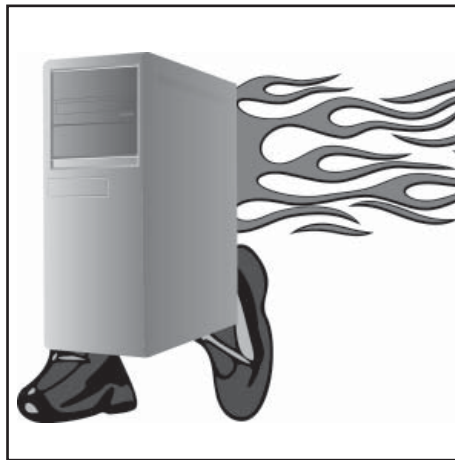


Schwerpunktthema

## Mehr Bandbreite im RZ mit Virtual I/O und optimierten Prozessorarchitekturen

von Dr. Franz-Joachim Kauffels

Bisher setzen virtuelle Systeme auf I/O-Architekturen auf, die noch aus der nicht-virtuellen Vergangenheit stammen. Nun kommen zum ersten Mal neue Standards auf den Markt, die speziell für virtuelle Umgebungen entwickelt wurden. Sie integrieren eine deutlich verbesserte Konfiguration, mehr Sicherheit zwischen virtuellen Maschinen und deutlich mehr Leistung. Dieser Artikel informiert über diese hochaktuellen Entwicklungen. Lesen Sie, welche Bandbreiten in Zukunft im Rechenzentrum möglich sind.



Zweitthema

### 1. Einführung und Problemstellung

In meinem ersten Artikel zu dieser Problematik im Insider Online vom 27.10.2009 konnten wir als Fazit folgende Leistungsgrenzen virtueller Systeme im Rechenzentrum feststellen...

weiter auf Seite 15

## Macht Carrier-Ethernet das WAN zum LAN?

von Dipl.-Inform. Andreas Meder

Weitverkehrsnetze (Wide Area Networks, WAN) und die ihnen zugrundeliegenden Technologien unterliegen seit einigen Jahren einem kontinuierlichen Wandel. Ausgehend von verbindungs-basierten Ansätzen auf Basis von TDM (Time Division Multiplex) mit aus heutiger Sicht - und vor allem im Licht heutiger applikations- und prozessbedingter Anforderungen - extrem geringen Übertragungsraten bei gleichzeitig

hohen Kosten geht die Tendenz hin zu breitbandigen Netzanschlüssen basierend auf preisgünstiger Ethernet-Technik. Das WAN nähert sich damit technologisch immer mehr dem LAN (Local Area Network) an, so dass ein Verschwinden oder gar Verschwinden der Grenzen zwischen diesen beiden Netzklassen scheinbar nicht nur bloß eine Frage der Zeit ist, sondern dies gar heute schon machbar erscheint.

Dieser Artikel beleuchtet die aktuellen Möglichkeiten des Einsatzes von Ethernet im WAN-Umfeld und untersucht dabei ausgehend von einem realen, aktuellen Vernetzungsprojekt insbesondere, wo sich LAN und WAN auf Ethernet-Basis bereits vereinigt haben und wo nach wie vor gewisse Unterschiede in Technologie und Anwendung bzw. Nutzung bestehen...

weiter auf Seite 9

Aktueller Kongress

**ComConsult  
Virtualisierungsforum  
2010**

ab Seite 4

Geleit

**Der iPad:  
Fortschritt für  
Unternehmen**

ab Seite 2

Aktuelles Seminar

**Aktuelle VPN  
Technik**

ab Seite 14

Zum Geleit

# Der iPad: Fortschritt für Unternehmen

Apple hat mit der Vorstellung des lange diskutierten iPads mal wieder erfolgreich den Markt aufgemischt. Das Gerät wirkt wie ein großes iPhone, tatsächlich aber generiert es einen neuen Typ von Endgerät, der auch zur Nutzung in den Unternehmen analysiert werden muss.

Deshalb gleich zu Beginn zwei Thesen:

1. Es gibt einen Bedarf für einen neuen Gerätetyp im Unternehmen
2. Die bisherigen Geräte können diesen Bedarf bisher mit den verfügbaren Technologien nicht abdecken

Die Grundidee ist die eines Personen-gebundenen Geräts, das handlicher ist als ein Laptop und vor allem die Medien-Integration auch inklusive des Lesens von Büchern und Dokumenten abdeckt. Dieses Gerät muss bei aller Qualität einen niedrigen Preis haben, um es zur Standard-Ausstattung für Mitarbeiter machen zu können.

Folgende Anwendungsfälle sollen als Beispiele genannt werden:

1. Besprechungen, für die viele Dokumente benötigt werden. Ein Laptop ist in Besprechungssituationen einfach häufig zu unhandlich. Außerdem steigert das nicht die Kommunikation, wenn jeder Teilnehmer einer Besprechung hinter einem Deckel sitzt. Auf der anderen Seite sind die bisherigen Tablets zu teuer, zu schwer und zu unhandlich.
2. Es fehlt eine „Weiterbildungsplattform“ im Markt. Wir haben mit ComConsult-Study.tv eine neue Form der Weiterbildung gestartet, die auf wissenschaftlichen Erkenntnissen des optimierten Lernens durch den gezielten Mix von Medien basiert. Wir brauchen das passende Gerät dazu, das diesen Medienmix begleitet. Als Lerngerät muss es Personen-bezogen und mobil sein.
3. Elektronische Lesegeräte wie das Amazon Kindle oder der Sony Reader stellen einen gewaltigen Fortschritt für Unternehmen da. Wann immer man eine Information in Buchform braucht, sie ist in Minuten verfügbar. Die Fähigkeit, in Projekten oder beim Arbeiten direkt auf eine riesige Bibliothek von Fachbüchern zugreifen zu können und immer alle relevanten Nachschlagewerke dabei zu haben, ist ein riesiges Plus. Wir haben den Amazon Kindle seit Wochen im Test für Anwendungen aus Unternehmens-



sicht und ich komme gleich auf die Ergebnisse zu sprechen.

4. Mobile Arbeitssituationen, bei denen Menschen zwischen Arbeitsstationen wechseln und dabei ein Geräte brauchen, das in handlicher Form sowohl Applikationen als auch Daten anbietet. Ärzte und Prüferingenieure sind typische Beispiele dafür.

Jetzt liegt die Frage nahe, warum wir also ein neues Gerät dafür brauchen. Immerhin gibt es ja sowohl Tablett-PCs als auch Reader. Starten wir mit den Nachteilen von Readern für Bücher.

Alle auf dem Markt angebotenen Reader basieren auf einem ePub ähnlichen Format, auch wenn es Amazon anders nennt. Nun ist ePub für einfache Bücher ohne viele Grafiken sicher ok, aber sobald die Bücher komplexer werden, versagt die Grundidee von ePub. ePub stellt Bücher in einem einfachen, Format-ungebundenen Fließtext dar. Damit kann man die Zeichengröße verändern oder zwischen horizontal und vertikal ohne Probleme wechseln. Der Text passt sich an. Aber das ist genau der springende Punkt: ePub kann strukturierte Texte mit aufwendigen Grafiken nicht darstellen. Im Prinzip fehlen genau die Möglichkeiten, die PDF geschaffen hat. Hinzu kommt, dass ein wesentlicher Fortschritt in der Arbeit mit Fachbüchern aus der Möglichkeit kommt, zu unterstreichen oder Notizen zu machen. An dieser Stelle ist der Standard aber mehr als mager. Auch wenn einige Reader wie der Kindle oder Stanza als Software Ansätze dazu zeigen, bleibt eines klar: eine Integration dieser Anmerkungen und Unterstreichungen über Ge-

rätengrenzen hinweg ist wegen der Mängel im Standard nicht möglich.

Gerade die Fähigkeit aber, flexibel auf Fachliteratur zugreifen zu können, ist für Unternehmens-Anwendungen wichtig.

Und diese Art von Literatur basiert auf strukturierten Dokumenten, die in ePub nur sehr schlecht abbildbar sind, auch wenn Layout-Programm wie Adobe InDesign die Erzeugung von ePub aus bestehenden Texten heraus ermöglichen. Zwar basiert ePub auf Teilmengen von XHTML und CSS, aber die hier genutzten Möglichkeiten sind zu beschränkt.

Außerdem ist dies eine verkrustete Denkweise der Vergangenheit. Fast alle heutigen Publikationen nutzen das Potenzial von Multi-Media nicht aus. Stellen wir uns mal ein Buch über Photoshop oder Dreamweaver vor. Der Umgang mit komplexer Software stößt in Buchform an seine Grenzen. Das gleiche gilt für reine Video-Schulungen, die häufig nicht zum Nachschlagen geeignet sind. Die Integration ist der Hit. Statt eines Bildes in einem Photoshop-Buch ein Video zu haben, das die Nutzung einer Funktion erklärt, würde den Lernerfolg in ganz neue Dimensionen katapultieren.

Dies ist genau das Beispiel, das Steve Jobs bei der Vorstellung des iPads mit der Anwendung der New York Times gezeigt hat. Eine Tageszeitung, die an dafür geeigneten Stellen an Stelle von Fotos auf Videos zugreift ist ein neuer Medientyp. Sicher ein Medientyp, der in der öffentlichen Presse zu massiven Diskussionen führen wird, da er Medienanbieter wie Rupert Murdoch direkt in die Arme spielt. Eine Multi-Media-Zeitung oder ein entsprechendes Magazin braucht eine andere Form von Redaktion. Und sie braucht den Zugriff auf Videoclips und Texte in gleichem Umfang. Sicher ein Horrorszenario für lokale Zeitungsredaktionen (wenn es die noch gibt). In diesem Sinne gefährdet das iPad ernsthaft Teile der bestehenden Media-Landschaft.

Halten wir fest: die bisherigen Reader für eBooks sind soweit ok, aber sie sind speziell für die Dokumente, die wir in Unternehmen häufig haben, technisch ungeeignet.

Und damit sind wir beim iPad. Das iPad schließt die Lücke, die es im Markt für Fachbücher, neue multimediale Zeitungen und Magazine oder Technologie-Reports gibt (glauben sie mir, ein ComConsult-Re-

## Der iPad: Fortschritt für Unternehmen

port oder der Netzwerk-Insider auf dem Kindle ist ein grafisches Desaster).

Das iPad macht es möglich:

- auch die Wirtschaftswoche, den Spiegel, den Economist oder was immer sie auch lesen, in e-Form in voller grafischer Qualität umsetzen zu können. Wer die Version der Wirtschaftswoche auf dem Kindle kennt, weiß was ich meine
- neue Formen von Multimedia-Dokumenten zu schaffen, die es so bisher nicht gab (man stelle sich den Netzwerk-Insider mit Video-Beiträgen an Stelle der Grafiken vor, wir unterstützen dies technisch übrigens ab der März-Ausgabe, aber noch mit der Einschränkung, dass die Bilder dann ein Link zu einem externen Video sind, das Video ist also nicht integraler Teil des Dokuments)
- auch komplexe Fachliteratur mit komplexen Grafiken, Zeichnungen und vor allem Farbe auf einen eReader zu bringen (Automobiltechnik, Medizin, Biologie, ....)

Das setzt eine entsprechende Gerätequalität voraus, ein stark mobiles Gerät und eine entsprechende Versorgungs-Plattform. Dies fehlt Netbooks und den bisherigen Tablett-PCs. Tablett-PCs sind zu teuer, zu klobig, zu schwer. Und sie liefern genau die zuvor beschriebenen Anwendungen nicht.

Es gibt weitere Argumente, die für einen iPad sprechen, auch wenn sie nicht jedem gefallen werden und einige davon auch eine Kehrseite haben:

- eine geschlossene Plattform steigert die Sicherheit für Unternehmen
- eine geschlossene Plattform macht eine bessere Umsetzung von DRM möglich
- die Apps-Plattform ist die ideale Basis, um entsprechende Multi-Media-Applikationen zu entwickeln und zu verbreiten
- die Apps-Plattform ist die ideale Basis für ein Personen-gebundenes Gerät
- keine Browser-Vielfalt, damit einfachere Programmierung von Web-Anwendungen auf dieser Plattform
- iPad-Apps sind immer noch sehr einfach zu entwickeln, auch Web-basierte Anwendungen mit integriertem Code auf Browser-Basis sind mit den neuesten Frameworks nicht komplex in der Erstellung. So entsteht auch für Unter-

nehmen eine Basis für „eigene“ Applikationen

Vereinfacht ausgedrückt liefert die Bindung an eine Hardware und einen Hersteller Möglichkeiten, die viele Vorteile bieten.

Naturgemäß muss auch an dieser Stelle die Kritik ansetzen. Ein Hersteller-gebundenes und nicht wirklich offenes Gerät stellt auf der anderen Seite die Eignung für den Unternehmens-Einsatz in Frage. Wer schon länger mit Apple arbeitet, der weiß, wie gut die Geräte sind, wie groß aber auch die Probleme sind, wenn man mal eine Funktion benötigt, die dort nicht angeboten wird (schon mal versucht, Option 66 im Apple DHCP-Server zu nutzen? Der Betrieb von IP-Telefonen basiert auf dieser Option, sicher, man kommt daran vorbei, aber ein typisches Beispiel für einen Mangel. Auch das Fehlen von VoIP oder Virtualisierung spricht nicht für Apple als Unternehmens-Technik, aber ich bin hier für Diskussionen im Diskussionsforum offen).

Aber auch wenn Apple mit seinen Desktops, Laptops und Servern aus meiner Sicht generell für Unternehmens-Anwendungen nur sehr eingeschränkt emp-

fehlbar ist, sieht die Situation beim iPad doch anders aus. Wir reden hier über ein Personen-gebundenes Gerät mit einem beschränkten Anwendungsprofil. Am Beispiel der Nutzung des iPads als Lernplattform zeigt sich auch, dass die lokale IT sogar entlastet wird. Ich muss Lernanwendungen, die stark individuellen Charakter haben, nicht mehr auf den Unternehmens-PCs installieren. Allerdings gibt es für die IT-Abteilungen auch keinerlei Kontrolle über das, was auf dem Gerät installiert wird.

Aus meiner Sicht ist das iPad trotz aller genannten und ungenannten Einschränkungen ein wichtiges Gerät für den Unternehmenseinsatz. Als Ausbildungsplattform passt es genau zu unserem ComConsult Study.tv-Ansatz. Im gezielten Medienmix liegt die Basis für eine erfolgreiche Ausbildung.

Sie teilen meine Meinung nicht? Prima. Diskutieren Sie mit mir im Diskussionsforum von ComConsult-Study.tv unter: <http://www.comconsult-study.tv/forum/viewforum.php?f=34>

Ihr Dr. Jürgen Suppan

## Kongress



### Netzwerk-Redesign Forum 2010 26. - 29.04.10 in Königswinter

#### NEU! Inklusive Plus-Modul zum Netzwerk-Redesign Forum 2010

Das neue Plus-Modul ermöglicht die optimale Vorbereitung auf das Netzwerk-Redesign Forum durch unsere HD-Videos, die durch ComConsult Study.tv produziert werden. Zum Abspielen der Videos ist ein von uns bereitgestellter Software-Client erforderlich.

Das Plus-Programm zum Netzwerk-Redesign-Forum umfasst:

1. Virtualisierung im Rechenzentrum und die Einbindung in Netzwerke, Dr. Jürgen Suppan
2. Carrier Ethernet in der Analyse, Dr. Franz-Joachim Kauffels
3. 10, 40, 100 Gigabit-Ethernet, Dr. Franz-Joachim Kauffels
4. Fazit der Veranstaltung mit Mitschnitten der Highlights ausgewählter Vorträge, Dr. Jürgen Suppan

Moderation: Dr. Franz-Joachim Kauffels, Dr. Jürgen Suppan  
Preis: € 2.290,- zzgl. MwSt.



Buchen Sie über unsere Web-Seite [www.comconsult-akademie.de](http://www.comconsult-akademie.de)

Aktueller Kongress

# ComConsult Virtualisierungsforum 2010

Die ComConsult Akademie veranstaltet vom 03.05. - 05.05.2010 ihren Kongress „ComConsult Virtualisierungsforum 2010“ in Königswinter.

Virtualisierung ist weder ein Werkzeug noch ein Produkt, es ist eine völlig neue Architektur-Form. Sie verändert die Nutzung und Einbindung einer ganzen Reihe von Technologien:

- Server
- Netzwerke
- Speicher
- Datenbanken
- Applikationen
- Basis-Hardware (CPU, ...)

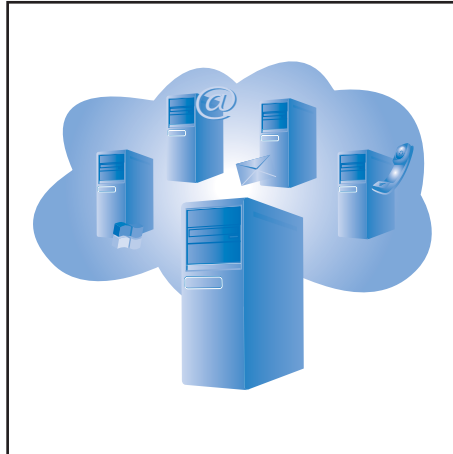
Die Vorteile, die daraus entstehen, gehen unvermeidbar einher mit Optimierung und somit Änderungen im Betrieb und in wichtigen Betriebsfunktionen:

- Lastverteilung
- Backup
- Disaster Recovery
- Hochverfügbarkeit
- Fehlertoleranz
- Standort-übergreifende Sicherheit
- Integration von neuen virtuellen Sicherheits-Appliances

Virtualisierung wird permanent weiter entwickelt. War es bis vor kurzer Zeit nur geeignet, einfache Dateiserver zu konsolidieren, so ist heute die Grenze bei Applikations-Servern, die 8 Kerne oder mehr erfordern. Die Virtualisierung von Email-Servern, Datenbank-Servern und Applikations-Servern wird mehr und mehr zur Realität. ERP-Applikationen wie SAP profitieren vor allem von den Architektur-Vorteilen, indem wichtige Teil-Prozesse äußerst kostengünstig mit Fehlertoleranz abgesichert werden können.

Gerade aber aus der Technologie-übergreifenden Architektur, den notwendigen Änderungen im Betrieb und der Einbeziehung von mehr und mehr Anwendungen, entstehen auch eine Reihe von ernst zu nehmenden Risiken:

- Technologie-Abhängigkeiten nehmen zu, Fehler in der Auslegung einer Technologie können andere Technologien zum Stillstand bringen
- Organisatorische Änderungen gehen quer über heute bestehende Abteilungs-grenzen hinweg
- Virtualisierung ist nicht stabil, die permanente Weiterentwicklung wirft auch



Fragen der Nutzbarkeit für bestimmte Anwendungen auf

Das Ganze wird komplettiert durch völlig unterschiedliche Formen von Virtualisierung:

- Server-Virtualisierung
- Desktop-Virtualisierung
- Applikations-Virtualisierung

Diese verschiedenen Formen befinden sich in sehr unterschiedlichen Reifestadien. Es ist generell riskant, aus guten Erfahrungen mit Server-Virtualisierung auf ähnliche Erfahrungen in den anderen Bereichen zu schließen.

Und als wäre das Ganze noch nicht genug, gibt es Abhängigkeiten zwischen Produkten und Herstellern. Auch die Frage, wer diesen Wettbewerb auf Dauer überleben wird, wird immer häufiger gestellt. So kämpfen ganz verschiedene Produkte und Hersteller um diesen Markt, davon sollen nur einige genannt werden:

- Citrix / Xen
- Microsoft
- Red Hat / KVM
- VMware

Aufgrund der vielen direkt umsetzbaren Vorteile und ROI-Zeiten von häufig unter 12 Monaten, besteht quasi für fast alle Anwender ein sehr hoher Druck, trotz der Dynamik dieser Entwicklung so schnell wie möglich einzusteigen.

Hier setzt das ComConsult-Virtualisierungs-Forum 2010 an. Wir analysieren für Sie:

- Welche Technologien sind betroffen, welche Abhängigkeiten bestehen

- Server
- Netzwerke
- Speicher
- Datenbanken
- Applikationen
- Basis-Hardware (CPU, ...)

- Welche Betriebsprozesse sind betroffen, welche davon werden erheblichen Änderungen unterliegen

- Welche Vorteile liefert Virtualisierung speziell für

- Hochverfügbarkeit
- Fehlertoleranz
- Disaster Recovery

- Wo sind die Grenzen der Technologie speziell bei Datenbank- und Applikations-Servern

- Wo stehen die einzelnen Hersteller, kann VMware den Markt weiter dominieren, überwiegend langfristig die Vorteile von Open Source Software, wird Microsoft auch diesen Markt früher oder später überrollen

- Welche Anforderungen entstehen speziell auf der Netzwerk-Seite

- Welche Bandbreite wird nur zum Betrieb der Virtualisierung selber benötigt

- Was bedeutet die Einbindung und Konsolidierung SAN-Speicher

- Welche betriebstechnischen Voraussetzungen bestehen, wie können Grenzen zwischen Server, Speicher und Netzwerk-Konfiguration organisatorisch erfolgreich gehandhabt werden

- Was bedeuten die unterschiedlichen Formen von Virtualisierung in Form von Server-, Desktop- und Applikations-Virtualisierung

- Wie ausgereift sind die unterschiedlichen Formen

- Welche Infrastruktur-Voraussetzungen müssen erfüllt werden

- Wie groß sind die erzielbaren Vorteile

- Wie verschieden sind die Hersteller in den einzelnen Bereichen positioniert

Virtualisierung ist die wichtigste Technologie- und Architektur-Veränderung der letz-

ComConsult Virtualisierungsforum 2010

ten 20 Jahre. Sie führt zu neuen Formen von Rechenzentren, sie verändert Betrieb und sie schafft völlig neue Kostenstrukturen.

Das ComConsult-Virtualisierungs-Forum 2010 ist unsere herausragende Veranstaltung des Jahres 2010 zu diesem Thema. Sie betrifft Planer, Entscheider und Pro-

jektspezialisten aus den einzelnen Fachrichtungen.

Sichern Sie sich rechtzeitig einen Platz in dieser herausragenden Veranstaltung.

## Frühbucherrabatt bis 28.02.10

# ComConsult Virtualisierungsforum 2010

**03.05. - 05.05.10 in Königswinter**

Für Besucher unserer bisherigen Kongresse bzw. für die Teilnehmer am VIP-Verteiler bieten wir Ihnen exklusiv eine Vorbuchungsphase für das ComConsult Virtualisierungsforum 2010 bis zum 28.02.2010 für eine rabattierte Teilnahmegebühr an.

ComConsult Virtualisierungsforum 2010  
zum Preis bei Buchung bis 28.02.10 von € 1.690,-- zzgl. MwSt.  
statt regulär € 1.890,-- zzgl. MwSt.

Die Buchung innerhalb der Frühbucherphase ist verbindlich, kann aber jederzeit auf einen anderen Mitarbeiter Ihres Unternehmens übertragen werden.

Fax-Antwort an ComConsult 02408/955-399

# Anmeldung ComConsult Virtualisierungsforum 2010

Ich buche den Kongress  
**ComConsult**  
**Virtualisierungsforum 2010**

03.05. - 05.05.10 in Königswinter  
zum Preis von € 1.690,--\* zzgl. MwSt.  
\* gültig bis zum 28.02.10

Bitte reservieren Sie mir ein Zimmer  
vom \_\_\_\_\_ bis \_\_\_\_\_ 10

\_\_\_\_\_  
Vorname

\_\_\_\_\_  
Nachname

\_\_\_\_\_  
Firma

\_\_\_\_\_  
Telefon/Fax

\_\_\_\_\_  
Straße

\_\_\_\_\_  
PLZ, Ort

 Buchen Sie über unsere Web-Seite  
[www.comconsult-akademie.de](http://www.comconsult-akademie.de)

\_\_\_\_\_  
eMail

\_\_\_\_\_  
Unterschrift

Aktueller Kongress

# Netzwerk-Redesign Forum 2010

Wie in jedem Jahr so ist auch in 2010 das Netzwerk-Redesign-Forum unsere zentrale Veranstaltung zum Thema Netzwerk-Design und Technologie-Veränderungen in Netzwerken und IT-Architekturen.

Das Forum besteht aus 3 Komponenten, die separat gebucht werden können:

1. Die Hauptveranstaltung vom 26.4. - 28.4.10
2. Unser Vertiefungs-Tag am 29.4. mit ausgewählten Schwerpunkt-Themen
3. Dem Plus-Modul aus Vorbereitungs-Videos zu wichtigen Themen und Nachlauf-Videos, die die Veranstaltung zusammen fassen und offen gebliebene Fragen adressieren

Die Hauptveranstaltung stellt folgende Themenbereiche in den Mittelpunkt:

1. IT-Architekturen verändern Netzwerk-Architekturen
  - a. Bandbreitenbedarf
  - b. Zukunftssichere Komponenten
  - c. Welche Komponenten nähern sich ihrem End-of-Life
2. Der Markt im Wandel
  - a. HP übernimmt 3Com, was bedeutet das?
  - b. HP kontra Cisco: wer hat das bessere Konzept?
  - c. Multi-Blade-Switches kontra Routing-Core: wohin geht der Tren

3. Technologie im Wandel
  - a. Das Ende von Spanning Tree: welches neue Verfahren wird die Zukunft bestimmen, SPB kontra Trill
  - b. Vom Netzwerk zum Systembus im Rechenzentrum: DCB, FCoE
  - c. Provider-Technik in die Unternehmen, Ablösung von OSPF durch Carrier Ethernet oder MPLS
  - d. Migration zu IPv6 im Netzwerk: was bedeutet das?
  - e. Wireless-LAN nach der Verabschiedung von IEEE 802.11n
  - f. Verkabelung 2010

4. Betrieb unter Druck
  - a. Sicherheit im Tagesbetrieb wirklich umsetzbar, welche Verfahren bereiten Probleme
  - b. Verschlüsselung auf MAC-Ebene: wirklich handhabbar?
  - c. PoE am Ende? Wirtschaftlichkeit und Zukunftsorientierung

5. Sonderthemen
  - a. Produktions-Steuerungen und Gebäude-Management im Netzwerk: isolieren oder integrieren?
  - b. Voice- und Video im Netzwerk: was bedeutet der Trend hin zu Kollaborations-Lösungen?

Der Vertiefungstag greift auch in diesem Jahr Themen auf, die hochaktuell, aber zu komplex für Einzelvorträge sind. Dies sind in diesem Jahr:

Workshop 1: Voice und Video im Netzwerk  
 Workshop 2: Disaster Recovery  
 Workshop 3: IPv6: Parallelbetrieb und Migration

Die Workshops gehen den ganzen Tag bis zum Ende der Veranstaltung. Von daher wählen Teilnehmer Ihren Workshop vor Beginn der Veranstaltung aus. Allerdings besteht während des Tages die Möglichkeit, zwischen den Workshops zu wechseln.

Das neue Plus-Modul ermöglicht die optimale Vorbereitung auf das Netzwerk-Redesign Forum durch unsere HD-Videos, die durch ComConsult Study.tv produziert werden. Zum Abspielen der Videos ist ein von uns bereitgestellter Software-Client erforderlich.

Das Plus-Programm zum Netzwerk-Redesign-Forum umfasst:

1. Virtualisierung im Rechenzentrum und die Einbindung in Netzwerke, Dr. Jürgen Suppan
2. Carrier Ethernet in der Analyse, Dr. Franz-Joachim Kauffels
3. 10, 40, 100 Gigabit-Ethernet, Dr. Franz-Joachim Kauffels
4. Fazit der Veranstaltung mit Mitschnitten der Highlights ausgewählter Vorträge, Dr. Jürgen Suppan

Fax-Antwort an ComConsult 02408/955-399

## Anmeldung

# Netzwerk-Redesign Forum 2010

Ich buche den Kongress  
**Netzwerk-Redesign Forum 2010**

mit Workshop am 4. Tag  
 vom 26.04. - 29.04.10 in Königswinter  
 zum Preis von € 2.290,- zzgl. MwSt.

### Workshopauswahl

- Workshop 1: Voice und Video im Netzwerk  
 Workshop 2: Disaster Recovery  
 Workshop 3: IPv6: Parallelbetrieb und Migration

ohne Workshop am 4. Tag  
 vom 26.04. - 28.04.10 in Königswinter  
 zum Preis von € 1.890,- zzgl. MwSt.

inkl. Report „Neue Standards bei IEEE, IETF und ANSI/INCITS“  
 zum Preis von 210,- € zzgl. MwSt.

inkl. Plus-Modul mit Vorbereitungs- und Nachlaufvideos  
 zum Preis von 299,- € zzgl. MwSt.

Bitte reservieren Sie mir ein Zimmer  
 vom \_\_\_\_\_ bis \_\_\_\_\_ 10

im Maritim Hotel Königswinter.

Vorname \_\_\_\_\_

Nachname \_\_\_\_\_

Firma \_\_\_\_\_

Telefon/Fax \_\_\_\_\_

Straße \_\_\_\_\_

PLZ, Ort \_\_\_\_\_

eMail \_\_\_\_\_

Unterschrift \_\_\_\_\_

 Buchen Sie über unsere Web-Seite  
[www.comconsult-akademie.de](http://www.comconsult-akademie.de)

Netzwerk-Redesign Forum 2010 - Programmübersicht

**Montag, den 26.04.2010**

**9:30 bis 11:00 Uhr**

**Markt- und Technologie-Analyse:**

**Neue IT-Architekturen und die Konsequenzen für Netzwerke: wie viel Bandbreite brauchen wir in Zukunft?**

- Neue Architekturen im Rechenzentrum
  - Web-Architekturen
  - Virtualisierung
  - Cloud-Computing
  - Speicher-Zentralisierung und Konsolidierung
- Endgeräte-Technologien im Wandel
  - Desktop-Virtualisierung
  - Applikationen im Browser: das Ende traditioneller Applikationen? Brauchen wir einen neuen Typ-Endgeräte à la Chrome oder Apple iPad?
  - Multi-Media-Applikationen im Netzwerk
- Auswirkung auf Netzwerke
  - Bandbreite im Rechenzentrum
  - Bandbreite im Campus-Backbone
  - Bandbreite für Endgeräte-Anbindung
  - Bandbreite WAN
  - Anforderungen an Komponenten
- Auswirkung auf Hersteller
  - Das Ende der Application Aware Networks?
  - Verdrängt Bandbreitenbedarf den Multi-Blade-Core-Switch?
  - Verschieben sich Marktanteile?
- Ausblick auf die nächsten Jahre

*Dr. Jürgen Suppan,  
ComConsult Research*

**11:00 bis 11:30 Uhr - Kaffeepause**

**11:30 bis 12:30 Uhr**

**Migration zu IPv6 im Netzwerk**

- Der Zeitpunkt: wann wird IPv6 zum Muss?
- Die Aufgabe: IPv6 im Netzwerk, was bedeutet das?
- Die Probleme: welche Komponenten sind kritisch?

- Die Migration: welche Alternativen bestehen?
- Ausblick und Fazit

*Dipl.-Inform. Petra Borowka-Gatzweiler,  
Unternehmensberatung Netzwerke UBN*

**12:30 bis 14:00 Uhr - Mittagspause**

**14:00 bis 15:30 Uhr**

**Neue Standards für WAN und Backbone: das Ende von OSPF?**

- Provider-Technologie im Unternehmen?
- Carrier Ethernet vs. MPLS
- Was passiert in Zukunft im WAN?

*Dr. Franz-Joachim Kauffels,  
Unternehmensberater*

**15:30 bis 16:00 Uhr - Kaffeepause**

**16:00 bis 17:15 Uhr**

**Brauchen wir mehr als Ethernet und IP? Wer braucht QoS und FCoE?**

- Erfahrungen aus bestehenden Netzwerken
- Was leistet die Basis-Technologie Netzwerk wirklich?
- Zurück zur Basis: Ethernet und IP reichen aus

*Dr. Behrooz Moayeri,  
ComConsult Beratung und Planung GmbH*

**17:15 bis 18:00 Uhr**

**Core-Switches 2010**

- Wann sterben alte Generationen?
- Minimalanforderung 100 Gb-Switching
- Technologiehaufen (Lossless, QoS, dynamische VLANs, ...)
- Was bekommen wir? Was brauchen wir?

*Dr. Franz-Joachim Kauffels,  
Unternehmensberater*

**ab 18:00 Uhr - Happy Hour**

**Dienstag, den 27.04.2010**

**9:00 bis 10:00 Uhr**

**Neue Switching-Standards**

- Neue Funktionen und Standards bei IEEE und IETF
- Das Ende von Spanning Tree: der Kampf zwischen Trill und SPB
- DCB, FCoE, FC-BB-5
- OSPF noch zeitgemäß?
- Ausblick

*Dipl.-Inform. Petra Borowka-Gatzweiler,  
Unternehmensberatung Netzwerke UBN*

**10:00 bis 11:00 Uhr**

**Wireless LANs nach der Verabschiedung von IEEE 802.11n**

- Was bringt die Verabschiedung von 11n?
- Wie sehen zukünftige Produkte aus, was leisten sie?
- Wie sieht eine geeignete Planung aus?
- Interoperability: welche Rolle spielen Standards in Zukunft?
- Trouble Shooting: was kann passieren, was ist zu tun?

*Dr. Simon Hoff, ComConsult Beratung und Planung GmbH*

**11:00 bis 11:30 Uhr - Kaffeepause**

**11:30 bis 12:30 Uhr**

**Gebäudeverkabelung im Wandel der Zeit**

- Aktuelle EN 51073-1, was ist neu und wie ist es zu bewerten?
- EN 50174-2, kaum bekannt und trotzdem wichtig?
- Wie zukunftssicher sind bestehende Installationen?
- Glasfaser versus Kupfer in der Tertiärverkabelung

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

**12:30 bis 14:00 Uhr - Mittagspause**

**14:00 bis 15:00 Uhr**

**Sicherheit im Netzwerk 2010**

- Sicherheit in der Tagespraxis des Netzwerk-Betreibers
- Tücken bei IEEE 802.1X
- Ist LLDP-MED zu unsicher?
- Kommt die MAC-Verschlüsselung mit 1XREV?
- Dynamische VLAN-Zuordnung bei Kaskadierung?
- Trennung von Sicherheitszonen mittels VLAN, VRF und MPLS zulässig?

*Dr. Simon Hoff,*

*ComConsult Beratung und Planung GmbH*

**15:00 bis 15:30 Uhr**

**Produktions-Steuerungen und Gebäude-Management im Netzwerk**

- Produktions-Steuerungen im Netzwerk: Status Quo und Trends
- Gebäude-Management im Netzwerk: Trend oder Sonderfall?
- Resultierende Anforderungen an Netzwerke
- Isolation kontra Integration: wer muss vor wem geschützt werden?
- Wireless-Techniken in der Automatisierung im Vergleich zu traditionellen WLANs

*Dr. Simon Hoff,*

*ComConsult Beratung und Planung GmbH*

**15:30 bis 16:00 Uhr - Kaffeepause**

**16:00 bis 17:00 Uhr**

**Analyse: Voice- und Video im Netzwerk**

- IP-Telefonie und Unified Communications: Status
- Wie werden UC-Lösungen in Zukunft aussehen?
- Was passiert bei Video-Technik im Netzwerk?
- Strategien der Hauptanbieter im Markt
- Wird Microsoft das Thema Kollaboration im Markt etablieren?
- Konsequenzen für Netzwerke

*Dr. Jürgen Suppan,  
ComConsult Research*

Netzwerk-Redesign Forum 2010 - Programmübersicht

**Mittwoch, den 28.04.2010**

**09:00 bis 10:30 Uhr**

**Markt-Analyse: Cisco kontra HP, Multi-Blade kontra Routing-Core: wohin geht der Markt?**

- Was bedeutet die Übernahme von 3Com durch HP für den Markt?
- HP kontra Cisco: Kampf der Konzepte
- Wie sehen Netzkomponenten in Zukunft aus?
- Welche Produkte sind End-of-Life?
- Multi-Blade kontra Routing-Core: wer wird überleben?
- Ausblick

*Dipl.-Inform. Petra Borowka-Gatzweiler,  
Unternehmensberatung Netzwerke UBN*

**16:00 bis 16:45 Uhr**

**Trouble-Shooting und Service-Level-Management 2010: wo sind die Grenzen?**

- Aufgaben in modernen Netzwerken
- Neue Messgeräte und Verfahren
- Berichte und Beispiele aus der Trouble-Shooting-Praxis

N.N.

**10:30 bis 15:30 Uhr**

**Hersteller stellen sich der Diskussion:**

- Bandbreitenbedarf
- Zukunftsorientierte Produkt-Strategien
- Neue Switching-Standards
- LAN-Design: wohin geht der Weg?

**11:00 bis 11:30 Uhr - Kaffeepause**

**12:30 bis 14:00 Uhr - Mittagspause**

**15:30 bis 16:00 Uhr - Kaffeepause**

**Donnerstag, den 29.04.2010 - Ein-Tages-Intensiv-Trainings/Workshops - 09:00 - 15:30 Uhr**

**Die Session laufen parallel über den ganzen Tag!  
BITTE BEI DER ANMELDUNG EIN THEMA ANKREUZEN!!**

**Workshop 1:**

**Voice und Video im Netzwerk**

- Bedarfswertung aus der Sicht von Unified Communication
- Gestaltungsparameter in LAN und WAN
- Prüfung bestehender Netzwerke
- Redesign-Gesichtspunkte

*Dipl.-Inform. Petra Borowka-Gatzweiler,  
Unternehmensberatung Netzwerke UBN*

**10:30 bis 11:00 Uhr - Kaffeepause**

**12:30 bis 14:00 Uhr - Mittagspause**

**15:30 Uhr - Ende der Veranstaltung**

**Workshop 2:**

**Disaster Recovery**

- Aufgabenstellung
- 10/40/100 auch über Distanz
- Eigenheiten optischer Transportnetze
- Konventionelle Lösungen
- Revolutionärer Ansatz
- Fazit und Konsequenzen

*Dr. Franz-Joachim Kauffels,  
Unternehmensberater*

**Workshop 3:**

**IPv6: Parallelbetrieb und Migration**

- Gründe für (Wahl des Zeitpunkts zum) Einstieg in IPv6
- Grundlegende Mechanismen von IPv6 - Kurzeinführung und Anschauungsbeispiele
- Mechanismen zur Koexistenz / Kopplung von IPv4 und IPv6 in einer (ggf. langen) Übergangsphase
- Optionen zum Umgang mit der Übergangsphase
- IPv6 und Sicherheit

*Dipl.-Inform. Oliver Flüs,  
ComConsult Beratung und Planung GmbH*

## Zweitthema

# Macht Carrier-Ethernet das WAN zum LAN?

Fortsetzung von Seite 1



Dipl.-Inform. Andreas Meder ist im Team der ComConsult Beratung und Planung GmbH als Senior Consultant beschäftigt. Er verfügt aufgrund seiner langjährigen beruflichen Praxis über umfangreiche Kenntnisse und Erfahrungen aus den Bereichen Konzipierung und Betrieb von Netzwerken. Sein Themenschwerpunkt als Berater und Planer liegt in den Bereichen Internetworking und IT-Security. Zu diesen Themengebieten ist er als Referent bei der ComConsult Akademie tätig.

## 1. Carrier-Ethernet

Über die immer mehr zunehmende Bedeutung der Standortvernetzung von Unternehmen oder Institutionen und die damit einhergehenden steigenden Anforderungen an die nutzbaren Kapazitäten einerseits und die Zuverlässigkeit der Ressource Weitverkehrsnetz andererseits ist - nicht zuletzt an dieser Stelle - bereits mehrfach berichtet worden. Der Markt hat diesem Umstand durch entsprechende Angebote (zumindest teilweise) Rechnung getragen - und tut dies weiterhin: in den aktuellen Planungs- und Realisierungsprojekten im Bereich der Weitverkehrsvernetzung konnte der Autor nach wie vor kein signifikantes Abflauen des Trends hin zu immer höheren Bandbreiten bei gleichzeitig sinkenden Kosten feststellen.

Mit dem Aufkommen erster WAN-Services, die dem Kunden als Netzabschluss einen Ethernet-Port anstelle der klassischen - typischerweise teuren und komplexen - Schnittstellen offerierten, tritt nun verstärkt das Bestreben eben dieser Kunden zutage, über das Schnittstellen-Format hinaus auch die aus dem lokalen Netzwerk gewohnte Funktionalität von Ethernet im WAN zu erhalten. Die Vorteile eines solchen Ansatzes liegen auf der Hand:

- Niedrige Kosten für die Netzhardware, da standardisierte massenhaft produzierte Komponenten verbaut werden können.
- Wegfall der Notwendigkeit spezieller WAN-Router, die nicht nur die entsprechenden WAN-Schnittstellen anbieten, sondern auch den Protokollwechsel vom LAN zum WAN ermöglichen.

- WAN und LAN können bei der Planung von Netzarchitekturen gedanklich als Einheit angesehen werden, so dass insbesondere Protokollmechanismen im gesamten Netz ohne Protokollbruch eingesetzt werden können.

Nach den Gesetzen des Marktes führt die so motivierte verstärkte Nachfrage zu einem entsprechend immer breiter werdenden Angebot einerseits und - da technischer Wildwuchs grundsätzlich nicht erstrebenswert ist und deshalb das Umsichgreifen proprietärer Verfahren und Lösungen weder im Interesse der Anbieter noch der Kunden sein kann - zu entsprechenden Standardisierungsbemühungen für derartige „Carrier Ethernet“-Lösungen andererseits. Diese Bemühungen werden derzeit maßgeblich im Metro Ethernet Forum (MEF) gebündelt. Das MEF definiert Carrier Ethernet wie folgt:

*Carrier Ethernet ist ein universeller, standardisierter Carrier-Class Netzwerk-Service. Er ist definiert durch fünf Attribute, die ihn vom gewohnten LAN-basierten Ethernet unterscheiden:*

- Skalierbarkeit
- Zuverlässigkeit
- Service Management
- Quality of Service
- Standardisierte Services

Der Carrier, der diesen Service anbieten will, muss dazu entsprechende standardisierte Netzelemente bereitstellen, die die zu transportierenden Ethernet-Frames weltweit übertragen - unter Nutzung nicht nur von Ethernet-basierten Netzen, sondern auch auf Basis althergebrachter Technologien und darauf basierender

Netzplattformen. Dazu muss der Ethernet-Datenstrom in geeigneter Weise verkapselt werden, so dass die gekapselten Dateneinheiten einerseits problemlos und zuverlässig in der Netzplattform übertragen werden können, und andererseits übliche Features von Ethernet abgebildet werden können. Den so gebildeten Tunnel bezeichnet man auch als „Ethernet Virtual Connection“ (EVC). Das MEF hat dazu entsprechende Vorgaben für die jeweils verwendeten Mechanismen und deren Übergabeschnittstellen spezifiziert, die ein Zusammenwirken unterschiedlicher Hersteller und Anbieter gewährleisten sollen. Welche Mechanismen insbesondere für die Verkapselung eingesetzt werden, ist nicht näher spezifiziert, so dass bereits heute unterschiedliche Ansätze existieren. Dies ist auch durchaus sinnvoll, ermöglicht es doch die möglichst flexible Nutzung verschiedenster vorhandener Netzplattformen. Beispiele für solche Tunnel-Mechanismen sind u.a. Ethernet over MPLS, Ethernet over SDH oder Ethernet over RPR.

Nun ist offenkundig Ethernet nicht notwendigerweise gleich Ethernet. Die Übertragung von Ethernet-Frames im WAN - auch ohne nativ Ethernet-fähige Netzinfrastruktur - wird schon seit einiger Zeit angeboten, etwa in Form von Ethernet-Verbindungen zwischen Standorten. Über EthernetConnect als Beispiel für ein derartiges Produkt hat der Autor an dieser Stelle bereits berichtet; vergleichbare Services werden aber auch von Mitbewerbern unter durchaus ähnlich klingenden Produktnamen vermarktet. Ein solcher Service weist aber - je nach Netzkonstellation aus Kundensicht - den Nachteil auf, dass zum Verbinden mehrerer Lokationen mithilfe

## Macht Carrier-Ethernet das WAN zum LAN?

dieser Technik eine große Zahl von Verbindungen notwendig ist, wenn diese Lokationen analog zum LAN alle direkt miteinander verbunden sein sollen. Es werden also in der Praxis meist weitergehende Konzepte benötigt, die über reine Punkt-zu-Punkt-Services hinausgehen. Hierfür hat das MEF drei grundlegende Service-Typen spezifiziert:

### • E-Line

E-Line beschreibt das klassische Punkt-zu-Punkt-Verbindungsmodell. Einsatzgebiete sind z.B. ethernetbasierte Inter-Netzwerke oder die Verbindung zweier entfernter Ethernet-Switches. Je nachdem, ob bei der Realisierung je Anschluss nur ein oder optional mehrere EVCs gemeinsam abgebildet werden, bezeichnet man entsprechende Dienste auch als „Ethernet Private Line“ (EPL) bzw. „Ethernet Virtual Private Line“ (E-PL).

### • E-LAN

E-LAN beschreibt ein Multipunkt-Verbindungsmodell, d.h. alle Anschlusspunkte können sich auf Basis eines solchen Dienstes unmittelbar gegenseitig erreichen. Auf der Basis dieses Service-Typs lassen sich transparente LAN-Services realisieren. Auch hier wird je nach Ausprägung der Schnittstelle und deren Multiplexing-Eigenschaften wieder unterschieden in „Ethernet Private LAN“ (EP-LAN) und „Ethernet Virtual Private LAN“ (EVP-LAN) Services.

### • E-Tree

E-Tree beschreibt ein spezielles Multipunkt-Verbindungsmodell, bei dem bestimmte Knoten („Blätter“) nur mit einem bestimmten Knoten („Wurzel“) kommunizieren können, nicht jedoch mit anderen Blättern. Es ist hauptsächlich für die Bereitstellung bestimmter netzbasierter Dienste, die zentral für eine gewisse Klientel angeboten werden, gedacht (z.B. Triple-Play-Angebote).

In die Kategorie E-LAN fallen unter anderem auch Implementierungen von „Virtual Private LAN Services“ (VPLS). Für letztere existieren in Form von RFC 4761 und RFC 4762 zwei IETF-Standards, in denen nicht nur die Verkapselung zum Transport über paketvermittelnde Netze spezifiziert ist, sondern insbesondere auch, wie in einem solchen Netz die Existenz von Layer 2-Anschlusspunkten signalisiert wird. Letzteres ist u.a. notwendig, um ohne manuellen Konfigurationsaufwand die jeweils genutzten MAC-Adressen an allen Anschlusspunkten bekannt zu machen. Solche Virtual Private LAN Services bieten offenbar die besten Voraussetzungen, dem Ziel mög-

lichst nahe zu kommen, das auf solcher Basis realisierte WAN wie ein LAN ansehen zu können.

## 2. Ethernet fürs Corporate Network - ein aktuelles Projekt

Die oben angestellten Überlegungen sind keineswegs akademischer Natur: es gibt entsprechende Angebote am Markt, so dass bei aktuellen und noch mehr bei zukünftigen Netzplanungen dieser Option Beachtung zuteil werden sollte. Doch kann man - Stand heute - tatsächlich so weit gehen, LAN und WAN über den sprichwörtlich einen Kamm zu scheren? Der Autor hatte Gelegenheit, im Rahmen eines aktuellen Projekts die angebotenen Leistungen einiger nationaler Anbieter insbesondere unter diesem Gesichtspunkt unter die Lupe zu nehmen. Von den dabei gemachten Erfahrungen soll im Folgenden die Rede sein.

Bei dem besagten Projekt waren insgesamt fünf Standorte miteinander zu vernetzen. Aufgrund des Geschäftsumfelds, in dem das Unternehmen tätig ist, waren netzbedingte Produktionsausfälle unbedingt zu minimieren, so dass sich entsprechend hohe Anforderungen an die Verfügbarkeit ergaben, die nicht ohne explizite Redundanzmaßnahmen erfüllbar waren. Da darüber hinaus der Wunsch bestand, hinsichtlich des Einsatzes von Kommunikationsprotokollen und insbesondere (s.o.) Redundanzverfahren zum einen autark und zum anderen möglichst flexibel zu sein, wurde ein ungemanagter Ethernet-Service projektiert und letztlich ausgeschrieben.

Eine bereits im Vorfeld durchgeführte Marktsichtung ergab, dass entsprechende Services - auch in der einem LAN am nächsten kommenden Ausprägung als EVP-LAN bzw. VPLS - hierzulande verfügbar sind; insofern sollte es also keine grundsätzlichen Schwierigkeiten geben. Allerdings steckt gewöhnlich - und auch in diesem Fall - der Teufel im Detail, d.h. es war zu verifizieren, inwieweit sich LAN-übliche Techniken tatsächlich 1:1 im WAN umsetzen lassen würden, bzw. wo diesbezüglich Abstriche zu machen sein würden.

Was das Projekt vor allem interessant machte, war, dass die insgesamt drei angebotenen Lösungen, die zumindest die Ausschlusskriterien erfüllten, auf mehr oder weniger unterschiedlichen technologischen Ansätzen basierten. Damit einher gingen entsprechende technische Vor- und Nachteile, vor allem auch im Hinblick auf die Abbildbarkeit der LAN-Mechanismen.

Im Folgenden sollen die einzelnen Lö-

sungen kurz beschrieben und vor allem die jeweiligen Besonderheiten herausgestellt werden; dabei soll ausdrücklich darauf hingewiesen werden, dass diese kurze Aufstellung von Anbietern und Lösungen nicht notwendigerweise abschließend ist. Es ist vielmehr davon auszugehen, dass kurz- und mittelfristig auch andere Carrier mit entsprechenden Services am Markt antreten werden, zumal prinzipiell jede MPLS-basierte Carrier-Infrastruktur auch entsprechende virtuelle Ethernet-Services bereitstellen kann...

### 2.1 VT Ethernet LAN der Versatel AG

Die von Versatel angebotene Lösung basiert auf dem Versatel NGN Backbone (Next Generation Network). Dieser stellt de facto ein MPLS basiertes Metro Ethernet Netzwerk nach dem VPLS Standard dar, so dass sich die Lösung kurz gefasst als „Ethernet over MPLS“ beschreiben ließe.

Der Funktionsumfang einer derartigen Netzrealisierung und damit in diesem Fall des NGN entspricht gewissermaßen einem virtuellen Ethernet Switch (Virtual Switch Instance, VSI): Für angeschlossene LAN-Komponenten in den Standorten des Kunden verhält sich das Netz im Wesentlichen wie ein zentraler Core-Switch. Dabei wird die Transportleistung jedoch vollkommen transparent erbracht, d.h. das Netz überträgt alle Ethernet-Frames nicht nur ohne Veränderung an die jeweiligen Empfänger-MAC-Adressen, sondern die VSI ist auch nicht „sichtbar“ und nimmt insbesondere nicht an etwaigem Protokoll-Datenverkehr mit Kunden-Netzequipment teil. (siehe Abbildung 1)

Die Anschaltung an das NGN erfolgt - je nach Situation vor Ort - über natives Ethernet mittels Versatel-Glasfaser oder über Ethernet over SDH, wenn lokale Subcarrier eingesetzt werden müssen. Aufgrund der Verfügbarkeitsanforderungen wurden hier grundsätzlich je zwei vollständig entkoppelte Anbindungen an den Backbone vorgesehen. Der Backbone selber kann aufgrund seiner redundanten Topologie als hinreichend ausfallsicher angesehen werden.

### 2.2. Ethernet Private Network (E-PN) der COLT Telecom GmbH

Auch die COLT Lösung nutzt ein sogenanntes Next Generation Network, d.h. eine gemeinsame Plattform, über die nach Möglichkeit alle Netzwerk-Services realisiert werden können. Die technische Basis ist auch hier MPLS, allerdings bietet der Backbone selbst - anders als bei Versatel - keinen E-LAN-Service, sondern lediglich E-Line.

## Macht Carrier-Ethernet das WAN zum LAN?

Die kundenseitig gewünschte E-LAN-Funktionalität wird bei der COLT-Lösung durch dedizierte Switch-Hardware in einem geeigneten Knotenpunkt des Backbones bereitgestellt. De facto werden also bei dieser Lösung die einzelnen LANs per „langem Ethernet-Kabel“ mit einem zentralen Switch verbunden. Bei diesem Switch handelt es sich um eine Einschubkarte in ein Carrier-Class-Chassis, die die Kundenports in der benötigten Anzahl zur Verfügung stellt. (siehe Abbildung 2)

Das Redundanzthema wird hier zunächst ähnlich behandelt wie zuvor bereits dargestellt: wegeredundante Anbindung der Kundenlokation an den Backbone. Es kommen allerdings zwei Besonderheiten zum Tragen:

- Zwar ist auch hier der Backbone als per se hinreichend verfügbar anzusehen, allerdings gilt das nicht für die dedizierte Switch-Hardware, auf der die Kundenlokationen aufgeschaltet sind. Diese ist bei entsprechenden Anforderungen wie im vorliegenden Fall durch eine zweite Hardware in einem anderen Netzknoten abzusichern, die mit der ersten wiederum redundant verbunden ist. Jeder Standort ist dann mit je einem virtuellen Ethernet-Link an beide Switches angeschlossen.

Bei moderateren Anforderungen an die Verfügbarkeit kann ggf. auf diese Hardware-Redundanz verzichtet werden, da die Unterbrechungsdauern bei Ausfall eines solchen Switch-Karte aufgrund der Rahmenbedingungen in den Netzknoten (RZ-Bedingungen, Betriebspersonal rund um die Uhr vor Ort) vergleichsweise kurz sind; nach Anbieteraussage liegen sie im Bereich von ca. 15 Minuten. Zu bedenken ist freilich, dass von einer solchen Störung alle Standorte betroffen wären, so dass sich die Gesamtstörungsdauer eventuell doch in nicht akzeptablen Größenordnungen bewegen könnte.

- COLT nutzt bei Direktanschlüssen, d.h. solchen, bei denen der Kundenstandort über eine COLT-Glasfaser ohne Sub-Carrier an den Backbone angeschlossen wird, eine Ringtopologie für jeden Anschluss. Hierdurch ist eine zusätzliche Redundanz im Bereich des Local Loop gegeben.

### 2.3 Ethernet VPN (Deutsche Telekom AG)

Bei der Realisierung ihres Produkts Ethernet VPN schlägt die Deutsche Telekom einen anderen Weg ein als die bisher betrachteten Mitbewerber. Ethernet VPN basiert nicht auf einem MPLS-Backbone,

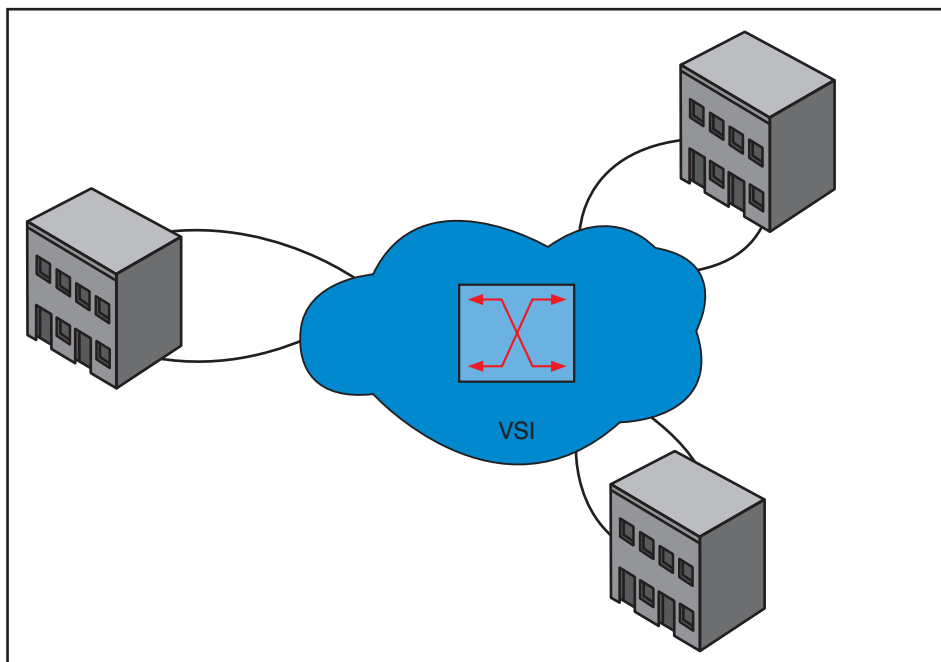


Abbildung 1: VT Ethernet LAN (Versatel)

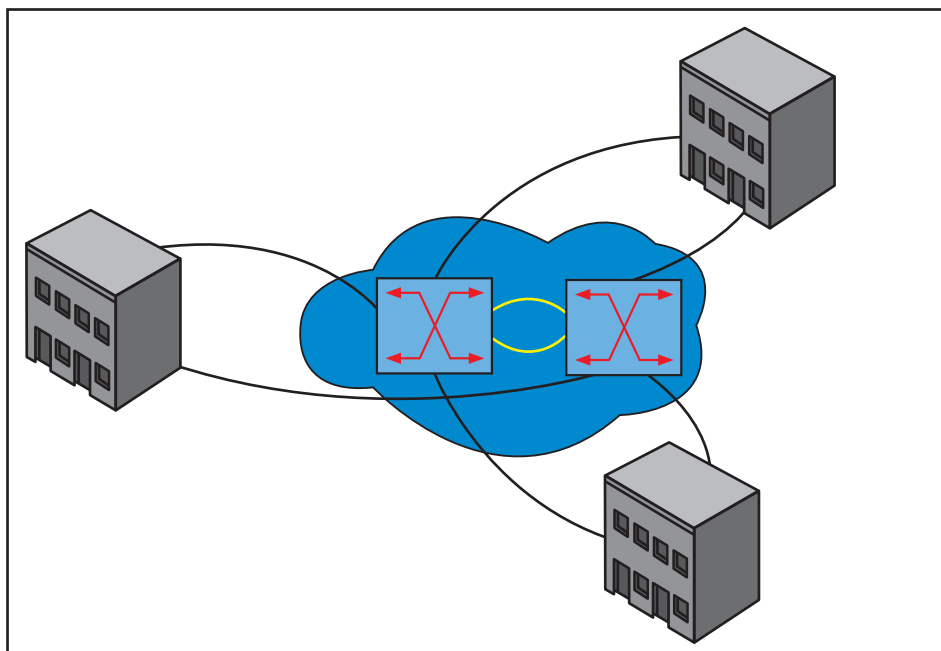


Abbildung 2: E-PN (COLT)

sondern setzt auf der Resilient Packet Ring (RPR) Technologie nach IEEE 802.17 auf. RPR ist eine bis dato am Markt wenig verbreitete Technologie, die einen effizienteren Datentransport über glasfaserbasierte Ringstrukturen ermöglichen soll, als dies mit dem klassischen TDM-basierten SDH-Verfahren möglich ist. Gleichwohl wurde RPR so spezifiziert, dass die SDH-Infrastrukturen weiterhin nutzbar bleiben. Somit ist für Carrier, die ihre Netzphysik zumindest anteilig auf RPR umstellen, ein

weitreichender Investitionsschutz gegeben. RPR behebt vor allem zwei wesentliche Nachteile von SDH bei der Abbildung von Datennetzen:

- SDH (Synchrone Digitale Hierarchie) teilt einen gewissen Anteil der zur Verfügung stehenden Übertragungskapazitäten mittels Time Division Multiplex (TDM) den eingerichteten Netzverbindungen fest zu. Damit steht diese Kapazität der jeweiligen Verbindung ex-

## Macht Carrier-Ethernet das WAN zum LAN?

klusiv zur Verfügung und kann selbst dann nicht von anderen Verbindungen genutzt werden, wenn die erste Verbindung sie nicht benötigt. Diese Vorgehensweise ist optimiert für z.B. Sprachverbindungen, jedoch nicht für moderne Datennetze, in denen auf den höheren OSI-Schichten praktisch ausschließlich paketbasierte Mechanismen zum Einsatz kommen - heutzutage im Wesentlichen Ethernet und IP.

- SDH basiert auf doppelten Glasfaserringen mit gegenläufiger Kommunikationsrichtung. Dabei dient der zweite Ring ausschließlich der Ausfallsicherung; er wird also im Regelfall nicht zur Kommunikation genutzt. Somit wird die durch die Infrastruktur in Summe darstellbare Kapazität nur zur Hälfte tatsächlich nutzbar gemacht.

RPR nutzt anders als SDH beide gegenläufigen Ringe (Ringlets) produktiv und arbeitet statt mit festen Zuweisungen paketorientiert. Somit können wesentlich höhere Kapazitäten realisiert werden. Erkauft wird dies mit potenziellen Kapazitätseinschränkungen im Fall einer Netzstörung, da dann beide Ringlets zu einem großen Ring zusammengeschaltet werden, in dem die verfügbare Bandbreite dann auf entsprechend mehr Stationen verteilt werden muss, und mit einem potenziell größeren Jitter, da an den Einspeisungspunkten in den Ring bei zeitgleich ankommenden Paketen diese nacheinander abgearbeitet werden müssen. Ein sogenannter Fairness-Algorithmus sorgt dafür, dass es dabei nicht zu inakzeptablen Wartezeiten kommt.

Beim Aufbau eines Ethernet VPN schaltet die Deutsche Telekom für den jeweiligen Kunden einen dedizierten RPR auf Basis der gegebenen Backbone-Strukturen. Somit bleibt das realisierte Netz zwar aufgrund der Ringeigenschaft ein Shared Medium, aber anders als z.B. MPLS-Netze erstreckt sich diese Eigenschaft nur auf den jeweiligen Kunden, nicht auf die Gesamtheit aller Kunden des Carriers. Bei Planungen zur notwendigen Kapazität (Stichwort „Überbuchung“) kann man sich also auf die Berücksichtigung der eigenen Belange beschränken; weitere Kunden desselben Carriers können diesbezüglich vollkommen außen vor bleiben. Die E-LAN-Funktionalität wird bei Ethernet VPN vom Ring selbst bereitgestellt; es kommt also auch hier (analog zur Lösung von Versatel) keine dedizierte Switch-Hardware zum Einsatz, sondern der Ring verhält sich wie ein Switch (was nichts bahnbrechend Neues ist: man denke nur an die seligen Token-Ring-Switches; auch dort entsprachen

sich Ring und Switch hinsichtlich ihrer Funktionalität). (siehe Abbildung 3)

Die Anschaltung der Kundenstandorte an den Ring erfolgt mittels Ethernet-Connect-Leitungen. Aufgrund der Verfügbarkeitsanforderungen im vorliegenden Projekt wurde dabei nicht nur (s.o.) eine redundante, knoten- und kantendisjunkte Anbindung geplant, sondern jeder dieser beiden Ethernet-Links in sich nochmals redundant ausgeführt. Insgesamt führte dies dann zu einer Vierfach-Abstützung jedes Standorts. Dies führt naturgemäß zu entsprechend höheren Kosten und war seitens des Kunden auch nicht explizit gewünscht, resultierte aber aus den Anforderungen an die maximalen Entstörzeiten, die eine andere Bauweise nicht zuließen.

### 3. WAN + Ethernet = LAN?

Wie man sieht, gibt es einen bunten Strauß von Möglichkeiten, Standorte mittels Ethernet zu vernetzen. Hinsichtlich der Grundanforderung, Ethernet transparent und hochverfügbar zu übertragen, gibt es auch keinerlei Einschränkungen, wenn es auch im Detail Unterschiede zwischen den Lösungen gibt. Spannend wird es dann, wenn man spezifische Anforderungen, insbesondere solche, die ihren Ursprung in LAN-typischen Mechanismen haben, betrachtet. Wir wollen dies exemplarisch für einige Aspekte aus besagtem WAN-Projekt untersuchen...

#### • Anschluss an LAN-Switches

Zum Anschluss klassischer WAN-Leitungen bedarf es entsprechend geeigneter

ter Router; bei Ethernet sollte das doch nicht erforderlich sein...

Und in der Tat: die Ethernet-basierten Local Loops können unmittelbar an LAN-Komponenten angeschlossen werden. Inwieweit hierfür gleich standortinterne Core-Komponenten herangezogen werden, muss im Anschaltekonzept unter Berücksichtigung diverser Aspekte - unter anderem auch Sicherheitsüberlegungen - untersucht und spezifiziert werden; ggf. sind dedizierte Komponenten vorzuschalten. Letztere können aber wiederum LAN-Switches oder ggf. auch gleich Firewall-Systeme sein, falls etwa das Sicherheitskonzept eine entsprechende Entkopplung der Standorte vom WAN vorsieht.

#### • Quality of Service

Quality of Service (QoS) ist im Grunde eher ein Thema für WAN, nicht so sehr für LAN, da QoS typischerweise dort eine Rolle spielt, wo Mangel zielgerichtet verwaltet werden muss. In LANs herrscht aber normalerweise Mangel weder hinsichtlich der Kapazitäten noch hinsichtlich schneller Netzdurchlaufzeiten. Setzt man aber eine LAN-Technik wie Ethernet im WAN ein, wird automatisch auch QoS ein Thema, insbesondere, wenn unterschiedliche Datenströme mit unterschiedlichen Anforderungen vorhanden sind (z.B. Voice- im Gegensatz zu sonstigen Anwendungsdaten).

Bei Ethernet wird QoS auf Basis von VLAN-Tagging (IEEE 802.1 Q/p) implementiert. Im vorliegenden Fall war al-

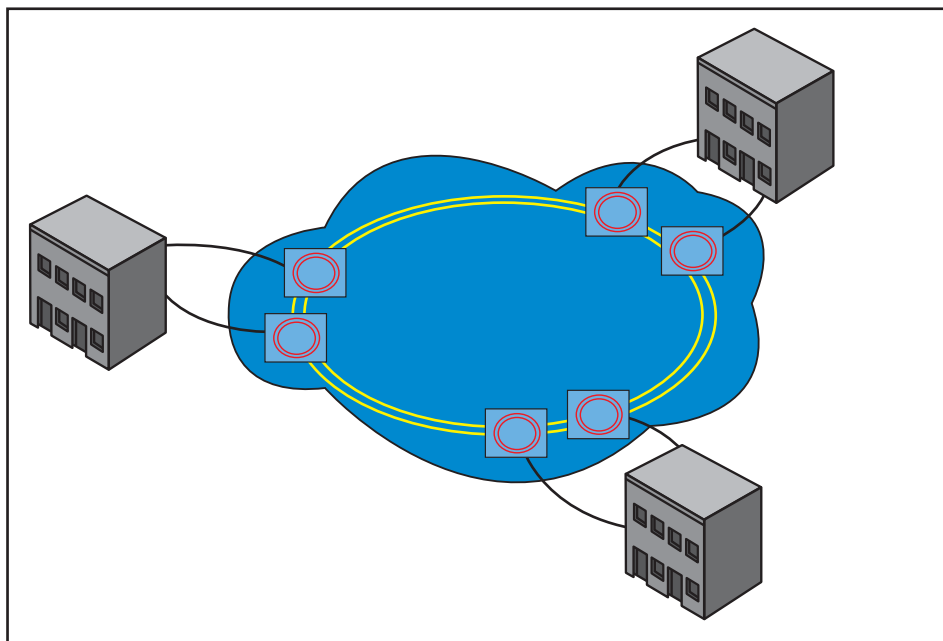


Abbildung 3: Ethernet VPN (Telekom)

## Macht Carrier-Ethernet das WAN zum LAN?

so zu prüfen, welche der Lösungen diesen Mechanismus unterstützt. Dabei ist Sorgfalt bei der Bewertung der diesbezüglichen Carrier-Aussagen geboten: mit Unterstützung ist nicht die transparente Übertragung der entsprechenden Tagging-Informationen gemeint, sondern die Auswertung dieser Tags und darauf basierende Priorisierung der Ethernet-Frames in der Netzplattform. Diese Funktionalität war beispielsweise bei der Lösung von Versatel zum Zeitpunkt der Ausschreibung nicht gegeben; sie soll allerdings zeitnah eingeführt werden, sobald die eingesetzte Netzhardware dies herstellerseitig unterstützt.

- **Link Loss Forwarding**

Link Loss Forwarding (LLF) ist ein Mechanismus, mit dessen Hilfe die Kupfer-Ports der Ethernet-Abschlusskomponenten eines Ethernet Virtual Circuit im Falle einer Leitungsunterbrechung abgeschaltet werden. Ohne einen solchen Mechanismus würden angeschlossene Kunden-Switches diese Unterbrechung nicht feststellen (der eigene LAN-Link bleibt ja aktiv), so dass etwaige Redundanzmechanismen, die den Port-Status referenzieren, nicht korrekt arbeiten.

Bei E-Line-Implementierungen wird LLF typischerweise implementiert. Bei E-LAN scheint das derzeit am Markt nicht so zwangsläufig zu sein: Beispielsweise unterstützt die COLT-Lösung LLF nicht.

Glücklicherweise sind Redundanzmechanismen auf höheren OSI-Schichten auf dieses Feature nicht zwingend angewiesen, da sie z.B. über den Austausch von Statuspaketen die Funktion des Links mittelbar selber überwachen. Letzteres mag der geneigte Leser durchaus als Anregung verstehen, auch in „reinen“ Ethernet-Umgebungen im Corporate Network im Zweifel klassische Routing-basierte Redundanzverfahren in Erwägung zu ziehen - diese sind in aller Regel robuster und stellen weniger spezifische Anforderungen an die jeweiligen Netzschnittstellen...

- **(Split) Multi Link Trunking**

Multi Link Trunking (MLT, IEEE 802.3ad) ist ein Protokoll zur Aggregation von einzelnen Links zu einem gemeinsamen Link (Trunk) mit entsprechend erhöhter Kapazität. Split MLT ist ein Erweiterung dieses Standards durch Nortel, die die Aufteilung der aggregierten Links auf mehrere Switches erlaubt.

In Nortel-Umgebungen kann mithilfe von SMLT eine entsprechende Redundanz-Architektur inklusive Load-Balancing rea-

liert werden. Aber kann dieser Ansatz auch im WAN zum Tragen kommen?

Die Antwort ist (zumindest derzeit): Nein! Dafür gibt es zwei Gründe: Zum Einen unterstützt keiner der drei hier betrachteten Anbieter SMLT, und es steht auch zu erwarten, dass sich daran in Zukunft nichts Signifikantes ändern wird. Eine Unterstützung eines solchen Features würde eine Interaktion der Netzkomponenten des Carriers mit denen des Kunden implizieren; dies jedoch würde dem Transparenzgedanken widersprechen. Zum Anderen ist es meist nicht ratsam, einen solchen Mechanismus im WAN überhaupt einzusetzen; weniger wegen der Redundanzeigenschaft, als vielmehr um des Load-Balancings willen: Dieses erfolgt Packet-per-Packet, was bei auch nur geringfügig unterschiedlichen Paketlaufzeiten der aggregierten Links unweigerlich zu Reordering-Effekten im Rahmen der TCP-Sessions führt.

- **Load Sharing**

Load-Balancing mittels (S)MLT scheidet also aus, aber ein Load Sharing lässt sich mittels geeigneter Routing-Protokolle problemlos implementieren. Hier ist dann allerdings im Fall der RPR-basierten Lösung der Deutschen Telekom darauf zu achten, dass es sich um ein Shared Medium handelt, dessen Ressourcen insbesondere im Falle einer Störung im Netzbackbone potenziell knapp werden können.

Sollen alle Standorte ihre jeweiligen per Load Sharing aggregierten Bandbreiten uneingeschränkt nutzen können, muss dies bei der Auslegung des Rings und

damit dessen Kapazität berücksichtigt werden. Zu bedenken ist insbesondere, dass bei überlappenden Kommunikationsbeziehungen auf dem Ring innerhalb der von der Überlappung betroffenen Teilstrecke auch tatsächlich die maximale Summenbandbreite zur Verfügung steht.

#### 4. Ein WAN ist eben doch kein LAN...

..., möchte man sagen, und wird es wohl auch nicht werden. Dem stehen einerseits physikalische Beschränkungen (insbesondere unvermeidbare Paketlaufzeiten in ausgedehnten Netzen) und andererseits die Notwendigkeit einer sauberen Schnittstelle zwischen Kunde und Provider entgegen. Letztere verhindert (siehe die Anmerkungen zum Transparenzgedanken) wirkungsvoll das Zusammenspiel von Carrier- und Kundenkomponenten auf Protokollebene, was dann zur Nichtanwendbarkeit diverser LAN-typischer Mechanismen führt.

Abgesehen davon scheint aber nichtsdestotrotz die Ethernet-basierte Technik auch im Weitverkehrsumfeld unaufhaltsam auf dem Vormarsch zu sein. Auch von der wirtschaftlichen Seite bieten die aktuellen E-LAN-Lösungen Vorteile - sowohl gegenüber den klassischen WAN-Technologien als auch gegenüber MPLS.

Man muss aber - auch das hat dieses Projekt klar gezeigt - sich als Carrier-Kunde verstärkt wieder selbst in die Planung der Netzarchitektur einbringen, und zwar in gleicher Art und Weise wie bei den eigenen Standort-LANs - ohne dabei die (teils anbieterspezifischen) technologischen Besonderheiten von Carrier-Ethernet aus dem Auge zu verlieren.

## Seminar



### WAN-Planung für zentrale Dienste 15.03. - 17.03.10 in München

Wide Area Networks (WAN) müssen kostengünstig, leistungsfähig, skalierbar, hochverfügbar, sicher und managebar sein. Während bis vor wenigen Jahren langfristige WAN-Verträge von drei bis fünf Jahren abgeschlossen wurden, legt die dynamische Entwicklung nahe, die Vertragsbindung zu verkürzen, was mit einem ständigen Planungsprozess einhergeht. Dieser Umstand und die fortlaufenden Veränderungen im Markt zwingen zu einem permanenten Lern- und Informationsprozess, dem auch dieses 3-tägige Seminar dienen soll.

Referenten: Dipl.-Inform. Andreas Meder, Dr.-Ing. Behrooz Moayeri

Preis: € 1.690,- zzgl. MwSt.



Buchen Sie über unsere Web-Seite [www.comconsult-akademie.de](http://www.comconsult-akademie.de)

Aktuelles Seminar

# Aktuelle VPN-Technik

Die ComConsult Akademie veranstaltet vom 14.04. - 16.04.10 erstmalig ihr neues Seminar „Aktuelle VPN-Technik“ in Aachen.

Die Nutzung von VPN-Technik hat sich in der jüngeren Vergangenheit insbesondere im Bereich des Remote Zugriffs mobiler oder auch stationärer Anwender (Stichwort: Telearbeit) auf zentrale Ressourcen als mehr oder weniger Standard-Lösungsansatz etabliert. Aber auch zur kostenoptimierten Anbindung von (typischerweise kleineren) Remote-Standorten an Corporate WAN-Strukturen bewährt sich dieser Ansatz. Dieses Seminar vermittelt die für einen erfolgreichen VPN-Einsatz notwendigen Kenntnisse der aktuell relevanten Technologien. Alle wesentlichen Bausteine typischer Lösungen werden detailliert erklärt und anhand praktischer Projektbeispiele und Übungen wird der Weg zu einer erfolgreichen VPN-Lösung aufgezeigt.

Themenschwerpunkte dieses Seminars sind:

#### Kryptografische Grundlagen

- Welche grundlegenden Prinzipien liegen kryptografischen Lösungen zugrunde?
- Wie arbeiten symmetrische und asymmetrische Verschlüsselungsalgorithmen?
- Was sind Hybridverfahren und wo werden sie eingesetzt?
- Wie funktionieren und wozu dienen Einweghashverfahren?
- Wie sind aktuelle Verfahren hinsichtlich ihrer heutigen und zukünftigen Sicherheit zu bewerten?



#### VPN-Techniken

- Was zeichnet ein VPN aus?
- Kernelemente eines VPN: Trennung von Verkehrsflüssen, Verschlüsselung und Authentifizierung
- Bandbreite von VPN-Techniken: Frame Relay, ATM, MPLS, IP-Tunnel
- IP-VPN mit IPsec
- Änderungen mit IKEv2 und den aktuellen IETF-Standards
- Funktionsweise von SSL-VPN und von Portal-Lösungen
- Anbindung mobiler Clients durch VPN
- Site-to-Site VPN

#### Remote Access via VPN

- Welche Bausteine werden zum Aufbau eines RAS-VPNs benötigt?
- Wie sind die einzelnen VPN-Komponenten gegenüber Bedrohungen aus dem Internet abzusichern?
- Warum ist insbesondere Authentifizierung

so wichtig und wie kann diese hinreichend sicher erfolgen?

- Was versteht man unter starker Authentifizierung und wie kann diese eingesetzt werden?

#### Planung und Einsatz von VPN-Lösungen

- Welche Aspekte sind beim Einsatz von VPNs zu berücksichtigen?
- Welche VPN-Architekturen sind sinnvoll und welche Vor- und Nachteile weisen sie auf?
- Wie können VPNs hochverfügbar ausgelegt werden?
- Wie und wo kommen Zertifikate und PKI-Strukturen im Zusammenhang mit VPNs zum Einsatz?
- Klärung umfangreicher typischer Fragestellungen beim Aufbau einer VPN-basierten RAS-Lösung anhand eines realen Projekts

#### Praktische Live-Übungen

- Entwurf einer optimierten VPN-Architektur anhand eines realen Fallbeispiels
- Parametrierung und Konfiguration eines Site-to-Site-VPNs in einer Laborumgebung
- Parametrierung und Konfiguration von Client-to-Site-VPNs in einer Laborumgebung

Durch das Seminar führt Sie Herr Dipl.-Inform. Andreas Meder. Er ist im Team der ComConsult Beratung und Planung GmbH als Senior Consultant beschäftigt. Er verfügt aufgrund seiner langjährigen beruflichen Praxis über umfangreiche Kenntnisse und Erfahrungen aus den Bereichen Konzipierung und Betrieb von Netzwerken.

Fax-Antwort an ComConsult 02408/955-399

## Anmeldung Aktuelle VPN-Technik

Ich buche das Seminar  
**Aktuelle VPN-Technik**

14.04. - 16.04.10 in Aachen  
zum Preis von € 1.690,- zzgl. MwSt.

Bitte reservieren Sie mir ein Zimmer

vom \_\_\_\_\_ bis \_\_\_\_\_ 10

 Buchen Sie über unsere Web-Seite  
[www.comconsult-akademie.de](http://www.comconsult-akademie.de)

Vorname \_\_\_\_\_

Nachname \_\_\_\_\_

Firma \_\_\_\_\_

Telefon/Fax \_\_\_\_\_

Straße \_\_\_\_\_

PLZ, Ort \_\_\_\_\_

eMail \_\_\_\_\_

Unterschrift \_\_\_\_\_

## Schwerpunktthema

# Mehr Bandbreite im RZ mit Virtual I/O und optimierten Prozessorarchitekturen

Fortsetzung von Seite 1



Dr. Franz-Joachim Kauffels ist einer der erfahrensten und bekanntesten Referenten der gesamten Netzwerkszene (über 20 Fachbücher und unzählige Artikel) und bekannt für lebendige und mitreißende Seminare.

- I/O und besonders die Kommunikation mit externen Speichersystemen können einen Hypervisor unter ungünstigen Bedingungen in die Knie zwingen
- In dieser Situation fällt das gesamte System ins Koma und tut gar nichts mehr, weil die I/O eine sehr hohe Systempriorität hat
- Eine Verlagerung der diese Situation auslösenden VMs z.B. durch vMotion bringt gar nichts, weil sie im Ziel-Server wieder das Gleiche anstellen
- Die Grenze liegt ohne Hardware-Auslagerung heute bei ca. 3 Gb/s
- Der Hypervisor kann sich (heutiger Stand) nicht selbst wirkungsvoll vor dem Eintritt einer solchen Situation schützen

Im Kern des Problems steht, dass der Hypervisor Software ist, wir aber von ihm mehr und mehr die Leistung eines Hardware-Switches erwarten. Von daher hilft auf Dauer auch die Optimierung der Software nicht weiter. D.h. die Lösung kann nicht alleine aus der Virtualisierungstechnik kommen.

Es gibt ja generell den Trend, Funktionen vom Prozessor zu nehmen und sie in einer externen Hilfs-Hardware zu erledigen, am bekanntesten ist hier sicher die Hardware-Beschleunigung bei iSCSI. So etwas kann man natürlich auch im Umfeld der virtualisierten Rechner machen, und es hilft auch sicher, aber die Frage ist, ob es nicht noch systematischere Ansätze gibt, die tiefer in die Architektur eingreifen und daher mehr bewegen oder die einfach durch eine Abkehr von bisherigen Konstruktionsprinzipien einen systematischen Durchbruch erzielen. Letztlich geht es auch darum, den Hypervisor von an und für sich unnützen Aufgaben zu entlasten.

## 1.1 Die Virtualisierungswelle

Für 2009/2010 sind folgende Trends zu erwarten: der Grad an Virtualisierung wird deutlich zunehmen und sich auf die meisten missionskritischen und leistungssensitiven Anwendungen ausdehnen. Die Virtualisierung dieser Anwendungen setzt virtualisierungs-optimierte Hardware zur Reduktion des Hypervisor-Overheads voraus und adressiert hierbei besonders die Bereiche I/O-Latenz und Durchsatz. Außerdem werden die Anzahl der Cores in einer CPU sowie die Speichergrößen ansteigen. Dadurch wird die Dichte von VMs in einem Server zunehmen. Neben der eigentlichen Konsolidierung werden Unternehmen vermehrt dazu tendieren, die Virtualisierungstechnologie für neue Aufgabenbereiche wie Hochverfügbarkeit, Disaster Recovery und Ressourcen-Optimierung einzusetzen. So schön das auch alles ist, eines ist sicher: die Anforderungen an die I/O steigen dramatisch.

Eine IDC-Studie zur Virtualisierung sagt aus, dass die Unternehmen zu Beginn von 2009 nur etwa 20% ihrer Server virtualisiert haben. Es bestehen aber Pläne, das in 2010 auf 50% der Server zu erweitern. Der Knackpunkt dafür ist aber eine Verbesserung der I/O in einer virtualisierten Umgebung, sonst macht es in vielen Fällen nämlich einfach keinen Sinn. Wenn viele VMs um die Bandbreite wetteifern, reicht es nicht nur, die aggregate Bandbreite zu erhöhen, sondern auch den Mechanismus für den Zugriff einer individuellen VM auf die I/O-Ressourcen zu verbessern.

## 1.2 Das Versprechen von „Virtual I/O“

Bei dem Ansatz der „Virtual I/O“ geht es darum, die Netzwerkadapter auf virtuelle I/O-Ressourcen zu unterteilen und diese im Rahmen einer optimierten Prozessorarchitektur ganz anders als bisher mit den VMs zu verbinden. Ziel ist es, jeder virtuellen Maschine einen exklusiven, wenn auch

virtuellen, Netzwerk-Adapter zuweisen zu können. Dazu müssen mehrere, neuartige Komponenten auf verschiedenen Ebenen zusammenwirken.

Durch die Konsolidierung der Konnektivität wird die Infrastruktur dramatisch vereinfacht: hunderte Kabel können durch ein paar Dutzend ersetzt werden, die meisten I/O-Adapterkarten (HBAs) fallen ganz weg und die Kosten fallen entsprechend, sowohl bei den Komponenten, als auch, primär, beim Betrieb.

Weitere Wohltaten sind:

- Wegfall des Virtuellen Switches im Hypervisor
- Entlastung des Hypervisors von Kommunikationsaufgaben
- Unterstützung sehr hoher I/O-Leistungen

Virtual I/O ist ein Gesamtbild, welches sich nur dann vollständig erschließt, wenn man die Komponenten auf den unterschiedlichen Ebenen (Prozessoren, physikalische Adapter, logische Adapter, Interrupts, Warteschlangensteuerungen, virtualisierungsbewusste I/O-Steuerungen und Hypervisoren IM Server, Netzwerkfunktionalitäten im Rack-Bereich sowie Netzwerkfunktionalitäten außerhalb des Rack-Bereichs) einzeln und im Zusammenwirken betrachtet.

## 1.3 Probleme mit Virtualisierung und heutiger I/O

Server I/O ist ein absolut essentieller Kernbereich der Virtualisierung. Virtualisierte Server benötigen mehr Bandbreite und Verbindungen zu mehr Netzen und Speichern als nichtvirtualisierte Systeme. Herstellerempfehlungen wie die „Best Practices“ von VMware empfehlen dedizierte Konnektivität für kritische Virtuelle Maschinen. Nach einer neueren Umfrage unter Benutzern von Virtualisierungssoft-

Mehr Bandbreite im RZ mit Virtual I/O und optimierten Prozessorarchitekturen

ware hat ein typischer virtualisierter Server 7 oder mehr I/O-Verbindungen, mit einer starken Tendenz zu 16. Außerdem muss er viel häufiger neu konfiguriert werden, wenn sich die Anforderungen durch die VMs ändern. Das steht natürlich in krasssem Gegensatz zu den Erwartungen, die man an Vereinfachungen durch die Beweglichkeit Virtueller Maschinen von der einfachen Lastverteilung über den unterbrechungsfreien Betrieb bis hin zur Disaster Recovery mit wandernden Virtuellen Maschinen eigentlich hat.

Natürlich hat der aufmerksame Leser sofort eine Frage: wenn alle I/O-Ressourcen durch eine Virtualisierung gemeinsam genutzt werden, wie kann man dann Leistung und Sicherheit für eine spezifische Anwendung sicher stellen? Keine Angst, darauf kommen wir noch.

Traditionelle Server haben nicht notwendigerweise die gleichen Anforderungen wie Virtualisierte Server. Sie sind oft nach den Maßgaben des bekannten dreilagigen RZ-Modells angeordnet, nach dem Server hinsichtlich ihrer I/O exakt so konfiguriert werden, wie es die Anwendungen auf ihnen erfordern.

Server-Virtualisierung ändert dieses Modell dramatisch. Das Ziel ist es ja, die Ausnutzung von Servern dadurch zu verbessern, dass man einen dynamischen Pool von Computing Ressourcen schafft, die so benutzt werden können, wie man es braucht. Um dieses Ziel erreichen zu können, müssen verschiedene Anforderungen erfüllt werden:

- Flexible Verteilung von Anwendungen: die meisten Anwendungen sollten auf einem beliebigen Rechner des Pools laufen können
- Multiple Anwendungen pro Server: ist ein Server nicht richtig ausgelastet, soll man weitere Anwendungen dazu packen können, um ihn besser auszunutzen
- Mobilität von Anwendungen: Anwendungen sollten über möglichst alle Server portierbar sein, um Hochverfügbarkeit oder Load Balancing zu erreichen

Diese Anforderungen haben erhebliche Implikationen auf die Server I/O:

- Erhöhtes Verlangen nach Konnektivität. Um sich flexibel entfalten zu können,

benötigen Server Konnektivität zu allen Netzen. Um nach wie vor eine Isolation zu erreichen, verlangen viele Nutzer separate physikalische Verbindungen zu diesen getrennten Netzen, was zu zahlreichen Verbindungselementen in einem Server führt, besonders dann, wenn man aus Sicherheitsgründen Redundanz verlangt

- Management Networks. Die Verwaltung der virtualisierten Umgebung führt zu zusätzlichen Anforderungen an die Konnektivität. So empfiehlt VMware z.B. dedizierte Konnektivität für das VMotion-Netzwerk
- Bandbreite. Konsequenz zu Ende gedacht, erhöht Virtualisierung den Bandbreitebedarf für Server I/O. Normale Server arbeiten oft nur mit 10% Auslastung, virtualisierte Server kommen leicht auf 50% oder mehr. Bei der I/O-Auslastung haben wir ein ähnliches Wachstum. Dies kann zu Engpässen auf dem I/O-Pfad führen (siehe Abbildung 1)

Die traditionelle I/O wurde für Umgebungen entworfen, bei denen auf einem Server im Wesentlichen nur eine Anwendung läuft. Sie kann zwar für virtualisierte Ser-

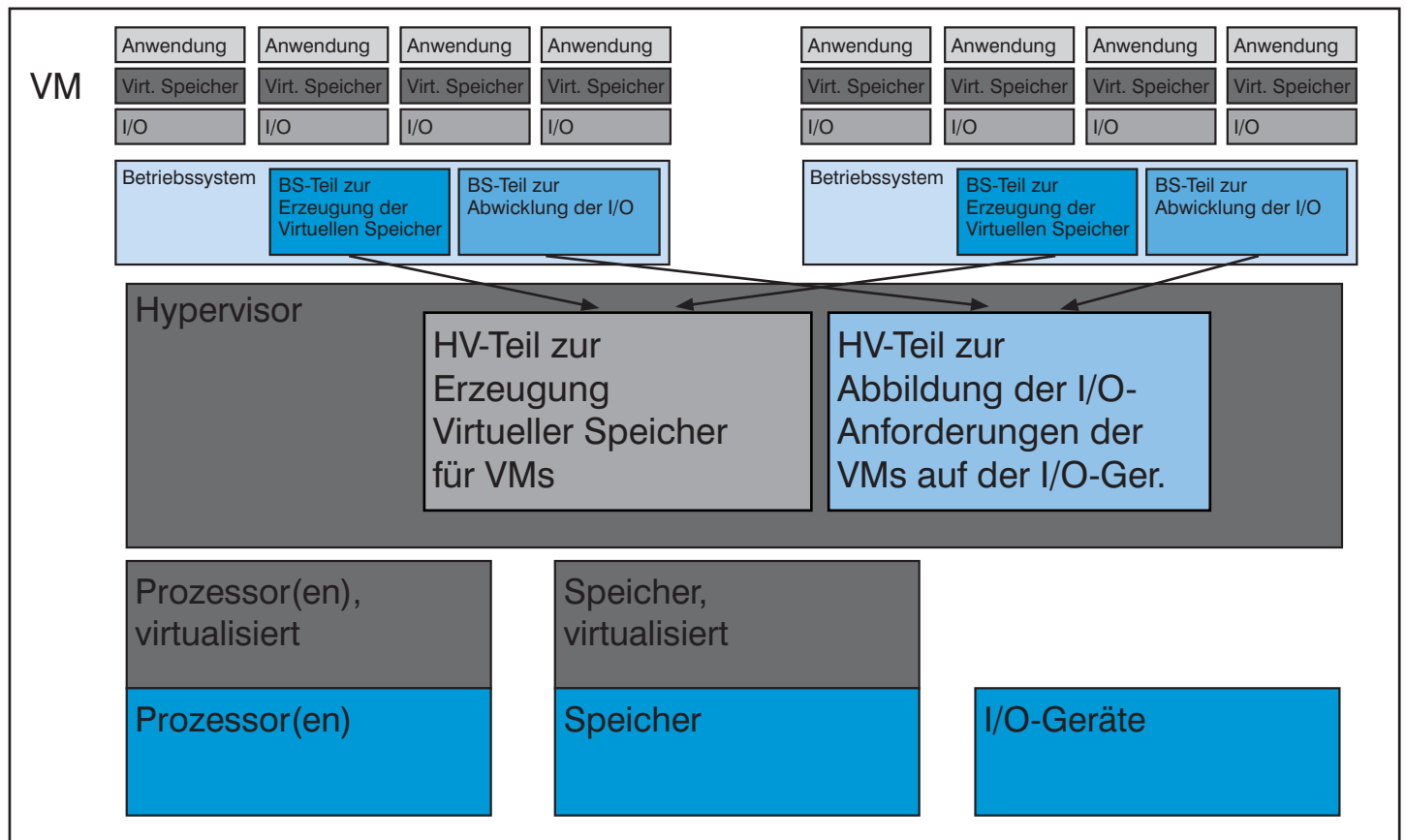


Abbildung 1: Virtuelle Maschinen und traditionelle I/O

Mehr Bandbreite im RZ mit Virtual I/O und optimierten Prozessorarchitekturen

ver wiederverwendet werden, es gibt aber deutliche Grenzen. Eine nahe liegende Option ist es, die bestehende I/O um ein paar Karten (NICs, HBAs) aufzurüsten und diese unter den VMs zu sharen. Das funktioniert nicht wirklich gut, denn bei Lastspitzen, wie sie z.B. bei VM Backups auftreten, können die Anwendungen Überlastungen erzeugen und sich gegenseitig behindern. Treten in einem solchen Zusammenhang Leistungsprobleme auf, so sind sie schwierig zu finden. Selbst wenn ein Administrator den Grund für einen Engpass findet, wird ihm oft nichts anderes übrig bleiben, als eine neue Adapterkarte zu kaufen, oder die Anwendungs-Workloads auf den VMs anders zu verteilen. Ein anderes Problem der konventionellen I/O ist die schiefe Masse der Verbindungen, die benötigt werden. Neben den Verbindungen zu den verschiedenen Datennetzen werden auch Verbindungen für das VM-Management und die Migration Virtueller Maschinen benötigt. Gibt es im RZ auch ein SAN, muss jeder Server auch noch mit FC-HBAs ausgestattet werden. (siehe Abbildung 2)

Alle diese Probleme sind bekannt und haben ja grade zu Entwicklungen wie FCoE geführt. Das Aufrüsten der konventionellen I/O ist zwar möglich, führt aber am Ende zu einer erheblichen Erhöhung der Komponentenmenge, einschließlich Unmengen zusätzlich notwendiger Kabel. In der Abbildung 3 sind nur 6 der mindestens 36 Leitungen eingezeichnet, sonst sieht man nichts mehr.

Was ist mit Blade Systemen? Server-Blades reduzieren das Kabel-Problem durch einen internen Backplane. Hier gibt es aber deutliche Beschränkungen für die Anzahl möglicher Verbindungen, was für die Virtualisierung wieder problematisch sein kann. Eine Aufhebung oder Milderung der Beschränkungen ist entweder teuer (manchmal benötigt man ein Expansions-Blade, welches wieder Geld kostet und einen extra Slot belegt) oder gar nicht möglich.

**1.4 Das Intra-Server Problem auf den Punkt gebracht**

Eine VM benutzt Virtuelle NICs oder Virtuelle HBAs. Diese werden im Rahmen der Erzeugung der VM (was ja nichts weiter als eine Laufzeitumgebung ist) vom Hypervisor erzeugt. Diese virtuellen Einheiten müssen auf reale physikalische NICs oder HBAs abgebildet werden. Diese Abbildung macht der Hypervisor durch Software, was den Hypervisor erheblich belastet. Ein vergleichbares Problem entsteht bei der Abbildung der Virtuellen Speicher der VMs auf den Virtuellen Speicher des Basis-Betriebssystems. Das Problem wird

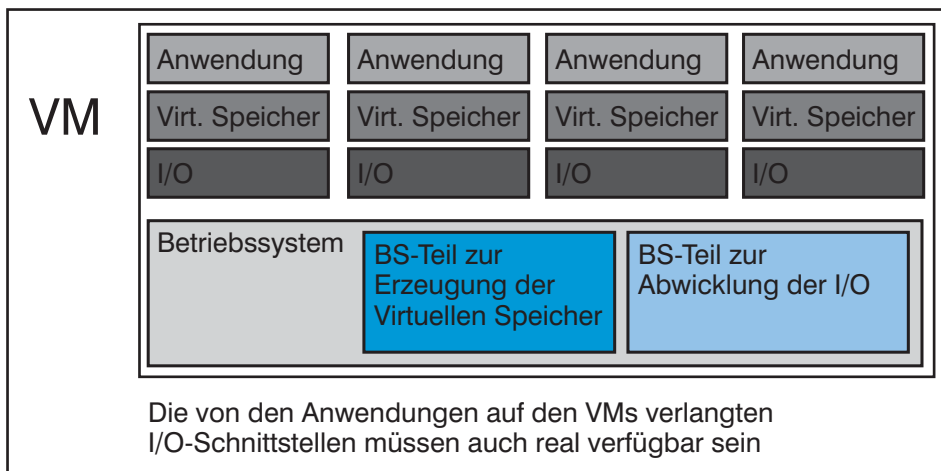


Abbildung 2: Problembereich: anspruchsvolle VMs

jetzt dadurch verschärft, dass die Anzahl der VMs auf einem Server stark ansteigt. In 2008/2009 hat IDC durchschnittlich 6 VMs auf einem Server gezählt. Mit der Einführung neuer HW-Plattformen (8,16 oder mehr Cores) steigt das aber auf 20 – 30 VMs pro Server. Heutige Server haben typischerweise oft 6 1 GbE-NICs, je zwei für Live Migration, für die Service Console und für die tatsächlichen VMs. Dazu gegebenenfalls noch zwei für FC-SAN. Die I/O-Konsolidierung auf Basis von 10 GbE und standardisierten Verfahren wie DCE oder proprietären wie Flex-10 sowie die Einführung von 8/16 GFC wird zu „dicken Pipes“ führen, deren Leistung besser als bisher auf die VMs verteilt werden kann und muss. Server-Virtualisierung benötigt eine höhere und engere Integration mit Netz,

I/O und Speicher. Kurzum: der „Soft-switch“ im Hypervisor muss dringend ersetzt werden. (siehe Abbildung 4)

**1.5 Taxonomie und Begriffsbildung**

Hersteller, Gremien und Dritte sprechen zuweilen eine unterschiedliche Sprache, wenn es um I/O-Virtualisierung geht. IDC hat eine sehr deutliche Taxonomie entwickelt, an der wir uns auch hier orientieren wollen:

**Software IOV** ist die default Konfiguration für die aktuelle Virtualisierungsgeneration. Hypervisoren virtualisieren einen Server einschließlich I/O komplett durch Software. Das erzeugt generell signifikanten Overhead

**Kongress**



**Netzwerk-Redesign Forum 2010  
26. - 29.04.10 in Königswinter**

Netzwerke sind der Lebensnerv unserer Unternehmen. Sie unterliegen einer permanenten Weiterentwicklung und Veränderung. Aus einem Mix aus Bedarf und technischen Möglichkeiten muss das individuelle Optimum für ein Unternehmen gefunden werden. Dieses Optimum muss zugleich an der Zukunft orientiert sein, da Netzwerk-Komponenten über einen langen Zeitraum stabil und ohne permanente Änderungen betrieben werden müssen. Hier setzt das ComConsult Netzwerk-Redesign Forum 2010 an. Es analysiert die wichtigsten Bedarfsentwicklungen, stellt diesen die neuesten Netzwerk-Technologien gegenüber und erarbeitet Empfehlungen für ein erfolgreiches Netzwerk-Design, eine zukunftsorientierte Auslegung und einen stabilen und zuverlässigen Betrieb.

Moderation: Dr. Franz-Joachim Kauffels, Dr. Jürgen Suppan  
Preis: € 2.290,- zzgl. MwSt.



Buchen Sie über unsere Web-Seite [www.comconsult-akademie.de](http://www.comconsult-akademie.de)

Mehr Bandbreite im RZ mit Virtual I/O und optimierten Prozessorarchitekturen

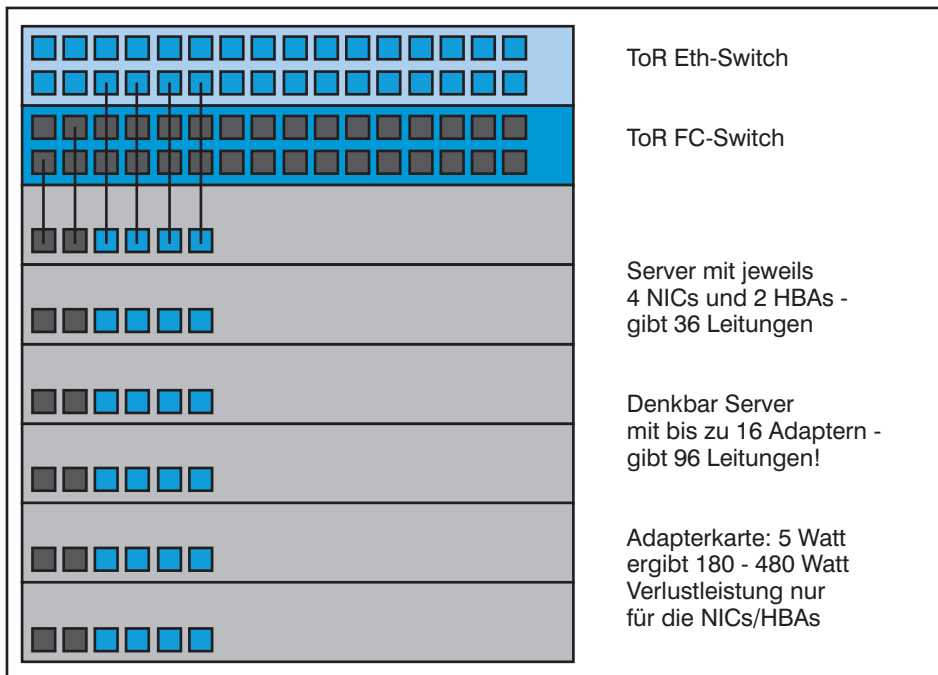


Abbildung 3: Folgen für das Server-Rack

**Intraserver IOV** bezeichnet einen Bereich Hardware-basierter Technologien für die Virtualisierung der I/O von VMs, die auf einem Server gehostet werden. Die meisten Lösungen sind rund um den Standard PCI-SIG SR-IOV gebaut. Komponenten sind:

- Plattform-Technologie (z.B. Intel® VT-d oder ATS-Fähigkeit)
- I/O-Adapter-Technologie (Multiqueue, SR-IOV Virtuelle Funktionen)
- Passendes BIOS und Treiber

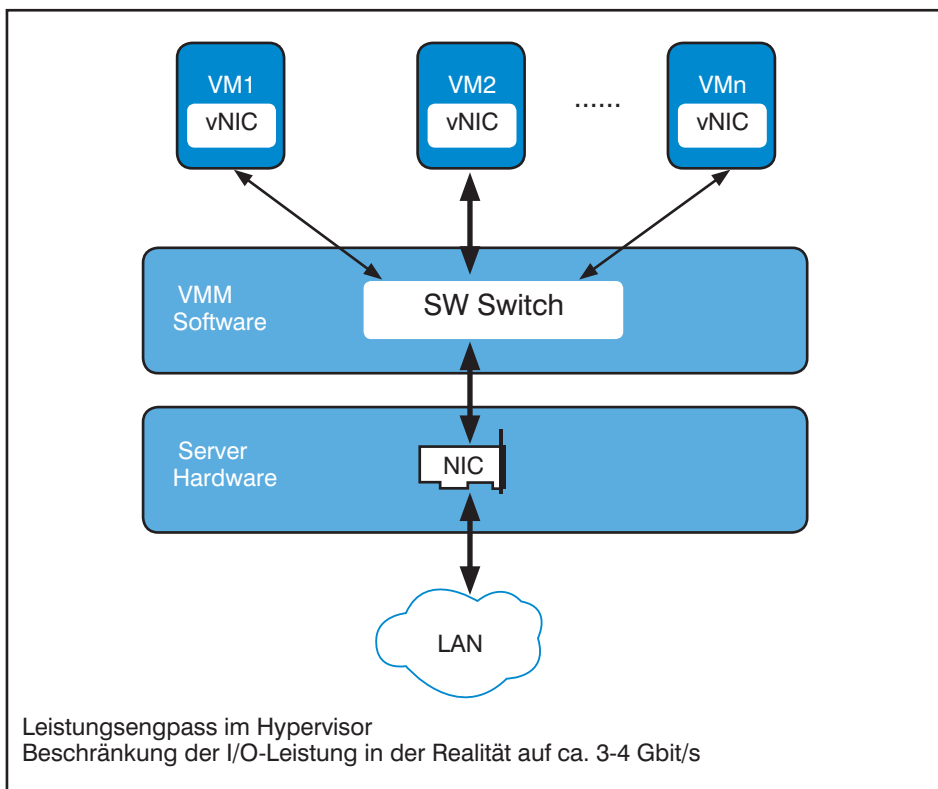


Abbildung 4: Die heutige Situation: Software-IOV

Grafik: Intel

**IOV-Switches** virtualisieren und konsolidieren die I/O über multiple Server in einem Rack oder einem Blade Chassis hinweg. Es entsteht Bandbreiten-Sharing, flexibles Provisioning und eine vereinfachte Verkabelung. Der Xsigo Director fällt z.B. in diese Klasse

**Konvergierte Fabrics.** Diese Technologien können verschiedene, bisher getrennte I/O-Protokolle über eine einheitliche Hardware-Verbindung (Fabric) abwickeln. FCoE Fabrics wären ein Beispiel dafür

Diese Taxonomie schafft endlich auch eine gewisse Abgrenzung von Systemen untereinander, die in der hitzigen Diskussion oft verloren geht:

- Intraserver I/O gehört IN einen Server (egal ob Rack- oder Blade-Server)
- IOV-Switches gehören im Wesentlichen Top of Rack
- Konvergierte Fabrics bilden im Wesentlichen das eigentliche Infrastruktur-Netz

Nur durch eine geeignete Eingrenzung können wir sinnvoll darüber diskutieren, welche Funktionen wo und in welchem Umfang sinnvoll sind. Das heutige Durcheinander kommt von den Herstellern. So platziert z.B. HP mit Flex-10 die Funktion eines proprietären IOV-Switches mitten in den Blade-Server. Das funktioniert zweifelsohne, hat aber z.B. den Nebeneffekt, dass die Diskussion über FCoE und vergleichbare Verfahren verharmlost wird, weil das ja nur auf einem sehr kurzen Stück zwischen Blade System und ToR-Switch stattfindet. Xsigo kann mit seinen Directors ein komplettes Netz zur I/O-Versorgung aufbauen, was aber dann technisch auf IB basiert. Die Frage ist doch immer, was passiert, wenn man solche Konfigurationen in größerem Maßstab ändern oder erneut konsolidieren möchte. Andererseits wird auch die Tragweite der Diskussion um FCoE klar: es ist nicht für Einzelverbindungen, sondern es wird ggf. das Infrastruktur-Netz bilden.

**2. Intraserver IOV**

Die besten Konzepte für Netzwerke im Rack und darüber hinaus nützen gar nichts, wenn das Problem der Hypervisor-Überlastung nicht systematisch gelöst wird. Dazu gibt es zum einen sehr interessanten Standard von PCI-SIG, den so genannten SR-IOV (Single Root – I/O Virtualization), der vor allem deshalb so eine hohe Bedeutung hat, weil er letztlich eine Erweiterung von PCIe, dem aktuell wichtigsten und erfolgreichsten aller internen Bus-Systeme, ist. Hardware-Hersteller orientieren sich an diesem Standard. Also reicht es aus, sich exemplarisch anzuse-

## Mehr Bandbreite im RZ mit Virtual I/O und optimierten Prozessorarchitekturen

hen, was der Prozessorgigant Intel® genau aus diesen Vorgaben macht, welche Anreicherungen es noch zusätzlich gibt und wie sich das Ganze sowohl in der Prozessorarchitektur als auch in erhältlichen Produkten niederschlägt. Dadurch wird auch klar, was ein Hersteller von Virtualisierungssoftware zu tun hat.

### 2.1 SR-IOV als mögliche Lösung für Virtual I/O

I/OV ist einfach die Abstraktion der logischen Details der I/O von den physikalischen Details. Das ist wichtig, um die höheren Protokolle von den physikalischen Verbindungs- oder Transportdetails zu befreien. Es gibt hier eine Reihe von Ansätzen, wir beschränken uns aber hier auf die, die mit Server-Virtualisierung zu tun haben, also besonders auf den SR-IOV-Standard. Neben dem bereits diskutierten Ansatz, die I/O durch die Emulation von I/O-Geräten wie NICs durch die Hypervisor-Software zu virtualisieren, gibt es ja auch durchaus die Möglichkeit der direkten Zuweisung von I/O-Geräten zu VMs. Das ist natürlich viel schneller, entlastet den Hypervisor maximal, hat aber den gravierenden Nachteil, dass man für jede VM auf einem Server einen individuellen Adapter-Port benötigt, was zu einem Skalierungsproblem führt. Hinzu kommt, dass diese Vorgehensweise auf 1 Gigabit-Technologie basiert und auf 10 Gigabit nicht übertragbar ist.

SR-IOV ist ein PCI-SIG-Standard, der das effiziente Sharing von PCI-Geräten unter VMs ermöglicht und in Hardware implementiert wurde, um in der Leistung möglichst nahe an nativer I/O-Leistung zu liegen. SR-IOV erzeugt eine Menge von Virtuellen Funktionsschnittstellen in der Hardware eines physischen PCI-Geräts. Die Virtuellen Funktionsschnittstellen sind im Wesentlichen Virtuelle Instanzen des physischen Geräts. Sie können den VMs unmittelbar zugeordnet werden und erlauben es, dass das physikalische Gerät von den VMs gemeinsam benutzt wird, z.B. zur I/O, OHNE dass ein Hypervisor dabei eingreifen müsste.

Damit SR-IOV funktioniert, müssen eine Reihe von Komponenten auf einem Server zusammenspielen:

- Ein System-Chipsatz, der I/O-Isolation und direkte Zuordnung unterstützt, wie z.B. Intel® Virtualization Technology for Directed I/O (Intel® VT-d)
- Eine SR-IOV-fähige NIC (oder ein anderes I/O-Gerät) mit eingebauten (Hardware) Funktionen für die Virtualisierung

- Ein BIOS, welches den Chipsatz und die SR-IOV-Adapter erkennt
- Ein Hypervisor, der dahingehend modifiziert sein muss, dass er die Möglichkeiten von SR-IOV nutzen kann und für den Nutzer einen Treiber installieren müssen, damit er SR-IOV-Geräte erkennt
- Ein Treiber für das Basis-Betriebssystem, der es ermöglicht, I/O direkt mit dem SR-IOV-Gerät auszuführen

Rein theoretisch kann man ein bestehendes System komponentenweise mit diesen Komponenten aufrüsten. Das ist aber mit Aufwand verbunden. Mit der Zeit wird SR-IOV in die Mehrheit der Server und Hypervisoren eingebaut sein. Normalerweise werden Nutzer den Weg gehen, ein System von ihrem Server-Anbieter zu kaufen, welches die Komponenten bereits besitzt oder dafür vorbereitet ist. Hier vielleicht der wichtige Hinweis, dass es durchaus sinnvoll sein kann, einen Server mit der passenden Ausstattung zu kaufen, auch wenn man das aktuell noch nicht nutzen möchte.

Wichtig ist, dass SR-IOV so konstruiert wurde, dass es kompatibel zu existierender PCIe-Technologie ist und somit nicht zu erwarten ist, dass es eine bestehende Infrastruktur stört.

SR-IOV bietet eine Menge von Vorzügen auf den Bereichen Leistung, I/O-Konsolidierung, Skalierbarkeit und Datenschutz:

- Durch die unmittelbare Zuordnung virtueller Funktionen eines I/O-Gerätes wird nahezu dessen native Leistung erreicht. Der Gesamt I/O-Durchsatz steigt enorm und die Latenz sinkt durch die Beseitigung des Software-Overheads
- Durch die Entlastung des Hypervisors wird auch die System-CPU entlastet
- Es wird ein effizientes, Hardware-unterstütztes Sharing von I/O-Ressourcen ermöglicht
- Die I/O-Konsolidierung erlaubt den System-Verwaltern die Benutzung virtueller Funktionen anstelle von multiplen physischen Geräten für die Separierung von I/O-Funktionen. Das umfasst nicht nur Netzwerk-Komponenten, sondern auch Speicher
- Man spart HW-Kosten, vereinfacht die Verkabelung, reduziert die Anzahl von benötigten Switch Ports und senkt somit den Verwaltungsaufwand

- Durch die systematische Benutzung EINER leistungsfähigen Schnittstelle statt vieler kleinerer steigt die Skalierbarkeit des gesamten Systems

Dadurch entstehen auch handfeste wirtschaftliche Vorteile:

- Höherer Konsolidierungsgrad mit gesteigerter Ersparnis bei Server-HW
- Ausdehnung der Spareffekte durch Virtualisierung auf Anwendungen, die bisher nicht virtualisiert werden konnten
- Ausdehnung der verbesserten Effizienz bei der Verwaltung von Systemen auch auf diese neue Klasse von Anwendungen
- Verbesserte Antwortzeiten und QoS für Anwendungen
- Kostenersparnis durch Reduktion von Adaptern, Kabeln, Switch Ports und Stromverbrauch sowie Management-Punkten

### 2.2 Weiterentwicklungen der Prozessorarchitekturen am Beispiel des Intel® Nehalem

Die Nehalem-Architektur hat eine Reihe von wesentlichen Fortschritten hinsichtlich Leistungsfähigkeit, Skalierbarkeit und Wirtschaftlichkeit moderner Prozessorarchitekturen mit sich gebracht. Aktuelle Prozessoren auf Basis dieser Architektur sind die Intel® Xeon® Prozessoren der Reihen 3500 und 5500. Sie werden von den bekannten Herstellern z.Zt. aktuell in Rack- und Blade-Servern sowie in Hochleistungs-Workstations verbaut. Wesentliche Innovationen sind:

- **Intel® Turbo Boost Technologie.** In Verbindung mit der Intelligent Power Technologie können Prozessoren zeitweise oberhalb der Standard-Taktrate laufen, um bestimmte Aufgaben schneller zu erledigen. Danach fallen sie wieder auf die Basis-Taktrate zurück und sparen Strom.
- **Intel® Hyper Threading Technologie.** Diese bekannte Innovation liefert mehr Leistung für Anwendungen, die für eine parallele Ausführung mit vielen Threads geschrieben wurden. Sie profitieren von größeren Caches im Rahmen der Mikroarchitektur und einer massiven Bandbreite für den Zugriff auf Speicher.
- **Intel® Quick Path Technologie.** Diese skalierbare Architektur für gemeinsam benutzten Speicher integriert einen Memory Controller in jeden Mikroprozessor

## Mehr Bandbreite im RZ mit Virtual I/O und optimierten Prozessorarchitekturen

und verbindet Prozessoren und andere Komponenten mit einer neuen Hochgeschwindigkeits-Verbindungstechnik.

- **Intel® Intelligent Power Technologie** erlaubt eine regelbasierte Kontrolle, die dazu dient, dass die Prozessoren in einem Optimum zwischen Geschwindigkeit und Stromverbrauch laufen können. Diese Kontrolle kann von Betriebssystemen oder Administratoren ausgeübt werden.
- **Intel® Virtualization Technologie.** Die neueste Version steigert die Leistung einer virtualisierten Umgebung durch den Einsatz von neuen Hardware-unterstützten Möglichkeiten nach Angaben des Herstellers mindestens um das Doppelte.

Blickt man auf die Quick Path Technologie, sieht man, welche Kommunikationsraten innerhalb eines Rechners auftreten können. Quick Path benutzt Links mit einer Leistung von bis zu 6,4 Gigatransfers/sec, umgerechnet ca. 25,6 GBytes/sec. oder ca. 200 Gbit/s. Unter Mitwirkung der Nehalem L3 Cache Technologie ist das die maximale Geschwindigkeit unter Prozessoren und zwischen Prozessoren und Speichern. Dabei macht das System noch CRC-Checks. Mit der Virtualisierung wird oft die Vision entworfen, dass das Netz zum Systembus der virtualisierten Systeme wird. Selbst wenn man ein 40 GbE einsetzen würde, gibt es immer noch erhebliche Unterschiede zwischen der Übertragungsgeschwindigkeit innerhalb und außerhalb eines Prozessors. Das ist auch nicht weiter schlimm, weil es eigentlich seit über 40 Jahren immer so war. Dennoch sollte man einerseits allzu großen Optimismus hinsichtlich der möglichen Verlagerungen dämpfen und sich andererseits im Klaren darüber sein, dass solche Systeme schlicht verhungern, wenn man sie mit nur 1 GbE irgendwo anschließen möchte. Welches Verhältnis zwischen interner und externer Kommunikationsleistung letztlich benötigt wird, hängt von vielen Installations- und Applikations-spezifischen Einflüssen ab, das können wir hier nicht weiter diskutieren.

Die nächste Generation der Intel® Virtualization Technology Intel® VT verbessert die Virtualisierungsleistung bei Workstations und Servern durch neue Hardware-unterstützte Möglichkeiten in Prozessor, Chipssets und Netzwerk Adapters.

Im Prozessor basieren die Verbesserungen von Intel® VT für IA-32, Intel® 64 und Intel® VT-x auf Hardware-unterstütztem Page Table Management, welches dem

Gast-Betriebssystem (der VM) einen direkteren Zugriff zur Hardware erlaubt und somit die rechenintensive Software-Umsetzung durch den Hypervisor reduziert. Das hatte ich ja schon in einem früheren Artikel detailliert dargestellt. Intel VT-x enthält darüber hinaus die Intel® VT FlexMigration und Intel® VT FlexPriority. Das sind Methoden zur Unterstützung der Workload-Migration und Leistungsoptimierung über den gesamten Bereich von 32- und 64-Bit-Umgebungen. Sehen wir uns das einmal näher an:

- **Intel® FlexPriority.** Es gibt ein spezielles Register im Prozessor, das APIC Task Priority Register, kurz TPR, welches die Prioritäten von Tasks beobachtet und dafür Sorge trägt, dass nur Interrupts, die eine höhere Priorität als die aktuell laufende Task haben, berücksichtigt werden. Das ist bei praktisch allen Rechnern und Betriebssystemen so. Natürlich wird dieser Mechanismus für jede virtuelle Maschine benötigt. Intel® FlexPriority erzeugt eine virtuelle Kopie des TPR, die durch die VM gelesen und in manchen Fällen auch verändert werden kann, ohne dass der Hypervisor eingeschaltet werden muss. Das kann z.B. bei 32-Bit Systemen, die die TPR häufig benutzen, zur Leistungsoptimierung eingesetzt werden und bringt nach Angaben des Herstellers bis zu 35% Gewinn.
- **Intel® FlexMigration.** Einer der Hauptvorteile der Virtualisierung ist die Möglichkeit, laufende Anwendungen ohne

Downtime von einem Server zum anderen zu bringen (Wandernde VMs). FlexMigration ist dazu gedacht, eine nahtlose Wanderung von VMs zwischen aktuellen und zukünftigen Servern mit Intel-Prozessoren zu ermöglichen, auch dann, wenn die neueren Prozessoren erweiterte Befehlsätze haben. Damit können Hypervisoren einen über alle physikalischen Server in einem Migrationspool hinweg konsistenten Befehlsatz festlegen. So können derartige Pools auch aus Maschinen unterschiedlicher Generationen gebildet werden.

Im Chipsatz dient die **Intel® Virtualization Technology for Directed I/O (VT-d)** der Beschleunigung des Datenverkehrs. Der Overhead wird dabei vor allem dadurch minimiert, dass die VMs ihre eigenen dedizierten I/O-Geräte bekommen und dadurch der Hypervisor massiv vom Management des I/O-Verkehrs befreit wird. Technisch wird das so realisiert, dass ein Hypervisor den spezifischen Gastbetriebssystemen (VMs) spezifische I/O-Geräte sicher zuordnen kann. Jedes Gerät hat einen dedizierten Bereich im Hauptspeicher, der nur für das Gerät und die assoziierte VM zugänglich ist. Sobald die initialen Zuordnungen gemacht sind, können Daten direkt zwischen einer VM und den ihr zugeordneten I/O-Geräten fließen. Dadurch werden auch Sicherheit und Verfügbarkeit verbessert, da auf Daten, die für eine spezifische VM bestimmt sind, weder von irgendeiner anderen Hardware noch von einer anderen VM zugegriffen werden kann. (siehe Abbildung 5)

## Seminar



### Ethernet Technologien neuester Stand 12.04. - 13.04.10 in Berlin

Dieses Premium-Seminar bieten wir Ihnen mit multimedialem erweitertem Leistungsspektrum an:

- Vorbereitungs-Videos im Vorfeld des Seminars
- Live-Seminar
- Vertiefungs-Videos zur Nachbereitung des Seminars
- Volltext-Dokumentation ca. 500 Seiten in Report-Qualität

Referent: Dr. Franz-Joachim Kauffels  
Preis: € 1.590,- zzgl. MwSt.



Buchen Sie über unsere Web-Seite [www.comconsult-akademie.de](http://www.comconsult-akademie.de)

## Mehr Bandbreite im RZ mit Virtual I/O und optimierten Prozessorarchitekturen

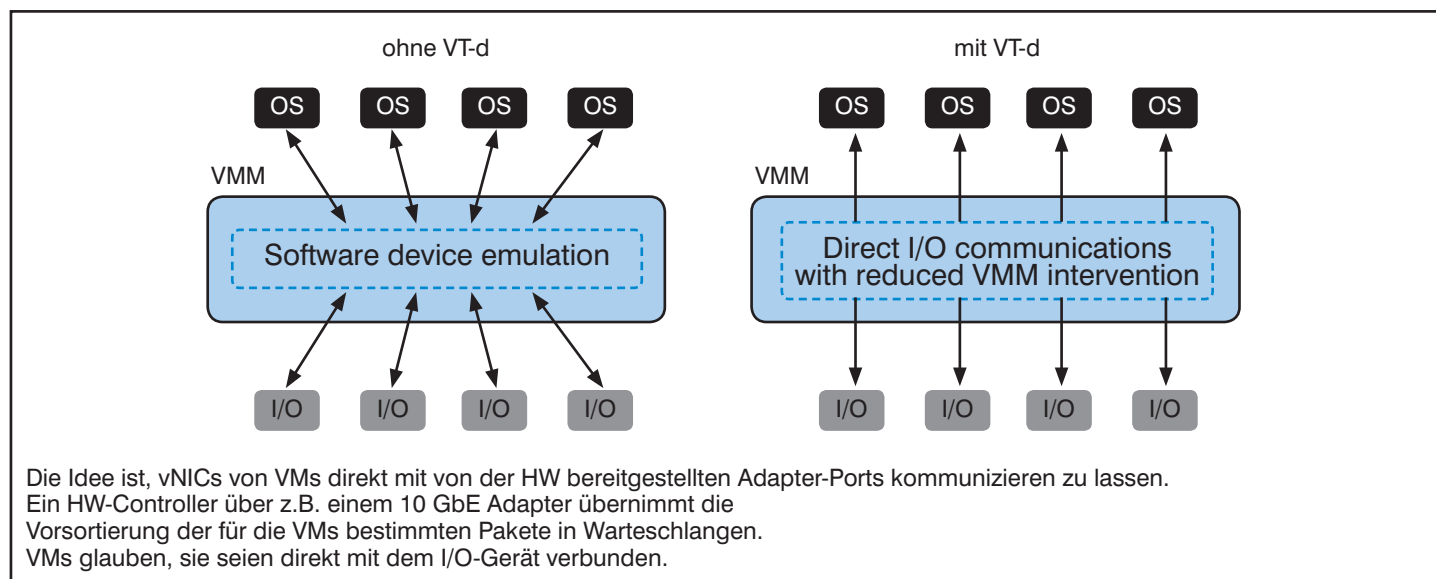


Abbildung 5: Intel Virtualization Tech. for Directed I/O VT-d

Grafik: Intel

Die **Intel® Virtualization Technology for Connectivity (VT-c)** verbessert die I/O-Lösungen für Server durch die Integration weitreichender Hardware-Unterstützung in die I/O-Geräte, die dazu benutzt werden, Server in einem RZ mit der Speicher-Infrastruktur und anderen externen Geräten zu verbinden, noch weiter. Durch die Ausübung von Routing-Funktionen zu und von den VMs in z.B. Netzwerk-Adapter-Chips beschleunigt Intel® VT-c die Auslieferung von Daten und reduziert die Last auf dem Hypervisor und den Server-Prozessoren. Die Leistung kann dabei gegenüber gleichartigen Adaptern ohne diese zusätzliche Funktionalität durchaus verdoppelt werden. Zur Realisierung von VT-c gibt es zwei wichtige technische Elemente, die heute von allen Intel® 10 GbE-Adaptern und ausgewählten 1 GbE-Adaptern unterstützt werden:

- **Virtual Machine Device Queues (VMDq).** In einer traditionellen Virtualisierungsumgebung muss der Hypervisor jedes einzelne Datenpaket sortieren und es dann zu der passenden VM weiterleiten. Das verbraucht viele Prozessorzyklen. Mit VMDq wird diese Sortierfunktion von spezieller Hardware in den Server-Adaptern ausgeführt. Das einzige, was der Hypervisor noch tun muss, ist, die vorsortierten Paketgruppen an die richtige VM weiterzuleiten. Dadurch wird die I/O-Latenz deutlich reduziert und der Prozessor hat mehr Zeit für seine eigentlichen Aufgaben.
- **Virtual Machine Direct Connect (VMDc).** VMDc ermöglicht den VMs den unmittelbaren Zugriff auf die I/O-Hard-

ware im Rahmen der weiter oben besprochenen Funktionen von PCI-SIG SR-IOV. Dadurch entsteht ein direkter Kommunikationsweg zwischen einer VM und einem physikalischen I/O-Port auf einem I/O-Gerät. SR-IOV ermöglicht aber darüber hinaus die Definition mehrerer direkter Kommunikationswege für jeden physikalischen I/O-Port auf dem Gerät. Seien z.B. 10 VMs auf einem Server, der einen 10 GbE Adapter besitzt. Dann kann z.B. jede VM eine isolierte und von den anderen Verbindungen völlig getrennte individuelle 1 GbE-Verbindung bekommen und sich über diesen Single Link mit dem Corporate Network verbinden. Diese Direct Links umgehen den Hypervisor-„Switch“ und führen so zu einer wesentlich gesteigerten I/O-Leistung bei gleichzeitiger Entlastung der Server Prozessoren. (siehe Abbildung 6)

Sehen wir uns jetzt einmal an, was ein Controller im Detail können muss, um die I/O-Virtualisierung im bis jetzt besprochenen Umfang zu unterstützen:

- Multiple Descriptor Queues
- Receive-Side Scaling
- Virtual Machine Device Queues (VMDq)
- Extended Message-Signalled Interrupts (MSI-X)

**Multiple Descriptor Queues.** Multiple Sende- und Empfangsschlangen im Controller ermöglichen es, Netzwerk-Verkehrsströme in Queues aufzugliedern. Diese Queues können dann spezifischen Prozessorkernen zugeordnet werden, was die Verteilung von Workload ermöglicht und dabei hilft, dafür zu sorgen, dass ein ein-

zelner Core nicht vom Datenverkehr überbeschwert wird. Auf die Paket Queues können Treiber-Threads zugreifen, die auf unterschiedlichen Prozessor-Cores laufen, so dass multiple Cores Netzwerk-Pakete parallel bearbeiten können.

**Receive-Side Scaling RSS.** Um zu bestimmen, welche Empfangsschlange für ankommende Pakete benutzt werden soll, können Controller auf Systemen mit Windows Server 2003 oder Vista RSS benutzen. Bei Linux-Systemen ist das als Scalable I/O bekannt. RSS leitet Pakete an unterschiedlichen Schlangen, ohne dass sie vorher sortiert werden müssten. So kann man z.B. dafür sorgen, dass multiple TCP/IP-Paketströme gezielt von verschiedenen Cores behandelt werden, wenn die Controller Multiple Queues unterstützen. Der Intel® 82575 1 GbE und der Intel® 82589 10 GbE Controller unterstützen beide RSS.

**Virtual Machine Device Queues VMDq.** Die Fähigkeit, Streams an verschiedene Cores zu leiten, ist ein wesentliches Element für die Unterstützung der Virtualisierung. Dieses Design ermöglicht, dass sich VMs, die von einem Hypervisor gehostet werden und Netzwerk-Controller emulieren, auf einen dedizierten Netzwerk-Strom verlassen können, der von einem einzigen Core behandelt wird. Sind multiple VMs aktiv, können sie sich die Controller Ports teilen, aber die Vorzüge eines „eigenen privat bearbeiteten Paket-Stroms“ genießen. Diese Lösung steigert die Leistung einer virtualisierten Umgebung erheblich. Die VMDq-Technologie liefert multiple Hardware-Schlangen und Offload-Möglichkeiten, die dazu benutzt wer-

Mehr Bandbreite im RZ mit Virtual I/O und optimierten Prozessorarchitekturen

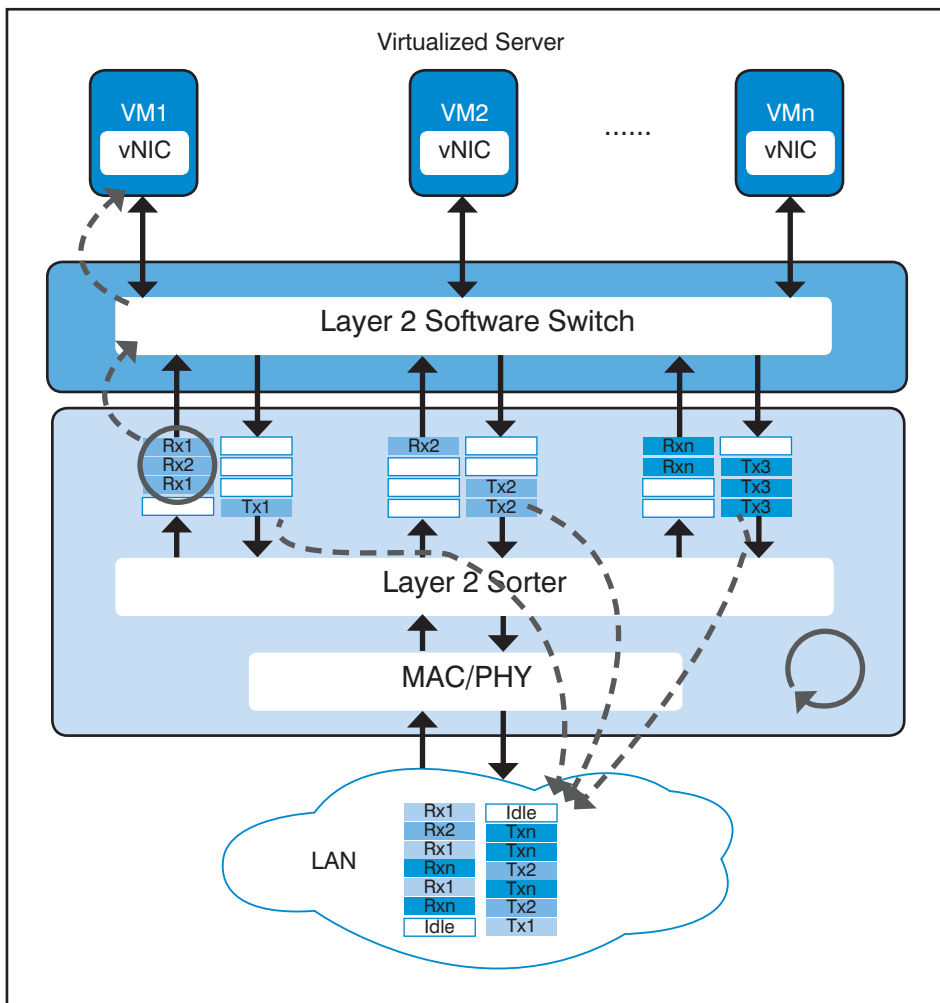


Abbildung 6: Intel Virtualization Tech. for Connectivity VT-c

Grafik: Intel

den können, den Software-Overhead, der durch eine simultane Benutzung eines einzigen physikalischen Netzwerk Controllers durch multiple VMs entsteht, zu reduzieren. Bevor es diese Technologie gab, musste ein Netzwerk-Switch, der in der Hypervisor-Software emuliert wurde, alle Pakete sortieren und sie individuell an die laufenden VMs weitergeben. Mit VMDq werden Zuordnungen zwischen individuellen Hardware-Queues und den emulierten Netzwerkschnittstellen der laufenden VMs hergestellt, d.h. der Controller selbst nimmt das Routing zwischen physikalischem Port und VMs vor, was den Overhead signifikant senkt. Die Funktion kann man auch auf Pakete anwenden, die die VMs nach draußen schicken, um Fairness bei der Sendung zu erzielen und die Blockierung eines Controllers durch eine einzelne VM zu verhindern.

**Extended Message-Signalled Interrupts (MSI-X).** Die Fähigkeit, effektiv zwischen Schlangen und Cores zu kommunizieren, wird durch MSI-X erbracht. MSI-X ist die

nächste Generation von MSI, die Interrupts auf einen spezifischen Core leitet. MSI-X arbeitet mit multiplen Interrupt-Vektoren.

Netzwerk-Controller, die alle die genannten Funktionen unterstützen, haben noch weitere Funktionen, wie die **Intel® I/O Acceleration Technology I/OAT**, die die Bandbreite z.B. dadurch optimiert, dass der Speicherzugriff zu Paketkomponenten verbessert wird und ordentliche Puffer, wie z.B. einen 512 KB Empfangspuffer und einen 320 KB Sendepuffer bei 10 GbE. Darüber hinaus werden Teilaufgaben von TCP/IP, wie Checksum oder Segmentierung, bereits im Controller erledigt.

Intel, DELL und VMware haben in verschiedenen Versuchen die Leistungsfähigkeit der neuen Konzepte belegt. Ich greife hier einmal einen heraus, der mir besonders typisch erscheint und bei dem der Server nicht allzu groß ist. Intel hat mit VMDq eine Technologie entwickelt, die das Sortieren und Weiterleiten der Datenpakete in die Hardware verlegt hat. VMware musste die

Hypervisor Switch Layer ändern, nicht nur um die Daten an die entsprechende Ziel-VM zu bringen, sondern auch, um die Interrupts an die entsprechenden CPU-Kerne und die passende VM zu bringen. Mit dieser kombinierten Implementierung der Queuing-Technologie in der Virtuellen Umgebung kann der Durchsatz mehr als verdoppelt werden. Im speziellen Szenario besteht die Konfiguration aus einem Intel® Xeon®-basierten Server mit Windows Server 2003 mit vier VMs unter VMware ESX 3.5 Update 4 und einem Intel® 82598 10 GbE Controller. Mit der IxChariot Benchmarking Anwendung wurde als receive-only Durchsatz ohne VMDq 4 Gbit/s gemessen. Das entspricht in etwa dem Wert, den ich in meinem früheren Artikel für die herkömmlichen Virtualisierungslösungen evaluiert und erklärt hatte. Mit VMDq konnte der Durchsatz mit 9,2 Gbit/s mehr als verdoppelt werden. Sieht man genau hin, ist das sehr nahe an der Obergrenze davon, was ein 10 GbE-Adapter überhaupt schaffen kann. Die Lesevorgänge wurden mit der Standard-Paketgröße 1500 Byte durchgeführt. Der Einsatz von Jumbo Frames mit einer Länge von 9000 Byte konnte der Durchsatz sogar auf 9,5 Gbit/s gesteigert werden. Beide Werte korrespondieren mit den generell möglichen Grenzwerten von 10 GbE Adaptern!

Das stützt meine Theorie, dass zukünftige Server mit 16, 32 oder 64 Cores in wenigen Jahren durchaus eine 40 GbE, 32 GbFC oder 40 GbIB-Ausstattung benötigen werden.

### 3. IOV-Switching

Nun haben wir das Problem für einen einzelnen Rack-Server oder für ein Blade-System gelöst. Was aber ist nun mit Stapeln solcher Systeme? Dafür gibt es das IOV-Switching, welches sowohl für herkömmlich ausgestattete virtualisierte Server als auch und im Besonderen für solche, die durch die im 2. Kapitel genannten Methoden und Verfahren optimiert wurden, ausgesprochen angemessene Konnektivität bietet.

IOV ist ein neuer, skalierbarer, flexibler und leicht zu verwaltender Ansatz. Er hebt die Beschränkungen traditioneller I/O auf und liefert optimale Konnektivität für multiple VMs auf einem physischen Server. Was erreicht das System?

Bei heutigen Produkten ist der Wirkungsbereich der Virtual I/O auf das Rack oder benachbarte Racks beschränkt. Schon hier werden sehr wirkungsvolle Vorteile erreicht. Das Konzept selbst ist aber allgemein und kann durchaus auf größere Be-

## Mehr Bandbreite im RZ mit Virtual I/O und optimierten Prozessorarchitekturen

reiche ausgedehnt werden.

IOV-Switching konsolidiert alle Speicher- und Netzwerkverbindungen auf ein einzelnes Kabel (ein Kabelpaar für Redundanz) pro Server. Das reduziert nicht nur die Kabel- und Adaptermenge. Virtuelle I/O-Verbindungen können nach Bedarf hinzugefügt werden. Damit das klappen kann, gibt es eine Reihe von Anforderungen an diese einzelne Datenverbindung:

- Fibre Channel ready: Virtual I/O trägt FC-Verkehr für die Verbindung zu Speichersystemen
- Hohe Leistung: die einzelne Verbindung darf niemals zum Engpass werden
- QoS: die einzelne Virtual I/O-Verbindung besitzt QoS-Mechanismen für die dedizierte Zuordnung von Bandbreite

IOV-Switching erscheint den Anwendungen, dem Hypervisor und dem zugrunde liegenden Basis-Betriebssystem wie konventionelle Verbindungs-Ressourcen (NICs und HBAs). Dies wird durch virtuelle NICs (vNICs) und virtuelle HBAs (vHBAs) erreicht. Genau wie virtuelle Maschinen den Anwendungen wie „echte“ Rechner erscheinen, erscheinen vNICs und vHBAs den VMs wie ihre realen Gegenstücke. Von einem Sicherheits-Standpunkt aus gesehen, liefern vNICs und vHBAs einen mit physikalisch getrennten Adapterkarten und Kabeln vergleichbaren Isolationsgrad.

Kommen wir zu den Elementen von IOV-Switching. IOV-Switching erzeugt eine Kommunikationsumgebung, die für die VMs und andere Systemteile konventionell erscheint, aber technisch anders arbeitet. Das versteht man sofort, wenn man sich die Komponenten ansieht.

- Virtual I/O-Director. Das ist die Schaltstelle. Rack-Server werden mit einer einzigen (Redundanz: Doppel-) Hochleistungsverbindung an den Virtual I/O Director angeschlossen. Dieser sitzt Top of Rack. Der Virtual I/O-Director stellt dann die Verbindungen zu konventionellen Ethernet- und FC-Geräten mittels konventioneller Ethernet- und FC-Verbindungen her.
- Hochleistungsverbindung. Jeder Server wird mittels einer Hochleistungsverbindung mit dem Virtual I/O-Director verbunden. Für die Gewährleistung von Redundanz können an jeden Server zwei Virtual I/O Directors mit separaten Hochleistungsverbindungen angeschlossen werden. Die Verbindungen müssen FC- und Ethernet-Datenverkehr tragen.

- Host Channel Adapter (HCA): eine ein-

zelne IB-Karte in jedem Server (oder zwei für Redundanz) für die Konnektivität zum (zu den) Virtual I/O-Director(s).

- Virtual NIC vNIC. Erscheint gegenüber Anwendung, Betriebssystem und Hypervisor genau wie ein physikalischer Netzwerk-Adapter. Möglichkeiten der vNICs umfassen:
  - Verfügbarkeit auf Anforderung. vNICs können on the fly generiert werden, ohne dass ein Re-Boot nötig wäre
  - Skalierbarkeit: auf einem Server können multiple vNICs kreiert werden
  - Mobilität: unter der Kontrolle eines Administrators und/oder einer Management-Anwendung können vNICs über physikalische Server hinweg bewegt werden
  - Dauerhafte Identität: die MAC-Adressen verändern sich auch bei Re-Boot oder Migration nicht
- Virtual HBA vHBA. Erscheint genau wie ein physischer FC Host Bus Adapter mit gleichen Eigenschaften wie eine vNIC und einem dauerhaften WWN.
- QoS: Definition garantierter Leistungsparameter für individuelle vNICs und vHBAs. (siehe Abbildung 7)

Die Abbildung 8 zeigt ohne viele Worte, wie man mit IOV-Switching aufräumen kann. Ein Server benötigt nur noch zwei Leitungen: eine zu „seinem“ I/O-Director und aus Redundanzgründen eine weitere zu einem zweiten I/O-Director.

Damit keine Missverständnisse entstehen: Virtual I/O ist KEIN Hypervisor. Es liefert Netzwerk- und Speicher-Konnektivität für Anwendungen, Virtuelle Maschinen, Hypervisoren und Betriebssysteme.

Wie versprochen stelle ich jetzt ein Gerät vor, welches seit einigen Monaten am Markt ist, sofort eingesetzt werden kann und die Versprechen der I/O-Virtualisierung durchsetzt und einlöst. Der Xsigo I/O Director hat schon verschiedene Auszeichnungen bekommen, darunter „Best of Show“ der VMworld 2009 in San Francisco. Außerdem war er dort die Basis für alle Demonstrationen von VMware. (siehe Abbildung 9)

Das Chassis enthält 24 Infiniband Ports SDR oder DDR (10 oder 20 Gbps), 15 Slots für I/O-Module und vollredundante Stromversorgung und Kühlung. Bis zu 24 Server können direkt an das Gerät angeschlossen werden, mittels Erweiterungs-switches kann das Gerät mit Hunderten

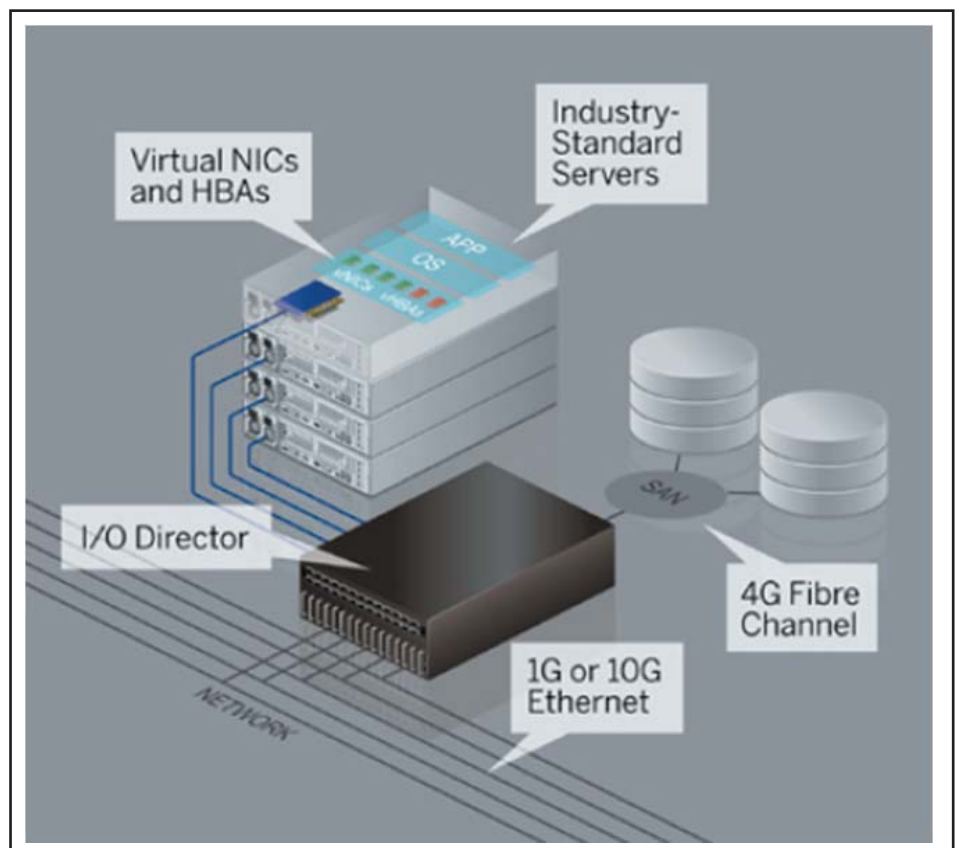


Abbildung 7: Elemente von Virtual I/O

Grafik: Xsigo

Mehr Bandbreite im RZ mit Virtual I/O und optimierten Prozessorarchitekturen

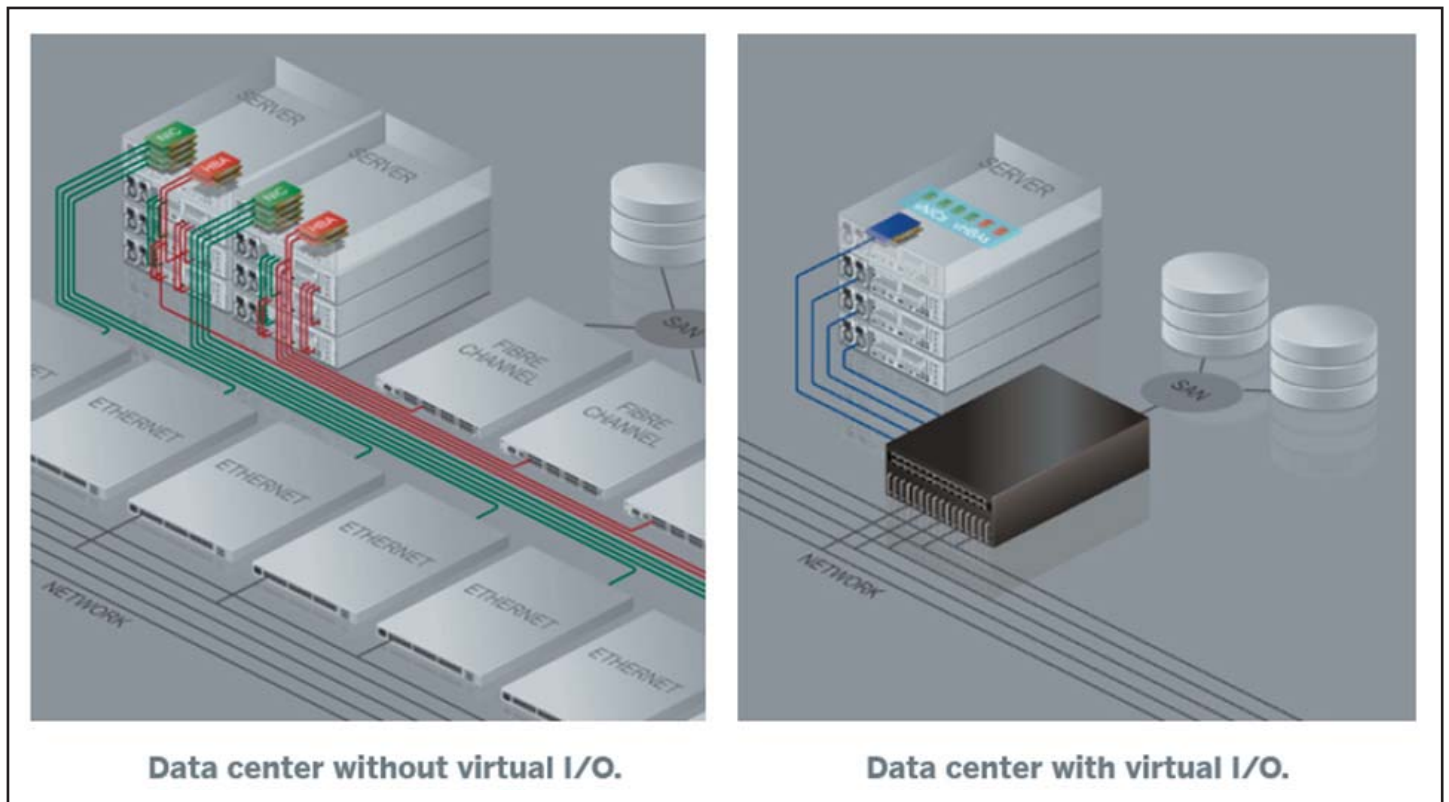


Abbildung 8: Aufräumen mit Virtual I/O

Grafik: Xsigo

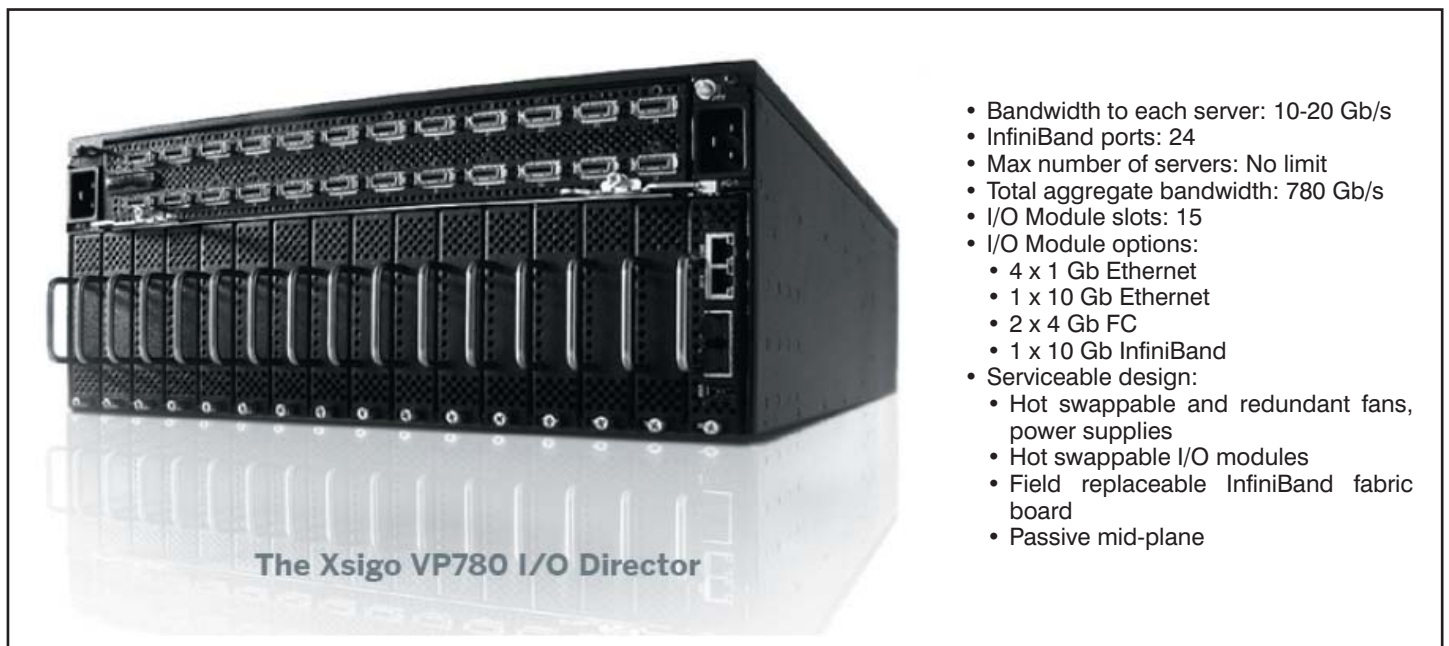
Servern verbunden werden.

Die aggregate Gesamtbandbreite des Geräts beträgt 780 Gb/s. Modul-Optionen umfassen z.Zt. 4X 1 Gb Ethernet, 1 X 10 Gb Ethernet, 2 X 4 GbFC und einmal 10

Gb InfiniBand. Wie schon zu erwarten ist, ist das Herz dieses Gerätes eine InfiniBand Switch Fabric. Die Mid-Plane ist passiv.

Das System-Management XMS erlaubt die Kreation von Server I/O-Profilen, individu-

elle Ressourcen oder Templates. Die Reporting Views von XMS erlauben den Blick auf alle z.Zt. konfigurierten Server, vNICs und vHBAs. Dazu gibt es Traffic Monitoring. Mit diesem können auch QoS CIR und PIR eingestellt und beobachtet wer-



- Bandwidth to each server: 10-20 Gb/s
- InfiniBand ports: 24
- Max number of servers: No limit
- Total aggregate bandwidth: 780 Gb/s
- I/O Module slots: 15
- I/O Module options:
  - 4 x 1 Gb Ethernet
  - 1 x 10 Gb Ethernet
  - 2 x 4 Gb FC
  - 1 x 10 Gb InfiniBand
- Serviceable design:
  - Hot swappable and redundant fans, power supplies
  - Hot swappable I/O modules
  - Field replaceable InfiniBand fabric board
  - Passive mid-plane

Abbildung 9: Xsigo Virtual I/O Director

Grafik: Xsigo

## Mehr Bandbreite im RZ mit Virtual I/O und optimierten Prozessorarchitekturen

den. Das 10 GbE-Modul kann darüber hinaus noch Zugriffskontrollen und Classifier per Flow für jeden Verkehrstyp festlegen. XMS kann als Stand-alone System benutzt werden, es gibt aber auch eine Integration in den VMware Infrastructure Client. Dadurch können VMs und Virtual I/O von einer Stelle aus gemanagt werden. Für das Server Management ändert sich sehr wenig, die vNICs und vHBAs können wie ihre physikalischen Gegenstücke verwaltet werden. Server Load Balancer und andere Network Appliances arbeiten nahtlos mit Virtual I/O zusammen.

Die Server-zu-Server-Kommunikation profitiert von der InfiniBand Fabric mit geringer Latenz und hoher Leistung. Zwischen zwei vNICs ist ein Verkehrsstrom mit einer Nutzdatenrate von ca. 5 Gbps bei einer Latenz von nur 30 msec. unter der Benutzung von Standard TCP/IP möglich. Dabei brauchen Ethernet-basierte Anwendungen und der TCP/IP-Stack nicht modifiziert werden. Richtig fliegt es aber, wenn die Server mit InfiniBand kommunizieren. Die erzielbaren Datenraten sind von der Nachrichtengröße abhängig. Bei 0-Byte Nach-

richten liegt die Latenz bei 3,5 msec, bei 4GB-Nachrichten erzielt das System eine Bandbreite von 846 MBytes pro Sekunde oder ca. 6,8 Gbit/s.

Es gibt verschiedene Konfigurationsmöglichkeiten für die Einbindung der Geräte in VMware HA oder Multipathing-Software wie PowerPath für FC. Das können wir hier nicht alles aufzählen, aber die Redundanz bewegt sich auf einem sehr hohen Niveau.

Das Gerät fügt sich in alle denkbaren Szenarien ein. Die Kompatibilitätsliste ist beeindruckend und umfasst z.Zt. 8 eng beschriebene Seiten. Neben praktisch allen wichtigen marktgängigen Prozessoren/Servern wurde die Funktionalität mit VMware, Citrix und Microsoft als Virtualisierungssoftware, Switches von Cisco, Brocade, Juniper und NetGear sowie Speichersysteme von NetApp, EMC, Hitachi usf. getestet.

Wegen der hohen aggregaten Gesamtleistung der Directors reichen auch für größere Umgebungen wenige von ihnen,

der Rest kann durch die Expansion Switches abgedeckt werden. Das Bild zeigt eine vollredundante Konfiguration mit automatischem Failover für 120 Server mit 2 Directors. Im Bild ist nur die Hälfte der angeschlossenen Server tatsächlich dargestellt. (siehe Abbildung 10)

#### 4. Konsequenzen für die Unternehmensnetze

Das Konzept der I/O-Virtualisierung hat weit reichende Konsequenzen für die Unternehmensnetze und die Gestalt von Virtualisierungs-Lösungen.

I/O-Virtualisierung findet in mehreren Stufen und an mehreren Stellen statt. Die wichtigste Erkenntnis ist sicherlich:

- Durchbruch der 10 GbE-Marke. Systeme, die mit den Hardware-Erweiterungen zur I/O-Virtualisierung ausgestattet sind, entlasten den Hypervisor enorm. Man kann also nicht mehr davon ausgehen, dass diese Systeme nur eine geringe I/O-Leistung haben. In 2010 sehen wir 20 Gb-Systeme, die 10 GbE

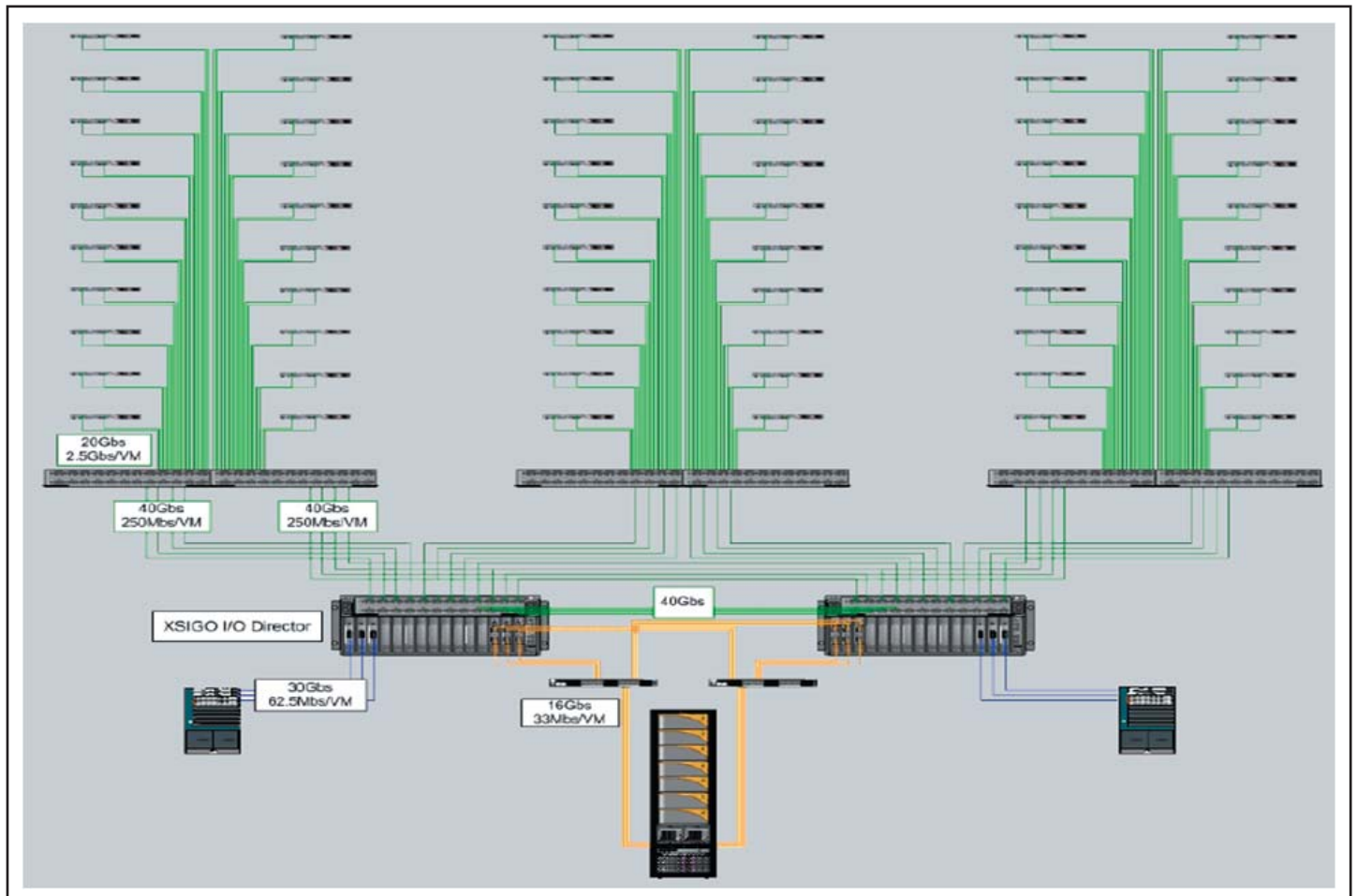


Abbildung 10: Vollredundante Konfiguration: 120 Server mit Virtual I/O-Switching

## Mehr Bandbreite im RZ mit Virtual I/O und optimierten Prozessorarchitekturen

und 8/10 GbFC unterstützen, in größtem Umfang. Muster gab es ja schon in 2009.

Das ist keine exotische Entwicklung, sondern findet im Rahmen von handelsüblichen Prozessorarchitekturen und Produkten wie dem Intel® Xeon® 5500-Prozessor statt. Virtualisierungssoftware ab z.B. VMware ESX 3.5 kann damit sinnvoll umgehen. Zukünftige Leistungssteigerungen sind vor allem dann zu erwarten, wenn die Intel® Quick Path Interconnect Architektur, die ich hier nur kurz ansprechen konnte, ihre völlige Entfaltung erlebt und gleichzeitig die Anzahl der Cores steigt. Damit kommen wir locker binnen der nächsten zwei Jahre in den 40 GbE-Bereich.

Der aufmerksame Leser wird gemerkt haben, dass ich die Intraserver-IOV mit dem Beispiel Intel am Server mit einer 10 GbE-Schnittstelle habe enden lassen. Das ist sozusagen die kleinste denkbare sinnvolle Schnittstelle. Andere Hersteller unterstützen via des SR-IOV-Standards weitere Schnittstellen, vor allem FC und IB. Mit Absicht habe ich dann beim IOV-Switching ein Beispiel mit IB-Anbindung gewählt. Das führt nämlich zu einem weiteren interessanten Diskussionsbereich:

- Einführung von Infiniband im Rack-Bereich. Durch den dramatischen Preisverfall können wir zum ersten Male auch im Bereich der kleineren Systeme von einer überragenden Netzwerktechnologie profitieren, die Ethernet und FC wirklich integrieren kann. Das dargestellte Produktbeispiel bezieht sich auf ein Rack und macht die Umsetzung von IB auf FC oder 10 GbE ToR. Das ist nur ein erster Schritt. Würde man einen IB-Switch ToR montieren, ergeben sich sofort viel weit reichendere Möglichkeiten.

Natürlich kann man im Rack-Bereich von den Vorzügen der Intraserver-IOV auch dann profitieren, wenn man für die Anbindung 10 GbE mit oder ohne FCoE oder iSCSI, 8/10 GbFC oder FLEX-10 benutzt. Das wird in vielen der Installationen so sein. Als technologischer Fundamentalist muss ich allerdings darauf hinweisen, dass das JETZT gut arbeitet, aber mit jeder Erweiterung oder Änderung kann sich die Frage nach der geeigneten Übertragungstechnologie im Rack erneut stellen. IB ist zwar im Moment aktuell etwas teurer, mit seiner Einführung ist aber dann für lange Zeit Ruhe.

Der nächste Punkt, der auf uns zukommt

ist der

- Durchbruch der 40 Gb-Marke.

Die einzige Kritik, die an den momentanen Virtual I/O Director-Lösungen anzubringen ist, ist die, dass diese Geräte im Grunde genommen selbst einen Engpass darstellen, weil sie mehrere DDR (20 Gb) IB-Leitungen, eben so viele, wie Server im Rack sind, auf mehrere 10 GbE oder 8/10 FC-Leitungen abbilden. Eine Abbildung auf 40 GbE und mindestens 16 GbFC wäre besser. Ich erwarte spätestens jenseits der 10 Gb erhebliche Probleme mit FCoE. Es funktioniert jetzt, weil man sehr viele Protokolle aufeinander stapelt, nämlich alle von IEEE-DCB und dazu nochmal die von FC-BB-5. Diese Protokolle müssen alle abgearbeitet werden und selbst bei großem Optimismus bin ich davon überzeugt, dass das bei 40 Gb FCoE gewaltige Probleme verursachen wird. Im nächsten Jahr kommt schon der 16 GbFC. Um ihn geeignet abzubilden, benötigt man 40 GbE, was auch in 2010 kommt, 2 X 10 GbE Trunking geht nicht. Das wird sehr spannend! Mit InfiniBand haben wir eine Technologie, die die 40 Gb heute schon problemlos beherrscht, auch weil das System vollständig Hardware-basiert ist.

## Kongress



### Netzwerk-Redesign Forum 2010 26.04. - 29.04.10 in Königswinter

Die Hauptveranstaltung vom 26.4. bis zum 28.4. stellt folgende Themenbereiche in den Mittelpunkt:

1. IT-Architekturen verändern Netzwerk-Architekturen
2. Der Markt im Wandel
3. Technologie im Wandel
4. Betrieb unter Druck
5. Sonderthemen

Der Vertiefungstag am 29.4. greift auch in diesem Jahr Themen auf, die hochaktuell, aber zu komplex für Einzelvorträge sind. Dies sind in diesem Jahr:

- Workshop 1: Voice und Video im Netzwerk  
Workshop 2: Disaster Recovery  
Workshop 3: IPv6: Parallelbetrieb und Migration

Das Plus-Programm zum Netzwerk-Redesign-Forum umfasst:

1. Virtualisierung im Rechenzentrum und die Einbindung in Netzwerke, Dr. Jürgen Suppan
2. Carrier Ethernet in der Analyse, Dr. F.J. Kauffels
3. 10, 40, 100 Gigabit-Ethernet, Dr. F.J. Kauffels
4. Fazit der Veranstaltung mit Mitschnitten der Highlights ausgewählter Vorträge, Dr. Jürgen Suppan

Moderation: Dr. Franz-Joachim Kauffels, Dr. Jürgen Suppan  
Preis: € 2.290,- zzgl. MwSt.



Buchen Sie über unsere Web-Seite [www.comconsult-akademie.de](http://www.comconsult-akademie.de)

# Aktuelle Veranstaltungen

## **IP-Telefonie: Vorbereitung, Migration, Management, 22.02. - 24.02.10 in Berlin**

Die Vorbereitung der Netze auf IP-Telefonie, die Migration von der klassischen Telekommunikation zu Voice over IP sowie der Betrieb der dadurch entstehenden komplexen Netz- und Anwendungsarchitektur konfrontieren alle Unternehmen mit neuen Herausforderungen. Das Wissen aus verschiedenen Bereichen, von der Netzinfrastruktur bis hin zu neuen und etablierten Kommunikationsapplikationen, muss zu einem interdisziplinären Know-how verdichtet und neu geordnet werden. Preis: € 1.690,- zzgl. MwSt.

## **Internetworking: optimales Netzwerk-Design mit Switching und Routing, 22.02. - 26.02.10 in Aachen**

Dieses 5-Tages-Intensiv-Seminar vermittelt Netzwerkbetreibern und Planern Methoden und Technologien zur erfolgreichen Strukturierung von Enterprise Netzwerken. Dabei wird das komplette Spektrum vom L2/L3 Switching über Redundanz/Routing bis hin zu Themen wie VLAN, WLAN-Integration, Multicast-Routing, VPN, MPLS, abgedeckt. Es werden sowohl die theoretischen Hintergrundkenntnisse als auch die Konsequenzen für den praktischen Betrieb von Netzwerken dargestellt. Fallstudien und Gruppenübungen mit Planungsbeispiel vermitteln Informationen, die in der Praxis sofort umgesetzt werden können. Preis: € 2.290,- zzgl. MwSt.

## **IP-Telefonie und Unified Communications erfolgreich planen und umsetzen, 01.03. - 03.03.10 in Düsseldorf**

Dieses 3-tägige Seminar behandelt die Projektschritte, Einsatz- und Migrations-Szenarien, einsetzbare Basis-Technologien, Komponenten und erweiterte TK-Anwendungen, Bewertungskriterien für eine TK-Lösung und gibt eine Übersicht über den bestehenden TK-Markt etablierter Hersteller wie Alcatel-Lucent, Avaya, Cisco, Nortel und Siemens aber auch des Newcomers Microsoft. Preis: € 1.690,- zzgl. MwSt.

## **Wireless LAN professionell, 01.03. - 03.03.10 in Nürnberg**

Dieses 3-tägige Seminar vermittelt den aktuellen Stand der WLAN-Technik und zeigt die in der Praxis verwendeten Methoden für Aufbau, LAN-Integration, Betrieb und Optimierung von WLANs im Enterprise-Bereich auf. Die verschiedenen WLAN-Varianten werden analysiert, Markt- und Produktsituation werden bewertet, und Empfehlungen für eine optimale Auswahl werden gegeben. Preis: € 1.690,- zzgl. MwSt.

## **E-Mail-Archivierung planen, evaluieren, umsetzen, 08.03. - 10.03.10 in Stuttgart**

Seit Anfang 2002 gibt es umfangreiche Vorschriften zur Speicherung und Archivierung digitaler Dokumente. Gleichzeitig gibt es Gründe der Auffindbarkeit von Dokumenten, der Beweissicherheit und der Informationssicherheit, um eine umfassende und zentrale Archivierung von Informationen im Unternehmen einzuführen. Durch effiziente Informationsarchivierung und Auffindbarkeit lassen sich erhebliche Kosten für jedes Unternehmen einsparen. Dieses 3-tägige Seminar behandelt einerseits die rechtlichen Vorschriften zur Speicherung von E-Mails und anderen digitalen Dokumenten sowie die zahlreichen Regelungen zur Beschränkung des Zugriffs auf die Daten aus Gründen des Persönlichkeitsrechts, des Fernmeldegeheimnisses, des Schutzes von Betriebsgeheimnissen und des Datenschutzes. Preis: € 1.690,- zzgl. MwSt.

## **Sicherheitsmechanismen für Voice over IP, 08.03. - 09.03.10 in Stuttgart**

Angesichts der Offenheit und geringeren Verfügbarkeit von Datennetzen ist das Thema Sicherheit das zentrale Projektthema bei der Umsetzung von Voice over IP. VoIP benötigt Sicherheitsmechanismen, die mindestens ein den konventionellen Telekommunikationsnetzen entsprechendes Niveau an Vertraulichkeit, Verlässlichkeit, Verfügbarkeit und Integrität sicherstellen. Darüber hinaus bietet die Umstellung die Chance, die Sicherheit der Sprachkommunikation über das bisherige Niveau hinaus zu verbessern. Preis: € 1.390,- zzgl. MwSt.

## **Trouble Shooting für Netzwerk-Anwendungen, 09.03. - 12.03.10 in Aachen**

Dieses Seminar beschreibt die typischen Störsituationen im Umfeld moderner Anwendungen, gibt Einblick in bisher als Black Box benutzte Mechanismen und Abläufe und trainiert die systematische und methodische Diagnose und Fehlerbeseitigung. Dabei wird die Theorie mit praktischen Übungen und vielen Fallbeispielen in einem Trainings-Netzwerk kombiniert. Die Teilnehmer werden durch dieses kombinierte Training in die Lage versetzt, das Gelernte sofort in der Praxis umzusetzen. Als Protokoll-Analysator kommt Wireshark zum Einsatz. Einer Verwendung selbst mitgebrachter Analyse-Software, mit deren Bedienung der Teilnehmer vertraut ist, steht nichts im Wege. Preis: € 2.190,- zzgl. MwSt.

## **Projektmanagement I: Projekte aus IT und Kommunikationstechnik leiten und organisieren, 15.03. - 19.03.10 in Aachen**

In diesem Intensiv-Seminar lernen Sie, ein Projekt aus IT und Kommunikationstechnik erfolgreich zu leiten und organisieren. Des Weiteren werden bewährte Wege aufgezeigt, wie Sie die Projektabwicklung in Ihrem Unternehmen konkret optimieren können. Preis: € 2.290,- zzgl. MwSt.

## **WAN-Planung für zentrale Dienste, 15.03. - 17.03.10 in München**

Wide Area Networks (WAN) müssen kostengünstig, leistungsfähig, skalierbar, hochverfügbar, sicher und managebar sein. Während bis vor wenigen Jahren langfristige WAN-Verträge von drei bis fünf Jahren abgeschlossen wurden, legt die dynamische Entwicklung nahe, die Vertragsbindung zu verkürzen, was mit einem ständigen Planungsprozess einhergeht. Dieser Umstand und die fortlaufenden Veränderungen im Markt zwingen zu einem permanenten Lern- und Informationsprozess, dem auch dieses 3-tägige Seminar dienen soll. Preis: € 1.690,- zzgl. MwSt.

## Zertifizierungen

### ComConsult Certified Network Engineer

#### Lokale Netze

19.04. - 23.04.10 in Aachen  
13.09. - 17.09.10 in Aachen  
22.11. - 26.11.10 in Aachen

#### TCP/IP und SNMP

03.05. - 07.05.10 in Bonn  
27.09. - 01.10.10 in Stuttgart

#### Internetworking

22.02. - 26.02.10 in Aachen  
17.05. - 21.05.10 in Bonn  
25.10. - 29.10.10 in Aachen

Paketpreis für alle drei Seminare € 6.183,- zzgl. MwSt. (Einzelpreise: je € 2.290,-)

### ComConsult Certified Trouble Shooter

#### Trouble Shooting 1

18.05. - 21.05.10 in Aachen  
21.09. - 24.09.10 in Aachen

#### Trouble Shooting 2

09.03. - 12.03.10 in Aachen  
22.06. - 25.06.10 in Aachen  
26.10. - 29.10.10 in Aachen

Paketpreis für beide Seminare, eine digitale Stromzange, die Prüfung und den Report „Fehlersuche in konvergenten Netzen“ € 4.120,- zzgl. MwSt.  
(Seminar-Einzelpreis € 2.190,-, mit Prüfung € 2.370,-)

### ComConsult Certified Voice Engineer

#### Basis-Seminar:

**Session Initiation Protocol-Basis-Technologie der IP-Telefonie**

15.03. - 17.03.10 in München  
28.06. - 30.06.10 in Bonn  
22.11. - 24.11.10 in Hamburg

#### Basis-Seminar:

**Sicherheitsmechanismen für Voice over IP**

08.03. - 09.03.10 in Stuttgart  
21.06. - 22.06.10 in Bonn  
03.11. - 04.11.10 in Bonn

#### Alternative 1:

**IP-Telefonie und Unified Communications erfolgreich planen und umsetzen**

01.03. - 03.03.10 in Düsseldorf  
07.06. - 09.06.10 in Königswinter  
04.10. - 06.10.10 in Bonn  
13.12. - 15.12.10 in Stuttgart

#### Alternative 2:

**IP-Telefonie: Vorbereitung, Migration, Management**

22.02. - 24.02.10 in Berlin

#### Optionales Einsteiger-Seminar: IP-Wissen für TK-Mitarbeiter

03.05. - 04.05.10 in Bonn  
27.09. - 28.09.10 in Stuttgart  
15.11. - 16.11.10 in Königswinter

Basis-Paket Alternative 1: Beinhaltet die zwei Basis-Seminare und Seminar „Alternative 1“  
Grundpreis: € 4.250,- zzgl. MwSt. statt € 4.770,- zzgl. MwSt.

Basis-Paket Alternative 2: Beinhaltet die zwei Basis-Seminare und Seminar „Alternative 2“  
Grundpreis: € 4.250,- zzgl. MwSt. statt € 4.770,- zzgl. MwSt.

Optionales Einsteigerseminar: Aufpreis € 990,- zzgl. MwSt. statt € 1.390,- zzgl. MwSt.

### ComConsult Zertifizierter Projektleiter

#### Projektmanagement I: Projekte aus IT und Kommunikationstechnik leiten und organisieren

15.03. - 19.03.10 in Aachen  
08.11. - 12.11.10 in Aachen

#### Projektmanagement II: Sitzungen moderieren, Projekte präsentieren, erfolgreich verhandeln und Teams führen

19.04. - 23.04.10 in Aachen  
29.11. - 03.12.10 in Aachen

Paketpreis für beide Seminare € 4.090,- zzgl. MwSt. (Einzelpreise: € 1.990,- und € 2.290,-)

## Impressum

Verlag:  
ComConsult Technology Information Ltd.  
ComConsult Research  
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](mailto:insider@comconsult-akademie.de)  
<http://www.comconsult-research.de>

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

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

Für unverlangte eingesandte Manuskripte  
wird keine Haftung übernommen  
Nachdruck, auch auszugsweise  
nur mit Genehmigung des Verlages  
© ComConsult Research