ComConsult Research

Der Netzwerk Insider

Februar 2010

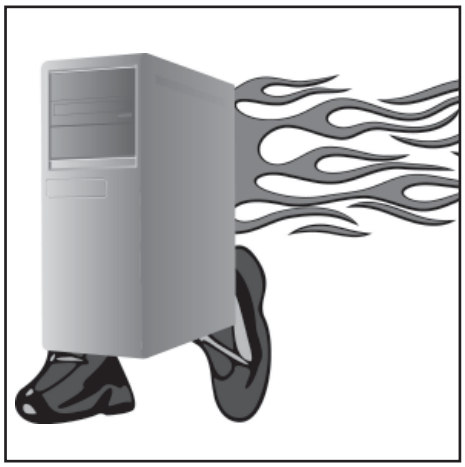
Systematische Weiterbildung für Netzwerk- und IT-Professionals

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.



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

Zweitthema

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 verbindungsbasierten 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 Verschwimmen 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 Tabletts 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 Mediemix 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 Prüfingenieure 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 Gerätegrenzen 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 gefährdert 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-

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

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 Internetzugänge 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“ (EVPL).

- **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 möglichst 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 Lösungen 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.

Schwerpunktthema

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

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.

Fortsetzung von Seite 1

- 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 Ressorcen-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 Verspechen 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-

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 krassem 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. Konsequent 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-

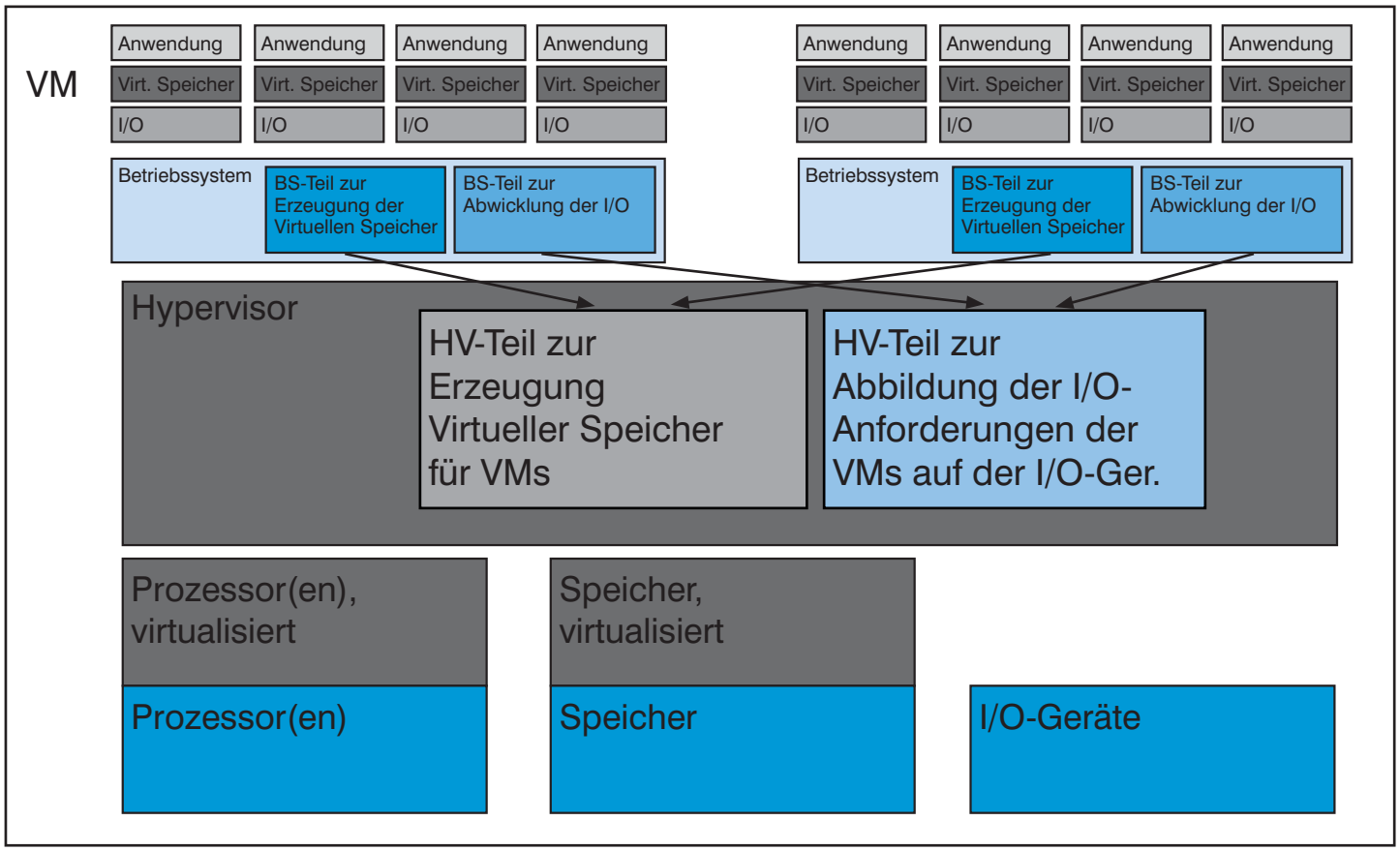


Abbildung 1: Virtuelle Maschinen und traditionelle I/O