ComConsult Research

Der Netzwerk Insider

März 2014

Systematische Weiterbildung für Netzwerk- und IT-Professionals

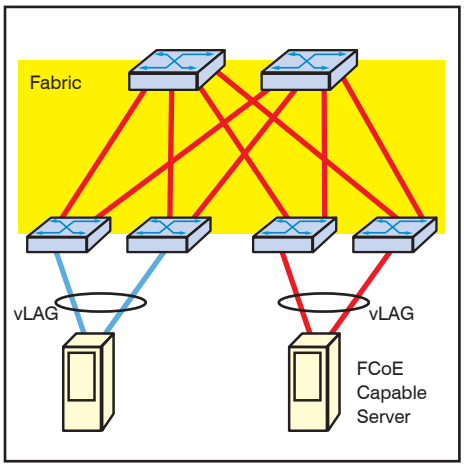
Schwerpunktthema

Netzwerk-Design in Zeiten von 10/40/100 Gbit: Wie sieht die Zukunft aus? - Teil 2

von Dipl.-Inform. Petra Borowka-Gatzweiler

4. Design-Elemente: Ringförmige Designs

Ringförmige Designs haben traditionell einen Gegenpool zu Sterndesigns gebildet, denken wir an Token Ring, FDDI und auch Ringe aus Produktionsumgebungen und Metro-Netzen mit sehr niedrigen Schaltzeit-Anforderungen unter 50 ms wie EAPS, HiPER Ring oder MRP. Wie schon erwähnt, sind Ring-Designs mit Spanning Tree sehr nachteilig, da der Ring nicht lastverteilt arbeitet und sehr lange Wege entstehen (siehe Abbildung 4.1). Mit neuen Technologien wie Layer-2 Multipath, gegebenenfalls kombiniert mit Routing im Campus, werden Ring-Designs, unter anderem aus Kostengründen, jedoch wieder interessant, da diese Verfahren den Ring in jeder Richtung und zielbezogen lastverteilt nutzen (siehe Abbildung 4.2).



Im Access Bereich kann das Ring Design bei kleiner Switch-Anzahl den Gebäude-Konzentrator einsparen. Im Beispiel-Szenario aus Abbildung 4.3 lassen sich an jedem gebäudeinternen Switch Endgeräte anschalten. Die zusätzliche Querverbindung in Gebäude 4711 optimiert die Lastverteilung im Fehlerfall (Ausfall einer Campus-Verbindung oder eines Campus-Switches).

weiter auf Seite 6

Zweitthema

Enterprise Mobility: Schmelztiegel der Informationssicherheit

von Dr. Simon Hoff

Moderne Arbeitsmethoden zeichnen sich verstärkt durch mobile und nomadische Nutzung von IT-Ressourcen aus. Smartphones und Tablets sind in Folge seit geraumer Zeit zu einem Standardelement der IT-Infrastruktur geworden. Klassische PCs verlieren dabei als Endgeräte zunehmend an Bedeutung. Inzwischen ermöglicht das mobile Internet den Zugriff auf die gesamte Anwendungsvielfalt der IT durch mobile Endgeräte und liefert insbesondere im Bereich Unified Communications & Collaboration (UCC) einen erheblichen Mehrwert. Damit werden automatisch sehr sensible Daten, z.B. vertrauliche personenbezogene Daten, auf mobilen Endgeräten verarbeitet und auch gespeichert.

Als Konsequenz ist die Wichtigkeit der Absicherung mobiler Endgeräte und ihrer Einbindung in die IT-Infrastruktur enorm gestiegen. Gleichzeitig zeigen gerade die populären mobilen Betriebssysteme wie Android und iOS immer wieder signifikante Schwachstellen auf und auch die Anbindung mobiler Endgeräte über Mobilfunk und WLAN hat immer wieder ihre Tücken.

weiter Seite 22

Geleit

Cisco unter Druck: symptomatisch für die Branche?

ab Seite 2

Standpunkt

Viel hilft viel – oder etwa nicht?

auf Seite 21

Aktuelle Kongresse

Netzwerk-Forum 2014

ab Seite 15

IT-Sicherheits-Forum 2014

ab Seite 4

Zum Geleit

Cisco unter Druck: symptomatisch für die Branche?

Umsatzrückgang, Personalabbau, neue Geschäftsbereiche werden wieder abgestoßen: Cisco ist sicherlich im Moment ein Gesprächsthema. Die Frage ist dabei, wie die Lage wirklich ist und in welchem Umfang das ein Abbild der ganzen Branche ist. Wir arbeiten im Moment an einem Exklusiv-Video zu diesem Thema, das für die Teilnehmer des ComConsult Netzwerk Forums 2014 gedacht ist (wenn Sie das Thema interessiert, das Video gibt es nur für Teilnehmer, sorry :-)). Trotzdem an dieser Stelle einige Gedanken dazu.

Die Kernfrage seit der Entwicklung der ersten Netzwerke ist die Frage, welchen Bedarf Unternehmen eigentlich an Netzwerken haben. Und damit verbunden natürlich die Frage, was passiert, wenn dieser Bedarf gedeckt ist, wir also in einen gesättigten Markt mit einem reinen Ersatzbedarf auslaufender Produkte kommen. Der Bedarf nach Netzwerken hängt dabei direkt ab von den Veränderungen in der Gesamt-IT. Die Ablösung der Terminals an Großrechnern und die Einführung von PCs haben zum Beispiel eben einen Bedarf für eine flächendeckende Netzwerk-Versorgung erzeugt. Die Applikationen wurden immer komplexer, die Rechner immer schneller und immer Daten mussten transportiert werden. So waren die 90er Jahre eine Zeit, in der der Bedarf immer vor den Produkten marschierte. Es war eine krasse Mangelsituation. Die Hersteller lebten davon schneller zu sein. Der Schlüssel lag in der Entwicklung neuer ASICs, die dem erhöhten Bandbreitenbedarf gerecht werden konnten.

Für lange Zeit ließ sich denn auch der Kernbedarf auf Bandbreite und Verfügbarkeit reduzieren. So entstanden die Gigabit-Netzwerke, die heute die Norm sind. Aber auch innerhalb der modernen Netzwerke gibt es Bereiche, in denen sich der Bedarf kaum noch bewegt. Dies ist seit über 10 Jahren der Access-Bereich. Hier hat sich 1 Gigabit-Ethernet zur Anbindung von Desktop-PCs etabliert und diese Kapazität ist ausreichend. Bewegung gibt es hier schon seit langer Zeit nicht mehr. Damit ist der Access-Bereich statisch geworden, er ist im Prinzip austauschbar. Die eingesetzten ASICs sind langweilig und die benötigten Verfügbarkeits-Verfahren bewährt und ausreichend. Entsprechend sind die Portpreise für diesen Versorgungsbereich völlig zusammen gebrochen. Zumindest an der Hardware lässt sich sicher kaum noch Geld verdienen.

Damit entstehen zwei Fragen:

- Wie sieht die aktuelle Bedarfssituation insgesamt aus, laufen wir in eine Sättigung und Stagnation? Kaufen wir unsere Switches in Zukunft lieber direkt als anonyme Massenprodukte in China so wie das im Moment der große Trend im Server-Markt ist (ausgelöst durch die Googles und Facebooks dieser Welt)?
- Wie gehen die Hersteller mit einer zunehmenden Sättigung des Marktes um?

Die Antwort zur ersten Frage liegt in der Weiterentwicklung der Gesamt-IT. Stagnieren IT-Architekturen, dann gibt es auch keinen Bedarf für neue Produkte. Der Markt für Server und PCs ist ein prominentes Beispiel dafür. Wenn IBM PCs und x86-Server an Lenovo verkauft werden, dann spricht das eine deutliche Sprache. Aber trotzdem gibt es natürlich Veränderungen. Wer also die Zukunft der Netzwerke und der gesamten Branche verstehen will, der muss sich mit der Weiterentwicklung der IT befassen. Hier liegt der Schlüssel. Dr. Kauffels wird dies in der Keynote zum Netzwerk Forum 2014 machen und er hat einige interessante Statements entwickelt.

Tatsache ist, dass wir weiterhin Veränderungen in unseren IT-Architekturen haben. Herausragend sind die Bereiche:

- Virtualisiertes und konsolidiertes Rechenzentrum
- Cloud-Services
- Mobile Endgeräte

So hat zum Beispiel die Trennung von Server und Speicher in Form von SAN und NAS den Bedarf nach Low-Latency-Bandreite in den Rechenzentren explodieren lassen. Damit geht die Spanne zwischen Access-Bandbreite und RZ-Bandbreite immer weiter auseinander. Während wir am Desktop mit 1 Gigabit zufrieden sind, diskutieren wir über 100 Gigabit im RZ.

Ohne das weiter vertiefen zu wollen, ist die Antwort auf die erste Frage, dass es weiterhin einen Bedarf nach Netzwerken gibt, dass aber das Netzwerk als Ganzes sich zu einem Gebilde aus Detailbausteinen mit stark unterschiedlichen Anforderungen entwickelt. Damit wird auch das Design immer komplexer, da scheinbar unbedeutende Änderungen in der IT-Architektur erhebliche Auswirkungen auf das Netzwerk-Design haben. So ist ein Campus-Netzwerk, das im Kern Desktop-PCs auf Anwendungen im RZ zugreifen lässt, in sich trivial. Aber sobald wir mit mehr als einem Rechenzentrum arbeiten und zwischen den verteilten RZs Daten transportieren müssen, explodieren die Anforderungen an Netzwerke. Noch komplexer wird das bei modernen verteilten Web-Applikationen, die über eine dynamische Zahl von virtuellen Maschinen skalieren. Diese Applikationen werden in Zukunft sehr stark an Bedeutung gewinnen, da sie unsere mobilen Endgeräte versorgen und zugleich die neue Applikations-Infrastruktur für unsere Kunden bilden. Diese Art von IT stellt selbst IP-Technologie auf den Prüfstand. Wir müssen uns mit der Frage von wandernden IP-Adressen über Subnetzgrenzen hinaus befassen und eine Lösung dafür haben (Cisco hat dafür LISP eingeführt, um ein Beispiel zu nennen). Das Problem kombiniert mit der Lösung ist ein sehr weitreichendes, da es den gesamten Zusammenhang von IP-Adressen und Strukturen neu definiert.

Also die Antwort auf die erste Frage ist: ja, es gibt weiterhin Bedarf, aber der ist nicht auf einen Bandbreitenbedarf trivialisierbar.

Das führt uns zur zweiten Frage: was machen die Hersteller? Nun, seit der Frühphase der Netzwerke ist das Hauptinstrument der Hersteller die Kundenbindung, also die Schaffung von Abhängigkeiten, die so groß sind, dass Kunden nicht zu einem anderen Hersteller wechseln. Am Anfang war das für die Hersteller einfach. Wer nur schnell genug neue Bandbreite lieferte, der konnte die Kunden binden. Kombiniert man das mit einem speziellen Management der Geräte, dann entsteht

Cisco unter Druck: symptomatisch für die Branche?

eine Barriere, die den Wechsel zu einem anderen Anbieter erschwert. Nun sind die Bandbreiten aus heutiger Sicht kaum noch spannend und das Management der Geräte ist so ähnlich geworden, dass viele Unternehmen mit Zwei-Hersteller-Strategien arbeiten und damit auch keine Probleme haben, im Gegenteil. Aber die Hersteller sind natürlich erfinderisch. So gibt es eine ganze Latte von neuen Möglichkeiten der Kundenbindung, einige Beispiele sind:

- Neue Redundanzverfahren wie TRILL und deren proprietäre Umsetzung
- Verfahren wie LISP, zu denen es einen Bedarf, aber noch keinen Standard gibt
- Eine Integration von Wireless und Wired, auch um die reinen Wireless-Anbieter auszublocken
- Eine Integration von Endgerätemanagement, speziell eine Integration von mobilen Endgeräten mit verkabelten Endgeräten
- Der gesamte Sicherheitsbereich
- Die Integration von weitergehenden Services in modulare Switches

Vereinfacht gesagt arbeiten die Hersteller - allen vorweg Cisco - mit der Strategie, ein so umfangreiches und verknüpftes Gesamtsystem aus Hardware, Software und Services zu schaffen, dass Kunden nicht zu anderen Herstellern wechseln können. Cisco geht tatsächlich noch einen Schritt weiter und sieht seine Zukunft in Gesamtarchitekturen aus Applikation, Netzwerk und Sicherheit. Je umfangreicher die Verknüpfung wird, je breiter die Architektur, desto intensiver die Bindung, desto höher die Hürde für Konkurrenten.

Hier kommt die wirkliche Bedrohung von Software Defined Networking SDN ins Spiel. Die Bedrohung liegt nicht wie vielfach angenommen in deutlich preiswerteren Switch-Systemen. Diese Situation haben wir heute schon, wer Switches mit deutlich niedrigeren Portpreisen kaufen will, der wird auch einen passenden Anbieter finden. Die Zukunft des Netzwerk-Marktes liegt nicht in einem Preiskampf.

Der Schlüssel zum Verständnis der Tragweite von SDN liegt darin, dass SDN die Verbindung von Hardware, Software und Service aufbricht und unabhängige Bereiche schafft. Es gibt eben in SDN Switches, Controller und Applikationen. Und die können von verschiedenen Herstellern kommen (theoretisch, dieser Kampf läuft gerade im Hintergrund ab).

Die Folge: mit SDN verlieren Hersteller wie Cisco ihre Chance, Abhängigkeiten gezielt zu konstruieren und Kunden zu binden. SDN ist der Kampf einer offenen Lösung gegen geschlossene Bindungen. Kombiniert man das noch mit OpenStack, dann entsteht eine weitreichende Architektur mit autonomen Elementen bis in die Applikations-Schicht. Das sieht auch die Börse in New York so und beobachtet dementsprechend die Entwicklung und speziell die Auswirkung auf Cisco mit großer Sorge. Um kein Missverständnis aufkommen zu lassen: Cisco ist sicher nicht in Gefahr. Es geht hier um die Frage, wie groß das Unternehmen ist und wird und wie profitabel es dabei ist. So wie Microsoft sicher nicht verdrängt werden kann, aber Bereiche wie Windows hat, die mit großen Fragezeichen versehen werden müssen, so muss sich auch Cisco neu positionieren. Und die große Frage ist, wie das funktionieren kann. Die Lage für die anderen Anbieter ist dabei durchaus anders. Für die anderen Anbieter ist die aktuelle Situation eine große Chance, in die Bindungsmechanismen von Cisco eingreifen zu können und sich damit eine größere Scheibe vom Kuchen abschneiden zu können. Das erklärt, warum HP und Extreme so intensiv an SDN mitwirken.

Wie sehen die nächsten Jahre aus? Wer werden Verlierer und Gewinner sein? Dies ist das Thema unseres Exklusiv-Videos für die Teilnehmer des ComConsult Netzwerk Forums 2014.

Ihr
Dr. Jürgen Suppan

Kongress

ComConsult Netzwerk Forum 2014
24.03. - 26.03.14 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.

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?

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?

Moderation: Dipl.-Inform. Petra Borowka-Gatzweiler, Dr.-Ing. Behrooz Moayeri
Preise: € 2.390,-- netto

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

Aktueller Kongress

ComConsult IT-Sicherheits-Forum 2014

15.05. - 16.05.14 in Bonn

Die ComConsult Akademie veranstaltet vom 15.05. bis 16.05.14 ihr "ComConsult IT-Sicherheits-Forum 2014" in Bonn.

Für die IT-Sicherheit sind Cloud, Smartphones, Tabletts, IPv6, Internet of Things aktueller denn je. Risiken und Lösungen werden auf dem ComConsult IT-Sicherheits-Forum diskutiert.

Die Informationssicherheit muss stets flexibel und schnell auf neue Informationstechnologien reagieren. Idealerweise gestaltet sie die neue Technologie möglichst frühzeitig mit. Wir werden uns bei dem diesjährigen IT-Sicherheits-Forum neben Best Practice in der Informationssicherheit daher mit folgenden aktuellen Themen befassen:

- Cloud Computing – anfänglich für den Enterprise-Bereich mehr belächelt als tatsächlich genutzt – ist inzwischen die strategische Ausrichtung für IT-Dienstleistungen geworden.

  Virtualisierungstechniken bilden die Basis für Cloud Computing. Das Data Center in a Box ist keine Vision mehr. Verschiedenste hochgradig dynamische komplett virtuelle IT-Infrastrukturen (d.h. Clients, Server, Netz und Storage), die gemeinsam auf einer physikalischen Hardware laufen, sind längst Realität.

  Sicherheitsmaßnahmen müssen sich daher stärker auf die Virtualisierungslösungen und die Anwendungen selbst konzentrieren.

- Plattformen für Unified Communications (UC) und für Collaboration wachsen zu UCC zusammen. Es bestehen hier erhebliche Anforderungen der Nutzer hinsichtlich eines flexiblen Datenaustauschs zwischen Unternehmen und Behörden. Die Absicherung von UCC muss dem gerecht werden.

- Im sogenannten Internet of Things erfassen Dinge (Things) – nicht Menschen wie im „Internet of Humans“ – Informationen, sind per IP vernetzt und stellen Informationen für andere Dinge oder Menschen zur Verfügung. Dahinter stecken natürlich unterschiedlichste Systeme und Anwendungen, bei denen Sensoren, Maschinen, Steuerungen, Fahrzeuge, etc. über IP untereinander und mit der Infrastruktur kommunizieren.

Sicherheitsvorfälle im Internet of Things können erhebliche Folgen haben und der Schutz der „Things“ und ihrer Kommunikation ist daher von besonderer Bedeutung.

Parallel zu diesen strategischen Entwicklungen haben wir in den letzten Monaten in einem gewissen Sinne das Ende der Privatheit bzw. Vertraulichkeit in der Informationstechnik erlebt: Es verging kaum noch eine Woche ohne das Bekanntwerden neuer qualitativ hochwertiger Spionage-Schadsoftware, neue trickreiche Lauschattacken und die Aufdeckung zugehöriger Schwachstellen in IT-Systemen. Außerdem haben sich immer mehr Abgründe in der grenzenlosen Überwachung der Kommunikation im Internet (und nicht nur dort) aufgetan.

Aus diesen Gründen konzentriert sich das IT-Sicherheits-Forum 2014 auf folgende Themenbereiche:

- Für den Nutzer einer virtuellen IT im Zeitalter des Cloud Computing muss sich die Informationssicherheit auf ihren Namen besinnen und Sicherheitsmaßnahmen müssen sich auf die Informationen selbst konzentrieren. Kernelemente sind nicht nur die Zusicherung von Vertraulichkeit und Authentizität durch Verschlüsselungstechniken sondern immer mehr auch die Nachvollziehbarkeit von Änderungen an Daten (Revisionsfähigkeit) und die Kontrolle von unerwünschtem Abfluss von Daten, d.h. letztendlich Klassifikation von Daten in Verbindung mit Data Loss Prevention.

- Die Absicherung von UCC muss verstärkt den Aspekt der Zusammenarbeit unterschiedlicher Unternehmen und Behörden berücksichtigen. Hier sind nicht nur Maßnahmen zur Absicherung von Voice und Video gefragt. Sicherheitsmaßnahmen müssen alle Kommunikationskanäle in UCC berücksichtigen, vom Chat, über Anwendungs- und Desktop-Sharing bis zum flexiblen Dokumentenaustausch.

- Wenn unterschiedliche, heterogene Gruppen von Nutzern und Geräten auf unterschiedlichem Sicherheitsniveau eine gemeinsame IT-Infrastruktur nutzen, muss diese in einem gewissen Umfang mandantenfähig sein. Dies erfordert stets die sichere Trennung der Informationen der Mandanten.

- Die traditionelle Methode der Informationssicherheit einer möglichst physikalischen Trennung auf Ebene des Netzes und der Endgeräte ist nicht mehr zeitgemäß. Virtualisierung erfordert ein Umdenken in Richtung logischer Trennung und insbesondere in Richtung kryptographischer Techniken.

- Zonenkonzepte in RZ und Campus sind zu einem normalen Gestaltungsinstrument geworden, stellen aber durch ihre Komplexität höchste Ansprüche an Planung und Betrieb. Schwerpunkte sind dabei die logische Trennung von Zonen in Virtualisierungsplattform, Netz und im Storage-Bereich.

- Wir benötigen sichere Identitäten in IP-Netzen und auf dieser Basis eine Netzzugangskontrolle mit dynamischer Berechtigung von Zugriffen

ComConsult IT-Sicherheits-Forum 2014

Frühbucherrabatt bis 31.03.14

Wir bieten Ihnen für das ComConsult IT-Sicherheits-Forum 2014 bis zum 31.03.2014 eine Vorbuchungsphase für eine rabattierte Teilnahmegebühr an:

vom 15.05. bis 16.05.14 in Bonn € 1.790,--* netto (statt € 1.990,-- netto)

Die Buchung innerhalb der Frühbucherphase kann nicht storniert werden. Gerne akzeptieren wir aber einen Ersatzteilnehmer.

Fax-Anmeldung
02408/955-399 oder 02408/955-398

Hiermit melde ich mich verbindlich zum **ComConsult IT-Sicherheits-Forum 2014** an.

☐ **Kongress**

vom 15.05. bis 16.05.14 in Bonn zum Preis von € 1.790,-- netto*
*gültig bis zum 31.03.2014

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

vom _____ bis zum _____14
im Günnewig Hotel Bristol Bonn zum Sonderpreis von 112,-- € inkl. Frühstück

_____
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

Schwerpunktthema

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

Teil 2

Fortsetzung von Seite 1

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

Hierfür sind jedoch Access Switches erforderlich, die mehr als zwei 10 Gbit Interfaces bereitstellen können (zum Beispiel vier fixe 10G Schnittstellen oder ein Uplink-Modul mit mehr als zwei 10G Schnittstellen. Soweit das Gebäude als einzelner Ring implementiert ist, macht es keinen Sinn, die Campus-Verbindung mit mehr als 10 Gbit zu bestücken, da ja die Ringleistung nicht mehr als 10 Gbit erbringt.

Soll der Ring innerhalb des Gebäudes abgeschlossen werden oder sollen mehrere Ringe im Gebäude implementiert werden, was sich bei einer größeren Anzahl Switches anbietet, können am Gebäude-Campus-Übergang nichtmodulare Layer-3 Switches zum Einsatz kommen, die Layer-2 Multipath zum Campus hin terminieren. Werden mehrere Ringe implementiert, kann die Campus-Anbindung bei entsprechendem Leistungsbedarf mit 40 Gbit bestückt werden – hier ist wiederum ein nichtmodularer Switch mit entsprechenden Schnittstellen-Möglichkeiten (mehrere 10G und mindestens eine 40G Schnittstelle) erforderlich.

Durch die ringförmige Verteilung der Gebäude-Campus-Anbindung auf mehrere Switches anstelle zweier zentraler Core Switches, lassen sich statt großer modularer Switches geeignete nichtmodulare Komponenten einsetzen, wobei jeder Campus-Switch mehrere Gebäude über 10 Gbit anbindet und der Campus-Ring mit n x 10G oder n x 40G ausgelegt ist, je nach Möglichkeit der eingesetzten Switches. Sofern das Gelände eine Ringtrasse für die Verkabelung hat, ist der Ring auch hinsichtlich Bedarf an LWL-Fasern optimal implementierbar.

Auch im Rechenzentrum lassen sich mit Layer-2 Multipath Verfahren Sternstrukturen durch Ringe ersetzen, was wiederum den Einsatz teurer modularer Konzentrator-Switches einsparen kann. Das Beispiel aus Abbildung 4.4 zeigt, wie durch eine Ring-Schaltung von Top-of-Rack (ToR) Switches mit 1fach 100Gbit die End-of-Row (EoR) Konzentrator-Switches vermieden werden. Eine Anbindung der ToR-Ringschaltung an den Campus Core ließe sich realisieren, indem die Core Switches einfach in den Ring eingefügt werden. Dies bedeutet jedoch, dass einige aktive Wege auch die Core Switches für Server-Server Verkehr mit nutzen, sofern diese nicht mittels hoher Kostensetzung "unbrauchbar" gemacht werden. Letzte-

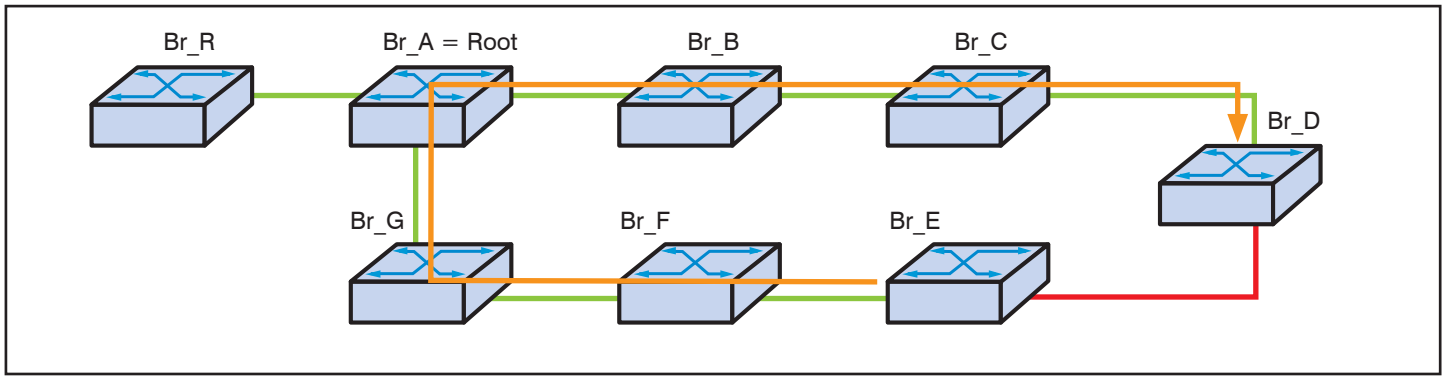


Abbildung 4.1: Probleme mit Ring-Design bei Spanning Tree

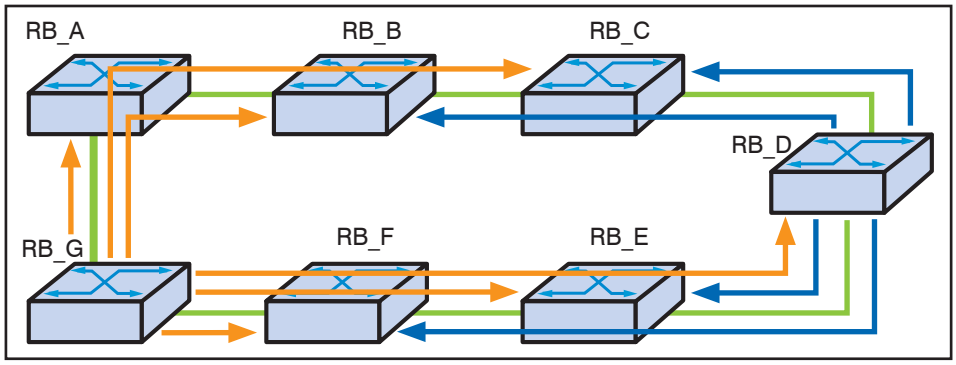


Abbildung 4.2: Lastverteiltes Ring-Design bei Layer-2 Multipath

Netzwerk-Design in Zeiten von 10/40/100 Gbit: Wie sieht die Zukunft aus? - Teil 2

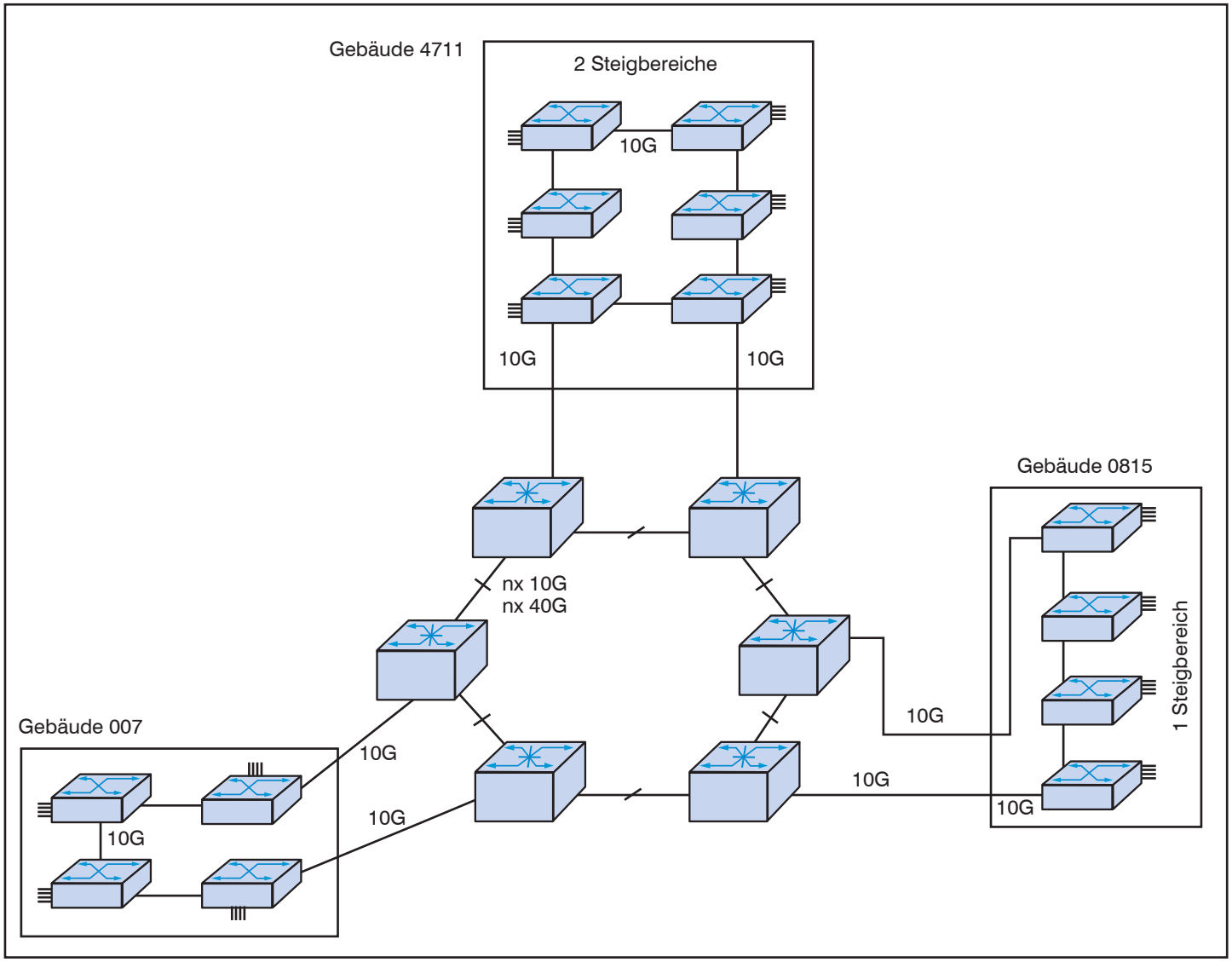


Abbildung 4.3: Campus und Gebäude mit Ring Design

res führt jedoch für die Nachbar-Switches der Cores wieder zu recht ungünstigen Wegen. Um beides: ungünstige Wege und Belastung der Cores mit Server-Server Verkehrslasten zu vermeiden, wird der Ring zwischen Server Access Switches geschlossen, und im Regelfall zwei, bei höherem Leistungsbedarf auch mehr Server Access Switches erhalten eine separate Anbindung an die Campus Core Switches, wie Abbildung 4.6 zeigt.

Da 40G zur Zeit in mehr Produkten verfügbar ist als 100G, zeigt das nächste Design-Beispiel ein 40 Gbit Design: In Abbildung 4.5 sind mehrere Server Access Switches mit einem 40G oder mehrfach 40G Ring verbunden. Solche Ringe können mit entsprechenden LWL-Interfaces auch über zwei Rechenzentren an verschiedenen Campus-Standorten verteilt werden. Je nach Routing-Bedarf kommen hier nichtmodulare Layer-2 oder Layer-3 Switches zum Einsatz. Eine Übersichtsgrafik mit Ring-Design für RZ und Campus ist in Abbildung 4.6 dargestellt.

In Abbildung 4.7 ist eine Bewertungsübersicht des Fat Tree Designs dargestellt.

Ring-Designs sind hinsichtlich der definierten Durchsatz-Leistung zwischen jeweils zwei Ring-Elementen schwerer kalkulierbar, kosten jedoch vergleichsweise wenige Switch-Interfaces und ermöglichen den Einsatz nichtmodularer Konzentrator-Komponenten. Sie stellen daher eine kostengünstige Alternative zum Baum-/Stern-Design dar.

5. Design-Elemente: Masche, Hybrid-Design

Wie der Name Hybrid-Design schon nahelegt, sind vermaschte Netzdesigns eine im Prinzip beliebige Kombination von Quer-Verbindungen, die je nach Leistungsbedarf und Verkabelungs-Möglichkeiten – hier gibt es hauptsächlich im Campus ja vielfältige Einschränkungen hinsichtlich Trassenführung, Fasernzahl und OM Fasernklasse – völlig flexibel konfiguriert werden können. In diesem Sinne lassen sich auch Fat Tree Designs zu den Maschen-Designs rechnen.

Genau wie Ring-Designs sind vermaschte Designs nur beim Einsatz von Multipath-Verfahren sinnvoll nutzbar. Ein klassisches Multipath Verfahren ist beispielsweise OSPF ECMP bei gerouteten Verbindungen, für Layer-2 Bereiche stehen SPBM und TRILL als Layer-2 Multipath Standards zur Verfügung.

Besonders interessant sind vollvermaschte Designs (Matrix-Designs), da sie die höchste Leistung und höchste Blockierungsfreiheit ermöglichen. Trotzdem erfordern sie nicht zwingend den Einsatz

Netzwerk-Design in Zeiten von 10/40/100 Gbit: Wie sieht die Zukunft aus? - Teil 2

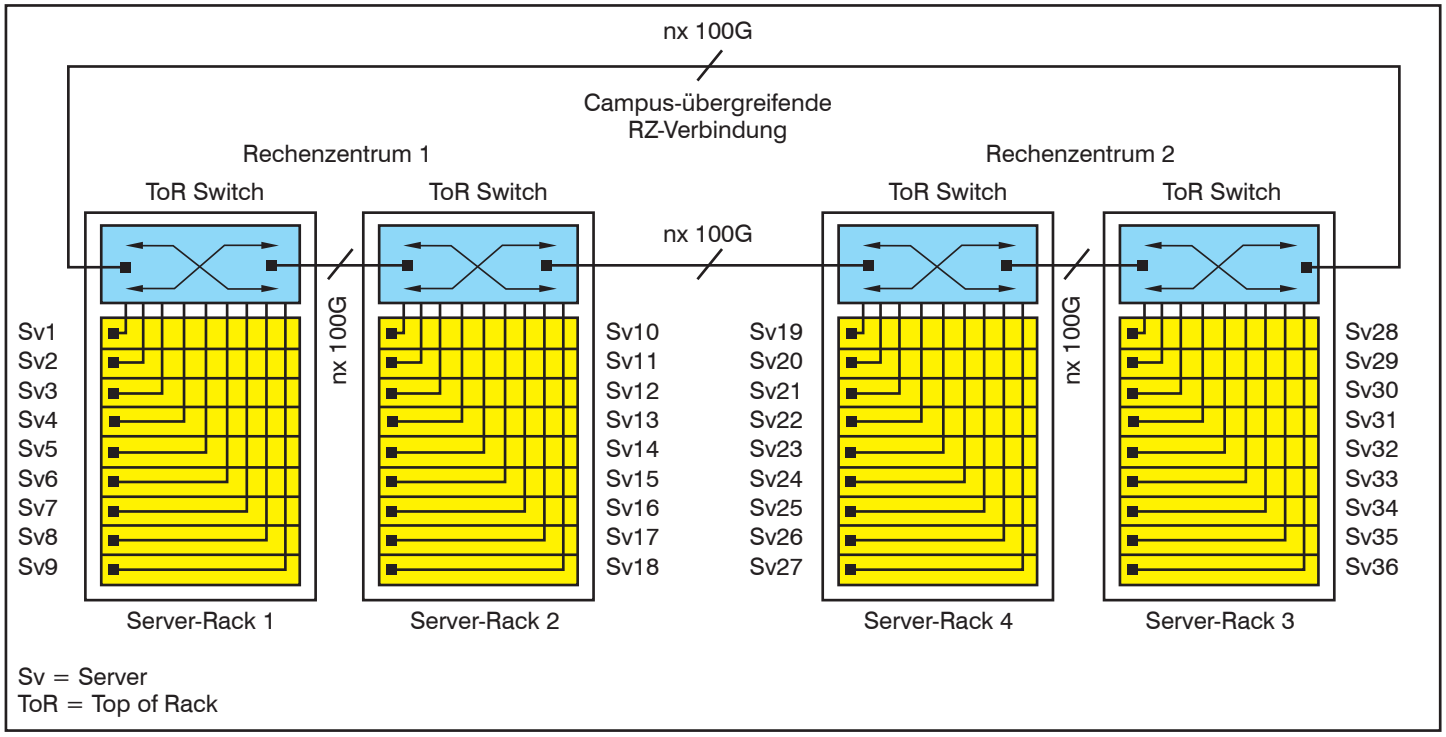


Abbildung 4.4: Einsparung des EoR Switches durch Ringschaltung der ToR Switches im RZ

teurer modularer Komponenten. Abbildung 5.1 zeigt eine vollvermaschte Konfiguration mit sechs nichtmodularen Serverswitches, die jeweils fünf Verbindungen zu den jeweils fünf anderen Serverswitches haben (das konkrete Produkt unterstützt sechs Uplinks, da ja auch noch die Core- / Campus-Verbindung erforderlich ist. Bei 40 Gbit Uplinks sind dies in Summe 200 Gbit fdx Querverbindungs-Leistung. Die Überbuchung ist durch die Anzahl angebundener Server bestimmt: Da die Server vorzugsweise redundant an jeweils zwei Serverswitches angeschaltet werden, rechnen wir mit einer Uplink-Leistung von 400 Gbit (zwei Switches mit jeweils 5-fach 40 Gbit). Unterstellen wir, dass jeder physische Server (Host) mit 2-fach 10 Gbit angeschaltet ist, so können 20 Server acitive / active oder 40 Server active / passive angeschaltet werden. Auch bei Ausnutzung von 48 Serverports (das ist die typische Switchbestückung) liegt mit Faktor 1,2 eine sehr moderate Überbuchung vor, die sich in den allermeisten Fällen problemlos verhalten wird.

Auch Fat Trees sind ein vermaschtes Netzdesign, das insbesondere blockierungsfreie 2-Tier Konnektivität zwischen allen angeschlossenen Endsystemen (im Regelfall Server) leistet. Bei einer hohen Anzahl angeschlossener Serverswitches müssen die Aggregierungs-Switches jedoch vielfach wegen der erforderlichen hohen Portkonzentration modulare Komponenten sein (siehe auch Abbildung 5.2). In diesem Fall ist der Fat Tree die teurere Variante im Vergleich zur nichtmodularen Vollvermaschung, die zuvor beschrieben wurde.

Da eine Vollvermaschung eine vergleichsweise hohe Anzahl physischer Querverbindungen erfordert, sind in Gebäude- und Campus-Bereichen die Verkabelungs-Voraussetzungen meistens nicht gegeben, insbesondere im Campusbereich wären zudem aufgrund der hohen Entfernungen die 40 Gbit Verbindungen aufgrund der erforderlichen Single Mode Interfaces vergleichsweise teuer. Ein Maschenkonzept im Campus ist eher als Ring-Stern mit einer sternförmigen Anschaltung der Gebäude an den Campus Core / RZ-Zugang sowie Ringschaltung der Gebäude untereinander für Peer-Verkehr (Voice, Video, UC) denkbar. Natürlich können einzelne Verbindungen je nach Leistungsbedarf gedoppelt oder in der Datenrate erhöht werden (zum Beispiel von 40 Gbit auf 100 Gbit). Ein Gesamt-Netzwerk mit Kombination von Vollvermaschung im Rechenzentrum und Bedarfs-Vermaschung im

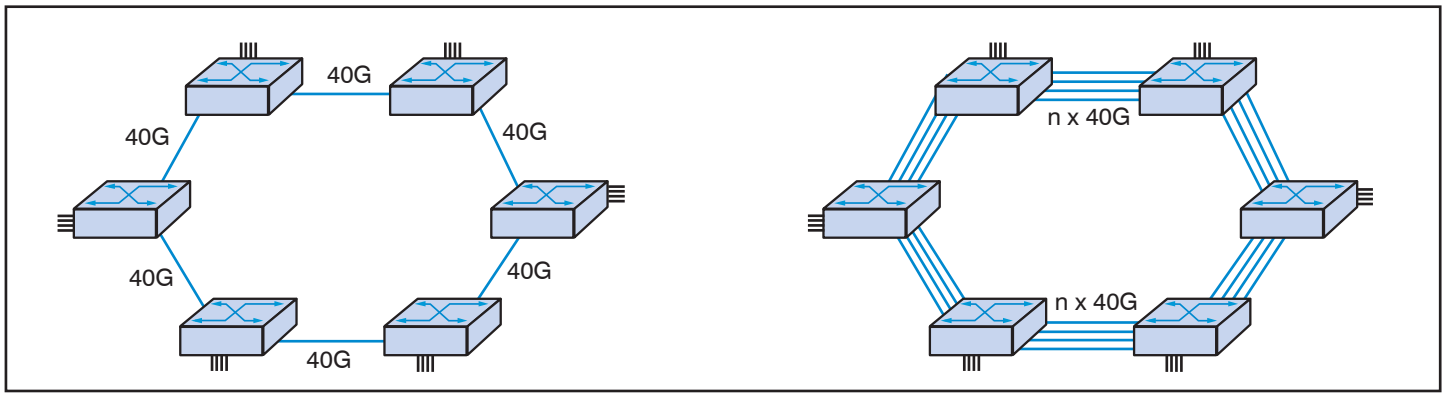


Abbildung 4.5: Data Center Einsatz-Szenarios mit Ring Design

Netzwerk-Design in Zeiten von 10/40/100 Gbit: Wie sieht die Zukunft aus? - Teil 2

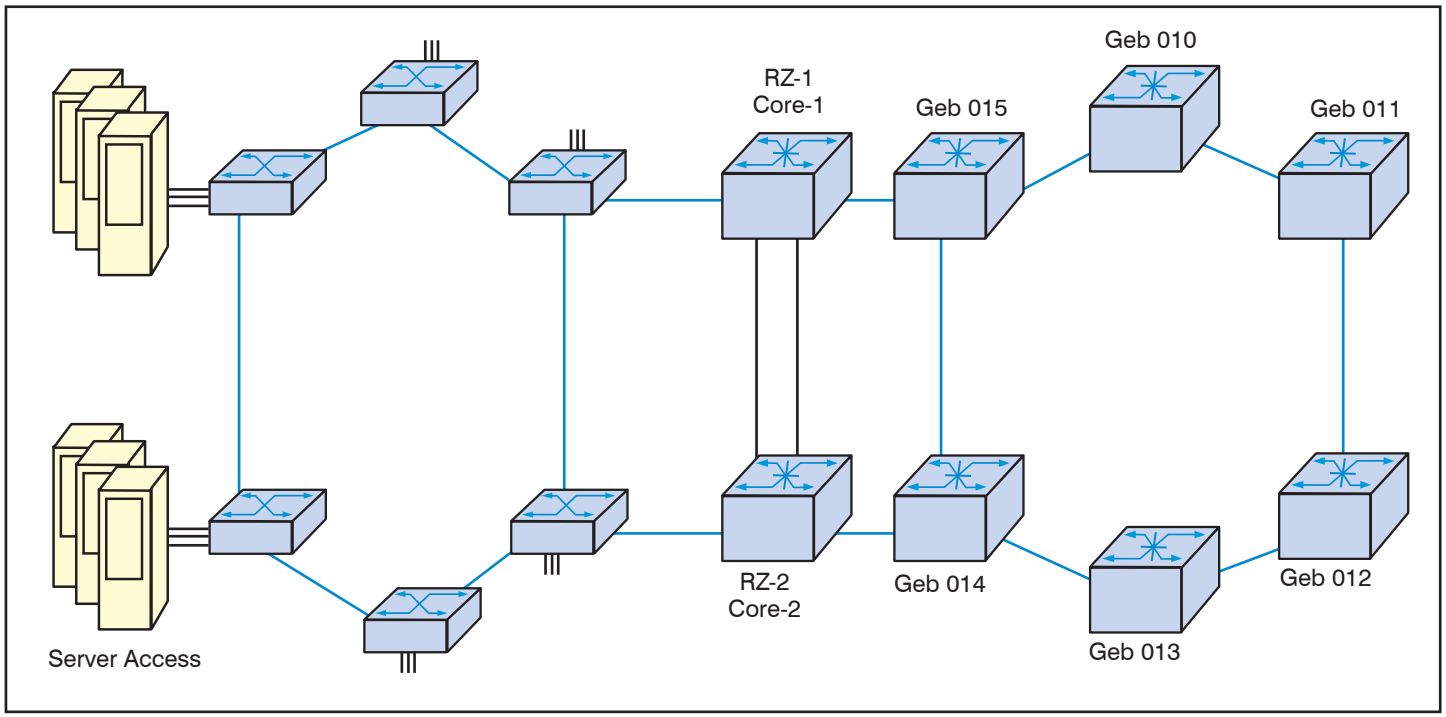


Abbildung 4.6: Data Center und Campus mit Ring Design

Ring-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	+
Summe					

Abbildung 4.7: Bewertung von Ring Designs

Netzwerk-Design in Zeiten von 10/40/100 Gbit: Wie sieht die Zukunft aus? - Teil 2

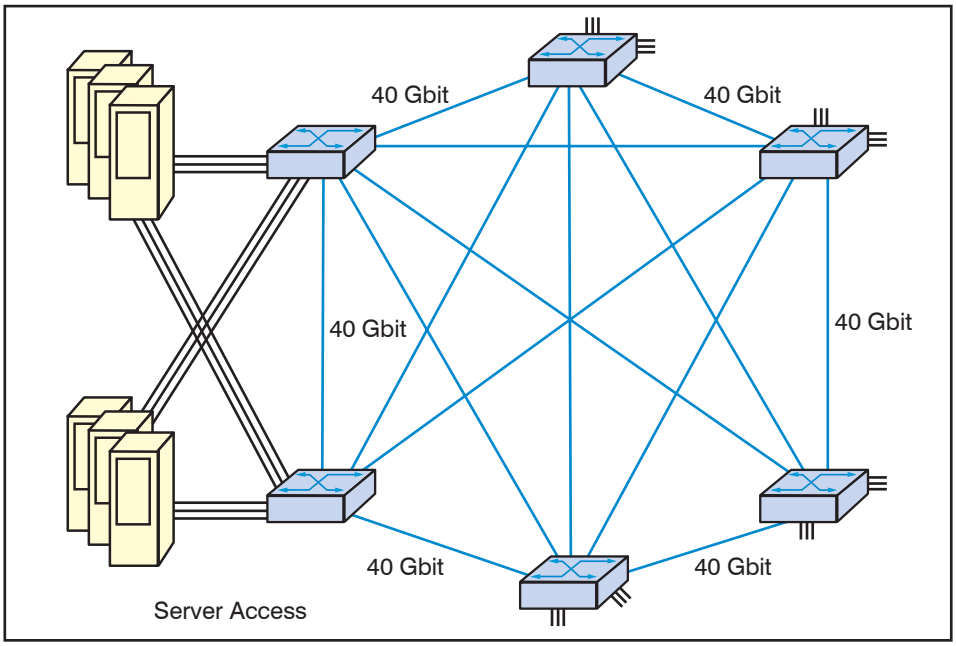


Abbildung 5.1: Vollvermaschtes Data Center Design, nichtmodulare Komponenten

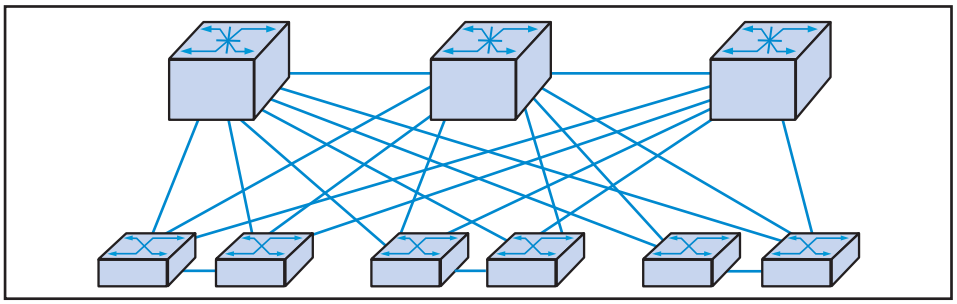


Abbildung 5.2: Fat Tree Data Center Design, modulare Aggregierung

Campus zeigt Abbildung 5.3. In diesem Beispiel wurden die Gebäude 011 und 013 aufgrund eines erhöhten Leistungsbedarfs mit einer doppelt so hohen Datenrate an den Campus / Core angeschaltet wie die anderen Gebäude. Die Gebäude-Anbindung an den Campus / Core ist mit 320 Gbit nicht überbucht, da der Core zum Rechenzentrum eine Leistung von 4-fach 100 Gbit hat. Eine Anschaltung von 1-fach 100 Mbit beider Cores würde zu einer Überbuchung von Faktor 1,6 führen, was sicherlich in vielen Fällen ebenfalls problemlos funktioniert. Bei einer einheitlichen Ausstattung mit 40 Gbit und folglich Core-Anschaltung an das Rechenzentrum mit 2-fach 40 Gbit ergibt sich eine Überbuchung von Faktor 2,0; auch hier sind im Regelfall keine Probleme zu erwarten. Die einheitliche Ausstattung mit 40 Gbit kann mangels Verfügbarkeit von 100 Gbit in einigen Produktlinien erforderlich oder aufgrund der Preispolitik für 100 Gbit sinnvoll sein.

In Abbildung 5.5 ist eine Bewertungsübersicht für vermaschte Designs dargestellt.

Als Sparvariante lassen sich in hybriden Design-Konzepten Maschen- und Ring-Konfigurationen sinnvoll miteinander kombinieren, insbesondere dann, wenn die Server-Server Verkehrslast erheblich höher ist als die Client-Server Verkehrslast. Ein entsprechendes Beispiel-Design zeigt Abbildung 5.4.

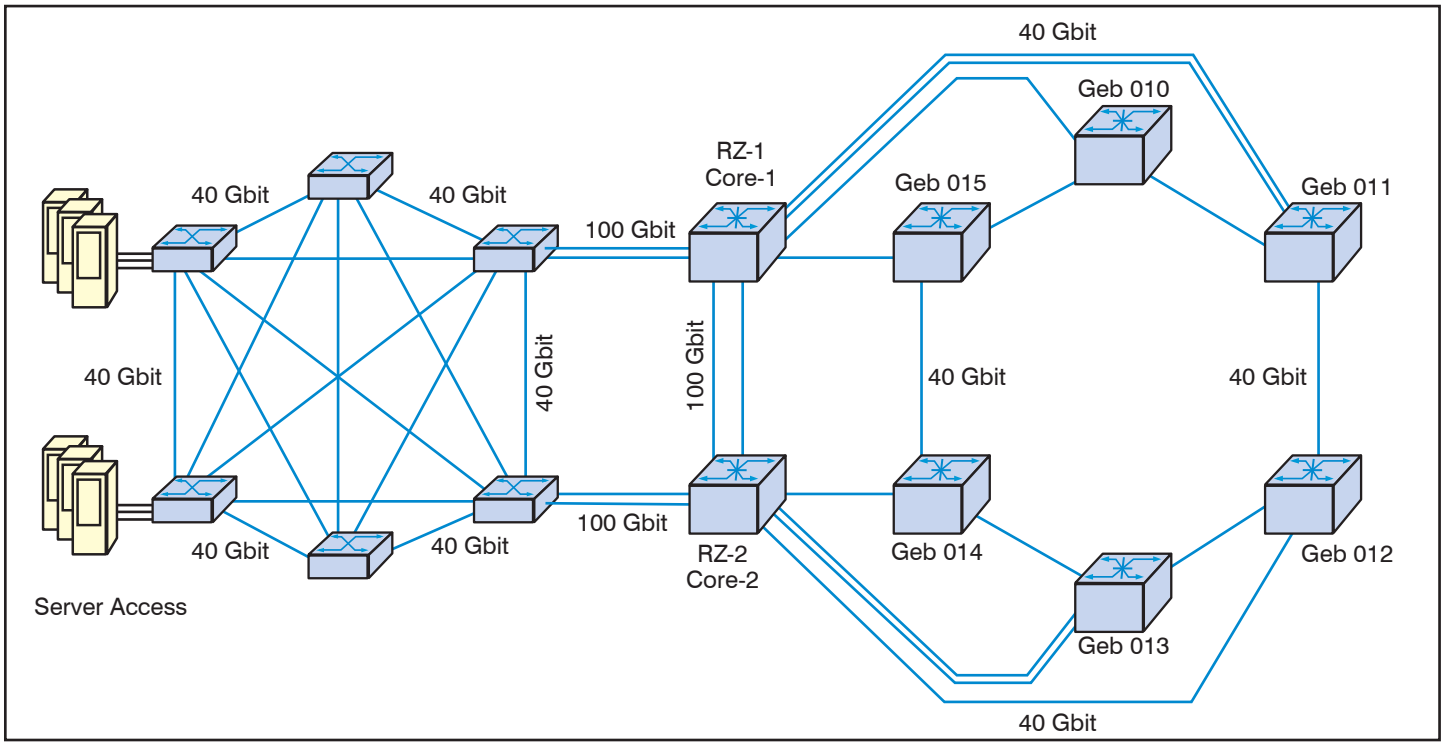


Abbildung 5.3: Vollvermaschtes Data Center und Campus mit Bedarfs-Vermaschung

Netzwerk-Design in Zeiten von 10/40/100 Gbit: Wie sieht die Zukunft aus? - Teil 2

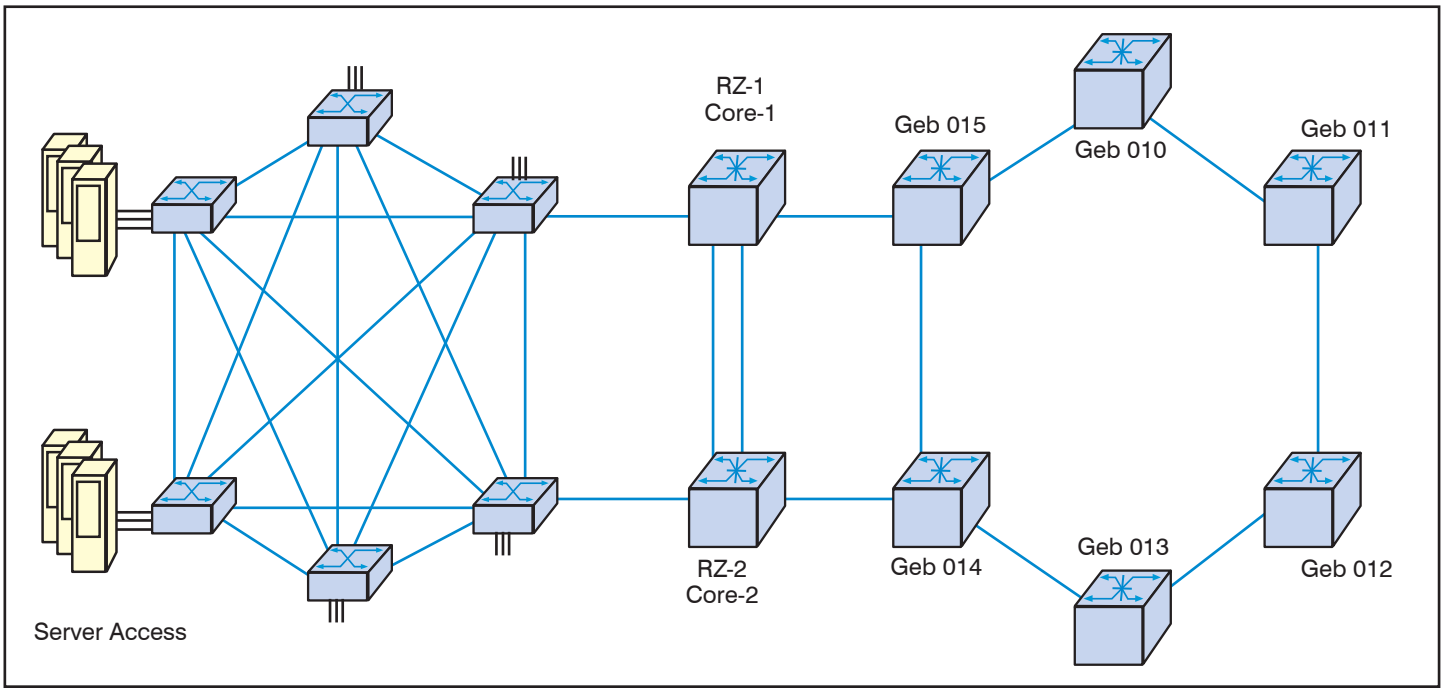


Abbildung 5.4: Vollvermaschtes Data Center und Campus mit Ring-Konfiguration

Vermaschtes 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	+
Summe					

Abbildung 5.5: Bewertung von vermaschten Designs

Netzwerk-Design in Zeiten von 10/40/100 Gbit: Wie sieht die Zukunft aus? - Teil 2

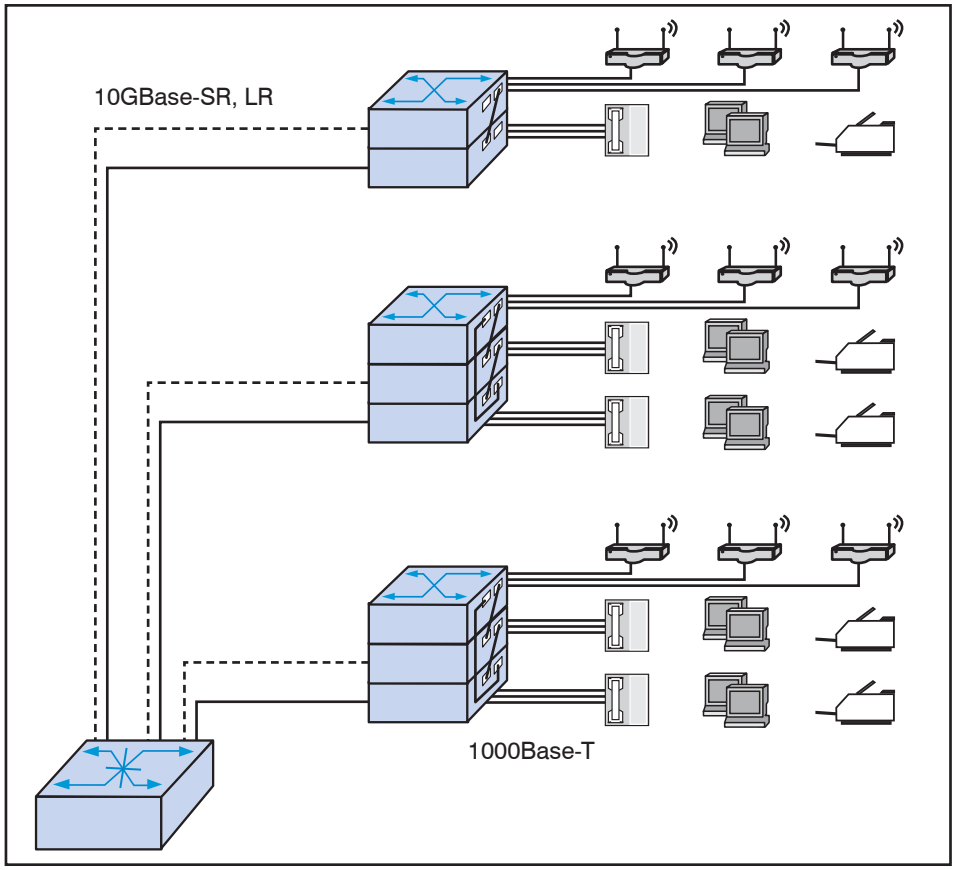


Abbildung 6.1: Beispiel-Design Access Bereich

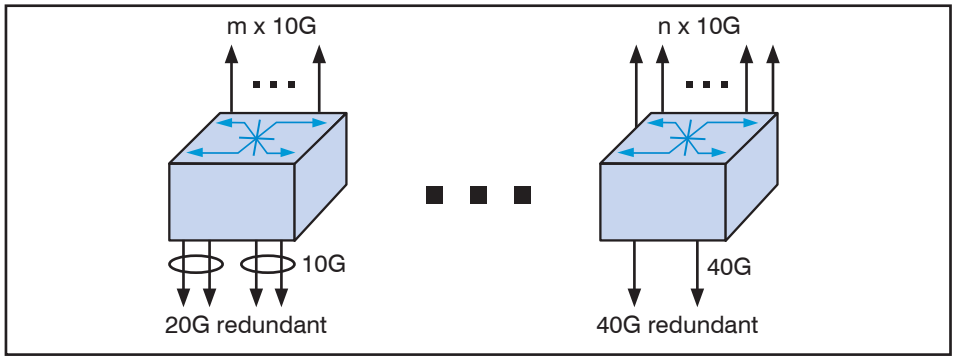


Abbildung 6.2: Beispiel-Design Gebäude-Konzentrationspunkt

6. Design-Regeln, generische Planung

Für ein gut funktionierendes Ende-zu-Ende Design ist insbesondere die Überbuchungs-Situation zu betrachten. Eine erste Daumenregel ist die 1:1 Regel: Die Summenleistung der RZ-Anbindung an das Campus-Netzwerk sollte etwa der Summendatenrate der Gebäude-Campus-Zugänge entsprechen: Bei einer Ausgangslage von 95% Client-Server Verkehrslast im Campus wird die Leistung des Campusnetzwerks im Wesentlichen nicht höher als die Server-Zugangsleistung sein, egal wie hochkarätig Sie das Campus Netzwerk auslegen!

Bei großen Netzwerken ist diese 1:1 Regel aus Kostengründen oft nicht mehr haltbar. Je größer die Gebäudezahl ist, desto höher kann die Überbuchung der Gebäude-Summenrate zum RZ-Zugang gewählt werden, da empirisch und unter Berücksichtigung der Warteschlangen-Theorie nicht davon auszugehen ist, dass alle Gebäude gleichzeitig einen Lastpeak generieren. Je größer die Serverzahl ist, desto höher lässt sich die Überbuchung des Server-Access Bereichs zum Campus Netzwerk planen, da sich typischerweise auch nicht alle Server gleichzeitig in einer Peaklast-Situation zu den Clients befinden. Die Netzwerk-Infrastruktur innerhalb des Data Centers ist so auszulegen, dass die Server-Server Verkehrslasten parallel oder zusätzlich zu den Client-Server Verkehrslasten bedienbar sind.

Access Bereich

Im Access Bereich etabliert sich 1 Gbit am Endgerät, 1 Gbit am WLAN AP (zukünftig mit 802.11ac 10 Gbit) kombiniert mit 10 Gbit Uplinks (siehe auch Abbildung 6.1). Als Sparvariante ist 1 Gbit am Endgerät / WLAN AP mit n-fach 1 Gbit Uplink an den Gebäude-Konzentrator oder Campus denkbar. Nach wie vor ist eine gute Einsetzbarkeit von Stack-Konzepten gegeben, bei Bedarf mit Link Aggregierung oder Ringschaltung. Im Access Bereich ist eine Überbuchung von 15:1 bis 30:1 in den meisten Fällen gut machbar, natürlich sollten die Uplinks entsprechend auf zu hohe Auslastung überwacht werden (mehr als 80% Auslastung legt eine Hochrüstung nah, konservative Netzbetreiber können die Schwelle auch niedriger setzen).

Wer Echtzeit-Anwendungen (VoIP, Video, UC) nutzen will, sollte sich an folgende Eckwerte halten:

- Voice / Video Delay: One Way Ende-zu-Ende 2 ms bis 100ms
- Jitter: One Way Ende-zu-Ende 1 ms
- Verlustrate: nahezu 0%
- PoE: die typische Leistung von kostengünstigen Switches ist nach wie vor 7,5W bis 15W pro Port, auch wenn einzelne Ports bis 30W einspeisen können

Campus Bereich

Als Aggregation / Distribution Switches im Gebäude kommen 10 Gbit Konzentratoren zum Einsatz. Die Gebäude-Anbindung wird auf n x 10 Gbit oder 40 Gbit migriert, wie in Abbildung 6.2 gezeigt. Überbuchungs-Faktoren von 2:1 bis 4:1 sind im Regelfall gut verkraftbar. Für Echtzeit-Anwendungen gelten wiederum die zuvor genannten Dienstgüte-Anforderungen hinsichtlich Delay, Jitter und Verlustrate.

Data Center

Die typische Netzwerk-Anbindung eines Host / Servers wird mit 1-fach bis n-fach 10 Gbit am Server geplant, somit lassen sich jeder VM n x 1 Gbit zuordnen. Auch hier gibt es für ältere Modelle noch die Sparvariante: n-fach 1 Gbit am Server, n x 1 Gbit Uplink am Server-Switch. Typischerweise kommen aber inzwischen n-fach 10 Gbit Uplinks oder 40 Gbit Uplinks am Server Access Switch zum Einsatz. Auch der einfache 10 Gbit Uplink am Server Access Switch ist inzwischen als Sparvariante zu bezeichnen. Überbuchungen von 2:1 bis 6:1 sind in den meisten Fällen gut realisierbar. Auslastungs-Überwachung der Uplinks schützt auch hier vor bösen Überraschungen. Eine Übersicht zeigt Abbildung 6.4.

Netzwerk-Design in Zeiten von 10/40/100 Gbit: Wie sieht die Zukunft aus? - Teil 2

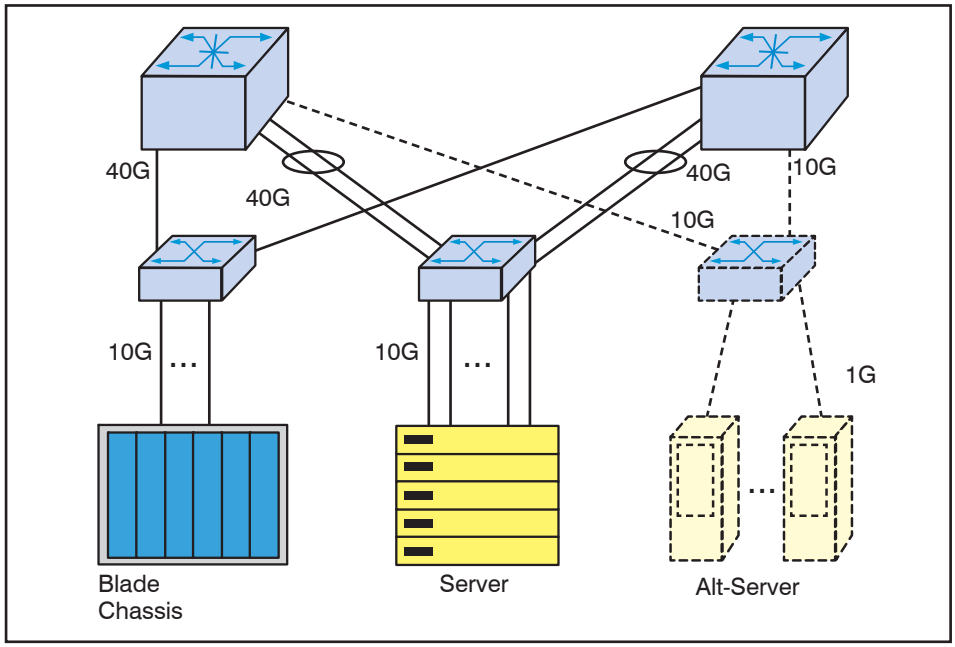


Abbildung 6.3: Beispiel-Design Data Center

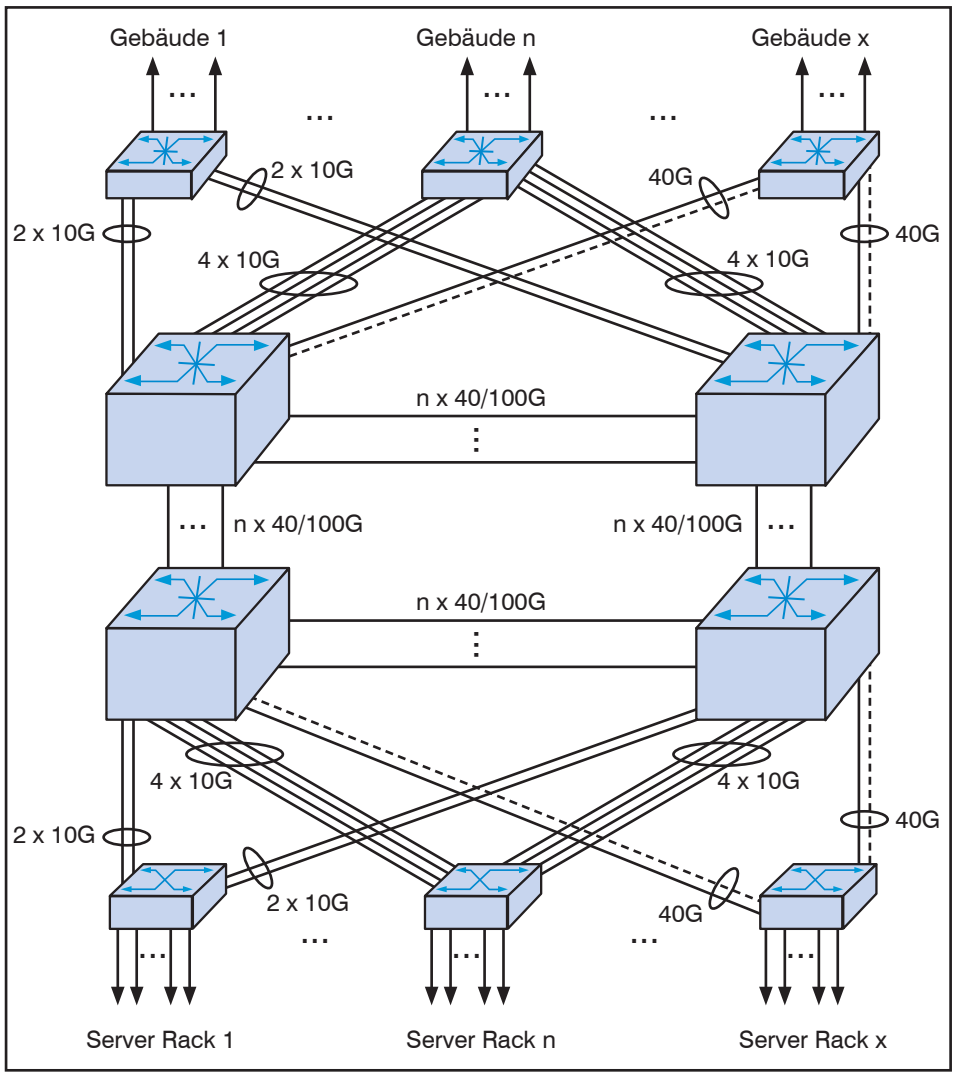


Abbildung 6.4: Beispiel-Design des Gesamtnetzwerks mit klassischer Stern-Konfiguration

Als kritisches Hochleistungs- und Anwendungs-Beispiel geben wir hier die Dienstgüte-Anforderungen für Cluster-Computing, Parallel Processing (MPP, Hadoop) an; der geneigte Leser wird feststellen, sie sind noch restriktiver als die Anforderungen für Echtzeit-Anwendungen:

- Delay 10 - 20 µs bis wenige ms
- Jitter: wenige µs
- Verlustrate: nahezu 0%

Netzwerk Core

Das klassische sternförmige Design erfordert Konzentratoren mit sehr hoher Portdichte für 10 Gbit und hoher Portdichte für 40 Gbit (siehe auch Abbildung 6.4). 1 Gbit Ports am Core kommen nur noch marginal zum Einsatz. Die Core-Querverbindung steigt auf n x 40 Gbit oder n x 100 Gbit; hierbei wären 100 Gbit in vielen Fällen sinnvoll, scheitern aber gegebenenfalls an der Verfügbarkeit oder am Preis. Insbesondere bei Einsatz von mehr als 2 Core Switches ist auf eine entsprechend hohe Kapazität der Querverbindung aller Core Switches zu achten! Wie sich anstelle des Stern-Designs mit Ring-Konfigurationen Kosten sparen lassen, wurde in den vorhergehenden Kapiteln dargelegt.

Grundsätzlich gilt: Bei jedem überbuchten Design sollte der Netzbetreiber an den Uplinks Lastschwellwerte setzen, bei deren Erreichen ein Alarm getriggert wird. Dies ist in jedem etablierten Switch über RMON möglich.

Abschließend sei nochmals eine Übersicht gegeben, welche Design-Elemente sich in welchen Netzwerk-Bereichen sinnvoll einsetzen lassen (siehe Abbildung 6.5).

Design-Elemente			
	RZ	Campus	Gebäude
Baum (Stern)	✓	✓	✓
Fat Tree	✓	✗	✗
Ring einfach	✓	✓	✓
Ring mehrfach	✓	✓	(✓)
Masche, vollständig	✓	✗	✗
Masche, teilvermascht	✓	✓	✗

Abbildung 6.5: Übersicht über die Einsetzbarkeit von Stern- Ring- und vermaschten Designs

Planung der RZ und Core Komponenten

Je nach gewünschtem Überbuchungsfaktor lässt sich die Auslegung beziehungsweise Anforderung an die Core Komponenten rechnerisch planen. Im um-

Netzwerk-Design in Zeiten von 10/40/100 Gbit: Wie sieht die Zukunft aus? - Teil 2

gekehrten Ansatz lässt sich bei Limitierungen der Portkonzentration bestimmter Hersteller-Produkte die resultierende Überbuchung oder bei einer festgesetzten akzeptierten Überbuchungsrate die Anzahl anschließbarer Server berechnen. Nachfolgend werden anhand entsprechender Planungs-Formeln Beispiele für eine 40 Gbit Planung aufgezeigt. Betrachten Sie hierfür Abbildung 6.6, so haben die Abkürzungen folgende Bedeutung:

- P = Anzahl Serverports (10G)
- U = Anzahl 40G Ports (4fach 10 G LAGs) je DC Core Switch
- f = Überbuchungsrate
- C = Anzahl DC Core Switches
- A = Anzahl DC Access Switches
- Cam = Anzahl 40G Verbindungen zum Campus
- CQ = Anzahl 40G Verbindungen zwischen je zwei DC Core Switches
- PCA = Anzahl 40G Verbindungen je Core Switch zum DC Access Layer
- PAC = Anzahl 40G Verbindungen je Access Layer Switch zum DC Core
- AQ = Anzahl 40G Verbindungen zwischen je zwei DC Access Switches (ToR)

Für die Core Switches ergibt sich hinsichtlich der Anzahl erforderlicher 40 Gbit Ports folgende Formel:

$$U = (P / 4Cf) + C_{am} + CQ$$

Ohne Überbuchung (f=1) bei 4 Core Switches, 16-fach 40 Gbit Anbindung je Core an den Campus und 16-fach Core Querverbindung ergibt sich beispielsweise bei 1536 Servern mit je 2 aktiven Ports als 40 Gbit Portkonzentration je Core:

$$U = (3072/(4*4*1)) + 16 + 16 = 224$$

Da eine solche Planung viele Hersteller, Anbieter ebenso wie unternehmensinterne Budgetverantwortliche zum Hyperventilieren bringen würde, nachfolgend ein moderateres Beispiel: Mit Überbuchungsfaktor 3:1 (f=3), mit 4 Core Switches, 16-fach 40 Gbit Anbindung je Core an den Campus ohne Core Querverbindung ergibt sich bei 1536 Servern mit je 2 aktiven Ports eine erheblich friedlichere 40 Gbit Portkonzentration je Core:

$$U = (3072/(4*4*3)) + 16 + 0 = 80$$

Die Formel für die anschließbaren Serverports ergibt sich zu:

$$P = 4 * C * f * P_{CA}$$

Planen wir in Anlehnung an das obige Beispiel 4 Core Switches mit Überbuchungsfaktor 3:1 und jeweils acht Modulen mit 8 Ports 40 Gbit, so resultieren 3072 anschließbare Serverports, respektive 1536 Server mit jeweils 2 aktiven Ports:

$$P = (4*4*3) * (8*8) = 3072$$

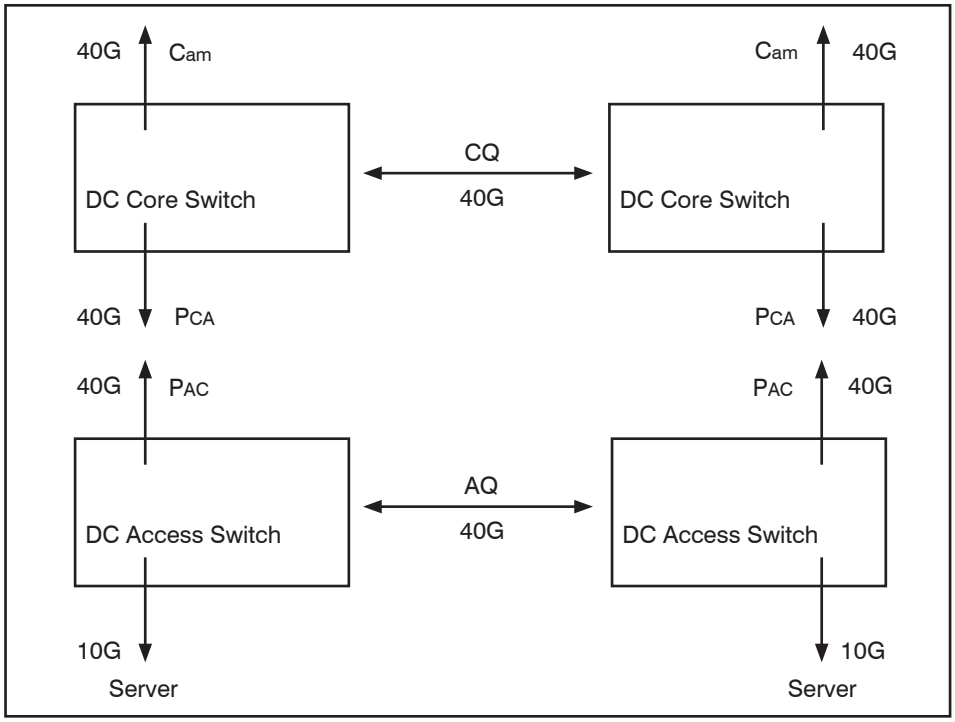


Abbildung 6.6: Generisches RZ – Core Design

Migrationsschritte

Soll eine Hochrüstung des Gesamtnetzwerks erfolgen, so macht es Sinn, zuerst den leistungsfähigeren Backbone zu installieren, um im Verbindungsnetzwerk zwischen Clients und Servern jeden Engpass zu vermeiden, da ein Leistungs-Engpass im Campus vergleichsweise hohe Seiteneffekte zur Folge haben kann.

Im zweiten Schritt sollte die Data Center und Server-Hochrüstung erfolgen, da die Server im Fall von Client-Server Verkehrslasten von den Clients getriggert sind und somit auch bei eigener Ausstattung mit hohen Datenraten keine Client-Überlastung erzeugen werden. Zudem stellt aktuell oft das RZ-Netzwerk den dringenderen Engpass dar als das Client-Acces-Netzwerk.

Die Hochrüstung des Client-Netzwerks bietet sich im dritten und letzten Schritt an, da bei Vertauschung von Schritt zwei und drei die Clients die Server überfordern und so Degradierungs-Phänomene hervorrufen könnten.

Überalterte Komponenten, die sich dem End-of-Service Stadium nähern, sind grundsätzlich in allen Bereichen ein zwingender Anlass für sehr zügiges Handeln (!).

Netzwerk-Design in Zeiten von 10/40/100 Gbit: Wie sieht die Zukunft aus? - Teil 2

Im nächsten Teil lesen Sie:
- Einbindung virtueller Netzkomponenten
- Wo kommt welches Failover-Verfahren zum Einsatz?

Abkürzungen, Links, Literatur

AP	Access Point
DRNI	Distributed Resilient Network Interconnect
EAPS	Ethernet Automated Protection Switching (Extreme Networks, IETF RFC 3619)
ECMP	Equal Cost MultiPath
EoR	End-of-Row
FC	Fibre Channel
fdx	full duplex
FDDI	Fiber Distributed Data Interface
FSPF	Fabric Shortest Path First
HiPER Ring	High-PErformance Redundancy (HiPER) ring protocol (Hirschmann EP 2343857 A1)
IRF	Intelligent Resilient Framework
LAG	Link Aggregation Group
LWL	Lichtwellenleiter
MC-LAG	Multi-Chassis LAG
MEC	Multi-Chassis EtherChannel (Cisco)
MLAG	Multiswitch LAG (Extreme)
MPLS	Multi Protocol Label Switching
MPP	Massively Parallel Processing
MRP	Media Redundancy Protocol
MRP	Metro Ring Protocol
NIC	Network Interface Card (Coupler)
OM	Optical Multimode
OSPF	Open Shortest Path First
phyNIC	physische NIC
PoE	Power over Ethernet
QF	QFabric (Juniper)
RFC	Request For Comment; TCP/IP Standard-Dokument
RZ	Rechenzentrum
SAN	Storage Area Network
SPB	Shortest Path Bridging
SPBM	Shortest Path Bridging MAC
SMLT	Split Multilink-Trunking
SPBM	Shortest Path Bridging MAC
SPBV	Shortest Path Bridging VID
SPoF	Single Point of Failure
ToR	Top-of-Rack
TRILL	TRansparent Interconnection of Lots of Links
UC	Unified Communications
VCS	Virtual Cluster Switching (Brocade)
vFW	virtuelle Firewall
vLB	virtueller Load Balancer
VoIP	Voice over IP
vR	virtueller Router
vSw	virtueller Switch

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.

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

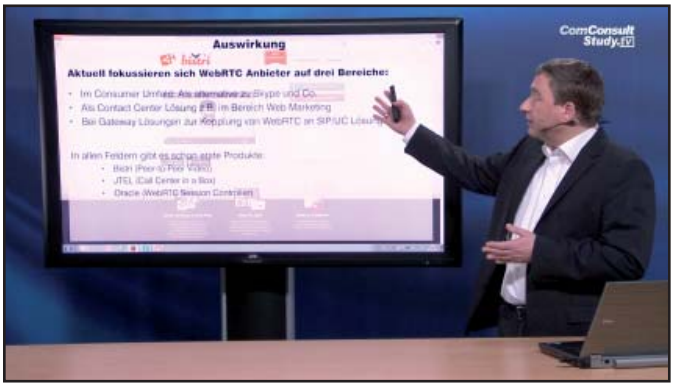
ComConsult-Study.tv

UCC Spezial im März bei ComConsult-Study.tv

Unified Communication and Collaboration (UCC) ist mittlerweile Alltag im Unternehmen. Oft wird jedoch nur damit telefoniert und auch das nur intern. Sobald man jemanden kontaktiert, der nicht im eigenen Unternehmen ist, wird das Gespräch am Amtskopf quasi zur "klassischen" Telefonie. Dabei haben auch viele Provider bereits auf Voice over IP umgestellt, so dass dieser Konvertierungsschritt im Grunde unnötig ist. Einen Ausweg würde SIP-Trunking bieten. Die Standards sind nicht neu, doch werden sie nur selten bis gar nicht angeboten.

SIP-Trunking: wo liegen die Probleme?
Referent: **Markus Geller** Einzelpreis: 49,00 € netto
Zeit: 00:37:22 Im Abo: kostenlos

UC hört in der Regel an der Unternehmensgrenze auf. Genau da wo Unternehmen Geld verdienen gehen die Effizienzvorteile einer modernen Kommunikation verloren. Der SIP-Connect-Standard schafft theoretisch die Voraussetzung zu einer Unternehmensübergreifenden Konnektivität. Markus Geller untersucht in diesem hochaktuellen Video, welche Standards und Zertifizierungen eine Rolle spielen und wie sich Hersteller und Provider dazu stellen.

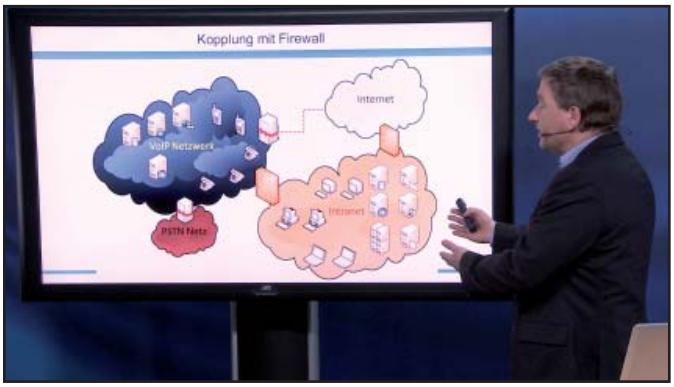


WebRTC: die neue Art der Kommunikation
Referent: **Markus Geller** Einzelpreis: 49,00 € netto
Zeit: 00:21:22 Im Abo: kostenlos

Mit WebRTC etabliert sich ein neuer Standard für Sprach und Video Kommunikation auf Basis von Browser Technologien. So wie die SIP Signalisierung seit einigen Jahren den Markt der Enterprise TK-Systeme beherrscht, so zeichnet sich eine neue Art der Client Entwicklung mittels WebRTC ab.

WebRTC: Funktionsweise, Standards und Codecs
Referent: **Markus Geller** Einzelpreis: 49,00 € netto
Zeit: 00:26:49 Im Abo: kostenlos

Der Markt der Videokonferenzlösungen wird durch die Entwicklung von WebRTC in eine neue Phase eintreten. Jetzt ist es zum ersten Mal möglich einen browserbasierten Client zu entwickeln, der auf allen nur denkbaren Endpunkten einsetzbar ist ohne Berücksichtigung der eingesetzten Betriebssysteme oder Laufzeitumgebungen. Dieser neue Ansatz wirft naturgemäß eine Reihe von Fragen auf.



Welches Netzdesign benötigt UCC?
Referent: **Markus Geller** Einzelpreis: 39,00 € netto
Zeit: 00:22:00 Im Abo: kostenlos

In unseren SIP und VoIP Veranstaltungen kommen immer wieder Teilnehmer auf uns zu und möchten erfahren, ob der Aufbau einer UC- oder VoIP-Lösung einer bestimmtes Netzwerkvorgabe folgen sollte. Diese Frage scheint also trotz all der Jahre immer noch nichts von ihrer Brisanz verloren zu haben. Dieses Video möchte daher die möglichen Vor- und Nachteile der verschiedenen Netzwerkdesigns vorstellen und auch die Sichtweise der UC- bzw. Netzwerkausrüster näher beleuchten.

Das Bundle bestehend aus den vier Videos für nur € 130,20*

*Dieses Angebot gilt nur im März 2014 .- Regulärer Preis € 186,-- netto

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

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.

Auf Abruf Service! Verlässlich und spezifikationsgemäß!

28. Februar 2014 von Paul G. Huppertz

Die Mitarbeiter der Fachabteilungen können nur dann geschäftliche Wertschöpfung realisieren, wenn ihnen jeder explizit abgerufene ICT-systembasierende Service verlässlich und spezifikationsgemäß sowie sicher und geschützt erbracht wird.
Kompletten Artikel lesen unter www.comconsult-research.de

Google präsentiert Enterprise Videolösung

21. Februar 2014 von Markus Geller

Und sie tuen es schon wieder. Google versucht mit seinen Cloud Lösungen immer neue Geschäftsbereiche zu erschließen. Nun ist also die Videokonferenzlösung am Zug. Seit vergangenem Freitag ist bekannt, dass Asus, Dell und HP, in Zusammenarbeit mit Google, eine Videokonferenzlösung für den Enterprise Markt anbieten werden.
Kompletten Artikel lesen unter www.comconsult-research.de

WAN-Umstellung: Totalausfall durch falsches IP-Design

14. Februar 2014 von Markus Schaub

Der Glaube, eine Umstellung der WAN-Technik von Standleitungen auf MPLS wäre nur eine Sache der Provider und der richtigen SLAs, ist ein weit verbreiteter Irrglaube. Vielmehr müssen Netzwerk-Betreiber auch das eigene Netz in allen Standorten unter die Lupe nehmen, um sicher zu stellen, dass es nicht zu einem Totalausfall kommt.
Kompletten Artikel lesen unter www.comconsult-research.de

Elektroanlagen aus Altbeständen für IT und deren Prüfungen

10. Februar 2014 von Karl-Heinz Otto

In vielen Geschäftsgebäuden, Büros und Liegenschaften des öffentlichen Dienstes sind die gleichen Situationen zur Versorgung der elektrischen Versorgung der Informationstechnologie, Gebäudesicherheitstechnik und elektronischer Systeme jeglicher Art zu beobachten.
Kompletten Artikel lesen unter www.comconsult-research.de

Wie lebendig ist Ihr Projekt?

26. Februar 2014 von Dr. rer. pol. Ralf Hillemacher

Über Zombie-Filme lässt sich trefflich streiten: Für die einen sind sie Kult, für die anderen nervig. Ich habe nie Zombie-Filme gemocht und doch konnte ich den Zombies nicht aus dem Weg gehen. Beinahe täglich begegne ich Projekten aus der IT, die zwar tot sind, sich aber trotzdem noch bewegen. Warum sind eigentlich so viele IT-Projekte so wenig lebendig, so träge, so ineffektiv? Wie hauchen wir unseren IT-Projekten wieder neue Dynamik ein?
Kompletten Artikel lesen unter www.comconsult-research.de

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**

Standpunkt Trouble-Shooting

Viel hilft viel – oder etwa nicht?

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

In den vergangenen Wochen trudelten zweimal Hilferufe bei mir ein, unabhängig voneinander. Die Kunden waren dabei, ihre neuen WLAN-Installationen in Betrieb zu nehmen und stießen dabei auf unerwartete Probleme: Die Abdeckung schien flächendeckend und überall einwandfrei zu sein. Dennoch verloren Handhelds die Verbindung zu ihren Servern, die WLAN-Performance von Laptops war miserabel. Und dabei hatten es beide Kunden doch gut gemeint und extra viele Access Points angebracht. Schließlich hatten sie gehört, dass die neuen WLAN-Techniken nur dann Übertragungsraten im Gigabit-Bereich erzielen, wenn die Funkzellen klein sind. Irgendwer hatte irgendwann einmal erzählt, man solle davon ausgehen, dass letztlich pro Büro ein Access Point zu installieren sei.

Das hatten die genannten Kunden auf ihre Fertigungshallen übertragen, in denen nun die Probleme auftraten. Eine hohe Access-Point-Dichte sollte überall gute Signalstärke sicherstellen und dementsprechend hohe Bitraten. Access Points waren an den Hallendecken montiert worden, die in die „Schluchten“ zwischen Lager- und Maschinenbereichen strahlen sollten, so dass Fahrwege von Staplern und andere Arbeitsbereiche gut ausgeleuchtet würden.

Eine erste Untersuchung der Situation mit Hilfe des zentralen WLAN-Managementsystems der Kunden bestätigte meinen Verdacht: Ein Parameter namens „Channel Utilization“ lag bei der großen Mehrzahl der WLAN Access Points im Bereich jenseits von 90%. Jedenfalls im 2,4-GHz-Band. Nachfragen bestätigte den Zusammenhang: „Nein, im 5-GHz-Band sind uns keine Probleme bekannt“. Ein weiterer Test bestätigte, dass sich die Access Points im 2,4-GHz-Band sehr gut untereinander hören könnten. Die Signalstärken benachbarter Access Points auf demselben Kanal lagen zum Teil im Bereich von -50 bis -60 dBm. Das ist bemerkenswert, empfehlen doch die Hersteller von WLAN-Komponenten zur Vermeidung von Gleichkanalinterferenzen viel geringere Werte, allgemein unterhalb -80 dBm.

Was passiert bei einer „Gleichkanalinterferenz“? Ganz einfach: Bevor eine Station senden darf, muss sie sicherstellen, dass das Medium frei ist (daher der Name für das Medienzugangsverfahren „Carrier Sense Multiple Access, CSMA“). Das gilt selbstverständlich auch für die Access Points. De facto kann hier also nur ein Access Point pro Kanal zu einer Zeit senden, da alle benachbarten Access Points das Medium als belegt erleben werden. Für die Clients in den „Schluchten“ der Halle ist es noch schlimmer. Sie hören ja im Wesentlichen nur „ihren“ Access Point, da aus ihrer Perspektive die anderen Access Points gut abgeschirmt sind. Die Wahrscheinlichkeit für Kollisionen, also gleichzeitiges Senden der Stationen und benachbarter Access Points, ist sehr hoch. Das ist der wesentliche Grund dafür, dass die Stationen so schlechte Performance erleben oder die Verbindung verlieren.

Was ist also zu tun? Nun, eine Halle ist sozusagen der Worst Case für WLAN mit hohen Bitraten. Grundsätzlich muss die Ausleuchtung nämlich so erfolgen, dass die Clients an jedem Ort mindestens einen Access Point sehen können. Gleichzeitig dürfen sich die Access Points untereinander nicht sehen. Wenn Access Points an der Hallendecke montiert werden, wären also Richtantennen einzusetzen, die genau das bewirken. Besser wäre es vielleicht, die Access Points an den Wänden anzubringen und von dort mit Richtantennen in die „Schluchten“ hineinstrahlen zu lassen. Eine allgemeine Aussage ist jedoch nicht möglich, zu sehr hängt es von der Beschaffenheit der Umgebung ab.

Ein weiterer Lösungsweg besteht darin, die Reichweite des WLAN zu begrenzen. Bedenken Sie: Ein WLAN langsamster Bit-rate (1 oder 2 Mbit/s) reicht theoretisch mindestens 50mal so weit wie ein Gigabit-WLAN. Würde man die Bitrate nach unten begrenzen, ließe sich das Problem in seiner Wirkung begrenzen. Aber darunter leidet die Kompatibilität zu „Legacy Devices“, also WLAN-Endgeräten, die eben nur die langsamen Bitraten unterstützen. Und diese Endgeräte werden eben vornehmlich bei 2,4 GHz eingesetzt.

Sie sehen, die Sache ist nicht so einfach. Und so freue ich mich auf eine angeregte Diskussion mit Ihnen auf dem ComConsult Netzwerk-Forum Ende dieses Monats.

Zweitthema

Enterprise Mobility: Schmelztiegel der Informations-sicherheit

Fortsetzung von Seite 1

Dr. Simon Hoff ist technischer Direktor der ComConsult Beratung und Planung GmbH und blickt auf jahrelange Projekterfahrung in Forschung, Standardisierung, Entwicklung, Planung und Betrieb in den Bereichen IT-Sicherheit, lokale Netze und mobile Kommunikationssysteme zurück.

Es kann sogar durchaus festgestellt werden, dass sich der Markt, der sich um Schadsoftware, Überwachungstools bzw. -Apps und Angriffswerkzeuge (insb. Lauschattacken) rankt, sich bereits stark auf mobile Endgeräte konzentriert.

Insgesamt bündeln sich im Bereich der mobilen Kommunikation alle aktuellen Probleme der Informationssicherheit auf eine ausgesprochen kritische Weise, was besondere, spezifisch gestaltete Sicherheitsmechanismen erfordert.

1. Mobile Betriebssysteme und Anwendungen

Die Palette mobiler Endgeräte reicht von traditionellen Mobiltelefonen, Smartphones, über Tablets und Notebooks bis hin zu Hybridformen (der Schwerpunkt in diesem Artikel liegt jedoch auf Smartphones und Tablets). Speziell Smartphones vereinen dabei nicht nur Telekommunikation, UCC und PC-Anwendungen, es entstehen auch vollständig neue Nutzungsformen durch die Kombination der Kommunikationsmöglichkeiten.

Smartphones sind üblicherweise mit einer Kamera und einem Empfänger für das Global Positioning System (GPS) ausgerüstet. Hiermit ist mehr als Fotografieren und Navigation möglich. Beispielsweise kann die Umgebung des Smartphones erkannt werden und es können positionsabhängig Dienste bereitgestellt werden. Augmented Reality ist erst mit Smartphones und Tablets für einen breiteren Nutzerkreis möglich geworden. Auch wenn solche Anwendungen derzeit oft noch im Consumer-Bereich verwurzelt sind, sind Anwendungspotentiale in Unternehmen und Behörden vorhanden. Diese Möglichkeiten bergen natürlich auch erhebliche Risiken für die Informationssicherheit und den Datenschutz. Die vielfältigen Möglichkeiten der Erstellung von Bewegungsprofilen, z.B. durch unberechtigtes Abgreifen von Positionsdaten durch eine App oder sogar durch den Hersteller des Betriebssystems selbst sind nur eine Facette der resultierenden Bedrohungen.

Neben einer nahezu unüberschaubaren Vielzahl von Hardware-Herstellern konkurrieren verschiedene Betriebssysteme in unterschiedlichen Ausprägungen um den Markt der mobilen Endgeräte. Beispiele für Betriebssysteme für Smartphones und Tablets sind Google Android, Apple iOS, Windows Phone 8 (bzw. Windows 8 für Tablets) und RIM Blackberry 10.

Sandboxing

Typisch für diese Betriebssysteme ist die Kapselung der Anwendungen (Apps) in sogenannten Sandboxes, über die kein Zugriff auf den Speicher anderer Apps erlaubt ist und deren Zugriff auf System-Ressourcen eingeschränkt ist, wie in Abbildung 1 dargestellt.

Android verwendet beispielsweise zur Ausführung von Applikationen virtuelle Maschinen, wodurch eine grundlegende Kapselung erzielt wird. Eine Android App kann, neben dem privaten Speicherbereich, lesend auf ein gemeinsames, unverschlüsseltes Dateisystem für Nutzerdaten zugreifen. Der Arbeitsspeicherinhalt wird ebenfalls nicht verschlüsselt. Unter An-droid sind Applikationen durch ein Rechtesystem voneinander getrennt. Anwendungen können aber immer eine Liste der installierten und ausgeführten Programme einsehen und andere Applikationen starten. Zudem können während der Installation weitere Rechte durch den Nutzer angefordert werden (z.B. Zugriff auf Ortsinformationen), die der Anwender gewähren darf. So kann das Rechtesystem zur Kontrolle der Systemressourcen aufgeweicht werden.

Anhand dieses Beispiels wird deutlich, dass die Betriebssystem-eigenen Sandboxing-Mechanismen zwar geeignet sind, um Applikationen voneinander zu isolieren, nicht jedoch, um den Zugriff auf Systemressourcen zu unterbinden. Zudem können Exploits im Betriebssystem genutzt werden, um die Isolation der Anwendungsdaten zu durchbrechen.

Sicherheitsfunktionen auf Ebene der mobilen Endgeräte

Die Sicherheitsfunktionen, die auf Ebene der mobilen Endgeräte zu erwarten sind, entsprechen grundsätzlich denen, die auch für konventionelle PCs etabliert sind, und beinhalten insbesondere die folgenden Punkte:

- Verschlüsselung der auf dem mobilen Endgerät gespeicherten Daten auf Ebene des Betriebssystems und bei Bedarf ergänzend auf Ebene der Apps
- Zugangsschutz durch Authentisierung des Nutzers durch PIN bzw. Passwort am mobilen Endgerät und bei Bedarf dedizierte Authentisierung für die Nutzung spezifischer Apps
- Befristete oder vollständige Sperre und ggf. sogar Löschung (Wipe) des mobilen Endgeräts bzw. einer App bei mehrfacher fehlerhafter Authentisierung
- Automatische Sperrung bei Inaktivität des Nutzers für einen gewissen Zeitraum
- Kontrolle und Einschränkung der Berechtigungen von Apps

Rollen und Berechtigungskonzepte für mobile Endgeräte, die es beispielsweise dem Nutzer nicht erlauben würden, gewisse Systemeinstellungen zu ändern, sind oft nicht von Betriebssystemen für

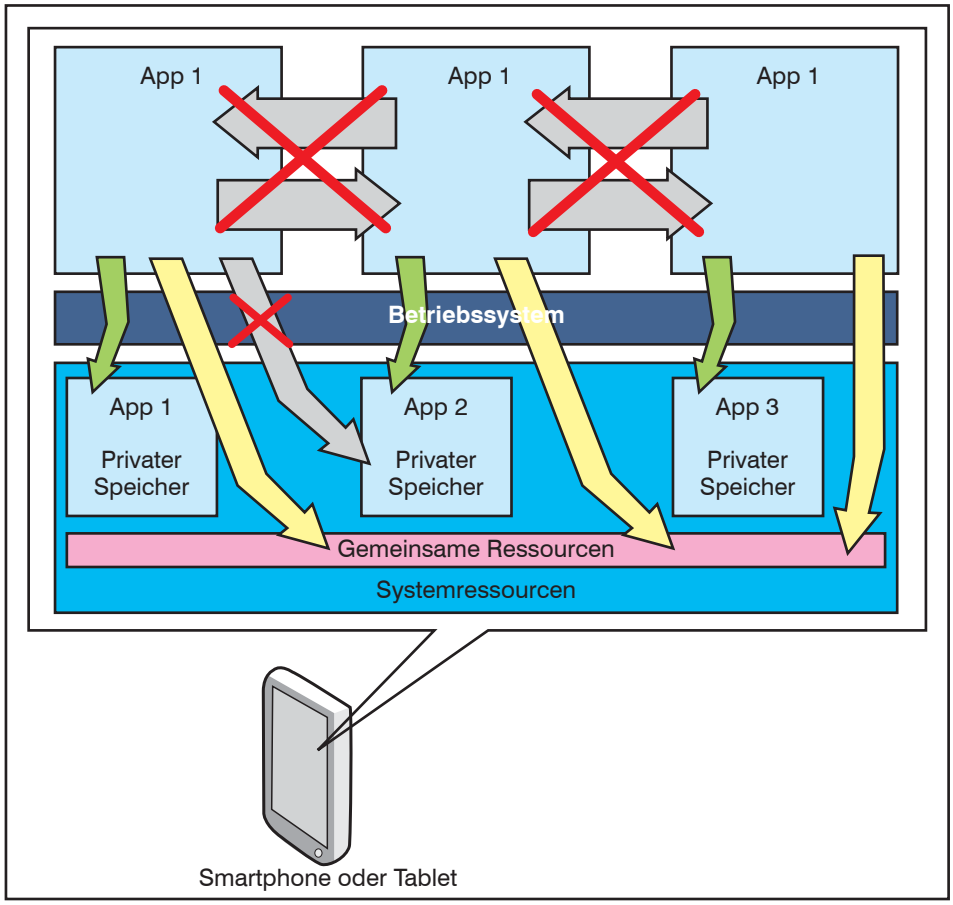


Abbildung 1: Sandboxing bei mobilen Betriebssystemen

mobile Endgeräte vorgesehen bzw. nur rudimentär umsetzbar. Daher ist die Kontrolle der Konfiguration und das Erzwingen von Einstellungen durch ein zentrales **Mobile Device Management (MDM)** von besonderer Bedeutung.

Consumer-Systeme in der Enterprise IT

Viele heute besonders populäre mobile Endgeräte und ihre Betriebssysteme adressieren den Consumer-Markt. Dies wird insbesondere in der Art und Weise deutlich, wie Apps über sogenannte App Stores, die spezifisch für die mobilen Betriebssysteme sind, den Nutzern zur Verfügung gestellt werden. Ein Nutzer wird hier im Normalfall nicht hinsichtlich der Auswahl einer App eingeschränkt. Konzepte, die sicherstellen, dass ein Nutzer nur eine beschränkte, ggf. gruppenspezifische Auswahl von Anwendungen erhält, die entsprechend geprüft und zugelassen werden, werden mit sogenannten Company (oder Enterprise) App Stores umgesetzt, die jedoch auf der Basis der Kanäle für die systemspezifischen App Stores aufgebaut sind.

Allgemein spricht man bei dem Trend, verstärkt Consumer-Produkte (Geräte und Software) in der Enterprise IT einzusetzen, von der „Consumerization of IT“. Dieser Trend hat erhebliche Konsequenzen für die Informationssicherheit, da bei Consumer-Produkten eher nicht davon auszugehen ist, dass bei der Produktentwicklung auch Anforderungen der Informationssicherheit umfänglich beachtet werden und dass Sicherheitsmaßnahmen, die z.B. bei PCs seit Jahren etabliert sind, sich ohne Probleme auch auf diese Consumer-Produkte anwenden lassen.

Qualitätsprobleme und die Folgen

Ein besonders schönes Beispiel von Qualitätsproblemen (nicht nur in Consumer-Produkten) hat vor kurzem Apple mit dem inzwischen berühmten „goto fail“ Bug geliefert (siehe hierzu auch Technische Warnung TW-T14/0018 vom 24.02.2014 des BSI[1]), der für Apple iOS bis einschließlich 6.1.5 bzw. 7.0.5 und Mac OS X bis einschließlich 10.9.1. relevant ist. Dieser Fehler ist ausgesprochen lehrreich und wird daher im Folgenden etwas genauer betrachtet.

Einerseits war der Fehler von erschreckender Trivialität: An einer gewissen Stelle des Codes für den Aufbau eines mit SSL/TLS geschützten Kommunikationskanals fand sich bei der der Zertifikatsprüfung ein Fehler, der dafür gesorgt hat, dass das Zertifikat des Kommunikationspartners nicht korrekt geprüft wird. Sinngemäß fand sich folgender Code:

```
{
if (“Teil 1 der Prüfung des Zertifikats fehlerhaft”)
        goto fail;
if (“Teil 2 der Prüfung des Zertifikats fehlerhaft”)
        goto fail;
        goto fail;
if (“Teil 3 der Prüfung des Zertifikats fehlerhaft”)
        goto fail;
…
        fail:
…
}
```

Auf den ersten Blick ist auch für den Nichtprogrammierer klar: Das zweite „goto fail“ hinter dem Teil 2 der Prüfung der Zertifikate gehört da nicht hin, und da es nicht im if-Statement steht, wird es gnadenlos ausgeführt, was dazu führt, dass Teil 3 der Prüfung übersprungen wird.

Dies ist eine wunderbare Einladung für einen Lauschangriff vom Typ Man in the Middle, die auch innerhalb kürzester Zeit genutzt wurde und bei der praktisch der vollständige verschlüsselte SSL-Verkehr im Klartext mitgelesen werden kann (siehe z.B. Blog von Aldo Cortesi vom 25. Februar 2014[2]).

Das Ergebnis ist ein GAU und dies leider in mehrfacher Hinsicht:

- Alle nicht mit einem Software-Update versorgten Maschinen mit iOS und Mac OS X sind nicht mehr für die wichtigen Dinge im Internet zu gebrauchen, ohne dass ein erhebliches Risiko besteht.
- Einem solchen Fehler kann der Hersteller nur durch schnelle Antwort und eine offene, ehrliche Informationspolitik begegnen. Die Reaktion von Apple war jedoch wieder ein zu langes Schweigen, bis der Update schließlich für alle Systeme bereitgestellt werden konnte.
- Der Fehler hätte bei einer simplen Code Inspection oder einfachen sicherheitsbezogenen Tests auffallen müssen. Zudem ist der Fehler so einfach, dass selbst ein Tool den Fehler automatisiert auf Basis einer einfachen Heuristik sicher hätte erkennen können. Ob das auch Rückschlüsse auf die Qualitätssicherung in der Software-Entwicklung bei Apple zulässt, sei dahin gestellt. Es ist zumindest ein massiver Reputations-

[1] Siehe https://www.buerger-cert.de/archive?type=widtechnicalwarning&nr=TW-T14-0018
[2] Siehe http://corte.si/posts/security/cve-2014-1266.html

schaden für Apple entstanden.

Apple hätte vielleicht besser von Microsoft lernen sollen. Vor geraumer Zeit hatten wir bei Microsoft Windows ähnliche Erlebnisse, die dazu geführt hatten, dass Microsoft die Methodik und die Prozesse für die Software-Entwicklung und -Wartung drastisch geändert hat und Informationssicherheit seitdem integraler Bestandteil des gesamten Lebenszyklus der Software ist. Hiermit kann zwar ein Bug vom Kaliber „goto fail“ nicht vollständig ausgeschlossen werden, jedoch wird die Wahrscheinlichkeit erheblich gesenkt.

2. Elemente der Absicherung mobiler Endgeräte

Neben Maßnahmen zur sicheren Konfiguration und Härtung sind folgende Maßnahmen auf Ebene der mobilen Endgeräte besonders relevant.

Schutz der dienstlichen Daten bei mobiler Nutzung

Kernelement der Absicherung mobiler Endgeräte ist der Schutz der dienstlichen Daten vor unberechtigten Zugriffen. Im Idealfall werden auf dem mobilen Endgerät keine dienstlichen Daten verarbeitet und gespeichert, sondern lediglich angezeigt, wie es bei einem Zugriff über Server-based Computing, d.h. über ein Terminal-Server-Protokoll der Fall ist. Dies ist allerdings oft nicht praktikabel, da offline (z.B. in einem Funkloch) kein Zugriff auf Anwendung und Daten bestünde. In Folge dessen kann oft auf Anwendungslogik und Datenhaltung auf den Endgeräten nicht verzichtet werden.

Umgang mit der dienstlichen und privaten Nutzung mobiler Endgeräte

Erschwerend kommt hinzu, dass die private Nutzung mobiler Endgeräte insbesondere angesichts moderner Arbeitsmethoden oft kaum noch untersagt, geschweige denn effektiv unterbunden werden kann. In dieser Lage ist die sichere **Trennung dienstlicher Daten von privaten Daten** auf Smartphone und Tablet unerlässlich.

Hier sind zunächst Container-Technologien zu nennen, die auf Ebene einer App eine Umgebung für Verarbeitung und Speicherung von dienstlichen Daten liefern können (Beispiel ist hier die Lösung von Good Technology).

Konsequenter ist der Einsatz von Virtualisierungstechniken, bei denen über einen Hypervisor das Endgerät zwischen einem privaten und einem dienstlichen Kontext umschalten kann. Unterschiedliche Techniken sind dabei auf dem Markt verfügbar: Typ-2-Hypervisoren werden auf Ebene einer App realisiert (Produktbeispiel ist Enterproid divide), d.h. ein virtuelles Smartphone wird als App realisiert und benötigt hierfür erhebliche Rechte auf dem zugrundeliegenden Betriebssystem des Smartphones.

Alternativ kann ein Hypervisor (oder ein vergleichbarer Trennungsmechanismus) in das Betriebssystem integriert werden. Für Android ist hier Samsung KNOX zu erwähnen. Die Technik sorgt durch Änderung und Ergänzung des Betriebssystems nicht nur für die sichere Trennung zweier Profile (einem privaten und einem dienstlichen) sondern stellt auch Instrumente für Dateisystem-Verschlüsselung, sichere Kommunikation und für ein erweitertes MDM bereit. KNOX basiert auf dem von der National Security Agency (NSA) entwickelten Secure Enhanced Android (SE Android). Nach den letzten Vorfällen stimmt eine Sicherheitslösung aus diesem Hause allerdings mehr als kritisch, auch wenn SE Android angeblich keine Backdoor enthalten soll.

Besser ist der Einsatz eines Typ-1-Hypervisor, der direkt auf der Hardware des mobilen Endgeräts aufsetzt. Die eigentlichen Betriebssysteme und Apps laufen dann als virtuelle Maschine (VM) auf dem Hypervisor und werden auf dieser Ebene voneinander getrennt (siehe Abbildung 2). Hiermit kann eine besonders sichere Umgebung für des Vorhalten und das Umschalten zwischen privatem und dienstlichem virtuellem Smartphone bzw. Tablet geschaffen werden. Dabei können ergänzend zur Kapselung der Systeme durch Virtualisierung mit kryptographischen Mitteln insbesondere die Daten einer dienstlichen VM im Speicher und beim Datentransport zusätzlich geschützt werden.

Einsatz von Krypto-Phones

In diesem Zusammenhang muss insbesondere auf sogenannte abhörsichere Mobiltelefone hingewiesen werden, die umgangssprachlich auch als Krypto-Phones oder Krypto-Handies bezeichnet werden. Hierbei handelt es sich um proprietäre Produkte, welche – wie der Name bereits andeutet – zunächst die konsequente Verschlüsselung der Daten eines mobilen Endgeräts bei Transport und bei Speicherung auf dem Endgerät ermöglichen.

Diese Absicherung betrifft insbesondere auch die Sprachübertragung. Dabei wird – unabhängig von einer Verschlüsselung auf der Ebene des Mobilfunknetzes oder der schnurlosen Kommunikation – eine Ende-zu-Ende-Absicherung der Sprach-

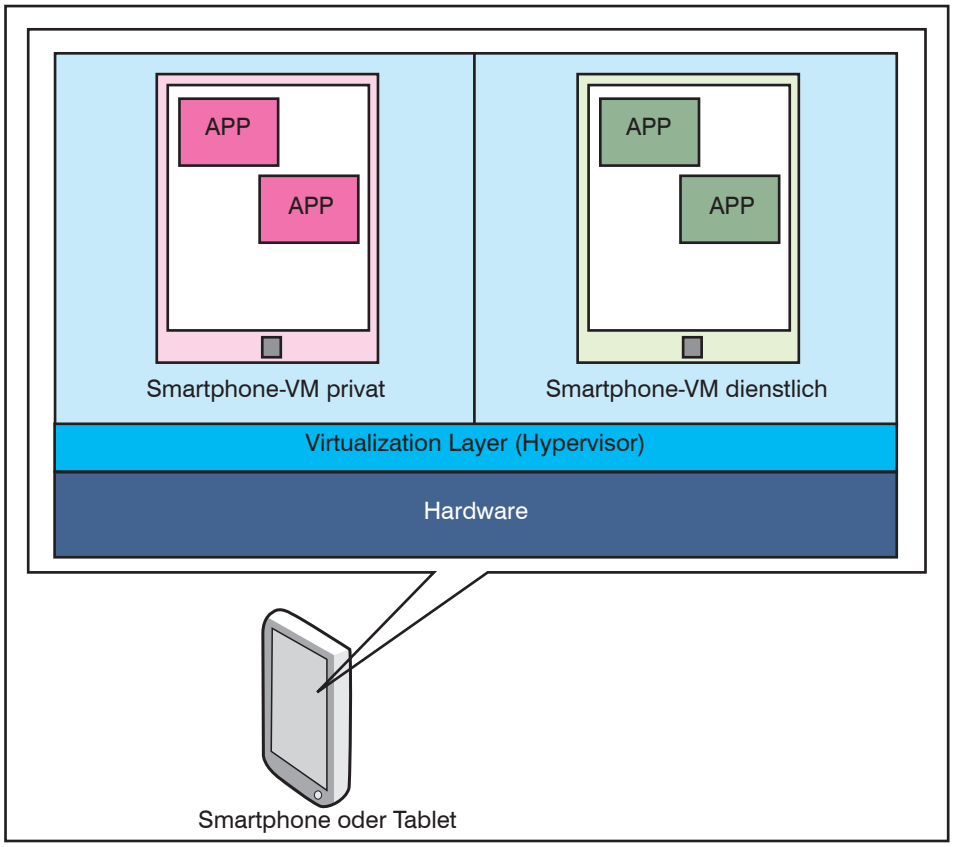


Abbildung 2: Einsatz von Virtualisierungstechniken zur Trennung dienstlicher und privater Daten

übertragung entweder direkt zwischen den mobilen Endgeräten oder zwischen einem mobilen Endgerät und einem zentralen Gateway hergestellt. In moderneren Produkten wird dabei vermehrt eine VoIP-Übertagung zur Infrastruktur der jeweiligen Institution genutzt.

Als Produktbeispiel sei hier SiMKo 3 von der Telekom genannt. Basis ist ein wie in Abbildung 2 dargestellter Typ-1-Hypervisor auf dem dann im Prinzip je eine Android-VM für die dienstliche und die private Nutzung läuft. Verfügbar ist diese Lösung z.B. auf Samsung Galaxy SIII und unterstützt grundsätzlich auch Android Tablets. SiMKo3 hat seit September 2013 nach Prüfung durch das BSI auch eine Zulassung für die Geheimhaltungsstufe VS-NfD (Verschlusssache - Nur für den Dienstgebrauch).

Solche Prüfungen durch eine dritte, möglichst neutrale Stelle sind insbesondere hinsichtlich einer potentiellen Backdoor und sonstiger Schwachstellen in der Implementierung des Herstellers von entscheidender Bedeutung. Wir benötigen (nicht nur für Krypto-Phones) dringend auch für den Enterprise-Bereich eine Zertifizierung und ein entsprechendes Gütesiegel für die Sicherheit mobiler Endgeräte.

Angesichts der Gefährdungen, denen mobile Endgeräte ausgeliefert sind, dürfen Krypto-Phones keinesfalls mehr als Exoten gesehen werden. Sobald Daten mit hohem Schutzbedarf hinsichtlich der Vertraulichkeit auf einem mobilen Endgerät verarbeitet und kommuniziert werden (und seien es „nur“ vertrauliche Gespräche und Kurznachrichten), sollten solche Lösungen ernsthaft in Betracht gezogen werden.

3. Sichere Infrastrukturanbindung mobiler Endgeräte

Mobiltelefone, Smartphones und Tablets haben eine entscheidende gemeinsame Eigenschaft: Sie kommunizieren ausschließlich (von USB-Synchronisation abgesehen) über drahtlose Techniken, d.h. Mobilfunk oder WLAN. Bei WLAN kann dabei sowohl ein öffentlicher Zugang (WLAN Hotspot) als auch ein Zugang über die eigene Infrastruktur auf dem Campus einer Institution genutzt werden.

Der Zugriff auf Daten im Netz einer Institution erfolgt oft über das Internet, auf das über Mobilfunk oder über einen WLAN Hotspot ein Zugang hergestellt wird. Zum Einsatz kommen dabei Web Applikationen, Web-Portale, VPN (z.B. auf Basis von IPsec oder TLS) oder Server-based Computing. Die Übertragung wird dabei mit den Mitteln abgesichert, die auch für die Remote-Anbindung von PCs eingesetzt werden, d.h. Authentisierung beispielsweise mit Zertifikaten, Verschlüsselung der Kommunikation beispielsweise mit dem Advanced Encryption Standard (AES) sowie Entkopplung der Kommunikation durch Gateways in einer Demilitarized Zone (DMZ) des Firewall-Systems für die Außenanbindung. Abbildung 3 illustriert das Grundprinzip.

Bei einem WLAN-Zugang auf dem Campus einer Institution ist grundsätzlich auch ein direkter Zugang zu Ressourcen im LAN möglich, sofern die Kommunikation auf der Luftschnittstelle angemessen abgesichert ist (z.B. durch Authentisierung mit IEEE 802.1X und eine Verschlüsselung mit AES).

Eine weitere Form der Anbindung mobiler Endgeräte ist der sogenannte Private Access Point Name (APN). Dabei wird durch den Mobilfunkbetreiber der paketvermittelte Datenverkehr eines mobilen Endgeräts nicht in das Internet ausgekoppelt, sondern über ein VPN an einen Router in der jeweiligen Institution geschickt, der der Private APN zugeordnet ist. Eine solche Lösung setzt natürlich voraus, dass dem Provider getraut werden kann.

4. Verwaltung mobiler Endgeräte - Mobile Device Management

Die wesentliche Aufgabe eines Mobile Device Management (MDM) besteht in der Unterstützung des zentralen Betriebs der mobilen Endgeräte einer Institution. Dies beinhaltet insbesondere die folgenden Punkte:

- Inventarisierung, Rollout und Fernkonfiguration
- Systemmanagement und Endgeräteüberwachung
- Fernwartung und Support

Eine Konfiguration aus der Ferne und die damit verbundene Möglichkeit Konfigurationsprofile erzwingen und überwachen zu können, sind jedoch auch wesentliche Sicherheitsfunktionen, von denen typischerweise MDM-Lösungen eine ganze Palette bieten. In diesem Sinne ist MDM eine der wichtigsten Sicherheitsmaßnahmen zur Integration mobiler Endgeräte. Produktbeispiele sind AirWatch, MobileIron und SAP Afaria. Hierbei handelt es sich durchweg um proprietäre Produkte. Obwohl sich mit der Zeit ein im durchaus ähnlicher Funktionsumfang der verschiedenen Produkte entwickelt hat, unterscheiden sich die Produkte im Detail erheblich. Im Folgenden werden die wesentlichen Kernfunktionen einer MDM-Lösung kurz vorgestellt.

Inventarisierung, Rollout und Fernkonfiguration

Zur Erfassung eines neuen Endgeräts muss oft zunächst eine spezielle App für das MDM auf dem mobilen Endgerät installiert und das Gerät dem zentralen MDM bekannt gemacht werden. Diese Erfas-

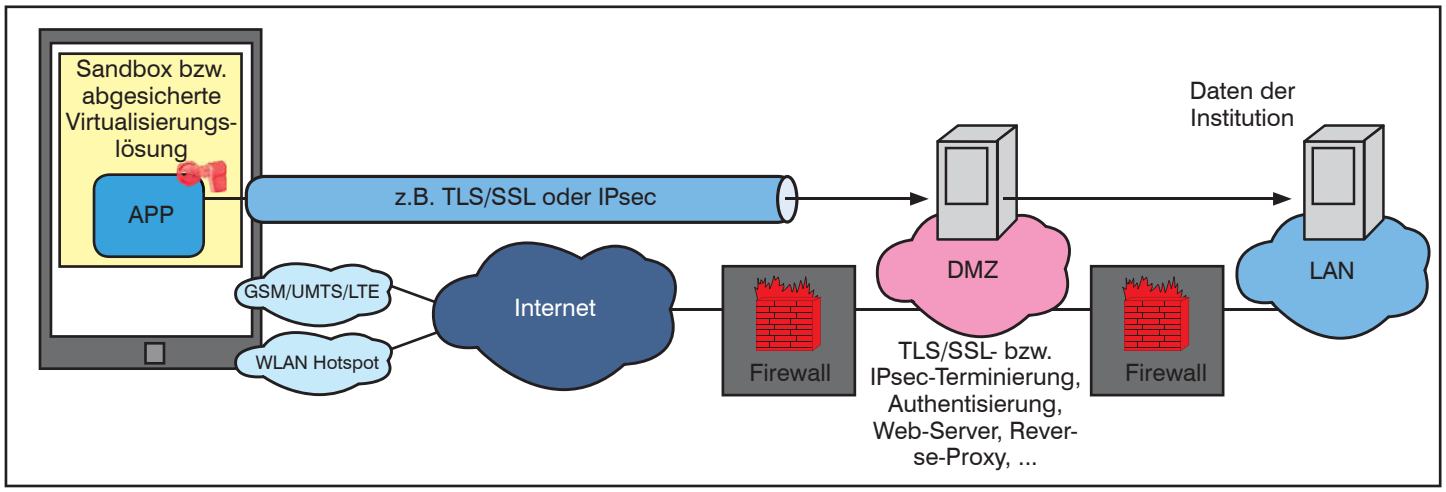


Abbildung 3: Typische Infrastrukturanbindung mobiler Endgeräte

sung eines neuen Endgeräts erfolgt entweder durch einen Administrator oder sogar durch den Nutzer selbst an einem Self-Service Portal.

Nach der Inventarisierung und der damit verbundenen Anbindung an das zentrale MDM kann das Gerät dann Over-the-Air (OTA) unabhängig vom Endgerätestandort mit Einstellungen konfiguriert werden. Dabei werden oft unterschiedliche Nutzergruppen unterschieden und entsprechende gruppenspezifischen Policies angesetzt.

Für die Softwareverteilung werden oft sogenannte Company App Stores eingesetzt, die jedoch auf den App Stores der eingesetzten mobilen Betriebssysteme und den hier bestehenden Verteilungsmechanismen basieren. Dabei handelt es sich – zumindest für die aktuell besonders populären mobilen Betriebssysteme – letztendlich um Dienste, die über eine Public Cloud bereitgestellt werden, was mit erheblichen Sicherheitsbedenken verbunden ist. In einem solchen Company App Store können dann für die Arbeit erforderliche (inkl. selbst entwickelter) Anwendungen für den Nutzer bereitgestellt und freigegeben werden. Auch eine Fernlöschung der Apps von den Endgeräten ist bei Bedarf möglich. Trotz der genannten Sicherheitsbedenken ist ein Company App Store von besonderer Wichtigkeit, da nur über diesen Weg auch sichergestellt werden kann, dass nur freigegebene Apps verwendet werden und die Apps auch nur die wirklich benötigten Zugriffsrechte erhalten.

Systemmanagement und Endgeräteüberwachung

Das Systemmanagement muss unmittelbar bei Anmeldung eines Nutzers aktiv werden und bei Bedarf aktualisierte Konfigurationsdaten, Apps oder Sperr- und Löschkommandos übermitteln können (auch als Push-Down-Funktion bezeichnet). Kommandos zum Sperren oder sogar Löschen (Wipe) können dabei eine App oder sogar das komplette Endgerät betreffen.

Ein weiteres Element des Systemmanagement ist die regelmäßige Sicherung (Backup) der Daten von einem mobilen Endgerät auf die zentrale Infrastruktur, um das Risiko von Datenverlusten bei Defekt oder Verlust des Geräts zu minimieren.

Die Endgeräteüberwachung beinhaltet folgende Punkte:

- **Event-Logs:** Es werden Logfiles mit unterschiedlichem Detaillierungsgrad über Systemzugriffe und Anwenderaktivitäten erstellt.
- **Reporting:** Die erfassten Ereignisse werden in Reports zu Statistiken verdichtet.
- **Kostenkontrolle:** Das Volumen von Sprach- und Datenverkehr kann überwacht und dokumentiert werden. Entsprechende Grenzwerte können vordefiniert werden und geben bei Überschreitung einen Warnhinweis.

Fernwartung und Support

Es werden durch das MDM-System Werkzeuge zur Verfügung gestellt, die eine Ferndiagnose und Fernzugriff auf das Gerät ermöglichen. Dadurch kann der IT-Support den Anwender, unabhängig von seinem Standort, bei der Behebung möglicher Probleme unterstützen. Zur Erfassung und Bearbeitung von Störungen und Wartungstätigkeiten kann dabei ein MDM-System auch an ein Incident-Management-System angebunden werden.

Sicherheitsfunktionen

Folgende Sicherheitsfunktionen sind für MDM-Lösungen (in unterschiedlichen Ausprägungen) typisch:

- **Erzwingung von Sicherheitsrichtlinien:** Es kann ein Passwort-Schutz sowie eine angemessene Komplexität des Passwortes erzwungen werden. Ebenso kann festgelegt werden wie viele Fehlversuche gestattet sind und wie darauf reagiert werden soll (z.B. Löschung des Geräts oder bestimmter Inhalte). Auch sollte eine Bildschirmsperre des Geräts nach einem definierbaren Zeitintervall erzwingbar sein.
- **App-Richtlinien:** Über Blacklists und Whitelists können bestimmte Apps explizit gesperrt bzw. freigegeben werden. Sofern vom Betriebssystem des Endgeräts unterstützt, können einzelne App-Berechtigungen unterdrückt werden. Auch ist eine Fernlöschen unerwünschter Apps nach dem Abgleich mit der Black-/Whitelist möglich.
- **Remote-Wipe:** Hierunter wird das Sperren und Löschen des Endgeräts per Fernadministration verstanden. Diese Funktion versetzt den IT-Betrieb bzw. den Anwender in die Lage, im Falle eine Endgeräteverlusts oder -diebstahls die auf dem Endgerät gespeicherten sensiblen Daten vor unbefugtem Zugriff zu schützen. Ggf. können Daten auch selektiv gelöscht werden. Manche Hersteller unterstützen auch eine Funktion, bei der die Daten nach einer festgelegten Zeitspanne ohne Anmeldung am Netzwerk gelöscht werden.
- **Endgeräte-Audits:** Die auf einem mobilen Endgerät installierte MDM-Software kann (ggf. angestoßen und gesteuert durch eine zentrale MDM-Komponente) regelmäßig und bei Bedarf eine Überprüfung auf Einhaltung von Richtlinien und Konfigurationsvorgaben durchführen. Dies beinhaltet insbesondere die Feststellung, ob erweiterte Berechtigungen auf dem mobilen Endgerät vorliegen (Jailbreak oder Root-Rechte) und entsprechende Maßnahmen eingeleitet werden.
- **Behandlung von Sicherheitsvorfällen (Security Incidents):** Wird bei der Prüfung eines Endgeräts ein Sicherheitsvorfall erkannt, können je nach Dringlichkeit unterschiedliche Aktionen angestoßen werden, die von der Information des Nutzers, der Benachrichtigung der IT-Abteilung bis hin zu einem Remote-Wipe rangieren können.
- **Verschlüsselung gespeicherter Daten:** Durch das MDM wird erzwungen, dass Daten der jeweiligen Institution auf dem Gerät und austauschbaren Speicherkarten nur verschlüsselt gesichert werden. Hierzu wird entweder die bordeigene Verschlüsselungsmethode des Endgeräts, oder aber ein eigenes Verfahren der MDM-Lösung verwendet.
- **Sandboxing:** Die Daten werden in einer speziell gesicherten Container App der MDM-Lösung verschlüsselt gespeichert. Der Zugang zur App ist mit einem eigenen Passwort geschützt. Die Verwendbarkeit der hier abgelegten Daten außerhalb der Sandbox kann per Richtlinie konfiguriert werden.
- **Gesicherte Verbindungen:** Der Zugang zum Netz einer Institution erfolgt ausschließlich über gesicherte Verbindungen.

Spätestens an dieser Stelle ist es notwendig sich nochmal an den „goto fail“ Bug zu erinnern.

Besonders wichtig für den Umgang mit durch Schwachstellen in Produkten verursachten Sicherheitslücken ist es nicht nur für den Hersteller schnellstmöglich einen Patch oder Update bereit zu stellen, sondern auch für den Nutzer diesen schnellstmöglich zu installieren.

Dies setzt zunächst eine geschlossene Kette vom Hersteller des mobilen Betriebssystems zum Nutzer voraus, d.h. die vollständige Kontrolle von Software und Hardware. Hier ist Google Android klar im Nachteil, denn nachdem eine Schwachstelle in einer neuen Version beseitigt ist, dauert es entsprechend lange bis die Her-

steller der Endgeräte und die Mobilfunkbetreiber die neue Version selbst getestet und freigegeben haben.

Für den Einsatz im Enterprise-Bereich ist ein effektives System Management für den Umgang mit Patches und Updates zwingend erforderlich, d.h. ohne die konsequente Nutzung der Möglichkeiten eines MDM geht es nicht. Dabei ist – wie so oft in der Informationssicherheit – ein Kompromiss auf Kosten von Freiheit und Komfort der Nutzer zu schließen.

Dies gilt auch für den Umgang mit der permanenten Überwachung von Nutzern im mobilen Internet durch Apps und durch die mobilen Endgeräte selbst. Informationen über die Identität des Nutzers, seine Kontakte, der Nutzungen von Diensten und den Aufenthaltsort sind in Zeiten von Big Data für Google und Co. Gold wert. Ohne weitreichende Änderungen an anderer Stelle kann dem nur durch die konsequente Einschränkung der Apps und ihrer Berechtigungen entgegengewirkt werden.

Aufbau einer MDM-Lösung

Für den Aufbau einer MDM-Lösung im eigenen Rechenzentrum sind üblicherweise folgende Komponenten erforderlich:

- **Mobile Device Services:** Über einen Server in einer DMZ erhalten die mobilen Endgeräte ihre Konfigurationsdaten. Die Kommunikation erfolgt hier meist über HTTPS.
- **Secure Application Gateways:** Über Application Gateways in einer DMZ erfolgt der Zugriff auf die eigentlichen Anwendungsserver der Institution (z.B. Exchange). Über einen solchen Weg kann auch eine sichere Browser-Umgebung für mobile Endgeräte geschaffen werden, indem eine Browser App über das Internet sich stets mit der eigenen Proxy-Infrastruktur verbindet und erst von hier das eigentliche Ziel im Internet erreicht.
- **MDM Managementsystem:** Zunächst werden die zentralen Komponenten des MDM-Systems über ein Managementsystem verwaltet. Zudem erfolgen gewisse Elemente von Inventarisierung, Rollout und Fernadministration lösungsabhängig über das Managementsystem. Typische Beispiele sind die Administration des Company App Store oder die Verwaltung von Zertifikaten und anderen Credentials für die Authentisierung von Endgeräten und Nutzern. Für den Zugriff auf einen Company App Store ist eine Kommunikation mit dem eigentlichen, externen App-Store erforderlich. Aus diesem Grund wird der entsprechende Server üblicherweise in einer eigenen DMZ platziert.

Abbildung 4 zeigt exemplarisch einen möglichen Aufbau der Infrastruktur.

Hinweis: Manche MDM-Lösungen benötigen eine zentrale Komponente in der Infrastruktur des jeweiligen Herstellers, über die der gesamte Verkehr zu den mobilen Endgeräten läuft. Aus Sicherheitsgründen ist eine solche Lösung bedenklich, da einerseits die Verfügbarkeit durch die zusätzliche Komponente in jedem Fall eingeschränkt ist und andererseits das grundsätzliche Risiko der Kompromittierung von Daten über die Infrastruktur des Herstellers besteht. Aus ähnlichen Gründen sind Cloud-basierte MDM-Lösungen kritisch zu sehen.

5. Neue Schnittstellen für mobile Endgeräte im Internet of Things

Im Internet of Things (IoT) erfassen Dinge (Things) – nicht Menschen wie im „Internet of Humans“ – Informationen, sind per IP vernetzt und stellen Informationen für andere Dinge oder Menschen zur Verfügung. Dahinter stecken unterschiedlichste Systeme und Anwendungen. Beispiele sind Messgeräte im Smart Grid, Sensoren und Steuerungen in der Automatisierungs- und Gebäudetechnik oder aber das vernetzte Fahrzeug, das mit anderen Fahrzeugen (Car2Car) oder mit der Infrastruktur (Car2-Infrastructure) kommuniziert [3].

Es ist einleuchtend, dass hier insbesondere die mobile und drahtlose Kommuni-

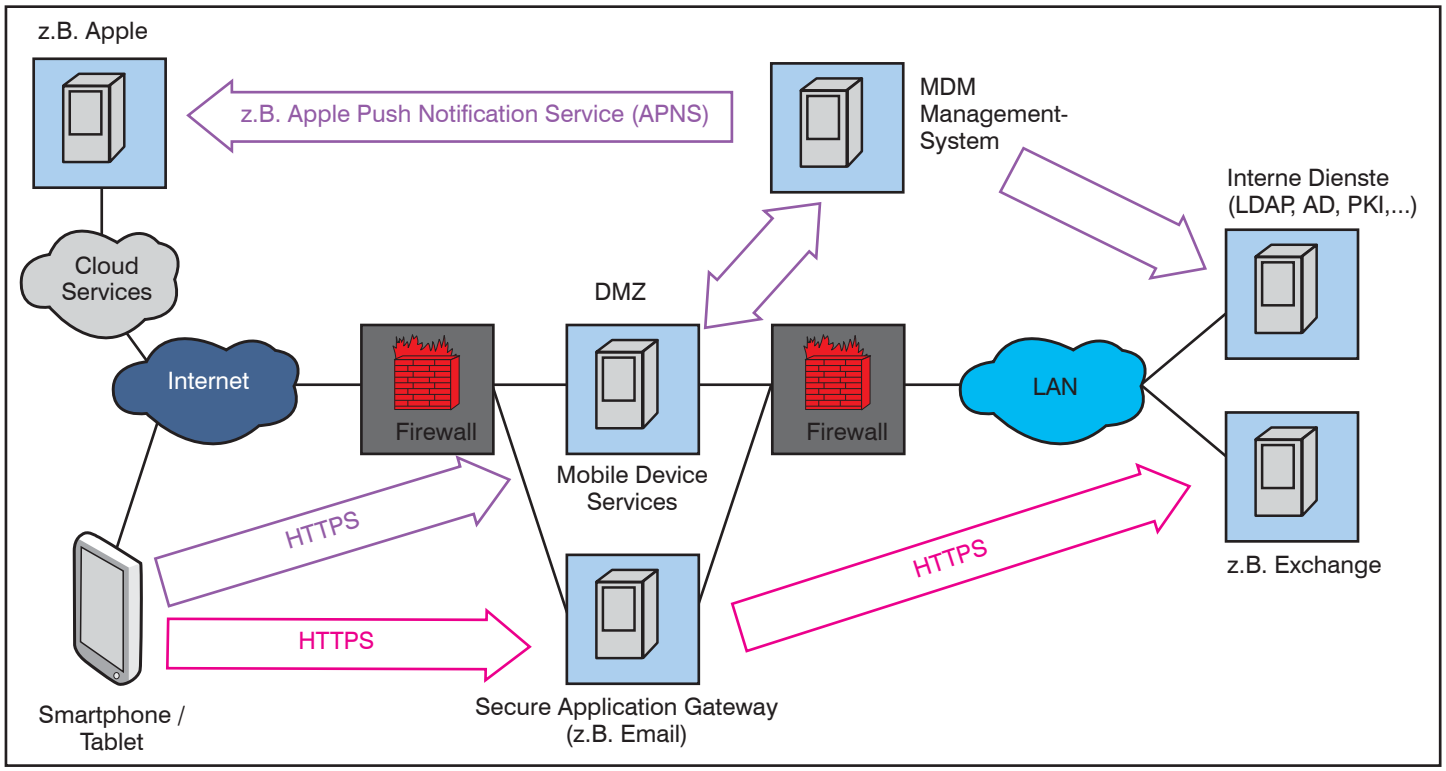


Abbildung 4: Exemplarische Darstellung der Komponenten eines MDM-Systems

[3] Siehe z.B. http://vector.com/vi_car2x_de.html

kation einen besonderen Stellenwert hat. Tatsächlich drängen alle wichtigen Hersteller mobiler Betriebssysteme und mobiler Endgeräte massiv in diesen Sektor und kooperieren entsprechend stark mit den Automobilherstellern und der Zulieferindustrie. Zu nennen sind hier insbesondere Google mit der Open Automotive Alliance und Apple mit CarPlay.

Mobile Endgeräte werden dabei immer stärker in Fahrzeuge integriert. Stellen wir uns als Ergänzung des Bordcomputers eines Fahrzeugs eine Schnittstelle zu einem gewöhnlichen Smartphone vor. Dann könnte einerseits über das Smartphone z.B. per Mobilfunk oder WLAN auf Funktionen des Fahrzeugs eingewirkt werden, wie Vorheizen im Winter oder Auf- und Abschließen des Fahrzeugs. Umgekehrt könnte das Smartphone über Bedienelemente im Fahrzeug (z.B. Schalter im Lenkrad) gesteuert werden und das Fahrzeug-Cockpit als Display für das Smartphone dienen.

Diese Integration ist erst am Anfang, sie wird immer stärker werden und immer neue Anwendungen erschließen. Es zeichnet sich durchaus jetzt schon ab, dass Smartphones und Tablets zu der wesentlichen Schnittstelle zwischen Mensch und IoT werden.

Mit diesen Möglichkeiten sind allerdings auch erhebliche Sicherheitsbedenken verbunden. Was könnte ein Virus alles auf einem Smartphone anrichten, das gerade mit der Elektronik eines Fahrzeugs verbunden ist? Was passiert bei systematischer Fälschung von Sensorwerten, was passiert bei zielgerichteter Sabotage von Standard-IT-Komponenten im Internet of Things, z.B. in einem Fahrzeug? Außerdem bieten sich hier ganz neue Möglichkeiten zur Datensammlung und Überwachung. Dies kann zwar positiv genutzt werden (z.B. zur Verkehrsteuerung), nur wird Big Data auch ganz andere Schlüsse erlauben, wenn das Verhalten eines Fahrers mit anderen Parametern korreliert wird.

Denken wir abschließend nochmal an den „goto fail“ Bug. Damit wir mit dieser Entwicklung nicht in ein offenes Messer laufen, ist ein drastisches Umdenken der Hersteller mobiler Betriebssysteme und Endgeräte erforderlich. Softwarequalität muss wieder im Vordergrund stehen (was natürlich einen Widerspruch zum notwendigen Entwicklungstempo im Consumer-Markt darstellt). Insbesondere muss die Informationssicherheit integraler, prüf- und zertifizierbarer Bestandteil der Systeme werden. Außerdem benötigen wir Standards für MDM, speziell bezüglich der Schnittstellen zwischen Endgeräten und zentralen MDM-Komponenten. Nur mit standardisierten Mitteln kann bei der Vielfalt von Endgeräten, Betriebssystemen und Anwendungen ein umfassendes System Management überhaupt geschaffen werden.

6. Abkürzungen

AD	Active Directory
AES	Advanced Encryption Standard
APNS	Apple Push Notification Service
BSI	Bundesamt für Sicherheit in der Informationstechnik
DMZ	Demilitarized Zone
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MDM	Mobile Device Management
NSA	National Security Agency
OTA	Over the Air
PKI	Public Key Infrastructure
SSL	Secure Sockets Layer
TLS	Transport Layer Security
UCC	Unified Communications & Collaboration
USB	Universal Serial Bus
VoIP	Voice over IP
VPN	Virtual Private Network
VS-NfD	Verschlusssache – Nur für den Dienstgebrauch
WLAN	Wireless LAN

ComConsult Veranstaltungskalender

Aktuelle Veranstaltungen

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

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

Video Intensiv-Tag: Markttrends und Technologien, 31.03.14 in Köln

Lernen Sie wie Sie wirtschaftlich und mit hoher Akzeptanz Video an jeden Arbeitsplatz, auf jedes Gerät und an jeden Ort bringen. Integrieren Sie erfolgreich mit modernster Technik Raumkonferenz, Desktop, Tablet, Smartphone und Browser. Diese Sonderveranstaltung zeigt wie es geht und welche Technologien heute und in Zukunft zum Einsatz kommen. Führende Hersteller stellen sich der Diskussion und präsentieren ihre Roadmaps. Für zukunftssichere Investitionen in die am schnellsten wachsende Kommunikations-Technologie.

Preis: € 990,-- netto

Storage: Planung moderner Speicherlandschaften, 31.03. - 01.04.14 in Berlin

In diesem Seminar werden bereits etablierte Technologien sowie die aktuellen Entwicklungen im Speicherumfeld vorgestellt, technisch erläutert und für die richtige strategische Entscheidung zu einem Gesamtkonzept zusammengeführt. Lernen Sie die Vor- und Nachteile der einzelnen Funktionen kennen für Ihr persönliches Speicher-Optimum. Entwickeln Sie ein tragfähiges Speicher-Fundament für die nächsten 5 Jahre.

Preis: € 1.590,-- netto

Das mobile Unternehmen, 31.03. - 01.04.14 in Berlin

Dieses 2-tägige Seminar gibt Ihnen einen umfassenden Überblick über Einsatzmöglichkeiten, Risiken und Chancen sowie Anforderungen und Auswirkungen mobiler Technologien im Unternehmen. Es werden die grundlegenden Veränderungen in Arbeitsweise und Arbeitsausstattung aufgezeigt, die die steigende Mobilität mit sich bringt und die Auswirkungen auf den IT-Betrieb, die Infrastruktur und das Management von mobilen Geräten diskutiert. Zum einen werden mögliche Gefährdungen aufgezeigt, die sich durch die zunehmende Konsumerisierung und den damit verbundenen Anstieg von privat genutzten Geräten entstehen. Zum anderen werden aber auch Möglichkeiten und Chancen, die mobile Applikationen und die lückenlose Vernetzung im „Internet of Things“ bieten, erläutert.

Preis: € 1.590,-- netto

IT-Projektmanagement Kompaktseminar, 07.04. - 09.04.14 in Aachen

Seminar über Projektmanagement in der IT. Es wird speziell auf die Anforderungen und Herausforderungen von IT-Projekten eingegangen. Lernen Sie wie Sie Projekte sauber aufsetzen und überwachen und mit welchen Methoden und Hilfsmitteln Sie die Termineinhaltung sicherstellen können.

Preis: € 1.890,-- netto

Internetworking: optimales Netzwerk-Design mit Switching und Routing, 07.04. - 11.04.14 in Aachen

Dieses Seminar vermittelt alles Wichtige, was Sie zum Thema LAN wissen müssen. Es werden unterschiedlichen Einsatzszenarien für Routing und Switching beleuchtet und das notwendige Wissen zur erfolgreichen Planung und dem Betrieb von Netzwerk Infrastrukturen vermittelt. Die Abdeckung der Themen erstreckt sich über Layer 2 Redundanzverfahren, Routing und Tunneltechnologien, sowie Netwerkmanagment Fragen. Einen weiteren Schwerpunkt bildet das Kapitel Office Network. Hier werden der Aufbau und die Integration von WLAN Strukturen detailliert beleuchtet. Abgerundet werden diese Informationen durch verschiedene praktische Übungen und einen Blick auf die aktuelle Markt- und Produktsituation der führenden Hersteller von Netzwerk-Komponenten.

Preis: € 2.490,-- 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
05.05. - 07.05.14 in Bonn
29.09. - 01.10.14 in Stuttgart
17.11. - 19.11.14 in Bonn

Basis-Technologie der IP-Telefonie
02.06. - 04.06.14 in Düsseldorf
20.10. - 22.10.14 in Berlin

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

Session Initiation Protocol

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