ComConsult Research

Der Netzwerk Insider

September 2012

Systematische Weiterbildung für Netzwerk- und IT-Professionals

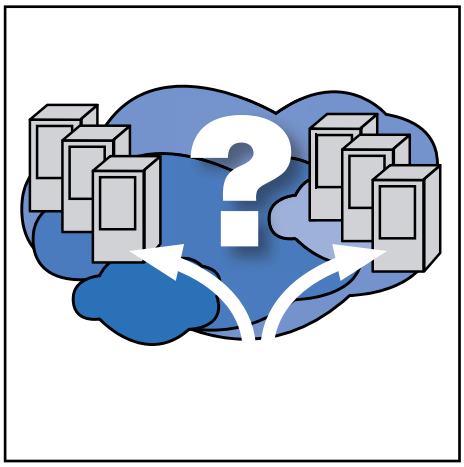
Schwerpunktthema

Routing im, vom und zum RZ

von Dr. Behrooz Moayeri

In den letzten Jahren wurde sehr häufig und sehr intensiv darüber diskutiert, wie eine skalierbare Layer-2-Netzstruktur für Rechenzentren aussehen soll. Diese Diskussion war angesichts der Herausforderungen, die durch die Servervirtualisierung verursacht werden, notwendig und wichtig.

Der Autor kann sich jedoch des Eindrucks nicht erwehren, dass wegen der Diskussion über Layer 2 ein anderer wichtiger Aspekt beim Design von RZ-Netzen in Vergessenheit geraten ist, nämlich das Routing im, vom und zum RZ. Oft kommt es dazu, dass sich Planer genau dazu wenig Gedanken gemacht haben, bis der Tag X kommt, an dem das Netz implementiert werden muss.



Häufig werden dann die Layer-3-Strukturen im und um das RZ irgendwie - vielleicht wie es gerade passt – aufgebaut. Das kann aber nicht im Sinne einer vorausschauenden Planung sein.

Warum Routing?

Fangen wir mit der grundsätzlichen Frage an, warum im Zusammenhang mit Rechenzentren Routing überhaupt noch erforderlich ist. Machen neue Layer-2-Verfahren das Routing im Zusammenhang mit RZ-Netzen nicht überflüssig?

weiter auf Seite 14

Zweitthema

Neue Protokolle im RZ: Funktionsumfang – Potential – Auswirkung auf die Infrastruktur

von Dipl.-Math. Cornelius Höchel-Winter

Reichen bestehende Netzwerktechnologien aus, um den Bedarf virtueller und verteilter Rechenzentren abzudecken? Die Idee, die in diesem Artikel diskutiert wird, ist die Verbindung von virtuellen Maschinen standortneutral in Form virtueller Layer-2-Netzwerke über beliebige dazwischen liegende Infrastrukturen hinweg.

Dahinter verbirgt sich die Frage, ob es überhaupt notwendig ist, dass virtuelle Maschinen zum Beispiel als Teil einer skalierenden Web-Applikation unabhängig von ihrem Standort Layer-2-Verbindungen untereinander pflegen müssen. Hinzu kommt, dass in Zukunft im Rahmen einer fortschreitenden Automatisierung virtuellen Maschinen automatisch Ressourcen zugewiesen werden und damit auch automatisch initiierte Wanderungen von VMs verbunden sein können. Gleichzeitig werden Rechenzentren und Ressourcen immer mehr verteilt aufgesetzt, sei es nur über Brandschutzgrenzen oder sogar über Standortgrenzen hinweg.

Natürlich ist das Thema komplex, eben weil der Aufbau verteilter Infrastrukturen mit Zugang zu Datenbanken und Speichersystemen zwischen verteilten Rechenzentren alles andere als einfach und allgemeingültig umzusetzen ist. Trotzdem gibt es einen schnell zunehmenden Bedarf für diese Art von Architektur, weil eben Web-Anwendungen für große und stark schwankende Teilnehmerzahlen über die dynamische Generierung von virtuellen Maschinen zur Laufzeit skalieren.

weiter auf Seite 24

Geleit

Software-Defined Networking: wer braucht das?

ab Seite 2

Standpunkt

Virtualisierung ohne Grenzen auch bei hohem Schutzbedarf?

auf Seite 22

Neuauflage

Professionelle Datenkommunikation

auf Seite 21

Aktuelle Sonderveranstaltung

Wireless Networking

ab Seite 23

Zum Geleit

Software-Defined Networking: wer braucht das?

Seit einiger Zeit wird in der Netzbranche intensiv über Software-Defined Networking (SDN) und damit zusammenhängend auch über OpenFlow diskutiert. Das Open Networking Foundation (ONF) genannte Konsortium hat sich beides, SDN und OpenFlow, auf die Fahne geschrieben und behauptet auf der eigenen Webseite, mit SDN werde man über Netze nie wieder wie früher denken. Nun, ewig das Gleiche denken tun nur jene, die nichts dazu lernen. Insofern wird jeder, der etwas davon versteht, in ein paar Jahren über eine so dynamische Technologie wie Kommunikationsnetze anders denken als heute. Die Frage ist nur, welche Rolle SDN und OpenFlow dabei spielen werden.

Ein Blick auf die Initiatoren der ONF gibt darüber Aufschluss, wen SDN und OpenFlow am meisten interessieren: Deutsche Telekom, Facebook, Google, Microsoft, Verizon und Yahoo, also allesamt Unternehmen, die sehr große Rechenzentren betreiben müssen. Technisches Kernstück von SDN ist das OpenFlow, ein Protokoll, mit dem Netzkomponenten mit sogenannten Controllern kommunizieren. Der Controller übernimmt Aufgaben, die bei einem konventionellen Switch oder Router von der sogenannten Control Plane übernommen werden. Die Unterscheidung der Control Plane und der Data Plane hat sich in den letzten ca. zwei Jahrzehnten bei Netzkomponenten etabliert. Aufgabe der Data Plane ist die (möglichst schnelle) Vermittlung von Paketen anhand sogenannter Forwarding-Tabellen. Diese legen fest, wie ein Netzgerät ein Paket mit bestimmten Merkmalen (zum Beispiel MAC- und/oder IP-Adressen) behandeln, d. h. vor allem verwerfen oder weiterleiten und über welchen Port senden soll. Die Einträge Forwarding-Tabelle können jedoch von Mechanismen der Control Plane stammen, zum Beispiel einem Routing-Protokoll, das in der Regel von der Central Processing Unit (CPU) eines Routers oder Switches bearbeitet wird.

Welchen Sinn kann es für die Konzentration der Control Plane auf den Controller geben? Die Idee ist, dass in einem großen Netz die Konfiguration vieler intelligenter Komponenten entfällt und komplexe Aufgaben der Control Plane nur noch vom Controller übernommen werden. Die Namensgleichheit mit einem Wireless Local Area Network (WLAN) Controller ist nicht zufällig. Auch in einem Controller-basierenden WLAN ist die Intelligenz auf die Controller konzentriert. Die WLAN Access Points werden von Controllern gesteuert. Der OpenFlow-Ansatz ist ähnlich. OpenFlow Switches sollen sich auf die Data Plane konzentrieren. Die Control Plane ist die Domäne des Controllers. Man stelle sich ein ganz großes Rechenzentrum vor, das aus hunderttausenden virtuellen Servern besteht, die auf tausenden physikalischen Servern laufen. Der Betreiber eines solchen RZs hat ein großes Interesse daran, dass die ganze Infrastruktur aus gleich aufgebauten und standardisierten Modulen besteht. Die Netzkomponenten dieser Module müssen dann einheitlich konfiguriert sein und nach den gleichen Verfahren und Modellen funktionieren. Die Konzentration der Intelligenz auf den Controller erleichtert die Einrichtung, den Betrieb und die Erweiterung einer solchen Infrastruktur.

Daher ist das Interesse großer RZ-Betreiber an OpenFlow kein Zufall. Auch kein Zufall ist die zeitliche Koinzidenz der OpenFlow-Aktivitäten mit dem Trend Cloud Computing. Wenn Betreiber öffentlicher Clouds erfolgreich Kunden anwerben, müssen sie eines ihrer wichtigsten Versprechen, nämlich dass sie eine IT-Infrastruktur dank Synergieeffekten effizienter und wirtschaftlicher betreiben können als ihre Kunden, einhalten. Sie müssen ein RZ der o. g. Dimensionen insgesamt mit deutlich weniger Mitarbeitern betreiben als die Summe der bisher dafür eingesetzten Mitarbeiter ihrer Kunden.

Die Motivation für die Standardisierung von OpenFlow ähnelt der Motivation jeder anderen Standardisierung, vor allem: Vermeidung der Abhängigkeit von einzelnen Herstellern, unkomplizierter Austausch einzelner Komponenten und Herstellung einer Marktmacht durch Bündelung der Potenziale mehrerer Hersteller. Ein Controller des Herstellers x soll eine Komponente des Herstellers y steuern können, solange beide die OpenFlow-Spezifikation einhalten.

Was hat das Ganze mit dem Begriff SDN zu tun? Der Controller basiert vor allem auf Software, die auf einem Standard-Server laufen soll. Dadurch soll die Möglichkeit eröffnet werden, dass ein Markt für Lösungsanbieter entsteht, die ihre Netzlösung auf Controller-Basis entwickeln. Die Konfiguration des Netzes erfolgt dann Software-gesteuert, womit wir bei der Namensgebung für SDN wären.

Soweit die Idee. Wie ist sie aber zu bewerten?

Grundsätzlich ist zu berücksichtigen, dass das Design und der Aufbau sehr großer Rechenzentren, die von Betreibern öffentlicher Clouds genutzt werden, anderen Gesetzmäßigkeiten und Prioritäten folgen als das Design und der Aufbau von wesentlich kleineren Umgebungen, die nur von einem Unternehmen genutzt werden. Ein privates RZ hat meistens nicht die dringenden Probleme, mit denen sich ein Public-Cloud-Anbieter auseinandersetzen muss. Andererseits kann sich ein Unternehmen für das eigene, privat genutzte RZ-Netz in der Regel keine Lösung leisten, für die kein einziger Lieferant verantwortlich ist. Stellen Sie sich die Situation vor, in der ein Controller- und ein Switch-Hersteller sich gegenseitig für eine Fehlfunktion im Netz verantwortlich machen. Bei der Komplexität von OpenFlow sind Fehlfunktionen und Interoperabilitätsprobleme trotz Standard nicht ausgeschlossen. Der Alptraum jedes Betreibers eines kleinen, privaten Rechenzentrums ist es, mit seinem Problem allein gelassen zu werden, weil ihm selbst die Expertise und der tiefe Einblick fehlen, um die Zuständigkeit für ein Problem eindeutig zuweisen zu können. Große Cloud-Anbieter haben völlig andere Möglichkeiten, Probleme selbst zu analysieren, den Verantwortlichen dafür zu finden und ihn zu einer Lösung zu motivieren. Eine Firma Microsoft oder Google ist für jeden Lieferanten so wichtig, dass die Bearbeitung jedes Problems auch für den Lieferanten oberste Priorität hat. Wie viele RZ-Betreiber gibt es, denen eine solche privilegierte Stellung zukommt?

Deshalb legen die meisten Betreiber privater Rechenzentren Wert darauf, in ihrer

Software-Defined Networking: wer braucht das?

Umgebung klare Zuständigkeiten für bestimmte Teilbereiche der Infrastruktur zu haben. Und es haben sich im Laufe der Jahre nun einmal spezialisierte Kompetenzbereiche für die Bereiche Netz, Speicher, Server und Virtualisierung herausgebildet. Für den Betreiber eines relativ kleinen Rechenzentrums ist die Situation mit diesen verschiedenen Kompetenzschwerpunkten bereits komplex genug. Viele sehnen sich ja nach weniger Komplexität, nach der guten alten Zeit, in der ein Unternehmen den Großrechner, die dazu gehörenden Kommunikationseinrichtungen, die Endgeräte und sogar viel Software dazu lieferte. Noch mehr Komplexität, zum Beispiel durch die Trennung der Zuständigkeit für die Control Plane und Data Plane innerhalb des Teilsystems Netz, ist das Letzte, wonach solche RZ-Betreiber fragen. In ihrem Bestreben nach Vereinfachung der Verhältnisse achten viele Betreiber kleiner und mittlerer Rechenzentren darauf, nur ja keine „exotische“ Lösung einzusetzen. Für solche RZ-Betreiber soll die Netzinfrastruktur am besten mit denselben Produkten und derselben Konfiguration vielfach erprobt und bewährt sein. Für die meisten kommen Netze mit Produkten verschiedener Hersteller nicht infrage.

Mit Unikaten und Sonderlösungen haben die großen Provider aber keine vergleichbaren Probleme. Vielmehr kommt es darauf an, Dienstleistungsprodukte anzubieten, die einen Markt möglichst schnell erschließen. Eine funktionierende Sonderlösung, die sich gut verkauft, d. h. im Falle der Public Clouds schnell Millionenumsätze generiert, ist kein Problem. Solche Anbieter erwarten gerade von SDN, dass sich Sonderlösungen schnell entwickeln lassen.

Wenn Sie zu den RZ-Betreibern gehören, die solche Sonderlösungen brauchen, wenn Sie schon nach Lösungen und Funktionen suchen, die von den bisherigen Netzprodukten nicht angeboten werden, dann sollten Sie SDN und OpenFlow mit großem Interesse verfolgen. Funktionierende, produktive Referenzinstallationen in großen Rechenzentren gibt es allerdings noch nicht. Aber mittlerweile haben sich viele führende Netzhersteller wie Alcatel-Lucent, Brocade, Cisco, Extreme, HP und Juniper der ONF angeschlossen. Sie wollen vor allem den o. g. Initiatoren der ONF zeigen, dass sie sich der Herausforderung stellen und nicht abseits stehen wollen, wenn es um die Lösung besonderer Herausforderungen großer Rechenzentren geht. Aber solche Situationen gab es in der Netzbranche häufig. Nicht die Idee jedes Konsortiums mit einer langen imponierenden Mitgliederliste hat sich durchgesetzt.

Wenn Sie Betreiber eines eher kleinen bis mittleren Rechenzentrums sind, in dem die Anzahl der Netzkomponenten im ein-, zwei- bis maximal unteren dreistelligen Bereich liegt, müssen Sie sich höchstwahrscheinlich Herausforderungen stellen, für die SDN und OpenFlow noch keine Lösung bieten. Ob es jemals dazu kommt, dass die Betreiber kleiner und mittlerer RZs wirklich von SDN und OpenFlow profitieren, ist noch offen. Diese RZ-Betreiber sollten SDN und OpenFlow auch nicht ignorieren, aber immer berücksichtigen, dass der Fokus dieser Trends noch bei den RZs großer Cloud-Anbieter liegt.

Ihr
Dr. Behrooz Moayeri

Aktueller Kongress

ComConsult Rechenzentrum Infrastruktur-Redesign Forum 2012

05.11. - 08.11.12 in Köln

Die ComConsult Akademie veranstaltet vom 05.11. - 08.11.12 ihr "ComConsult Rechenzentrum Infrastruktur-Redesign Forum 2012" in Köln.

2012 ist ein anstrengendes Jahr für Planer und Betreiber von Corporate IT-Infrastrukturen. Auch wenn verschiedene technische Einzelfragen der Vergangenheit wie z.B. die Konvergenz von „normalem“ und Speicherverkehr weitest gehend geklärt werden konnten und angesichts der Entwicklung von 10, 40 und 100 GbE auch für einen größeren Zeitraum im Netz hinreichend Leistung zu noch nie dagewesenen günstigen Preisen zur Verfügung stehen wird, verbleiben schwer wiegende Fragestellungen vor allem hinsichtlich der Zusammenfügung von Einzeltechnologien zu einer modernen, flexiblen, skalierbaren, beherrschbaren und wirtschaftlichen IT-Infrastruktur, deren Herz das RZ ist.

BYOD. Der Access Bereich ist dabei, einen tiefgreifenden Wandel zu durchlaufen. In den vergangenen 25 Jahren konnte man davon ausgehen, dass die Desktop-PCs die in der Menge dominierenden Endgeräte sind, die überwiegende Anzahl dieser PCs fest an Arbeitsplätzen steht und im Rahmen einer strukturierten Verkabelung angeschlossen werden können. Das war der Normalfall, eine wireless Anbindung hatte statistisch eher Sonderstatus.

Durch die massive Einführung neuartiger Endgeräte, allen voran das iPad oder vergleichbare Geräte, wird sich das schnell ändern. Im Privatbereich wird ein Benutzer einen kleinen Zoo dieser Geräte mindestens bestehend aus einem Smartphone, einem Pad und einem Notebook haben. Alle diese Geräte stellen unterschiedliche Formfaktoren grundsätzlich vergleichbarer Dienste wie Internet, eMail usf. dar und unterscheiden sich lediglich in Art und Geschwindigkeit der Darstellung und der I/O. Sie synchronisieren sich automatisch und der Anwender wird immer das Gerät verwenden, was grade am praktischsten für seine Zwecke ist. Natürlich sind alle diese Geräte drahtlos vernetzt, sowohl untereinander, als auch mit Peripherie und weiteren Geräten wie TV. Das wichtigste Peripheriegerät ist der Wireless Router für die Verbindung zur Außenwelt.

Dies alles ist heute schon Realität und der Trend ist unumkehrbar. Ein Anwender wird über kurz oder lang verlangen, dass er die gleiche Bequemlichkeit auch hinsichtlich der Unternehmensanwendungen bekommt. Er wird sich weigern, seinen Gerätepark um Geräte zu erweitern, die nur für die Nutzung im Zusammenhang mit Unternehmensanwendungen stehen, sondern die gleichen Geräte benutzen wollen wie zuhause. Der Versuch, ihn daran hindern zu wollen, wird erfahrungsgemäß scheitern.

Also ist es die Aufgabe des Unternehmens, ihm den gleichen Komfort verbunden mit Sicherheit für die sensiblen Unternehmensdaten und allgemeiner Rechtssicherheit zur Verfügung zu stellen.

Das rückt die Frage nach der sinnvollen Bereitstellung der Unternehmensdaten in einer privaten oder hybriden **Cloud**-Struktur, auf die die neuen Geräte üblicherweise angewiesen sind, in den Vordergrund. Spannend ist hierbei natürlich auch die Zugriffskontrolle und die Thematik um die Desktop Virtualisierung, die sich um die Dimension der Pad-Virtualisierung erweitert.

Waren noch in 2011 die meisten Cloud-Angebote für Unternehmen eher weniger nutzbar, hat sich dies vor allem durch die Schaffung von Angeboten mit angereicherter Funktionalität geändert. Die Frage, welche Daten und Anwendungen doch vielleicht statt des Eigenbetriebes aus wirtschaftlichen Gründen in eine Cloud ausgelagert werden könnten, stellt sich sozusagen jeden Tag aufs Neue. Es werden sich auch völlig neue Distributionsmodelle für Unternehmens-Software materialisieren. So verwenden z.B. viele Unternehmen die Software von SAP. SAP unternimmt aber durch die Übernahme von SuccessFactors und die geplante Übernahme von Ariba wesentliche Anstrengungen, Software in Mietmodellen anzubieten. Für die Unternehmen, die das Angebot nutzen können, würden sich erhebliche wirtschaftliche Vorteile ergeben. Für SAP ergibt sich nicht nur die Möglichkeit, die Walldorfer Software in Unternehmen zu tragen, die sie sich bisher einfach nicht leisten konnten, sondern auch Upgrades und Updates in erheblich schnellerem Takt als bisher mit wesentlich vereinfachter Distribution zu ermöglichen und damit die Qualität letztlich deutlich zu erhöhen. Unter der Voraussetzung geeigneter Infrastrukturen in den Unternehmen entsteht so eine eindeutige Win-Win-Situation.

Letztlich laufen alle diese Anforderungen im RZ zusammen.

Dort sollen hinsichtlich der Netze die von allen Herstellern vollmundig angekündigten „Data Center Fabrics“ das Ei des Kolumbus sein. Mit zweistufiger Strukturierung, hoher Leistung, extrem geringer Latenz und Konvergenzfunktionen wie DCE und FCoE sollen sie der neue Systembus der Virtualisierten Umgebung werden. Aber, es gibt auch Kritik...

Die Fabrics der Hersteller haben teilweise eine enorme Leistung zu einem ebenso enormen Preis. Ist es wirklich wirtschaftlich, Funktionen einzukaufen, die man wahrscheinlich nie benötigt oder wartet man besser ab? Redundanz ist ein gerne hoch strapaziertes Schlagwort und die gibt es auch reichlich. Sieht man aber genau hin, basiert Vieles auf proprietären Multi Chasssis Verfahren. Eigentlich wollen wir doch durchgängig standardisierte Lösungen. Wie steht es damit? Durch die Entwicklung neuer speicherbasierter Switch ASICs ist in den meisten Kästen, besonders bei Access Switches, nicht mehr viel verbaut. Also sollten die Preise massivst fallen. Die Hersteller bemühen sich nun krampfhaft, viele proprietäre Zusatzfunktionen von enger VM-Anbindung über Flow-Konzepte bis hin zu Management-Tools hinzuzufügen, die mögliche Kunden zur Anschaffung genau ihrer Fabric bewegen sollen. Aber sind diese Funktionen wirklich so nützlich, dass sie eine Abkehr von einem standardisierten Weg und ggf. erhebliche Mehrkosten rechtfertigen? Gibt es nicht auch alternative Wege, wenn man diese Funktionen zu brauchen glaubt? Schließlich stellt sich dann noch die Frage, ob das RZ-Netz in seiner bisherigen Form nicht zu großen Teilen völlig verschwinden wird, weil Switch-ASICs auf Server-Blades mit geeigneter ScaleOut-Software wie im HPC-Umfeld schon üblich die Funktionen von RZ-Distribution- und Access-Bereich übernehmen. Welche Konsequenzen hätte das?

Storage Virtualisierung und -Integration sind seit Jahren heiße Themen. Die Hersteller haben sich endlich auf breiter Front dazu durchgerungen, Strategien zu entwerfen, die es einem Betreiber im Sinne einer Speicher-Virtualisierung ermöglichen, im Laufe der Zeit die verwendete Laufwerktechnik zu ändern und neuen Mög-

lichkeiten, wie aufkommenden professionell nutzbaren SSD-Speicher, über die Zeit und nach Bedarf flexibel anzupassen. Außerdem gibt es noch viele nützliche Zusatzfunktionen. Allerdings hat das auch Risiken und Nebenwirkungen, weil die Anforderungen an Netze in diesem Umfeld massiv steigen können. Es zeigt sich sogar, dass im Höchstleistungsbereich eine konvergierte Ethernet-Technik ggf. nicht mehr benutzt werden kann, sondern nur InfiniBand Lösungen hinreichender Leistung bereitstellt.

Server- und Anwendungs-Virtualisierung. Die Stufe der einfachen Server-Virtualisierung dürfte in den meisten Unternehmen erfolgreich verlaufen sein und auch Zusatzfunktionen, z.B. hinsichtlich eines stabileren Betriebs werden gerne genutzt. Aber, das ist ja noch längst nicht das Ende der Entwicklung. Es besteht Einigkeit darin, dass die Zukunft eines großen Teils der Anwendungsentwicklung bei kooperierenden Web-Anwendungen liegt. Diese Thematik wurde ja in den letzten Jahren schon aufgenommen und führte zum Bild vom „Netz als Systembus“. Spätestens mit vSphere 5 hat VMware aber ein wesentlich weiter übergreifendes Systembild entworfen, bei dem VMs sich nicht nur freizügig im RZ oder Unternehmensnetz bewegen, sondern auch zwischen privaten und öffentlichen Clouds hin- und herwandern können. In vFabric 5 findet sich eine koordinierte Sammlung von Entwicklungswerkzeugen und mit vCloud soll man dieses Sznenario komplett steuern und betreiben können. Alleine für die Entwicklung anspruchsvollerer BYOD-Strategien wäre das höchst praktisch. Aber was bedeutet das für andere, mehr konventionelle Anwendungen? Und: welche Anforderungen an die Infrastruktur (Server, Speicher, Netz) sind damit verbunden?

Management und Betrieb. Die angesprochenen Entwicklungen führen zu einer noch nie da gewesenen Komplexität von Corporate Networks. Durch Konzentration und Konvergenz bei hohen Datenraten spart man zwar Verbindungen, Kabel und Wartungpunkte, aber dafür hat es jetzt jede Verbindung wirklich „in sich“. Baut man mit dem RZ wirklich eine private Cloud für die Versorgung Tausender Mobilgeräte auf, wird man selbst mit einer vierstelligen Anzahl von Netzwerk-Administratoren nicht mehr im Einzelnen sehen können, was auf dem Netz wirklich passiert. Eine weitere neue Dimension entsteht durch die wandernden Virtuellen Maschinen. Anfallende Management-Daten müssen mehr und mehr automatisch mit regelbasierten Systemen ausgewertet werden. Ein Netz muss so konstruiert sein, dass Fehler im herkömmlichen Sinne eigentlich gar nicht mehr auftreten dürfen, denn man wäre mit der Suche nach ihnen heillos überfordert. Nun, Providernetze haben diese Probleme schon seit geraumer Zeit und funktionieren dennoch. Können wir hier etwas übernehmen? Was bieten uns die Hersteller dafür an? Es gibt natürlich viele Systeme für die Steuerung begrenzter Prozesse, wie solche, die den Paketfluss im Netz überwachen oder solche, die kontrollieren, was mit den VMs passiert. Durch das Zusammenwachsen von Servern, Speichern und Netzkomponenten zu einem virtualisierten Ganzen stellt sich wieder die längst vergessen geglaubte Frage nach Instrumenten für das integrierte Netz- und System-Management.

Das ComConsult Rechenzentrum Infrastruktur-Redesign Forum 2012 ist die zentrale Veranstaltung des Jahres, auf dem die Problemkreise nicht nur singulär, sondern vor allem übergreifend von Spezialisten, Beratern und Herstellern diskutiert werden. Neben dem Hauptforum gibt es vertiefende Workshops und eine Ausstellung, die thematisch tief in das Forum eingebunden ist. Flankiert von Reports, Videos und weiteren Sonderpublikationen entsteht ein einzigartiges Informationsspektrum. Sichern Sie sich frühzeitig einen Platz in dieser meist schnell ausgebuchten Veranstaltung!

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

ComConsult Rechenzentrum Infrastruktur-Redesign Forum 2012

Ich buche den Kongress

ComConsult Rechenzentrum Infrastruktur-Redesign Forum 2012

mit Intensiv-Tag
☐ vom 05.11. - 08.11.12 in Köln
zum Preis von € 2.490,-- netto

ohne Intensiv-Tag
☐ vom 05.11. - 07.11.12 in Köln
zum Preis von € 2.090,-- netto

nur Intensiv-Tag
☐ am 08.11.12 in Köln
zum Preis von € 990,-- netto

☐ inklusive Report
zum Preis von € 338,-- netto

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

☐ Bitte reservieren Sie mir ein Zimmer

vom _____ bis_____ 12

im Radisson Blu Hotel Köln

_____ Vorname

_____ Nachname

_____ Firma

_____ Telefon/Fax

_____ Straße

_____ PLZ,Ort

_____ eMail

_____ Unterschrift

Programmübersicht - ComConsult Rechenzentrum Infrastruktur-Redesign Forum 2012

Montag, den 05.11.2012

9:30 bis 10:45 Uhr
Neue IT-Technologien und die Auswirkungen auf RZ-Infrastrukturen
- Cloud-Technologien im Unternehmen: was bedeutet das?
- Neue Endgeräte-Technologien und Auswirkungen auf Architekturen
- Infrastrukturen für mobile Endgeräte • Gibt es den Server der Zukunft?
- Wie wichtig wird OpenStack? • Virtualisierung: am Anfang oder am Ende?

Dr. Jürgen Suppan, ComConsult Research Ltd.

10:45 - 11:15 Uhr Kaffeepause

11:15 bis 12:30 Uhr
Analyse: Data-Center-Architekturen:
- Architekturmodell für die Unterstützung kooperierender Web-Anwendungen • Aktuelle Entwicklungen der Schaltkreistechnologie und Auswirkungen auf zukunftssichere Investitionen
- Traditionelle Netzwerke am Ende? SDN und Open Flow ändern unser Verständnis von Netzwerken
- Leistungsfähige Alternativen der VM-Anbindung

Dr. Franz-Joachim Kauffels, freier Unternehmensberater

12:30 bis 14:00 Uhr Mittagspause

14:00 bis 14:45 Uhr
Analyse: Server-based Computing, Virtualisierung und Cloud Computing
- Kapselung von Daten und Anwendungen im RZ mit Server-based Computing und Desktop Virtualisierung
- Gefährdungen durch Zentralisierung von Clients
- Malware-Schutz: Umdenken ist erforderlich
- Data Center Firewalls: Neue Konzepte und deren Tücken
- Kerndisziplin: Data Loss Prevention (DLP)
- Sicherheitsarchitekturen für Private Clouds
- Rolle von Public Clouds für die Enterprise IT
- Anforderungen an sichere Public Clouds

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

14:45 bis 15:30 Uhr
Mandantenfähigkeit und Zonenkonzepte im RZ
- Mandantenfähige RZ-Netze: Techniken und deren Praxistauglichkeit
- Brauchen wir angesichts Server-based Computing und Cloud Computing noch Sicherheitsmaßnahmen im Netz?
- Zonen- und Firewall-Architekturen im RZ
- Zwiebelschalen-Modelle im Widerspruch zu Mehrmandantennetzen

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

15:30 bis 16:00 Uhr Kaffeepause

16:00 bis 16:45 Uhr
Sicherer Betrieb von Zonenarchitekturen
- Terminal Server als Jump Host: Möglichkeiten und Grenzen
- Virtualisierungstechniken zur sicheren Entkopplung administrativer Zugriffe
- Zonen für die Administration und Überwachung: Firewall-Infation droht
- SIEM: Sondermülldeponie oder sinnvolles Instrument des Security Incident Management? • Kurzschluss in SAN und NAS vermeiden

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

16:45 bis 17:30 Uhr
Web-Anwendungen im Rechenzentrum
- Webanwendungen: mehr als nur Webseiten
- Architektur und Skalierbarkeit
- Integration von Kunden, Partnern und Mitarbeitern
- Windows, Mac, iOS, Android: eine App für alle?
- Sicherheitsrelevante Aspekte • Was bringt die Zukunft?
- Empfehlungen

Markus Schaub, ComConsult Research Ltd.

17:30 bis 18:00 Uhr
Service-basierte Netzwerke: das Ende des normalen Netzwerk-Designs
- Mandentenfähigkeit und Trennung von Datenströmen über L2/L3-Grenzen gefordert
- MPLS hat im Enterprise ausgedient
- L2/L3-Abgrenzungen sind Diskussionen von Gestern
- VXLAN ohne die Komplexität von PIM /PIM-SM/PIM-SSM etc.
- L2/L3-übergreifende Multicast-Dienste sind erforderlich
- Vision: Anwendungs-orientierte Netzwerk-Services

Heinz Behrens, Avaya GmbH & Co KG

Ab 18:00 Uhr Get Together

Dienstag, den 06.11.2012

9:00 bis 10:00 Uhr
Performance Optimized Data Center POD
- Bedarf für modulare Data Center Lösungen
- Was ist ein POD (Performance Optimized Data Center, Point of Delivery, Point of Deployment)?
- POD Architektur-Elemente (Container, Server-Block, Storage-Block, Netzwerk-Block) • Referenz-Architekturen
- POD-Beispiele (Cisco VMDC, Dell vStart, HP EcoPOD, IBM PMDC, SGI CloudRack)

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

10:00 bis 11:00 Uhr
Auf dem Weg zum RZ und den Infrastrukturen der Zukunft
- Migration DC zum Fabric enabled DC
- POD Design und Cloud Ready
- Überblick SW Router CSR1000v: liegt hier die Zukunft für virtuelle Umgebungen? • Erster Blick auf „onePK“
- Ciscos Sicht zu SDN/OF

Gerd Pflueger, Matthias Wessendorf, Cisco Systems GmbH

11:00 bis 11:30 Uhr Kaffeepause

11:30 bis 12:15 Uhr
Optimierte Switche für den RZ-Bedarf
- Erfüllen Standard-Chip-Architekturen den Bedarf?
- Vorteile einer offenen Linux-Lösung
- Software Defined Networking
- Low Latency
- Wieviel Stromverbrauch darf es ein?
- Wie wichtig wird VxLAN?

Manfred Felsberg, Frank Laforsch, ARISTA Networks, Inc.

12:15 bis 12:45 Uhr
Technologie-Statements

12:45 bis 14:00 Uhr Mittagspause

14:00 bis 14:45 Uhr
Positionierung der TCP/IP-Intelligenz
- Welche Alternativen gibt es? • Ist Offload wirklich die beste Lösung?
- Vor- und Nachteile, Empfehlung

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

14:45 bis 15:30 Uhr
RZ-Netze: Evolution oder Revolution?
- Mängelbereiche bisheriger Konstruktionen
- Entwicklung von Switching-Substraten mit speicherbasierenden ASICs
- SDN: neuer Provider-Hype oder nutzbar für alle?
- Das RZ im Schrank • Migrationsempfehlungen

Dr. Franz-Joachim Kauffels, freier Unternehmensberater

15:30 bis 16:00 Uhr Kaffeepause

16:00 bis 16:45 Uhr
BYOD, DLP und mobile Virtualisierungs-Technologien
- Welche Anforderungen stellt BYOD an die Datenhaltung?
- Sind diese Anforderungen auch für Company-owned-Devices relevant?
- Welche Technologien eignen sich zur Trennung privater und geschäftlicher Daten?
- Was ist mobile DLP und eignet es sich zur Umsetzung von BYOD/COD?
- Sandboxing, Server-based Computing und Virtualisierung - ein Überblick

Dominik Zöller, ComConsult Beratung und Planung GmbH

16:45 bis 17:30 Uhr
Smartphones, Tablets und der Gast-Zugang
- Einsatzszenarien für mobile Endgeräte im Unternehmen
- Mobile und nomadische Nutzung von Smartphones & Tablets
- Netzanbindung via 3G/4G und WLAN
- BYOD, Zonenkonzepte und Gastzugänge

Dominik Zöller, ComConsult Beratung und Planung GmbH

Programmübersicht - ComConsult Rechenzentrum Infrastruktur-Redesign Forum 2012

Mittwoch, den 07.11.2012

9:00 bis 09:45 Uhr
Aktuelle Trends und Entwicklungen am Hypervisor-Markt
- Welche entscheidenden Neuerungen brachte die VMworld 2012 für den VMware ESX?
- Was wurde auf der Synergy 2012 in puncto Citrix XenServer vorgestellt?
- Wie hat Microsoft im Windows Server 2012 seine Virtualisierungsplattform Hyper-V verbessert?
- Welche Relevanz haben diese Entwicklungen auf aktuelle Data Center Designs?
- Wie haben sich die Hersteller damit strategisch positioniert?

Dipl.-Inform. Matthias Egerland, ComConsult Beratung und Planung GmbH

9:45 bis 10:30 Uhr
Automatic Storage Tiering: Wunderwaffe oder technischer Overkill?
- Herausforderung exponentiellen Speicherwachstums
- Hierarchisches Speicher-Management (HSM), Information Lifecycle Management (ILM) und ihre Grenzen
- Voraussetzung: Definition unterschiedlicher Speicherklassen (Storage Tiers)
- Wie funktioniert Automatic Storage Tiering?
- Welche Unterschiede gibt es bei den marktführenden Storage-Systemen?
- An welche Grenzen stößt dieser technische Ansatz?
- Wie positionieren sich die Hersteller?
- Welche Strategie sollte im modernen Data Center verfolgt werden?

Dipl.-Inform. Matthias Egerland, ComConsult Beratung und Planung GmbH

10:30 bis 11:00 Uhr Kaffeepause

11:00 bis 11:45 Uhr
Zukunftsorientierte Speicherlösungen und -methoden
- Herausforderungen an Speicherlösungen
- Senkung der Investitionskosten
- Eindämmung der Betriebskosten
- Enterprise Funktionalitäten zu einem auch für kleine Unternehmen bezahlbaren Preis

Dr. Georgios Rimikis, Hitachi Data Systems GmbH

11:45 bis 12:30 Uhr
Service-orientierte Infrastruktur: Konvergierte HP-Lösungen für das RZ *Florian Bettges, Hewlett-Packard GmbH*

12:30 bis 14:00 Uhr Mittagspause

14:00 bis 14:45 Uhr
Aktuelles zu IBM XIV Storage
- Neue Ankündigungen
- Ausblick
- Kundenbeispiel
- Live-Demo *Dirk Vogelsang, IBM Deutschland GmbH*

14:45 bis 15:30 Uhr
Projektbericht Datensicherung
- Herausforderung: Einheitliche Backup-Landschaft für eine komplexe Systemumgebung
- Backup2Disk- versus Backup2Tape-Lösungen
- Chancen durch den Einsatz moderner VTLs
- Backup- & Redundanzkonzepte für Datenbanken

Dipl.-Ing. Peter Koch, inforsacom Informationssysteme GmbH

15:30 bis 16:15 Uhr
Virtualisierte Serveranbindung: Kampf der Konzepte
- Software-basierte vSwitches
- Direct I/O
- Probleme bei der vMotion+FT
- Hybrides Treiber-Design, SR-IOV
- Unterstützung der offenen Standards
- VMware vCloud
- VXLAN
- STT
- NVGRE

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

16:15 Uhr Ende der 3-tägigen Veranstaltung
Kaffeepause für Teilnehmer der 4-tägigen Veranstaltung

Donnerstag, den 08.11.2012 - Cloud Computing und die Auswirkungen auf das Rechenzentrum der Zukunft

9:00 bis 09:45 Uhr
Analyse: Was leistet Cloud-Computing: was leistet es und wo sind die Grenzen?
- Ziele, Vorteile und Versprechen
- Cloud Service- und Liefermodelle im Vergleich
- Analyse der verschiedenen Lager: wer will was erreichen?
- Vor- und Nachteile von Public Cloud Diensten
- Private Cloud: die Lösung?
- Bewertung: werden die Ziele eingehalten?
- Empfehlungen für eine Cloud-Strategie

Dr. Jürgen Suppan, ComConsult Research Ltd.

9:45 bis 10:30 Uhr
Wie ist eine Private Cloud aufzubauen?
- Betriebliche und technische Anforderungen
- Auswahl des Hypervisors
- Dimensionierung der Virtualisierungsumgebung
- Cluster-Design
- DMZ-Design
- Storage-Design
- Migration und Provisioning
- Monitoring und Reporting

Dipl.-Inform. Matthias Egerland, ComConsult Beratung und Planung GmbH

10:30 bis 10:50 Uhr Kaffeepause

10:50 bis 12:05 Uhr
Virtualisiertes RZ als Basis für die Private Cloud
- Was bedeuten HA, FT, und Disaster Recovery Mechanismen für unsere Ressourcen?
- Globale und regionale RZ-Virtualisierung
- Anforderungen an Storage und Netz

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

12:05 bis 13:00 Uhr
Public-Cloud-Marktübersicht
- Dienste aus der Public Cloud: Übersicht
- Public Cloud Produkte und Anbieter
  - IaaS
  - PaaS
  - SaaS
  - UCaaS

Dominik Zöller, ComConsult Beratung und Planung GmbH

13:00 bis 14:00 Uhr Mittagspause

14:00 bis 14:45 Uhr
Worauf ist bei der Ausschreibung von Cloud-Diensten zu achten?
- Daten- und Rechtssicherheit
- Integration in das Service-Portfolio
- Service-Vereinbarungen
- Anbietersicherheit und Rückmigration

Claus Elfering, ComConsult Beratung und Planung GmbH

14:45 bis 15:45 Uhr
Rechtliche Aspekte bei Public Clouds
- Was ist erlaubt, was nicht?
- Helfen individuelle Verträge?
- Wie wichtig ist die Unternehmens-seitige Verschlüsselung?

Ulrich Emmert, esb Rechtsanwälte

15:45 Uhr Ende der 4-tägigen Veranstaltung

Aktueller Kongress

ComConsult TK-, UC- und Videokonferenzforum 2012

19.11. - 22.11.12 in Düsseldorf

Die ComConsult Akademie veranstaltet vom 19.11. - 22.11.12 ihr "ComConsult TK-, UC- und Videokonferenzforum 2012" in Düsseldorf.

Dieses hochaktuelle Forum analysiert aktuelle Trends, neue Technologien und Produkt-/Hersteller-Strategien im Bereich TK, UC und Videokonferenztechnik. Die Kernthemen sind: wie viel UC braucht TK; zukunftsweisende Client-Strategien; User Centric Communications; der Kunde, das unbekannte UC-Wesen; Videokonferenztechnik der Zukunft.

In diesem Jahr stehen fünf Themen im Mittelpunkt des Forums:

Wie viel UC braucht TK?
Telefonieren muss Jeder, aber wie viel Unified Communication wird wirklich benötigt und welche Alternativen der Umsetzung gibt es? Wir analysieren:

- Wo stehen integrierte Lösungen, die TK und UC aus einem Guss liefern?
- Wie sinnvoll sind Ergänzungs-Lösungen, die mehr TK-orientierte Installationen durch eine externe UC-Lösung ergänzen?
- Was bieten die Hersteller?
- Welche Lösungen werden bevorzugt umgesetzt?
- Welche Anforderungen stellt der Mittelstand an die Kommunikationsinfrastruktur?

Zukunftsweisende Client-Strategien – Welche Bedeutung haben mobile Endgeräte in Zukunft und wie werden sie integriert?
Für viele Benutzer ist der zeitgleiche Umgang mit mehreren Endgeräten inzwischen die Normalität. Der traditionelle Ansatz mit Desktop PC und Telefon wird der aktuellen Lage nicht mehr gerecht. Nach Apple und Google wird nun auch Microsoft den Markt der mobilen Endgeräte attackieren – und bietet erstmals eine einheitliche Plattform für alle Endgeräte. Parallel bieten die mobilen Endgeräte ein völlig neues Bedienverständnis, das speziell UC unter erheblichen Druck setzt. Wir analysieren:

- Welche Rolle spielen mobile Endgeräte in Zukunft?
- Lassen mobile Endgeräte die Bedienbarrieren zwischen verschiedenen Apps verschwinden? Brauchen wir dann UC überhaupt noch?
- Wie sieht UC im Umfeld mobiler Endgeräte aus? Wie spielen die verschiedenen Geräte zusammen?
- Wohin entwickelt sich die Client-Technik auf mobilen Geräten?
- Was passiert mit privaten iPads und iPhones, die dienstlich genutzt werden sollen?

User Centric Communications UCC
Nach der Infrastrukturkonvergenz rückt der Anwender von UC-Lösungen wieder in den Mittelpunkt. UC kann nur funktionieren, wenn der Client alle Funktionen intuitiv nutzbar umsetzt. Hieran scheitern bisher fast alle Lösungen. Anders im Bereich der mobilen Kommunikation: Apple hat mit dem iPhone den Markt verändert und den Benutzer in die Mitte der Architektur gestellt. Traditionelle Anbieter wie Nokia sind mit ihren Bedienkonzepten in der Versenkung verschwunden. iOS und Android prägen heute das Verständnis der Benutzer in der Handhabung auch komplexer Kommunikations-Funktionen. Unter den inzwischen weit verbreiteten Apps auf den mobilen Geräten befinden sich viele Apps, die Funktionalität aus dem Bereich UC anbieten. An diesen Lösungen aus dem Konsumenten-Markt muss sich UC messen lassen. UC wird nur überleben, wenn Benutzer-zentrische Lösungen von den Herstellern auch tatsächlich umgesetzt werden. Wir analysieren:

- Von UC zu UCC: was bedeutet das?
- Die Rolle von Social Media im Unternehmensumfeld
- Neue Messaging Dienste und ihre Nutzung
- UCC aus der Cloud: eine wirkliche Alternative?
- Wie sollte der ideale Client aussehen?
- Sollte es einen einheitlichen Client über alle Plattformen geben?

Der Kunde, das unbekannte UC-Wesen?
Unternehmen verdienen ihr Geld mit Kunden. Aber genau an dieser Stelle hören UC-Lösungen typischerweise auf. Dabei liegt genau hier der größte potenzielle Mehrwert. Das Contact Center ist dabei einer der Angelpunkte der Unternehmenskommunikation. Hier entfalten moderne Kommunikationsplattformen und Social Media ihr volles Potenzial. Wir analysieren:

- Welche Alternativen der Einbindung externer Kommunikationspartner gibt es?
- Wann kommt die wirklich offene UC-Lösung?
- Ist Skype die Lösung und welche Rolle spielt die Skype-Integration in Microsoft Lync?
- Das Contact Center – Zwischen Vermittlungsplatz 2.0 und Social Media Hub.

Videokonferenz in der Sackgasse?
Die Anbieter von Videokonferenz-Lösungen treten seit Jahren auf der Stelle. Genau die im Marketing immer wieder beschworene Integration aller Mitarbeiter und Kunden in eine Gesamtlösung, also der Übergang von einer teuren Lösung für wenige Teilnehmer hin zu einer bezahlbaren Lösung für viele erfolgt im Rahmen von UC bisher nicht. Dabei fordert die Explosion mobiler Endgeräte mit Diensten wie Fuze und WebEX aber genau diesen Übergang. Wir analysieren:

- Wie sieht die Video-Konferenz-Lösung der Zukunft aus?
- Wird die Webkonferenz die Videokonferenz verdrängen?
- Welche neuen Standards sind wann verfügbar und verändern sie die Welt?

In einem weiteren Schwerpunkt widmen wir uns dem aktuellen Portfolio der Hersteller. Mit Cisco Jabber erzielt erstmals ein Konkurrent eine vergleichbar tiefe Integration in die Client-Welt wie Microsoft Lync. Aber auch die Konkurrenz schläft nicht und feilt eifrig an intuitiven Bedienkonzepten. Microsoft legt mit Lync 2013 nach. Wie die Hersteller die Anforderungen der Kunden lösen wollen und wie sie sich strategisch positionieren erfahren Sie im Rahmen des Intensivtages:

- Wie setzt Microsoft den Markt mit dem neuen Release unter Druck?
- Welche Konzepte verfolgen die anderen Hersteller?
- Wie setzen die Hersteller die Kundenanforderungen um?
- Was kommt in den nächsten Jahren?

Das ComConsult TK-, UC- und Videokonferenzforum 2012 bietet Top-aktuelle Information und Analysen mit ausgewählten Experten. Eine ausgewogene Mischung aus Analysen, Hintergrundwissen und Projekterfahrungen in Kombination mit Produktbewertungen und Diskussionen liefert das ideale Umfeld für alle Planer, Betreiber und Verantwortliche solcher Lösungen. Zögern Sie nicht, sich rechtzeitig einen Platz in dieser Veranstaltung zu sichern.

Programmübersicht - ComConsult TK-, UC- und Videokonferenzforum 2012

Montag, den 19.11.2012

9:30 bis 10:30 Uhr
Keynote
- UC 2015 - wo steht UC?
- Auswirkungen mobiler Endgeräte auf die UC-Architektur
- Alle Funktionen auf allen Geräten?
- Welche Auswirkungen werden Windows 8 und iOS 6 haben?
- Ist All-in-One noch eine attraktive Lösung?
- Wie viel Social Media brauchen UC und CC?
- Braucht UC Video Conferencing oder Web Conferencing oder beides?
- Wie viel UCC braucht der Mittelstand?
- … und was ist mit DECT?

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

10:30 bis 11:00 Uhr
Von UCC zu User-centric Communications
- Von der Infrastruktur-Konvergenz zum intuitiven Bedienkonzept
- Prozessoptimierung durch UCC
- Soziale Medien im Unternehmen
- Konsumerisierung des Clients und der Kommunikation

Dominik Zöller, ComConsult Beratung und Planung GmbH

11:00 bis 11:15 Uhr
Hersteller-Vortrag

11:15 - 11:45 Uhr Kaffeepause

11:45 bis 12:30 Uhr
UCaaS – Kommunikation aus der Cloud
- UCaaS-Architekturen
- Erfahrungen aus der Praxis
- Cloud trifft Realität – Typische Probleme bei der Umsetzung von UCaaS
- Cloud Readiness Assessments – was ist zu beachten?

Tolga Erdogan, Dimension Data Germany AG & Co KG

12:30 bis 13:00 Uhr
Videokonferenz im Wandel
- Merkmale verschiedener Videolösungen aktuell und zukünftig
  - Qualitätsstufen
  - Zusatzfunktionen
  - Erforderliche Hardware und Software
- Merkmale von Webkonferenzen aktuell und zukünftig
  - Präsentations-Anteil
  - Videoanteil
  - Videoqualität
  - Erforderliche Hardware und Software
- Aktuelle technische Veränderungen
  - Bandbreiten im Internet
  - Server, Mediagateways
  - Neue Codecs
- Konsequenzen und Fazit

Markus Schaub, ComConsult Research

13:00 bis 14:30 Uhr Mittagspause

14:30 bis 15:15 Uhr
Stand der Videokonferenz-Technik
- Integration von Web- und Videoconferencing
- Standardisierungsbemühungen - SVC, H.265 und Co.
- Hardware- vs. Software-MCU

N.N.

15:15 bis 15:45 Uhr
UCC, Video und Mobility
- Sinnvolle Anwendungsszenarien von Mobile UCC
- Smartphones & Tablets als Videoendpunkt?
- Bedienkonzepte mobiler UCC-Clients

Mario Seefried, Vidyo GmbH

15:45 bis 16:15 Uhr Kaffeepause

16:15 bis 17:00 Uhr
Clientstrategien
- Workstation, Notebook, Tablet und Smart-phone
- Zukunftsweisende Client-Strategien
- Welche Funktionalität braucht/soll der UCC-Client haben?

Dominik Zöller, ComConsult Beratung und Planung GmbH

17:00 bis 17:30 Uhr
Kontextbasierte Kommunikation
- Medienvielfalt und überforderte Anwender
- Zielgerichtet kommunizieren durch Kontext-basierte Kommunikation
- Kundenszenarien und Praxisbeispiele

Thomas Römer, Avaya Deutschland GmbH

17:30 bis 18:00 Uhr
These zum Get Together – UCC gehört ins Internet
- Ist die Cloud-Paranoia gerechtfertigt?
- Wie viel Mehrwert bietet ein geschlossenes Kommunikationssystem?
- Wie könnte eine offene UC-Architektur aussehen?
- Was braucht man zur Umsetzung?

Dominik Zöller, ComConsult Beratung und Planung GmbH

Ab 18:00 Uhr Get Together

Dienstag, den 20.11.2012 - Vormittag

9:00 bis 10:00 Uhr
UC-Lösungs-Ansätze: Best of Breed vs. All-in-One
- All-In-One Lösungen
  - Umfang
  - Schnittstellen
  - Betrieb
- Best-of-Breed Varianten
  - Welche Kombinationen machen Sinn?
  - Frontend Integration
  - Backend Integration
- Wie stehen die Hersteller zu Frontend und Backend Integration?
- Hersteller-Beispiele
  - Alcatel-Lucent
  - Cisco
  - Innovaphone
  - Siemens
- Managed Service

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

10:00 bis 10:45 Uhr
Kommunikation und Kollaboration mit Lync 2013
- Neuerungen in Lync 2013 – Video, Voice, Apps
- Client-Integration mit Windows 8
- Hybrid-Cloud-Architektur mit Office 365

André Liesenfeld, Microsoft Deutschland GmbH

10:45 bis 11:15 Uhr Kaffeepause

11:15 bis 12:15 Uhr
Mehrstandort-Konzepte
- Mehrstandort UC-Architekturen
- Datenraten in WAN und Internet
- Managed Service vs. UCaaS
- Providerkonzepte: Integration von On-Premise Managed Service und Hosted PBX

Claus Elfering, ComConsult Beratung und Planung GmbH

12:15 bis 12:45 Uhr
Warum ISPs an Cloud-Produkten scheitern …
- Welche Rolle spielen Cloud-Produkte im Portfolio der ISPs?
- Warum bleibt der Erfolg aus?
- Wie kann kollaborative Produktentwicklung helfen?

Dipl.-Kfm. Robin Häberle, Bauhaus-Univesität Weimar

12:45 bis 14:15 Uhr Mittagspause

Programmübersicht - ComConsult TK-, UC- und Videokonferenzforum 2012

Dienstag, den 20.11.2012 - Nachmittag

14:15 bis 15:00 Uhr
Die Kommunikationspläne des Mittelstandes
- Wie viel UC braucht der Mittelstand?
- Was sind unabdingbare Leistungsmerkmale?
- Welche Technik muss integriert werden?
- Wie funktioniert die Migration?

Dominik Zöller, ComConsult Beratung und Planung GmbH

15:00 bis 15:45 Uhr
State of the Art bei SIP Trunking
- Einsatzpläne der Unternehmen
  - Marktstudien
  - Praxisbeispiele
- Angebote der Provider
  - BT
  - COLT
  - T-Systems
  - Vodafone
  - …
- Zertifizierungen: Hersteller, Provider, neutrale Gremien
  - SIPconnect oder any-to-any?
  - SIPforum
  - BITkom

Markus Geller, ComConsult Research GmbH

15:45 bis 16:00 Uhr
Hersteller-Vortrag

16:00 bis 16:30 Uhr Kaffeepause

16:30 bis 17:15 Uhr
Heterogene UC-Lösungen und ihr Management
- Multi-Vendor-Architekturen
- Video-Integration
- Integration von Drittanbieter-Telefonen
- Management von heterogenen UC-Lösungen

N.N., Siemens Enterprise Communications GmbH & Co KG

17:15 bis 18:00 Uhr
UC-Integration von Leitständen
- Integration von VoIP und Funksystemen
- Integration der Video-Überwachung
- Kommunikation für Werksfeuerwehr, Werkschutz und Energieversorger
- Herausforderung Notfall-Szenarien

Dr. Alexander Koenen-Dresp, CONET Solutions GmbH

Mittwoch, den 21.11.2012

9:00 bis 10:00 Uhr
Moderne Contact Center Lösungen
- „Vermittlungsplatz 2.0“
- Integrierte ACD-Lösungen
- Multimedia Contact Center
- Data Mining und Social Media

Claus Elfering, ComConsult Beratung und Planung GmbH

10:00 bis 10:30 Uhr
Avaya Contact Center
- Lösungsübersicht
- Aktuelle Features
- Kundenszenarien

Stefan Dietrich, Avaya Deutschland GmbH

10:30 bis 11:00 Uhr
Cisco UCCE
- Lösungsübersicht
- Aktuelle Features
- Kundenszenarien

Cisco Systems GmbH

11:00 bis 11:30 Uhr Kaffeepause

11:30 bis 12:15 Uhr
Voxtron Lync CC
- Zusammenspiel von UC und Contact Center
- Contact Center mit Lync
- Kundenszenarien

Dipl.-Betrw. Ralf Mühlenhöver, Voxtron GmbH

12:15 bis 12:30 Uhr
Hersteller-Vortrag

12:30 bis 14:00 Uhr Mittagspause

14:00 bis 15:00 Uhr
UC-Firewalls
- Firewall-Architekturen und Zonenkonzepte
- Welche Probleme bestehen bei Firewalling und UC?
- Welche Rolle spielen STUN und ICE?
- UC-Firewalls und Session Border Controller

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

15:00 bis 15:30 Uhr
UC-Firewalls und SBCs
- Gerätetypen, Feature Sets und Einsatzzweck
- Referenzarchitektur(en)
- Erfahrungen aus Kundenprojekten

Andreas Wächter, ACME Packet

15:30 bis 16:00 Uhr
Standpunkt UC
- Wo steht UC heute?
- Wo geht es hin?
- Wrap-up des UC-Forums

Dominik Zöller, ComConsult Beratung und Planung GmbH

16:00 Ende der 3-tägigen Veranstaltung
Kaffeepause für Teilnehmer der 4-tägigen Veranstaltung

Donnerstag, den 22.11.2012 - Intensivtag User-centric Communications - UC-Clients und Anwendungsszenarien

9:30 bis 16:30 Uhr

Der Intensiv-Tag beginnt mit einer Vorstellung des Tagesprogramms und der aktuellen Fragestellung im Themenfeld UCC.

Im weiteren Tagesverlauf folgen 4 Herstellervorträge mit Präsentationen/ Live Demos zum Thema UC-Clients

Beendet wird dieser Intensiv-Tag mit einem Abschlussvortrag und einem Fazit.

11:00 bis 11:30 Uhr Kaffeepause
12:30 bis 14:00 Uhr Kaffeepause

16:30 Ende der Veranstaltung

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
ComConsult TK-, UC- und Videokonferenzforum 2012

☐ 3 Tage	☐ 4 Tage	☐ 1 Tag
Kongress vom 19. - 21.11.12 in Düsseldorf zum Preis von € 1.890,-- netto*	**Kongress mit Intensiv-Tag** vom 19. - 22.11.12 in Düsseldorf zum Preis von € 2.290,-- netto*	**Intensiv-Tag** am 22.11.12 in Düsseldorf zum Preis von € 790,-- netto*

*Preise gültig bis zum 30.09.12. Die Buchung eines Kongresses innerhalb der Frühbucherphase kann nicht storniert werden. Gerne akzeptieren wir aber einen Ersatzteilnehmer.

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

vom _____ bis zum _____12
im Van der Valk Airporthotel Düsseldorf.

Selbstzahler-Sonderpreis von € 139,-- pro Übernachtung inklusive Frühstück

Zusätzlich bestelle ich folgenden Technologie-Report

☐ Session Initiation Protocol - zum Sonderpreis von 338,- € netto

☐ Unified Communications: Cisco versus Microsoft - zum Sonderpreis von 338,- € netto

☐ Sicherheitsmechanismen für Voice over IP - zum Sonderpreis von 338,- € netto

☐ VoIP-Kollektion - alle drei Reports zum Sonderpreis von 890,- € netto

_____
Vorname

_____
Nachname

_____
Firma

_____
Straße

_____
PLZ, Ort

_____
Telefon, Fax

_____
E-Mail

Ich habe die Kongressbedingungen zur Kenntnis genommen.

_____
Unterschrift

ComConsult Akademie
Pascalstraße 25 - 52076 Aachen
Telefon +49 (2408) 955-300
info@comconsult-akademie.de
www.comconsult-akademie.de

Das Wissensportal

Das Wissensportal

"Das Wissensportal“ ist das neu gestaltete Web-Portal von ComConsult Research. Hier finden Sie eine bunte Mischung aus aktuellen Informationen, persönlichen Meinungen und ausführlichen Grundlagen-Artikeln über die gesamte Themenpalette der IT- und Netzwerkwelt. Die Artikel des ComConsult Wissensportals geben Ihnen die Möglichkeit der Stellungnahme, des Kommentars oder der Diskussion mit anderen Lesern. Nutzen Sie diese Gelegenheit, die Sichtweise anderer Spezialisten zu erfahren. Unser Newsletter informiert Sie hierbei regelmäßig über Neuerscheinungen.

Warum Layer2?

13. September 2012 von Dr. Behrooz Moayeri

Angesichts der Herausforderungen, vor die der Trend zu Layer 2 in Rechenzentren die IT-Verantwortlichen in Unternehmen stellt, ist eine Diskussion um die Frage entbrannt, wie es zu diesem Trend kommen konnte, nachdem sich die Entwicklung der unternehmensinternen Netze jahrelang am durch und durch Layer-3-strukturierten Internet ein Beispiel genommen hatte.

Kompletten Artikel lesen unter www.comconsult-research.de

Schnittstellen im RZ: einfacher oder komplexer?

12. September 2012 von Dr. Behrooz Moayeri

Mit der Servervirtualisierung übernahm die Virtualisierungslösung eine Netzfunktionalität, nämlich das Bereitstellen von virtuellen Switch Ports für die virtuellen Maschinen (VMs). Daher hat der Marktführer VMware diese Funktionalität als den sogenannten vSwitch implementiert. Später wurde zwischen dem in Standard Switch umbenannten einfachen vSwitch und dem Distributed Switch unterschieden. Die Idee beim Distributed Switch ist, dass mehrere vSwitches zu einer logischen Einheit zusammengefasst und an einer Stelle, in der Regel im Rahmen der Managementlösung für die ganze Virtualisierungsumgebung, konfiguriert und administriert werden.

Kompletten Artikel lesen unter www.comconsult-research.de

Software Defined Networking: Quo Vadis

10. September 2012 von Markus Nispel

Endlich! Eine Technologie, die alle Probleme mit der Netzwerkinfrastruktur lösen wird. Wieder einmal. Aber hatten wir das nicht schon einmal? In schöner Regelmäßigkeit sehen wir Technologien dem Gartner Hype und seinen Phasen folgen. Was vor 2 Jahren noch die Fabrics und auch FCoE (Fibre Channel over Ethernet) waren – und wobei FCoE sich gerade im “Through of desillusionment” befindet – ist SDN auf dem “Peak of inflated expectations”. Oder kann man die Diskussionen zu den Problemlösungen durch SDN, die Anzahl der Startups in diesem Bereich, eine unklare Definition von SDN und der Kauf eines kleinen Startups für 1,25 Milliarden USD durch VMware anders interpretieren? Klar ist für mich, dass SDN eine Technologie ist, die zum Bleiben gekommen ist. Die Konzepte machen sehr viel Sinn, wir bei Enterasys hatten schon in den frühen 90ern damit experimentiert und forcieren seit einigen Jahren diese Art des Networking, ohne es je SDN genannt zu haben. Viele Kunden setzen die heute erfolgreich ein. Auch in der Telefonie waren IN Intelligente Netze auch schon immer präsent. Was aber genau ist ein SDN?

Kompletten Artikel lesen unter www.comconsult-research.de

Nick McKeown Video: Reinventing the Internet

11. September 2012 von Dr. Jürgen Suppan

Nick McKeown von der Stanford University gehört zum harten Kern der Entwickler der Technologie von Software Defined Networks SDN. Dieses Video gibt einen guten Einstieg in die Technologie.

Kompletten Artikel lesen unter www.comconsult-research.de

Software Defined Networking: nur weil VMware technisch versagt?

7. September 2012 von Dr. Jürgen Suppan

Software Defined Networking SDN wird momentan in den USA als die Zukunft der Netzwerke dargestellt. In der Tat gibt es Gründe über die Architektur und Qualität unserer bestehenden Netzwerke und insbesondere das Versagen im schnellen Einführen neuer Lösungen nachzudenken. Tatsächlich aber ist für viele Anwender der durch Virtualisierung von Servern kreierte Bedarf die Hauptmotivation für SDN, erlaubt SDN doch eine Netzwerk-neutrale Mandantenfähigkeit und die Ausdehnung von L2-Netzen über beliebige Infrastrukturen hinweg. Aber wird hier das Pferd nicht von hinten aufgezäumt? Nur weil VMware und die anderen Virtualisierungsanbieter unfähig sind ihre Systemkommunikation auf L3 umzustellen, sollen ganze Architekturen geändert werden?

Kompletten Artikel lesen unter www.comconsult-research.de

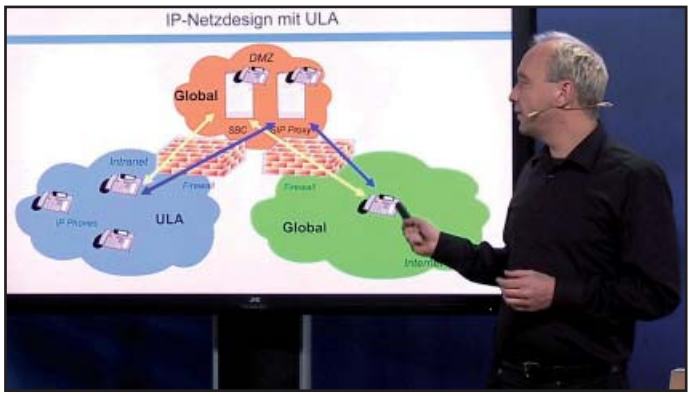
ComConsult-Study.tv

Aktuelle Neuerscheinungen bei ComConsult-Study.tv

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

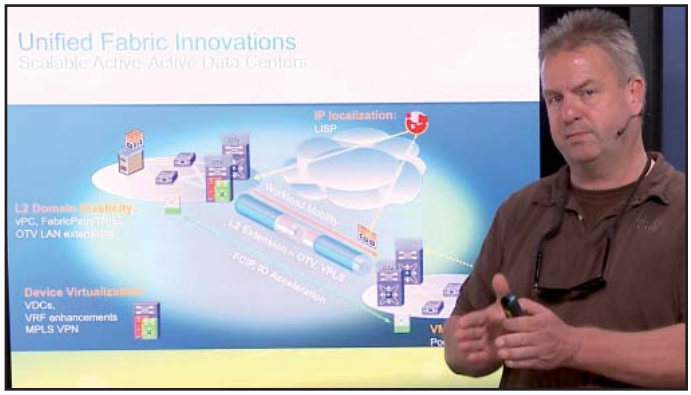
Software Defined Networks werden momentan als die Zukunft der Netzwerke gehandelt. Geringere Kosten, mehr Flexibilität, geringere Komplexität und weniger Fehler sind die Attribute, mit denen diese Technologie beworben wird. Dr. Suppan analysiert und bewertet was hinter SDN steckt und inwieweit Unternehmen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

Themenbereich: Netzwerke
IPv6 Grundlagen
Referent: **Markus Schaub**
Zeit: 02:13:54 gesamt
Im Abo: kostenlos



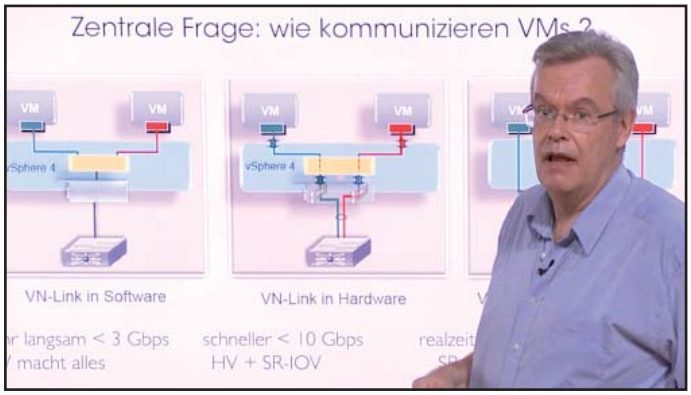
In den beiden letzten Teilen der IPv6 Grundlagenreihe werden die Adress-Autokonfiguration und DHCPv6 vorgestellt.

Themenbereich: Hersteller
Nexus 7000 Update
Referent: **Gerd Pflüger**
Zeit: 00:31:50
Preis: kostenlos



Der Nexus 7000 ist Ciscos strategisches Produkt für das Rechenzentrum. Dieses Video bringt sie in 30 Minuten auf den neuesten Stand hinsichtlich der verfügbaren Harware- und Software-Optionen sowie der zukünftigen Roadmap. Typische Einsatz-Szenarien bis hin zum Betrieb verteilter Rechenzentren werden beschrieben.

Themenbereich: Analyse und Strategie
Aktuelle Entwicklungen bei IT-Architekturen und Auswirkungen auf Netzwerke
Referent: **Dr. Franz-Joachim Kauffels**
Zeit: 01:56:12 gesamt
Preis: kostenlos



In der zweiteiligen Videoreihe analysiert Dr. Kauffels die aktuellsten Entwicklungen in der IT und leitet daraus Anforderungen an die Leistung und das Design zukünftiger Netzwerke ab.

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

Schwerpunkthema

Routing im, vom und zum RZ

Fortsetzung von Seite 1

Dr. Behrooz Moayeri ist bei der ComConsult Beratung und Planung GmbH als Mit-glied der Geschäftsleitung tätig. Er hat in den letzten Jahren unter anderem viele Unternehmen zu Themen der RZ-Vernetzung beraten.

Die Antwort ist ein klares Nein und wird im Folgenden begründet.

Man stelle sich ein RZ-Netz vor, an das verschiedene RZ-typische Endgeräte wie Server, Network Attached Storage (NAS) etc. angeschlossen sind (Abbildung 1).

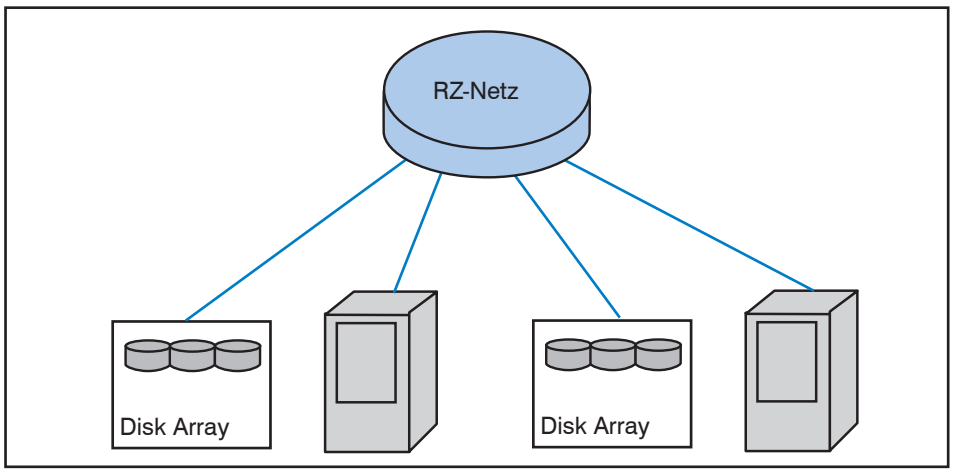


Abbildung 1: RZ-Netz mit Servern, NAS etc.

Wenn das in der Abbildung 1 dargestellte RZ-Netz als eine Layer-2-Broadcast-Domäne aufgebaut wird, gilt diese Broadcast-Domäne zugleich als eine einzige Sicherheits- und Fehlerdomäne, wenn man vom Einsatz der bisherigen Layer-2-Netzverfaheren (einschließlich neuer Verfahren wie Shortest Path Bridging SPB, Transparent Interconnection of Lots of Links TRILL etc.) ausgeht.

Das ist jedoch in fast keinem RZ erwünscht. Es darf nicht sein, dass die fehlerhafte IP-Konfiguration irgendeines Endgeräts im RZ potenziell das gesamte RZ-Netz oder jedes beliebigen Servers darin lahmlegen kann. Und es darf nicht sein, dass die Kompromittierung eines einzelnen Systems im RZ die Sicherheit des gesamten Rechenzentrums beeinträchtigen kann.

Also teilt man das RZ-Netz in mehrere Layer-2-Broadcast-Domänen auf, die aus Gründen der Verfügbarkeit über mindestens zwei Routing-Instanzen miteinander verbunden sind (Abbildung 2).

Die in der Abbildung 2 dargestellten Routing-Instanzen müssen nicht unbedingt klassische Router oder Layer-3-Switches sein. Infrage kommen auch Sicherheitskomponenten mit Routing-Funktion, zum Beispiel Firewalls.

Aus denselben Gründen wie für die interne RZ-Netzstruktur angeführt ist kein RZ-Netz zu empfehlen, das sich in derselben Broadcast-Domäne befindet wie alle Clients, die auf das RZ zugreifen. Das bedeutet, dass der Zugriff der Clients auf das RZ über Routing-Instanzen erfolgen muss. Soll dieser Zugriff von keinem Single Point of Failure abhängig sein, ist das RZ über mindestens zwei Layer-3-Instanzen mit den Clients verbunden sein (Abbildung 3).

Abbildung 3 zeigt die minimale Routing-Struktur eines RZ-Netzes. Kein RZ, das diesen Namen verdient, kann ohne die dargestellte Routing-Funktion im, vom und zum RZ auskommen.

Ungünstiges Routing

Nun, da wir die grundsätzliche Frage geklärt haben, was die Notwendigkeit von Routing im Zusammenhang mit dem RZ-Netzdesign betrifft, betrachten wir die Probleme, um die es in diesem Beitrag hauptsächlich geht und die wir als „ungünstiges Routing“ zusammenfassen wollen.

Um die Problematik „ungünstiges Routing“ zu verstehen, müssen wir zunächst definieren, was „optimales Routing“ bedeutet. Einigen wir uns auf die Definition, dass optimales Routing die Auswahl der Pfade mit den kürzesten Signallaufzeiten und den niedrigsten Paketverlustraten ist. Letzteres setzt häufig voraus, dass die Übertragungskapazitäten im Netz optimal genutzt werden, zum Beispiel durch Verteilung der Last auf verschiedene Wege. Das heutige Internet weist diesbezüglich einerseits noch Optimierungspotenziale auf und ist andererseits das Ergebnis von über vierzig Jahren Erfahrungen bei der Optimierung von Routing.

Die Abbildung 4 zeigt zwei verschiedene Wege zwischen einem Server und einem Speichersystem in unserem „Minimal-RZ“.

In unserem Minimaldesign sind die beiden in der Abbildung 4 dargestellten Pfade hinsichtlich der Anzahl der Layer 3 Hops gleichwertig, d. h. bei Anwendung optimaler Routing-Verfahren kommt es zur Nutzung beider Pfade.

Nun stelle man sich vor, einer der Wege

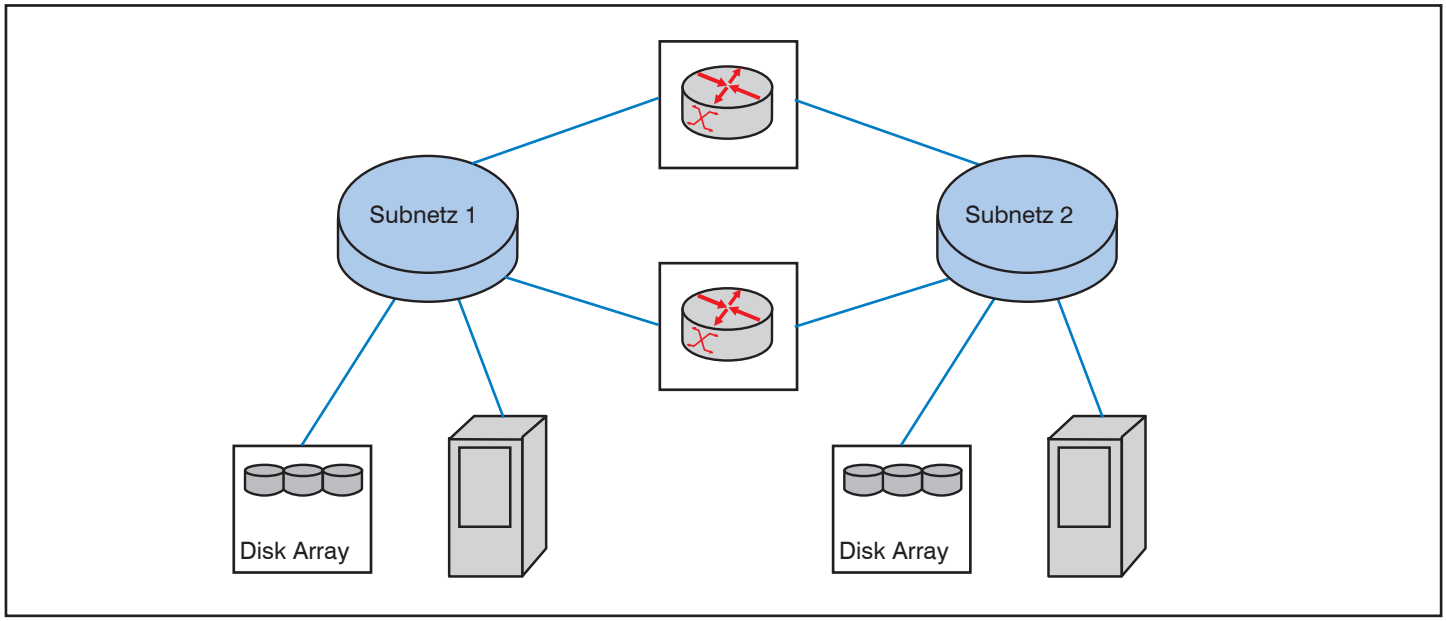


Abbildung 2: Aufteilung des RZ-Netzes in Broadcast-Domänen

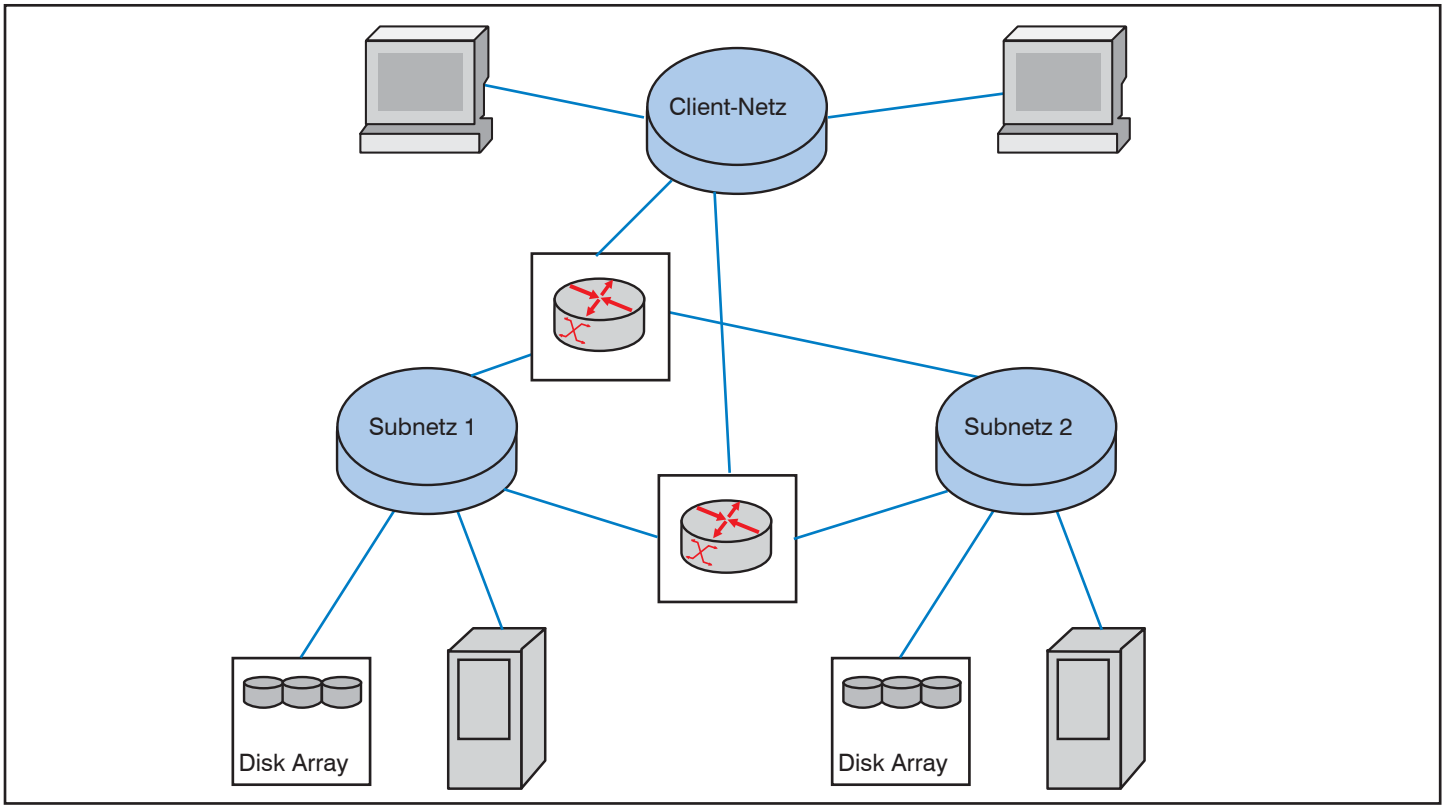


Abbildung 3: Routing im RZ sowie zwischen RZ und Clients

sei hinsichtlich der tatsächlichen Signallatenz weniger optimal als der andere. Das gilt zum Beispiel, wenn der Server, das NAS-System und einer der Router am selben Standort, aber der andere Router an einem anderen Standort aufgestellt sind. Dazu kann es leicht kommen, wenn die beiden RZ-Standorte, wie häufig gefordert, über Layer 2 transparent verbunden sind.

Wegewahloptimierung im RZ

Um sicherzustellen, dass eine optimale Layer-3-Route auch mit optimalen Layer-2-Pfaden verbunden ist, dürfen die Wegewahlentscheidungen auf Layer 3 und Layer 2 nicht entkoppelt werden. Damit kommen wir zu dem in der Abbildung 5 dargestellten Design.

Wie aus der Abbildung 5 hervorgeht, müssen die beiden Netzkomponenten nicht nur Layer-3-, sondern Layer-2-Intelligenz besitzen, um für eine aus Gesamtsicht optimale Wegewahlentscheidung treffen zu können. Eine solche Entscheidung kann zur Auswahl des in der Abbildung 5 dargestellten Pfades vom Server zum NAS-System führen. Der Pfad geht über die erste Layer-2/3-Komponente in

Routing im, vom und zum RZ

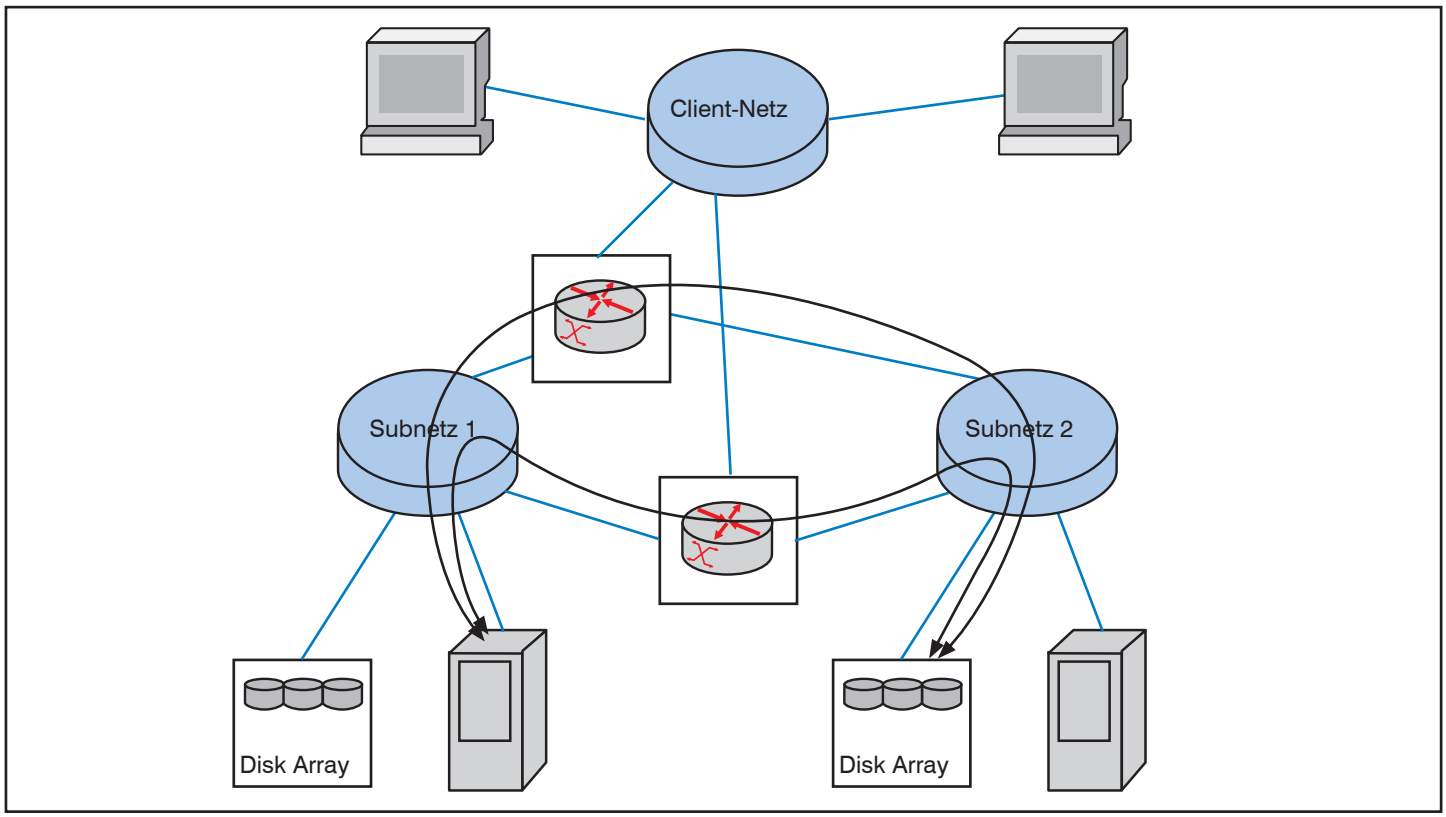


Abbildung 4: Alternative Wege im RZ

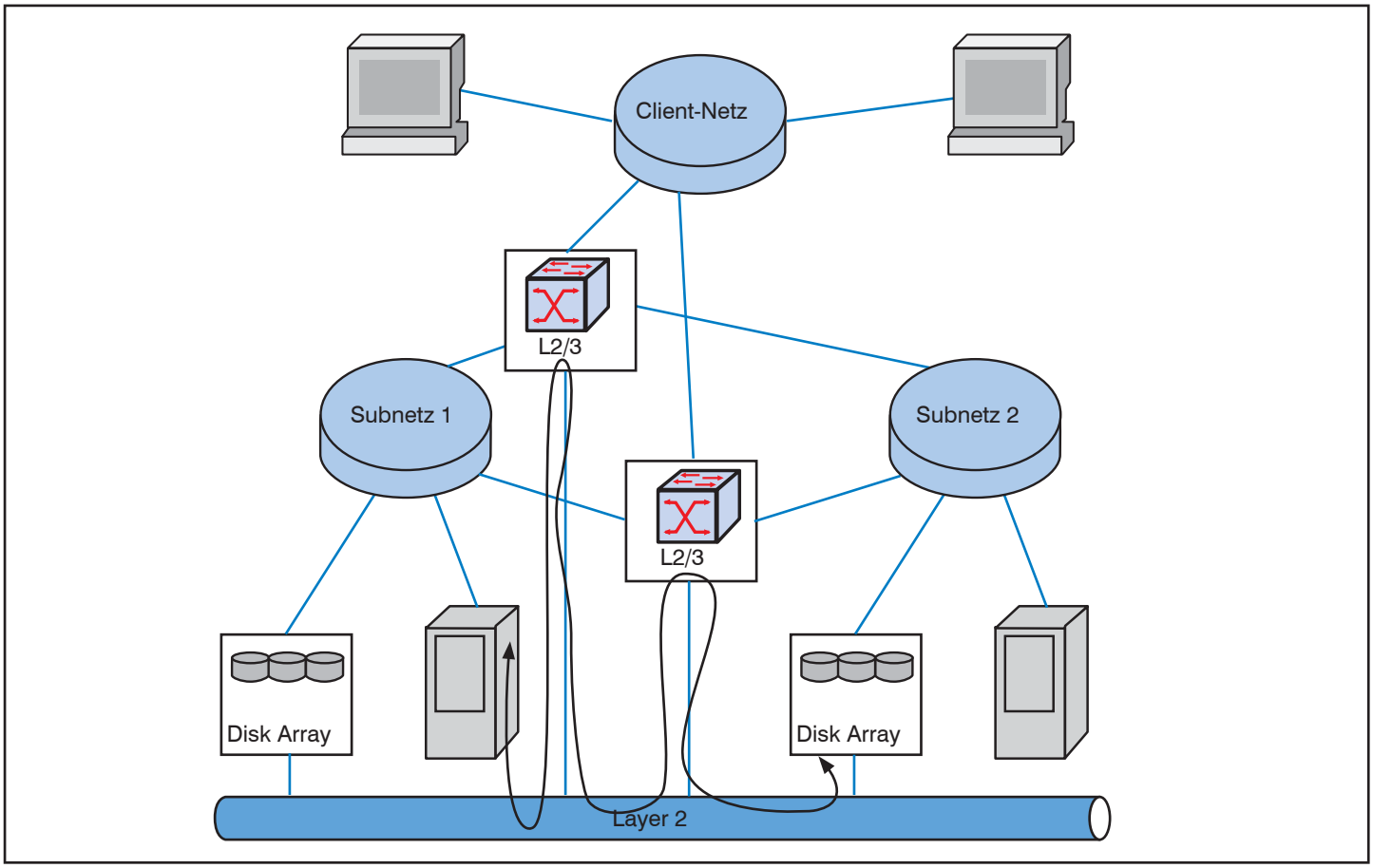


Abbildung 5: Optimale Wegewahl im RZ

der „Nähe“ des Servers, der zum Subnetz des NAS-Systems routet, in diesem Subnetz aber erkennt, dass das NAS-System über die andere Layer-2/3-Komponente erreichbar ist. Wenn die beiden L2/3-Komponenten an unterschiedlichen Standorten aufgestellt sind, kommt es im Übertragungspfad nur zu einem standortübergreifenden Hop.

Die Voraussetzungen für eine solche Gesamtoptimierung sind wie folgt:

- Beide L2/3-Komponenten haben Interfaces in beiden IP-Subnetzen.
- Jeder L2/3-Switch ist aktiver Default Router in jedem der beiden IP-Subnetze, denn sonst müsste der erste Hop aus der Sicht des Servers, der vielleicht kein aktiver Default-Router im Serversubnetz ist, das Paket des Servers an den anderen L2/3-Switch weiterleiten.

Die erste Anforderung kann von jeder RZ-Netzstruktur erfüllt werden, die aus Layer-2-/3-Switches besteht. Mit diesen Switches ist es möglich, eine flächendeckende Layer-2-Versorgung des gesamten Rechenzentrums zu erreichen, zum Beispiel mittels Multi-Chassis Link Aggregation (MC-LAG), SPB oder TRILL. Ferner ist es mit solchen Switches möglich, jeden Switch mit einem IP Interface in jedem RZ-Subnetz zu versehen.

Die Erfüllung der zweiten Anforderung ist schon schwieriger. Standardmäßig kennt zum Beispiel das Virtual Router Redundancy Protocol (VRRP) zu jedem Zeitpunkt einen aktiven Default Router pro IP-Subnetz. Einige Hersteller haben Mechanismen in Ergänzung zur Standard-Default-Router-Virtualisierung implementiert, die dafür sorgen, dass zum Beispiel alle Mitglieder einer VRRP-Gruppe jedes an die VRRP-MAC-Adresse gerichtetes Paket einer Layer-3-Verarbeitung unterziehen. So routet jedes Mitglied ein zu routendes Paket weiter.

So ist es mit heutigen Mitteln möglich, das Routing im RZ zu optimieren.

Optimales Outboud Routing

Optimales Routing im RZ reicht nicht aus, wenn man an das Szenario in der Abbildung 6 denkt.

Wie aus der Abbildung 6 hervorgeht, kann der Server den Client über zwei Wege erreichen. Wenn sich der Server am RZ-Standort A und der Router am RZ-Standort B befindet, geht der Pfad vom RZ-Standort A zum RZ-Standort B und von dort zum Client. Das kann aber schon eine ungünstige Route sein, wenn Server und Client in derselben Region und der Standort B in einer entfernten Region liegen.

Dieselben Mechanismen wie für das RZ-interne Routing beschrieben können angewandt werden, um das Outbound Routing, also das Routing vom RZ zum Client, zu optimieren. Der Lösungsansatz geht aus der Abbildung 7 hervor.

Die Abbildung 7 zeigt, wie vom Server ausgehen der erste Hop das Paket direkt Richtung Client weiterleitet, ohne es zu einer anderen RZ-Routing-Instanz senden zu müssen. Wenn also jede Layer-2/3-Komponente im RZ erstes Interfaces in allen RZ-Subnetzen unterhält, zweitens dort auch aktiver Default Router ist und drittens zum Client-Netz die gleiche „Routing-Entfernung“ hat wie andere Layer-2/3-Instanzen im RZ. Die erste und zweite Bedingung haben wir schon für optimales Routing im RZ aufgestellt. Die dritte Bedingung kommt hinzu, damit das Paket vom ersten Layer-2/3-Switch aus den kürzesten Weg nach außen findet. Ist die dritte Bedingung nicht erfüllt, kann das Paket nämlich von dem einen zum anderen Layer-2/3-Switch im RZ weitergereicht werden. Angesichts der Verteilung dieser Komponenten und des Layer-2-RZ-Netzes auf verschiedene Standorte kann das bereits zum ungünstigen Routing führen.

Symmetrisches RZ-Netzdesign ist also wichtig, wenn es darauf ankommt, ungünstiges Outbound Routing zu vermeiden.

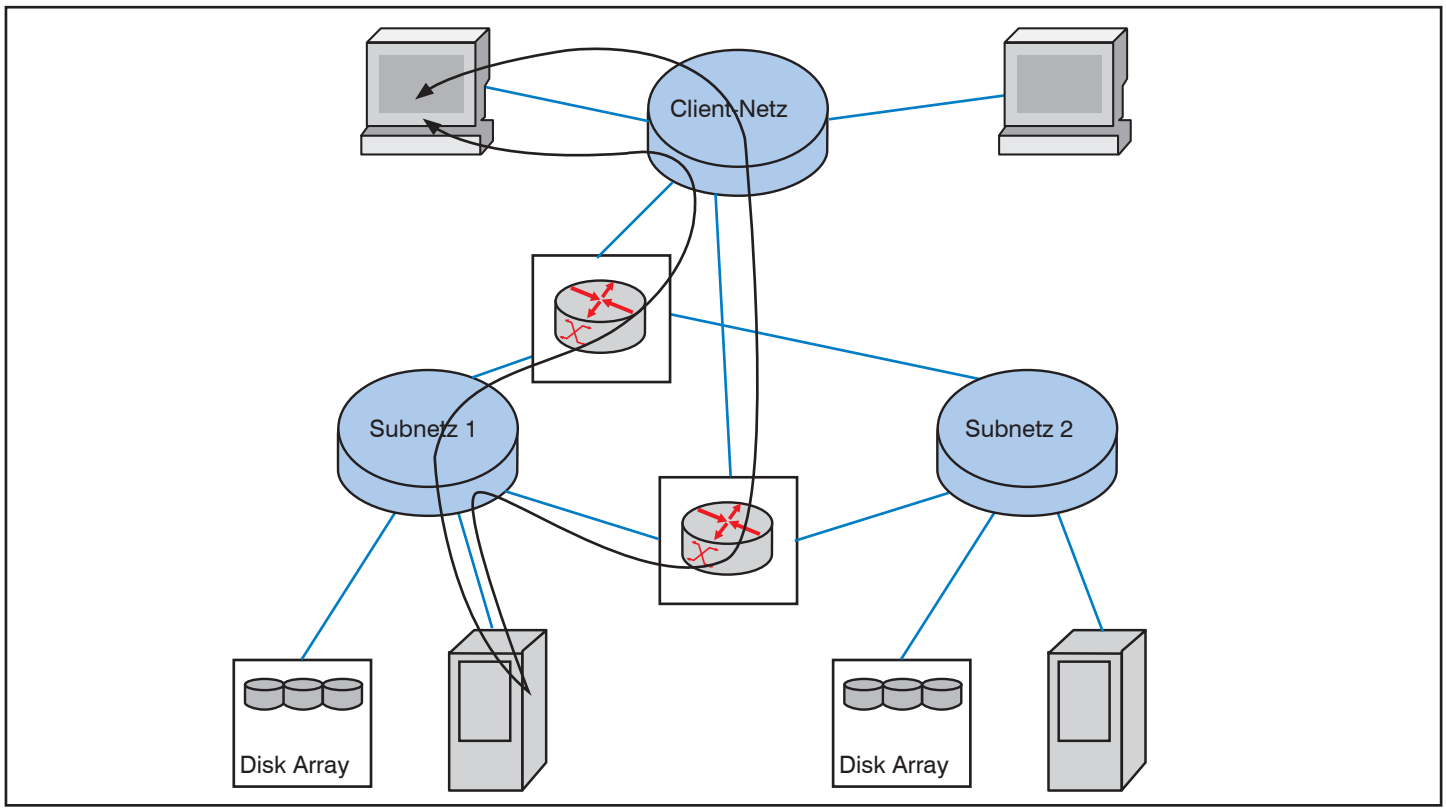


Abbildung 6: Alternative Pfade zwischen dem RZ und einem Client

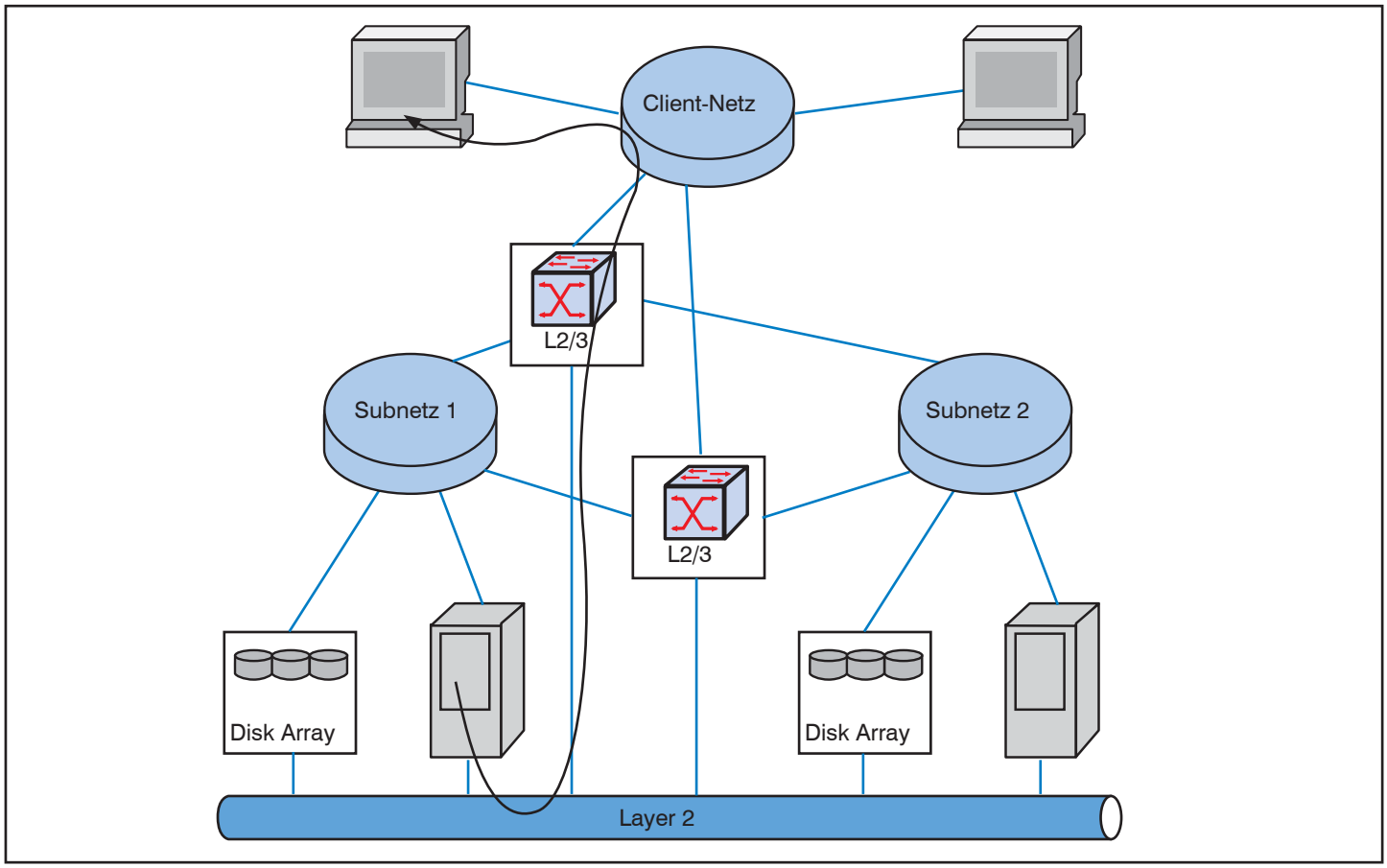


Abbildung 7: Optimales Outbound Routing

Mit denselben Mitteln wie auf RZ-internes Routing angewandt und zusätzlich mit einem symmetrischen Netzdesign kann also ungünstiges Outbound Routing vermieden werden.

Ungünstiges Inbound Routing

Abbildung 8 zeigt zwei alternative Wege vom Client zum Server.

Da alle L2/3-Switches im RZ-Netz Interfaces in jedem Serversubnetz haben, leitet der erste L2/3-Switch, der das Paket bekommt, dieses direkt über Layer 2 an den Server weiter. Der erste Layer-2/3-Switch, der das Paket bekommt, wird im Prinzip von dem ersten Routing Hop bestimmt, der das Client-Paket erhält. Beschränkt sich die Layer-2-Domäne auf das RZ, entscheidet der Router ausschließlich anhand von Layer-3-Merkmalen. Da jedoch alle L2/3-Switches im RZ die gleiche Distanz zum Client haben, kann es dazu kommen, dass aus RZ-Layer-2-Sicht die ungünstigere Route gewählt wird, nämlich vom Client zum RZ-Standort B und von dort zum RZ-Standort A.

Nun könnte man auf die Idee kommen, auch die Client-Subnetze in dieselbe Layer-2-Domäne aufzunehmen wie das RZ, um das Inbound Routing genauso zu gestalten wie das RZ-interne Routing („alle sprechen Layer 2 und Layer 3“). Das ist aber genau nur in Umgebungen möglich, in denen das ungünstige Routing toleriert werden kann, nämlich in Campusnetzen. Befindet sich der Client nicht auf demselben Gelände wie das RZ, sondern greifet über ein WAN oder über ein VPN oder schlicht und ergreifend über das Internet ohne VPN auf das RZ zu, kann man die Idee einer großen, im Internet-Fall weltweiten Layer-2-Wolke gleich wieder vergessen, es sei denn, man wolle das Internet neu erfinden.

Layer-2-Tunnel

Man könnte auf die Idee kommen, eine Art Layer-2-Tunnel von jedem Client-Standort aus zum RZ aufzubauen. Dann besitzt die Netzkomponente in der Nähe des Clients, welche die Wegewahlentscheidung treffen soll, nicht nur Layer-3-, sondern auch Layer-2-Intelligenz. Mit dieser Layer-2-Intelligenz wird die Wegewahlentscheidung so getroffen, dass das Paket den kürzesten Weg vom Client zum Server nimmt, wie aus der Abbildung 9 hervorgeht.

Layer-2-Tunnel haben aber einige Nachteile. Sie müssen zum Beispiel per definitionem alle Layer 2 Broadcasts und Pakete mit unbekannter MAC-Zieladresse über den Tunnel weiterleiten. Man hebt also mit Layer-2-Tunneln wichtige Vorteile einer Layer-3-Segmentierung auf. Ferner ist nicht sichergestellt, ob Tunnelenden zwischen allen Clients und dem großen Layer-3-Netz möglich sind. Das passt gar nicht zu solchen Trends wie Bring Your Own Device.

LISP

Ebenfalls auf eine Art Tunneling setzt das Location/ID Separation Protocol (LISP), dessen Funktionalität in der Abbildung 10 dargestellt ist.

LISP trennt die Location-Information von der ID der Endgeräte. LISP-fähige Router führen zusätzlich zu normalen Routing-Tabellen für Location-Informationen auch Tabellen mit IDs einzelner Endgeräte. So erfährt der in der Abbildung 10 dargestellte L2/3-Switch auf der Client-Seite von der LISP-Infrastruktur, dass der Server über den linken LISP-Tunnel zu erreichen ist und nicht über den rechten.

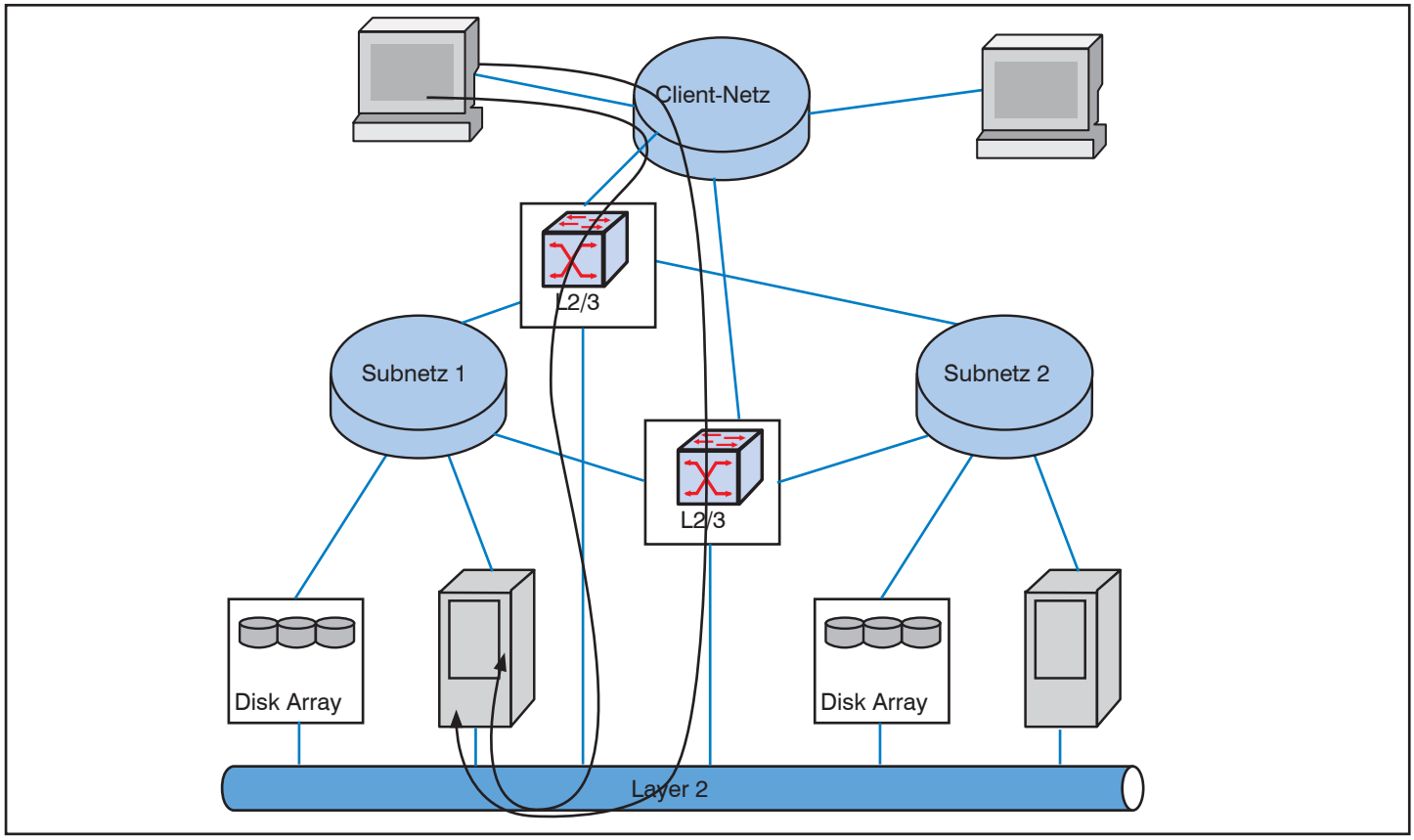


Abbildung 8: Alternative Wege zum RZ

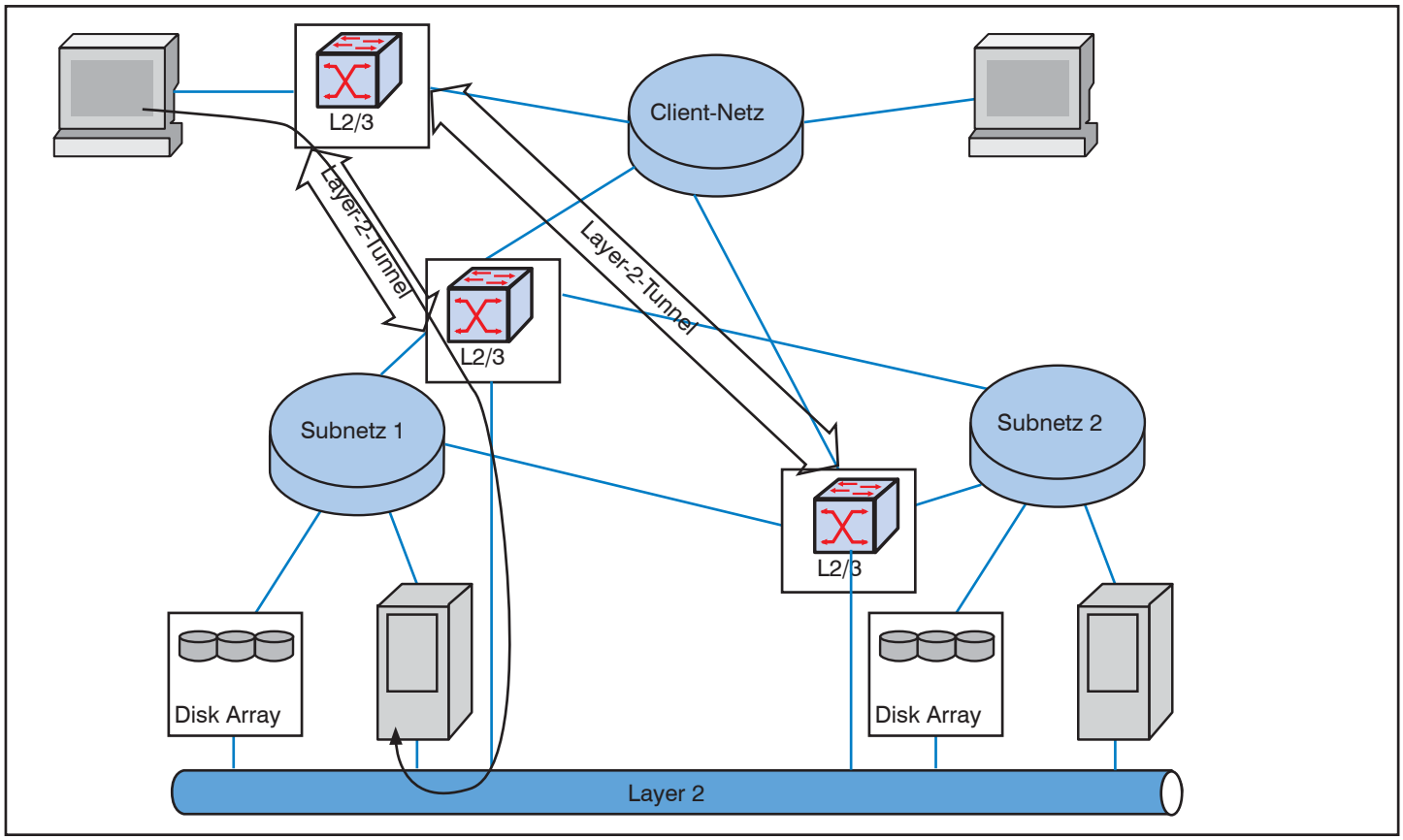


Abbildung 9: Layer-2-Tunnel

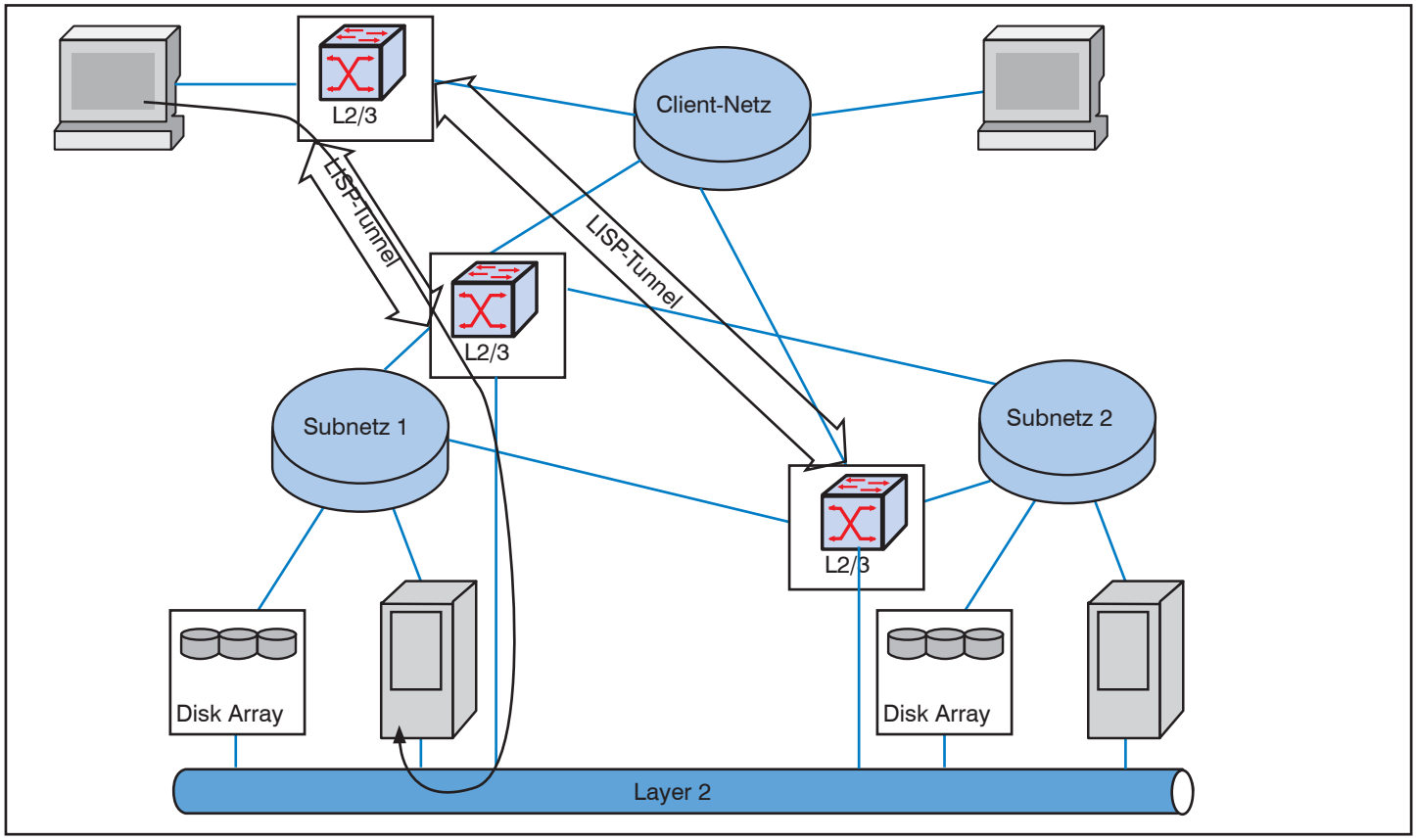


Abbildung 10: LISP

LISP wird jedoch Stand heute von den meisten Herstellern nicht unterstützt, und es fehlen die Langzeiterfahrungen mit der Stabilität und der Skalierbarkeit dieses Protokolls.

Fazit

In diesem Beitrag wurde begründet, warum das Routing im, vom und zum RZ weiterhin notwendig ist. Wir zeigten, wie das Routing im RZ und vom RZ zu Clients mit heutigen Mitteln optimiert werden kann.

Das Routing zum RZ bleibt jedoch ein Problem, wenn sich Layer-2-Strukturen über RZ-Standorten erstrecken, welche auf große Regionen oder gar die ganze Welt verteilt sind.

Report Neuauflage

Professionelle Datenkommunikation

Im August 2012 hat ComConsult Research das umfassende Grundlagenwerk von Dr. Kauffels „Professionelle Datenkommunikation“ neu aufgelegt.

Die fulminante Entwicklung der Daten- und Rechnernetze stellt den Einsteiger vor allem zunächst vor ein massives Orientierungsproblem. Verschiedene Elemente kennt er aus seinem beruflichen oder privaten Umfeld, aber wie sie alle zusammenhängen, welche Komponenten, Systeme und Verfahren es gibt, bleibt ihm zunächst verborgen. Grade das Erkennen der Zusammenhänge und der den Konstruktionen zugrunde liegenden Systematik ist, wie in vielen anderen Bereichen auch, der erste und wichtigste Schritt vom interessierten Laien zum standfesten Profi. Der Report „Professionelle Datenkommunikation“ ist ein fundierter und bewährter Begleiter bei diesem Schritt.

Auch wenn sie noch so unterschiedlich aussehen und viele verschiedene Anwendungsbereiche haben, sind alle Netze nach der gleichen Grundarchitektur, dem ISO-OSI-Referenzmodell organisiert. Nach einer kurzen Einführung in generelle Arten und Aufgaben von Daten- und Rechnernetzen wird diese allen Netzen gemeinsame generelle Systemarchitektur verständlich erklärt und dient dann auch als Grundsystematik für alles Weitere.

Physikalische Datenübertragung und Übertragungsmedien wie Kabel, Glasfasern und Luft sind die Grundlage eines jeden Netzes. Lokale Netze, Wide Area Netze WANs und Zugangstechniken, optische Netze und drahtlose Nachrichtenübertragung verwenden heute jeweils andere Kombinationen und Technologien auf dieser Ebene.

Die Ethernet-Technologie hat sich über die letzten Jahrzehnte als Welt-Standard für die Datenübertragung etabliert und bildet mit ihren verschiedenen Ausprägungen vom einfachen Heimnetz bis zu höchst leistungsfähigen Varianten für den Einsatz in Rechenzentren und auf WAN-Strecken sozusagen eine gemeinsame Basis für die unterschiedlichen Übertragungsalternativen. Deshalb wird sie natürlich ausführlich vorgestellt.

Um komplexere Übertragungswege implementieren zu können, müssen Netze zusammen geschaltet werden. Das geschieht mit den Techniken des Internetworking, zu denen auch z.B. Verfahren gehören, die Wege in noch so verzweigten Netzen finden. Die Schnittstelle zu den Anwendungen wird meist durch die so genannte TCP/IP-Protokollfamilie realisiert. Sie wurde ursprünglich im Rahmen der Entwicklung des Internets entworfen und hat sich letztlich auch durch den Erfolg des Internets auf alle anderen Bereiche ausgedehnt.

Weitere Kapitel befassen sich mit den anwendungsorientierten Internet-Protokollen, die beginnend mit HTTP im Laufe der Zeit ein Universum kooperierender Web-Anwendungen aufgespannt haben, mit dem wir heute leben. Ganz besonders wichtig sind hier natürlich Fragen von Datenschutz, Datensicherheit und Transaktionssicherheit in verkabelten und wireless-Netzen. Sie werden ausführlich behandelt.

Intranets, Unified Communications und Kollaborationstechniken sind heute in vielen Unternehmen eine wichtige Basis für die Produktivität. Netzwerk-, Service- und Anwendungs-Management sind wesentliche Hilfsmittel für einen möglichst störungsfreien Betrieb. In abschließenden Kapiteln wird in diesem Report jeweils ein Überblick über die wichtigsten Elemente und Verfahren dieser Technologien gegeben.

Der Autor dieses Reports hat in den letzten 30 Jahren Tausende Teilnehmer durch einführende Kurse zu Netzwerktechnologien geführt und eine Reihe sehr erfolgreicher Bücher dazu geschrieben. Jeder Leser des Reports profitiert von dieser umfangreichen Erfahrung.

Fax-Antwort an ComConsult 02408/955-399

Bestellung

Professionelle Datenkommunikation

☐ Ich bestelle den Report
Professionelle Datenkommunikation
zum Preis von € 398,-- netto

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

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

Standpunkt Sicherheit

Virtualisierung ohne Grenzen auch bei hohem Schutzbedarf?

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

In modernen IT-Infrastrukturen geht nichts mehr ohne Virtualisierung von Netzen, Servern, Clients und Anwendungen. Dabei wird immer häufiger eine maximale Konsolidierung angestrebt, was in der Praxis letztendlich bedeuten würde, dass Systeme unterschiedlichsten Sicherheitsniveaus auf einer gemeinsamen Infrastruktur betrieben werden. Dies könnten beispielsweise VMs einer Internet DMZ und Datenbanken für hochkritische Unternehmensdaten sein, die zusammen auf einer Server-Farm laufen („Data Center in a Box"). Das andere Extrem sind Lösungen für BYOD, wo durch verschlüsselte Sandboxes sichere Laufzeitumgebungen für Unternehmens-Apps auf privaten Endgeräten geschaffen werden sollen. Egal um welche Technik und Anwendungsform es sich handelt, letztendlich geht es immer um die Realisierung einer möglichst wasserdichten logischen Trennung von Systemen auf einer gemeinsamen Hardwarebasis.

Dieses Thema hat der Informationssicherheit schon immer massive Sorgen bereitet, denn die Sicherheit einer logischen Trennung steht und fällt nun einmal mit Qualität der Sandbox (oder wie immer der Trennungsmechanismus bezeichnet wird). Der GAU ist dabei ein z.B. durch einen Implementierungsfehler ermöglichter Ausbruch aus der Sandbox in Verbindung mit schadenstiftenden Zugriffen.

Typische Formulierungen in Sicherheitsrichtlinien bzw. -konzepten versuchen daher der ungezügelten Virtualisierung und Sandbox-Nutzung Grenzen zu setzen: „Komponenten mit erheblich unterschiedlichem Sicherheitsniveau müssen auf getrennten Systemen realisiert werden." Nur wird es immer schwerer hier auch eine physikalische Trennung durchzusetzen. Notgedrungen wird die Informationssicherheit weich und lässt unter gewissen Rahmenbedingungen Virtualisierung ohne Grenzen zu.

Ein passendes Beispiel findet sich in den BSI IT-Grundschutz-Katalogen im Baustein

B 3.304 Virtualisierung in Maßnahme M 5.153 „Planung des Netzes für virtuelle Infrastrukturen". Hier heißt es:

„Wurden vor der Virtualisierung Netze aufgrund unterschiedlichen Schutzbedarfs physikalisch getrennt, müssen diese Netze auch in virtuellen Umgebungen voneinander isoliert werden. Es ist dann zu prüfen, ob die Mechanismen zur Netztrennung, sowie der Kapselung und Isolation der virtuellen IT-Systeme in der eingesetzten Virtualisierungslösung ausreichen, ***um virtuelle IT-Systeme mit hohem Schutzbedarf gemeinsam mit solchen niedrigen Schutzbedarfs auf einem Virtualisierungsserver betreiben zu können."***

Die spannende Frage ist nun, wie eine solche Prüfung aussehen kann. Die eben zitierte Maßnahme sagt hierzu:

„Diese Prüfung kann z. B. darin bestehen, dass der Hersteller der betreffenden Virtualisierungslösung die genannten Mechanismen für diesen Einsatzzweck (Trennung von Maschinen unterschiedlichen Schutzbedarfs) als geeignet bezeichnet und dies durch eine ***entsprechende Zertifizierung*** *nachweist."*

Wenn es ein allgemein anerkanntes Bewertungs- und Prüfschema gäbe, das eine Virtualisierungs- oder Sandboxing-Lösung hinsichtlich eines angestrebten Sicherheitsniveaus einordnen kann, das spezifische Sicherheitsanforderungen insbesondere an das Sandboxing stellt und eine Auditierung nach allen Regeln der Kunst inklusive Zertifizierung ermöglichen würde, wären wir einen Schritt weiter.

Nun gibt es ja seit geraumer Zeit die Zertifizierung nach Common Criteria (CC) und diverse IT-Systeme sind auf Basis verschiedener Schutzprofile (Protection Profiles) für unterschiedliche Vertrauenswürdigkeitsstufen (Evaluation Assurance Level, EAL) zertifiziert.

Beispielsweise hat VMware vSphere 5.0 seit Mai 2012 ein CC-Zertifikat mit EAL4+, was für IT-Komponenten eine durchaus hohe Stufe darstellt. Nur wurde als Prüfbasis das Protection Profile für Betriebssysteme in einer Netzwerkumgebung zu Grunde gelegt. Nun ja, die betrachtete Virtualisierungsplattform hat eine ganze Menge Ähnlichkeiten zu einem Betriebssystem, nur beinhaltet das angewendete Protection Profile beispielsweise keine Anforderungen hinsichtlich der Sicherheit der Kapselung und Isolation der virtuellen IT-Systeme. In der Spezifikation für die Prüfung von vSphere 5.0 wurden daher zusätzliche Anforderungen aufgenommen und im Rahmen der Zertifizierung getestet. Da es noch kein Protection Profile gibt, das spezifisch für Virtualisierungslösungen ist, gab es auch keine Alternative.

Nur was bedeutet dann ein solches Zertifikat? Dürften wir jetzt VMs mit unterschiedlichstem Sicherheitsniveau (vielleicht sogar interne VMs und Internet-DMZ-VMs, die permanent Angriffsversuchen ausgesetzt sind) auf einer Hardware betreiben? Solange keine strengen, dediziert für Virtualisierungslösungen entwickelten Schutzprofile vorliegen, ist die Antwort ein klares Nein.

Trotzdem ist dies besser als nichts und die Forderung nach einem CC-Zertifikat (möglichst natürlich EAL4+) bleibt auch bei Verwendung des Protection Profile für Betriebssysteme ein essentieller Bestandteil des Anforderungskatalogs für eine Ausschreibung. Nebenbei bemerkt: Wäre auch Java zertifiziert gewesen, hätte es vielleicht den GAU vom August dieses Jahres nicht gegeben, als dank einer Schwachstelle in Java ein effektiver Ausbruch aus der Sandbox demonstriert werden konnte[1].

Es bleibt daher bis auf weiteres, dass bei erheblich unterschiedlichem Sicherheitsniveau (was im Einzelfall individuell festzulegen ist) eine physikalische Trennung notwendig ist, und die Informationssicherheit sollte hier der Forderung nach Virtualisierung ohne Grenzen Widerstand leisten.

[1]Siehe z.B. http://www.heise.de/security/artikel/Java-0-Day-unter-der-Lupe-1676764.html

Neue Sonderveranstaltung

Sonderveranstaltung Wireless Networking

Die ComConsult Akademie veranstaltet vom 29.11. - 30.11.12 Sonderveranstaltung „Wireless Networking“ in Köln.

Die Sonderveranstaltung Wireless Networking greift die aktuellsten Entwicklungen im Bereich der drahtlosen Kommunikationstechnik auf. Sie ist die zentrale Veranstaltung des Jahres 2012 zur drahtlosen Kommunikation. Sie ist für jeden Entscheider, IT-Architekten, Planer und Betreiber in diesem Bereich ein absolutes Muss. Hier trifft sich die Branche.

Die Zukunft der Kommunikation mit Clients ist drahtlos, d.h. WLAN, UMTS/LTE und Co. werden das klassische Kabel für die Client-Anbindung zur Nischenlösung machen. Folgende Entwicklungen deuten darauf hin, dass wir dabei vor einem wesentlichen Umbruch stehen:

Geschäftskritische Anwendungen
- In Office, Logistik, Retail, Produktion und Automatisierungstechnik werden immer häufiger auch geschäftskritische Anwendungen drahtlos genutzt, was leistungsfähige, sichere und hoch verfügbareWireless-Infrastrukturen erzwingt.
- Die Erwartungshaltung des Anwenders ist dabei: Maximale Mobilität ohne spürbare Leistungseinbuße im Vergleich zur kabelbasierten Anbindung.

Dies erfordert zunächst Gigabit-Leistungen auf der Luftschnittstelle. Konsequenzen sind neue drahtlose Übertragungstechniken im WLAN, die sich mit IEEE 802.11ac und IEEE 802.11ad abzeichnen sowie entsprechende Verfahren für LTE.

Das Controller-basierte WLAN-Design muss der kommenden höheren Leistung bei der Funkübertragung gerecht werden. Hier werden wir verstärkt eine Integration von Controller-Design und Switching-Infrastruktur erleben. Neben proprietären Techniken sind insbesondere bereits erste Ansätze sichtbar ein Controller-basiertes WLAN-Design im Rahmen von Software Defined Networking (SDN), z.B. auf Basis von OpenFlow, zu realisieren.

Die Nutzung von WLAN für geschäftskritische Anwendungen bedingt in vielen Fällen auch eine angemessene Überwachung. Bei 2,4 GHz ist durch die Vielzahl unterschiedlicher sich gegenseitig beeinflussenden Übertragungstechniken insbesondere eine systemübergreifende Messtechnik sinnvoll. In diesem Zusammenhang muss auch eine Neuregulierung des 2,4-GHz-Bereichs beachtet werden, die sich mit einer Neuauflage von ETSI EN 300 328 im Juni 2012 materialisiert hat und die speziell Auswirkungen auf drahtlose Techniken in Automatisierungsbereichen hat.

Neue Endgeräte-Typen und Nutzungsformen der IT
- Die Nutzung mobiler Endgeräte wie Smartphones und Tablets in Unternehmen und Behörden steigt exponentiell. Der traditionelle PC hat immer mehr ausgedient. Insbesondere das App-Konzept in den Betriebssystemen für Smartphones und Tablets (primär iOS und Android) lässt die Grenzen zwischen einem lokalen WLAN-basierten Zugang und dem Zugang per Mobil-funk immer mehr verwischen.
- Innovation in der IT findet im Consumer-Bereich statt und damit drängen Consumer-Techniken automatisch verstärkt in die Enterprise-IT. Mit Bring Your Own Device (BYOD) materialisiert sich zusätzlich der Wunsch private Endgeräte im Unternehmensnetz für Zugriff und Verarbeitung von dienstlichen Daten einzusetzen. Daneben ist es immer häufiger notwendig auch für Fremdgeräte einen drahtlosen Zugang zur Infrastruktur (z.B. für Wartungszwecke) zu schaffen. Hierbei besteht im schlimmsten Fall keinerlei Einfluss mehr auf die Konfiguration eines Endgeräts.

Damit der Zugriff von unsicheren Endgeräten auf Unternehmensdaten auf eine sichere Weise erfolgen kann müssen spezifische Konzepte umgesetzt werden, die neben Mobile Device Management (MDM), Sandboxing und Container-Apps auch Virtualisierung und Server-based Computing umfassen.

Diese Entwicklungen haben unmittelbare Konsequenzen für drahtlose Übertragungstechniken, Kommunikationsprotokolle und Netzarchitekturen, die wir in einer zweitägigen Sonderveranstaltung erörtern wollen:

- Gigabit WLAN und andere neue WLAN-Standards
- Neuregulierung der WLAN-Frequenzen bei 2,4 GHz und bei 5 GHz
- IPv6 und WLAN
- Betrieb und Trouble Shooting von WLAN
- Cisco CleanAir-Technologie, was steckt dahinter?
- Neue Entwicklungen im Controller-basierten WLAN-Design
- WLAN in der Shop Floor IT
- Konkurrenz zu WLAN durch LTE
- Anbindung von Smart Phones und Tablets an die Infrastruktur

Fax-Antwort an ComConsult 02408/955-399

Anmeldung Wireless Networking

☐ Ich buche die Sonderveranstaltung
Wireless Networking

vom 29.11. - 30.11.12 in Köln
zum Preis von € 1.690,-- netto

☐ Bitte reservieren Sie mir ein Zimmer

vom _____ bis_____ 12

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

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

Zweitthema

Neue Protokolle im RZ: Funktionsumfang – Potential – Auswirkung auf die Infrastruktur

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

Fortsetzung von Seite 1

Dahinter steckt das Phänomen, dass einzelne Nutzer einer Web-Applikation kaum Last erzeugen und die Last nur als Funktion der Anzahl der Teilnehmer entsteht. Es entsteht also der Bedarf nach einer dynamisch wachsenden Infrastruktur in Abhängigkeit von der Teilnehmerzahl. Wenn also ein Unternehmen eine neue Web-Anwendung für Kunden oder Zulieferer im Internet anbieten will, dann entsteht automatische die Frage nach der Skalierung.

Der andere Megatrend ist die automatische Provisionierung von Anwendungsserver in einer virtuellen Infrastruktur. Heute werden Anwendungsserver in der Regel von Hand aufgesetzt und physischen Servern zugewiesen. Auch mögliche Wanderungen dieser virtuellen Server werden manuell konfiguriert. Damit werden über den Tag hinweg die Ressourcen in einer virtuellen Infrastruktur nicht optimal ausgenutzt. Ideal wäre eine vollautomatische Zuweisung und Pflege dieser Zuweisungen. Damit verbunden sind automatische Wanderungen von virtuellen Maschinen auch zwischen Standorten oder über Brandschutzbereiche hinweg. Heutige Lösungen dieser Art sind häufig zu komplex und auch zu teuer, sie werden häufig unter dem Schlagwort Private Cloud angeboten und umgesetzt, da die automatische Provisionierung ein zentrales Merkmal von Cloud-Lösungen ist. Aufgrund dieses hohen Preises kommen diese Lösungen bisher eher selten zum Einsatz. Aber es ist erkennbar, dass Hersteller wie VMware oder auch HP intensiv in dieser Richtung arbeiten. Und damit entsteht ebenfalls die Frage, in welchem Umfang virtuelle Layer-2-Verbindungen über Netzwerkgrenzen hinweg erforderlich sein werden, um dieses Konzept der automatischen Provisionierung wirklich rund zu machen.

Brandaktuell wird das Thema durch die Aktivitäten von VMware mit VXLAN und der großen Unterstützung, die dieses Thema seitens der Netzwerkhersteller erhält. Auch der Gegenentwurf NVGRE schafft vergleichbare Lösungen. Im Folgenden soll daher speziell untersucht werden, welches Potenzial diese Protokolle haben.

An dieser Stelle soll auch erwähnt werden, dass es weitere technische Ansätze zur Lösung dieses Problems gibt, die zum Teil auch deutlich weiter gehen. Das sind zum einen Software Defined Networks (SDN) und zum anderen Service-Architekturen unter Nutzung des Service Tags von Shortest Path Bridging. Wir werden in weiteren Artikeln auf diese Optionen eingehen und Lösungsstrategien natürlich auch auf dem Rechenzentrum Redesign-Forum der ComConsult Akademie Anfang November in Köln diskutieren.

Bevor wir uns an dieser Stelle aber Einsatzszenarien und Zukunftsperspektiven widmen, lassen Sie uns zunächst die technischen Grundlagen der beiden Protokolle VXLAN und NVGRE klären.

VXLAN – Die Grundlagen

VXLAN ist als sogenannter „Internet-Draft“ bei der IETF veröffentlicht. Das aktuelle Dokument (draft-mahalingam-dutt-dcops-vxlan-02 vom 22.8.2012) hat den Status „Experimental“, mit einer Verabschiedung als „Internet-Standard“ ist vorerst nicht zu rechnen, was aber erfahrungsgemäß keinen Einfluss darauf hat, in wie weit das Protokoll in neuen Produkten zum Einsatz kommt.

Autor ist Mallik Mahalingam, führender Software-Architekt bei VMware, weitere Autoren sind von Arista, Broadcom, Cisco, Citrix und Rad Hat.

Das Protokoll selbst kann als MAC-in-IP- oder genauer als MAC-in-UDP-Verfahren bezeichnet werden, das Frame-Format ist in Abbildung 1 dargestellt.

Der Original-Frame (ohne dessen ursprünglicher FCS) wird also nacheinander um vier Header erweitert:

- Der VXLAN-Header enthält im Wesentlichen einen 24 Bit großen Identifier (VNI = VXLAN Network Identifier). Damit

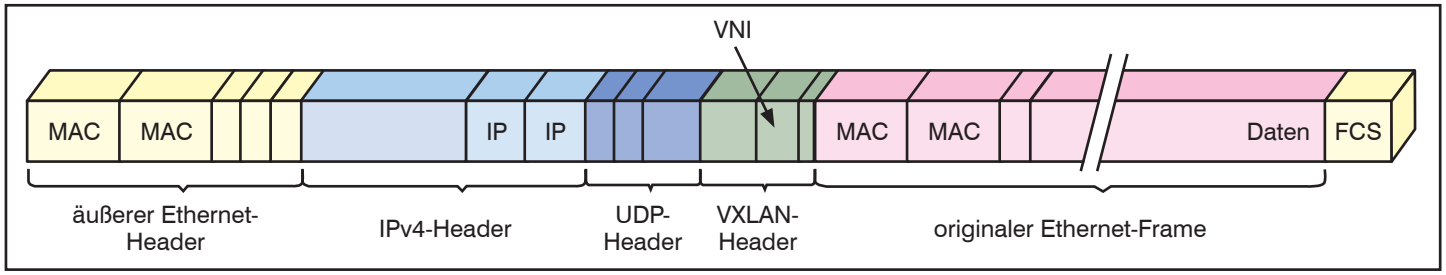


Abbildung 1: VXLAN Frame-Format

können mehr als 16 Millionen VXLAN-Segmente unterschieden und somit deutlich mehr als mit der nur 12 Bit großen 802.1Q-VLAN-ID. Wie bei 802.1Q können virtuelle Maschinen in verschiedenen VXLAN-Segmenten nicht miteinander kommunizieren.

- Die UDP- und IP-Header sorgen dafür, dass der eingekapselte Frame über Layer 3 transportiert werden kann. Die Zieladresse im IP-Header ist hierbei die IP-Adresse des Tunnelendpunktes, über den das eigentliche Zielsystem (MAC-Adresse im originalen Frame) erreicht werden kann.

- Und abschließend folgt ein passender äußerer MAC-Transport-Header, der sich vermutlich beim Durchgang durch das IP-Netz regelmäßig ändert.

Das Verfahren definiert also pro VNI je ein Layer-2-Overlay-Netz über ein Layer-3-Transportnetz und verbindet so alle Layer-2-Segmente, denen dieselbe VXLAN-ID zugewiesen wurde. Oder anders ausgedrückt: Layer-2-Netze werden so über Layer 3 hinweg aufgespannt.

Segmente mit unterschiedlicher VNI sind völlig voneinander getrennt und können nicht miteinander kommunizieren. Daher spielt es auch keine Rolle, wenn in solchen Segmenten gleiche VLANs oder gleiche MAC-Adressen verwenden werden.

Der Draft schränkt den Einsatzbereich von VXLAN explizit auf RZ-Netze mit virtuellen Servern ein („VXLAN addresses … data center network infrastructure in the presence of VMs in a multitenant environment“). Die Tunnelendpunkte (VTEP = VXLAN Tunnel End Point) werden dementsprechend auch innerhalb des Hypervisors der Virtualisierungs-Hosts positioniert. Gleichwohl merken die Autoren aber auch an, dass VTEPs auch in physischen Komponenten realisiert werden können („Note that it is possible that VTEPs could also be on a physical switch or physical sever and could be implemented in software and hardware.“).

Grundlage des Protokolls sind im Wesentlichen Zuordnungstabellen, in denen jeder VTEP einerseits die MAC-Adressen der lokalen Endsysteme (also im Wesentlichen die „seiner“ virtuellen Server) einer VNI und andererseits die MAC-Adressen der entfernten Zielsysteme der IP-Adresse des zugehörenden VTEPs zuordnet:

- Durch die Zuordnung zu einer VNI wird die jeweilige MAC-Schnittstelle einem bestimmten VXLAN-Segment, sprich Layer-2-Segment zugeordnet. Diese Zuordnung geschieht initial via Management auf dem System, das die betreffende VM hostet. Diese Zuordnung ist vergleichbar mit der im vSwitch üblichen Zuordnung eines Endsystems zu einer VLAN-ID.

- Die Zuordnung zur IP-Adresse des zugehörenden VTEPs wird benötigt, um bei der Enkapsulierung eines Datenpakets die Ziel-IP-Adresse im äußeren IP-Header setzen zu können. Wie diese Zuordnung erfolgt lässt der Draft explizit offen, als ein mögliches Verfahren wird lediglich das sogenannte „data plane learning“ beschrieben. Hierbei lernt, wie bei normalen Switches auch, die Zielkomponente die Zuordnung des Absenders anhand der Adressen im empfangenen Paket.

Eine Besonderheit dieses „data plane learning“ ist, dass Broadcasts, Multicasts und Unicasts an unbekannte Zieladressen mittels IP-Multicasts weitergeleitet werden. Damit auch diese Kommunikation innerhalb des jeweiligen VXLAN-Segments bleibt, erhält jedes VXLAN-Segment eine eigene IP-Multicast-Adresse. Diese Zuordnung von IP-Multicast-Adresse zu VNI erfolgt laut Draft-Dokument auf Management-Ebene und wird über einen nicht näher spezifizierten „management channel“ an die verschiedene VXLAN-Endpunkte verteilt werden („This mapping is done at the management layer and provided to the individual VTEPs through a management channel.“). Die Endpunkte selbst propagieren dann ihre jeweilige Zugehörigkeit zu bestimmten Multicast-Gruppen (also welche VXLAN-Segmente von ihnen bedient werden) dann via IGMP an das Transportnetzwerk.

NVGRE – Die Grundlagen

NVGRE („Network Virtualization using GRE“) ist ein alternativer Vorschlag von Microsoft in Zusammenarbeit mit Arista, Intel, Dell, HP, Broadcom und Emulex. Das Dokument (aktueller Stand: draft-sridharan-virtualization-nvgre-01 vom

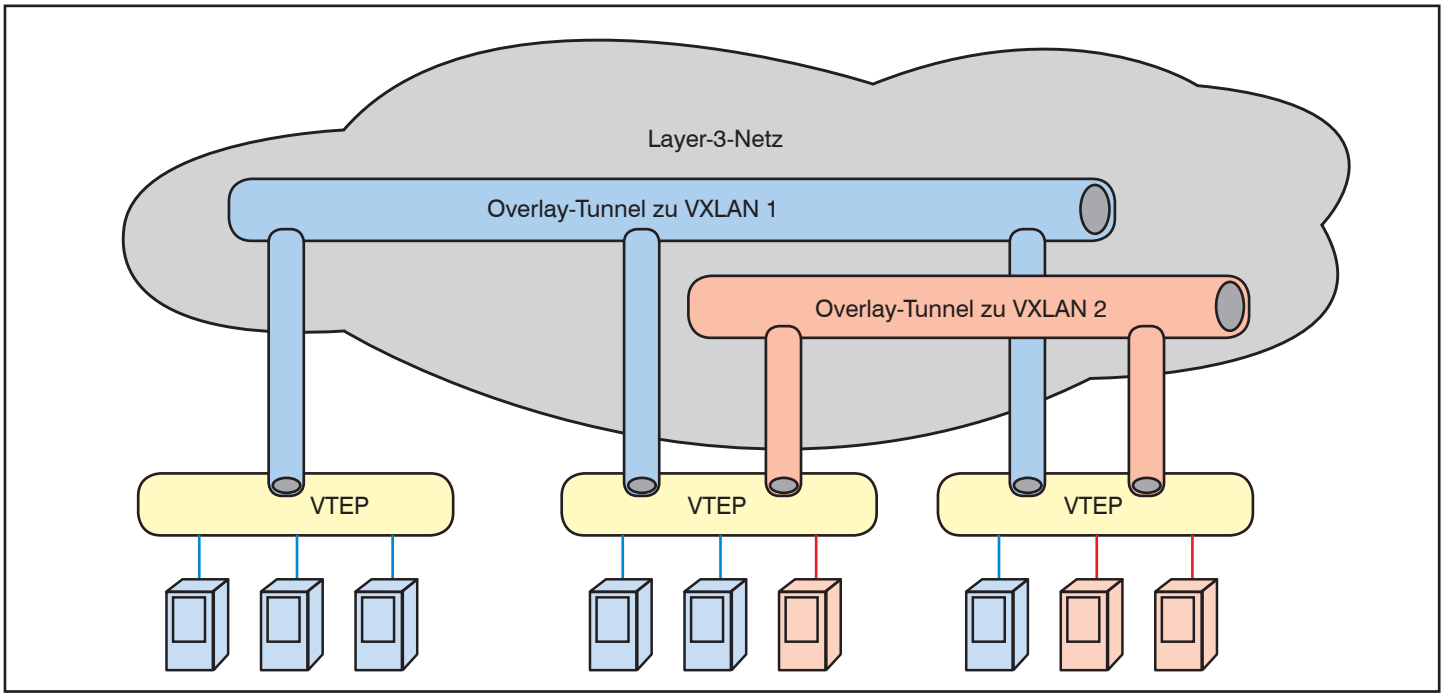


Abbildung 2: Overlay-Netze durch VXLAN

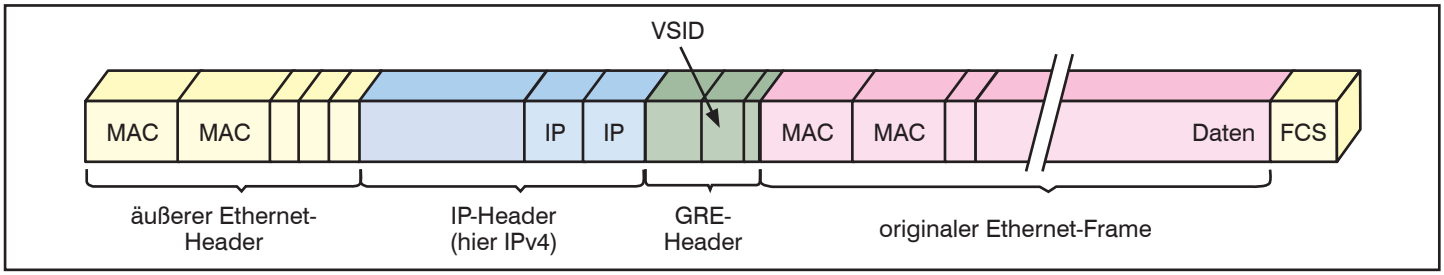


Abbildung 3: NVGRE Frame-Format

9.7.2012) ist ebenfalls als „Internet-Draft“ bei der IETF veröffentlicht.

Das Protokoll hat überwiegend große Ähnlichkeiten mit VXLAN und unterscheidet sich nur in wenigen Details (Frame-Format siehe Abbildung 3):

- NVGRE ist ebenfalls ein MAC-in-IP-Tunnelprotokoll. Statt auf die Kombination UDP mit einem neu erfundenen VXLAN-Header setzt NVGRE jedoch auf GRE („Generic Routing Encapsulation“), einem älteren, generischen Tunnelprotokoll, spezifiziert im RFC 2784.

- NVGRE nutzt genau wie VXLAN ein 24 Bit langes Feld (die Bezeichnung lautet hier VSID – Virtual Subnet ID) zur Unterscheidung von knapp 17 Millionen verschiedener Layer-2-Segmente (NVGRE spricht hierbei von virtuellen Subnetzen).

- Wie bei VXLAN können Segmente mit unterschiedlichen VSIDs standardmäßig nicht miteinander kommunizieren. Allerdings sieht die NVGRE-Spezifikation explizit die Möglichkeit vor, dass optional auch Tunnelendpunkte zwischen virtuellen Subnetzen routen können.

- Zusätzlich gibt es bei NVGRE eine 8 Bit lange FlowID, mittels der innerhalb eines virtuellen Subnetzes unterschiedliche Flows (Datenströme) definiert werden können, die dann im Transportnetz gegebenenfalls über unterschiedliche Wege geleitet werden, um so eine gleichmäßigere Auslastung des Transportnetzes zu erreichen.

  VXLAN sieht einen vergleichbaren Mechanismus vor, jedoch soll bei VXLAN der UDP-Quellport hierfür genutzt werden.

- Wie bei VXLAN werden subnetzinterne Multicasts und Broadcasts über IP-Multicasts im Transportnetz verteilt. Hierzu wird ebenfalls wie bei VXLAN jedem virtuellen Subnetz eine dedizierte IP-Multicast-Adresse administrativ zugewiesen.

- Wie bei VXLAN benötigen die Tunnelendpunkte eine Zuordnungstabelle, in der festgelegt ist, welche lokale MAC-Adresse welcher VSID zugeordnet ist und über welche IP-Adressen entfernte MAC-Adressen erreicht werden können. Genau wie die VXLAN-Spezifikation überlässt es auch das NVGRE-Dokument der konkreten Implementation, woher diese Zuordnungen kommen: über eine Management-Schnittstelle, über einen Kommunikationskanal zwischen den Tunnelendpunkten oder über simples Lernen, wie es oben beschrieben wurde.

- Anders als VXLAN lässt NVGRE explizit IPv6 als Transportprotokoll zu!

Wobei an dieser Stelle anzumerken ist, dass es nicht einzusehen ist, warum VXLAN nicht über IPv6 transportiert werden könnte. Der Protokollentwurf ist genauso wie der von NVGRE völlig unabhängig von der Version des IP-Protokolls.

Vergleicht man die beiden Protokollentwürfe, stellt man schnell fest, dass der NVGRE-Entwurf in den Details vollständiger und ausgereifter ist. Im Wesentlichen unterscheiden sich die beiden Entwürfe aber nur in einem Punkt: VXLAN wird über UDP und NVGRE über GRE transportiert. Puristen werden an dieser Stelle einwenden, dass UDP wesentlich weiter verbreitet ist als GRE, andererseits kann man GRE auch nicht gerade als exotisches Protokoll bezeichnen. Wichtig ist dieser Unterschied sowieso nur für ein mögliches Equal-Cost-Multipathing im Transportnetz: Sollen die Pakete verschiedener Subnetze über unterschiedliche Wege geführt werden (um beispielsweise das Transportnetz besser auszulasten), so müssen Switches und Router den GRE-Header erkennen können. Bei VXLAN wird hierfür in der Regel der UDP-Header genügen, wenn nämlich die „Flows“ über den UDP-Quellport unterschieden werden.

Für unsere weiteren Betrachtungen spielt das aber keine Rolle. Konzeptionell, bezüglich ihrer Leistungsfähigkeiten und ih-

rer Auswirkungen auf die RZ-Infrastruktur sind die beiden Protokolle als gleich zu bewerten.

Mancher Leser wird sich jetzt fragen, warum überhaupt neue Tunnelprotokolle entwickelt werden mussten. Die Aufgabenstellung, Layer-2-Bereiche transparent miteinander zu verbinden, ist schließlich nicht gerade neu.

Zielvorgaben

Nun, in der Einleitung des VXLAN-Dokuments werden vier wesentliche Zielvorgaben genannt, die mit dem Protokoll adressiert werden:

1. Nutzung der durch Spanning Tree geblockten Verbindungen,
2. Nutzung von deutlich mehr als 4.000 Subnetzen pro physischer Infrastruktur,
3. Aufbau mandantenfähiger Netze auf einer gemeinsamen physischen Infrastruktur,
4. Reduzierung der Adresstabellen in den ToR-Switches

und auch das NVGRE-Dokument zählt praktisch dieselben Probleme auf.

Lassen Sie uns diese vier Punkte im Folgenden kurz einzeln begutachten:

Nutzung der durch Spanning Tree geblockten Verbindungen:

Die Anforderung ist nicht neu, bereits verabschiedete Standards wie TRILL oder Shortest Path Bridging nach 802.1Qaq lösen die Spanning-Tree-Verfahren im Netzwerk ab. VXLAN und NVGRE sind aber Layer-3-Protokolle! Wie soll damit ein Spanning Tree ersetzt werden?

Nun, folgt man der Argumentation der Autoren, erreicht man dies dadurch, dass man durch Einsatz des jeweiligen Tunnelprotokolls von Layer 2 auf Layer 3 ausweicht und so dort die bekannten Lastverteilungsverfahren auf Layer 3 nutzt. Das klingt zwar ganz nett, hat aber einen Haken: Denn natürlich greifen Layer-3-Verfahren nur auf Layer 3, also bei subnetzübergreifendem Verkehr! Befinden sich aber beispielsweise beide Tunnelendpunkte im selben Subnetz – was ja per Definition des Protokolls zunächst nicht ausgeschlossen ist –, dann erfolgt der Transport gemäß Layer-2-Regeln und je nach Umgebung greift dann eben doch der Spanning Tree. Dasselbe gilt, wenn zwischen zwei Tunnelendpunkten ein Layer-2-Bereich durchquert werden muss: Kein Layer-3-Verfahren kann einen Link aktivieren, der vom Spanning Tree blockiert wird!

VXLAN und NVGRE lösen also <u>nicht</u> das Spanning-Tree-Problem und bringen auch keine „Multipathing"-Funktionalität oder ähnliches auf Layer 2!

Nimmt man diese erste Zielvorgabe trotzdem ernst, wird klar welches Netzwerkdesign den Autoren vorschwebt: Möglichst viele, kleine IP-Subnetze auf der Seite des Transportnetzes. Ein verbreitetes Design ist beispielsweise: Jedem Server-Rack wird jeweils ein dediziertes IP-Subnetz zugeordnet, so dass jeder Rack-übergreifende Datenverkehr geroutet werden muss und so die bekannten Layer-3-Verfahren zur Wegefindung und Lastverteilung greifen.

Zu beachten ist bei solchen Designs jedenfalls, dass, wie oben geschrieben, das Transportnetz IP-Multicasts unterstützt. Und viele Subnetze bedeuten viele IP-Multicast-Adressen. Neben IGMP ist daher zumindest in großen Netzen die Unterstützung eines Multicast-Routing-Protokolls wie PIM sicherlich von Vorteil.

Nutzung von deutlich mehr als 4.000 Subnetzen pro physischer Infrastruktur:

Die Zahl 4.000 kommt natürlich von der Anzahl möglicher VLANs nach IEEE-Standard 802.1Q. Der dort definierte VLAN-Identifier ist 12 Bit lang und erlaubt damit maximal 4.096 unterschiedliche IDs, 4.094 können als VLAN-ID vergeben werden. Der VXLAN-Identifier und der NVGRE-Identifier sind dagegen mit 24 Bit doppelt so lang und ermöglichen so mehr als 16 Millionen Subnetze.

Diese Vorgabe kann man also schnell abhaken: 16 Millionen sind mehr als 4094.

Zu beachten ist, dass diese Vergrößerung in heutigen Netzen nicht ganz problemfrei umsetzbar ist, da Sie in der Regel ja für jedes Subnetz auch eine Routing-Instanz benötigen – und mehrere zehn- oder hunderttausend VRF-Instanzen sind auch für große Router eine spannende Aufgabe.

Aufbau mandantenfähiger Netze auf einer gemeinsamen physischen Infrastruktur:

Durch die Einkapselung des originalen MAC-Frames werden sämtliche Layer-2- und Layer-3-Informationen des Kundennetzes im Transportnetz (was man in diesem Zusammenhang auch als Providernetz bezeichnen kann) versteckt. Es können also problemlos in unterschiedlichen virtuellen Subnetzen gleiche MAC-Adressen, gleiche VLAN-IDs und gleiche IP-Adressen verwendet werden, ohne dass es hierdurch zu Konflikten käme.

Spannend wird es allerdings in den Tunnelendpunkten. Beide Protokollentwürfe fokussieren sich zwar auf den Fall, dass der Tunnelendpunkt im Virtualisierungs-Host als Teil des Hypervisors integriert ist, es ist aber offensichtlich, dass man Tunnelendpunkte auch in anderen Netzwerkgeräten brauchen wird, um beispielsweise nicht virtualisierte Server, Speichersysteme etc. integrieren zu können oder ganz allgemein mit Systemen außerhalb der virtuellen Subnetze zu kommunizieren (siehe Abbildung 4).

Da hinter solchen Netzwerkgeräten natürlich ihrerseits wieder ganze Netze hängen können, muss an diesen Tunnelendpunkten eine Zuordnung der VXLAN- bzw. NVGRE-IDs zu lokal genutzten VLAN-IDs erfolgen. Je nach Infrastruktur (z.B. verschiedene Mandanten teilen sich einen Uplink-Port) kann das bedeuten, dass

- die VLAN-ID am Tunnelausgang nicht dieselbe ist wie am Tunneleingang,
- VLAN-IDs dynamisch erzeugt und zugeordnet werden müssen,
- die VLAN-IDs schlicht nicht ausreichen.

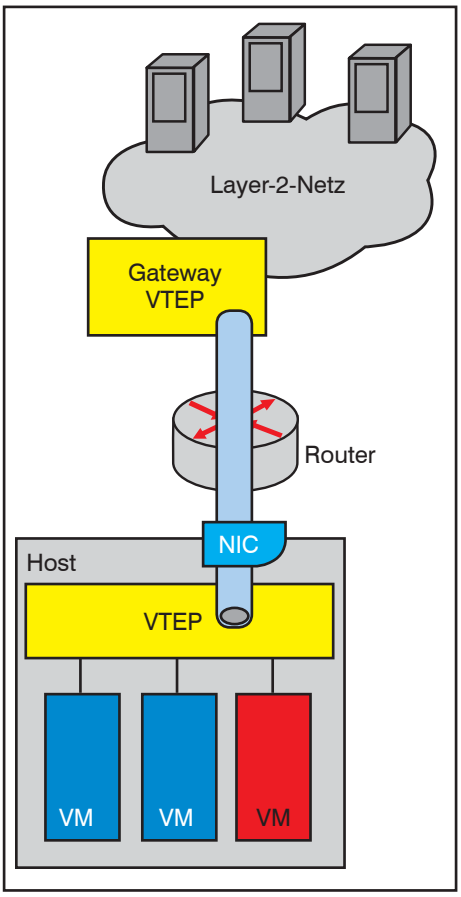


Abbildung 4: Anbindung externer Systeme durch VXLAN-Gateway

Beide Protokollentwürfe gehen übrigens davon, dass im inneren MAC-Paket keine VLAN-ID transportiert wird und dass daher die VLAN-IDs hinter den Tunnelendpunkten nur jeweils lokale Bedeutungen haben. Nichtsdestotrotz fehlt ganz offensichtlich ein Verfahren, um diese (lokalen) VLAN-IDs auszuwählen. TRILL und SPB sind da bedeutend konkreter.

Reduzierung der Adresstabellen in den ToR-Switches:

Dieser Punkt wird nur im VXLAN-Dokument angeführt und – na ja, er ist im Grunde ein ziemlicher plumper Versuch, Netzwerkdienste aus Hardware-Geräten heraus in softwarebasierende Lösungen zu diskutieren. Aber letztlich müssen die Zuordnungstabellen ja irgendwo verwaltet werden, und in der Regel werden Sie in Ihrem Rechenzentrum deutlich mehr Virtualisierungs-Hosts haben als ToR-Switches…

Bevor Sie jetzt aber anfangen sich Sorgen um den Tabellenplatz in Ihren ToR-Switches zu machen, klären Sie doch erst einmal die Fragen, wie groß die Kapazität dieser ToR-Switches tatsächlich ist und wie viele MAC-Adressen im schlimmsten Fall verwaltet werden müssen. Der VXLAN-Draft geht hier äußerst großzügig von Hunderten virtueller Maschinen pro Virtualisierungs-Host aus! Mir ist kein Rechenzentrum bekannt, in dem das auch nur annähernd der Realität entspricht.

Kommen wir jetzt zu der Frage, für welche RZ-Designs und welche Umgebungen die neuen Protokolle überhaupt geeignet sind.

Einsatzszenarien

Klar ist anhand dessen, was wir bis jetzt besprochen haben: Beide Protokolle erzeugen Overlay-Netze zur transparenten Verbindung nicht zusammenhängender Layer-2-Segmente. Das bedeutet **eine logische Aufteilung des RZ-Netzes in einen Transportbereich**, in dem die VXLAN- bzw. NVGRE-Tunnel aufgebaut werden, **und einen Bereich der verschiedenen Anwendungsnetze**, in dem die Endsysteme angebunden sind und miteinander kommunizieren. Je nach Sichtweise kann man diese beiden Bereiche auch **als Providernetz und als Kunden- bzw. Mandantennetze** bezeichnen!

Der VXLAN-Entwurf nennt als typisches Beispielszenario ein Rechenzentrum, das aus mehreren PoDs aufgebaut ist, jedem PoD-Container ist ein dediziertes IP-Subnetz zugewiesen, die PoD-übergreifende Kommunikation läuft also über Layer

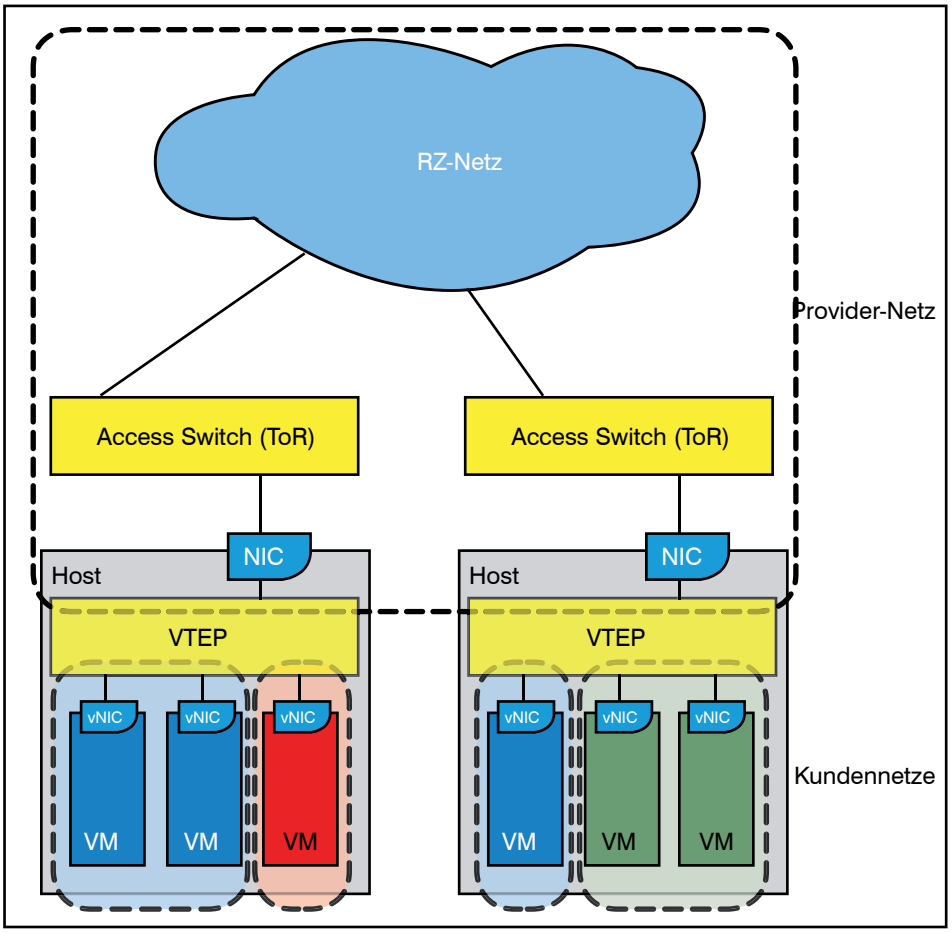


Abbildung 5: Aufteilung in Provider/Transportnetz und Kundennetze

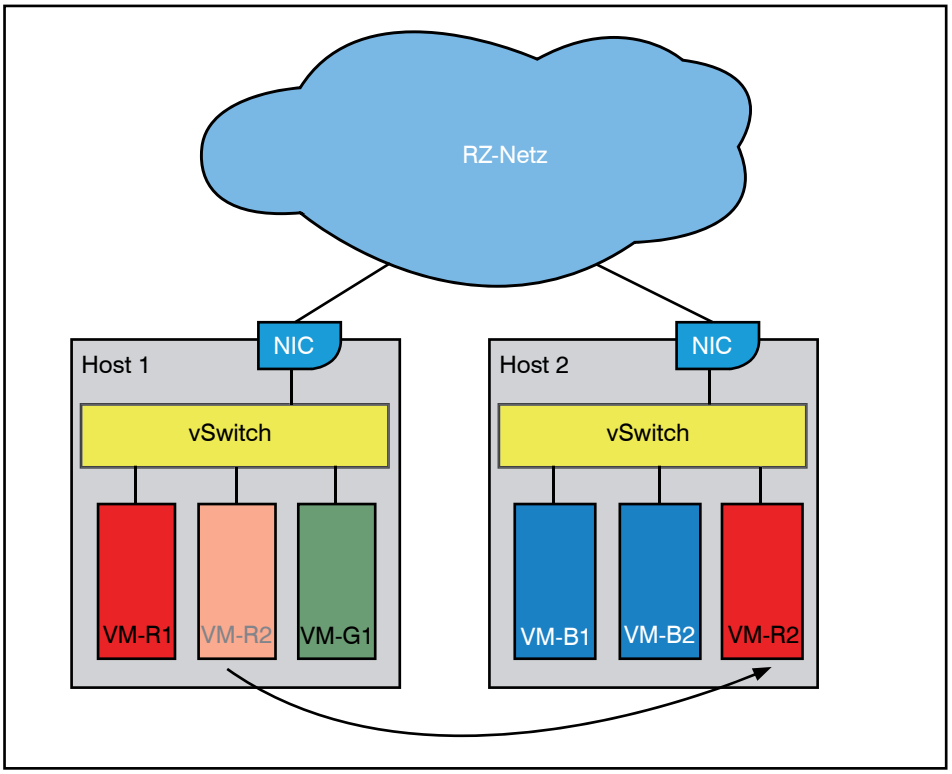


Abbildung 6: vMotion im RZ

3. Das Tunnelprotokoll kommt hier dann zum Einsatz, wenn beispielsweise einzelne Mandanten Ressourcen aus mehr als einem PoD nutzen. Sei es, weil die Ressourcen eines einzigen PoD für sie nicht ausreichen, oder weil die Ressourcen mehrerer PoDs nicht vernünftig ausgenutzt werden und brachliegen.

In der öffentlichen Wahrnehmung steht aber ein ganzer anderer Anwendungsfall im Vordergrund, nämlich vMotion, das transparente Verschieben virtueller Maschinen auf andere Hosts.

Die beiden Szenarien unterscheiden sich aber nicht unwesentlich!

Ich werde daher diesen Punkt im Folgenden etwas detaillierter diskutieren:

Ausgangspunkt (siehe Abbildung 6) ist die Kommunikation zweier virtueller Maschinen im gemeinsamen VLAN „rot“. Eine dieser VMs (VM-R2) wird auf einen anderen Host (Host 2) verschoben.

Welche Möglichkeiten gibt es jetzt die Kommunikation zwischen diesen beiden Maschinen aufrechtzuhalten?

Fall 1:
Die Uplink-Ports der beiden virtuellen Switches, denen die VMs auf ihren jeweiligen Hosts zugeordnet sind, sind über Layer-2-Komponenten miteinander verbunden:

a) Das VLAN „rot“ ist dem Uplink-Port des Ziel-Hosts bereits (statisch) zugeordnet (siehe Abbildung 7):

   Dann passiert im Wesentlichen gar nichts, der virtuelle Switch des Ziel-Hosts schickt lediglich ein ARP-Paket mit der MAC-Adresse „seiner“ neuen VM heraus, um das restliche Netzwerk über den neuen Standort der virtuellen Maschine zu informieren.

b) Das VLAN „rot“ ist dem Uplink-Port des Ziel-Hosts noch nicht zugeordnet:

   Dann brauchen Sie irgendeinen Mechanismus, der das VLAN „rot“ dorthin bringt. Standardkonform kommt hierfür in erster Linie das VLAN Registration Protokoll MVRP nach IEEE 802.1Q in Frage, es gibt aber natürlich auch eine Reihe herstellerproprietärer Lösungen.

   Im Ergebnis wird dasselbe herauskommen wie im Fall a), entscheidend ist aber, dass jetzt Ihr Netzwerk auf eine Topologie-Änderung – denn genau darum handelt es sich – reagieren muss:

   - Standardmäßig wird der (Rapid) Spanning Tree loslaufen und Ihnen die eine oder andere Verbindungsunterbrechung, wenn auch nur für wenige Sekunden, bescheren.
   - Oder Sie haben eine Shortest-Path-Bridging-Technologie für Ihr Layer-2-Netz wie beispielsweise TRILL oder SPB nach 802.1Qaq im Einsatz. Dann wird lediglich der kürzeste Weg zwischen den beiden Hosts neu berechnet, es gibt aber keine Unterbrechungen der anderen, bereits etablierten Kommunikationsverbindungen.

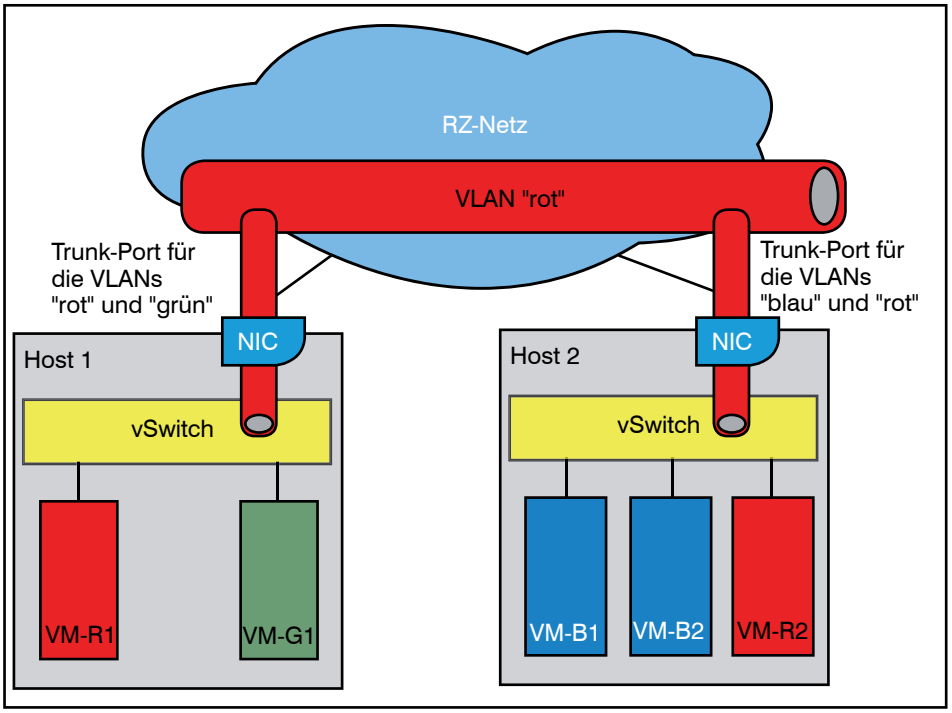


Abbildung 7: „Overlay“-Architektur auf der Basis von Standard-VLANs

Fall 2:
Die beiden Uplink-Ports befinden sich in unterschiedlichen Layer-2-Domänen und können nur über Layer 3 verbunden werden:

Dies ist genau das Szenario, in dem Sie zwingend eine MAC-über-IP-Tunnellösung brauchen, die Ihre beiden Layer-2-Fragmente miteinander verbindet!

Da außerdem im Allgemeinen ein einziger Punkt-zu-Punkt-Tunnel nicht ausreichen wird (es sei denn Sie verbinden genau zwei Standorte miteinander), brauchen Sie eine Lösung, die Mehrpunktverbindungen aufbauen kann – und das möglichst noch dynamisch.

Wann ist in diesen Fällen VXLAN bzw. NVGRE hilfreich?

In Fall 1 offensichtlich gar nicht!

Ist Ihr Netz klein genug, kommen Sie mit Standard-VLANs nach 802.1Q aus. Sie sollten dann lediglich ein Auge auf Ihre Spanning-Tree-Konfiguration werfen, damit keine unliebsamen Überraschungen erleben.

Wollen oder müssen Sie ganz ohne Spanning Tree auskommen, könnten Sie speziell in Szenario 1 b) natürlich auf die Idee kommen, eines der beiden IP-Tunnelprotokolle einzusetzen. Sie setzen dann im Grunde auf ein Design, das dem von Punkt 1 a) entspricht: Das notwendige VLAN, jetzt allerdings das des Transportnetzes, ist bereits im Vorfeld am Ziel-Host vorhanden. Der einzige Vorteil im Vergleich zu 1 a) ist, dass Sie mit den neuen Protokollen deutlich mehr Daten-VLANs unterstützen können.

Bei dem alles entscheidenden Punkt helfen Ihnen diese Protokolle aber nicht weiter: Sie haben ja jetzt unter Umständen einen ganz neuen Kommunikationspfad quer durch Ihr Netz und es wäre doch äußerst hilfreich, wenn dieser Pfad jetzt optimiert werden könnte. Die deutlich bessere Lösung ist daher in diesem Fall eine RZ-Infrastruktur, die auf MLAG oder TRILL oder vergleichbare Technologien aufsetzt.

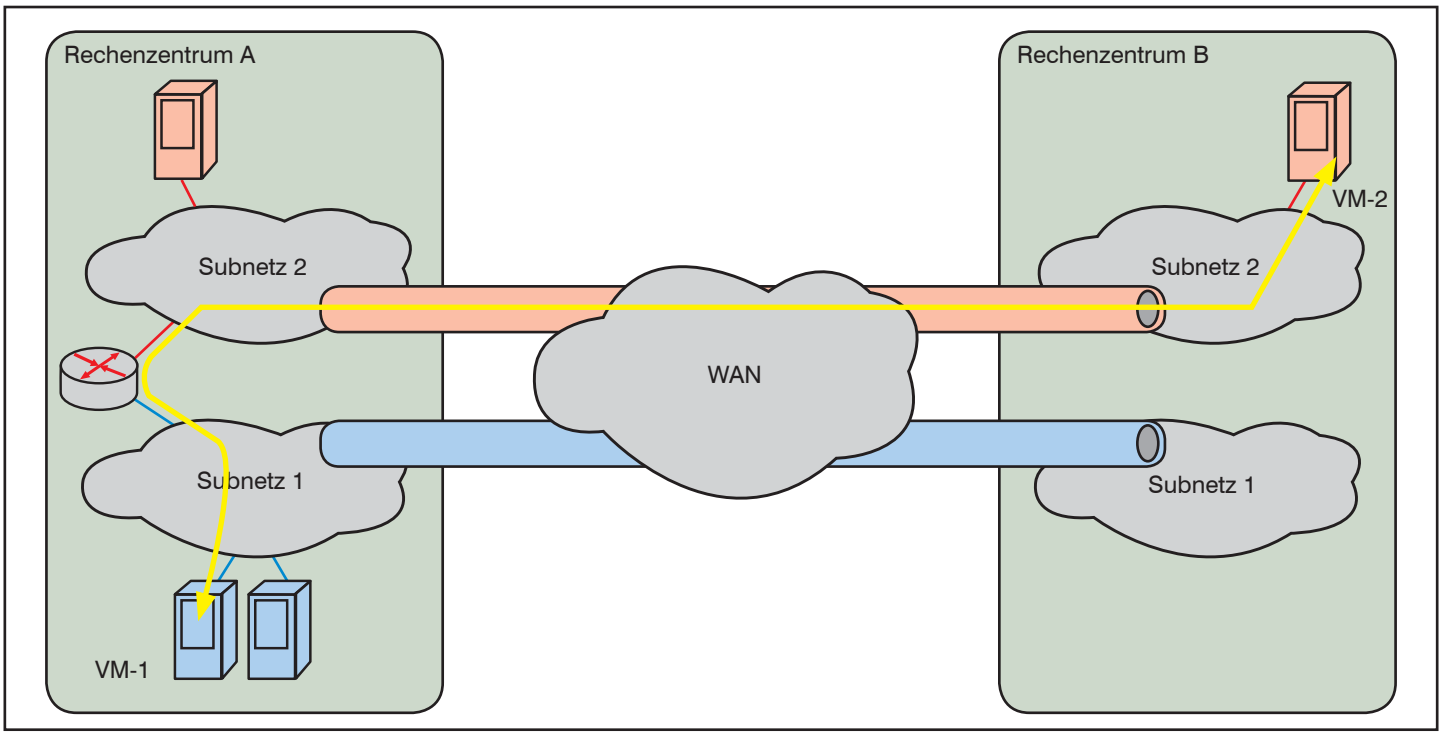


Abbildung 8: Verkehrsströme beim Routing zwischen virtuellen Subnetzen

Eine IP-Tunnellösung ist dann völlig überflüssig.

Für große Netze mit mehr als 4.000 Subnetzen steht SPBM (IEEE 802.1Qaq) zur Verfügung, womit ebenfalls optimale Layer-2-Wege quer durch das Netzwerk berechnet werden. Die ISID des Provider Backbone Bridgings, worauf SPBM ja beruht, ist genau wie die VID und die VSID von VXLAN und NVGRE 24 Bit groß. Das heißt, Sie können damit ebenfalls mandantenfähige Infrastrukturen betreiben und sind mengenmäßig nicht beschränkt. Ähnliches leistet im Übrigen auch Ciscos proprietäre Lösung FabricPath.

Bleibt also Fall 2: Die Layer-2-Fragmente sind nur über ein Layer-3-Transportnetz erreichbar.

Dies entspricht schon eher dem Zielszenario von VXLAN.

Das typische Design hatten wir schon angesprochen: Ihr Rechenzentrum ist in mehrere IP-Subnetze aufgeteilt, die untereinander nur doch Routing-Instanzen erreichbar sind. Beispiele sind:

- je ein IP-Subnetz pro Server-Rack und alle Racks sind untereinander über einen Layer-3-Core verbunden,
- ein PoD-Design, bei dem jeder PoD-Container komplett mit Layer-2- und Layer-3-Komponenten ausgestattet ist.

Wenn Sie jetzt die Anforderung haben Layer-2-Bereiche wie beispielsweise Kundennetze oder Cloud-Anwendungen über mehrere Racks oder PoDs zu verteilen, weil zum Beispiel die Kapazität eines einzelnen Racks nicht ausreicht, dann sind VXLAN und NVGRE durchaus geeignete Instrumente.

Was aber ist mit vMotion?

VXLAN und NVGRE werden in Fachkreisen gerne als angebliche Lösung für georedundante Rechenzentren angepriesen, um via vMotion virtuelle Maschinen quer über die ganze Welt zu verschieben und trotzdem die Konnektivität der VMs untereinander aufrecht zu halten.

Vom Prinzip her leisten die Protokolle dies auch, wir haben aber bislang über einen Punkt noch gar nicht gesprochen, der spätestens jetzt zum Tragen kommt: Das Routing auf der Seite der Kundennetze und die hiervon verursachten Verkehrsströme. Damit meine ich sowohl das Routing innerhalb einzelner virtueller Subnetze als auch das Routing zwischen verschiedenen Subnetzen als auch das Routing zu externen Systemen.

Betrachten Sie Abbildung 8. Dargestellt sind zwei (räumlich getrennte) Rechenzentren und zwei virtuelle Maschinen VM-1 und VM-2, die sich in verschiedenen Subnetzen (Subnetz 1 und Subnetz 2) befinden. Beide Subnetze sind in beiden Rechenzentren realisiert, die jeweiligen Segmente durch jeweils einen IP-Tunnel verbunden. Die Kommunikation zwischen VM-1 und VM-2 wird über die Routing-Instanz links in Rechenzentrum A sichergestellt, die jeweils ein Beinchen in beiden Subnetzen hat und zwischen den beiden IP-Netzen routet. Dieser Router könnte beispielsweise das Default Gateway für eine oder für beide virtuellen Maschinen sein.

In Abbildung 8 residiert die virtuelle Maschine VM-1 in Rechenzentrum A, die virtuelle Maschine VM-2 in Rechenzentrum B. Der Datenstrom zwischen VM-1 und VM-2 muss folglich über die WAN-Strecke, (Layer-2-)Verkehr zwischen dem Router und VM-2 im Subnetz 2 wird durch den entsprechenden IP-Tunnel geleitet.

So weit, so gut. Was passiert aber, wenn VM-1 zum Kommunikationspartner in dasselbe Rechenzentrum B verschoben wird? Abbildung 9 zeigt: Jetzt laufen alle Verkehrsströme zweimal über die WAN-Strecke! Der Grund hierfür ist natürlich, dass die Routing-Instanz im Rechenzentrum A geblieben ist. Die englische Fachliteratur spricht hierbei von „traffic trombone“ (wenn man geschickt zeichnet, zeigt der Verkehrsstrom die Form einer Posaune).

Wie man leicht erkennen kann, passiert dasselbe auch, wenn man die Verkehrsströme zu und von externen Systemen untersucht.

VXLAN und NVGRE neigen also gerade im Zusammenhang mit vMotion offensicht-

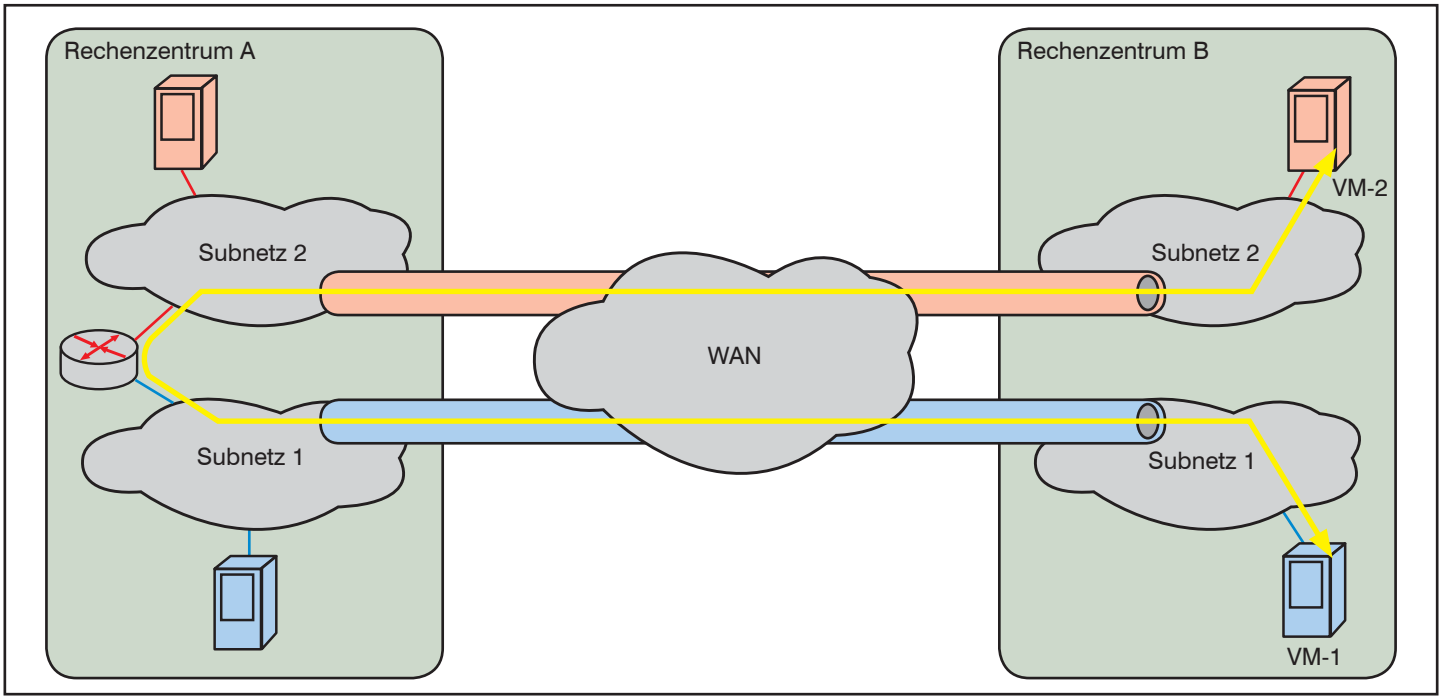


Abbildung 9: Traffic tromboning, verursacht durch Routing

lich zu solchen „Verkehrsposaunen“. Und selbst über kleinste Entfernung (z.B. benachbarte Racks) kann man hier nicht gerade von optimaler Wegeführung sprechen.

Erschwerend kommen einige Mängel der Protokollspezifikationen selbst hinzu:

1. Beide Protokolle setzen, wie oben erwähnt, im Transportnetz IP-Multicast-Funktionalität voraus. Etwas, was bei Verbindungen, die über das Internet geführt werden, gar nicht und bei Verbindungen über Provider-Netze eher selten zur Verfügung steht.

2. Die Dokumente setzen sich mit der Möglichkeit „vMotion“ überhaupt nicht auseinander, im VXLAN-Dokument wir die Möglichkeit, virtuelle Maschinen zu verschieben erst gar nicht angesprochen. Daher bleibt es beispielsweise offen, wie Tunnelendpunkte darüber informiert werden sollen, dass eine gelernte Zuordnung einer MAC-Adresse nach dem Umzug der virtuellen Maschine ungültig geworden ist.

Zusammenfassend kann man also feststellen, dass sowohl VXLAN als auch NVGRE völlig ungeeignet sind, um vMotion über große Entfernungen wie beispielsweise zwischen georedundanten Rechenzentren zu unterstützen, und auch innerhalb eines Rechenzentrums können sich ungünstige Wegeführungen ergeben.

Damit kommen wir zu einer sehr engen Designvorgabe für VXLAN- und NVGRE-Infrastrukturen:

VXLAN oder NVGRE kommt als Infrastrukturprotokoll in Frage

1. wenn sehr viele (d.h. mehrere tausend oder zehntausend) Layer-2-Domänen in Form von Kunden- oder Mandantennetze verwalten müssen und

2. wenn das Rechenzentrum auf Basis von Layer-3-Konnektivität organisiert und strukturiert ist (Transportnetz) und

3. wenn das Routing in und aus den Kundennetzen im Wesentlichen statisch bleiben kann.

4. Falls im Transportnetz kurze, optimierte Wege und Multipathing eine Rolle spielen, muss dieses Netz ein entsprechend kleinteiliges Layer-3-Netz sein (Zusätzlich zu VXLAN oder NVGRE auch noch TRILL oder SPB einzusetzen, macht nun wirklich keinen Sinn.).

Beachten Sie, dass diese drei Punkte durchaus beispielsweise zu Cloud-Services passen können! Entscheidet wird hierbei Punkt 3 sein: Ist es akzeptabel, wenn alle Clients, also auch mobile, externe Clients über denselben Weg auf die ausgelagerten Dienste zugreifen?

Layer 2 versus Layer 3

Was bedeutet aber Punkt 2 für zukunftsorientierte RZ-Designs? Fällt hier eine Grundsatzentscheidung für oder wider Layer 2 bzw. Layer 3?

Bei Diskussionen über Layer 2 und Layer 3 werden immer wieder gebetsmühlenartig die gleichen Argumente wiederholt:

- Layer 2 ist eine gemeinsame Fehler-Domäne.
- Layer 2 wird von Broadcasts bedroht.
- Es dürfen maximal so und so viele Systeme in eine Layer-2-Domäne.

Daran ist zunächst ja auch nichts falsches, das Problem hierbei ist vielmehr, dass diese Sprüche erstens viel zu sehr verallgemeinern und zweitens vom eigentlichen Thema ablenken. Was wir im Rechenzentrum brauchen, ist ein tragfähiges und vor allem flexibles Konzept, mit dem aktuelle und zukünftige Anforderungen abgedeckt werden können. Die Weisheiten von vor 20 Jahren helfen da nicht weiter.

Gestatten Sie mir daher ein paar ergänzende Anmerkungen:

- Oft wird behauptet, für vMotion brauche man eine einzige, alles umfassende Layer-2-Domäne:

  - Gerade im Zusammenhang mit modernen Layer-2-Infrastrukturprotokollen wie TRILL, SPB oder anderen

spricht vieles dafür im Rechenzentrum Zonen unterschiedlicher Service-Qualität einzuführen. Qualitätskriterien können sein: Prozessorleistung, Netzwerkanbindung, Art und Anbindung des Festplattenspeichers, Verfügbarkeit, Supportleistungen und vieles mehr.

vMotion, was ja per se nur zwischen Hosts gleicher Prozessorarchitektur funktioniert, ist dann natürlich nur noch innerhalb solcher Zonen sinnvoll – ansonsten würde die VM ja ihren zugesagten Service-Level verlassen. Solche Zonen werden in der Regel aber deutlich kleiner ausfallen als die eine einzige Zone, die das gesamte Rechenzentrum umfasst.

- Solche Service-Zonen gestatten auf Layer 2 zusammen mit den genannten SPB-Protokollen neuartige, leistungsfähigere Netzwerkdesigns bis hin zur Vollvermaschung hochwertiger Zonen.

- Diese SPB-Protokolle bilden ähnlich wie VXLAN und NVGRE ebenfalls Overlay-Netzwerke (nur eben „MAC-in-MAC“ auf Layer 2). Die „alles umfassende“ Layer-2-Domäne gibt es in solchen Netzen gar nicht: Was Sie brauchen, ist lediglich ein geeignetes Transportnetz zwischen den Uplink-Ports der ToR-Switches bzw. Rand-Switches.

- Selbst klassische, VLAN-basierende Designs schaffen keine allumfassende Layer-2-Domäne, sondern unterteilen das Netzwerk in kleinere Broadcast-Domänen.

- Standort-überreifendes vMotion ist nicht zuletzt wegen des oben diskutierten Routing-Problems so oder so problematisch. Weitere Probleme ergeben sich, wenn man auch noch die Speicheranbindung mit einbezieht. Daher kann man den Sinn von Standort-überreifendem vMotion zumindest bei größeren Entfernungen getrost bezweifeln.

- Kommende Technologien zeigen einen eindeutigen Trend hin zu mandantenfähigen Teilstrukturen innerhalb des Rechenzentrums:

  - Die Server-Virtualisierung, was ja bislang im Grunde nur die Virtualisierung von Server-*Hardware* ist, wird sich dahingehend entwickeln, dass komplette Anwendungsstrukturen virtualisiert zur Verfügung gestellt werden. Solche Strukturen werden derzeit unter dem Schlagwort Cloud-Service vermarktet. Diese Strukturen umfassen aber nicht nur Rechenleistung (in Form virtueller Maschinen) und Speicher, sondern auch Netzwerkdienste, die die Erreichbarkeit, die Sicherheit und die Verfügbarkeit der Anwendung gewährleisten. Hier ist es unsinnig beispielsweise Firewall-Regeln getrennt von der Anwendung auf einem zentralen Core-System zu definieren. VMware spricht nicht ohne Grund von „virtual data center“.

  - Die verschiedenen Virtualisierungsprodukte unterstützen zunehmend die automatische Bereitstellung solcher komplexer Cloud-Strukturen aus vorgefertigten Katalogen heraus. VMwares vCloud Director ist prominentestes Beispiel hierfür. Das funktioniert jedoch nur, wenn solche automatisch ausgerollten Teilnetze und ihre Anwendungen möglichst keinerlei Einfluss auf den Kern des RZ-Netzes haben.

  - „Bring your own device“ ermöglicht Geräten, die nicht unter der Kontrolle der IT-Abteilung stehen, den Zugang zu unternehmensinternen Diensten – und zwar sinnvollerweise sowohl aus dem internen Netz als auch aus dem Internet. Es macht also zukünftig keinen Sinn mehr zwischen beiden Zugängen groß zu unterscheiden. Die Folge ist, dass der Perimeter-Schutz der Anwendung näher an die Anwendung selbst rückt. Die eine, große Firewall, die sämtliche Schutzfunktionen übernimmt, hat ausgedient.

  - Die Anbindung solcher virtueller Netz- und Anwendungsstrukturen im Rechenzentrum erfolgt am einfachsten und auch sichersten, wenn diese Strukturen für das Rechenzentrum völlig transparent sind.

Zusammenfassend bedeutet das, dass **wir zukünftig RZ-Netze wie Provider-Netze betreiben werden!** Damit meine ich Netze, die unabhängig von den transportierten Inhalten (Anwendungen) rein hinsichtlich des Transports optimiert sind.

Solche Netze bauen aber auf möglichst flachen Transportstrukturen auf und nur am Rande (!) auf Layer 3. Produkte mit dem Begriff „Fabric“ im Namen zeigen in diese Richtung.

Netzwerkvirtualisierung:
Wo endet das RZ-Netz?

Spannender und mit viel tiefgreifenderen

Auswirkungen auf die RZ-Infrastruktur verbunden als diese Diskussion „Layer 2 versus Layer 3“ sind Überlegungen, die mit dem Begriff **Virtualisierung des Netzwerks** verbunden sind.

Dieser Begriff ist nicht klar definiert, manche bezeichnen damit die Trennung der sogenannten Control Plane, der Steuerungsebene, von der Data Plane, der eigentlichen Datenweiterleitung, oder einfach aufgedrückt: Die Steuerung der (physischen und virtuellen) Switches wird an eine übergeordnete, zentrale Instanz übertragen.

Ich möchte mich aber im Folgenden auf einen anderen Aspekt des Begriffs Virtualisierung konzentrieren, nämlich die Definition einer Abstraktionsschicht, die die reale Welt von den virtualisierten Systemen trennt und diesen stattdessen allgemeingültigere, generalisierte Schnittstellen zur Verfügung stellt.

So funktioniert die Virtualisierung von Servern bis hin zur Virtualisierung von Storage – und jetzt soll das Netzwerk folgen. Auf die Ziele einer solchen Strategie einzugehen, würde den Umfang dieses Artikels deutlich sprengen, aber einiges wurde schon angesprochen: automatisierte, schnelle Bereitstellung von Diensten, Integration von Cloud-Services, flexible Nutzung und Verschiebung von Ressourcen. All das erfordert im Kern eine Grundvoraussetzung: ortsunabhängig zu sein!

Und wie die Server-Virtualisierung die Ortsunabhängigkeit von Diensten fördert, indem sie die System unabhängig von der eingesetzten Hardware macht, ist es eine Grundanforderung an die Netzwerkvirtualisierung, dass **die Netzwerkadressierung der Systeme ortsunabhängig wird**.

Das ist eine durchaus interessante Forderung, da insbesondere IP-Adressen per Design ortsgebunden sind! Daher rührt ja auch das oben andiskutierte Routing/Default-Gateway-Problem.

Netzwerkvirtualisierung erfordert also die Einführung einer Abstraktionsschicht, die die Netzwerkadressen der realen Welt (das ist das RZ-Netz) von den Adressen, die die bereitgestellten Dienste nutzen, trennt. Diese Forderung ist übrigens weitestgehend gleichbedeutend mit der Forderung nach einer mandantenfähigen Infrastruktur und läuft auf eine Overlay-Struktur, d.h. eine Tunnellösung hinaus.

Die Kernfrage, die Sie für Ihr Rechenzentrum jetzt beantworten müssen, ist: Wo ziehe ich diese Abstraktionsschicht ein? Diese Frage ist deshalb so bedeutend,

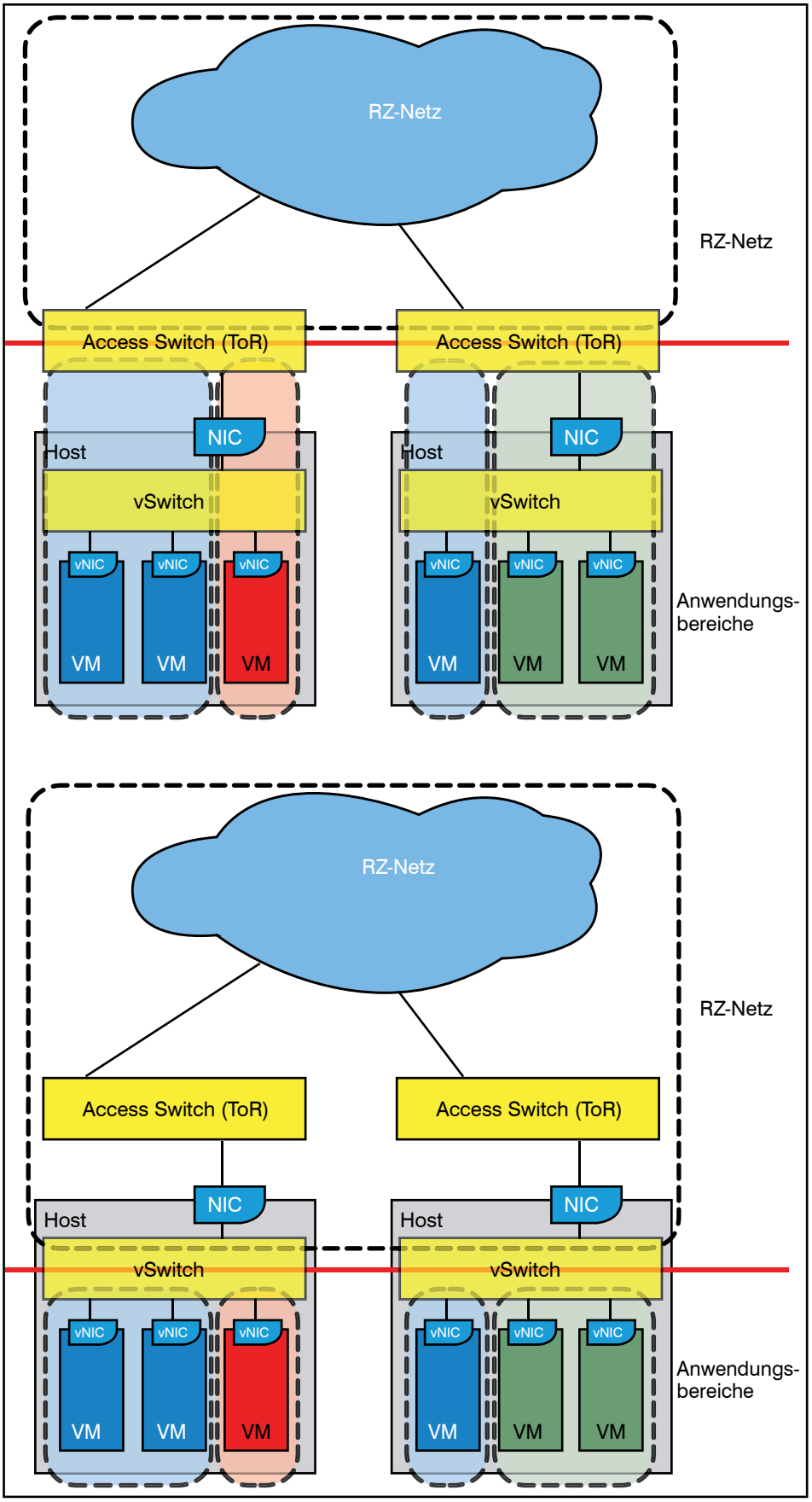


Abbildung 10: Trennungsebenen zur Netzwerkvirtualisierung

weil die Antwort gleichzeitig auch die Frage beantwortet, wo das RZ-Netz endet und wo der Anwendungsbereich beginnt. Die Frage nach dem Wie ist hiergegen eher unbedeutend.

Nun gibt es erkennbar zwei prinzipielle Möglichkeiten, diese Trennschicht einzuziehen: innerhalb der Hypervisor oder außerhalb der Virtualisierungs-Hosts in den Access-Switches. Die Folge einer Entscheidung zwischen beiden Möglichkeiten geht aus dem Abbildung 10 hervor: Im einen Fall gehört der virtuelle Switch zusammen mit der physischen Netzwerkkarte des Hosts zum RZ-Netz (und beide müssen dann zwangsläufig auch gemeinsam mit dem Netz administriert werden) und in anderen Fall nicht.

Wo die Präferenzen der Hersteller von Virtualisierungs-Software liegen, ist offensichtlich. Weniger offensichtlich ist, warum RZ-Betreiber nach wie vor auf RZ-Designs setzen, die eine klare Trennung von RZ-Netz und virtualisierter Umgebung im Grunde unmöglich machen.

Bereits die Einführung virtueller Switches mit den allerersten Virtualisierungsprodukten vor über 10 Jahren war der Problematik geschuldet, dass man ein Konstrukt brauchte, über das virtuelle Maschinen desselben Hosts miteinander kommunizieren können. Die überwiegende Zahl physischer Switches ermöglicht das bis zum heutigen Tage nicht!

Mittlerweile haben sich die Produkte weiterentwickelt und aus der Notlösung wurde ein strategisches Konzept: der Ersatz physischer Netzwerkkomponenten von Switches über Router und VPN-Gateways bis zur Firewall durch virtuelle Appliance und deren Steuerung durch die Hypervisor.

Und dieses Konzept ist ja durchaus schlüssig: Eine schnelle und trotzdem kunden- oder anwendungsspezifische Bereitstellung und Anpassung von Cloud-Diensten oder virtuellen Data Centern oder wie Sie das auch immer nennen mögen, erfordert Automatisierung. Und die automatische Bereitstellung solcher unter Umständen komplexer Strukturen kann nicht gelingen, wenn nicht auch die dazugehörenden Netzwerkdienste automatisch bereitgestellt, verlagert, neu gestartet, neu dimensioniert etc. werden können. Wie oben geschrieben: Es ist im Grunde unsinnig, beispielsweise Firewall-Regeln getrennt von der Anwendung auf einem entfernten, zentralen System zu definieren, wo sie im Zweifelsfall auch noch vor sich hin filtern, wenn die Anwendung längst ersetzt, weggewandert oder nur weiterentwickelt wurde.

Die gleichzeitige Nutzung von Diensten sowohl aus dem internen Netzwerk als auch aus dem Internet heraus ist ein anderes Beispiel dafür, dass es sinnvoll sein kann, Zugriffskontrolle anwendungsspezifisch und nicht netzwerkspezifisch zu definieren.

VXLAN und NVGRE kann man durchaus als weitere Bausteine in diesem Konzept ansehen: Beide Spezifikationen sehen die Tunnelendpunkt-Funktionalität standardmäßig innerhalb der Hypervisor. Außerdem führt zumindest VXLAN ein neues Frame-Format ein, und neues Frame-Format bedeutet in aller Regel neue Chips, sprich neue Hardware. Die große Ausnahme hierzu bilden lediglich die Nexus-Switche von Co-Autor Cisco, da das Frame-Format von VXLAN erstaunlicherweise ;-) praktisch identisch mit dem Frame-Format von OTV ist; der virtuelle Switch Cisco Nexus 1000V ist so auch das einzige Produkt, das heute VXLAN unterstützt. Physische Netzwerkkomponenten, die als Tunnelendpunkt und damit beispielsweise als Gateway zur Außenwelt fungieren könnten, sind bislang nur vage angekündigt.

Solange es aber keine physischen Gateways gibt, bleiben nur virtuelle Gateway-Anwendungen mit je einem Beinchen (virtuelle NIC) im VXLAN- bzw. NVGRE-Subnetz und einem in der Außenwelt.

Damit kommen wir vom virtuellen Switch zum virtuellen Router!

Und diese virtuellen Router leiten Datenströme Ihres RZ-Netzes weiter! Damit werden selbst virtuelle Maschinen zum Bestandteil des RZ-Netzes! Die Linie in Abbildung 10 verschiebt sich noch weiter nach unten, Virtualisierungs-Host und Netzwerk werden noch enger miteinander verflochten.

Heißt das, dass diese Technologien schlecht sind? Nein. Das heißt lediglich, dass sie eine einfache und klare Trennung zwischen RZ-Netz, Dienste und Anwendungen verhindern. Es spricht ja auch nichts gegen den Einsatz virtualisierter Netzwerkanwendungen, ob als Teil des Hypervisors oder als virtuelle Appliance, die Frage ist lediglich, ob sie als Teil einer Anwendung oder als Teil des RZ-Netzes fungieren. Ganz im Gegenteil: Man kann heute zumindest mittelfristig die Entwicklung immer leistungsfähigerer Chips prognostizieren, die in immer weiterem Umfang auch netzwerktechnische Aufgaben wahrnehmen. Es ist schlichtweg unwahrscheinlich, dass diese Kapazitäten dann nicht auch genutzt würden. Die Zeiten, in denen man sich wegen der integrierten virtuellen Switches Sorgen um die CPU-Ressourcen machte, sollten spätestens mit der nächsten Server-Generation vorbei sein.

Diese Entwicklung hin zu dezentralen, verschiebbaren (weil ortsunabhängigen) Anwendungsstrukturen hat übrigens eine Analogie in der hinter uns liegenden Entwicklung im Telefoniemarkt: „Intelligenz“ (sprich Entscheidungsfähigkeit, Zugriffskontrolle etc.) wird aus den zentralen Core-Komponenten hinein in die Endsysteme verlagert. Der Core selbst (also das RZ-Netz) wird, wie heute bereits das Internet, zum reinen, diensteneutralen Transportnetz.

Bedeutet die in Abbildung 10 skizzierte logische Trennung auf der Ebene der Access-Switches das Ende aller Probleme? Unglücklicherweise gibt es hier kein eindeutiges Ja, zumindest sehr große Strukturen können Schwierigkeiten bekommen. Sie können zwar VXLAN, NVGRE oder auch SPB, TRILL oder eine vergleichbare Lösung in die Access-Switches integrieren und ihr RZ-Netz wie ein Provider als reines Transportnetz betreiben, auf den Links zwischen Access Switch und virtuellen Switches stehen Ihnen standardmäßig dann aber nur die üblichen 4094 VLAN-IDs zur Verfügung. Kommen Sie damit aus, ist alles gut, falls nicht, müssen Sie wohl oder übel die Tunnellösung, wie von VXLAN oder NVGRE vorgesehen, bis in die virtuellen Switches bzw. Hypervisor ziehen oder eine andere Möglichkeit finden, die Datenströme zu trennen (z.B. mit 802.1BR - Port Extension).

Es hängt also wesentlich von Ihrer Umgebung ab, welche Optionen Ihnen zur Verfügung stehen:

- In kleinen Umgebungen ist eine solche Trennung vermutlich eher überflüssig.
- In sehr großen Umgebungen brauchen Sie eine geeignete Lösung, wenn Sie tatsächlich mehrere tausend Subnetze an jedem einzelnen Access-Port zur Verfügung stellen wollen (z. B. für ein völlig flexibles vMotion).
- Der Rest hat die Möglichkeit zu entscheiden zwischen einer klaren Trennung zwischen Netz- und Anwendungsbetrieb und einer im Laufe der Zeit immer engeren Integration von virtualisierten Diensten in den Netzwerkbetrieb.
  - Trennung bedeutet einfache organisatorische Strukturen, klare Zuständigkeiten, aber die Übergabe anwen-

dungsspezifischer Netzwerkdienste an das Team, das die Anwendung betreut. Das RZ-Netz wird als Provider-Netz betrieben, alle Overlay-Strukturen bzw. Transporttunnel enden an den Access-Switches. Kein VXLAN, kein NVGRE, kein VEPA, kein VN-Link oder ähnliches.

- Integration bedeutet schon aus Stabilitätsgründen eine enge Zusammenarbeit und vermutlich die organisatorische Zusammenlegung von Netzwerk- und Serverbetrieb.

Die Entscheidung liegt bei Ihnen, Sie sollten sich aber über die Konsequenzen im Klaren sein.

Fazit

VXLAN und NVGRE sind keine universell einsatzbaren Lösungen. Im Gegenteil, sie adressieren sehr spezielle Probleme vornehmlich sehr großer Rechenzentren:

- Sie benötigen eine MAC-in-IP-Tunnellösung?
- Weil Sie Mandantennetze auf einer gemeinsamen Infrastruktur voneinander trennen müssen?
- Weil Sie verteilte, durch Layer 3 getrennte Layer-2-Bereiche transparent miteinander verbinden müssen?
- Weil die üblichen circa 4.000 VLANs Ihnen hierfür nicht ausreichen?

Wenn Sie jetzt viermal Nein gesagt haben, müssen Sie sich nicht weiter mit diesen Protokollen auseinandersetzen.

Aber selbst, wenn Sie den Einsatz eines der Protokolle in Erwägung ziehen, bleiben einige Probleme:

- Das Transportnetz muss IP-Multicasts unterstützen.
- Es gibt keine flexible Lösung für das diskutierte Routing-Problem (traffic trombones).
- Die Protokolle sind nicht dafür geeignet, vMotion über größere Entfernungen zu unterstützen.
- Die Datenpakete werden größer, d.h. die MTU-Size muss gegebenenfalls angepasst werden.

Darüber hinauf konterkarieren VXLAN und NVGRE praktisch alle technischen Entwicklungen der letzten Jahre, die die netzwerktechnische Anbindung virtueller Maschinen verbessern sollten:

- IP-offload und andere Offload-Funktionen der Netzwerkkarten werden ausgebremst und unwirksam,
- EVB (802.1Qbg), egal ob VEB oder VEPA, ist inkompatibel,
- SR-IOV ist im Grunde überflüssig,
- direkter Hardware-Zugriff (Direct Path) funktioniert nicht,
- lossless Ethernet-Technologien werden unwirksam (da der Datenverkehr über IP getunnelt wird),
- TRILL oder SPB sind ebenfalls unnötig (Warum sollte man zwei Overlay-Tunnel laufen lassen?)
- und als Knüller wird die IPv6-Unterstützung bei VXLAN auf eine spätere Version verschoben.

Der letzte Punkt zeigt lediglich wie unausgegoren der VXLAN-Entwurf noch ist, bei den anderen Punkten liegt der Grund für die jeweiligen Einschränkungen in der standardmäßigen Positionierung der Tunnelendpunkte: Beide Protokolle ziehen das Transportnetz (Provider-Netz, RZ-Netz) in den Virtualisierungs-Host hinein und terminieren erst dort die Transporttunnel.

Die Kernfragen lauten daher: Wollen Sie das? Wo endet Ihr RZ-Netz? Welche Aufgaben soll das RZ-Netz leisten? Und was ist im Grunde anwendungsspezifisch?

Ein einfaches Beispiel: Stellen Sie sich vor, VMware führt in seinen Produkten VXLAN ein und Microsoft in seinen NVGRE. Sie haben im Rechenzentrum hauptsächlich Virtualisierungs-Hosts auf Basis ESXi, die Konnektivität wird über VXLAN sichergestellt. Und jetzt bekommen Sie einen Server mit Hyper-V. Ist es akzeptabel, dass Sie dann keine Layer-2-Verbindung zwischen virtuellen Maschinen auf beiden Hosts herstellen können?

Ich bin der Meinung, dass produktspezifische Infrastrukturprotokolle im Rechenzentrum nichts zu suchen haben.

ComConsult Veranstaltungskalender

Aktuelle Veranstaltungen

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen, 24.09. - 26.09.12 in Bonn

Dieses Seminar behandelt die Projektschritte, Einsatz- und Migrations-Szenarien, einsetzbare Basis-Technologien, Komponenten und erweiterte TK-Anwendungen, Bewertungskriterien für eine TK-Lösung und gibt eine Übersicht über den bestehenden TK-Markt etablierter Hersteller wie Alcatel-Lucent, Avaya, Cisco, Nortel und Siemens aber auch des Newcomers Microsoft. Preis: € 1.890,-- netto

Virtualisierungstechnologien in der Analyse, 26.09. - 28.09.12 in Bonn

Dieses Seminar liefert einen umfassenden und zugleich detaillierten Einblick in die aktuellen Virtualisierungstechnologien der marktführenden Anbieter. Vom Server über das Netzwerk bis zum Speicher und schließlich auch zum Client werden die Möglichkeiten und Grenzen der Virtualisierungslösungen analysiert. Dabei bleiben auch Sicherheitsaspekte nicht unberücksichtigt. Basis hierfür bilden neben den technischen Grundlagen und Hintergründe die Erfahrungen aus dem Projektalltag sowie die Diskussion mit den Teilnehmern.

Preis: € 1.890,-- netto

Verkabelungssysteme für Lokale Netze, alles standardisiert, alles klar?, 01.10.12 in Düsseldorf

Dieses Seminar erklärt die Zusammenhänge der wichtigsten Standards und Normen, vergleicht diese mit dem aktuellen Stand der Technik und bewertet insbesondere die Praxistauglichkeit der im Normenumfeld getroffenen Empfehlungen. Neben einer Betrachtung des aktuellen Normungsstands aus der Sicht eines Normennutzers, der Bewertung von ausgewählten herstellerspezifischen Lösungen wird auch auf Planungs- und installationsbegleitende Maßnahmen eingegangen, die im Rahmen einer anstehenden Verkabelung zu beachten sind. Preis: € 990,-- netto

RZ-RZ-Kopplung - alles nur eine Frage der Bandbreite?, 01.10.12 in Düsseldorf

Immer mehr Unternehmen sehen sich derzeit damit konfrontiert, ihre Rechenzentrumsdienstleistungen über entfernte Standorte redundant anzubieten. Neben den entsprechenden Vorgaben des Bundesamts für Sicherheit in der Informationstechnik (BSI) für Desaster Recovery Konzepte fordert auch die Kundenseite entsprechende Service Level Agreements zur Hochverfügbarkeit ihrer Dienste und Daten ein. In diesem Seminar werden die aktuellen Techniken vorgestellt, technisch erläutert und für die richtige strategische Entscheidung zu einem Gesamtkonzept zusammengeführt. Preis: € 990,-- netto

Umfassende Absicherung von Voice over IP und Unified Communications, 01.10. - 02.10.12 in Düsseldorf

Dieses Seminar zeigt Wege auf, wie die Vorteile von Unified Communications für das Unternehmen nutzbar gemacht werden können ohne gleichzeitig die Sicherheit geschäftsentscheidender Kommunikation aufs Spiel zu setzen. Preis: € 1.590,-- netto

Sonderveranstaltung: UC - Cisco versus Microsoft - Wer hat die bessere Unified-Communications-Lösung?, 22.10.12 in Bonn

Diese einmalige Sonderveranstaltung analysiert die bestehenden UC-Lösungen von Cisco und Microsoft auf dem Stand der neuesten Releases und stellt die spannende Frage, wer die bessere Lösung hat. Auch die erkennbaren Weiterentwicklungen werden dabei berücksichtigt. Preis: € 990,-- netto

Internetworking: optimales Netzwerk-Design mit Switching und Routing, 22.10. - 26.10.12 in Aachen

Dieses 5-tägige 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: € 2.490,-- netto

IT-Projektmanagement Kompaktseminar, 22.10. - 24.10.12 in Hamburg

Ein Projekt stellt an einen Projektleiter hohe Anforderungen. In diesem Kurs vervollständigen Sie praxisnah Ihre Kenntnisse aus der gesamten Bandbreite des Projektmanagements: Der Kurs umfasst sowohl Administratives, wie Planen und Überwachen des Projekts, als auch Softskills, wie Moderation von Projektsitzungen und Präsentation von Information. Denn die in der Regel nur „lose“ unterstellten Projektmitarbeiter müssen überzeugend auf Basis einer strukturierten Planung geführt werden. Und jede Chance, sich und sein Projekt erfolgreich zu präsentieren, ist zu nutzen! Preis: € 1.890,-- netto

Rechenzentrumsdesign - Technologien neuester Stand, 22.10. - 24.10.12 in Hamburg

Das 3-tägige Seminar „Rechenzentrumsdesign – Technologien neuester Stand“ fokussiert sich auf aktuelle Technologien und Trends im Rechenzentrumsumfeld. Sie lernen von der Verkabelung über die Stromversorgung, die Klimatisierung und den Schrankaufbau, wie ein ausfallsicheres und energieeffizientes Rechenzentrum heute strukturiert wird. An den Tagen zur aktiven Netztechnik lernen Sie, welche Mechanismen für Redundanz, Lastverteilung und Standort-übergreifende Hochverfügbarkeit in aktuellen RZ-Planungen zu berücksichtigen sind und wie diese mit dem fortwährenden Trend zur Virtualisierung zusammenspielen. Abschließend werden aktuelle Speichersysteme, deren Anbindung über die am Markt verfügbaren Übertragungsprotokolle sowie Aspekte zur Datensicherung und Disaster Recovery diskutiert. Preis: € 1.890,-- netto

Zertifizierungen

ComConsult Certified Network Engineer

Lokale Netze
12.11. - 16.11.12 in Aachen
21.01. - 25.01.13 in Aachen
22.04. - 26.04.13 in Aachen
09.09. - 13.09.13 in Aachen
25.11. - 29.11.13 in Aachen

TCP/IP intensiv und kompakt
18.02. - 22.02.13 in Stuttgart
13.05. - 17.05.13 in Bonn
07.10. - 11.10.13 in Stuttgart

Internetworking
22.10. - 26.10.12 in Aachen
11.03. - 15.03.13 in Aachen
17.06. - 21.06.13 in Aachen
14.10. - 18.10.13 in Aachen

Paketpreis für alle drei Seminare € 6.720,-- netto (Einzelpreise: je € 2.490,-- netto)

ComConsult Certified Trouble Shooter

Trouble Shooting in vernetzten Infrastrukturen
23.10. - 26.10.12 in Aachen
05.02. - 08.02.13 in Aachen
11.06. - 14.06.13 in Aachen
24.09. - 27.09.13 in Aachen

Trouble Shooting für Netzwerk-Anwendungen
04.12. - 07.12.12 in Aachen
12.03. - 15.03.13 in Aachen
09.07. - 12.07.13 in Aachen
05.11. - 08.11.13 in Aachen

Paketpreis für beide Seminare inklusive Prüfung € 4.280,-- netto
(Seminar-Einzelpreis € 2.290,-- netto , mit Prüfung € 2.470,-- netto)

ComConsult Certified Voice Engineer

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen
26.11. - 28.11.12 in Bonn
25.02. - 27.02.13 in Köln
03.06. - 05.06.13 in Bonn
16.09. - 18.09.13 in Berlin
02.12. - 04.12.13 in Bonn

Session Initiation Protocol Basis-Technologie der IP-Telefonie
29.10. - 31.10.12 in Bonn
18.03. - 20.03.13 in Berlin
24.06. - 26.06.13 in Köln
07.10. - 09.10.13 in Stuttgart

Umfassende Absicherung von Voice over IP und Unified Communications
01.10. - 02.10.12 in Düsseldorf
11.04. - 12.04.13 in Bonn
18.07. - 19.07.13 in Bonn
04.11. - 05.11.13 in Bonn

Optionales Einsteiger-Seminar: IP-Wissen für TK-Mitarbeiter
18.02. - 19.02.13 in Stuttgart
13.05. - 14.05.13 in Bonn
30.09. - 01.10.13 in Düsseldorf

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

ComConsult Certified Service Catalogue Manager

Servicialisierung - Leitkonzept für verlässliche Service-Erbringung
01.10. - 02.10.12 in Düsseldorf

Service-Identifizierung - Von Service-Begriff bis Service-Konsumentennutzen
29.10. - 30.10.12 in Bonn

Service-Offerierung - Von Service-Spezifizierung bis Service-Katalogisierung
12.11. - 13.11.12 in Bonn

Paketpreis für alle drei Seminare € 4.290,-- netto (Einzelpreise: je € 1.590,-- netto)

Impressum

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

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

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

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