieren, dass nicht einzelne Geräte oder Protokolle, sondern eine komplette konstruktive Welt bestehend aus zugrunde liegender Logik und Konstruktion, Hardware und Software, Betriebskonzepten und sonstigen Elementen in einem zu ihrer Lebensdauer relativ kurzen Zeitraum vollständig durch eine ganz andere Konstruktion ersetzt wird.

Ich möchte dazu zwei Beispiele nennen, die jeder Leser kennt: den Sprung von herstellerabhängigen zu herstellerneutralen Netzarchitekturen und die Virtualisierung.

Zu Beginn der 70er Jahre des letzten Jahrhunderts haben führende Computerhersteller wie IBM, DEC oder Siemens eigenständige proprietäre Netzarchitekturen wie SNA, DECnet oder TRANSDATA vorgestellt und in großem Maßstab eingeführt. Etwa 20 Jahre später hatten die diagonalen Sichtweisen eine kritische Masse erreicht, die den relativ abrupten Wechsel zu den heute immer noch installierten autonomen, herstellerneutralen Netzen initiiert hat. Aus der Perspektive des Betreibers ergab sich einfach die Möglichkeit, die bereits für das Internet definierten Funktionen und Protokolle erfolgreich einzuführen. Aus der Perspektive der Hersteller war es entscheidend, dass sie auch beim besten Willen die neuen Funktionen nicht auf der Grundlage ihrer bisherigen Architekturen herbeiführen konnten. Das kann man am besten bei IBM nachvollziehen, die zu der Zeit, als abzusehen war, dass der SNA-Technologiezyklus sich seinem Ende zuneigt, hektisch in immer schnellerer Folge Detailverbesserungen wie APPC, APPN oder Networking Blueprint nachgeschoben und sogar versucht haben, die WAN-Technik ATM in das Segment der privaten Netze in Unternehmen und Organisationen zu schieben. Wie wir wissen, waren diese Versuche vergeblich.

Die Verdichtung hektischer Detailverbesserungen ist ein wesentliches Vorzeichen eines bevorstehenden fundamentalen technischen Umbruchs.

Festzuhalten ist jedoch eine weitere interessante Tatsache: die Abkehr von SNA und vergleichbaren Systemen wurde von der Einführung eines völlig neuen Endgerätes begleitet: dem PC. Der wesentliche Unterschied zwischen einem PC und einem Dialog-Terminal ist nicht nur die Autonomie bei der Verarbeitung, sondern auch die völlige Veränderung der Benutzer-Erfahrung.

Ein weiterer wichtiger Zusammenhang ist, dass ein fundamentaler Technologiewechsel natürlich, wie der Name schon sagt, eine oder mehrere technologische Komponenten benötigt, die in ihrer Form neuartig sind. Im Fall des Untergangs von SNA & Co. war dies natürlich der PC, genau genommen der autonome Prozessor. Blickt man tiefer, wurde der PC-Prozessor nur dadurch technisch erreichbar, dass die mögliche Anzahl der auf einem integrierten Schaltkreis realisierbarer Transistor-Funktionen die kritische Masse erreicht hat, die man für einen funktionsfähigen autonomen Prozessor benötigt. Ausschlag gebend ist hier also gar nicht so sehr der PC, er ist eigentlich nur eine logische Folge der zunehmenden Integrationsdichte. In dieser Zeit wurde auch Moore´s Law bekannt, welches letztlich besagt, dass sich die Anzahl der auf einer Fläche realisierbaren Transistorfunktionen alle 18 bis 24 Monate verdoppelt.

Man kann es so formulieren: *ein wichtiger Anstoß für einen fundamentalen Technologiewechsel kommt daher, dass Moore´s Law mit der Zeit zu einer Dichte der Transistorfunktionen führt, die es erlaubt, die Komplexität der Strukturen auf einem integrierten Schaltkreis so weit zu steigern, dass eine Technologie, die bisher nur mit viel größerem Aufwand und einer hohen Zahl von singulären Komponenten realisiert wurde, in einem einzigen IC implementiert werden kann, was in Folge die Kosten für den Einsatz der Technologie dramatisch reduziert.*

Aber, wie bei einem Fußballspiel ist es mit dem Anstoß alleine nicht getan. Es gehört noch eine weitere Komponente hinzu: Software, die die neuen physikalischen Komponenten auch nutzbar und möglichst einfach betreibbar macht. Intel, AMD & Co. hätten den Grand Canyon mit Prozessoren füllen können, ohne einen wirt-

schaftlichen Vorteil zu erzielen, wenn nicht Bill Gates auf den Gedanken gekommen wäre, eine simplifizierte Treibersammlung mit einer einfachen Oberfläche zu verbinden und damit ein extrem kompaktes Betriebssystem für die ersten extrem kompakten Prozessoren zu schreiben. Die weiter oben beschriebene Benutzererfahrung wurde dann vor allem von Steve Jobs verbessert.

Ein fundamentaler Technologiewechsel wird durch die Verfügbarkeit neuartiger Technologie in Kombination mit neuartiger Software zur leichten Benutzung und Steuerung dieser Technologie ermöglicht.

Damit nicht genug. Jede Ansammlung technologischer Komponenten bekommt erst dann einen übergreifenden, zusammenhängenden Sinn, wenn man ein Paradigma formulieren kann. Das Paradigma bei SNA war die zentrale DV mit zentraler Verarbeitung und zentraler Steuerung. Das extreme Gegenteil der zentralen DV ist die völlig dezentrale DV. Das wären untereinander nicht verbundene PCs, die ungesteuert vor sich hinarbeiten. Man hat schnell erkannt, dass das für Unternehmen und Organisationen kein sinnvolles Konzept sein kann. Daher kam es zur verteilten DV, bei der die informationsverarbeitenden Komponenten (PCs, Abteilungsrechner, Hosts) durch ein seinem Charakter her universelles Netz verbunden werden.

Ein großer technologischer Wandel ist mit einem Paradigmenwechsel verbunden. Das kann man jetzt noch an vielen weiteren Beispielen belegen, wir beschränken uns hier aber auf die Virtualisierung.

Betreiber freuen sich heute über die Vorteile der Virtualisierung, die nicht nur in der Konsolidierung längst altersschwacher Server liegen, sondern auch eine Reihe angenehmer Zusatzfunktionen, wie z.B. den unterbrechungsfreien Betrieb, ermöglichen. Was sie auch nicht so richtig verinnerlicht haben, ist die Tatsache, dass es die Virtualisierung nicht deshalb im heutigen Umfang gibt, weil man den Betreibern etwas Gutes angedeihen lassen wollte, sondern schlicht aufgrund der Tatsache, dass Intel und andere Prozessorhersteller händeringend nach einer Beschäftigung für ihre vielen neuen Prozessorkerne gesucht haben.

Die oftmals übersehene „Nebenwirkung“ von Moore´s Law ist nämlich, dass zwar bezogen auf einen der Standard-VLSI-Herstellungsprozesse die Anzahl der Transistoren immer weiter steigt, die Taktrate jedoch durch physikalische Randbedingungen des VLSI-Prozesses nicht beliebig gesteigert werden kann. Bei dem CMOS-VLSI-Prozess, der die letzten 20 – 25 Jahre dominierend war, liegt die Grenze für die mögliche Taktrate so um den Bereich von 3 GHz. Natürlich gibt es andere Prozesse, wie z.B. die GaAs-Technik. Sie haben aber den Nachteil einer erheblich geringeren Integrationsrate bei gleichzeitig erheblich höheren Kosten. Das zieht sich durch die gesamte Technologie, die wir benutzen. Hersteller wie Intel können zwar immer mehr Cores auf einem Chip unterbringen und auch gewisse Optimierungen vornehmen, die Taktrate ändert sich jedoch dadurch nicht wirklich. Also stellt sich schnell das Problem, wie man die vielen Cores beschäftigen kann. Normale Anwendungen lassen sich üblicherweise nur in geringem Maße parallelisieren. Anwendungen, die hoch parallelisierbar sind, entstehen nur in begrenztem Umfeld. Beispiele wären Simulationen, Wettermodelle oder Ähnliches. Die Betreiber von HPC-RZs für derartige Anwendungen haben aber eigene Vorstellungen über Rechner, die dafür geeignet sind. Und da sind immer weiter gewachsene Standard-Prozessoren eher seltener gefragt und selbst wenn, wäre der Markt viel zu klein für die Stückzahlen, die Intel, AMD oder andere Hersteller mit neuen Prozessorgenerationen unter wirtschaftlichen Gesichtspunkten erzielen müssen.

Also hat man sich in einer ersten Stufe auf die Endgeräte gestürzt und es kam zu PCs oder Notebooks mit zwei oder vier Cores. Dabei kann man eben noch damit argumentieren, dass bestimmte Grundaufgaben anders verteilt werden, also kann man z.B. einen Core mit der Kommunikationsanbindung beschäftigen, während der zweite die aktuell benutze Anwendung, wie z.B. ein Office-Programm, laufen lässt. Der dritte Core kann dann noch im Hintergrund das Gerät aufräumen und Hilfsprozesse wie Druckertreiber steuern und der vierte dann noch die Grafik aufbereiten, aber, wie man an der Aufzählung schon leicht sieht, endet das Konzept dann auch schnell.

Erst die Virtualisierung führt eine weitere Abstraktionsstufe ein, mit der Cores besser beschäftigt werden können. Jeder Core wird mit einer (oder mehreren) VMs besetzt, die ihrerseits Laufzeitumgebungen für normale Anwendungen darstellen. Dadurch wird es möglich, eine Konsolidierung altersschwacher Server vorzunehmen und in diesem Zug auch neue Funktionen einzuführen.

Virtualisierung ist an und für sich kein wirklich neues Konzept. Schon vor vielen Jahrzehnten gab es VM von IBM für die Großrechner. Interessant für die breite Masse der Betreiber wurde es aber erst mit neuer Prozessortechnologie in Verbindung mit einer Software, z.B. VMware, die eine grundsätzliche Modernisierung der Serverlandschaft ermöglichte. Dies führte zusammen genommen zum Paradigmenwechsel von verteilter DV auf einer Menge isolierter Server zu verteilter DV auf Basis der Virtualisierung.

Schließlich muss man sich die Frage stellen: wie lange kann ein technologischer Ansatz in der Praxis eigentlich überleben? Nennen wir ein paar Zahlen:

SNA, dialogorientierte DV: Beginn 1974, Ende statistisch 1990 – 1995

Segmentorientierte Ethernets: Beginn ca. 1985, Ende statistisch 1995

Token Ring: Beginn ca. 1984, Ende ca. 1990 – 1995

PC-Netze (Novell Netware): Beginn ca. 1986, Ende ca. 1993

Klassischer PC: Beginn ca. 1984, Ende ab ca. 2005 (ab da rückläufige Volumina)

Zwei Dinge fallen jetzt besonders auf:
- selbst hartnäckige Technologien leben kaum länger als 20 Jahre
- 1995 war ein besonders „dramatisches“ Jahr mit vielen dramatischen Abgängen

Warum ausgerechnet 1995? Nun, das ist rückblickend gesehen ungefähr das Jahr, in dem wir damit begonnen haben, RZ-Netze so aufzubauen, wie sie heute sind: Basis Ethernet-Switching, Sixpack-Grund-Design mit den Bereichen Access, Distribution und Core, Spanning Tree und OSPF. Sinn dieser Netze war die Unterstützung der verteilten DV mit vorwiegender Nutzung der TCP/IP-Protokolle.

Und was ist seither mit den RZ-Netzen passiert? In den ersten 15 Jahren relativ wenig, wenn man davon absieht, dass die Leistung einer nach außen bereitgestellten Schnittstelle von 100 MbE auf 1 GbE gestiegen ist. Aber nach 2010 begannen die ersten Unzufriedenheiten und seit 2012 prasseln die neuen, angeblich heilsbringenden Verfahren so schnell auf die Betreiber hernieder, dass diese überhaupt keine Zeit mehr finden, sie zu testen und einzusetzen. Ganz besonders auffällig ist auch, dass die Weiterentwicklung bis ca. 2010 entlang der IEEE-Standards erfolgt ist. Heute haben wir die Situation, dass es schon reicht, wenn sich zwei oder drei Hersteller zu einem Verfahren zusammenrotten, um es als „Standard“ zu bezeichnen und sich größere Organisationen erfolgreich gegenseitig blockieren, wie man

am Beispiel „TRILL“ vs. „PLSB“ deutlich nachvollziehen kann. Das alles sind überdeutliche Vorzeichen eines nahenden Niedergangs.

Nach diesen Erläuterungen können wir die wesentlichen Charakteristika für einen unmittelbar bevorstehen umfangreichen technologischen Wandel zusammenstellen:

1. *Es gibt eine neuartige Hardware, die entweder an der gleichen Stelle wie die bisherige Hardware erheblich mehr leistet oder zu einem völlig neuen System-Modell führt.*

2. *Es gibt eine neue Software, die auf die Nutzung der neuartigen Hardware abgestimmt ist und somit den bequemen Betrieb dieser Hardware ermöglicht. Es stört offensichtlich nicht, wenn diese Software zu Beginn nicht den vollen gewünschten Funktionsumfang hat.*

3. *Die neue Hard- und Software bildet insgesamt ein System, welches die bisherige Benutzererfahrung vollständig verändert.*

4. *Die Verdichtung der hektischen Detailverbesserungen bei den existierenden Systemen ist ein grobes Maß für deren Untergang.*

5. *Die Summe der Detailverbesserungen führen entweder nicht zu dem gewünschten Ergebnis, sind in Summe unwirtschaftlich oder beides. Im Extremfall kann man ein eindeutiges K.O.-Kriterium für die bestehende Technologie definieren.*

6. *Die durchschnittliche Lebensdauer eines bestehenden technologischen Konzeptes ist von wenigen Ausnahmen abgesehen auf ca. 20 Jahre beschränkt*

Wir werden zunächst 4, 5 und 6 belegen. Die neue Hardware ergibt sich aus den neuen hoch funktional angereicherten Switching-Chips, zu denen wir weiter unten etwas sagen. Die neue Software ergibt sich aus den SDN-Konzepten, die z.B. im Video von Herrn Dr. Suppan sehr anschaulich erklärt werden. Die Veränderung der bisherigen Benutzererfahrung (in dieser Perspektive ist der Betreiber der „Benutzer“) besteht in Dynamisierung und Automatisierung.

2. Die Störung des konventionellen Planungsvorgangs

Beschränken wir uns ab jetzt auf die Situation in einem RZ, weil dies nach wie vor die Stelle ist, an der die Funktionalität einer privaten DV-Infrastruktur mit Leistung hinterlegt wird. Seit einigen Jahren ist eigentlich bekannt, dass die Planung von Erweiterungen nicht wie vor 5 oder 10 Jahren üblich auf der Grundlage der Entwicklung der Teilnehmerzahlen vorgenommen werden kann, sondern der durch die vielen neuen Komponenten im Rahmen von Virtualisierungslösungen ein erheblicher Systemverkehr entsteht, der praktisch nichts mit den Benutzern zu tun hat und meist auch als Ost-West-Verkehr bezeichnet wird.

Normalerweise werden eine neue Technologie oder eine neue Ansammlung von Komponenten und Verfahren gegenüber den möglichen Betreibern so eingeführt, dass man in einer Menge marketing-orientierter Auflistungen zunächst die Mängel bestehender Strukturen und den dadurch möglicherweise entstehenden Schaden darstellt, dann zu der neuen Technologie und ihren – meist zu diesem Zeitpunkt noch nicht bewiesenen – Vorteilen und schließlich zu den Komponenten (Geräte und Software) kommt, die angeblich diese neue Technologie optimal umsetzen und die man natürlich verkaufen möchte.

Dieser „normale“ Ablauf ist aktuell massiv gestört. Dafür gibt es verschiedene Gründe:

- die Möglichkeit, dass die Einführung einer Dynamisierung der Virtualisierungsumgebungen bisherige Netzwerk-Strukturen und –Techniken über ihre Grenzen belastet, wird massiv unterbewertet

- die Dramatik der Entwicklung bei Switching-Chips wird nicht verstanden, weil sich bislang kaum jemand ernsthaft mit dieser Technologie auseinandergesetzt hat.

- die eigentlichen Konzepte des SDN werden allgemein nicht verstanden

Aufgrund dieser Tatsachen wird im Markt völlig übersehen, dass wir vor einem fundamentalen technologischen Umbruch stehen, dessen Konsequenz sein wird, dass die bisherigen Netzwerkstrukturen in einem RZ fast völlig verschwinden und in Folge auch andere Netzwerkbereiche, allerdings in unterschiedlichem Maße, davon betroffen sein werden.

Das an sich ist schon starker Tobak, aber ich setze noch einen „drauf“:

Die neuen, funktional hoch angereicherten, Switching-Chips führen zu völlig neuen, extrem flexiblen Networking-Strukturen. Diese Strukturen brauchen eine ganz andere Art der Steuerung. Neben der eigentlichen Funktionalität wird diese Steuerung endlich auch einen den allgemeinen Anforderungen angepassten Grad von Automatisierung erlauben. SDN kann und wird diese Steuerungs-Strukturen liefern. In diesem Sinne bilden die neuen Switching-Chips und SDN einen sinnvollen Verbund von Hard- und Software für die nächste Generation von Kommunikationssystemen virtualisierungs-bewusster verteilter Datenverarbeitung.

Die Kombination hoch angereicherter Switching Chips mit geeigneter SDN-basierter Steuerung ist die Basis-Technik für die Evolution der Verteilten Datenverarbeitung zur Multidimensionalen Datenverarbeitung und führt zu einem Paradigmenwechsel: bisher wurde ein Netz aus Standard-Bausteinen aufgebaut, um einen weitest gehend festgelegten Standard-Leistungsumfang zu implementieren. Anwendungen mussten sich den Möglichkeiten des Netzes anpassen. Die nächste Evolutionsstufe ändert das: Anwendungen werden (indirekt im Rahmen geeigneter Schnittstellen) die benötigte Netzwerkleistung einschließlich der benötigten Qualität definieren. Die Kombination aus SDN und hoch angereicherten Switching Chips hat die Aufgabe und die Mittel, diese dynamischen Anforderungen geeignet umzusetzen.

Genau das lässt sich mit bisherigen Strukturen nicht oder in Ausnahmefällen nur sehr umständlich umsetzen.

Insgesamt stehen wir unmittelbar vor einem massiven technologischen Umbruch. Wer glaubt, sich diesem Umbruch z.B. durch hektische Hinzufügung von Funktionen zu bestehenden Netzen dauerhaft entziehen zu können, begreift nicht, was ein solcher Umbruch tatsächlich bedeutet und dass er sich mit der Zeit in eine Isolation von der allgemeinen technologischen Entwicklung begibt, die umso mehr Geld verbrennt, je länger sie dauert.

Deshalb ist es geradezu tragisch, dass verschiedene Hersteller, um es einfach zu sagen, planlos ziemlichen Unsinn erzählen, was dazu führt, dass jeder, den man fragt, was SDN nun eigentlich ist, etwas anderes sagt. Noch schlimmer ist, dass die Kernkonzepte dadurch verdeckt werden, dass vielfach „OpenFlow“ als SDN bezeichnet wird. Gemessen am generellen Konzept von SDN hat OpenFlow etwa die Bedeutung sagen wir einmal eines Druckertreibers für ein Betriebssystem. Die Konzepte eines Betriebssystems werden sich kaum erschließen, wenn man den Druckertreiber in den Vordergrund stellt und betrachtet.

Warum ist die Situation so verfahren? Na ja, die wirklichen wissenschaftlichen Köpfe hinter den SDN-Konzepten haben schnell ein Unternehmen mit dem Namen Niciria gegründet. Bevor Niciria aber mehr als PowerPoint Folien und ein Controller-Muster auf den Markt bringen konnte, ist das Unternehmen für schlappe 2 Mrd. US$ von VMware gekauft worden. VMware hat offensichtlich das Potential schnell erkannt und ohne Vorwarnung gehandelt. Das hohe Interesse von VMware ist auch dadurch zu erklären, dass bisher existierende Netzwerk-Strukturen das, was VMware eigentlich mit der Weiterentwicklung seiner Virtualisierungsumgebungen beabsichtigt, massiv behindern.

Daher ist die Phase, in der ein oder mehrere Unternehmen zunächst sorgsam erklären, welche Konzepte sie haben und wie sie sie umsetzen möchten, bis auf ein paar Rudimente völlig „ausgefallen". Und VMware ist ja dafür bekannt, Informationen zu bunkern. Selbst bei verfügbaren Produkten ist es ausgesprochen schwierig, die dahinter liegenden Konzepte für eine Bewertung hinreichend zu durchleuchten. Das kann man VMware nicht wirklich vorwerfen, denn sie spielen in einem extrem harten Markt.

Aber, auch Niciria und somit VMware kochen nur mit Wasser. Es gibt eine ganze Reihe von Technologien, die aus der Betriebssystem-Entwicklung kommen und nicht den Namen „SDN" tragen, aber dennoch vergleichbare Funktionen haben.

In 2013 werden wir Hersteller sehen, die, wie ich es einmal nennen möchte „bereinigte Strukturen" anbieten. Hardware mit den neuen Switch-ASICs wird von schlanker Software gesteuert, die einen erstaunlichen Funktionsumfang hat.

3. 2015: ein ganz schlechtes Jahr für bestehende Netze

Der Einfachheit halber könnte ich jetzt einfach sagen, dass 2015 die 20 Jahre für die bestehenden Netzkonzepte abgelaufen sein werden. Aber wir führen das hier schon weiter aus.

Das Jahr 2015 stellt einen statistischen Kompromiss dar. Große Anwender wie Provider befinden sich bereits im Umbruch auf die neue Technologie. Betreiber von privaten Netzen für Unternehmen und Organisationen wechseln ihre Geräte vornehmlich entlang eines Abschreibungszyklusses von meist fünf Jahren aus. Wenn wir davon ausgehen, dass die ersten in 2013 durch Neuanschaffungen die Gelegenheit haben werden, wenigstens teilweise auf eine neue Technologie umzusteigen und sich der Markt bis 2015 in der üblichen Weise stabilisiert, kann man davon ausgehen, dass ab 2015 keine Geräte mehr in größerem Umfang angeschafft werden, die der traditionellen Bauart nachhängen, wenn die Betreiber halbwegs verantwortungsbewusst sind. Im Zeitraum von 2015 – 2017 wird der überwiegende Teil der bisher existierenden Geräte als Sondermüll terminiert.

3.1 Die generellen Problemstellungen

Die generelle Problemstellung für die Entwicklung eines unternehmenseigenen RZs für mehr klassische Aufgabenstellungen ist durch folgende Stichworte zu kennzeichnen:

- Leistungsexplosion Virtueller Server
- I/O-Konvergenz und Anschlussproblematik
- Anforderungen Virtueller Gesamtlösungen: das Netz als Systembus
- Integration moderner Speichersysteme

Aus der Perspektive der Systemarchitektur kann man vereinfachend sagen, dass die Kommunikation im RZ zunächst grundsätzlich von drei neuen Verkehrsströmen geprägt wird:

- Kommunikation zwischen virtuellen Maschinen als Teil von verteilten (Web-) Architekturen
- Systemkommunikation aus dem Umfeld der Virtualisierung wie z.B. das Wandern Virtueller Maschinen, High Availability und Fault Tolerance
- Verlagerung von Plattenspeicher aus dem Direct Attached Bereich hin zu Storage Area Networks

Das ist die Perspektive für ein herkömmliches, „normales" RZ. Damit kann man auch durchaus eine Private Cloud aufbauen um z.B. im Rahmen von Desktop-Virtualisierung Geräte, die z.B. über einen BYOD-Prozess in das Unternehmen gekommen sind, zu unterstützen. Denkt man weiter in Richtung einer Hybrid Cloud, die die unternehmenseigene Lösung mit einem Dienstleistungsangebot eines Providers zusammenführt, kommen weitere Verkehrsströme hinzu:

- Kommunikation von virtuellen Maschinen im privaten mit solchen im „öffentlichen" Teil der Hybrid Cloud
- Unterstützung von Redundanz- und Lastverteilungsszenarien mit zwischen den beiden Teilen der Hybrid Cloud wandernden VMs mit entsprechender Systemkommunikation
- Kommunikation der Storage Area Networks in beiden Teilen der Hybrid Cloud

Kurz charakterisiert war das Ziel des bisherigen Konzentrationsprozesses die Ablösung bestehender Strukturen aus vielen singulären älteren Servern durch ein modernes virtuelles System mit wenigen Servern hohen Konzentrationsgrades. Auch wenn wir heute im Rahmen der Virtualisierung nur 10 bis 20 „alte" Server auf Virtuelle Maschinen in einem neuen Server abbilden, wird diese Zahl mit der Zeit getrieben durch die Entwicklung bei Prozessoren und Virtualisierungssystemen deutlich steigen.

Intel hat in 2011 die 3D-Technik für die Höchstintegration vorgestellt und baut die ersten Prozessoren in 22 nm-Technologie. Für die Prozessoren bedeutet das mehr

Cores und mehr Threads und für die Speicher eben mehr Kapazität auf gleichem Raum. Wenn ein Unternehmen heute auf einem Prozessor sagen wir einmal 10 Virtuelle Maschinen betreibt, wird es in 4 bis 5 Jahren einen Prozessor kaufen können, der in etwa das gleiche kostet und auf dem aber nun 80 bis 100 VMs laufen können. Dieser Prozessor freut sich dann über den auch etwa um den Faktor 10 gewachsenen Speicher. Und wenn der heutige Prozessor für seine 10 VMs eine I/O-Leistung von 10 Gbps benötigt, braucht er in 4 bis 5 Jahren einen 100 G-Anschluss.

Diesem Konzentrationsprozess mit dem Faktor 10 innerhalb von 4 bis 5 Jahren wird sich kaum jemand entziehen können. Dafür ist der wirtschaftliche Vorteil einfach zu groß.

3.2 Das Komplexitätsproblem

Um uns der Tatsache, dass bestehende RZ-Strukturen in Zukunft nicht mehr in der Lage sein werden, die VM-Kommunikation und VM-Migration sinnvoll abzuwickeln, müssen wir noch tiefer in die zugrunde liegenden funktionalen Zusammenhänge blicken.

In einem Multiprozess-Betriebssystem existiert eine Menge von Elementarprozessen, die durch einen Scheduler abwechselnd auf den Prozessor (oder einen Core, wenn der Prozessor mehrere davon hat) abgebildet werden und dann eine Zeitscheibe zum Arbeiten erhalten. Grundsätzlich werden die Prozesse unterteilt in Systemprozesse und anwendungsunterstützende Prozesse. Möchte ein anwendungsunterstützender Prozess während seiner Arbeit etwas ausgeben, kann er das nur in ein Register legen. Er kann dann anders weiterarbeiten, die I/O kann er aber nicht selbst machen. Dazu dient ein I/O-Prozess.

So weit, so gut. Die bei der VM-Migration notwendige Verlagerung von Speicherseiten bedeutet grob, dass der Systemprozess, der die VM-Migration steuert, einem anderen I/O-Prozess, der den TCP/IP-Stack implementiert, die Seiten Register für Register übergibt oder einen weiteren Hilfsprozess anstößt, der diese Übergabe erledigt. Der TCP/IP-Prozess erzeugt dann die Datenpakete und durchläuft seine Verfahren. Das kann er aber nicht alleine, denn er hat keinerlei physikalischen Mittel zur Kommunikation. Die hat einzig der I/O-Prozess, der die Adapterkarte nutzt und steuert. Also gibt der TCP/IP-Prozess die Daten paketweise an den I/O-Prozess. Im Zielsystem läuft das Ganze ebenfalls auf die besprochene Art und Weise ab. Das funktioniert zwar, aber durch die vielen beteiligten Prozesse und die vielen notwendigen Prozesswechsel wird das beliebig langsam. Kommt dann noch wie im Falle von VMware ein virtueller Switch mit ins Spiel, verkompliziert sich das Ganze weiter, denn dann gibt es auf beiden Seiten noch zusätzliche anwendungsunterstützende Prozesse, die den V-Switch implementieren.

Alleine die Anzahl der benötigten Komponenten und die vielfältige Kommunikation zwischen ihnen verlängert nicht nur den Weg und erhöht die Latenz, sondern ist auch die Ursache dafür, dass der Prozessor oder Core durch diese Konstruktion erheblich belastet wird. Das eigentliche Problem ist aber, dass die in den letzten Jahrzehnten benutzten Netzwerk-Infrastrukturen einfach vorne und hinten nicht zu der Denkweise der dynamischen virtualisierten Umgebungen passen. Das beginnt schon damit, dass die VMs nicht auf eine hochwertige Schnittstelle zugreifen können, die sie als Prozesse in Betriebssystemen normalerweise benutzen würden. Also hilft man sich heute damit, eine Menge von kooperierenden Hilfsprozessen einzuführen, die die VM-Kommunikation und VM-Migration „irgendwie“ hinbiegen. Und in diesem Zusammenhang kommt es dann eben zu eigentlich unsäglichen Komponenten wie dem VMware Hypervisor-Softswitch oder dem Nexus 1000 V von Cisco.

3.3 Das Kostenproblem

Heute sind die Virtualisierungs-Strukturen in privaten RZs überwiegend sehr übersichtlich sowohl hinsichtlich der Anzahl der VMs als auch der Nutzung von Zusatzfunktionen wie FT. Außerdem ist das Ganze relativ starr strukturiert. In der Zukunft kann hier eine zunehmende Dynamisierung erwartet werden, wie es sie in großen RZs schon gibt. Die VM-Migration ist dann eine Basisfunktion der gesamten virtualisierten Umgebung und wird dann nicht nur alle paar Tage, sondern Tausende Male im ganz normalen Betrieb z.B. bei der dynamischen Provisionierung von VMs für Kunden-Anwendungen oder bei einem automatisierten System ausgeführt. Belastet dann die VM-Migration die CPUs allzu stark, könnte diesen entweder einfach die Puste ausgehen, was für alle anderen Anwendungen, die auf einem betroffenen Core oder Prozessor laufen, mindestens ungünstig ist, oder fortgeschritten dynamische Konzepte völlig ad absurdum führen.

- die Implementierung von VM-Kommunikation und VM-Migration auf bestehenden Netzwerk-Infrastrukturen führt zu einer Ansammlung von (eigentlich überflüssigen) Komponenten, deren einzige Aufgabe darin besteht, notwendige Anpassungen zwischen der Welt der VMs und den Möglichkeiten der bestehenden Netzwerk-Infrastrukturen herbeizuführen.

- die überwiegende Zahl dieser Komponenten wird in Software implementiert. Das bedeutet, dass jede Komponente zur Funktion eine Laufzeitumgebung benötigt. Da es sich um eine Vielzahl von Komponenten handelt, die untereinander kooperieren, werden entsprechend viele Prozesswechsel notwendig. Das führt zu einer erheblichen CPU-Last für die (eigentlich überflüssigen) Anpassungsfunktionen

- der durch diese Konstruktion entstehende Overhead konnte für sehr große Umgebungen (10.000 Server mit jeweils 128 VMs, also gesamt 1,28 Mio. VMs) mit etwa 25% hinsichtlich der benötigten Rechenleistung nur für die Angleichungsprozesse bestimmt werden. Rein nachrichtentechnisch ergab sich nur ein Overhead von ca. 1%. Das zeigt, dass die hinsichtlich der Anpassungsleistung benötigte Performance fast ausschließlich zu Lasten der CPUs geht

- da die Server mit 45 % den größten Posten bei den Kosten für ein RZ darstellen, und diese nunmehr zu einem Viertel mit eigentlich produktiv völlig unnützen Funktionen belastet werden, entstehen durch diesen unsinnigen Posten Kosten von ca. 11 bis 12 % der Gesamtkosten

Wenn also jetzt durch die schlechte Anpassung zwischen Virtualisierungs-Elementen und einem nach alten Prinzipien aufgebauten Netz Software-Komponenten notwendig werden, die wiederum ca. 11 bis 12% Overhead-Kosten nach sich ziehen, muss dieses Konzept insgesamt überdacht werden.

Die Motivation großer Cloud-Betreiber ist es ja, Verarbeitungsleistung billiger als ein durchschnittliches privat betriebenes RZ zu erzeugen und, um es erfolgreich zu verkaufen, mit dem End-Preis dieser Leistung immer noch deutlich günstiger zu sein als die Kosten der Erzeugung der Leistung in einem privat betriebenen RZ. Mittelfristig sind auch Betreiber privater RZs letztlich gezwungen, vergleichbare Technologien einzusetzen, um die Kosten zu senken.

Die Dynamisierung virtueller Umgebungen ist ein K.O.-Kriterium für bestehende Netze, weil diese nur mit erheblichem Aufwand und dadurch unangemessenen Overhead zu Lasten der CPUs in die Lage versetzt werden kön-

nen, VM-Kommunikation und VM-Migration angemessen zu unterstützen. Das heillose Aufeinanderstapeln software-basierter Hilfsmittel ist derart unwirtschaftlich, dass es die möglichen Vorteile einer dynamisierten virtuellen Umgebung mehr als kompensiert.

4. Zwischenfazit und Konsequenzen

Wir konnten Indizien 4,5 und 6 für einen unmittelbar bevorstehenden Technologiewechsel bei den RZ-Netzen weiter erklären und erhärten. Zusammenfassend:

4. *Die Verdichtung der hektischen Detailverbesserungen bei den existierenden Systemen ist ein grobes Maß für deren Untergang.*

In den ersten 15 Jahren gab es bei den Ethernet-basierten geswitchten RZ-Netzen im „Six-Pack"-Design kaum gravierende Änderungen, wenn man von der Steigerung der Datenrate auf den Ports absieht. In den Jahren 2010 und 2011 kamen relativ plötzlich rund 50 bis 70 neue Verfahren und Protokolle in die Diskussion, die alle an irgendwelchen Stellen des RZ-Netzes Verbesserungen herbeiführen sollten. Ab Mitte 2011 und 2012 wurden wir dann noch mit Protokollen und Verfahren zur Verbesserung der VM-Kommunikation beglückt, wie z.B. SR-IOV, DP, VEB, VEPA, VXLAN, NVGRE und LISP.

Ganz abgesehen davon, dass es bei 50 bis 70 verschiedenen Verfahren 2500 bis 4900 mögliche Kombinationen gibt, von denen der überwiegende Teil unsinnig ist aber die Menge der funktionsfähigen Kombinationen so unübersichtlich wird, dass kein Betreiber das wirklich entscheiden kann, trägt diese Entwicklung die deutlichen Anzeichen einer Panik.

5. *Die Summe der Detailverbesserungen führen entweder nicht zu dem gewünschten Ergebnis, sind in Summe unwirtschaftlich oder beides. Im Extremfall kann man ein eindeutiges K.O.-Kriterium für die bestehende Technologie definieren.*

Selbst wenn es gelingt, sinnvolle funktionsfähige Kombinationen von Verfahren zu finden, ist die Lösung wegen des damit verbundenen Overheads schlicht und ergreifend unwirtschaftlich. Damit haben wir ein K.O.-Kriterium definiert.

6. *Die durchschnittliche Lebensdauer eines bestehenden technologischen Konzeptes ist von wenigen Ausnahmen abgesehen auf ca. 20 Jahre beschränkt*

Na ja, die sind ohne weitere Erläuterung rum!

5. The Next Generation: Power Chips + SDN

Um den Indizienbeweis für das unmittelbare Bevorstehen gravierender technischer Änderungen zu vervollständigen, müssen wir natürlich noch die ersten drei Indizien belegen. Der Beleg besteht schlicht und ergreifend in der Darstellung der neuen Technologien sowie den sich daraus ergebenden Änderungen des Paradigmas und der Benutzererfahrung, wobei wir hier auch von einer „Betreibererfahrung" sprechen können.

Eine wesentliche technologische Änderung ist das Aufkommen der hoch leistungsfähigen speicherbasierten Switch-ASICs. Die Grundlagen dazu wurden ja bereits in meinen Artikeln in der Serie Ethernet Evolution (Teile 18 und 19) auf dem Wissensportal und in meinem Video "Speicherbasierte Switch ASICs" auf ComConsult Study.tv dargestellt.

Eine Hand voll dieser neuen Switch-Chips kann auf der Fläche einer besseren Tafel Schokolade ein konvergentes Multi-Terabit Ethernet mit L3- und (demnächst) L4-Funktionalität bilden. Alle Umsetzungen von Adressen unterhalb der IP- oder TCP-Schnittstelle geschehen automatisch, sämtliche innerhalb des Verbundes notwendigen Strukturfunktionen sind bereits in Hardware implementiert. Übrigens: der Stromverbrauch der Konfiguration liegt unter 1 % des Verbrauchs aktueller Switch-Modelle.

Natürlich kommt mit diesen Chips auch der größte Teil der bisherigen Verkabelung auf den Sondermüll, weil sie einfach nicht mehr benötigt wird. Letztlich ist die geeignete Positionierung dieser Chips z.B. in Blade-Servern ein interessantes Problem.

Es sollte bereits an dieser Stelle klar geworden sein, dass diese Chips mit nichts vergleichbar sind, was es vorher in dieser Richtung gab.

Nun, trotz allen funktionalen Reichtums bilden die neuen Power-Chips noch kein Netz, das man jetzt sofort benutzen kann. Da fehlt noch eine Software-Ebene, die einerseits die gesamte Steuerung des Netzes ermöglicht und andererseits die Schnittstellen so zur Verfügung stellt, dass sie z.B. von VMs unmittelbar benutzt werden können.

Und hier kommt SDN, das Software Defined Networking, ins Spiel.

Die zentrale Komponente von SDN sind die Controller. Sie haben die Kern-Aufgabe, auf hohem logischen Niveau die Definition logischer Verbindungen zu er-

möglichen und diese Definition, zu der natürlich auch Qualitätsparameter gehören, geeignet durch Nutzung der Elemente der Hardware durchzusetzen. Die Kommunikation zwischen den Controllern und der Hardware geschieht durch eine definierte Schnittstelle, die letztlich auch ausschließlich diesem Zweck dient und nicht noch „nebenher" Nutzdaten überträgt. In diesem Rahmen kann es notwendig sein, eine Art Treiber zu definieren, der die relativ abstrakten Wünsche der Controller in konkrete Informationen umsetzt, die z.B. die Adresstabellen der Switches füllen.

Das Verständnisproblem, was viele heute mit SDN haben, ist, dass SDN ein abstraktes Konzept ist, welches zunächst einmal völlig unabhängig von den Möglichkeiten einer realen Netzwerk-Hardware entwickelt wurde. Die erste wirklich bekannt gewordene Implementierung eines SDN-Konzeptes ist OpenFlow. Sieht man aber genau hin, ist OpenFlow nichts anderes als ein Treiberkonzept, welcher die Kommandos, die von einem Controller kommen, entsprechend in (dumme) Switching-Hardware umsetzt.

Festzuhalten ist an dieser Stelle auch sofort, dass OpenFlow in seinen jetzigen Versionen ausschließlich für ganz dumme, existierende L2-Switches entwickelt wurde. Das kann man natürlich so für die neuen Power-Chips nicht mehr brauchen und es müssen andere Entwicklungen her, die OpenFlow erheblich erweitern oder ganz obsolet machen. Trotzdem ist es gut geeignet, das SDN-Konzept zu verdeutlichen.

Ein weiterer wichtiger zu betrachtender Bereich ist die VM-Anbindung. Dynamische Virtualisierungsumgebungen haben immerhin das K.O.-Kriterium für bestehende Netze gebildet. Wir können den Standpunkt einnehmen, dass die VMs eine hochwertige Kommunikationsschnittstelle wie IPC oder TCP/IP mit zusätzlichen Session-Layer-Funktionen benutzen und es Aufgabe der SDN-Controller sein wird, genau diese Schnittstelle durchzusetzen, und zwar völlig unabhängig vom aktuellen Aufenthaltsort einer VM. Die Vorstellung, dass VMs vNICs, vHBAs oder vHCAs mit vMAC-Adressen benutzen sollen, ist marketingtechnischer Unsinn und ein Teil der Ursache des aktuellen Desasters. Eine VM ist ein Prozess. Daher benötigt sie auch eine ordentliche Schnittstelle für die Kommunikation zu anderen VMs (die auch Prozesse sind) oder für die I/O und sonst nichts. Die Betriebssystem-Prozesse, die VMs migrieren lassen, brauchen das auch.

6. Konsequenzen für Betreiber privater Netze

Was können Unternehmen oder andere Betreiber privater Netze jetzt tun?
Der massive technologische Umbruch hin zur multidimensionalen DV wird sich erfahrungsgemäß über einen längeren Zeitraum erstrecken. Momentan befinden wir uns in einer „Desorientierungsphase", auch die gehört dazu.

Die in Zukunft benötigte Hardware ist bereits verfügbar, wenn auch noch nicht in ihrer endgültigen Darreichungsform. Die Power-Chips kann man kaufen und Hersteller setzen sie schon in die gewohnten Blechkästen, damit man genügend Ethernet-Buchsen montieren kann. In den nächsten Jahren werden diese Kästen im Rahmen einer engeren Integration zwischen Servern und Netzkomponenten als singuläre Komponenten natürlich verschwinden.

Die Umsetzung von BYOD-Konzepten und die Schaffung passender wireless Versorgungsstrukturen müssen, können und werden konkret angegangen werden.

Dies schafft einen Zeitrahmen, in dem die aktuell noch in hinreichender Breite greifbaren SDN-Konzepte reifen werden.

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

Für unverlangte eingesandte Manuskripte
wird keine Haftung übernommen