ComConsult Research

Der Netzwerk Insider

Februar 2014

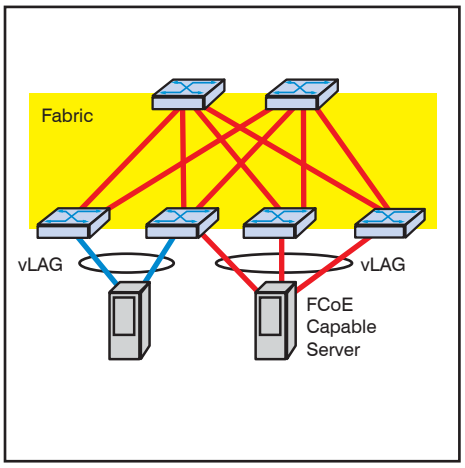
Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

Netzwerk-Design in Zeiten von 10/40/100 Gbit: Wie sieht die Zukunft aus? - Teil 1

von Dipl.-Inform. Petra Borowka-Gatzweiler

Aktuelle Trends in der Kommunikations-Entwicklung verändern das das Netzwerk-Design. Dies gilt sowohl für den Data Center als auch den Campus und Access Bereich. 10 Gbit Technologie ist Legacy geworden. 40 Gbit Technologie ist in den meisten etablierten Produktlinien vorhanden, 100 Gbit stellt derzeit die Technologie-Spitze dar. Modernes Netzwerk-Design reduziert sich jedoch nicht nur auf Datenraten sondern nutzt auch intelligente und neue Technologien. Hat die Lebenszeit von sternförmigen Spanning Tree Strukturen somit ihr Ende erreicht? Der nachfolgende Beitrag befasst sich mit grundlegenden Design-Aspekten



und ihrer Umsetzung in der Welt der 10/40/100 Gbit Komponenten und Produkte. Er erläutert, welche herstellereigenen und standardbasierten Nachfolgertechnologien aktuell in Entwicklung sind und welche Marktgruppen diese Technologien nach vorne tragen wollen.

weiter auf Seite 10

Zweitthema

VMware NSX – Anfang oder Ende einer Entwicklung?

von Dip.-Math. Cornelius Höchel-Winter

In der Netzwerkbranche wird seit längerem mit vielen Emotionen über Sinn und Unsinn von Software in Netzwerken diskutiert – und gemeint ist natürlich nicht die Firmware von Switches, Routern und Firewalls. Begonnen wurde diese Diskussion im Grunde vor über 10 Jahren als sich die Erkenntnis verbreitete, dass das ursprüngliche Entwicklerspielzeug „Virtuelle Maschine“ produktiv genutzt werden kann, aber leider nur mit einem Stückchen Software funktioniert, das die Konnektivität zwischen den virtuellen Maschinen untereinander und mit der Außenwelt realisiert – einem virtuellen Switch.

Der Großteil der Netzwerkbranche reagierte darauf skeptisch bis feindselig, eine Reihe von Entwicklungen war die Folge mit dem Ziel diese virtuellen Switche überflüssig zu machen oder sie höchstens als funktionseingeschränkte Krüppel zu tolerieren, indem man alles Spannende vom Monitoring bis hin zu Sicherheitsfunktionen außerhalb des Hypervisors erledigen wollte.

weiter Seite 24

Geleit

Immer mehr mobile Endgeräte in unseren Netzwerken: wie gehen wir damit um?

ab Seite 2

Standpunkt

Überwachung ist und bleibt der wesentliche Business Case des Internet

auf Seite 22

Aktueller Kongress

Netzwerk Forum 2014

ab Seite 4

Neu! Das Kongress-Portal

Artikel, Videos und Hintergrund-informationen

ab Seite 8

Neuer Report

100 G: Technologie und Standards

auf Seite 20

Zum Geleit

Immer mehr mobile Endgeräte in unseren Netzwerken: wie gehen wir damit um?

Alle Prognosen deuten auf eine erhebliche Zunahme der Menge an mobilen Endgeräten in den Unternehmen in den nächsten drei Jahren hin. Wir haben etablierte und bewährte Methoden, um mit den vorhandenen stationären PC-Systemen umzugehen. Können wir die einfach übertragen oder brauchen wir einen völlig neuen Ansatz?

Tatsächlich adressieren wir mit dieser Frage die Kernfragen, um die sich alles dreht:

- Warum haben wir eigentlich mobile Endgeräte?
- Was tun wir mit ihnen? Machen sie Sinn?
- Wie viele werden wir denn nun haben?
- Warum können wir sie nicht mit den etablierten Tools betreiben?

Gehen wir der Reihe nach auf diese Fragen ein:

Der Durchbruch der mobilen Endgeräte kam mit dem iPhone 2007, dem 2009 die Android Smartphones folgten. Wie immer wir auch in Zukunft mit unseren mobilen Endgeräten umgehen, wir müssen davon ausgehen, dass potenziell jeder Mitarbeiter ein solches Smartphone besitzt und auch nutzt. Die Leistungsfähigkeit dieser Geräte nimmt immer mehr zu und mit der Einführung des 64 Bit A7 durch Apple hat das erste Gerät in Form des iPhone 5s die Leistung eines traditionellen Desktop-Computers erreicht (Pentium 4 um präzise zu sein). Samsung wird vermutlich in wenigen Wochen mit dem Galaxy 5 folgen und allgemein können wir für die nächsten Jahre davon ausgehen, dass Smartphones genügend Leistung für nahezu alle Office-Applikationen haben.

Der nächste große historische Schritt kam mit der Einführung des iPads im April 2010. Smartphones sind sicher eine interessante Geräteklasse, aber sie werden immer unter dem zu kleinen Bildschirm und der eher umständlichen Tastatur-Eingabe leiden. Es fehlt einfach Platz. Die Tablets sind deutlich universeller nutzbar, sowohl von der Eingabe als auch von der Lesefähigkeit her. Die Masse der Geräte bewegt sich bisher im Bereich zwischen 7 und 10 Zoll Größe, doch noch in diesem Jahr wird sich vermutlich eine neue Kategorie um die 12 Zoll etablieren. Ähnlich wie bei den Smartphones haben Tablets in Zukunft ganz eindeutig Desktop-Leistung. Die Größe ermöglicht eine optimalere Kombination aus Display, Leistung und Batterie-

Kapazität. Im Gegensatz zu den Smartphones können wir bei den Tablets aber nicht unterstellen, dass in Zukunft generell jeder Mitarbeiter auch eines haben wird. Wir brauchen also auf jeden Fall eine Klarstellung, in welchem Umfang wir unter mobilen Geräten auch Tablets sehen.

Damit sind wir bei der Frage, wozu die mobilen Geräte eigentlich eingesetzt werden und was wir denn mit ihnen machen. Bei den Smartphones hatten wir zu Beginn noch eine starke Bindung an unser traditionelles IT-Verständnis. Die Kombination aus Email-Client, Kalender, Instant Messenger und Internet-Browser war kein Bruch mit dem etablierten IT-Verständnis. Dies ist mittlerweile durchaus in Frage zu stellen. Tablets sind sicher nicht dazu geschaffen unsere traditionellen Büro-Anwendungen von Word bis SAP auszuführen. Sie kommen mit einem neuen Typ von Betriebssystem, der auf kleine, leichte und mobile Geräte optimiert ist. Dementsprechend kommen sie mit weniger Speicher aus, brauchen weniger Leistung und haben eine deutlich längere Batterie-Nutzungsdauer. Viel wichtiger aber ist, dass die Bedienung eine völlig andere ist. Apple hat mit der Erfindung der Gestensteuerung einen Quantensprung der IT-Technik bewirkt. Ob Google das mit Android unzulässig kopiert hat oder nicht sei an dieser Stelle egal. Fakt ist, dass wir jetzt eine neue Art von IT haben, die völlig anders genutzt wird als bisher.

Dies hat Konsequenzen:

- Tablets sind nicht dafür geschaffen, traditionelle Windows-Applikationen auszuführen. Jeder Versuch in diese Richtung mit Container-Technologie, Virtualisierung oder was auch immer wird an der Akzeptanz und der mangelnden Leistung scheitern. Traditionelle Applikationen sind einfach für eine andere Umgebung entwickelt. Allerdings ist es denkbar, dass solche Applikationen auf einen Multi-Geräte-Einsatz angepasst werden, wie es Apple gerade mit Keynote und Pages eindrucksvoll gezeigt hat.
- Tablets schaffen eine neue Dimension von Benutzer-Akzeptanz. Die neue Art der Bedienführung hat die Fähigkeit, Benutzerkreise an IT-Prozesse heran zu bringen, die bisher nur sehr unbefriedigend integriert werden konnten.
- Die ganze Gerätetechnik (im Sinne von Gewicht und Größe) und das Bedienkonzept sind auf Mobilität ausgelegt. Dies bedeutet, ein Tablet kann in einer Hand gehalten werden und es können Abfragen, Eingaben und beliebige Manipulationen im Stehen, Liegen und wo auch immer ausgeführt werden.
- Die schnelle und einfache Art der Nutzung in Kombination mit der Größe ermöglicht Anwendungen, die sich mit traditionellen Laptops nur sehr unbefriedigend abdecken lassen.

Noch einmal im Klartext: Tablets sind nicht dazu da, die alten traditionellen IT-Applikationen auszuführen. Es gibt klar eine Überschneidung in dem Sinne, dass sie natürlich einen Email-Client haben, einen Internet-Browser, einige Office-Programme, ein Dateisystem usw. Aber der eigentliche Vorteil und der Nutzen der Geräte für Unternehmen liegt in der Erschließung neuer Prozesse.

Beispiele für solche Prozesse sind:

- Der gesamte Vertriebsbereich
- Service-Prozesse
- Gutachter- und Bewertungs-Prozesse
- Krankenhäuser
- Verkehr und Transport

Typische Mehrwertfunktionen sind die Kombination aus der sehr detailreichen Anzeige mit intelligenten Abfragefunktionen. Auch die Nutzung der integrierten Kamera und die gesamte Kommunikationsfähigkeit sind eine ideale Basis für verteilte Service-Prozesse. Wer konkrete Beispiele dazu sucht, der sei auf die Apple-Webseite verwiesen (http://www.apple.com/ipad/business/profiles/), die genügend spannende Projekte vorstellt. Die Schlüsselfragen für Unternehmen sollten also mit Bezug auf Tablets ein:

Immer mehr mobile Endgeräte in unseren Netzwerken: wie gehen wir damit um?

Abbildung 1: Tablet-Einsatz in der Energiewirtschaft bei Eaton Power Management Quelle: Apple

Abbildung 2: iPad-Einsatz bei American Airlines Quelle: ipadinsight.com

- Haben wir Benutzer, die in ihrer Arbeit von einem Tablet profitieren würden (zum Beispiel durch ein intuitiveres Benutzer-Interface)?
- Haben wir Prozesse, die wir mit Tablets besser und effizienter abwickeln können?

Damit sind wir bei der Frage, wie viele wir denn davon haben werden. Speziell bei den Tablets lässt sich die Frage für professionelle Anwendungen im Moment nicht beantworten. Die Kernfrage für die Zukunft ist, ob die beiden Welten des traditionellen Desktops und der Tablets irgendwann zusammen wachsen und dann zur universellen Endgeräteklasse werden. Von der Hardware-Leistung ist das ohne Frage denkbar. Der Schlüssel liegt in den Applikationen. Microsoft hat mit Windows 8 hier einen mutigen Schritt gewagt. Aber das Experiment ist voller Haken und Ösen und wird in der jetzigen Form kaum Erfolg haben können. Die Bedienung ist zu komplex, der App-Shop ist bisher nur sehr unbefriedigend eingebunden und nach wie vor dominieren Geräte, die auf die Nutzung traditioneller Windows-Anwendungen ausgelegt sind. Der Microsoft-Weg von 8 auf 8.1 und das für April erwartete Patch für 8.1 zeigen dann auch, dass sich Microsoft immer mehr dem Look- und Feel von Windows 7 annähert. Auch das Surface Pro 2 wirbt zwar mit seiner Tablet-Eigenschaft, ist aber als Tablet viel zu schwer, zu teuer und klar auf die traditionelle Welt ausgelegt. Mit der besseren Einbindung des App-Shops in die Metro-Darstellung im April wird trotzdem hoffentlich auch der Tastatur-freie Betrieb besser als bisher.

Lassen Sie uns an dieser Stelle auch einen Blick in die Zukunft werfen. Wird es bei dieser Trennung zwischen „alter“ und „neuer“ IT bleiben? Mit hoher Wahrscheinlichkeit nicht. Wir stehen am Anfang einer Entwicklung, an deren Ende das jeweilige Endgerät und sein Betriebssystem keine Bedeutung mehr haben werden. HTML5, das Google Chromebook, Apples Geräte-übergreifende Applikations-Lösung und die Integration der Cloud zeigen einen klaren Weg weg von der bisherigen Geräte-zentrischen Welt auf. Trotzdem bleiben Unklarheiten. Microsoft wird sicher alles versuchen, die „alte“ Welt so lange wie möglich zu erhalten. Immerhin bedroht die neue Welt mit dramatisch niedrigeren Preisen für Software das Microsoft-Geschäftsmodell nicht unerheblich. Aber auch bei Microsoft ist Windows 365 eine der großen Zukunfts-Hoffnungen.

Damit ist auch schon fast die letzte Frage beantwortet. Wir können mobile Endgeräte wie Smartphones und Tablets nicht mit unseren etablierten Tools betreiben, weil sie eine neue Form der IT darstellen. Zwar gibt es eine Grauzone, einen Überlappungsbereich mit Apps aus beiden Welten, aber im Kern erfordern mobile Endgeräte einen komplett neuen Betriebs- und Architektur-Ansatz. Für diesen Ansatz wurde der Begriff „Mobility System“ geschaffen.

Zu einem „Mobility System“ gehören typischerweise:

- Der Zugang zu internen und externen Netzwerken
- Die Benutzer- und Rechteverwaltung, die zum Beispiel jetzt Ortsabhängig sein kann und andere Funktions- und Datenquellen einbeziehen kann
- Die Bereitstellung von Daten
- Ein App-Store mit Apps, die für ein Unternehmen wichtig sind
- Einen Zugriff auf ausgewählte Elemente der „alten“ Welt

Dieses Mobility-System lässt sich so nicht von der Stange kaufen. Es gibt zwar gute und bewährte Tools in diesem Bereich, aber die Kombination zu einer Gesamtlösung ist in jedem Fall ein größeres Projekt. Einzelne Hersteller wie AirWatch (jetzt VMware) versuchen zwar immer mehr, die notwendigen Funktionselemente aus einer Hand zu liefern, aber es gibt einen Bereich, der nur durch das betreibende Unternehmen selbst kommen kann: die Klärung, welche Daten und Applikationen wie eingebunden werden. Dazu gehört auch die Frage, welche Prozesse im Unternehmen überhaupt optimiert werden sollen und in welchem Umfang dazu eigene Apps erforderlich sind.

Kommen wir auf die Ausgangsfrage zurück: brauchen wir einen neuen IT-Ansatz für mobile Endgeräte? Der Schlüssel zur Antwort auf diese Frage liegt in der Erkenntnis, dass speziell Tablets nicht dazu da sind, die etablierte IT mit preiswerteren Geräten abzulösen. Ihr Mehrwert liegt in einer neuen Form der Nutzung für genau definierte Prozesse. In diesem Sinne macht auch die unreflektierte Unterstützung von Tablets in einem BYOD-Projekt eigentlich keinen Sinn. Sie produziert nur Probleme ohne einen Mehrwert zu schaffen. Mobile Endgeräte sind dann wirtschaftlich und profitabel, wenn sie dafür eingesetzt werden, wofür sie eigentlich geschaffen sind.

Lohnt sich der Aufwand der Schaffung eines Mobility Systems? Der aktuelle Zustand muss als Beginn einer Migration in ein verändertes IT-Verständnis gesehen werden. Die Beherrschbarkeit dieser Entwicklung erfordert ein solides Fundament. Mit dem Blick nach vorne lohnt sich der Aufbau eines Mobility Systems also auf jeden Fall. Das Problem liegt auch nicht mehr im Bereich Mobile Device Management. Diese Tools haben einen gewissen Reifegrad erreicht. Die große Aufgabe liegt vielmehr in der Gesamtlösung, in der Integration aller Bereich inkl. der sicheren Bereitstellung von Daten und Applikationen.

Ihr
Dr. Jürgen Suppan

Aktueller Kongress

ComConsult Netzwerk Forum 2014

Praxis und Zukunft von Unternehmensnetzen

24.03. - 26.03.14 in Königswinter

Die ComConsult Akademie veranstaltet vom 24.03. bis 26.03.2014 ihr "ComConsult Netzwerk Forum 2014" in Königswinter.

Traditionell ist die Dienstneutralität das Hauptmerkmal aller Netzwerke. Alle bisherigen Versuche, eine Applikations-spezifische Ende-zu-Ende Kontrolle und Garantie einzuführen sind in den letzten 20 Jahren gescheitert. Auch Prioritäten und Bandbreitenreservierungen für Verkehrsklassen sind trotz diverser Standards umstritten. Nun haben sich Netzwerke auf der Server-Seite in den letzten 5 Jahren deutlich verändert. Hier dominieren inzwischen die Software-Ports in den virtuellen Switches gegenüber den Hardware-Ports. Aus Sicht der Applikationen und virtuellen Maschinen spielt sich das Netzwerk mehr und mehr in Software ab. Verbindet man das mit dem zunehmenden Bedarf nach „One-Touch-Installationen“ und der schnellen Inbetriebnahme auch komplexer Applikationen innerhalb von Minuten, dann hat sich in der Server-Welt der Netzwerk-Schwerpunkt von der Hardware in die Software verschoben.

Dies wird eine Reihe von Fragen auf:

- Liegt die Zukunft der Server-Vernetzung in der Software?
- Hat das dienstneutrale Netzwerk damit ausgedient?
- Wie kann eine automatische Netzwerk-Konfiguration bei der Installation von Servern erreicht werden?
- Wie kann der Bedarf dynamischer virtueller Umgebungen am besten erfüllt werden?
- Wer wird die Zukunft bestimmen: Anbieter wie VMware mit NSX oder die traditionellen Netzwerker mit Application Aware Networks?

Gleichzeitig sind wir mitten im Übergang von 1/10 Gigabit-Netzwerken zu 10/40/100 Gigabit. Dies geht einher mit einer Vielzahl sehr verschiedener Gestaltungsmerkmale, die unter dem Begriff Fabric-Design laufen. Auch im Design wird dabei die Neutralität des Netzwerkes immer mehr mit einem Fragezeichen versehen. Hier ist nicht nur das RZ-Netzwerk eine treibende Kraft, sondern die hier entwickelten Technologien dehnen sich immer mehr auf den Campus aus. Abgerundet wird das mit der sich ausdehnenden Problematik der Integration mobiler Endgeräte.

Auch hier haben sich brisante Fragen entwickelt:

- Wie sieht ein übergreifendes 10/40/100 Netzwerk-Design in Zukunft aus?
- Wie sieht das Campus-Netzwerk der Zukunft aus, wird es zunehmend von Design-Prinzipien des Rechenzentrums beeinflusst?
- Ist das Ende modularer Switches nahe?
- Brauchen wir wirklich mehr als 10 Gig parallele Verkehrsströme?

Der Endgerätebereich wird sich in den meisten Unternehmen in den nächsten 5 Jahren deutlich verändern. Mobile Endgeräte und neue Endgerätevarianten werden die Zukunft bestimmen. Das führt nicht nur zur Frage des besten physikalischen Anschlusses, sondern vor allem zur Frage eines schlüssigen Gesamtkonzepts von der Physik über die Architektur bis zur Sicherheit.

Die Fragen der Zukunft sind:

- Wie sieht ein Konzept zur schlüssigen Integration mobiler Endgeräte aus?
- Was bedeutet das für unsere Netzwerke?
- Wie sehen Gesamtarchitekturen von Endgerät bis zum App-Shop aus?
- Wie kann die notwendige Sicherheit wirtschaftlich umgesetzt werden?

Das ComConsult Netzwerk Forum 2014 stellt sich den herausragenden Fragen der Entwicklung der Unternehmensnetzwerke. Nach 10 Jahren des Konzept-Stillstands ist das traditionelle Netzwerk unter Druck sowohl aus der Server- als auch aus der Endgeräte-Welt. Kombiniert man dies mit dem notwendigen Bandbreitenwechsel auf 10/40/100, dann steht das Unternehmensnetzwerk der Zukunft auf dem Prüfstand.

Wir analysieren für Sie wohin die Netzwerk-Entwicklung geht, wer die Kontrahenten sind, welche Vor- und Nachteile die verschiedenen Alternativen für Ihr Unternehmen haben und wie relevant einzelne Technologien sind. Investieren Sie zukunftssicher in Ihre Netzwerke, das ComConsult Netzwerk Forum 2014 unterstützt Sie dabei.

Neu! Das Kongress-Portal

Auf dem Kongress-Portal stellen wir Ihnen einige Hintergrundinformationen rund um die Themen des ComConsult Netzwerk-Forum 2014 zur Verfügung. Die markierten Beiträge sind spezielle Angebote, auf die ausschließlich Kongressteilnehmer Zugriff haben, um sich optimal auf die Veranstaltung vorzubereiten. Diese Seite wird laufend erweitert und aktualisert.

Als Teilnehmer des Forums benötigen Sie einen Online-Account, um auf exklusive Beiträge des Kongress-Portals zugreifen zu können.

http://www.comconsult-research.de/kongresse/netzwerk-2014/

Programmübersicht Netzwerk-Forum 2014

Montag 24.03.2014

9:30 Uhr (45 Minuten) — **Keynote: Aktuelle Technologie-Trends und ihre Bedeutung für die IT**
- Mobile Endgeräte: Entwicklung und Potentiale
- BYOD: vom Alptraum zur neuen Basis für die IT
- Anwendungsbewusste Netze: Top oder Flop?
- Entwicklung der Netze: Standards oder nicht?

Dr. Franz-Joachim Kauffels, unabhängiger Unternehmensberater

Themenblock: Kampf um die Steuerung der Netzwerke

10:15 Uhr (45 Minuten) — **Dienstneutrale Netzwerke auf dem Prüfstand: wie Anwendungs-bewusst sollen Netzwerke wirklich sein?**
- Dienstneutrales Netz: was bedeutet das?
- Sind alle heutigen Netze dienstneutral?
- Ist Dienstneutralität der Netze überholt? Sollen Applikationen Netze steuern?
- Welchen Stellenwert hat Software-getriebene Netzsteuerung?
- Wenn Software-getrieben, dann welche Software und von wem?

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

11:00 Uhr Kaffeepause

11:30 Uhr (45 Minuten) — **Intelligente Dienste - Dumme Netzwerke: Kampt der Technologien und der Hersteller**
- Ausgangslage: Schnelle Installation und Aktivierung von Anwendungen im Netzwerk
- Die Schnittstelle zum Netzwerk: was nach der Server-Virtualisierung fehlt, typische Probleme
- Die technischen Alternativen
  - Overlay-Konzepte und Protokolle am Beispiel VMware NSX
  - Dienst-Erkennung und Unterstützung im Netzwerk am Beispiel Avaya SPB
  - Application-Aware Networks am Beispiel Cisco • SDN
- Bewertung: • Welche Probleme werden womit gelöst? • Welcher Hersteller hat die Nase vorn?
  • Wie sollte eine gute Lösung wirklich aussehen?

Dipl.-Math. Cornelius Höchel-Winter, ComConsult Research GmbH

12:15 Uhr (je 15 Minuten) — **Technologie-Statements Aussteller**

N.N.

12:45 Uhr Mittagspause

14:00 Uhr (45 Minuten) — **Intelligente Netzwerke und Applikationskontrolle – wie das Netzwerk zur Analytics Plattform werden kann**
- Wie erkenne ich heute Applikationen im Netzwerk?
- SDN und applikationszentrische Architekturen in der Control und Data Plane
- Innovation durch das Netzwerk: Analytics and BI durch Daten aus dem Netzwerk – ein prominentes Fallbeispiel

Dipl.-Ing. Markus Nispel, Extreme Networks GmbH

14:45 Uhr (45 Minuten) — **Netzwerk-Monitoring als Gesamtkonzept: wie können Overlays und Software-Komponenten sauber integriert werden?**

N.N.

15:30 Uhr Kaffeepause

Themenblock: Netzwerk-Design für 10/40/100 Netzwerke

16:00 Uhr (45 Minuten) — **Netzwerk-Design mit 10/40/100 Gigabit: wie sieht die Zukunft aus?**
- Design-Elemente für Access, Campus und RZ
- Berechnung der Überbuchungs-Faktoren
- Campus Design-Regeln / RZ Design-Regeln
- Welche FO-Verfahren sollten wo eingesetzt werden?
- Empfehlung für die schrittweise Umstellung auf 10/40/100
- Produktbeispiele etablierter Hersteller

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

16:30 Uhr (45 Minuten) — **Innovation im Campus: gibt es das?**
- Cisco Catalyst 6800 – das ist neu
- ENC – Enterprise Network Controller – erste Einblicke
- Campus Fabric – ein Ausblick

Gerd Pflüger, Cisco GmbH

17:15 Uhr (30 Minuten) — **Statement zur Happy Hour: SDN‘s ungelegte Eier**

Markus Schaub, ComConsult-Study.tv

18:00 Uhr — **Happy Hour**

Programmübersicht Netzwerk-Forum 2014

Dienstag 25.03.2014

9:00 Uhr
45 Minuten

Chancen und Tücken des Einsatzes von MPO und Alternativen bei 40GbE
- Die Grundelemente
- Das Polaritätsproblem bei MPO Systemen
- Der Umgang mit High Density Rangierungen
- Die sinnvolle Messung und Dokumentation von MPO Strecken
- Die Rahmenbedingungen bei proprietären 40 GbE-Lösungen mit zwei Fasern

Dipl.-Ing. Hartmut Kell, ComConsult Beratung und Planung GmbH

9:45 Uhr
45 Minuten

WLAN-Architektur der Zukunft: Migration aus 11n in die Folgestandards
- Wie die neuen WLAN-Techniken 7 Gbit/s erreichen wollen
- Welche Datenraten sind heute realistisch?
- Kompatibilität oder Fortschritt: Das Dilemma zukünftiger WLAN-Planung!
- Wann kommt der 10-Gigabit-Anschluss am Access Point?
- Wird es zukünftig noch WLAN-Controller geben? *Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH*

10:30 Uhr Kaffeepause

Themenblock: Mobile Endgeräte in Netzwerken

11:00 Uhr
45 Minuten

Mobile Enterprise – Der Trend zu App Stores
- App Stores für alle (und von allen)!
- Die Chancen und Herausforderungen von App Stores
- Der Trend zu App Stores und die Herausforderungen für die Unternehmens-IT
- Die Auswirkungen von App Stores auf die Infrastruktur

Dipl.-Inform. Dominik Franke, ComConsult Beratung und Planung GmbH

11:45 Uhr
45 Minuten

Mobile Enterprise – Auf dem Weg zum Mobilen Unternehmen
- Welchen Stellenwert haben mobile Endgeräte und Applikationen im Unternehmen?
- Was bietet der Markt für mobile Endgeräte dem Unternehmen?
- Welche Entwicklungen im Mobile-Markt sind für Unternehmen relevant?
- Was sind mobile Killer-Applikationen im Geschäftsumfeld?

Dipl.-Ing. Dominik Zöller, ComConsult Beratung und Planung GmbH

12:30 Uhr
15 Minuten

Technologie-Statement Aussteller

N.N.

12:45 Uhr Mittagspause

14:00 Uhr
45 Minuten

Internet of Things und Unternehmensnetzwerke
- IoT - die Entwicklung hin zu einer vollvernetzten Welt
- Neue Möglichkeiten für Unternehmen
- Sicherheit im IoT - alte Gefahren in neuen Bereichen
- Empfehlungen zur Vorgehensweise

Prof. Dr. Marko Schuba, Fachhochschule Aachen

14:45 Uhr
45 Minuten

15:30 Uhr
45 Minuten

Von der simplen Integration Mobiler Endgeräte zu Mobility Öko-Systemen für Unternehmen
- Transformation der Arbeitsplätze wird Fokus der Enterprise IT
  - Arbeitskraft, Arbeitsplatz, Arbeitsweise
- Zusammenhang der Elemente einer ganzheitlichen Mobility Architektur
  - Applikationen/Apps, Endgeräte, Entwicklungsumgebungen, Geräte-/App-Management, Infrastrukturen, Sicherheit, Dienste
- Implementierung einer IT Architektur für Mobility
  - Planung und Design • Applikation und Nutzerfahrung
  - Mehrwert für das Unternehmen

Dipl.-Ing. Axel Simon, Hewlett-Packard GmbH

Sicherheits-Konzept für mobile Endgeräte im Netzwerk
- Bedrohungen ohne Ende: Von der Lauschattacke bis zum Abfluss kritischer Daten
- Sandboxing, Virtualisierungstechniken und Verschlüsselung: Reichen solche Sicherheitsmechanismen aus?
- Profiling-Techniken, Erkennung von Endgeräten und Policy-Zuweisung
- Mobile Device Management und Company App Stores als Sicherheitsmaßnahmen: Möglichkeiten und Grenzen
- Sichere Netzanbindung und Abgrenzung unterschiedlicher Benutzergruppen

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

16:15 Uhr Kaffeepause für Teilnehmer der 3-tägigen Veranstaltung

16:15 Uhr Ende der 2-tägigen Veranstaltung

Programmübersicht Netzwerk-Forum 2014

Mittwoch 26.03.2014

9:00 Uhr
ganzer Tag

Netzwerk-Design im Zeitalter von 10/40/100 GbE

- Anforderungs-Analyse, Planungsschritte
- Aktuelle Design-Technologien:
  - Layer-2 Multipath: TRILL, SPBM
  - Fabric-Konzepte
  - Einsatz von VLANs und Overlay-Technologien: SPBM, VXLAN, NVGRE, LISP
  - Technische Grundlagen von SDN, hat SDN Mehrwerte für ein modernes Netzdesign?
- Planungs-Ansätze, Migrations-Szenarien 10G / 40G / 100G
- Markt für Enterprise-Netze 10G / 40G / 100G: Vergleich der Hersteller-Portfolios
- Kostenvergleich verschiedener Lösungen anhand von Beispiel-Szenarien

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

10:30 Uhr Kaffeepause

12:45 Uhr Mittagspause

15:30 Uhr Ende der 3-tägigen Veranstaltung

Fax-Anmeldung

02408/955-399 oder 02408/955-398

Hiermit melde ich mich verbindlich zum **ComConsult Netzwerk Forum 2014** an.

☐ Kongress 3 Tage	☐ Kongress 2 Tage	☐ Intensiv-Tag
vom 24.03. - 26.03.14 in Königswinter zum Preis von € 2.390,-- netto	vom 24.03. - 25.03.14 in Königswinter zum Preis von € 1.990,-- netto	am 26.03.14 in Königswinter zum Preis von € 990,-- netto

☐ **Bitte reservieren Sie für mich ein Zimmer**

vom _____ bis zum _____14
im Maritim Hotel Königswinter zum Sonderpreis von 119,-- € inkl. Frühstück

☐ **Reportauswahl**

Ich bestelle zusätzlich den Report „100 G: Technologie und Standards “ zum Sonderpreis von nur €338,-- netto

_____
Vorname, Nachname

_____
Firma

_____
Straße

_____
PLZ, Ort

_____
Telefon, Fax

_____
E-Mail

Ich habe die Kongressbedingungen zur Kenntnis genommen.

_____
Datum, Unterschrift

Bis zu 14 Tagen vor Kongressbeginn behält sich der Veranstalter das Recht vor, den Kongress zu stornieren. Schriftliche Absagen von Teilnehmern sind bis 15 Tage vor Veranstaltungsbeginn kostenlos möglich, ab dem 14. Tag vor Veranstaltungsbeginn sind 50 % des Teilnahmebetrages zu zahlen. Bei Nichterscheinen oder Stornierung am Veranstaltungstag wird der gesamte Teilnahmebetrag fällig; der Teilnehmer erhält nach Ablauf der Veranstaltung die kompletten Schulungsunterlagen per Post. Die Übertragbarkeit auf andere Mitarbeiter ist möglich. Bitte informieren Sie uns. Die Gebühr ist im Voraus zu entrichten. Die Buchung eines Kongresses innerhalb der Frühbucherphase kann nicht storniert werden. Gerne akzeptieren wir aber einen Ersatzteilnehmer. Der Veranstalter behält sich Änderungen im Programm vor.

ComConsult Akademie
Pascalstraße 25
52076 Aachen
Telefon: 02408 - 955300
mail@comconsult-akademie.de

NEU! Das Kongress-Portal

Das Kongress-Portal

Artikel, Videos und Hintergrundinformationen

Mit dem ComConsult Netzwerk Forum 2014 startet die ComConsult Akademie eine neue Dimension von Erlebnis für Kongress-Teilnehmer. In einer Zeit, in der Mitarbeiter immer mehr Probleme haben, für längere Zeit von der Arbeit weg zu sein und gleichzeitig einen immer höheren Bedarf an Information haben, musste unser bisheriges Kongress-Konzept auf den Prüfstand. Unser Ergebnis: mehr und intensivere Information in weniger Präsenz-Zeit.

Mit dem neuen Kongress-Portal, das sowohl frei zugängliche Informationen für alle als auch exklusive Artikel und Videos zu den Inhalten des Kongresses enthält, die nur für Teilnehmer zugänglich sind, können sich alle Interessierten optimal auf die Veranstaltung vorbereiten. Die Vortragsunterlagen werden im exklusiven Bereich der Site veröffentlicht. In der Vorbereitungsphase können Interessente hier ihre Fragen und Wünsche bereits vor der Veranstaltung einreichen. Ab dem ersten Tag der Veranstaltung gibt es den kompletten Vortrag als PDF-Dokument in der jeweils aktuellen Form. Diese Seite wird laufend erweitert und aktualisiert.

Artikel

Internet vs. Intranet of Things
6. Februar 2014 von Dominik Franke

Das Internet of Things (IoT) wird gerne als Vision für ein vernetztes Konstrukt aus grenzenlos kommunizierenden Komponenten und Objekten gesehen. So können beispielsweise Fahrzeuge das Schaltverhalten der nächsten Ampel auslesen, der Amazon-Kunde den Lieferwagen mit seinem Paket aus der Vogelperspektive beobachten und die Vertragswerkstatt ihre Kapazitäten anpassen, wenn in der Umgebung mehrere Fahrzeuge zugleich Mängel melden...

Application-Aware, Controlled, Centric, Software-Defined … Networking
5. Februar 2014 von Markus Nispel

Offene SDN-Diskussion: aus einem US-Blog von Markus Nispel auf SDNcentral, hier ins Deutsche übersetzt

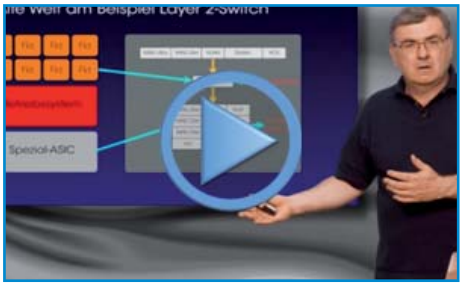
Es ist sehr interessant zu sehen, wie Ciscos „Insieme"-Announcement letzten Herbst die Diskussion über die verschiedenen Aspekte der Application-Awareness im Netz und des Software-Defined Networking erneut angestoßen hat...

VMware kauft MDM- und Sicherheits-Spezialisten AirWatch
4. Februar 2014 von Dr. Franz-Joachim Kauffels

Die Paradigmenwechsel bekommen Grip. Kunden strafen IBM ab, weil sie statt Spezial-Hardware lieber virtualisierte Software-Lösungen auf flexiblen Plattformen haben möchten. BYOD und Mobilität breiten sich trotz aller höchst berechtigten Sicherheitsbedenken ungehemmt aus. Wer mitspielen will, muss Technologie in Form kompletter Unternehmen zukaufen. Aus aktuellem Anlass betrachten wir heute die neuesten Aktivitäten von VMware...

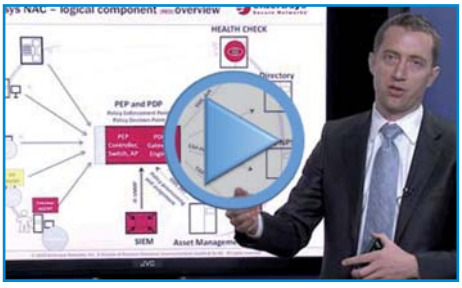
Videos

SDN in 10 Minuten



Gigabit WLANs: Konsequenzen für das Design

Implementierung von NAC



NEU! Das Kongress-Portal

Vorträge

Keynote: Aktuelle Technologie-Trends und ihre Bedeutung für die IT
Dr. Franz-Joachim Kauffels

Die fulminante Entwicklung mobiler Endgeräte führt zu neuen Herausforderungen und Möglichkeiten bei Betriebskonzepten für die sinnvolle Materialisierung der gewachsenen Leistung für die IT eines Unternehmens. Ein weiterer aus dem Bereich der Providersysteme kommender Trend ist das so genannte „Anwendungs-Bewusstsein“ von Netzen. Ist es wirklich sinnvoll, ihn mittels völlig neuer Steuerungs-Ansätze auch auf private Campus- und RZ-Netze zu übertragen oder reicht es, den seit 30 Jahren erfolgreichen Weg der Steigerung von Grundqualitäten entlang standardisierter Lösungen fortzusetzen?

Dienstneutrale Netzwerke auf dem Prüfstand: Wie anwendungsbewusst sollen Netzwerke wirklich sein?
Dr. Behrooz Moayeri

Vor dem Hintergrund neuester Initiativen führender Hersteller, in deren Mittelpunkt sogenannte applikationszentrische Infrastrukturen stehen, stellt sich die Frage, ob einem streng dienstneutralen oder einem anwendungsbewussten Netz der Vorzug zu geben ist. Der Vortrag geht von der etablierten Definition der Dienstneutralität aus und führt Beispiele für dienstneutrale und nichtdienstneutrale Netze an. Es wird diskutiert, ob die Dienstneutralität angesichts der wachsenden Integration verschiedener Infrastrukturdisziplinen wie Netz, Computing und Storage auf den Prüfstand gehört bzw. einem Ansatz weichen soll, bei dem die Applikationen Netze steuern.

Netzwerk-Design mit 10/40/100 Gigabit: Wie sieht die Zukunft aus?
Petra Borowka-Gatzweiler

Der Vortrag betrachtet die drei typischen Bereiche „Access“, „Campus“ und „Rechenzentrum“ eines Standort-Netzwerks. Aus den Anforderungen an modernes Netzdesign werden Design-Elemente und Design-Regeln abgeleitet, mit denen sich ein modernes Netzwerk planen lässt. Hierzu gehört insbesondere auch die Diskussion von Überbuchungs-Faktoren und Redundanz-Anforderungen und Einsatz von Failover-Verfahren. Es werden Design- und Produktbeispiele für die Migration auf 10/40/100 Gbit dargestellt und Empfehlungen für eine sinnvolle und zukunftssichere Migration gegeben.

Aussteller

AixpertSoft
BELDEN SENDING ALL THE RIGHT SIGNALS
ComConsult BERATUNG + PLANUNG
ComConsult Research
ComConsult Study.tv
Extreme networks
MICROSENS fiber optic solutions euromicron group
psiber

Schwerpunktthema

Netzwerk-Design in Zeiten von 10/40/100 Gbit: Wie sieht die Zukunft aus?

Teil 1

Fortsetzung von Seite 1

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

1. Aktuelle Trends

Anwendungstrends

Mobilzentrische Applikationen und Nutzerschnittstellen: Das Zeitalter von Fensteroberflächen, Icons und Menüs nähert sich seinem Ende. Weboberflächen, Touchscreens und Gestenbedienung oder Sprach¬steue¬rung bestimmen das kommende Zeitalter. Applikationen werden einfacher und vielfältiger werden. Verteilte Appstores werden das klassische Rechenzentrum zumindest ergänzen. Mit Web 2.0, HTML5 und WebRTC / RTC-Web werden auch Web-Applikationen multimediafähig werden.

Cloud Computing: Wurden in 2012 noch 111 Mrd. USD für Cloud Computing ausgegeben, so wurden für 2013 schon 131 Mrd. USD geschätzt, was einem Wachstum von 18,5% entspricht (Quelle: Gartner, 02/2013). Damit hat sich der anfängliche Einsatz in 2011 zu einem deutlichen Boom vergrößert. 451 Research sieht von 2011 bis 2016 ein CAGR von 36% für Cloud Dienste (19,5 Mrd. USD Umsatz in 2016; Quelle: TheInfoPro Wave 5 Cloud Computing Study, 1. Hj. 2013).

Fortschreitende Konvergenz: Multimediaunterstützung auf vielen bis allen Endgeräten wird zum verstärkten Einsatz von Voice und Video in Kombination mit IT-Applikationen sowie zur Anreicherung aller etablierten Applikationen mit Kommunikations-Funktionen führen (Stichwort: WebRTC).

Trends im Nutzerbereich

Mobilität: Hand in Hand mit BYOD geht der Trend zur Mobilität: "Always on" ist das neue Schlagwort, und Smartphone oder Tablet machen es möglich. Auch der Laptop-Formfaktor wird immer transportabler. Mobilität wird ebenfalls neue Anforderungen an die Zugangs-Administration des Netzwerks stellen.

Multimedia: Der moderne Nutzer gibt sich nicht mehr mit PC und Telefon zufrieden. Aus dem Trend zur Mobilität wird der Trend zur mobilen Multifunktionalität: IT und UC – d.h. Daten, Kontakte, Terminkalender, Anwendungen, Voice und Video in einem Gerät und überall.

BYOD: Bring Your Own Device wird zu einer weiter erhöhten Vielfalt von Endgeräten im Netzwerk führen. Dies stellt völlig neue Herausforderungen an die Zugangs-Administration und wird die Einführung neuer Sicherheits-Konzepte bedingen.

Die genannten Trends werden mit IEEE 802.11ac und IEEE 802.11ad und den resultierenden hohen möglichen Datenraten auch auf Wireless LAN Infrastrukturen durchschlagen.

Data Center Trends

Server-Virtualisierung: Server werden zunehmend virtualisiert und somit in weiten Teilen unabhängig von der Hardware, auf der sie gerade laufen; dies beinhaltet auch Servermobilität über mehrere RZs hinweg. Im Gegensatz zur Netzwerk-Virtualisierung, die noch in den Kinderschuhen steckt, hat sich Servervirtualisierung in den letzten 3 Jahren massiv durchgesetzt: X86 Server sind inzwischen weltweit schon mit deutlich über 50% virtualisiert (451 Research TheInfoPro, 2013), über alle Server betrachtet ist die Workload schon zu 60% virtualisiert (Quantum Survey, 2013). Allerdings stießen dabei viele IT-Manager in der Umsetzung auf unerwartete Schwierigkeiten, nur 10 Prozent fanden die Umstellung problemlos (Quantum Survey, Cisco Survey, siehe auch Abbildung 1.1). Zunehmend leistungsfähigere Hardware bedingt höhere Datenraten, 10 Gbit wird Legacy Technologie zur Serveranbindung.

Extreme Datenvolumen: Größe, Format-Komplexität und Zugriffsgeschwindigkeit wachsen in einem Maß, das aktuelle Technologien und das "Single Warehouse" Paradigma an ihre Grenzen bringt. Zukünftig werden Nutzer sehr großer Unternehmen ihre Daten aus verteilten Speicherzentren abrufen.

Data- / Storage Konvergenz: SAN-Umgebungen werden zunehmend mit dem RZ-LAN integriert. FCoE hat zwar keinen echten Durchbruch erreicht, aber mit zunehmenden Datenraten (10 Gbit, 40 Gbit, 100 Gbit Ethernet) bietet iSCSI eine Alternative. Die Integration von Verkehrslasten für Speicher-Zugriffe mit Applikations- und Nutzerzugriffen stellt neue Herausforderungen an die RZ-LAN Infrastruktur. (siehe Abbildung 1.1)

Netzwerktrends

40/100 Gbit Ethernet: 1 Gbit am Endgerät ist bereits Legacy-Technologie; 10 Gbit wird Legacy-Technologie für Server, Backbone und Serverswitch-Uplinks werden schrittweise auf 40 Gbit und 100 Gbit hochgerüstet.

IoT (Internet of Things): Das Internet der Dinge (Haushalts-Zähler, Kfz-Leitsysteme, Lieferungs-Tracking etc.) wird ein Push-Faktor für IPv6 werden.

Steigender Managementbedarf: Integriertes zentrales Management für Storage, LAN und WLAN, für physische und virtuelle Ports ist die Aufgabe, die die Hersteller lösen müssen. Konfiguration, Administration und Monitoring muss zentral bereitgestellt werden. Der Trend geht vom historischen Monitoring zum Online-Monitoring, insbesondere auch mit dem Ziel eines proaktiven Managements.

2. Resultierende Anforderungen an moderne Netzwerke

Applikations-Anforderungen

Cloud Computing bedeutet hochdyna-

Netzwerk-Design in Zeiten von 10/40/100 Gbit: Wie sieht die Zukunft aus? - Teil 1

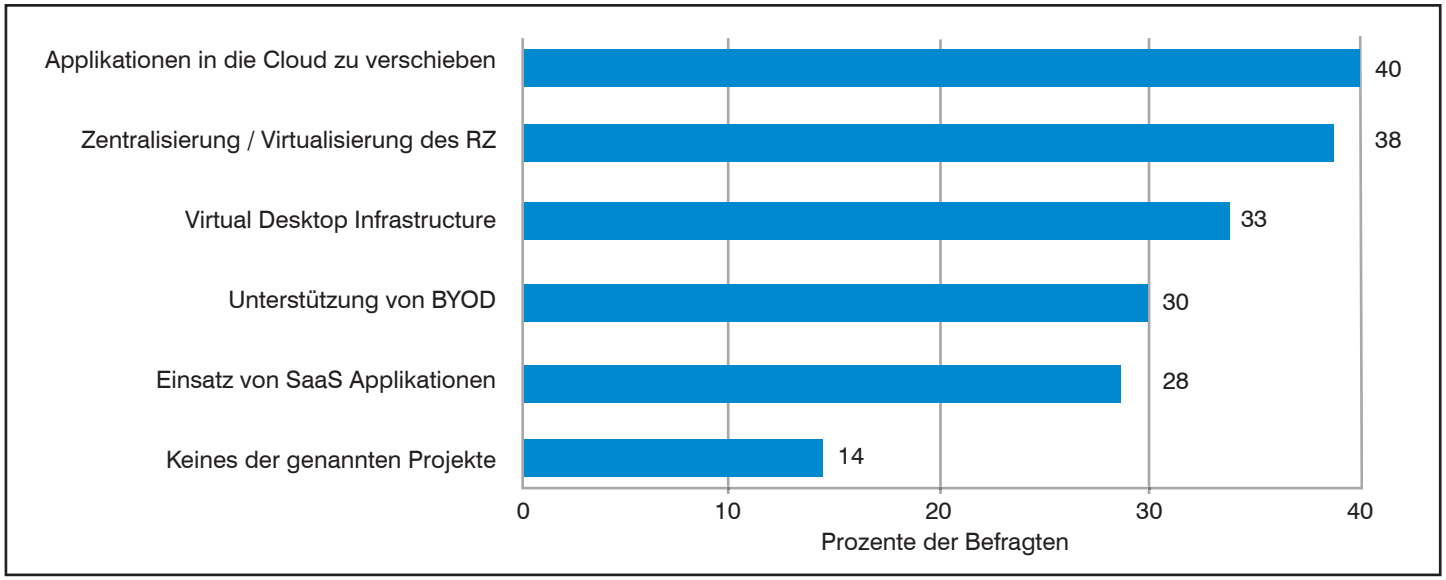


Abbildung 1.1: Welche IT Projekte brachten überdurchschnittliche Schwierigkeiten mit sich? Quelle: 2013 Cisco IT Global IT Impact Survey

mische Bereitstellung von Server- und Netzwerk-Ressourcen inklusive der hierfür notwendigen Leistungsbedingungen für Bandbreite, Delay und Verlust-Minimierung.

Gleiches gilt für Multimedia-, Web- und mobilzentrische Applikationen, die zusätzlich sehr unterschiedliche QoS-Bedarfe und variable Bandbreitenbedarfe bei Datenzugriff und Echtzeit-Video / UC generieren.

Anforderungen im Nutzer- / Access-Bereich

Mobilität verschiedenster Endgeräte wie Tablets, Laptops oder Smartphones wird die feste Zuordnung von Nutzern und Geräten zu spezifischen Netzwerkports beenden. Gleiches gilt für den immer stärkeren Einsatz von Multimedia-Endgeräten (PC, Laptop, "UC-Telefone", iPad, Android Tablet, Smartphone und weitere).

Multimedia-Fähigkeit und -Einsatz führt zu steigenden und sehr variablen Datenraten am Endgerät und am Etagen-Uplink. QoS-Zuordnung muss applikationsbezogen und nicht mehr geräte- / VLAN-bezogen erfolgen. Einer Studie von Information Week (03/2010) zufolge ist Paketverlust immer noch ein Problem in aktuellen Netzwerken: 7,5% der Uplinks von 20 untersuchten Unternehmen hatten Fehlerpakete und Input Discards. Es wurden durchschnittlich 745 Paketverluste je Interface pro Stunde gemessen. Für Hochqualitäts-Video ist dies nicht mehr akzeptabel, zumal es sich nicht immer um Einzelverluste handelt sondern bei Eingangs-Überlasten auch Burst-Verluste auftreten können.

BYOD wird ebenfalls die (von uns immer wieder kritisierte) Netzwerk-Trennung nach Gerätetypen (Telefon-VLAN, PC-VLAN, Drucker-VLAN) endgültig ad absurdum führen. Die für Mobilität und BYOD erforderlichen neuen Sicherheits-Konzepte werden auch Einfluss auf das VLAN-Design haben.

Zusammenfassend muss ein modernes Netzdesign folgende Aspekte und Anforderungen im Access Bereich berücksichtigen und abdecken:

- Mobilität, dynamische Anschaltung desselben Nutzers an wechselnden Netzwerkports
- Seiteneffekte campusweiter VLANs (Beispiel: Gast WLANs, Ethernet VLAN für Externe)
- Beseitigung des Bottlenecks zentrale Steuerung (Beispiel: WLAN VLANs)
- dynamische Bereitstellung von Ressourcen
- Bedarf nach Automatisierung
- Netzwerk Access übernimmt bisher zentrale Kontrollfunktionen
- Netzwerk Access kann beliebig Switch oder Access Point sein
- Authentisierung, NAC und QoS-Implementierung am Edge
- keine zwingende Trennung von drahtgebundener und drahtloser Kommunikation mehr "hinter" dem Access-Punkt
- Management-Integration von Wired und Wireless

Data Center Anforderungen

Die fortschreitende Server-Virtualisierung bringt eine Reihe von Herausforderungen mit sich: Dynamische Bereitstellung des Kommunikations-Kontexts (IP-Adresse, VLAN) über zwei oder mehr Data Center Standorte hinweg, dynamisch geänderte MAC-Adressen, Handhabung virtueller MAC-Adressen und virtueller serverinterner Switches, hochdynamische Verkehrslasten und Online-Überwachung dynamisch bewegter Server- und Kommunikationskontexte. Massives Tracking einer hohen Anzahl von MAC-Adressen und IP-Adressen wird erforderlich. Link Aggregierung, verteilte Link Aggregierung, NIC Teaming und Bonding müssen in Switches und Servern zueinander passend konfiguriert und überwacht werden.

Virtuelle Switches sowie gegebenenfalls auch andere virtuelle Netzkomponenten (Router, Firewalls, Loadbalancer), die auf den Hostsystemen implementiert werden, müssen netzwerktechnisch und managementseitig in die Netzwerk-Infrastruktur integriert werden.

Die Verbindung von n-Tier-Architekturen mit Sicherheits-Zonen sowie die zunehmende Server-Mobilität (z.B. vMotion) und dynamische Serverbereitstellung führt Im Rechenzentrum zu neuen Netzwerk- und VLAN-Designanforderungen.

Die Verbindungs-Infrastruktur zwischen Speichermedien und Servern wird zunehmend mit der Server-Server-Verbindungs-Infrastruktur integriert, RZ-LAN und RZ-SAN konvergieren zu einer gemeinsamen Ethernet-basierten Infrastruktur.

Vielfältige Server-Server-Verkehrsströme in Verbindung mit massiven Speicherzugriffen führen zum Bedarf nach eklatant höherer Ost-West Bandbreite und vermaschten Infrastrukturen, da Stern-strukturen hinsichtlich Delay und Leistung an den Konzentrationspunkten überlastet werden.

Zusammenfassend muss ein modernes Netzdesign folgende Aspekte und Anfor-

Netzwerk-Design in Zeiten von 10/40/100 Gbit: Wie sieht die Zukunft aus? - Teil 1

derungen im Data Center berücksichtigen und abdecken:

- Mobilität, dynamische Anschaltung desselben (Virtuellen) Servers an wechselnden Netzwerkports
- Einsatz kritischer Applikationen hinsichtlich Bandbreite und Latenzzeit
- dynamische Bereitstellung von Ressourcen
- dynamische Bereitstellung von QoS Policies und ACLs für Basis-Sicherheit auf Basis physischer Ports
- Bedarf nach Automatisierung
- Seiteneffekte RZ-übergreifender VLANs (Beispiel: HA, Cluster, Heartbeats, Management)
- 2-Tier Hierarchie anstelle einer 3-Tier oder mehr-Tier Hierarchie
- Ausdehnung von Layer-2 über DCs hinweg
- Nutzung effizienterer Schaltverfahren mit Lastverteilung zur Erreichung der Verfügbarkeitsanforderungen
- Core-Switches mit hoher bis sehr hoher Portkonzentration
- Niedrige Überbuchungsraten für DC Uplinks
- "Lossles" Ethernet, Data Center Bridging (DCB) Verfahren
- Overlay-Netze und VLANs zur Connectivity und Kontrolle der Broadcast-Domänen
- Haupt-Verkehrslast: Server – Server = Ost – West → Optimierung des Ost-West Verkehrs (Server-Server Verkehrslast)
- integriertes / konvergentes Design für Daten- und Speicherzugriff

Anforderungen im Campus-Bereich

Der Campus-Bereich stellt die Verbindungs-Infrastruktur zwischen den Gebäuden bzw. dem nutzerseitigen Access-Bereich und dem Data Center beziehungsweise den Servern und Daten bereit, das heißt er muss die Endgeräte sinnvoll und zuverlässig mit den verschiedensten Servern verbinden.

Für die Anbindung der einzelnen Gebäude ist jeweils zu entscheiden, wie über das Campus-Netzwerk einerseits eine angemessene Datenrate und Dienstgüte hinsichtlich Latenzzeit, Jitter und Verlustraten, andererseits angemessene Redundanz realisiert werden soll. Benötigt das Gebäude 10G, 40G oder 100G als Campus-Zugang? Wird es nicht-redundant, mit zwei Interfaces redundant oder mit zwei Gebäudeswitches redundant an den Campus angebunden?

Für die RZ-Anbindung wird typischerweise eine HA-Redundanz vorgesehen, da dies einer der kritischsten Netzwerk-Infrastruktur-Bereiche ist: Kein RZ-Zugang, kein Server- und Daten-Zugriff … Zu entscheiden ist jedoch, mit welcher Datenrate, respektive Überbuchung das Rechenzentrum an den Campus anzubinden ist. Dies sollte natürlich in Relation zur Summenbandbreite der Gebäude-Anschaltungen geplant werden.

Zusammenfassend muss ein modernes Netzdesign folgende Aspekte und Anforderungen im Access Bereich berücksichtigen und abdecken:

- angemessene Datenrate und Dienstgüte für die Gebäudezugänge
- angemessene Redundanz für die Gebäudezugänge
- angemessene Datenrate und Dienstgüte für die Verbindungs-Infrastruktur zwischen Gebäuden und Data Center
- angemessene Redundanz für die Verbindungs-Infrastruktur zwischen Gebäuden und Data Center
- angemessene Datenrate und Dienstgüte für den Data Center Zugang
- HA-Redundanz für den Data Center Zugang

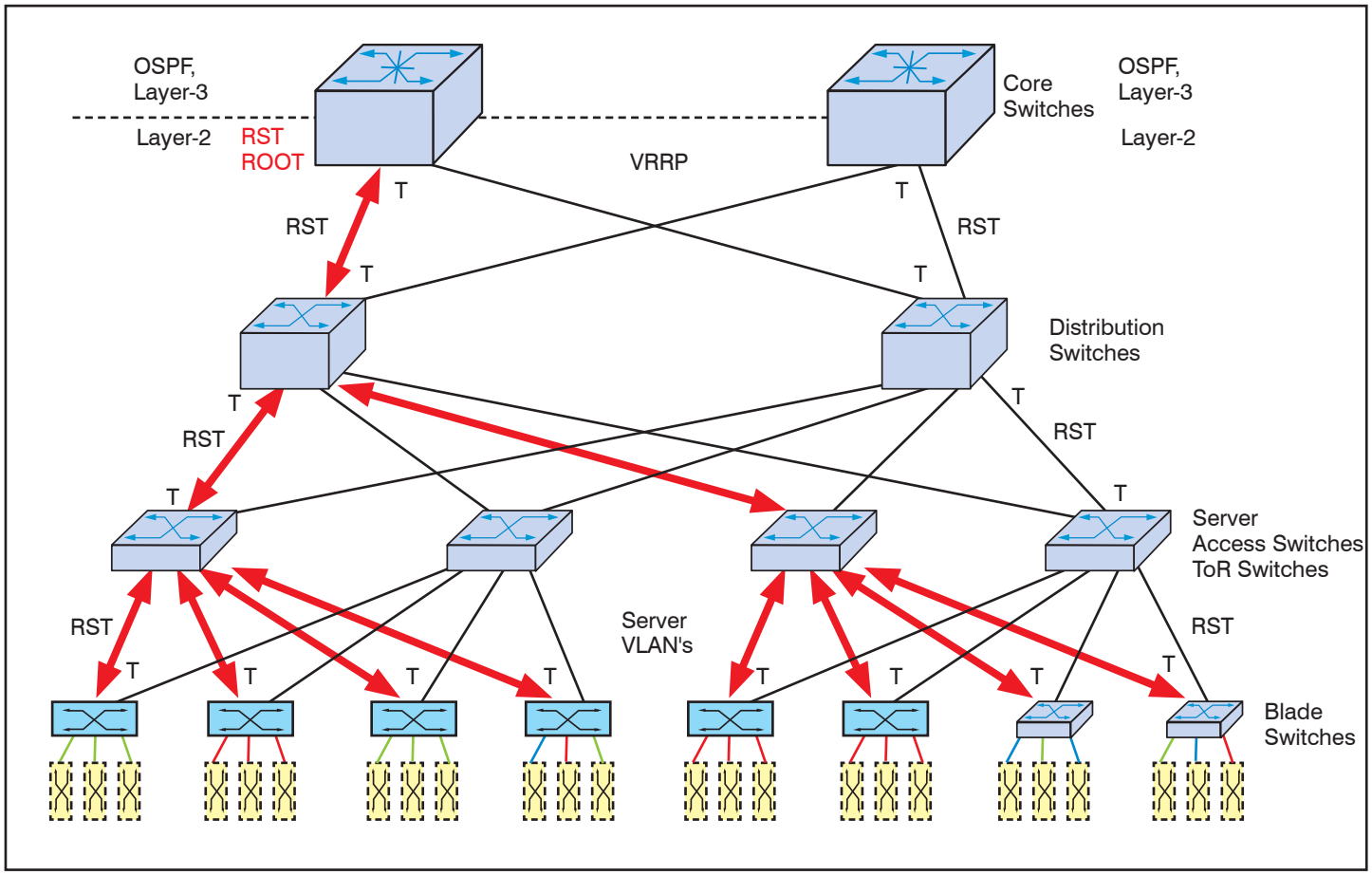


Abbildung 2.1: Nachteile von Spanning Tree Designs in großen Layer-2 Domänen

Netzwerk-Design in Zeiten von 10/40/100 Gbit: Wie sieht die Zukunft aus? - Teil 1

Fazit: Welche Designziele ändern sich, welche bleiben erhalten?

Wir halten fest: Die aktuellen Trends von IT und Kommunikation verändern das Gesicht unserer Netzwerke. Mehrere lang gehegte Design-Prinzipien lassen sich zukünftig nicht mehr ohne weiteres aufrechterhalten. Aktuelle Redesign-Überlegungen betreffen entsprechend die Designziele

- Minimierung der VLAN-Anzahl
- kleine Brodadcast-Domänen
- sternförmige Designstrukturen
- statische Provisionierung von Bandbreite und QoS
- statische IP Subnetzstrukturen
- statische NAC-Vorgaben

Die zunehmende Anwendungsvielfalt und IT-Durchdringung steigert nach wie vor die Abhängigkeit vom Netzwerk. Einige seit Jahren bekannte Anforderungen bleiben daher mit steigender Relevanz erhalten:

- Netzwerk-Skalierbarkeit
- Netzwerk-Robustheit
- Fehlerabschottung
- Fehlertoleranz
- Redundanzauslegung
- automatisierte Fehlerumschaltung
- schnelle Fehlerumschaltung
- Beherrschbarkeit des Betriebs
- Überwachbarkeit
- Sicherheit

Was ändert sich? Die etablierten Layer-2 Redundanzverfahren und resultierenden sternförmigen Strukturen sind nicht mehr zeitgerecht. Ring-Strukturen haben mit Spanning Tree hinsichtlich Durchsatz und Delay eine schlichtweg grauenhafte Leistung und kommen daher nicht zum Einsatz. Einfache Link Aggregierung hat den Totalausfall eines Switches als Single Point of Failure. Sternstrukturen führen an den zentralen Konzentrationspunkten zu potenziellen Bottlenecks, aufgrund der hohen Switchkaskaden zu erhöhten Delays und aufgrund der ungenutzten Redundanzen zu erhöhten Investkosten. Die tatsächliche Ausnutzung einer hochredundanten sternförmigen Netzwerkinfrastruktur und das resultierende Bottleneck-Risiko zeigt Abbildung 2.1.

Geroutete Ringstrukturen haben zwar eine bessere Leistung als mit Spanning Tree, sind jedoch bei campusweiten VLANs nur bedingt einsetzbar und effizient, da sie für die campusweiten VLANs mit Spanning Tree überlagert werden müssen. Wir gehen an späterer Stelle nochmals näher auf dieses Design ein.

Der Wunsch nach besserer Ressourcen-Ausnutzung sowie der Bedarf nach höherer Summen-bandbreite und ständig niedrigerem Delay führt insbesondere im Data Center Bereich zum Bedarf für verteilte und vermaschte Netzarchitekturen. Hier etablieren sich neue Technologien im Markt. Verteilte und und vermaschte Netzarchitekturen können aber auch im Access und Campus Bereich Vorteile bringen und werden sich daher langfristig auch in diesen Bereichen etablieren. Potenzielle Kandidaten sind:

- Verteilte Link Aggregierung (IRF, MC-LAG, Bonding, Virtuelles Chassis, VSS)
- Layer-2 Multipath (TRILL, SPBM)
- Fabric-Architekturen (Cisco VPC, Brocade VCS, Juniper QFabric)
- Netzwerk-Virtualisierung (SDN, OpenFlow)

Nachfolgend werden wir anhand von Design-Beispielen die Vorteile und Nachteile von Design-Elementen diskutieren, die sich aus den zuvor genannten Verfahren ergeben, und darstellen, welche Hersteller welche Technologien favorisieren.

3. Design-Elemente: Baum-/ Sternförmige Designs

Nicht nur beeinflusst durch den Spanning Tree haben sternförmige Netzwerk-Designs die letzten 20 Jahre geprägt. Auch in gerouteten Umgebungen sind sternförmige Designs oft eine leistungsstarke Alternative zur aufwändigen Vollvermaschung. Baum- oder Sternstrukturen sind übersichtlich und gut durchschaubar, was die spezifische Leistung (Datenrate) an einem bestimmten Netzwerk-Punkt betrifft. Allerdings hat eine reine Sternstruktur den Nachteil fehlender Redundanz. Trotzdem kann sie bei entsprechend moderaten Verfügbarkeitsanforderungen aus Kostengründen im Access Bereich zum Einsatz kommen: Die Endgeräte werden über nichtmodulare Access Switches sternförmig an einen Gebäude-Konzentrator (Switch) angeschaltet. Dieser hat wiederum eine Anbindung an das Campus-Netzwerk, respektive einen Core-Switch (siehe Abbildung 3.1).

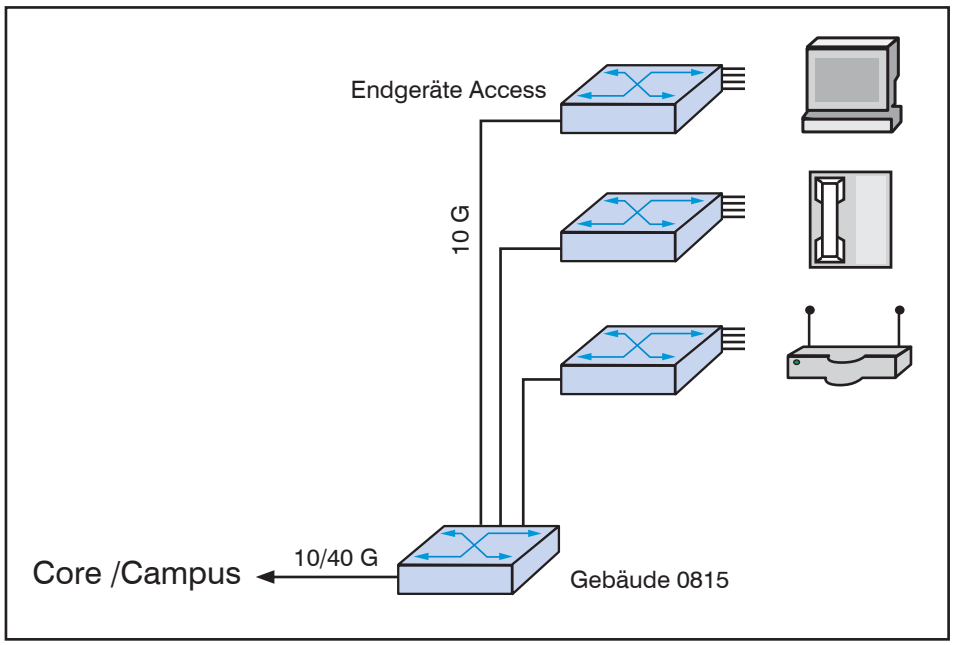


Abbildung 3.1: Sternförmiges Access Netzwerk Design

Mit zunehmender Gbit-Fähigkeit der Endgeräte migriert der Access Switch Uplink in Richtung 10 Gbit. Die sinnfällige Anbindung des Gebäude-Konzentrators an das Campus-Netzwerk ist bei mehr als 4 Access Switches dann 40 Gbit. Sind die Lasten erkennbar niedrig, kann natürlich eine Gebäude-Anbindung mit 10G oder 2-fach 10G LAG erfolgen, was die Kosten für Gebäude-Konzentrator und Core/Campus-Netzwerk deutlich senken wird. Bei entsprechender Gebäude-Größe (mehr als 250 bis 500 Endgeräte) macht es Sinn, das Gebäude mit Layer-3 vom Campus/Backbone-Netz abzukoppeln, in diesem Fall kommt im Beispiel-Szenario am Gebäude-Campus-Übergang ein Layer-3 Switch zum Einsatz.

Ein sternförmiges Data Center Design sieht im einfachsten Fall so aus wie in Abbildung 3.2 gezeigt. Aufgrund der vorherigen Überlegung, dass nicht-redundante RZ-Designs wenig sinnvoll sind, zeigt das Beispiel die vollredundante Anbindung der Server/Storage Access Switches an (mindestens) zwei Core Switches, die die Anbindung des RZ an den Campus realisieren. Unterstellen wir, dass moderne Server/Hosts mit 10 Gbit an die Server/Storage Access Swit-

ches (ToR) angeschaltet sind, so muss der Serverswitch Uplink mindestens 40 Gbit oder je nach Anzahl und Power der angeschalteten Hosts 100 Gbit erhalten.

Eine gemeinsame Ethernet-Anbindung von Server- und Storage-Komponenten ist nur dann möglich, wenn das SAN über FCoE oder iSCSI realisiert ist. Bei FCoE Einsatz zur Speicher-Anbindung müssen die Ethernet Switches dieses Verfahren unterstützen.

In Abbildung 3.2 ist deutlich erkennbar, dass der Data Center Core eine hohe Anzahl 40 Gbit oder 100 Gbit Ports benötigt, was für die Beschaffung entsprechend hohe Kosten generiert. Da die Serverseite vom Campus-Netz schon aus Sicherheits- und Fehlerabschottungs-Gründen mit Layer-3 vom Campus abgekoppelt sein sollte, zeigt auch das RZ-Designbeispiel Layer-3 Switches zur Data Center Anbindung an das Campus-Netzwerk.

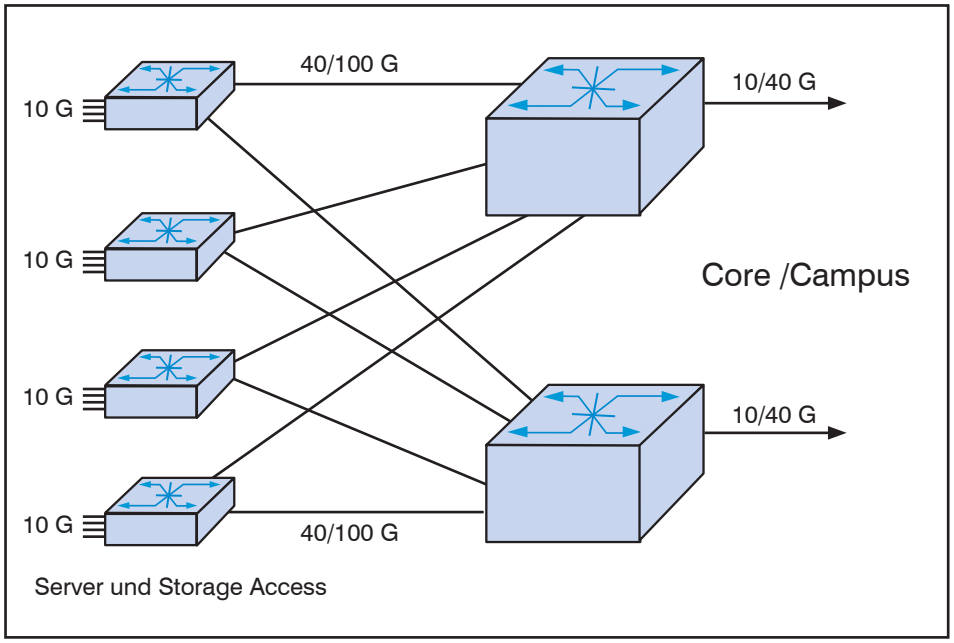


Abbildung 3.2: Sternförmiges Data Center Design

Ein resultierendes Gesamt-Design zeigt Abbildung 3.3. Je nach Größe des Netzwerks hinsichtlich Server- und Gebäude-Anzahl werden zwei Core / Campus-Switches nicht mehr ausreichend sein. Die erste Maßnahme ist dann vielfach eine Aufteilung in RZ-Core und Campus-

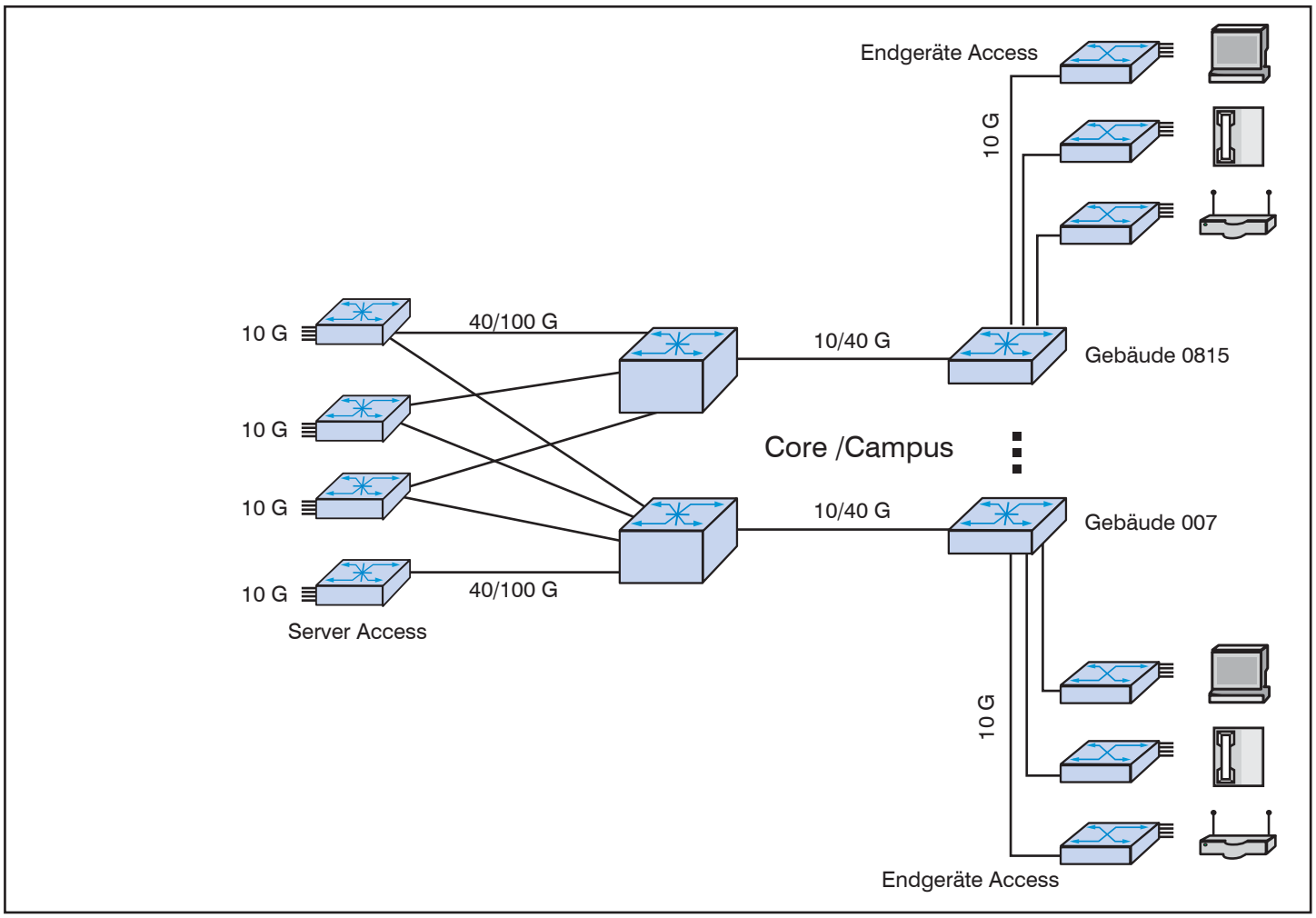


Abbildung 3.3: Sternförmiges Gesamt-Design

Netzwerk-Design in Zeiten von 10/40/100 Gbit: Wie sieht die Zukunft aus? - Teil 1

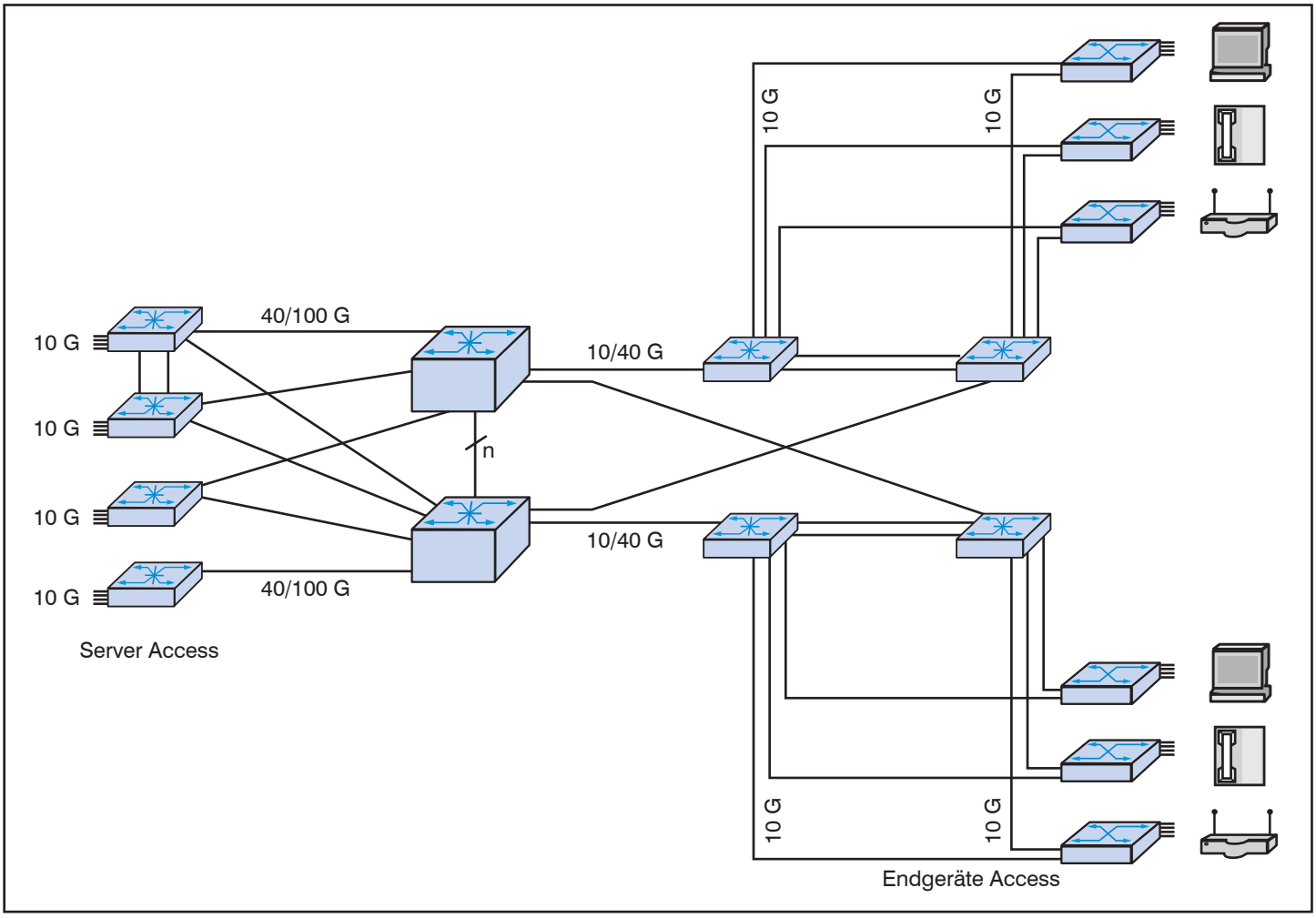


Abbildung 3.4: Sternförmiges vollredundantes Gesamt-Design

Core Switches, die wiederum mit angemessen hohen Datenraten miteinander verbunden werden müssen. Für die gezeigten Access und RZ-Beispiele kann hier sinnfälligerweise nur n-mal 40 Gbit oder 100 Gbit zum Einsatz kommen. Bei sehr großen Geländenetzwerken lässt sich eine weitere Konzentrator-Stufe einfügen, die im Regelfall dann die Überbuchung zwischen Gebäude-Summenlast und RZ erhöht. Mehrere Gebäude werden in Bereichs-Netzen (Areal-Netzen) gebündelt, die Areal-Netze werden über Core-Konzentratoren gebündelt. Ein Beispiel-Szenario mit einer Kaskadentiefe von 6 zeigt Abbildung 3.5. Für ein solches n-Tier Design ist natürlich eine entsprechende Geländeverkabelung erforderlich.

Höhere Verfügbarkeits-Anforderungen für einzelne oder alle Gebäude erfordern ein redundantes Design, bei dem zumindest jedes Gebäude vom Gebäude-Konzentrator aus an zwei Core / Campus Switches angeschaltet wird, um den RZ-Zugang sicher zu stellen, falls ein Campus / Core Switch ausfällt. Ob der Gebäude-Campus-Zugang mit zwei Gebäude-Konzentratoren ebenfalls vollredundant ausgelegt werden muss, ist im Einzelfall zu entscheiden. Typischerweise spielt hier die Gebäudegröße (hinsichtlich Anzahl angebundener Anschlüsse) sowie Wichtigkeit der dort betriebenen Anwendungen respektive angebundenen Anwender

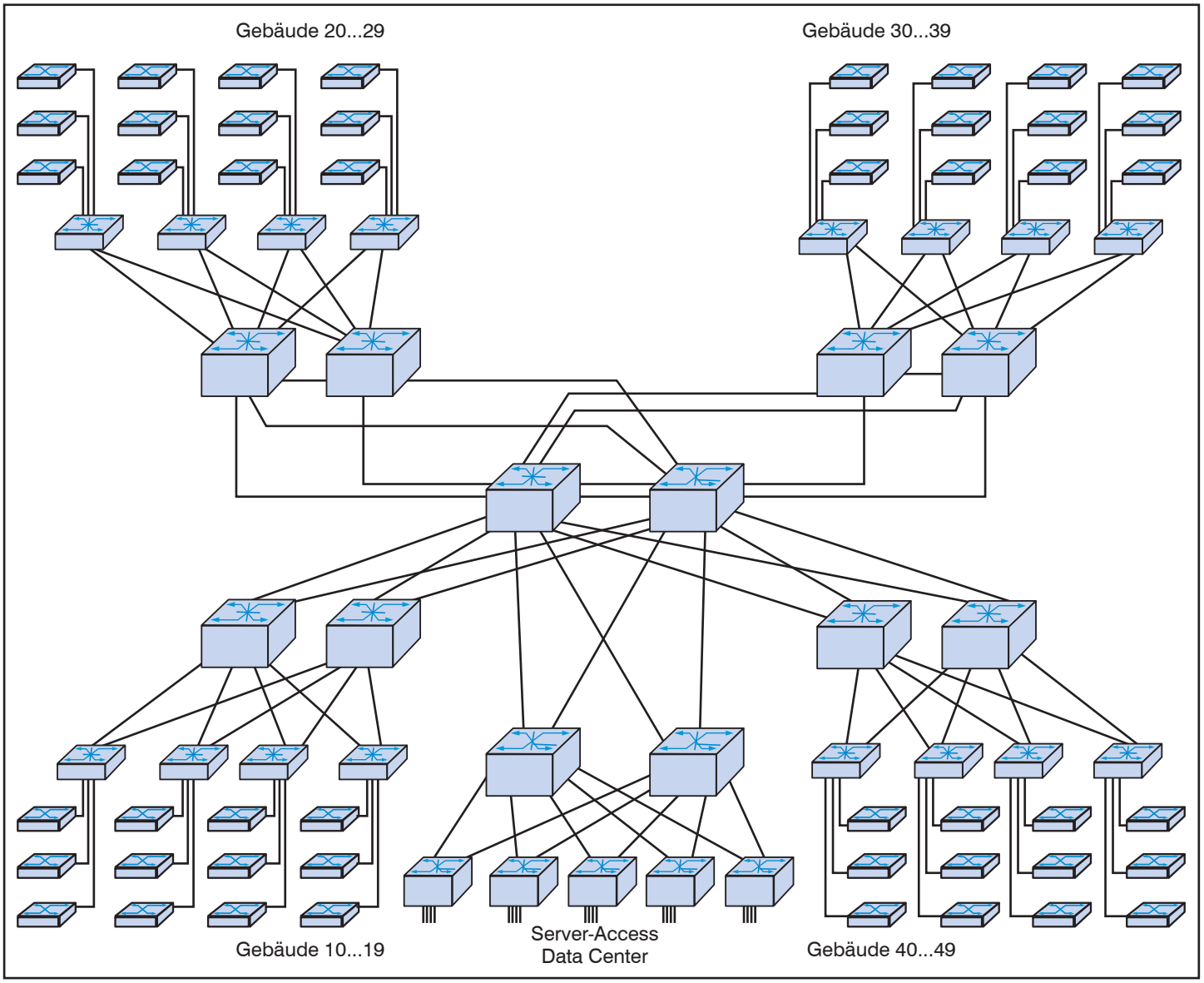


Abbildung 3.5: Sternförmiges 6-Tier Gesamt-Design

eine Rolle. Sofern die maximale Wiederherstellungszeit unter 1,5 bis 2 Stunden liegen soll, empfiehlt sich eine vollredundante Bestückung der Gebäude-Campus-Anbindung mit zwei Gebäude-Konzentratoren. Dieses vollredundante Stern-Design ist in Abbildung 3.4 gezeigt. Bei Betrachtung der Grafik wird sofort klar, dass dieses Design sowohl hohe Datenraten als auch hohe Verfügbarkeit bereitstellt, jedoch auch eine hohe Anzahl an 10/40/100Gbit Interfaces und LWL-Fasern erfordert. Ringförmige oder sternförmige Trassenführung im Gelände spielt hier eine untergeordnete Rolle, da sich auch über eine ringförmige Trasse sternförmige Patchungen vornehmen lassen.

In Abbildung 3.6 ist eine Bewertungsübersicht von Stern-Designs dargestellt.

Mehrfach-Stern: Fat Tree Design

Fat Tree Designs kommen typischerweise im Data Center zum Einsatz, da sie darauf optimiert sind, eine maximale Durchsatzleistung und minimale Kaskade zwischen zwei Endpunkten zu realisieren. Wie der Name schon sagt, ist das Design ein "in die Breite gezogener" Mehrfach-Baum, der die Leistung eines einzelnen Baumes einfach vervielfältigt. Dies ist im Gelände sowohl aufgrund der benötigten Anzahl Interfaces als auch insbesondere verkabelungstechnisch meistens viel zu aufwändig sprich: unbezahlbar teuer. Während im Gelände bei sehr hoher Gebäudezahl mehr Konzentrator-Ebenen installiert werden (3-Tier oder 4-Tier), wird im RZ der Stern oder hier besser Baum in die Breite vervielfältigt.

Das Beispiel aus Abbildung 3.7 zeigt einen Fat Tree mit 4-fach Stern beziehungsweise vier Core Switches, die mit jeweils 160 Gbit Summenleistung eine beliebige Server-Server- oder Server-Storage-Verbindung mit einer Kaskade von zwei Hops ermöglichen. Ein zweiter Blick auf das Fat Tree Design zeigt, dass hier auf keinen Fall Spanning Tree zum Einsatz kommen kann, da dieser drei von vier Verbindungen für den Datenverkehr abschalten würde! Fat Tree Designs arbeiten auf der Basis von Multi-Chassis Link Aggregierung, Layer-2 Multipath Verfahren wie TRILL oder SPBM oder proprietäre Varianten der Layer-2 Multipath Verfahren.

Eine gemeinsame Ethernet-Anbindung von Server- und Speicher-Komponenten ist nur dann möglich, wenn das SAN über FCoE oder iSCSI realisiert ist. Bei FCoE

Netzwerk-Design in Zeiten von 10/40/100 Gbit: Wie sieht die Zukunft aus? - Teil 1

Stern-Design					
Gebäude-/ Access-Netzwerk		**Campus-Netzwerk**		**Data Center Netzwerk**	
Gesamtleistung	++	Gesamtleistung	++	Gesamtleistung	+
dynamische Bereitstellung von Ressourcen und VLANs	++	Skalierbarkeit	++	Konfigurations-Flexibilität, Skalierbarkeit	+
Seiteneffekte campusweiter VLANs	++	Flexible Subnetzbildung	++	Flexible Server-Positionierung und Subnetzbildung	++
Verfügbarkeit, Redundanz	+/-	Verfügbarkeit, Redundanz	+	Lasteffizienz (Lastverteilung, unterstützte Hashverfahren, Anzahl ECMPs)	+
		Trennung von Fehlerdomänen, Fehlereingrenzung	++	Nutzung von Standards	+
Größe des Single Point of Failure	+	Größe des Single Point of Failure	+	Größe des Single Point of Failure	++
Sicherheit, Zugangsschutz	+	Sicherheit, Zugangsschutz	+	Sicherheit, Zugangsschutz	+
Optimierung der Betriebskomplexität	+	Optimierung der Betriebskomplexität	+	Optimierung der Betriebskomplexität	+
Infrastruktur-Bedarf	+/-	Infrastruktur-Bedarf	+/-	Infrastruktur-Bedarf	+/-
Investitions-Kosten	-	Investitions-Kosten	-	Investitions-Kosten	-
				Durchgängigkeit der Produktlinien für Data Center und Campus	+
				Integration des Speicherzugriffs / SAN	+
				Unterstützung von Server-Virtualisierung	+
				Unterstützung aller gängigen Hypervisoren	+

Abbildung 3.6: Bewertung von Stern-Designs

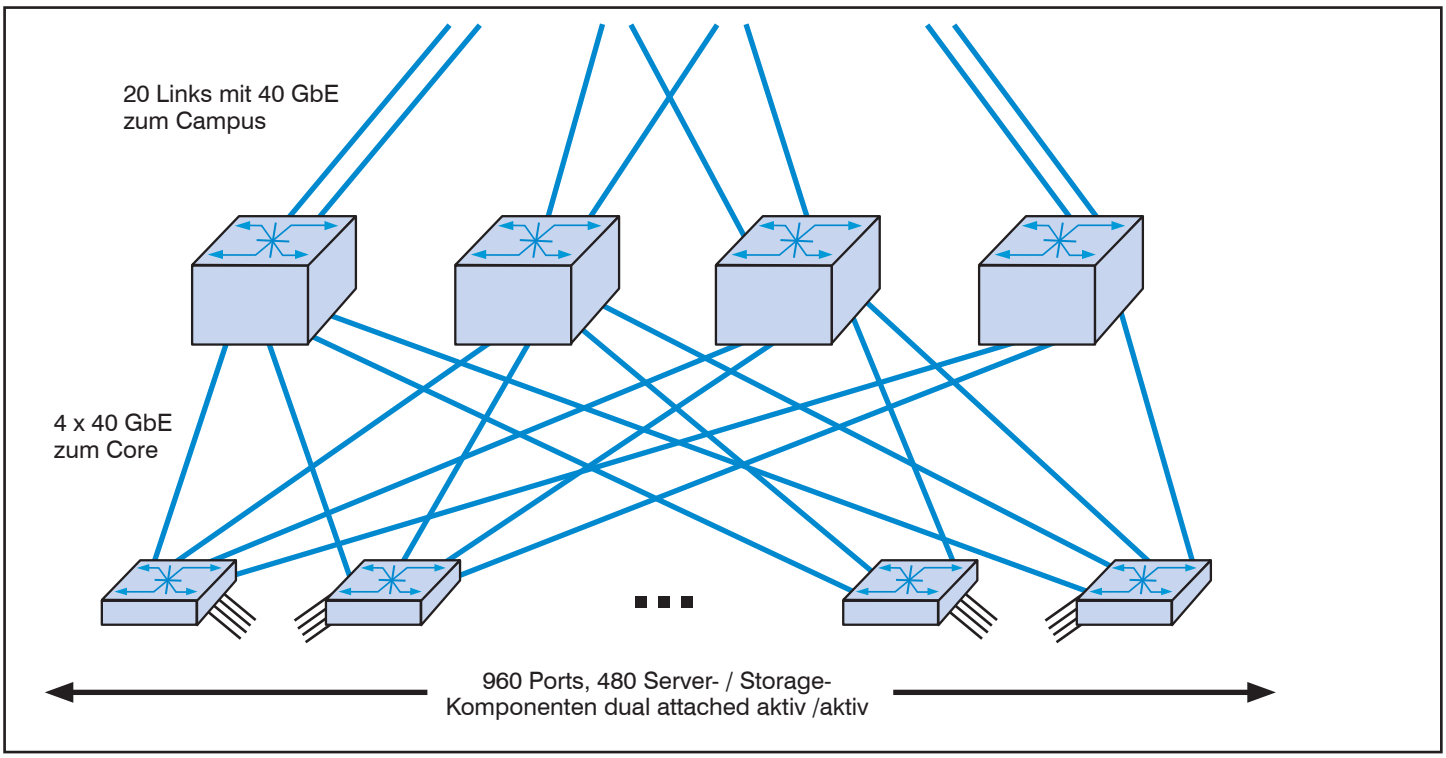


Abbildung 3.7: Fat Tree Data Center Design mit 4-fach Baum

Netzwerk-Design in Zeiten von 10/40/100 Gbit: Wie sieht die Zukunft aus? - Teil 1

Fat Tree Design	
Data Center Netzwerk	
Gesamtleistung	++
Konfigurations-Felxibilität, Skalierbarkeit	++
Flexible Server-Positionierung und Subnetzbildung	++
Lasteffizienz (Lastverteilung, unterstützte Hashverfahren, Anzahl ECMPs)	++
Nutzung von Standards	+/-
Größe des Single Point of Failure	++
Sicherheit, Zugangsschutz	+
Optimierung der Betriebskomplexität	+/-
Infrastruktur-Bedarf	-
Investitions-Kosten	-
Durchgängigkeit der Produktlinien für Data Center und Campus	+
Integration des Speicherzugriffs /SAN	+
Unterstützung von Server-Virtualisierung	+
Unterstützung aller gängigen Hypervisoren	+

Abbildung 3.8: Bewertung des Fat Tree Designs

Einsatz zur Speicher-Anbindung müssen die Ethernet Switches dieses Verfahren unterstützen.

In Abbildung 3.8 ist eine Bewertungsübersicht des Fat Tree Designs dargestellt.

Stern-Designs sind hinsichtlich Durchsatz-Leistung leicht kalkulierbar, kosten jedoch vergleichsweise viele Switch-Interfaces und erfordern vielfach den Einsatz modularer das heißt teurerer Konzentrator-Komponenten.

Im nächsten Teil lesen Sie:
- Design-Elemente: Ringförmige Designs
- Design-Elemente: Maschen, Hybrid-Designs
- Einbindung virtueller Netzkomponenten
- Design-Regeln, Generischer Planungs-Ansatz
- Wo kommt welches Failover-Verfahren zum Einsatz?

Abkürzungen

ACL	Access Control List(e)
BYOD	Bring Your Own Device
CAGR	Compound Annual Growth Rate
CPU	Central Processing Unit
DC	Data Center
DCB	Data Center Bridging
FCoE	Fibre Channel over Ethernet
FDDI	Fiber Distributed Data Interface
HA	High Availiable
HTML	Hypertext Markup Language
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Internet Protocol
IRF	Intelligent Resilient Framework (HP)
iSCSI	internet Small Computer System Interface
IT	Informations-Technologie
L2/L3	Layer-2/ Layer-3
LAG	Link Aggregation Group (IEEE 802.3ad)
LAN	Local Area Network
LWL	Lichtwellenleiter
MAC	Media Access Control
MC-LAG	Multi-Chassis Link Aggregation Group
MRP	Metro Ring Protocol
NAC	Network Access Control
NIC	Network Interface Card (Coupler)
OSPF	Open Shortest Path First
PC	Personal Computer
QoS	Quality of Service
RTC-Web	Real-Time Communication - Web
RZ	Rechenzentrum
SAN	Storage Area Network
SDN	Software-Defined Networking
SPB	Shortest Path Bridging
SPBM	Shortest Path Bridging MAC
ToR	Top-of-Rack
TRILL	TRansparent Interconnection of Lots of Links
UC	Unified Communications
VCS	Virtual Cluster Switching (Brocade)
VLAN	Virtual Local Area Network
VM	Virtual Machine
VPC	Virtual Port Channel (Cisco)
VSS	Virtual Switching System
WLAN	Wireless LAN

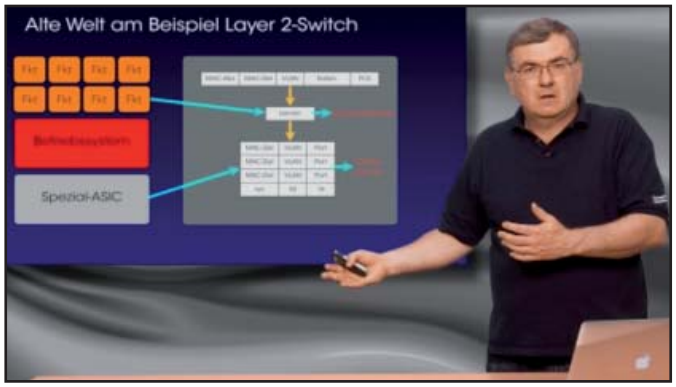
ComConsult-Study.tv

SDN-Spezial im Februar bei ComConsult-Study.tv

Software Definied Networking (SDN) scheint aktuell in aller Munde. Ist er der Gral der Netzwerktechnik oder nur wieder ein Hype? In diesem Paket haben wir vier Videos zusammengestellt, die SDN von verschiedenen Seiten beleuchten:

- Was ist SDN?
- Wie funktioniert es?
- Wie positionieren sich die Hersteller am Beispiel von Cisco?

Zum Einstieg empfiehlt sich "SDN in 10 Minuten". Dieses Video fasst kurz und knapp die Wesensmerkmale von SDN zusammen. Das Video ist kostenfrei und kann auch ohne Erwerb des Paketes gesehen werden.

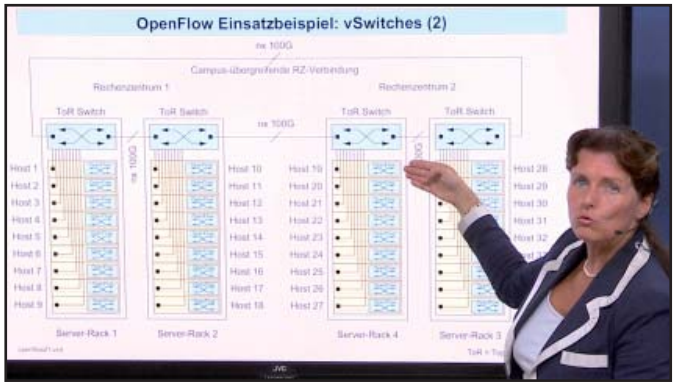


SDN in 10 Minuten
Referent: **Dr. Jürgen Suppan**
Zeit: 00:12:12 Einzelpreis: kostenlos

Ist SDN wichtig oder nicht? Vor dieser Frage stehen im Moment fast alle Betreiber größerer Netze. Keine andere Technologie kann und wird die Zukunft der Netzwerke so bestimmen und verändern wie SDN. Dieses Video erklärt in sehr kurzer Form worum es bei SDN geht und gibt Ihnen Hilfe bei der Entscheidung, ob Sie sich mit dem Thema befassen sollten oder nicht.

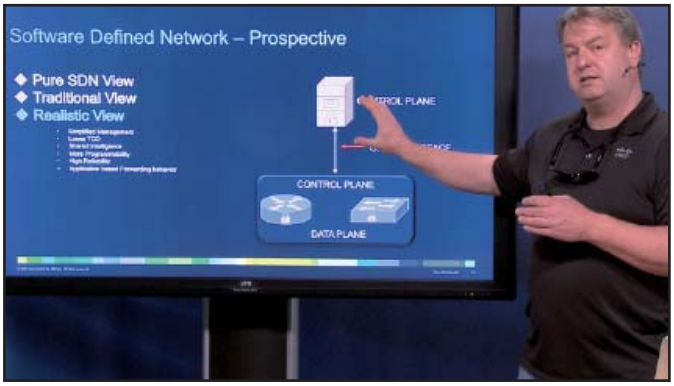
Analyse: Software Defined Networking SDN
Referent: **Dr. Jürgen Suppan**
Zeit: 00:36:34 Einzelpreis: kostenlos

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.



Software Defined Networking SDN in der technischen Analyse
Referent: **Dipl.-Inform. Petra Borowka-Gatzweiler**
Zeit: 01:22:06 gesamt Einzelpreis: 59,00 € netto
Im Abo: kostenlos

SDN ist die Basis für die nächste Generation von Netzwerken. Es schafft neue Möglichkeiten mit einem erheblichen Zuwachs an Dynamik und Flexibilität. SDN ist gleichzeitig ein zentrales Element für das Software Defined Data Center. Das völlig neue



Software Defined Networking SDN: ... the Cisco Way
Referent: **Gerd Pflüger** Einzelpreis: 49,00 € netto
Zeit: 00:36:05 Im Abo: kostenlos

SDN ist im Moment der Mega-Hype im Netzwerk-Bereich. Einige Hersteller investieren enorm hohe Summen, um sich im Kampf um das Netzwerk der Zukunft ganz vorne zu positionieren. Gerd Pflueger analysiert in diesem sehr empfehlenswerten Video was SDN ist und wie Cisco dazu steht.

Das Bundle bestehend aus den vier Videos für nur € 75,60*

*Dieses Angebot gilt nur im Februar 2014 .- Regulärer Preis € 108,-- netto

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

Report Neuerscheinung

100 G: Technologie und Standards

Im März 2014 erscheint bei ComConsult Research der neue Report "100 G: Technologie und Standards" von Dr. Franz-Joachim Kauffels.

Dieser Report bietet Ihnen einen umfassenden Überblick über Technologie und Standards der nächsten Ethernet Evolutionsstufe und gibt Ihnen wertvolles Grundlagenwissen für zukünftige Planungen und Entwicklungen in allen Netzwerk-Kategorien mit dem Schwerpunkt RZ.

Die Anforderungen z.B. an ein RZ-Netz wachsen nicht wie gewohnt kontinuierlich, sondern schlagartig. Es ist deutlich zu sehen, dass RZ-Netze konventioneller Bauart diesen Anforderungen in vielen Fällen nicht wirklich gewachsen sein werden. Die Skalierbarkeit ist einfach nicht ausreichend.

Dies ist niemandem anzulasten. Auch nach bisherigem Kenntnisstand sorgfältig geplante und aufgebaute Netze können es nicht verkraften, wenn sie im Zeitraum weniger Monate das Drei- bis Zehnfache leisten sollen. Dafür ist schon die Basistechnologie nicht ausgelegt.

Nicht nur die Planer und Betreiber, sondern auch die Standardisierung und die Hersteller kommen bei diesem Entwicklungstempo an ihre Grenzen. Es ist zu befürchten, dass selbst mit der Lösung des Problems der leistungsfähigen Serveranbindung und der Einführung eines wirkungsvollen und schnellen Strukturverfahrens keine wirkliche Ruhe eintreten wird. Dafür gibt es viel zu viele Entwicklungen, die sich jetzt in einer Phase befinden, die unmittelbar vor der möglichen Ausbreitung in der Fläche stehen, vor allem bedingt durch Trends wie BYOD und Mobilität, neue virtualisierte Speichersysteme oder Kooperation zwischen privaten und öffentlichen Clouds.

Es gibt eine wieder aufgeflammte Diskussion über „Anwendungs-bewusste“ Netze. Sie entsteht immer dann, wenn die Hersteller die eigentlich notwendige nächste Leistungsstufe noch nicht in gewünschtem Preis/Leistungsverhältnis liefern können und den Mangel durch irgendwelche Software-Mechanismen verdecken wollen. Tatsache ist, dass jedwedes Qualitäts- oder Priorisierungs-Merkmal letztlich durch eine technische Grundqualität (Übertragungsrate, Latenz, Jitter ...) hinterlegt sein muss.

Cisco hat bereits 100 G-Komponenten für den Einsatz im RZ vorgestellt, andere Hersteller werden schnell folgen. „100-G-ready“ Switches gibt es ja schon lange. Erfahrungsgemäß legen sich die Qualitätsdiskussionen, wenn eine neue Leistungs-Stufe verfügbar ist.

Auch wenn RZ-Betreiber aktuell noch keine Notwendigkeit für den Einsatz von 100 G sehen, sollten sie sich mit der Technik befassen, denn hier ist Einiges anders als bei den langsameren Übertragungsverfahren. Das liegt nicht nur an der rein optischen Übertragungstechnik, sondern auch am komplexen Zusammenwirken optischer und in VLSI-Technik ausgelegter physikalischer Komponenten.

Ein weiterer, ganz wesentlicher Punkt ist, dass 100G-Varianten sowohl für Provider als auch für den Einsatz auf Kurzstrecken (im RZ) bereits seit einigen Jahren vollständig standardisiert sind und dadurch auch ihr Zusammenwirken, z.B. im Zusammenhang mit einer RZ-Fernkopplung, erleichtert wird.

Deshalb stellt dieser Report Technologie und Standards von 100 G ausführlich vor.

Fax-Antwort an ComConsult 02408/955-399

Bestellung

100 G: Technologie und Standards

☐ Ich bestelle den Report
100 G: Technologie und Standards
zum Preis von € 398,-- netto
zzgl. Versandkosten

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

Bestellen Sie über auch über
www.comconsult-research.de

Das Wissensportal

Das Wissensportal

Auf dem Wissensportal finden Sie eine bunte Mischung aus aktuellen Informationen, persönlichen Meinungen und ausführlichen Grundlagen-Artikeln über die gesamte Themenpalette der IT- und Netzwerkwelt. Die Artikel des ComConsult Wissensportals geben Ihnen die Möglichkeit der Stellungnahme, des Kommentars oder der Diskussion mit anderen Lesern. Nutzen Sie diese Gelegenheit, die Sichtweise anderer Spezialisten zu erfahren.

Verschlüsselungswahn

5. Februar 2014 von Markus Schaub

Experten sagen uns, wir müssen verschlüsseln. Das sagen sie nicht erst seit dem NSA-Skandal. Und weil wir brav sind, verschlüsseln wir auch was das Zeug hält. Nehmen wir mal als Beispiel eine Email, die ich von meinem Homeoffice aus an einen Mitarbeiter einer anderen Firma sende, der sie mit seinem Smartphone liest.

Kompletten Artikel lesen unter www.comconsult-research.de

Die Zukunft von TCP hat begonnen

29. Januar 2014 von Markus Schaub

Die Belgier haben es und Apple kann es auch: MPTCP.

Überall scheint sich die IT-Welt weiter zu entwickeln, so auch im Netzwerk. Ethernet wurde immer schneller; aus dem Spanning Tree wurde über Zwischenstationen TRILL und SPB; selbst der Dinosaurier IPv4 wankt und weicht langsam der Version 6. TCP scheint das alles nicht zu berühren. Und doch passiert dort gerade etwas wirklich Spannendes: Multipath TCP, kurz MPTCP.

Kompletten Artikel lesen unter www.comconsult-research.de

Die Rolle von Ethernet Fabrics in virtualisierten Umgebungen

27. Januar 2014 von Cornelius Höchel-Winter

Der aktuelle Gartner Report „Emergence of Ethernet Fabric Will Push Users to Rethink Their Data Center Physical Switch Networks“ (16. Okt. 2013) beginnt mit dem Satz, Netzwerk-Profis sollten sich (endlich) auf den Weg zu höherer Effizienz und Automatisierung in ihren RZ-Netzen machen, und kommt schließlich zu dem Schluss, dass Netzwerke in Rechenzentren mit Ethernet Fabrics besser als mit allen anderen Optionen vereinfacht und automatisiert werden können.

Kompletten Artikel lesen unter www.comconsult-research.de

VoIP-Sicherheit ist immer noch von Bedeutung

3. Februar 2014 von Markus Geller

Sicherheit ist sicher nicht die erste Sache, die einem bei VoIP in den Sinn kommt, aber Sie sollte doch einen der führenden Plätze bei der Realisierung einnehmen, da man sich sonst einem erheblichen Risiko aussetzt.

Kompletten Artikel lesen unter www.comconsult-research.de

Das Tischtelefon muss schnurlos werden

20. Januar 2014 von Markus Geller

Nachdem ich in der vergangenen Woche die Totenglocke für das klassische Tischtelefon geläutet habe, möchte ich jetzt ein weiteres kontrovers diskutiertes Thema aufgreifen: VoIP (SIP) over WLAN oder auch VoWLAN genannt.

Kompletten Artikel lesen unter www.comconsult-research.de

Das ewige Dilemma: Architekten planen ungeeignete IT-Verteilerräume

17. Januar 2014 von Hartmut Kell

Die richtige Planung eines Technikraumes in einem Neubau, der zur Unterbringung von passiven und insbesondere aktiven Komponenten der IT-Kommunikation genutzt werden kann und dauerhaft den Betrieb des Netzwerkes einfach gestaltet, beginnt in einer sehr frühen Phase, häufig bereits bevor die den Raum nutzende IT-Abteilung intensiv in die Planung der passiven IT-Infrastruktur involviert wird. Denn eine ganze entscheidende Prägung der Nutzungsqualität entsteht durch die Planung des Architekten, gerade bei der Festlegung der Lage und der Größe des Technikraumes. Viele Erfahrungen aus unterschiedlichen Projekten zeigen, dass teilweise absurde Vorstellungen der beim Architekten mit der Grundrissplanung beauftragten Planer zur Art der Nutzung der IT-Technikräume oder der notwendigen Ausbaubarkeit herrschen.

Kompletten Artikel lesen unter www.comconsult-research.de

Standpunkt Sicherheit

Überwachung ist und bleibt der wesentliche Business Case des Internet

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

In einem höchst interessanten bei Spiegel Online veröffentlichten Interview[1] hat der international anerkannte Sicherheitsexperte Bruce Schneier in einem einzigen kurzen Satz unser Dilemma mit dem Internet wunderbar zusammengefasst: „Überwachung ist das Geschäftsmodell des Internet".

Dieses Statement hat zwei Seiten:

- Jegliche Kommunikation im Internet wird irgendwo überwacht, aufgezeichnet, hinsichtlich eines Nutzwerts analysiert, mit anderer Kommunikation korreliert, statistisch analysiert und zu Kenngrößen verdichtet. Google, NSA und Co. sind hier nicht alleine. Für z.B. Google und Amazon ist die Überwachung ein fundamentales Geschäftsmodell. Die NSA ist hier eigentlich nur das Beispiel eines ausgesprochen lästigen Parasiten, der sich von den Daten ernährt, die Google, Amazon und Co. erfassen. Auch verschlüsselte Kommunikation ist natürlich davon betroffen. Wenn das Verschlüsselungsverfahren oder das Schlüsselmanagement Schwachstellen haben, ist klar, NSA oder andere vergleichbare Institutionen lauschen mit. Darüber hinaus sind aber die Metadaten oft viel interessanter. Wer wann und wo kommuniziert, ist ausgesprochen spannend.

- Wenn wir die Überwachbarkeit des Internet ändern wollen, müssten wir uns damit abfinden, dass wir auch den grundsätzlichen Charakter des Internet zu etwas anderem wandeln, in dem Google, Facebook und viele andere kostenfreie Dienste nicht mehr wie bisher möglich sind.

Die Frage ist tatsächlich, was wir wollen, und zwar als Bürger, Unternehmen und Behörden. Der Ruf nach einem eigenen „sichereren" Europa- oder sogar Deutschland-Internet ist längst schon laut geworden und verschiedenste Gruppen arbeiten an Vorschlägen für ein sicheres Internet. Wir benötigen nämlich scheinbar eine Quadratur des Kreises: Wir wollen das Internet, so wie es ist, aber ohne NSA und andere Parasiten. Nur ist das nicht möglich. Wir müssen, wie im realen Leben, leider auch unseren Lebensraum mit Lebewesen teilen, die uns nicht immer wohl gesonnen sind und trotzdem eine Daseinsberechtigung haben.

Nichts tun wäre jedenfalls mehr als fahrlässig. Deutsche Unternehmen sind beispielsweise wesentlich stärker dem Risiko der systematischen Industriespionage ausgesetzt, als in der Vergangenheit angenommen. So trivial es klingt: Wenn sich eine Risikoeinschätzung ändert und ein Risiko erheblich zunimmt, müssen wir uns entsprechend stärker schützen. Die Schrauben der Informationssicherheit sind dabei in allen Bereichen notgedrungen stärker anzuziehen, was automatisch auch Einschränkungen lieb gewonnener Freiheiten der Endnutzer bedingt:

- **Eigene Überwachung und Kontrolle verstärken:** Die eigene Überwachung und Kontrolle des Kommunikationsverkehrs ist und bleibt ein wesentliches Instrument gegen externe Überwachungs- und Lauschangriffe. Hier sind nicht nur die klassischen Firewall-, IPS und Content-Security-Konzepte zu betrachten. Wichtig sind z.B. die Bewertung der Vertrauenswürdigkeit von Kommunikationszielen und die übergreifende Korrelation von Merkmalen des Kommunikationsverkehrs, die auf Anomalien hinweisen. Die strikte Kapselung kritischer Systeme und die konsequente Kontrolle der Kommunikation zu solchen Systemen in sogenannten Zonenkonzepten gehört zwar seit Jahren zum elementaren Rüstzeug der Informationssicherheit, der damit verbundene Aufwand für die entsprechenden internen Firewall-Infrastrukturen ist aber oft gescheut worden. Eine nicht zonierte Infrastruktur (Rechenzentrum und ggf. auch Campus) ist jedoch Stand heute nicht mehr zeitgemäß.

- **Stärkere Kapselung von Web-Surfen und E-Mail:** Sicherer Web-Zugriff und sichere E-Mail bleiben ein Kernthema, da hier zentrale Infektionspfade und Möglichkeiten des unerwünschten Datenabflusses bestehen. Konzepte der Kapselung von Web-Surfen und E-Mail, sind zwar für den Nutzer mit erheblichen Einschränkungen verbunden, müssen jedoch stärker in Betracht gezogen werden.

- **Stärkung der Endgerätesicherheit:** Hier geht es um klassische Themen wie Schutz vor schadenstiftender Software, Härtung, konsequentes Patch-Management und strikte Berechtigungskonzepte. Eine wesentliche Lehre, die wir aus den Snowden-Veröffentlichungen ziehen müssen ist, dass schadenstiftende Lauschsoftware (z.B. Trojaner) für Endgeräte seit Jahren in einem erschreckenden Umfang und dabei höchst professionell, mit bester Qualität und fast grenzenlosen Budget hergestellt wird und zum Einsatz kommt.

- **Konsequente Kontrolle und Härtung mobiler Endgeräte:** Der Schutz mobiler Endgeräte, insbesondere Smartphones und Tablets, ist dabei von besonderer Bedeutung. Bring Your Own Device (BYOD) muss dabei weitgehend auf der Strecke bleiben, da das Erzwingen von Policies ein striktes Mobile Device Management (MDM) erfordert, das nur mit Company Owned Devices in dem notwendigen Umfang möglich ist. Eine private Nutzung mobiler Endgeräte wird jedoch kaum sinnvoll einschränkbar sein. Daher sind hier Techniken auf Ebene der mobilen Betriebssysteme, insbesondere Verschlüsselungs- und

[1] Siehe http://www.spiegel.de/netzwelt/netzpolitik/bruce-schneier-im-interview-die-nsa-schadet-den-usaa-944413.html

Überwachung ist und bleibt der wesentliche Business Case des Internet

Virtualisierungstechniken zur Trennung privater und dienstlicher Bereiche essentiell.

- **„Raus aus der Cloud“:** Public Clouds und externe Private Clouds, die nicht auf dedizierter durch den Nutzer überwach- und auditierbarer Infrastruktur realisiert oder entsprechend zertifiziert sind, muss mit erheblicher Zurückhaltung begegnet werden. Wer nicht wirklich zusichern kann, dass in einer solchen Cloud keine Daten landen, die dort nicht hingehören, sollte eher davon Abstand nehmen. Dies gilt speziell auch für MDM-Lösungen aus der Cloud.

- **Konsequente Verschlüsselung auf allen externen Kommunikationsverbindungen:** Sich auf das Internet zu konzentrieren wäre fatal. Lauschangriffe sind in allen öffentlichen Netzen und sogar in WANs offensichtlich Bestandteil des alltäglichen Angriffsspektrums. Auch eigene Glasfaserstrecken über öffentlichen Grund dürfen hier nicht ausgeklammert werden. Die Verschlüsselung von standortübergreifender Kommunikation ist ein zentrales Element, bei dem wir in der Vergangenheit zu stark lediglich die Internet-Kommunikation im Fokus hatten. Auch bei Sprachdiensten müssen wir hier genau hinsehen. Wenn ein Vorstand eines Unternehmens oder ein hochrangiger Politiker über ein handelsübliches Smartphone, das ohne spezielle zusätzlichen Sicherheitsmaßnahmen geschützt ist, wichtige Entscheidungen bespricht, darf sich die Person nicht wundern, wenn diese Informationen in falsche Hände gelangen.

- **Unsichtbar machen:** Außerdem müssen wir in unserer Kommunikation über das Internet und öffentliche Netze unsichtbarer, d.h. anonymer werden. Dies gilt speziell für Mobilfunknetze und der umfangreichen Möglichkeiten der Korrelation von Daten, Ort und Person. Eine statistische Auswertung des Kommunikationsverhaltens der Mitarbeiter einer Unternehmung kann heute durchaus auf wesentliche strategische Entscheidungen einen Rückschluss liefern und einer Gegenseite nicht unerhebliche Verhandlungsvorteile verschaffen. Dies bedeutet allerdings auch, dass wir uns „entgooglen“ müssen. Die bequeme Nutzung dieser Dienste muss auf den Prüfstand!

Auch wenn sich diese Maßnahmen praktisch auf die gesamte IT-Infrastruktur und Anwendungslandschaft beziehen, es gibt einen besonders kritischen Bereich, der hinsichtlich Überwachbarkeit besonderes exponiert ist: Unified Communications & Collaboration (UCC) bündelt praktisch alle besonders kritischen Bedrohungen. Daher die Empfehlung: Machen Sie angesichts NSA und Co. das Jahr 2014 zum Jahr der umfassenden Absicherung von UCC. Ihre Daten werden es Ihnen danken.

Zweitthema

VMware NSX – Anfang oder Ende einer Entwicklung?

Fortsetzung von Seite 1

Dipl-Math. Cornelius Höchel-Winter ist Leiter des Testlabors der ComConsult Technologie Information GmbH. In dem Labor werden regelmäßig Messungen und Evaluierungstests neuester Hard- und Softwareprodukte durchgeführt und ausgewertet. Herr Höchel-Winter besitzt langjährige Erfahrung in der Konzeptionierung, im Aufbau und Betrieb von Windows- und Unixnetzen; so hat er als verantwortlicher Projektmanager die Rechenzentren und Netzwerke auf dem Gelände der EXPO2000 in Hannover aufgebaut und während der Weltausstellung betrieben.

Einzig Cisco hat mit dem Nexus 1000V einen eigenen virtuellen Switch gebracht, der den Netzwerkadministratoren ihr vertrautes Look-and-Feel zurückgab und in Richtung Serveradministration die Botschaft übermittelte „Seht Euch dieses CLI an, so werden echte Netzwerke gesteuert." Die andere Botschaft war natürlich „Cisco und VMware sind enge Partner. Cisco ist der Hersteller, der Ihre VMware-Umgebung auf der Netzwerkseite am besten unterstützt." Die beiden Marktführer im Segment Virtualisierung und im Segment Netzwerk hatten sich zusammengetan.

Leider strotzten beide Strategien, die Abwehr und der virtuelle Nachbau, nicht gerade vor innovativen Ideen und können mittlerweile als größtenteils vergebliche Verteidigungsstrategien eines veralteten Status-Quo entlarvt werden. Kaum jemand aus dem Netzwerkbereich hat sich aber ernsthaft mit der Frage beschäftigt, wie virtuelle Switche ins Netzwerk integriert werden könnten. Über 10 Jahre nicht! In meinem Beitrag über die Rolle von Ethernet Fabrics in virtualisierten Umgebungen auf unserem Wissensportal (http://www.comconsult-research.de/ethernet-fabrics-virtualisierte-umgebungen) habe ich aus einem aktuellen Gartner Report zitiert, der mit der Aufforderung beginnt, Netzwerk-Profis sollten sich (endlich) auf den Weg zu höherer Effizienz und Automatisierung in ihren RZ-Netzen machen. Die Branche scheint jede Innovation zu verschlafen.

Dabei ist das Netzwerk bekanntlich kein Selbstzweck, sondern Dienstleister: Daten, Anwendungen, Workloads müssen möglichst schnell, möglichst ungestört und möglichst sicher von A nach B transportiert werden. Und die Anforderungen an diese Dienstleistung sind gestiegen:

- Automatisierung,
- Mobilität virtueller Server,
- Zentralisierung von Speicher,
- Ost-West-Verkehr im Rechenzentrum,
- Multi-Pathing,
- Cloud Computing

sind nur einige der bekannten Bedarfe, die immer wieder genannt werden und die mit klassischen RZ-Architekturen nur unzureichend adressiert werden.

Zugegeben, nicht jedes mittelständische Rechenzentrum hat momentan diese Anforderungen. Wer aber Server virtualisiert, muss über flexiblen, zentralen Speicher nachdenken. Wer mobile Endgeräte nutzen will, braucht eine passende Infrastruktur, sowohl sicherheitstechnisch als auch versorgungstechnisch – da ist die Cloud nicht mehr weit. Einiges davon kann man sicher noch einige Zeit mit traditionellen Techniken abfangen, auf die Dauer steht jedoch zu befürchten, dass Ihnen irgendwann die Komplexität Ihrer Umgebung über den Kopf wächst.

Die Rolle von SDN

Und mittlerweile versetzt das nächste Thema die Gemüter in Aufregung: SDN – Software Defined Networks: Ein zentraler Controller soll komplett alle Entscheidungen über die Wege durch das Netzwerk übernehmen, die Intelligenz und damit natürlich auch die Komplexität aller Netzwerkkomponenten wird weitgehend reduziert. Die aktiven Komponenten sollen die Entscheidungen des Controllers nur noch umsetzen und gegebenenfalls neue Flows erkennen und dem Controller zur Entscheidung vorlegen. Technisch ausgedrückt: Die Control Planes werden von den Forwarding Planes getrennt und in einem Controller zentral zusammengeführt, lediglich die Forwarding Plane bleibt auf den Komponenten.

Dieses Erkennen von Flows – egal ob bereits bekannt oder neu – wurde übrigens anfänglich völlig unterschätzt. Die mit SDN verbundene Erwartung, Switches, Router, Firewalls etc. durch einheitliche, billige Standardsysteme ersetzen zu können, wird sich daher wohl nicht realisieren lassen.

Trotzdem skizziert SDN eine völlig neue Idee von Netzwerk: nicht mehr das Netzwerk, das als komplexer Verbund individuell entscheidender Knoten jedes einzelne Paket Hop-by-Hop hoffentlich letztlich zum Ziel bringt, sondern ein zentral gesteuertes Netzwerk, in dem spezialisierte Softwarekomponenten für jeden Flow einen geeigneten Weg durch das Netz festlegen.

Im Vergleich zu den virtuellen Switches ist SDN also eher eine Revolution als eine Innovation und revolutionäre Umwälzungen sind in einer so – milde ausgedrückt – innovationsskeptischen Branche wie der Netzwerkbranche eher unwahrscheinlich.

Warum wird SDN also so viel Beachtung beigemessen?

Nun das hat mehrere Gründe, zwei wollen wir kurz beleuchten: die Erwartungshaltung an Software und die Marktposition einiger Protagonisten.

Es gibt im Netzwerkbereich, aber insbesondere in RZ-Netzen einen deutlichen Innovationsdruck:

- Die Komplexität der Betriebssysteme vieler heutiger Switche ist nicht mehr akzeptabel, einige Hersteller wie beispielsweise Cisco versuchen schon fast verzweifelt, sich von Uralt-Betriebssys-

temen zu lösen, was ihnen jedoch vom Markt immer wieder verwehrt wird.

- Die anachronistische, textbasierende Steuerung dieser Systeme durch die Eingabe ellenlanger CLI-Kommandos ist schwerfällig, fehleranfällig und behindert nicht zuletzt die Personalplanung.

- Auch die Netze selbst haben einen Komplexitätsgrad erreicht, der ihre Administration aufwändig und unflexibel macht. Neue Netzwerkkomponenten, neue Netzwerkdienste, neue Firmware-Versionen brauchen immens viel Zeit, insbesondere in der Planungs- und Testphase.

- Aus der Server-Virtualisierung kommen neue Anforderungen hinsichtlich Flexibilität und Geschwindigkeit von Umkonfigurationen, die letztlich nur durch automatisierte Vorgänge erfüllt werden können.

- Die tonangebenden, herstellerübergreifenden Standardisierungsgremien wie IEEE und IETF arbeiten einfach viel zu langsam. Die Entscheidungsfindung dauert zu lange. Klassische Beispiele sind die Verabschiedung von TRILL und SPB: 10 Jahre haben die Organisationen darüber diskutiert und dann ist noch nicht einmal ein gemeinsamer Entwurf dabei herausgekommen.

Diesem Innovationsdruck meinen viele durch Software begegnen zu können:

- Software ist schneller entwickelt.
- Software ist schneller eingesetzt.
- Software erlaubt Automatisierung.
- Wenn man auf Open Source setzt, könnten durch eine große Entwicklergemeinschaft auch die Innovationszyklen deutlich verkürzt werden.

Die Risiken hierbei sind natürlich nicht zu unterschätzen, gerade der Verzicht auf standardsbasierende Protokolle bedeutet schnell auch den Verzicht auf Interoperabilität!

Aber SDN, zumindest die reine Lehre davon, ist weit entfernt. Noch sind zu viele Fragen offen und ganz offensichtlich fehlt der überzeugende Anwendungsfall für betriebliche Netzwerke, die nicht die Größe der RZ-Netze von Google und anderen Providern haben. Was aber definitiv bleibt, ist eine gewisse Sehnsucht nach Software, nach schnellerer Innovation, nach einfacherer Administration.

Der zweite Aspekt betrifft die Marktsituation von VMware: VMware war lange Zeit unangefochtener Marktführer und Innovationstreiber im Bereich Server-Virtualisierung.

Das hat sich aber geändert. Mit Xen, KVM und Hyper-V wird VMware gleich von mehreren Seiten angegriffen, und zwar sowohl von der Open-Source-Seite als auch von Microsoft als führenden Software-Hersteller. Darüber hinaus sind damit ernsthafte vSphere-Alternativen in allen gängigen Server-Betriebssystemen quasi vorinstalliert.

VMware brauchte also eine neue Perspektive – und hat sie im Netzwerk gefunden.

Die Akquisition von Nicira und deren Produkt NVP passte da genau ins Konzept. VMware NSX – das ist die Kombination aus VMware vCloud Network and Security und Nicira NVP - ist für VMware das perfekte Produkt:

- Mit der Einführung weiterer virtueller Netzwerkkomponenten wird der virtuelle Switch zu einer zentralen Kernkomponente im (virtualisierten) Netzwerk.

- Durch die Overlay-Strukturen wird ein für VMware wichtiges Problem gelöst, das bislang von Netzwerkseite eher wegdiskutiert wurde als dass Lösungen präsentiert wurden, nämlich die Konnektivität zwischen virtuellen Maschinen nachdem sie über Layer-3-Grenzen hinweg verschoben wurden.

- Last but not least wird mit NSX ein neues Marktsegment erschlossen, der alte Führungsanspruch im Virtualisierungsumfeld erneut untermauert. Die Kröte, dass man damit das gute Verhältnis zu Cisco praktisch aufkündigt, hat VMware anscheinend ohne zu zögern geschluckt.

Was ist VMware NSX konkret?

VMware bezeichnet NSX als „Plattform für Netzwerkvirtualisierung und -sicherheit für das Software-Defined Datacenter“. NSX ist quasi das Gegenstück zu vSphere auf der Netzwerkseite. So wie bei der Servervirtualisierung virtuelle Computing-Kapazitäten durch eine Software-Schnittstelle zusammengebaut und den Anwendungen zur Verfügung gestellt werden, werden bei der Netzwerkvirtualisierung virtuelle Netzwerke, also Transportwege und Netzwerkdienste, zusammengebaut und zur Verfügung gestellt.

Dies geschieht wie bei jeder Virtualisierungstechnologie durch die Einführung einer softwarebasierenden Abstraktionsebene, um die folgenden Ziele umzusetzen:

- Physische Ressourcen und Dienste werden weitestgehend hinter der Abstraktionsebene versteckt, die Anwendungen kennen keine Details der (meist komplexen) physischen Welt und müssen sich daher auch nicht damit auseinandersetzen.

- Stattdessen werden benötigte Ressourcen und Dienste auf der virtuellen Seite in standardisierter Form softwaretechnisch nachgebildet.
  - Typische Netzwerkdienste, die in virtueller Form bereitgestellt werden, sind: Layer-2-Switching, Layer-3-Routing, Firewalls und andere.

- Damit erreicht man eine deutliche Reduzierung der Komplexität in der virtuellen Welt:
  - Nicht jede virtuelle Instanz braucht alle verfügbaren Dienste.
  - Bei der Servervirtualisierung werden beispielsweise standardisierte Hardware-Komponenten emuliert, sodass auf virtuellen Servern keine speziellen Treiber installiert werden müssen.
  - Bei der Netzwerkvirtualisierung werden kleine, überschaubare IP-Netze emuliert, inklusive genau der Netzwerkdienste, die für die konkrete Aufgabe benötigt werden.

- Darüber hinaus sind die virtualisierten Dienste unabhängig von den speziellen Details in der physischen Welt. Das heißt,
  - physische Ressourcen können ausgetauscht werden, ohne dass Anwendungen auf der virtualisierten Seite angepasst werden müssen,
  - virtuelle Instanzen können in der physischen Welt verschoben und deren Dienste und Ressourcen anderen physischen Ressourcen zugeordnet werden (z. B. vMotion),
  - virtuelle Instanzen wie virtuelle Server oder virtuelle Netze können als Software-Container gespeichert, kopiert, im Internet verteilt und automatisiert bereitgestellt werden.

- Die Dienste und Ressourcen auf der virtuellen Seite sind völlig entkoppelt von denen auf der physischen Seite.

- Somit hat man die Möglichkeit Ressource-Pools zu bilden beziehungsweise physische Ressourcen als Pool zu behandeln und bedarfsorientiert den virtuellen Instanzen zuzuweisen. So erreicht man eine bessere Ausnutzung der physischen Ressourcen, da diese von mehreren virtuellen Instanzen gleichzeitig genutzt werden können. Je nach Anwendung ist hierbei sogar eine Überbuchung der physischen Ressource möglich.

VMware NSX – Anfang oder Ende einer Entwicklung?

- Bei virtuellen Servern werden CPU und Hauptspeicher typischerweise als Pool behandelt.
- Bei virtuellen Netzen wird natürlich die Transportkapazität des physischen Netzes als Pool behandelt und kann auf die virtuellen Netze verteilt werden.

- Verschiedene virtuelle Instanzen sind untereinander komplett voneinander entkoppelt:
  - Das heißt, „Mandantenfähigkeit“ ist quasi ein Teil des Konzepts.
  - Speziell bei Netzwerkvirtualisierung bedeutet das, dass Netzwerkadressen wie MAC oder IP in unterschiedlichen virtuellen Netzen mehrfach genutzt werden können.

Wie jede Virtualisierungstechnologie adressiert also auch Netzwerkvirtualisierung primär betriebliche Aspekte:

- Virtuelle Netze können in Form von Templates vorbereitet und automatisiert ausgerollt werden.

- Virtuelle Netze können zusammen mit virtuellen Endpunkten (Servern) verschoben werden.

- Virtuelle Netze können beispielsweise zu Testzwecken einfach dupliziert werden, ohne dass Netzwerkadressen, Routing-Einträge oder Firewall-Regeln angepasst werden müssen – die werden nämlich einfach als virtuell zur Verfügung gestellte Dienste mitkopiert.

- Monitoring und Troubleshooting auf Anwendungsebene geschieht innerhalb der virtuellen Netze und damit ebenfalls in Software, selbst so etwas wie ein virtueller TAP ist möglich und kann per Knopfdruck eingerichtet und wieder abgebaut werden.

Zusammenfassend: **Der Netzwerkbetrieb wird einfacher, die Netze weniger komplex:**

- Die virtuellen Netze sind kleine, überschaubare Einheiten.

- Das physische RZ-Netz wird zum reinen Transportnetz, das nichts über die transportierten Dienste weiß, das noch nicht einmal die angebundenen virtuellen Endpunkte kennt. Somit hat das physische Netz auch nichts mit den MAC-Adressen der Endpunkte und deren IP-Adressstruktur zu tun.

Klar ist damit aber auch, dass Sie ein in weiten Teilen völlig neues Betriebsmodell erhalten. Hier nur einige mögliche Problempunkte:

- Wenn Sie Firewall-Regeln virtualisieren, bedeutet das auch eine Dezentralisierung der Prüfpunkte. Das hat zweifellos Vorteile für den Betrieb und wird letztlich auch die Sicherheit der einzelnen Anwendung erhöhen, da so tatsächlich jeder Verkehr zur Anwendung geprüft wird und nicht nur solcher aus dem Internet. Trotzdem müssen Sicherheitsbeauftragte erst einmal vom neuen Konzept überzeugt werden.
  So oder so: Zuständige Sicherheitsbeauftragte müssen also mit ins Boot.

- Die Unabhängigkeit von einem übergreifenden IP-Adresskonzepts klingt gut, führt aber spätestens dann zu Problemen, wenn Sie Verkehr von einem virtuellen Netz ins andere routen wollen und in beiden Netzen dasselbe IP-Subnetz verwenden.

- Trotz der schönen neuen virtuellen Welt brauchen Sie Gateways um Verkehr aus den virtuellen Netzen aus- und wieder einzukoppeln. Typische Beispiele für physische Kommunikationsendpunkte sind:

  - Datenbanksysteme,
  - Speichersysteme und
  - natürlich Clients.

Wie schon bei der Einführung der Servervirtualisierung wird auch die Netzwerkvirtualisierung darauf hinaus laufen, dass eine engere Kooperation zwischen Serverbetrieb und Netzwerkbetrieb nötig sein wird.

Interessant ist wie diese Änderungen im Betriebsmodell schon im „Einführungsvideo“ zu NSX von VMware dargestellt werden: Zunächst verweigert der Netzwerk-Administrator kategorisch seine Unterstützung, wird dann natürlich vom Virtualisierungsexperten überzeugt und fährt zur Belohnung aus dem Keller, wo er mit Schraubendreher und Zange physische Systeme wartete, auf in die oberen Geschosse, wo er sich zukünftig um seine „wirklichen“ Aufgaben kümmert: Netzwerkdesign, Kapazitätsplanung und Traffic Engineering.

Vergessen Sie aber nicht: Unten im Keller stehen immer noch ein paar Geräte herum, ohne die genau nichts funktioniert.

Die Architektur von NSX im Überblick

Bislang gibt es zwei Versionen:

- NSX für Linux-Hypervisor (unterstützt werden Xen und KVM)
  Das ist im Wesentlichen das Nicira NVP-Produkt.

- NSX für vSphere
  Das ist NVP zusammen mit vCNS (VMware vCloud Network and Security), dem Produktnachfolger von vShield. vCNS stellt im Wesentlichen eine direkt im Kernel des Hypervisors integrierte, virtuelle Firewall zur Verfügung.

Im Folgenden werden wir uns im Wesentlichen auf die Version für vSphere beschränken.

Die wesentlichen Komponenten einer

VMware NSX – Anfang oder Ende einer Entwicklung?

NSX-Installation sind:

- ein physisches Layer-2- oder Layer-3-Netzwerk als Transportnetz,
- mit diesem Netzwerk verbundene Hypervisor-Hosts
- die virtuellen Switches auf diesen Hypervisors,
- virtuelle Maschinen,
- NSX-Controller,
- Gateways.

Zusammen mit vCloud Network and Security stehen dabei folgende Netzwerkdienste zur Verfügung:

- Layer-2-Switching,
- Layer-3-Forwarding (statisches und dynamisches Routing),
- Firewalls (sowohl als Port-Filter pro Netzwerkschnittstelle als auch als zentralisierte Firewall für ganze Subnetze),
- ACLs,
- Load Balancer (Layer 4 bis Layer 7),
- NAT,
- DNS und DHCP,
- VPNs (IPSec und SSL).

Zur Realisierung der notwendigen Abstraktionsschicht nutzt NSX Overlay-Techniken. Das heißt, die virtuellen Netze werden als logisches Konstrukt über das physische Netz gelegt und via IP-Tunnel durch das RZ-Netz getunnelt. Als Tunnelprotokoll stehen drei Möglichkeiten zur Verfügung:

- VXLAN,
- STT,
- GRE,

wobei NSX für vSphere nur VXLAN unterstützt.

Alle drei Verfahren sind standardmäßig nicht verschlüsselt. Falls notwendig, also zum Beispiel zwischen remote Sites, können aber auch verschlüsselte Tunnel aufgebaut werden.

GRE ist übrigens nicht NVGRE, das Tunnelprotokoll, das Microsoft präferiert, sondern das „normale“ GRE, wobei das Frame-Format von NVGRE und GRE identisch sind. Die beiden Varianten unterscheiden sich lediglich in der Interpretation einiger Felder im GRE-Header.

STT ist ein Tunnelprotokoll, das Nicira entwickelt hatte, um TCP-Offloading in den Server-Netzwerkkarten zu nutzen. Hierzu wird das Frame-Format von TCP imitiert, obwohl kein TCP gesprochen wird. Aus naheliegenden Gründen (Verwechslungsgefahr mit TCP) können wir STT nicht empfehlen, zumal moderne Serverkarten mittlerweile sowohl GRE/NVGRE als auch VXLAN in Hardware unterstützen und so der anfängliche Performance-Vorteil von STT durch die Nutzung von TCP-Offloading weggefallen ist.

VXLAN ist das präferierte Tunnelprotokoll von VMware. VXLAN ist ein „MAC-in-UDP“-Verfahren, das Frame-Format ist in Abbildung 1 dargestellt.

Wie man erkennt, wird der Original-Frame nacheinander um drei Header erweitert:

- Der VXLAN-Header enthält im Wesentlichen einen 24 Bit Identifier. Damit können mehr als 16 Millionen VXLAN-Segmente unterschieden und somit

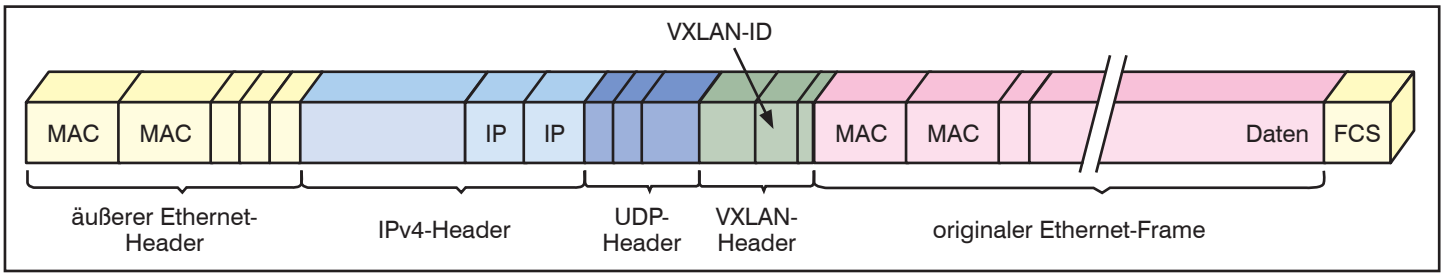


Abbildung 1: VXLAN Frame-Format

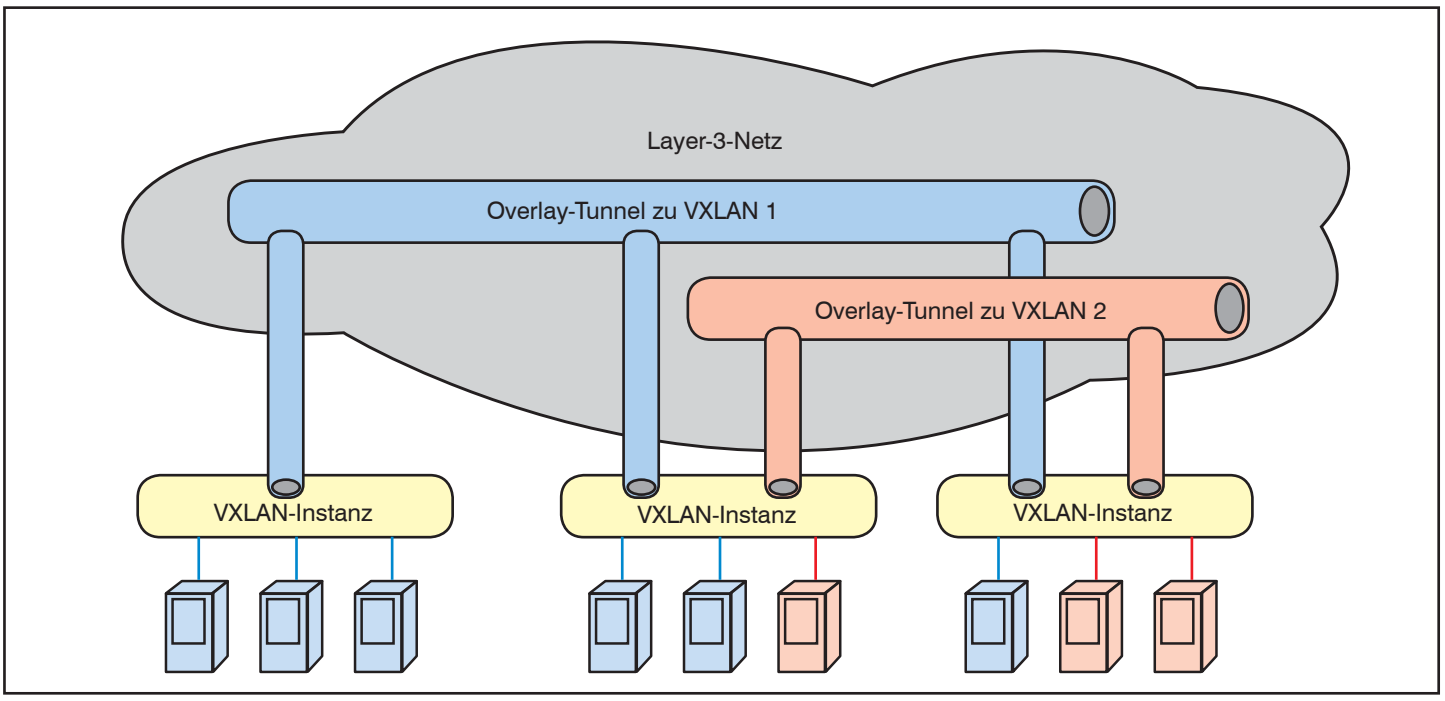


Abbildung 2: Pro VXLAN-ID ein virtuelles Overlay-Netz

deutlich mehr als mit 802.1Q-VLANs. Außerdem sorgt dieser Header dafür, dass virtuelle Maschinen in verschiedenen VXLAN-Segmenten nicht miteinander kommunizieren können.

- Der UDP/IP-Header sorgt dafür, dass der eingekapselte Frame über Layer 3 transportiert werden kann. Hierfür wird in den Tunnelendpunkten eine Zuordnungstabelle „innere Ziel-MAC-Adresse“ – „IP-Adresse des entsprechenden Tunnel-Endpunktes“ aufgebaut – dies geschieht wie üblich durch Lernen.

- Und schließlich ein passender MAC-Transport-Header, der sich wie üblich beim Durchgang durch das IP-Netz regelmäßig ändert.

Eine Besonderheit des Konzepts ist, dass Broadcasts (und unbekannte Unicast-Adressen) mittels IP-Multicasts weitergeleitet werden können. Damit auch diese Kommunikation innerhalb des VXLAN-Segments bleibt, braucht jedes VXLAN-Segment eine eigene IP-Multicast-Adresse. Die Zuordnung von IP-Multicast-Adresse zu VXLAN-ID erfolgt auf Management-Ebene durch den NSX-Controller. Die Endpunkte selbst propagieren ihre jeweilige Zugehörigkeit zu bestimmten Multicast-Gruppen dann via IGMP an das zugrundeliegende Transportnetzwerk.

Falls das Transportnetz kein IP-Multicast unterstützt, muss die Replikation der Pakete bereits im Tunnelstartpunkt durch den Versand mehrfacher IP-Unicasts erfolgen. NSX hält für dieses „Flooding“ eine Reihe spezialisierter Verfahren bereit, um die Hypervisor beim Versand vieler Unicasts zu entlasten. So sieht das Konzept zum Beispiel auch sogenannte Service-Nodes vor, dedizierte Knoten, auf die der Massenversand ausgelagert werden kann.

Das Verfahren definiert also pro VXLAN-ID je ein Layer-2-Overlay-Netz über ein Layer-3-Transportnetz und verbindet so alle Layer-2-Segmente, denen dieselbe VXLAN-ID zugewiesen wurde. (siehe Abbildung 2) Segmente mit unterschiedlichen VXLAN-IDs sind völlig voneinander getrennt und können nicht miteinander kommunizieren. Daher spielt es auch keine Rolle, wenn in solchen Segmenten gleiche VLANs, gleiche MAC-Adressen, gleiche IP-Adressen etc. verwenden werden.

Der „Kopf“ bei NSX ist der sogenannte NSX-Controller. Dieser Controller wird als „Controller Cluster“ ausfallsicher aufgesetzt, wobei entweder drei oder fünf Controller-Nodes im Cluster unterstützt werden, die alle die identische Informationsdatenbank bereithalten.

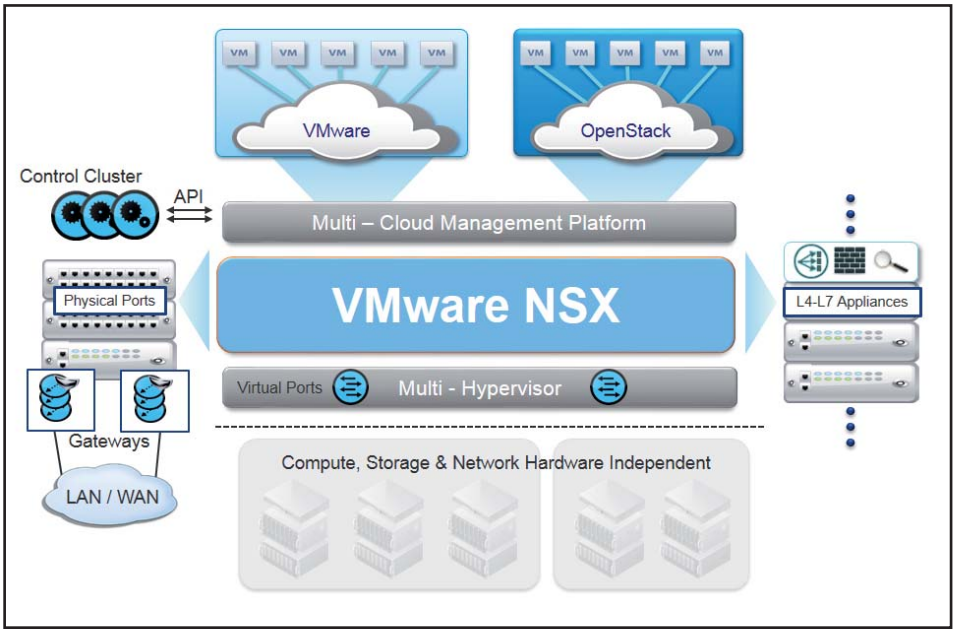


Abbildung 3: VMware NSX Architektur Quelle: VMware

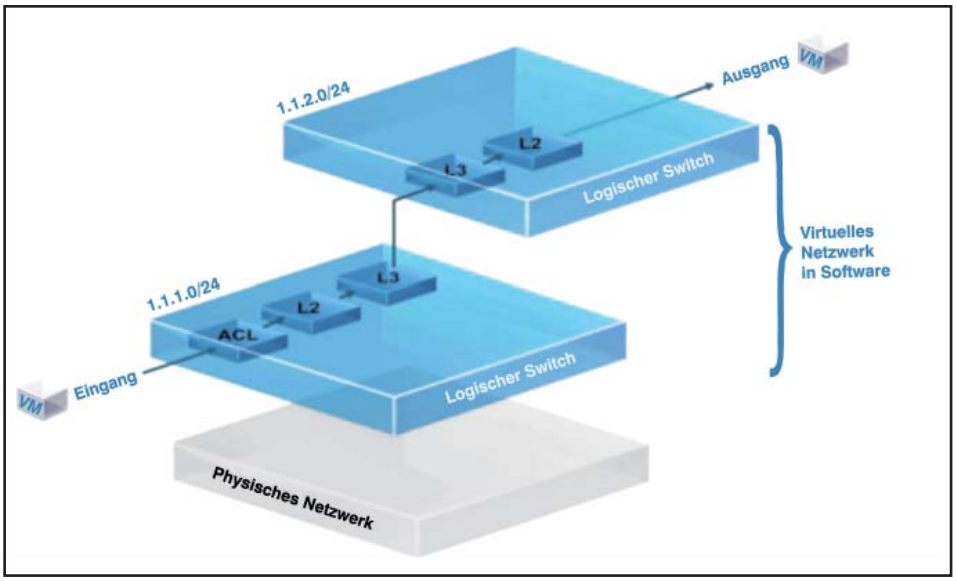


Abbildung 4: Netzwerkdienste werden innerhalb der virtuellen Switche bereitgestellt und mit der jeweiligen VM verbunden Quelle: VMware

Der Controller-Cluster wird seinerseits über ein Northbound-Interface von einer geeigneten Management-Plattform gesteuert. Hier werden aktuell der VMware vCloud Manager und OpenStack (Horizon Dashboard) unterstützt. (siehe Abbildung 3)

Des Weiteren ist jedem NSX-Controller-Cluster bei der vSphere-Version ein vCenter(-Cluster) zugeordnet, sodass der Controller zu jeder Zeit eine vollständige Übersicht über alle Hosts, virtuelle Maschinen und virtuelle Switches hat.

Die Aufgabe des NSX-Controllers besteht jetzt darin, die virtuellen Switche in den jeweiligen Hypervisors entsprechend den Vorgaben der Management-Plattform zu „programmieren“ und so die notwendigen Dienste für die virtuellen Netze zu realisieren. (siehe Abbildung 4) Die geforderten Netzwerk- und Sicherheitsdienste werden hierzu mit den virtuellen Maschinen in einem Netzwerk verknüpft und an die entsprechenden virtuellen Switches verteilt. Wenn eine VM zu einem anderen Host verschoben wird, bleiben diese Dienste mit der VM verknüpft und werden gemeinsam mit ihr verschoben. Wenn dem virtuellen Netzwerk neue VMs beispielsweise zur Skalierung einer Anwendung hinzugefügt werden, können ent-

VMware NSX – Anfang oder Ende einer Entwicklung?

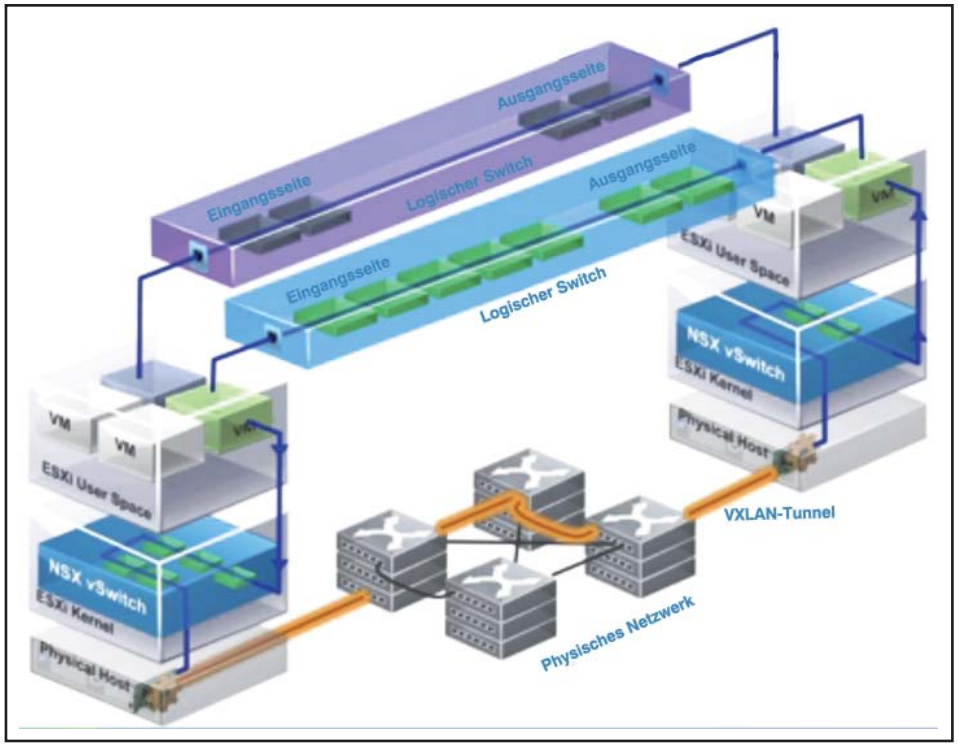


Abbildung 5: Logischer und physischer Kommunikationsfluss Quelle: VMware

sprechende Richtlinien dynamisch auf die neuen VMs angewendet werden.

Darüber hinaus sorgt der Controller dafür, dass alle Pakete, die den Hypervisor verlassen, in das gewünschte Protokollformat eingepackt und im zugeordneten Tunnel verschickt werden, so dass die virtuellen Netze wie gefordert sowohl von einander als auch vom physischen Netzwerk isoliert bleiben. (siehe Abbildung 5)

Bei den Linux-Hypervisors Xen und KVM wird hierzu auf den dort integrierten Open vSwitch gesetzt und via OpenFlow kommuniziert. Bei vSphere wird dagegen der sogenannte Distributed Virtual Switch (vDS) genutzt, die Kommunikation zwischen NSX-Controller und vSwitch läuft hier über ein proprietäres Protokoll.

Neben der so realisierten Kommunikation zwischen virtuellen Maschinen, braucht man in der Regel auch Kommunikationsbeziehungen zu Systemen in der physischen Welt, seien es physische Datenbankserver, Speichersysteme oder einfach Verbindungen zu Clients oder ins Internet. Für solche Verbindungen zwischen virtuellen Netzen und der Außenwelt braucht man Gateways.

NSX stellt Gateways als Layer-2-Gateways und Layer-3-Gateways zur Verfügung. Layer-2-Gateways sind virtuelle Ressourcen, die sogenannte Layer-2-Gateway-Services bereitstellen. Jeder Layer-2-Gateway-Service bildet jeweils ein virtuelles Netz auf ein VLAN im physischen Netz ab.

Physische Layer-2-Gateways werden unter anderem angeboten von:

- Brocade
- Dell
- HP
- Juniper.

Layer-3-Gateway-Dienste werden bei vSphere durch eine erweitere Version von vShield Edge zur Verfügung gestellt. Funktionen dieser Gateways sind:

- Layer-3-Forwarding
- Layer 4-7 Load Balancing
- NAT
- VPN Endpunkt
- SSL Offloading
- Stateful Firewall
- OSPF und BGP als Routing-Protokolle

Daneben gibt es eine ganze Reihe physischer Appliances, die die virtualisierten Dienste von NSX erweitern, ergänzen oder ersetzen können:

- virtuelle und physische Firewall-Services von Palo Alto
- Intrusion Detection, Intrusion Prevention oder Anti Virus von
  - McAfee
  - Symantec
  - TrendMicro
  - Rapid7

Ausblick

Die Kernfragen zur abschließenden Bewertung sind:

- Brauchen wir NSX oder eine andere Form der Netzwerk-Virtualisierung wirklich?
- Wird das physische Netzwerk dadurch weniger wert?
- Ist das das Ende oder der Anfang einer Entwicklung?

Netzwerk-Virtualisierung ist für mindestens zwei Anwendungsbereiche unverzichtbar:

- Installation und Betrieb von komplexen verteilten Anwendungen, die aus dynamisch vielen virtuellen Maschinen bestehen und während des Betriebs im Netzwerk wandern. Beispiele für solche Anwendungen sind private Clouds, die mobile Endgeräte mit einer Infrastruktur versorgen, oder Web-Anwendungen für Kunden, bei denen die Teilnehmerzahl stark schwankt oder zunimmt.

- Die Automatisierung der Installation und des Betriebs von Anwendungen durch ein OpenStack-Framework. Für größere Rechenzentren ist das eindeutig der Weg der nächsten fünf Jahre. Dabei wird auch im laufenden Betrieb die Last zwischen Servern verschoben, um die jeweils optimale Belastung einer minimalen Menge von Hardware-Servern zu erreichen.

Nicht jedes Unternehmen wird von diesen beiden Anwendungsbereichen im Moment betroffen sein, aber im Prinzip muss damit gerechnet werden, dass diese Szenarien an Bedeutung gewinnen. Vor allem OpenStack entwickelt sich schnell und dynamisch weiter und kann sich schnell zur Standard-Installations-Plattform für alle Anwendungen entwickeln.

Natürlich wird das physische Netzwerk durch NSX oder jede andere Form der Netzwerk-Virtualisierung nicht überflüssig. Im Gegenteil muss es weiterhin performant und zuverlässig funktionieren. Aber Netzwerk-Virtualisierung reduziert das Hardware-Netzwerk auf seine elementare Grundaufgabe: die Vermittlung von IP-Paketen in einem standardisierten Netzwerk.

Noch ist die Abgrenzung zwischen Hardware-Transportnetz und virtuellen Anwendungsnetzen vergleichsweise scharf: Ein Cloud-Management definiert die Anforderungen an die virtuellen Netze, die die Hypervisor umsetzen. Beides geschieht im Wesentlichen ohne Rücksicht und ohne Kenntnis irgendwelcher Details des physischen Netzwerks. Und umgekehrt sind

VMware NSX – Anfang oder Ende einer Entwicklung?

die Anforderungen an ein solches Netzwerk auch genau so: Es möge jeden Verkehrstyp ohne Kenntnis, was da gerade transportiert wird, möglichst optimal, schnell und auf kürzesten Wegen transportieren. Natürlich fällt einem an dieser Stelle der Begriff Fabric ein. Fabrics sind genau diese, sich im Kern selbst organisierenden Netze, die man hierfür braucht.

Was NSX macht, ist im Grunde Edge-Provisionierung und Tagging von Verkehrsströmen (Blinken jetzt die MPLS-Lampen auf?). Am Edge kann man offensichtlich Anwendungen und Anforderungen leichter identifizieren, als irgendwo unterwegs im Core. Und natürlich ist es sinnvoll, wenn nicht sogar notwendig, dafür zu sorgen, dass eine einmal vorgenommene Klassifizierung (Tunnel-ID) erhalten bleibt. Das ist ja auch die große Diskussion bei SDN: Ohne irgendeine Art von Kennzeichnung eines Flows (ob das jetzt Tunnel oder einfache Tags sind, ist nicht wesentlich) muss jeder Switch im Netzwerk dazu in der Lage sein, diesen Flow wiederzuerkennen.

Fabrics sind beileibe keine simplen Netzwerke mit billiger Hardware. Trotzdem ist eine solche Entwicklung nicht im Interesse jedes Herstellers. Ethernet-Switches werden sich in ihrem Hardware-Kern immer ähnlicher. Alleinstellungsmerkmale erringen die Hersteller in der Regel durch Zusatzfunktionen, die über das einfache Paket-Vermitteln hinausgehen. Mit NSX wandern diese wichtigen Zusatzfunktionen in die Software und in die virtuellen Switches. Damit wird Netzwerk-Hardware austauschbar und beliebig, selbst bei den Ethernet-Fabrics zeichnet es sich ab, dass sich die diversen TRILL-Derivate immer mehr SPB annähern.

Austauschbarkeit ist aber nie im Interesse der Hersteller. Es drohen ein drastischer Preisverfall und der Verlust von Abgrenzung zur Konkurrenz. Die Diskussion über NSX ist daher auch eine Diskussion über die Zukunft der Netzwerk-Industrie.

Damit sind wir bei der letzten Frage, ob dies das Ende oder der Anfang einer Entwicklung ist. Rundet NSX die Virtualisierung im Rechenzentrum ab, indem zu Compute und Storage auch Netzwerk-Ressourcen integriert werden? Oder ist das der erste konkrete Schritt hin zu SDN?

Martin Casado ist nicht nur Gründer von Nicira, er gehört auch zu der kleinen Gruppe von Leuten, die SDN entwickelt haben. Diese Gruppe will die Kontrolle über das Netzwerk nicht den heutigen Switch-Systemen überlassen. Und SDN ist die logische Weiterentwicklung von NSX und passt voll in den Rahmen eines automatisierten Rechenzentrums mit OpenStack. Mit SDN verschwindet die Grenze zwischen virtuellem und physischem Netz, virtuelle und physische Switche, Router, Firewalls werden gleichbehandelt, aus der Sicht des steuernden Controllers gibt es diese Unterscheidung überhaupt nicht.

Das Ziel wird sein, dass der zentrale Controller die Routen für NSX schaltet und die Flows in den Switches im Hardware-Netzwerk setzt. Dies ist nur konsequent und ermöglicht vor allem eine wesentlich dynamischere Handhabung der Gateways und die Berücksichtigung der aktuellen Auslastung physischer wie virtueller Ressourcen.

So gesehen ist NSX ein Angriff auf das komplette traditionelle Netzwerk. Hier geht es wirklich um die Zukunft von Netzwerk-Industrien. Es ist also kein Wunder, dass einzelne Hersteller in Verteidigungsposition gegangen sind und äußerst nervös auf das Thema reagieren.

ComConsult Veranstaltungskalender

Aktuelle Veranstaltungen

Wireless LAN professionell, 17.02. - 19.02.14 in Bonn

Dieses Seminar vermittelt den aktuellen Stand der WLAN-Technik und zeigt die in der Praxis verwendeten Methoden für Aufbau, LAN-Integration, Betrieb und Optimierung von WLANs im Enterprise-Bereich auf. Die verschiedenen WLAN-Varianten werden analysiert, Markt- und Produktsituation werden bewertet, und Empfehlungen für eine optimale Auswahl werden gegeben.

Preis: € 1.890,-- netto

IPv6 Grundlagen - SeminarPlus, 24.02. - 25.02.14 in Düsseldorf

Diese Schulung bietet allen Planern, Betreibern, Administratoren und Softwareentwicklern, die von einer Migration zu IPv6 betroffen sind, ein tiefes Verständnis der Basis von IPv6. Das neue Konzept „SeminarPlus“ sorgt mit vielen Videos zur individuellen Vor- und Nachbereitung der Präsenz-Schulung für einen optimalen Lernerfolg.

Preis: € 1.790,-- netto

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen, 24.02. - 26.02.14 in Düsseldorf

Dieses Seminar behandelt die Projektschritte, Einsatz- und Migrations-Szenarien, einsetzbare Basis-Technologien, Komponenten und erweiterte TK-Anwendungen, Bewertungskriterien für eine TK-Lösung und gibt eine Übersicht über den bestehenden TK-Markt etablierter Hersteller wie Alcatel-Lucent, Avaya, Cisco und Siemens aber auch des Newcomers Microsoft.

Preis: € 1.890,-- netto

SIP (Session Initiation Protocol) - Basis-Technologie der IP-Telefonie, 10.03. - 12.03.14 in Stuttgart

SIP ist der Schlüssel für offene, leistungsfähige und kostenoptimale Kommunikationslösungen. Es umfasst Sprache, Video, Daten und Präsenz. Lernen Sie, was SIP leistet, worin sich wesentliche Herstellerlösungen unterscheiden und wie Sie das Beste aus beiden Welten zukunftsorientiert nach Ihrem Bedarf optimieren.

Preis: € 1.890,-- netto

Sicherheitsmanagement mit BSI-Grundschutzmethodik/ ISO 27001, 10.03. - 12.03.14 in Stuttgart

Angemessene Sicherheit mit optimalem Aufwand: geht das? Die Antwort liegt in der Nutzung bewährter Architekturen und Lösungen bei gleichzeitiger Erfüllung von Compliance Richtlinien. Anders formuliert: das Rad muss nicht von jedem Unternehmen neu erfunden werden. Dieses Seminar stellt die BSI-Grundschutzmethodik vor und zeigt auf, wie auf der Basis dieser etwas abstrakten Methodik eine Praxis-gerechte Sicherheitslösung mit optimalem Aufwand erreicht werden kann.

Preis: € 1.890,-- netto

RZ-RZ-Kopplung - alles nur eine Frage der Bandbreite?, 17.03.14 in Bonn

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

Preis: € 990,-- netto

Verkabelungssysteme für Lokale Netze, alles standardisiert, alles klar?, 17.03.14 in Bonn

Dieses Seminar erklärt praxisnah und herstellerneutral wie Sie hohe Qualität, Verfügbarkeit und lange Nutzbarkeit bei der Planung und im Betrieb einer Verkabelungs-Lösung erreichen.Die Bausteine einer Verkabelung werden vorgestellt und zu einem handhabbaren Gesamtsystem kombiniert. Lernen Sie wo sich gute von schlechten Lösungen unterscheiden. Dabei werden die Normen diskutiert und die praktische Handhabung der Normungsvorgaben erklärt. Produktbewertungen wechseln sich mit bewährten Tipps aus der Praxis zu Installation und Betrieb ab.

Preis: € 990,-- netto

Umfassende Absicherung von Voice over IP und Unified Communications, 17.03. - 18.03.14 in Bonn

Dieses Seminar beschäftigt sich mit dem Gefährdungspotenzial und den erforderlichen Sicherheits- und Abwehr-Maßnahmen rund um das Thema VoIP und UC. Im Rahmen der Umstellung auf IP-basierte Kommunikationslösungen ergeben sich neue Gefährdungsszenarien. Die Teilnehmer lernen wie sie mit diesen Bedrohungen umgehen können.

Preis: € 1.590,-- netto

Netzzugangskontrolle: Technik, Planung und Betrieb, 17.03. - 19.03.14 in Bonn

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

WAN: Konzept, Planung und Ausschreibung, 17.03. - 18.03.14 in Bonn

Seminar über die erfolgreiche Konzeption, Planung und Betrieb von WAN-Netzwerken. Lernen Sie wie Sie mit modernsten Technologien und erprobten Architekturen wirtschaftliche, verfügbare und leistungsfähige WAN-Lösungen aufbauen können. Erfahren Sie wie Sie sinnvoll SLAs für die Praxis aufsetzen können, die auch im Tagesbetrieb standhalten. Mit vielen Tipps und Tricks aus der Praxis.

Preis: € 1.590,-- netto

Zertifizierungen

ComConsult Certified Network Engineer

Lokale Netze
05.05. - 09.05.14 in Aachen
08.09. - 12.09.14 in Aachen
17.11. - 21.11.14 in Aachen

TCP/IP-Netze erfolgreich betreiben
02.06. - 04.06.14 in Aachen
20.10. - 22.10.14 in Aachen

Internetworking
07.04. - 11.04.14 in Aachen
23.06. - 27.06.14 in Aachen
03.11. - 07.11.14 in Aachen

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

ComConsult Certified Trouble Shooter

Trouble Shooting in vernetzten Infrastrukturen
20.05. - 23.05.14 in Aachen
28.10. - 31.10.14 in Aachen

Trouble Shooting für Netzwerk-Anwendungen
24.06. - 27.06.14 in Aachen
18.11. - 21.11.14 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
24.02. - 26.02.14 in Düsseldorf
05.05. - 07.05.14 in Bonn
29.09. - 01.10.14 in Stuttgart
17.11. - 19.11.14 in Bonn

Session Initiation Protocol Basis-Technologie der IP-Telefonie
10.03. - 12.03.14 in Stuttgart
02.06. - 04.06.14 in Düsseldorf
20.10. - 22.10.14 in Berlin

Umfassende Absicherung von Voice over IP und Unified Communications
17.03. - 18.03.14 in Bonn
30.06. - 01.07.14 in Bonn
03.11. - 04.11.14 in Bonn

Optionales Einsteiger-Seminar: IP-Wissen für TK-Mitarbeiter
08.04. - 09.04.14 in Aachen
15.09. - 16.09.14 in Düsseldorf

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

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

Impressum

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

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

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

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