ComConsult Research

Der Netzwerk Insider

April 2010

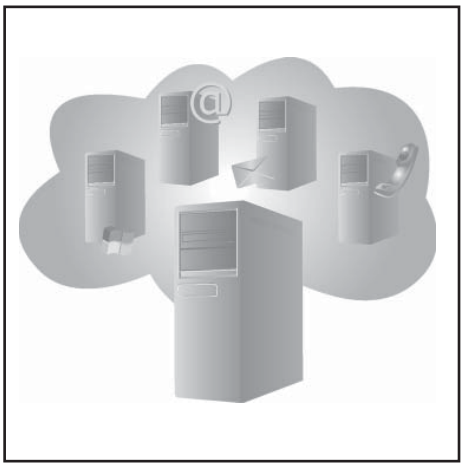
Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

Virtualisierung: Virtual Desktop Infrastructure - steht das Rechenzentrum vor dem Kollaps?

von Dipl.-Inform. Matthias Egerland, Jonas Goede

Nach der erfolgreichen Virtualisierung des Serverumfelds und den damit verbundenen Konsolidierungsvorteilen steht nun in vielen Unternehmen die Virtualisierung der Client-Seite an. Auch hier locken eine flexiblere, einfachere Administration, mehr Energieeffizienz und ein höherer Sicherheitsgrad über die zentralisierten Daten. Doch welche Anforderungen stehen dem im Rechenzentrum gegenüber? Müssen die Rechenzentren von morgen einem völlig anderen Design unterliegen, um die Ansprüche einer Virtual Desktop Infrastructure (VDI) bedienen zu können?



Dieser Artikel analysiert den Übertragungsweg der virtualisierten Desktops in Richtung Clients und beleuchtet den architektonischen Unterschied der marktgängigen Desktop-Übertragungsprotokolle RDP, ICA und PCoIP. Daraus werden die Anforderungen an die Rechenzentrumsinfrastruktur abgeleitet.

weiter auf Seite 20

Zweitthema

IP Version 6 - das Internet der nächsten Generation (Teil 2)

von Dipl.-Inform. Petra Borowka-Gatzweiler

3. Autokonfiguration, DNS und DHCP

3.1 Autokonfiguration

Aktuell fließt immer noch ein erheblicher Aufwand in die statische oder automatische Konfiguration von IP-Endgeräten / IP Hosts (IP-Adresse, Maske, Default Gateway und weitere Optionen). Um diesen Betriebsaufwand für IPv6 zu reduzieren, wurden Mechanismen festgelegt, die eine Autokonfiguration der Endgeräte erlauben. Die explizite Konfiguration von IP-Adressen und Router-Einträgen in Endgeräten sollen künftig entfallen - diesen Job regelt das IPv6-Protokoll dynamisch und selbstlernend: Bei der Autokonfiguration wird nach dem Booten von IP dynamisch eine Link-lokale Adresse festgelegt, die netzweit eindeutig, aber nicht fix im Endgerät konfiguriert ist. Darüber hinaus werden weitere für die Kommunikationsfähigkeit erforderliche Parameter wie „nächster Router“, MTU, Hop Limit etc. in Erfahrung gebracht. Die IPv6 Standardisierung bezeichnet Endgeräte / IP Hosts als „Station“. Dieser Artikel übernimmt im nachfolgenden Text diese Diktion.

weiter auf Seite 12

Aktueller Kongress

ComConsult IT-Sicherheits-Forum 2010

ab Seite 6

Geleit

Der Wechsel auf IPv6 muss jetzt starten!

ab Seite 2

Angebot bis zum 15.04.2010

ComConsult-Study.tv Sonderaktion

auf Seite 19

Zum Geleit

Der Wechsel auf IPv6 muss jetzt starten!

Die Diskussion über IPv6 ist jetzt fast 10 Jahre alt. Genauso alt sind die Prognosen, wann der IPv4-Adressraum so langsam ausgehen wird. Tatsache ist, dass einige der Megatrends der letzten Jahre erheblichen Einfluss auf diese Entwicklung haben:

- Die Anzahl mobiler Endgeräte, die eine fast permanente Adresse benötigen, explodiert. Die aktuelle Diskussion über das Apple iPad kontra HP Slade und den Bedarf für einen neuen Typ von Endgerät ist das perfekte Beispiel dafür

- Die Zahl der Anbieter für Cloud Computing und Software as a Service nimmt immer schneller zu. Neue Service-Infrastrukturen im Web entstehen und müssen ggf. stärker als bisher eingebunden werden

- Die Anzahl der Geräte in den Unternehmen, die in permanenten Verbindungen mit der Außenwelt stehen, nimmt genauso explosiv zu wie die der mobilen Endgeräte im Konsumermarkt, Unified Communications und Collaborations lassen grüßen

- Wussten Sie, dass der PKW der Zukunft mindestens 20 IP-Adressen benötigt?

Darüber hinaus gibt es auch eine Reihe von direkten Argumenten auf der Unternehmensseite, um nicht länger mit dem Einstieg in IPv6 zu warten:

- Auf die meisten Unternehmen kommt im Rahmen dieser Entwicklung eine schnell steigende Zahl von mobilen Endgeräten zu. Je später der Wechsel auf IPv6 erfolgt, desto aufwendiger wird der Umstieg

- Neue Installationen größerer Gerätemengen sollten am besten jetzt in IPv6 erfolgen

- Ab 2011 werden die ersten Service-Anbieter im Web nur noch über IPv6 erreichbar sein, ein Dual-Stack wird dann nicht mehr möglich sein. Betrachtet man die rapide Ausbreitung einiger neuer Web 2.0 Dienste, dann muss man in Betracht ziehen, dass ihr Unternehmen ggf mit diesen Diensten arbeiten will. Damit entsteht bereits der erste Parallelbetrieb mindestens im Router / in der Firewall für ihr Unternehmen

- Für viele Unternehmen steht der Wechsel auf Windows 7 auf der Projektliste.

Eigentlich der perfekte Zeitpunkt, um wirtschaftlich und mit optimalem Aufwand zu wechseln. Ansonsten packen sie genau diese Geräte in ein bis zwei Jahren schon wieder an, also besser jetzt sofort

- Der Umstieg wird mindestens für die größeren Unternehmen Jahre erfordern. Zum einen ist eine nicht zu unterschätzende Lernphase für die Betreiber erforderlich, IPv6 ist deutlich mehr als nur ein Adresswechsel. Zum anderen gibt es eine Reihe von Geräten in den Unternehmen, die sich vermutlich nicht oder nur schwer migrieren lassen. Dafür müssen Konzepte ausgearbeitet werden, ein Test ist unvermeidbar

- IPv6 kann das gesamte Sicherheits-Szenario verändern. Zum einen sind Firewalls und Router direkt betroffen, zum anderen erhält mit IPv6 der Aspekt der sicheren Peer-to-Peer-Verbindung eine gewisse Bedeutung. Viele der bestehenden Konzepte, Angriffsmuster und Abwehrverfahren müssen komplett neu durchdacht werden.

Fasst man die Situation der Unternehmen nach diesen Ausführungen zusammen, dann gilt:

1. Der Wechsel nach IPv6 ist unvermeidbar

2. Er ist komplex und wird in der Regel unterschätzt

3. Er wird in den meisten Fällen zwischen 1 und 3 Jahren dauern

Betrachtet man angesichts dieser Aussagen die Entwicklung im Internet und die zunehmende Knappheit der IPv4-Adressen, das massive Umstellen in China, Japan und auch in den USA addiert den Druck der EU auf dieses Thema, dann wird klar, dass der Zeitpunkt zum Start dieses Projekts für die meisten Unternehmen jetzt gekommen ist. Wer jetzt noch wartet, handelt mehr als fahrlässig.

So schön, so gut. Aber IPv6 ist weit mehr als der simple Austausch einer IPv4-Adresse durch eine neue IPv6-Adresse. Hinter IPv6 steckt ein völlig neues Konzept von Netzwerk. Dies betrifft viele wichtige Bereiche unserer Netzwerke, darunter vor allem auch DNS und DHCP.

Wer also jetzt mit der Planung beginnt, der läuft auf eine Reihe von Kernfragen. Wir diskutieren diese auf unserem Netzwerk-Redesign Forum 2010, sowohl in einem Vortrag von Frau Borowka als auch in einem ganztägigen Workshop von Herrn Flüs. Eine einmale Chance, schnell und kompakt auf den aktuellen Stand der Diskussion zu kommen. Als Vorgeschmack auf das Forum sollen die folgenden Fragen dienen:

- Ist IPv6 wirklich ausgereift?
- Stateless kontra Stateful, was ist der bessere Weg?
- Ist Autokonfiguration sinnvoll, kann auf DHCP ganz verzichtet werden?
- Wie wird DNS integriert?
- Wie erfolgen Adresswechsel?
- Was bedeutet IPv6 für Firewalls und Application Level Gateways?
- Was passiert mit NAT?
- Wie sehen Migrations-Konzepte aus?
- Wo sollen wir beginnen?

K.O.-Kriterium wird für die meisten Unternehmen die Frage sein, ob IPv6 ausgereift genug ist. Die Antwort ist schwierig. Für die Massenprodukte ist sie mit einem klaren ja sehr positiv. Windows 7 ist ein typisches Beispiel. Aber dem stehen jede Menge von Sonderprodukten gegenüber, zum Beispiel Fertigungs-Steuerungen, Zugangskontrollen, Videoüberwachungen, Spezial-Produkte der Automatisierungstechnik, alte Geräte im allgemeinen. Aus der Liste ist sofort zu entnehmen, dass kein Unternehmen an einem Test vorbei kommen wird. Der wird in der Regel schon deshalb erforderlich, weil Implementierungs-Varianten verglichen werden müssen und das Betriebspersonal sich einarbeiten muss. IPv6 ist sehr umfangreich und beinhaltet viele Optionen und auch noch offene Bereiche wie den von Mobile IPv6. Die Einarbeitung wird Zeit kosten.

Der Wechsel auf IPv6 muss jetzt starten!

Eine der Kernfragen wird für die meisten Unternehmen die Diskussion über Stateless kontra Stateful sein. IPv6-Endgeräte können ihre IP-Adresse automatisch bilden, indem sie den Netzwerk-Identifikator vom Router beziehen und den Rest der Adresse selber bilden. Von daher ist DHCP so wie wir es kennen nicht zwingend erforderlich. Trotzdem muss aber eine Integration in DNS erfolgen, Netzwerke müssen überwachbar bleiben, Bestandführungen müssen die Adressen von Endgeräten kennen, Teile von DHCP im Betrieb von IP-Telefonie sind unverzichtbar und viele weitere Argumente fallen einem da spontan ein. Auch eine Kombination aus stateless und stateful ist möglich, um die Sache ganz abzurunden. Hier müssen Entscheidungen getroffen werden.

Wie diese Diskussion zeigt, ist die Spannbreite der IPv6-Diskussion erheblich. Antworten müssen erarbeitet werden, es wird kein Konzept geben, das blind auf alle Unternehmen angewandt werden kann.

Wir starten unsere IPv6-Diskussion auf dem ComConsult Netzwerk-Redesign Forum 2010. Versäumen Sie diese einmalige Chance nicht, in dieses komplexe Thema einzusteigen und auch von den Erfahrungen der anderen Teilnehmer zu profitieren.

Beachten Sie auch unsere Ipv6-Videos auf ComConsult-Study.tv.

Ihr
Dr. Jürgen Suppan

Netzwerk-Redesign Forum 2010

Die ComConsult Akademie veranstaltet vom 26.04. - 29.04.10 ihren Kongress „Netzwerk-Redesign Forum 2010“ in Königswinter.

Netzwerke sind der Lebensnerv unserer Unternehmen. Sie unterliegen einer permanenten Weiterentwicklung und Veränderung. Aus einem Mix aus Bedarf und technischen Möglichkeiten muss das individuelle Optimum für ein Unternehmen gefunden werden. Dieses Optimum muss zugleich an der Zukunft orientiert sein, da Netzwerk-Komponenten über einen langen Zeitraum stabil und ohne permanente Änderungen betrieben werden müssen.

Hier setzt das ComConsult Netzwerk-Redesign Forum 2010 an. Es analysiert die wichtigsten Bedarfsentwicklungen, stellt diesen die neuesten Netzwerk-Technologien gegenüber und erarbeitet Empfehlungen für ein erfolgreiches Netzwerk-Design, eine zukunftsorientierte Auslegung und einen stabilen und zuverlässigen Betrieb.

Die Schwerpunktthemen des ComConsult Netzwerk-Redesign Forums 2010 sind:

Neue Redundanz-Verfahren im Layer 2
Speziell aus dem Umfeld der Rechenzentren kommt der Bedarf für neue Redundanz-Verfahren. In diesem Umfeld hat sich ein Konflikt zwischen der Normung von IEEE und der IETF entwickelt. Hier stehen mit Shortest Path Bridging und TRILL zwei Verfahren im direkten Wettbewerb. Ergänzt wird dieses Szenario um Lösungen, die auf virtuellen Chassis-Technologie-Lösungen basieren. Wer ist auf dem richtigen Weg?

Wie viel Bandbreite brauchen wir in Zukunft?
10 Gigabit-Ethernet ist bei Servern inzwischen Standard. Aber was bedeutet das für den Backbone, den Access-Bereich und das WAN?

Speziell im Rechenzentrum bekommt das Netzwerk immer mehr den Charakter eines System-Busses mit sehr kurzen Schaltzeiten und einer extrem hohen Verfügbarkeit. Die weitere Entwicklung im Umfeld Virtualisierung und Speicher-Integration lässt bereits Diskussionen um den Folgestandard 40 oder 100 Gigabit Ethernet aufkommen. Hier stehen zwei Lager gegenüber. Die einen haben 40 Gigabit bereits in ihre Komponenten integriert, die anderen setzen auf den technisch naheliegenden Sprung auf 100 Gigabit.

Gleichzeitig besteht der Bedarf, Zugriff auf Speicher und Server zu verteilen, zum Teil sogar zwischen Standorten auszudehnen. Lastskalierung und Desaster Recovery sind hier die treibenden Faktoren. Auch Desktop-Virtualisierung geht in Richtung eines speziellen LAN-Protokolls, das bei höheren Bandbreiten die Videoqualität eines normalen Desktops erreicht. Wie hoch wird der Bandbreiten-Bedarf?

Layer-2 kontra Layer-3 WAN
Neue Layer-2-Verfahren im Verbund mit aus dem Provider-Bereich kommendem Carrier Ethernet stellen die Frage nach Layer-2 oder Layer-3 im WAN neu.

Produkt- und Technologie-Sicherheit
Mit der Weiterentwicklung der Netzwerktechnik stellt sich in vielen Bereichen die Frage, ob die bisherigen Produkte die Basis für die Zukunft legen können oder ob sie am Ende ihrer Nutzbarkeit ankommen.

Produktions-Steuerungen und Gebäude-Management im Netzwerk
Seit Jahren gibt es schon den Trend, Produktionsnetzwerke als große Layer-2-Bereiche in bestehende Netzwerk-Strukturen zu integrieren. Nun kommt als nächstes Thema das Gebäude-Management hinzu. Was bedeutet das, welche Optionen bestehen?

Wireless LANs nach der Verabschiedung von IEEE 802.11n
Nach der Verabschiedung von IEEE 802.11n steht der Weg nun offen, vor allem auch die optionalen Bereiche des Standards zu nutzen. Dies bedeutet vor allem mehr Leistung und mehr Stabilität.

IPv6
Seit Jahren diskutiert, nun wird es endlich real. Die ersten Unternehmen haben mit der Einführung von IPv6 begonnen. Die Hersteller und Provider sind soweit, alles wartet auf den Massenmarkt. Da gleichzeitig der Druck der internationalen Adressverwaltung immer größer wird, wird es auf jeden Fall Zeit, dieses Thema zu adressieren.

Neue Netzwerk-Standards
Eine ganze Reihe neuer Netzwerk-Standards stehen vor der Tür. Nutzen oder nicht nutzen?

Sicherheit
Der zunehmende Schutzbedarf, rechtliche Rahmenbedingungen und Compliance-Richtlinien machen Druck im Bereich Sicherheit. Da die Netzwerk-Basistechnologie im Prinzip zumindest bisher unsicher ist, wird Sicherheit durch die Netzwerk-Architektur, sprich Switching und Routing-Verfahren erreicht. Reicht das aus?

Das ComConsult Netzwerk-Redesign Forum 2010 ist die zentrale Netzwerk-Veranstaltung des Jahres 2010. Sie ist für jeden Entscheider, Planer und Betreiber in diesem Bereich ein absolutes Muss. Hier trifft sich die Branche.

Sichern Sie sich rechtzeitig einen Platz in dieser herausragenden Veranstaltung!

Netzwerk-Redesign Forum 2010 - Programmübersicht

Montag, den 26.04.2010

9:30 bis 11:00 Uhr
Markt- und Technologie-Analyse:
Neue IT-Architekturen und die Konsequenzen für Netzwerke:
wie viel Bandbreite brauchen wir in Zukunft?

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

Dr. Jürgen Suppan, ComConsult Research

11:00 bis 11:30 Uhr - Kaffeepause

11:30 bis 12:30 Uhr
Migration zu IPv6 im Netzwerk

- Der Zeitpunkt: wann wird IPv6 zum Muss?
- Die Aufgabe: IPv6 im Netzwerk, was bedeutet das?
- Die Probleme: welche Komponenten sind kritisch?
- Die Migration: welche Alternativen bestehen?
- Ausblick und Fazit

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

12:30 bis 14:00 Uhr - Mittagspause

14:00 bis 15:30 Uhr
Neue Standards für WAN und Backbone:
das Ende von OSPF?

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

Dr. Franz-Joachim Kauffels, Unternehmensberater

15:30 bis 16:00 Uhr - Kaffeepause

16:00 bis 17:15 Uhr
Brauchen wir mehr als Ethernet und IP?
Wer braucht QoS und FCoE?

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

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

17:15 bis 18:00 Uhr
Core-Switches 2010

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

Dr. Franz-Joachim Kauffels, Unternehmensberater

ab 18:00 Uhr - Happy Hour

Dienstag, den 27.04.2010

9:00 bis 10:00 Uhr
Neue Switching-Standards

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

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

10:00 bis 11:00 Uhr
Wireless LANs nach der Verabschiedung von IEEE 802.11n

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

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

11:00 bis 11:30 Uhr - Kaffeepause

11:30 bis 12:30 Uhr
Gebäudeverkabelung im Wandel der Zeit

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

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

12:30 bis 14:00 Uhr - Mittagspause

14:00 bis 15:00 Uhr
Sicherheit im Netzwerk 2010

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

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

15:00 bis 15:30 Uhr
Produktions-Steuerungen und Gebäude-Management im Netzwerk

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

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

15:30 bis 16:00 Uhr - Kaffeepause

16:00 bis 17:00 Uhr
Analyse: Voice- und Video im Netzwerk

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

Dr. Jürgen Suppan, ComConsult Research

Netzwerk-Redesign Forum 2010 - Programmübersicht

Mittwoch, den 28.04.2010

09:00 bis 10:30 Uhr
Markt-Analyse: Cisco kontra HP, Multi-Blade kontra Routing-Core: wohin geht der Markt?
- Was bedeutet die Übernahme von 3Com durch HP für den Markt?
- HP kontra Cisco: Kampf der Konzepte
- Wie sehen Netzkomponenten in Zukunft aus?
- Welche Produkte sind End-of-Life?
- Multi-Blade kontra Routing-Core: wer wird überleben?
- Ausblick

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

10:30 bis 15:30 Uhr
Hersteller stellen sich der Diskussion:
- Bandbreitenbedarf
- Zukunftsorientierte Produkt-Strategien
- Neue Switching-Standards
- LAN-Design: wohin geht der Weg?

11:00 bis 11:30 Uhr - Kaffeepause

12:30 bis 14:00 Uhr - Mittagspause

15:30 bis 16:00 Uhr - Kaffeepause

16:00 bis 16:45 Uhr
Trouble-Shooting und Service-Level-Management 2010: wo sind die Grenzen?
- Aufgaben in modernen Netzwerken
- Neue Messgeräte und Verfahren
- Berichte und Beispiele aus der Trouble-Shooting-Praxis

N.N.

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

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

Workshop 1:
Voice und Video im Netzwerk
- Bedarfbewertung aus der Sicht von Unified Communication
- Gestaltungsparameter in LAN und WAN
- Prüfung bestehender Netzwerke
- Redesign-Gesichtspunkte

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

Workshop 2:
Desaster Recovery
- Aufgabenstellung
- 10/40/100 auch über Diistanz
- Eigenheiten optischer Transportnetze
- Konventionelle Lösungen
- Revolutionärer Ansatz
- Fazit und Konsequenzen

Dr. Franz-Joachim Kauffels, Unternehmensberater

Workshop 3:
IPv6: Parallelbetrieb und Migration
- Gründe für (Wahl des Zeitpunkts zum) Einstieg in IPv6
- Grundlegende Mechanismen von IPv6 - Kurzeinführung und Anschauungsbeispiele
- Mechanismen zur Koexistenz / Kopplung von IPv4 und IPv6 in einer (ggf. langen) Übergangsphase
- Optionen zum Umgang mit der Übergangsphase
- IPv6 und Sicherheit

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

10:30 bis 11:00 Uhr - Kaffeepause

12:30 bis 14:00 Uhr - Mittagspause

15:30 Uhr - Ende der Veranstaltung

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
Netzwerk-Redesign Forum 2010

Ich buche den Kongress
Netzwerk-Redesign Forum 2010

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

Workshopauswahl
☐ Workshop 1: Voice und Video im Netzwerk
☐ Workshop 2: Desaster Recovery
☐ Workshop 3: IPv6: Parallelbetrieb und Migration

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

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

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

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

☐ Bitte reservieren Sie mir ein Zimmer

vom _____ bis _____ 10

im Maritim Hotel Königswinter.

_____ Vorname

_____ Nachname

_____ Firma

_____ Telefon/Fax

_____ Straße

_____ PLZ,Ort

_____ eMail

_____ Unterschrift

Aktueller Kongress

ComConsult IT-Sicherheits-Forum 2010

Die ComConsult Akademie veranstaltet vom 07.06. - 08.06.10 ihren Kongress „ComConsult IT-Sicherheits-Forum 2010“ in Königswinter.

Schwerpunktthema des diesjährigen IT-Sicherheits-Forums ist die Sicherheit im Rechenzentrum. Der massive Einsatz der Server-Virtualisierung erfordert neue Sicherheitskonzepte für den Umgang mit der Dynamik und Mobilität von VMs und für den Aufbau von Sicherheitszonen im Rechenzentrum. Damit einhergehend drohen Cloud-Konzepte in das Rechenzentrum einzuziehen und eine neuartige Risikolage zu schaffen.

Das aktuelle Redesign im Rechenzentrum steht häufig im krassen Gegensatz zu klassischen Konzepten der IT-Sicherheit. Beispielsweise ist die Vorgabe, dass VMs mit einem unterschiedlichen Sicherheitsniveau nicht auf einem gemeinsamen physischen System laufen dürfen, in der Praxis immer schwerer durchsetzbar. Im Sinne eines möglichst hohen Konsolidierungsgrads wird nicht selten sogar der Wunsch geäußert, selbst eine Internet DMZ innerhalb der gleichen Virtualisierungsumgebung abzubilden, wie die internen Serverbereiche. Dem steht eine erschreckend lange Liste mit gemeldeten Sicherheitslücken in Virtualisierungs-Produkten gegenüber. Aus einer Sicherheitsperspektive muss man hier nicht nur die Herstelleraussagen kritisch prüfen, sondern auch darüber nachdenken, wie ein Patch-Management für Virtualisierungslösungen angesichts der extrem hohen Verfügbarkeitsanforderungen noch sinnvoll gestaltet werden kann.

Diese Trends haben auch Auswirkungen auf die Sicherheit in SAN und NAS. Hier stellt sich zunächst die Frage, wie konsequent die Zonierung in Server-Bereich und LAN auch im SAN fortgesetzt werden muss und ob die Mittel der logischen SAN-Zonierung ausreichen.

Wir erleben im Moment einen konsequenten Umschwung weg von einer an Fat Clients orientierten IT hin zur Anwendungs- und Desktop-Virtualisierung. Aus einer Sicherheitsperspektive ist hier entscheidend, dass Ressourcen, die bisher im Campus-LAN verteilt waren, plötzlich zentral in das Gehirn der IT-Infrastruktur - das RZ - rücken. Eine Infektion eines Clients mit einer schadenstiftenden Software breitet sich plötzlich nicht mehr im Campus-LAN aus, sondern würde direkt in zentralen Komponenten im RZ wirken. Hier müssen für die verschiedenen

in Frage kommenden Techniken die Gefährdungslage analysiert und die bestehenden Maßnahmenkataloge für die Endgerätesicherheit angepasst werden.

Die Entwicklung zur Desktopvirtualisierung stellt auch fundamentale Konzepte der LAN-Sicherheit in Frage. Wenn Clients zentral im RZ laufen bzw. Anwendungen nur noch zentral zur Verfügung gestellt werden, muss beispielsweise diskutiert werden, ob überhaupt noch eine Notwendigkeit für eine Netzzugangskontrolle besteht. Denn letztendlich bedeuten diese Entwicklungen, dass sich das für das Intranet zu schaffende Sicherheitsniveau immer mehr reduziert und sich dafür wesentliche Aspekte der IT-Sicherheit in das RZ verlagern.

Auf eine Sicherheit für die physischen Endgeräte wird jedoch nicht verzichtet werden können, denn Fat Clients werden uns mit Notebooks zunächst in der klassischen Art erhalten bleiben und müssen entsprechend abgesichert werden. Interessant ist in diesem Zusammenhang aber die Frage, wie sich Smartphones weiter entwickeln werden, denn dass diese ein ausgesprochen interessantes Angriffsziel darstellen, auf dem vertrauenswürdige Daten lagern können und das sich vorzüglich als Transportwirt für schadenstiftende Software eignet, ist keineswegs neu. Neu ist die Tatsache, dass Smartphones der Normalfall geworden sind und ein fast unüberschaubarer Zoo an Anwendungen sich explosionsartig entwickelt hat.

Ein Seiteneffekt von Zentralisierung und Virtualisierung auf die Zonierung im RZ-Bereich ist die enorm gestiegene Anforderung an die Leistung von Firewall-Systemen und Intrusion-Prevention-Systemen. Nicht selten ist hier eine effektive Durchsatzleistung bei produktivem Regelwerk von 10 Gbit/s und mehr gefordert. Diese Forderung in Verbindung mit immer komplexeren zu filternden Protokollen und Kommunikationsbeziehungen gehen an die Grenze dessen, was die Hersteller bieten. Auch hier müssen traditionelle Zonierungskonzepte überdacht werden. Besonders kritisch wird die Situation bei der Kommunikation zwischen Rechenzentren, denn hier kommt es nicht nur auf Verfügbarkeit und Performance sondern auch auf Vertraulichkeit an. In solchen Situation kann es notwendig sein, eine hochverfügbare Verschlüsselungsleistung von 10 Gbit/s und mehr liefern.

Außerdem ändern sich die Rahmenbedingungen für den Virenschutz durch Virtualisierung. Auch ruhende VMs können infiziert werden und ein Full System Scan, der simultan auf mehreren VMs auf einem physischen Server abläuft, kann die Leistung signifikant beeinflussen, Hier sind neue Konzepte auf Ebene der Virtualisierungslösung gefragt, die durch geeignete Schnittstellen den Sicherheitszustand einer Vielzahl von VMs bewerten können.

Inwieweit diese Anforderungen an die RZ-Sicherheit mit einem realistischen Aufwand überhaupt umgesetzt werden können und welche Konzepte aktuell in den Rechenzentren implementiert werden, erfahren Sie im ComConsult IT-Sicherheits-Forum 2010. Hier werden die wichtigsten Bedarfsentwicklungen analysiert, die neuesten Technologien gegenübergestellt und Empfehlungen für ein sicheres RZ-Design einen sicheren Betrieb erarbeitet.

Das ComConsult IT-Sicherheits-Forum 2010 ist die zentrale IT-Sicherheits-Veranstaltung des Jahres 2010. Sie ist für jeden Entscheider, IT-Sicherheitsbeauftragten, Planer und Betreiber in diesem Bereich ein absolutes Muss. Hier trifft sich die Branche.

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

ComConsult IT-Sicherheitsforum 2010 - Programmübersicht

Montag, den 07.06.2010

9:30 - 10:30 Uhr

Keynote: RZ im Wandel - Herausforderung an die IT-Sicherheit

- Konsequenzen der Virtualisierung für Sicherheitskonzepte und -prozesse
- Geänderte Rolle des Intranet angesichts Desktop- und Anwendungsvirtualisierung: Brauchen wir noch eine Netzzugangskontrolle?
- Aufbau von Sicherheitszonen im RZ jenseits von 10 Gbit/s: Hochleistungs-Appliances, MACsec und Co.
- Sicherheit auf Ebene der Anwendung oder Pauschalmaßnahmen auf Netzebene?
- Risiko Kurzschluss von Sicherheitszonen im Storage-Bereich

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

10:30 - 11:00 Uhr Kaffeepause

11:00 - 12:00 Uhr

Methodische RZ-Sicherheit mit den BSI IT-Grundschutz-Katalogen

- Umbruchphase: Sicherheitskonzepte für das moderne RZ
- RZ-Sicherheit: bestehende und geplante relevante Bausteine der IT-Grundschutz-Kataloge
- Umgang mit der Dynamik und Mobilität der Virtualisierung in den Prozessen zur IT-Sicherheit
- Was thematisiert der neue Baustein zur Virtualisierung?

Oliver Flüs, ComConsult Beratung und Planung GmbH

12:00 - 12:45 Uhr

Auswirkungen der Desktop- und Anwendungsvirtualisierung auf die IT-Sicherheit

- Gefährdungen durch Zentralisierung von Clients
- Sind neue Konzepte beispielsweise für den Virenschutz erforderlich?
- Wie sicher sind Terminal Server wirklich?
- Vergleich der Herstellerkonzepte zur Desktop-Virtualisierung

Matthias Egerland, ComConsult Beratung und Planung GmbH

12:45 - 14:00 Uhr Mittagspause

14:00 - 14:45 Uhr

Sorgenkind Datenbanksicherheit

- Datenbank-Hacking, SQL-Injection und andere Gefährdungen
- Sicherheitsmaßnahmen für Datenbanken
- Sichere Datenbankzugriffe über Portal-Architekturen: erfolgreiche Risikoverlagerung?
- Schatten-Datenbanken

Oliver Flüs, ComConsult Beratung und Planung GmbH

14:45 - 15:30 Uhr

Sicherheit von Web-Anwendungen

- Verbreitete Schwachstellen und Angriffstechniken
- Herangehensweisen zur Absicherung von Web-Anwendungen
- Best-Practices und Hilfe zur Selbsthilfe (BSI, OWASP)
- Automatische Sourcecodeanalyse
- Einsatzvarianten von Web Application Firewalls (WAFs)

Thomas Schreiber, SecureNet GmbH

15:30 - 16:00 Uhr Kaffeepause

16:00 - 16:45 Uhr

Konzepte für den Aufbau von Sicherheitszonen im RZ

- Zwiebelschalenmodell: Wie praxistauglich ist ein mehrschichtiger Zonenaufbau?
- Kriterien für die physikalische Trennung und die Virtualisierung von Netzen und Servern
- Umgang mit Administrationsbereichen und Konsolennetzen
- Anforderungen an Firewalls, Intrusion-Prevention-Systeme und Security Gateways
- Verschlüsselung mit 10 GBit/s und mehr: Technologien und Hersteller
- Link Layer Encryption: Proprietäre Produkte oder wo steht MACsec?

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

16:45 - 17:30 Uhr

Unified Communications über Vertrauensgrenzen hinweg

- Problem Firewalling von VoIP und Unified Communications (UC)
- VoIP und UC im WAN
- Umgang mit Verschlüsselung von Medienstrom und Signalisierung in Firewall-Architekturen
- Rolle von Session Border Controllern
- Einbindung mobiler Nutzer und Heimarbeitsplätze

N.N.

ab 18:00 Uhr Happy Hour

Dienstag, den 08.06.2010

9:00 - 9:45 Uhr

Sicherheit in SAN und NAS

- Welche Gefährdungen sind in SAN und NAS relevant?
- Maßnahmen zur Absicherung von SAN und NAS -Elemente einer SAN-Sicherheitsrichtlinie • Konzepte für eine Zonierung im SAN
- Wann sollte verschlüsselt werden?

Matthias Egerland, ComConsult Beratung und Planung GmbH

9:45 - 10:30 Uhr

Projekterfahrungen zur Verschlüsselung im SAN

N.N.

10:30 - 11:00 Uhr Kaffeepause

11:00 - 11:45 Uhr

Security Appliances, Firewalls und IPS im Hochleistungsbereich

- Load-balancing und Load Sharing: Was geht wirklich?
- Wie sinnvoll sind Layer 2 Firewalls?
- Ist ein Durchsatz von 10 Gbit/s und mehr tatsächlich bei einem produktiven Regelwerk noch realistisch?
- Einsatzmöglichkeiten virtueller Firewalls
- Leistungsgrenzen von Intrusion- Prevention-Systemen
- Hersteller im Vergleich (Juniper, Checkpoint, Tipping Point)

Andreas Meder, ComConsult Beratung und Planung GmbH

11:45 - 12:30 Uhr

Infrastruktur-Sicherheit im RZ

- Was passiert, wenn die Zutrittskontrolle streikt und den Zugang zum RZ verweigert?
- Zutrittskontrolle, Vereinzelungsanlagen, Video-Überwachung, etc.: Auch die Infrastruktur-Sicherheit braucht aktive Komponenten, die angemessen abgesichert werden müssen
- Elektromagnetische Verträglichkeit: ein unterschätztes Risiko?
- Stromausfall: immer noch der Präzedenzfall für die Notfallvorsorge

Hartmut Kell, ComConsult Beratung und Planung GmbH

12:30 - 14:00 Uhr Mittagspause

14:00 - 14:45 Uhr

Sicherheit und Nachvollziehbarkeit administrativer Zugriffe

- Identity Management für privilegierte administrative Zugriffe
- Protokollierung von Adminstrationssitzungen auf Servern und Netzkomponenten
- Verfügbare Lösungsansätze und ihre Grenzen
- Marktüberblick und Auswahlkriterien

Stefan Strobel, Cirosec GmbH

14:45 - 15:30 Uhr

Grenzen der Protokollierungim Netz

- Folgen der Verfassungsgerichtsentscheidung zur Vorratsdatenhaltung
- Änderungen am Datenschutzgesetz
- Empfehlungen zur Protokollierung in Netzkomponenten und Servern
- Neue Regeln zur Auftragsdatenverarbeitung

Ulrich Emmert, e/s/b Rechtsanwälte

Ende der Veranstaltung 15:30 Uhr

ComConsult IT-Sicherheits-Forum 2010

Frühbucherrabatt bis 15.04.10

ComConsult IT-Sicherheits-Forum 2010

07.06. - 08.06.10 in Königswinter

Für Besucher unserer bisherigen Kongresse bzw. für die Teilnehmer am VIP-Verteiler bieten wir Ihnen exklusiv eine Vorbuchungsphase für das ComConsult IT-Sicherheits-Forum 2010 bis zum 15.04.2010 für eine rabattierte Teilnahmegebühr an.

ComConsult IT-Sicherheits-Forum 2010
zum Preis bei Buchung bis 15.04.10 von € 1.490,-- zzg. MwSt.
statt regulär € 1.690,-- zzg. MwSt.

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

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

ComConsult IT-Sicherheits-Forum 2010

Ich buche den Kongress
ComConsult IT-Sicherheits-Forum 2010

☐ 07.06. - 08.06.10 in Königswinter
zum Preis von € 1.490,-- * zzgl. MwSt.

*gültig bis zum 15.04.2010

☐ Bitte reservieren Sie mir ein Zimmer

vom _____ bis_____ 10

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

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

Aktueller Kongress

ComConsult Verkabelungs- und Infrastrukturforum 2010

Die ComConsult Akademie veranstaltet vom 17.05. - 18.05.2010 ihren Kongress „Verkabelungs- und Infrastrukturforum 2010“ in Bonn.

Die Planung und Realisierung einer anwendungsneutralen Kommunikationsverkabelung bleibt nach fast 15 Jahren Standardisierung weiterhin eine Herausforderung. Fokussiert sich die Auswahl der Techniken für den Tertiärbereich im klassischen Büroumfeld auf die Frage, „braucht man 10 Gbit/s am Arbeitsplatz oder nicht und mit welchen Materialien ist das möglich“, so stecken wir im Bereich der Rechenzentren sehr häufig erst am Anfang der Entwicklung und der Praxiserfahrungen mit den unterschiedlichen Lösungsstrategien. Wurde die Glasfaser mehr oder weniger aus dem Tertiärbereich verdrängt, so nimmt ihre Bedeutung im Rechenzentrum wieder zu. Welche Stärken, welche Schwächen hat dieses Medium in den unterschiedlichen Einsatzumgebungen, wie ist dieses einzumessen, welche besonderen Techniken müssen in Erwägung gezogen werden, welche Datenraten lassen sich über diese Glasfasern realisieren?

Die Einführung einer „IT-Verkabelung“ zur Regelung von Non-Office-Communication ist gerade für den traditionellen IT-ler bisher kein Thema. Im industriellen Umfeld wird beispielsweise eine relativ strenge Separierung vorgelebt, Anlagenbauer und IT-ler sorgen jeweils für ihre eigenen Netze, keiner kommt dem anderen ins Gehege. Es zeigt sich zunehmend in Projekten der Bedarf, die Kommunikation von Gebäudeleittechniken bzw. Mess- und Regelungstechnik ebenfalls mit Hilfe von Ethernet-Technologie zu realisieren. Lassen sich die bisherigen, allseits bekannten Regeln des Office-Umfeldes auf diese Bereiche übertragen? Die Antwort muss „nein“ sein, die Anforderungen in diesen Bereichen unterliegen nicht immer den gleichen Rahmenbedingungen, insbesondere die Maxime „Gigabit/s-und-mehr“ um jeden Preis ist zu hinterfragen. Datenrate ist nicht mehr alleine ein Kriterium für eine gute IT-Verkabelung, verstärkt wird auf Einfachheit und Zuverlässigkeit gesetzt. Dieses erfordert aber teilweise eine Abkehr von bisherigen Planungs- und Realisierungsumsetzungen, nur mit Kenntnis dieser veränderten Technologieanforderungen kann die IT-Verkabelung der Zukunft den neuen Herausforderungen begegnen.

Das ComConsult Verkabelungs- und Infrastrukturforum 2010 analysiert die Technologie-, Markt- und Produktsituation für neue und zukünftige Verkabelungsstrategien und gibt wesentliche Empfehlungen sowohl zur Aktualisierung bestehender als auch zur Umsetzung neuer Infrastrukturen. Darüber hinaus werden Themen behandelt, die eigentlich jedem Planer von Kommunikationsverkabelungen bekannt sein sollten. Die Erfahrung zeigt aber, dass sowohl auf Seiten der ausführenden Firmen als auch auf Seiten der Bauherrn in vielen Fällen elementares Basiswissen fehlt, welches letztendlich zu fehleranfälligen Verkabelungen, Verletzung von allgemein anerkannten Regeln der Installationstechnik oder zur verkürzten Nutzungsdauer der Infrastruktur führen kann. Das Forum geht unter anderem auf die Technikvarianten der neuen Generationen von Kommunikationsverkabelungen ein, analysiert werden die Rahmenbedingungen, die zur Vorbereitung einer Kommunikationsverkabelung notwendig sind und es werden bisher vernachlässigte Randthemen wie z.B. Brandschutz oder Potenzialausgleich näher beleuchtet.

Im Einzelnen geht das Forum auf folgende Fragen ein:

- Welche Anforderungen müssen Verkabelungslösungen erfüllen, um die Einführung von neuen Techniken der Gebäudemelde- und Leittechnik zu vereinfachen, warum kann der Normungsansatz der EN50173 hier nicht vollständig greifen? Welche Alternativen gibt es?
- Haben die Verkabelungsnormierungen einen Stand der Vollständigkeit erreicht, wo steht die EN 50173 heute?
- Wie sieht die Dokumentation einer Kommunikationsverkabelung aus, wie lassen sich moderne Datenbanksysteme sinnvoll nutzen?
- Lassen sich vorhandene und neue Verkabelungssysteme mit Kupferverkabelungen für 40 Gbit/s oder 100 Gbit/s nutzen, wann wird die Leistungsfähigkeit von Twisted Pair das Ende erreicht haben?
- Muss mit einem neuen Planungsansatz für die Gebäudevollverkabelung im Sinne einer Technischen Gebäudeausstattung (TGA) gerechnet werden, warum kann die Technik der Office-Verkabelung nur bedingt in einer solchen Umgebung eingesetzt werden?
- Warum stellt der Consolidation Point ein wenig bekanntes aber effizientes „neues“ Teilelement der Datenverkabelung dar? Wie ist er in der Planung zu berücksichtigen?
- Arbeitsplatzverkabelung: Glasfaser kontra Kupfer. Ist eine Abkehr von der Lösung „Glasfaser bis zum Arbeitsplatz“ festzustellen? Haben sich die Prognosen zur Zukunftssicherheit bei beiden Medien bewahrheitet? Für wen ist die eine oder andere Variante die richtige Lösung?
- Einsatz von Mehrfaserstecker im Rechenzentrum. Welche unterschiedlichen Strategien gibt bei es MPO-Systemen, wann geht an ihnen kein Weg vorbei? Wann lassen sich erhebliche Kosten mit ihnen sparen?
- Welche Bedeutung hat ITIL für den Betrieb einer Kommunikationsverkabelung?
- Technische Gebäudeanlagen: Kommunikation ist das eine, was ist mit der Stromversorgung der Geräte? Der BUS war früher, moderne IP-basierende Leit- und Automatisierungssysteme benötigen neue Strategien, reicht PoE aus?

Wer immer sich für die zukünftigen neuen Aufgaben einer Kommunikationsverkabelung vorbereiten muss, wer nach sinnvollen Alternativen und Empfehlungen für

ComConsult Verkabelungs- und Infrastrukturforum 2010

optimale Lösungen sucht, wer nicht mehr weiter weiß mit der vorhandenen Verkabelung, der sollte dieses Forum nicht verpassen.

Konkret sind unter anderem folgende Vorträge auf dem Forum geplant:

- Kabelstandardisierung: was ist neu, was passiert hinter den Kulissen; Informationen aus erster Hand
- Neue Wege der Endgeräteverkabelung mit dem Consolidation Point? Anforderungen, Lösungen und Rahmenbedingungen
- Normen und Standards zur Glasfasermesstechnik: Notwendigkeit , Defizite und Ergänzungen
- Nachhaltigkeit durch Unified Physical Infrastructure - Konvergenz in Gebäuden und Rechenzentren
- Energieversorgung in der IT Umgebung, neue Wege beschreiten
- Leistungsexplosion Virtualisierter Systeme und Konsequenzen für Netze und Verkabelung
- ITIL und dessen Bedeutung für den Betrieb einer Kommunikationsverkabelung
- Pro- und Kontra-Diskussion: Zukunftssicherheit durch Glasfaser bis zum Arbeitsplatz, Illusion oder Realität?
- Pro- und Kontra-Diskussion: Einsatz von Mehrfaserstecker-Techniken im Rechenzentrum, Vor- und Nachteile?
- Konzeption, Aufbau, Realisierung von Erdungssystemen unter Berücksichtigung von EMV, LEMP- und HPEM-Störschutzzonen
- Moderner Brandschutz bei IT-Verkabelung; Brandschutztechnische Anforderungen aus der Betrachtung des TÜV

Die Darstellungen von Vision, Innovation und Praxisnähe, beides lässt sich kombinieren, dafür stehen ComConsult-Foren seit vielen Jahren. Bereiten Sie sich auf die nächste Epoche der Kommunikationsverkabelung vor, hören Sie sich die unterschiedlichen Standpunkte an, hinterfragen diese kritisch und bilden sich Ihre eigene Meinung. Zögern Sie nicht, sich einen Platz auf dieser herausragenden Veranstaltung zu sichern.

Die Moderation dieses Kongresses übernimmt Dipl.-Ing. Hartmut Kell.

Herr Kell kann bis heute auf eine mehr als 20-jährige Berufserfahrung in dem Bereich der Datenkommunikation bei lokalen Netzen verweisen. Als Leiter des Competence Center IT-Infrastrukturen der ComConsult Beratung und Planung GmbH hat er umfangreiche Praxiserfahrungen bei der Planung, Projektüberwachung, Qualitätssicherung und Einmessung von Netzwerken gesammelt und vermittelt sein Fachwissen in Form von Publikationen und Seminaren.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Verkabelungs- und Infrastrukturforum 2010

Ich buche den Kongress
Verkabelungs- und Infrastrukturforum 2010

☐ 17.05. - 18.05.10 in Bonn
zum Preis von € 1.690,-- zzgl. MwSt.

☐ Bitte reservieren Sie mir ein Zimmer

vom _____ bis_____ 10

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

_____ Vorname

_____ Nachname

_____ Firma

_____ Telefon/Fax

_____ Straße

_____ PLZ,Ort

_____ eMail

_____ Unterschrift

ComConsult Verkabelungs- und Infrastrukturforum 2010 - Programmübersicht

Montag, den 17.05.2010

9:30 - 11:00 Uhr
Kabelstandardisierung: was ist neu, was passiert hinter den Kulissen, Informationen aus erster Hand
Thomas H. Wegmann, DKE Deutsche Kommission

11:00 - 11:30 Uhr Kaffeepause

11:30 - 12:15 Uhr
Neue Wege der Endgeräteverkabelung mit dem Consolidation Point?
- Klassische Kabelführung mit Unterflursystemen, wohin mit den Kabeln?
- Unbekanntes Element der EN 50173: Der Sammelpunkt
- Richtlinien zur Planung, Nutzung der Vorteile, Gefahren
- Herstellerübersicht

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

12:15 - 13:00 Uhr
LWL-Messtechnik: Methoden, Aussagefähigkeit, Geräte
- Vor- und Nachteile von Pegel- und OTDR-Messungen
- Normierte Methoden der Messung
- Was bedeuten die gemessenen Werte, was bedeuten sie nicht?
- Typische Mess- und Interpretationsfehler

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

13:00 - 14:30 Uhr Mittagspause

14:30 - 15:30 Uhr
Nachhaltigkeit durch Unified Physical Infrastructure - Konvergenz in Gebäuden und Rechenzentren
- Wesentliche Aspekte bei der heutigen Planung von Infrastrukturen sind deren künftige Skalierbarkeit, Flexibilität und Zuverlässigkeit
- Der Trend: eine zunehmend vereinheitlichte physikalische Infrastruktur für alle Anwendungsbereiche
- Die Herausforderung: ein deutlich erweitertes Risikomanagement für die „Unified Physical Infrastructure (UPI)“
- Die Chance: mehr Effizienz bei steigender Flexibilität, Senkung der Kosten und des Verbrauchs natürlicher Ressourcen

Lars-Hendrik Thom, Panduit EEIG

15:30 - 16:00 Uhr
Dokumentation der physikalischen Infrastruktur
- Notwendiges Übel oder „Abfallprodukt“ aus der Planung?
- Wo liegt die Grenze zwischen Nutzen und Aufwand?
- Visualisierung der CI – Beziehungen
- „Biologisches“ Wissen allen zugänglich machen
- Die physikalische Infrastruktur innerhalb ITIL Prozessen

Detlef Klugseder, FNT GmbH

16:00 - 16:30 Uhr Kaffeepause

16:30 - 17:15 Uhr
Energieversorgung in der IT Umgebung, neue Wege beschreiten
- Dezentrale Stromversorgungssysteme
- Flachkabelsysteme „Dezentral Modular Steckbar“
- Integrierbare Bussysteme • Komplettlösungen: Am Beispiel einer Arbeitsplatzlösung gemäß DIN VDE 0100-410
- Alle Netze (NN, EDV, USV) jederzeit überall verfügbar. Konzepte am Beispiel eines Bussystems für das Schrankmanagement im Rechenzentrum

Peter Pardeyke, Dätwyler Cables GmbH

17:15 - 18:00 Uhr
Moderner Brandschutz bei IT-Verkabelung; Lösungen, Techniken und Gefahren
- MLAR - Richtlinie über brandschutztechnische Anforderungen an Leitungsanlagen
  - Schutzziele nach § 14 „Brandschutz“ und § 40 „Leitungsanlagen“ MBO • Definition „notwendige Treppenräume, notwendige Flure“ nach § 35 und 36 MBO
  - Möglichkeiten der Verlegung von Leitungsanlagen in notwendigen Fluren / Treppenräumen nach MLAR
- Kabelschottungen nach DIN 4102 Teil 9
  - Baurechtliche Vorgaben nach MBO und MLAR
  - Allgemeine Bauaufsichtliche Zulassung, was steht drin?
  - Verschiedene Systeme, Vor- und Nachteile
  - Vermeidbare Fehler bei der Ausführung

Michael Ulman, TÜV SÜD Industrie Service GmbH

ab 18:00 Uhr Happy Hour

Dienstag, den 18.05.2010

9:00 - 10:30 Uhr
Konzeption, Aufbau, Realisierung von Erdungssystemen unter Berücksichtigung von EMV, LEMP- und HPEM-Störschutzzonen; moderne und sichere Erdungssysteme und Störschutzzonen planen und errichten
- Netzformen nach VDE 0100 und Bedeutung der TN-S-Netzform
- Die Erdungsanlage: Grundlagen, Grenzwerte (Ciritical Facility), Frequenzen, Retrofit, Erdungswiderstand, Beispiele
- Übergang von LPZ 1/SSZ1 nach LPZ 2/SSZ2 (Störschutzzonenübergang) und Schirmdämpfungsmessung an den Übergängen
- Schutz einer Kabeltrasse
- Induktion im Rechenzentrum
- LEMP/HPEM-Schutz von baulichen Anlagen mit elektrischen und elektronischen Systemen in der praktischen Ausführung am Beispiel vom Flughafen Paderborn und Flughafen Siegerland

Dipl.-Ing. Bernd Steinkühler, Beratender Ingenieur der Ingenieurkammer Bau NRW

10:30 - 11:00 Uhr Kaffeepause

11:00 - 11:45 Uhr
ITIL und dessen Bedeutung für den Betrieb einer Kommunikationsverkabelung
Dipl.-Ing. Hartmut Kell, ComConsult Beratung und Planung GmbH

11:45 - 12:45 Uhr
Pro- und Kontra-Diskussion: Einsatz von MPO-Techniken im Rechenzentrum, Vor- und Nachteile?
- Was bedeutet MPO-Technologie
- Welche Vorteile, welche Nachteile, wann für wen geeignet
- Zwei Hersteller nehmen Position
- Podiumsdiskussion

Dipl.-Ing. Thorsten Punke, Tyco electronics, Dipl.-Ing. Heinz Wollenweber, Leoni Kerpen GmbH

12:45 - 14:00 Uhr Mittagspause

14:00 - 15:00 Uhr
Leistungsexplosion Virtualisierter Systeme und Konsequenzen für Netze und Verkabelung
- Leistungsexplosion Virtualisierter Systeme durch SR-IOV
- Netzwerkstrukturierung mit (Multi-) 40/100 GbE
- Entwicklungsstand bei 40- und 100 GbE, 16/32 FC, QDR-IB sowie Terabit-ISL
- 40/100-fähige LWL-Verkabelung
- 40/100-fähige Kupferverkabelung

Dr. Franz-Joachim Kauffels, Unternehmensberater

15:00 - 16:00 Uhr
Pro- und Kontra-Diskussion: Zukunftssicherheit durch Glasfaser bis zum Arbeitsplatz, Illusion oder Realität
- Grundsätzliche Methodik bei Glasfasertechnik im Tertiärbereich
- Lösungsvarianten Fiber to the Desk und Fiber to the Office
- Technologievergleich mit Kupfer
- Einsatzszenarien für und gegen Glasfaser

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

16:15 Uhr Ende der Veranstaltung

Zweitthema

IP Version 6 - das Internet der nächsten Generation (Teil 2)

Fortsetzung von Seite 1

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

Autokonfiguration wird über die so genannte „Nachbarerkennung“ implementiert. Dies hat folgende Vorteile:

- **Leichte Änderbarkeit,** indem die Station bei einer Adressänderung (z.B. neue Adapterkarte) ein so genanntes Nachbar Update als Multicast an alle Hosts / Knoten und Router sendet.
- **Höhere Effektivität:** Den intervallmäßig gesendeten Router Updates (Advertisements) kann eine Station alle erforderlichen Konfigurationis-Parameter entnehmen (Netzteil der Adresse, Präfixe, MTU).
- **Sicherheit:** Der Router wird automatisch gefunden, der ARP Request an den Router entfällt. Fehlen ein oder mehrere Präfixe im Router Advertisement, so kann die Station nicht direkt kommunizieren und muss den Router für die Kommunikation benutzen (indirect Routing).
- **Fehlertoleranz:** Endgeräte können den für sie zuständigen Router auf Erreichbarkeit prüfen und im Fehlerfall einen Backup Router finden.

Die **Nachbarerkennung** beinhaltet neun Funktionen / Dienste, die nachfolgend kurz erläutert werden.

1. **Router Discovery (NDP):** Die Station wartet auf eines der periodisch gesendeten Router Advertisements oder macht sich mit dem Neighbor Discovery Protokoll auf die Suche d.h. sendet eine **Router Solicitation Nachricht**. So „findet“ sie alle Router, die am lokalen Link angebunden sind und baut eine Liste von Default Routern auf. Das NDP basiert auf ICMPv6. Eine Blockierung aller ICMPv6 Pakete (analog zur heutigen Praxis, alle ICMPv4 Pakete auszufiltern) wird daher im Normalfall nicht praktikabel sein.
2. **Präfix Discovery:** Die Station lernt die Adress-Präfixe, die festlegen, welche Adressen Link-lokal (im selben Subnetz) oder über einen Router anzusprechen sind. Hierzu wertet sie ein Router Advertisement aus oder fordert per Router Solicitation eines an.
3. **Parameter Discovery:** Über Warten / Anfordern werden die notwendigen IP-Parameter wie MTU oder Hop Limit gelernt.
4. **Adress-Autokonfiguration:** Wird nicht automatisch die MAC-Adresse als Hostadresse (Interface-Adresse) verwendet, so kann eine Adresse angefordert werden. Hierfür spricht die Station z.B. einen DHCP Server an, der nach dem bekannten Request/Response Protokoll dem Endgerät seine Adresse sendet.
5. **Next Hop Bestimmung:** Anhand der gelernten Präfixe erkennt die Station, für welche Zieladressen sie einen Router ansprechen muss. Diesen wählt sie aus der Default Router Liste aus. Die entsprechende Router-IP-Adresse speichert sie in einem Cache.
6. **Adress-Resolution:** Ein IP Host kann die Link-Adresse (im LAN: MAC-Adresse) einer Peer Station im selben Subnetz mit der sogenannten Neighbor Solicitation anfordern und somit lernen (Auswerten des Neighbor Advertisement, das als Antwort gesendet wird). Die Adress-Resolution wird durch das NDP geleistet, welches das ARP Protokoll der IPv4-Welt ablöst.
7. **Entdecken der Nichterreichbarkeit:** Durch Senden einer Neighbor Solicitation Anfrage kann eine Station überprüfen, ob die Zielstation (im selben Subnetz) oder der Zielrouter noch erreichbar sind.
8. **Entdecken einer Adress-Duplizierung (DAD):** Über eine Neighbor Solicitation Nachricht kann abgefragt werden, ob die eigene autokonfigurierte Adresse schon vorhanden ist.
9. **Redirect:** Ein Router kann einer Station mit einer Redirect Nachricht die Adresse eines anderen Routers mitteilen, der für eine bestimmte Zielstation (=Zieladresse) besser geeignet ist. Ein Redirect kann der angesprochenen Station auch mitteilen, dass die Adresse des Zielpartners Link-lokal ist und demzufolge gar kein Router zu benutzen ist.

Für die Nachbarerkennung und alle damit zusammenhängenden Funktionen werden verschiedene **Caches** und **Listen** aufgebaut, die für die weitere Kommunikation benutzt und gepflegt werden.

Im **Nachbar-Cache** tragen Stationen die Link-lokalen Adressen ein, mit denen zuletzt kommuniziert wurde. Hierzu gehören Flags für Typ (Station, Router), Erreichbarkeit, Status, Anzahl unbeantworteter Anfragen, Timer für die nächste Überprüfung etc. Dieser Cache ist erkennbar aufwändiger (Speicher, CPU) als der unter IPv4 geführte ARP-Cache.

Im **Empfänger-Cache** tragen Stationen die Link-lokalen und globalen Adressen ein, mit denen zuletzt kommuniziert wurde. Diese Adressen werden, soweit nötig, auf den nächsten Link-lokalen Router gemappt. Ebenso werden Redirect Nachrichten in den Cache eingepflegt. Zwischen Empfänger-Cache und Nachbar-Cache gibt es einen Abgleich.

In die **Präfix-Liste** werden alle gelernten Präfixe ein getragen, anhand derer Adressen als Link-lokal oder global klassifiziert werden.

IP Version 6 - das Internet der nächsten Generation (Teil 2)

In die **Router-Liste** trägt eine Station analog die gelernten Adressen der Link-lokalen Router ein, die die sie zur Kommunikation benutzen kann. Zu diesen Eintragungen werden Erreichbarkeits-Informationen aus dem Nachbar-Cache in der Liste mitgeführt.

Auf der Basis der Nachbarerkennungs-Funktionen / -Dienste erfolgt die Autokonfiguration in insgesamt neun Schritten:

1. **Automatische Konfiguration** der eigenen IP-Adresse, alternativ über zustandsfreie / zustands-abhängige (stateful / stateless) Konfigurations-Anforderung: Die **zustandsfreie** d.h. **Autokonfiguration** erfolgt durch Auswerten oder Anfordern von Router Advertisements, d.h. Empfang/Senden der Multicast-Gruppe FF02::1 (alle Knoten, alle Router) und Kombination mit der eigenen MAC-Adresse. Zur initialen Kommunikation mit dem Router weist sich der IP Host eine Link-lokale Adresse zu, die z.B. aus der Hardware-Adresse (d.h. MAC Adresse) berechnet werden kann, sofern ein Ethernet NIC vorhanden ist. Diese Konfiguration wird als **stateless** bezeichnet, weil praktisch nirgendwo „Buch geführt wird“, welches Endgerät sich welche Adresse gegeben hat. Alternativ zur Autokonfiguration kann die Station als zustandsabhängige Konfiguration eine Host-Adresse über DHCP anfordern (siehe Unterpunkt 3.2)
2. **Überprüfung** der Adresse auf **Eindeutigkeit** durch Abfrage / Senden einer Solicitation Nachricht; jeder IP Host muss die Duplicate Adress Detection (DAD) durchführen, wenn er sich per Autokonfiguration eine IP Adresse ausgewählt hat. Die DAD findet automatisch mittels NDP statt ohne dass der Benutzer hier aktiv werden muss.
3. **Lernen der Link-lokalen Router** bzw. ihrer IP-Adressen über die Router Discovery
4. **Lernen der Präfixe** der Link-lokalen Stationen (des eigenen Subnetzes) über die Präfix Discovery; Router können bei der Präfix-Mitteilung endliche Gültigkeitszeiten mitteilen (valid lifetime, preferred lifetime). Innerhalb der Valid Lifetime darf der IP Host das mitgeteilte Präfix zur Kommunikation verwenden, innerhalb der Preferred Lifetime soll er es einem Präfix vorziehen, dessen Lifetime abgelaufen ist. Die Verlängerung der Gültigkeitszeiten erfolgt automatisch durch die Router Advertisements.
5. **Erfragen der Link-lokalen MTU und des Hop Limit** über die Parameter Discovery
6. **Lernen der Link-Adressen von IPv6-Partnern**, die Link-lokal sind und deren IPv6-Adresse bekannt ist, über die Adress-Resolution
7. **Lernen des nächsten Routers** für nicht Link-lokale Zielpartner über die Präfix Discovery und Next Hop Bestimmung
8. **Überprüfen der Erreichbarkeit** gewünschter Zielpartner über die Neighbor Solicitation
9. **Auswerten von Redirect** Nachrichten und somit Optimierung der Kommunikationswege.

3.2 DHCP und DNS

DHCP

Autokonfiguration macht die IP Adresse typischerweise abhängig von der MAC-Adresse sprich NIC Hardware. Aus Gründen der Flexibilität und Hardware-Unabhängigkeit (weltweit überall dieselbe IPv6 Adresse, auch bei Nutzung unterschiedlicher Zugangstechnologien wie WLAN, WiMax, Ethernet) kann dies unerwünscht sein. Ein weiterer Nachteil der Autokonfiguration ist die Nutzung / Lieferung der Hardware (MAC) Adresse anstelle von sprechenden Namen für PTR bei reverse DNS. Eine flexible Alternative für beide Probleme bietet hier der Einsatz von DHCPv6.

Anstelle von Autokonfiguration kann die Station eine Host-Adresse über DHCP anfordern: Diese **zustandsabhängige Konfiguration** findet statt, wenn kein Router vorhanden ist oder das Router Advertisement besagt, dass zustandsfreie Autokonfiguration aus Sicherheitsgründen nicht erwünscht ist. In diesem Fall wird über den Multicast FF02::1:0 der nächste DHCP Server gefunden und eine komplette Adresse von diesem Server angefordert. Diese Konfiguration unterscheidet sich prinzipiell von der stateless Autokonfiguration: Sie wird als **stateful** bezeichnet, weil der DHCP Server darüber „Buch führt“, welchem Endgerät er welche Adresse gegeben hat.

Die Autokonfiguration ist zwar wunderschön, liefert dem Endgerät aber keine Informationen über Hostnamen, Domänennamen, DNS Server, NTP Server, TFTP Server etc. Ein Hauptproblem liegt darin, dass das Endgerät bei der Autokonfiguration keine DNS Server Adresse lernt. Diese Adresse mag zwar einigermaßen stabil sein, aber das Endgerät hat trotzdem ein Problem, den DNS Server respektive seine korrekte IP Adresse zu finden und zu konfigurieren. Zur Abhilfe für dieses Problem wurden einige Lösungen vorgeschlagen, darunter Multicast, Anycast und: der Einsatz eines DHCPv6 Servers.

Daher kann trotz stateless Autokonfiguration zusätzlich ein DHCPv6 Server zum Einsatz kommen. Das NDP (Neighbor Discovery Protokoll) kann sogar explizit auf die Möglichkeit einer weitergehenden Konfiguration durch DHCPv6 verweisen. Der DHCPv6 Server liefert den Endgeräten in diesem Fall die gewünschten Zusatz-Informationen, kümmert sich aber nicht um die Adressvergabe. Die Kombination von Autokonfiguration mit DHCPv6 wird als „**stateless DHCPv6**“ bezeichnet (RFC 3736).

DNS

Fällt es dem Otto-Normal-Verbraucher schon schwer, sich IPv4 Adressen zu merken, die dezimal codiert und nur 4 Byte lang sind, so hat er mit IPv6 bei einer Adresslänge von 16 Byte und Hexcodierung ganz verloren. Für Nutzer und Betreiber wird es daher noch wichtiger, DNS als funktionierendes Namenssystem zur Verfügung zu haben.

Der DNS Dienst

DNS besteht aus einer Reihe von Funktionen und Diensten, die ein zuverlässiges Mapping beziehungsweise eine Übersetzung von Namen (FQDNs) in Adressen (IPv4, IPv6) und vice versa leisten. Zusätzlich bietet DNS Funktionen zur Unterstützung spezieller Anwendungen (MX für das Routen von E-Mail, ISATAP, NAT-PT).

Die Implementierung von DNS läuft auf Namensservern (Master Server, Slave Server, verteilte Namens-Datenbank), die untereinander und mit den anfragenden Clients kommunizieren. Der DNS-Agent im Client heißt Resolver. Seine Anfragen (Query Requests) lauten entweder auf Forward oder Reverse Domänennamen-Suche. Forward Lookup übersetzt den angefragten Namen in eine IP Adresse, Reverse Lookup liefert einen Namen für eine angefragte IP Adresse. Letzteres ist insbesondere für Management-, Sicherheits- und Debugging Tools wichtig.

Zur Nutzung von DNS für IPv6 wurde in RFC 3596 als Ressourcentyp (RR) ein Quad-A Record (AAAA) für DNS-Abfragen definiert. Der AAAA Record löst genau wie der A Record einen Namen in eine IPv6 Adresse auf (Forward Lookup). Die Auflösung einer IPv6 Adresse in einen Namen (reverse Lookup) nutzt nach wie vor den PTR Record Typ, der ebenfalls neu definiert wurde. Allerdings ist die Reverse Domäne

IP Version 6 - das Internet der nächsten Generation (Teil 2)

jetzt nicht mehr IN-ADDR.ARPA (IPv4) sondern IP6.ARPA. Subdomänen werden nicht mehr an 8-Bit-Grenzen sondern an 4-Bit-Grenzen delegiert.

Auch das so genannte dynamische DNS, bei dem die Endgeräte ihren Namen selbst im DNS eintragen, kann die IPv6 Autokonfiguration sinnvoll ergänzen.

DNS hat in RFC 3484 für die Auswahl des genutzten Protokolls eine Default Policy Tabelle, nach der die Nutzung von IPv6 gegenüber IPv4 bevorzugt wird, wenn ein Endgerät / eine Verbindung beide Protokolle unterstützt. Hierdurch entsteht ein Risiko, wenn einer Portalseite ein A- und ein AAAA Record zugewiesen wird: Mit IPv6 tauchen plötzlich neue Namen auf, da IPv6 ja bevorzugt genutzt wird (z.B. ipv6.google.com). Mit der Angabe des Namens wählt der Benutzer im Prinzip schon das zugehörige Protokoll. Im Regelfall ist aber auch im Browser einstellbar, welches Protokoll bevorzugt oder ausschließlich genutzt wird. Im weltweiten Web unterstützen sieben von dreizehn Root Namensservern und mindestens zwei Namensserver der meisten Top-Level Domänen bereits IPv6.

Um eine korrekte Funktionsweise des DNS zu sicherzustellen, muss dem Informationsfluss zwischen Server und Clients besondere Beachtung gewidmet werden. Insbesondere ist hierbei wichtig, dass es keine „feste“ Beziehung zwischen den Recordtypen in der Datenbank (A-Record für IPv4 und AAAA-Record für IPv6 Adressen) und dem zur Übertragung genutzten Protokoll gibt: Das unterliegende genutzte IP Protokoll ist unabhängig von den übertragenen Informationen. Das heißt insbesondere, dass ein Endgerät über IPv4 bei einem Namensserver AAAA-Records anfragen kann. Natürlich gilt das auch umgekehrt (Anfrage von A-Records über IPv6). Typisch für die aktuelle Migrations-Situation ist es, IPv6 Datenbank-Informationen zu speichern, diese aber mit IPv4 Kommunikation anzufragen und abzurufen. Diese Praxis hat den großen Vorteil, dass die Software vorhandener Namensserver nur sehr geringe Änderungen benötigt, was erheblich zur Beibehaltung der vorhandenen Stabilität des Internet beiträgt. Andererseits entsteht dadurch der Nachteil, dass die Endgeräte typischerweise einen IPv4 Protokollstack benötigen, um mit dem DNS zu kommunizieren, selbst wenn sie anwendungstechnisch schon IPv6 unterstützen und nutzen. Sofern aus technischen oder strategischen Gründen kein Dual Stack eingesetzt werden soll, muss hier ein wesentlich komplexeres System von Resolvern und Namensservern implementiert werden.

4. Migrationswege von IPv4 nach IPv6

Trotz aller Pushfaktoren aus dem öffentlichen Bereich wird sich die Migration hin zu IPv6 eher als Evolution denn als Revolution vollziehen. Für eine Übergangszeit werden im Regelfall beide Protokolle parallel im Einsatz sein. Allein aufgrund der riesigen installierten IPv4 Basis wird kein Hersteller, der einen radikalen Wechsel ohne diesen Parallelbetrieb voraussetzt, seine Produkte de facto verkaufen können. Daher gibt es aktuell so gut wie keine Geräte, die ausschließlich IPv6 und kein IPv4 mehr unterstützen.

Für die Migration sind verschiedene Komponententypen zu betrachten:

- IPv4-only: Komponente, die IPv4-fähig ist, aber kein IPv6 unterstützt
- IPv6-only: Komponente, die IPv6 unterstützt, aber nicht mehr IPv4-fähig ist
- IPv4/v6: Komponente, die IPv4 und IPv6 unterstützt

Eine IPv4/v6 Komponente kann eine Dual IP Layer Architektur haben, d.h. IPv4 und IPv6 sind parallel implementiert (siehe Abbildung 4.1), die TCP/UDP Schicht setzt sowohl auf IPv4 als auch auf IPv6 auf. Der Next Generation TCP/IP Stack in Windows Server 2008 und Windows Vista hat die Dual IP Layer Architektur implementiert. Eine ältere Alternative zur Dual Layer Architektur ist der Dual Stack (siehe Abbildung 4.2). Hier ist der komplette IP/UDP/TCP Stack zweimal implementiert, einmal mit IPv4 und einmal mit IPv6. Windows Server 2003 und Windows XP verwenden Dual Stack. Beide Varianten: Dual Layer und Dual Stack können IPv4, IPv6 und üblicherweise IPv6-over-IPv4 Pakete generieren. Da beide Varianten sich nach außen gleich verhalten, verwendet dieser Artikel nachfolgend einheitlich den Begriff Dual Stack.

Geräte, die nur IPv4 und kein IPv6 unterstützen, benötigen eine irgendwie geartete Verbindung und Übersetzung zwischen der alten IPv4-Welt und der neuen IPv6-Welt, die IPv4 Pakete in IPv6 Pakete umwandelt. Für den Übergang von IPv4 nach IPv6 stehen verschiedene Möglichkeiten zur Verfügung:

- Dual Stack
- Tunnelverfahren
  - Tunnel Broker
  - 6in4
  - 6over4
  - ISATAP
- Translation / Gateway
  - 6to4 Translation (Gateway-Einsatz)
  - Teredo (NAT-T)
  - Stateless IP/ICMP Translator (SIIT)
  - Transport Relay Translator

Die wichtigsten Verfahren sind Dual Stack, manuell konfigurierte Tunnel und dynamische ISATAP Tunnel. Translation Verfahren / Gateway-Komponenten) haben eine deutlich geringere Verbreitung.

RFCs, die die IPv4 → IPv6 Migration behandeln, sind in Abbildung 4.3 zusammengestellt.

Dual Stack
Dual Stack Router und Server oder Endgeräte / Hosts haben beide Stacks IPv4 und IPv6 implementiert, ähnlich wie früher in der Multiprotokolltechnik IP, DECnet, IPX und AppleTalk. Die Dual Stack Funktionalität ist in RFC 4213 beschrieben. Ein Gerät mit Dual Stack Implementierung kann Pakete aus beiden Welten handhaben, so können beide Protokolle in einem gemeinsamen Netzwerk koexistieren. Dual Stack ist die ideale Implementierung für

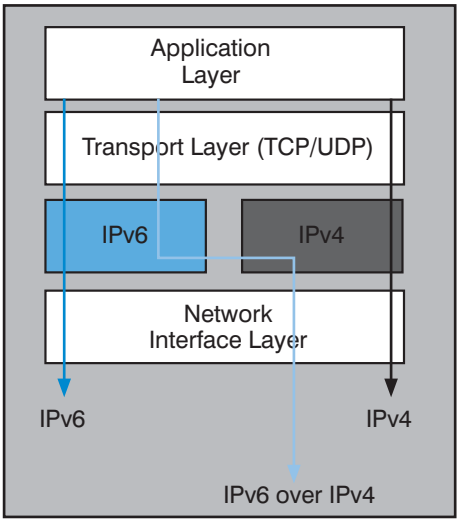


Abbildung 4.1: Komponente mit Dual IP Layer und Paketgenerierung

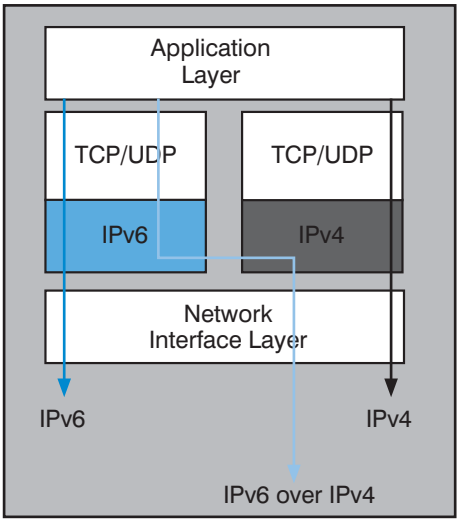


Abbildung 4.2: Komponente mit Dual Stack und Paketgenerierung

IP Version 6 - das Internet der nächsten Generation (Teil 2)

RFC 4213	Basic Transition Mechanisms for IPv6 Hosts and Routers (obsoletes RFC 2893)
RFC 4966	Reasons to Move the Network Address Translator – Protocol Translator (NAT-PT) to Historic Status (obsoletes RFC 2766 NAT-PT)
RFC 2185	Routing Aspects of IPv6 Transition
RFC 3493	Basic Socket Interface Extensions for IPv6
RFC 3056	Connection of IPv6 Domains via IPv4 Clouds
RFC 4380	Teredo: Tunneling IPv6 over UDP through Network Address Translations NATs
RFC 4214	Intra-Site Automatic Tunnel Addressing Protocol ISATAP
RFC 3053	IPv6 Tunnel Broker
RFC 3142	An IPv6-to-IPv4 Transport Relay Translator

Abbildung 4.3: RFCs für die IPv4 → IPv6 Migration

eine Migrationsphase, in der in allen Subnetzen schon neue IPv6 Geräte aber auch noch herkömmliche IPv4 Geräte betrieben werden (siehe Abbildungen 4.4 und 4.5). Jede Dual-Stack Komponente kann dann mit anderen Kommunikationspartnern das Protokoll nutzen, das diese implementiert haben. Haben beide Kommunikationspartner einen Dual Stack, wird vorzugsweise IPv6 verwendet. Es ist leicht nachvollziehbar, dass die Dual Stack Implementierung erhöhte Anforderungen an Speicherplatz und CPU-Leistung stellt, insbesondere für Router und deren Routing Tabellen. Außerdem erfordert Dual Stack den Zugang zu einem IPv6 DNS Server.

Laufen die Server und Router mit Dual Stack, können die Endgeräte als Single Stack entweder IPv4 oder IPv6 fahren, was in den Endgeräten die Komplexität reduziert (siehe Abbildung 4.6). Nutzen die Endgeräte jedoch Peer-to-Peer An-

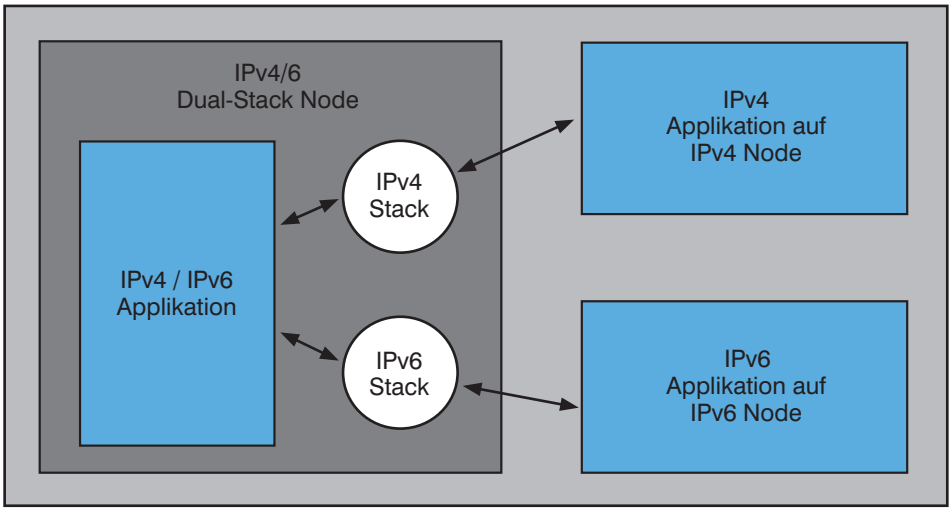


Abbildung 4.4: Dual Stack Implementierung für IPv4 und IPv6

wendungen wie Telefonie oder Video über IP, so müssen sie bei einem vorhandenen Implementierungs-Mix ebenfalls als Dual Stack betrieben werden, ansonsten sind nur jeweils IPv4 Peers und IPv6 Peers untereinander kommunikationsfähig.

Beide Stacks können voneinander vollkommen unabhängig oder als so genannte Hybrid-Implementierung laufen. In den aktuellen Server- und Endgeräte-Produkten ist üblicherweise die hybride Variante implementiert. Typischerweise wird der Code so programmiert, dass er transparent für IPv6 und IPv4 arbeitet, die Sockets sind so designed, dass sie sowohl IPv4 als auch IPv6 Pakete handhaben können. Im Fall von IPv4 Kommunikation nutzen hybride Stacks im Regelfall intern IPv6 Semantik und stellen IPv4 Adressen in einem besonderen IPv6-Format dar, dem IPv4-gemappten Adressformat, das unter dem Punkt „IPv6 Adressierung“ in Teil 1 (Netzwerk Insider vom Februar 2010) beschrieben wurde.

Tunnelverfahren

Um Router, die kein IPv6 unterstützen, auf dem Weg zu einem IPv6 Netzwerk nutzen zu können, gibt es verschiedenste Tunnelverfahren. Dabei werden die IPv6 Pakete als Nutzlast in andere Protokolle eingepackt (meistens in IPv4) und bis zu einem Punkt getunnelt, der sich am Übergang zwischen dem IPv4- und dem IPv6-Netzwerk befindet (siehe Abbildung 4.7). Dort wird die Nutzlast ausgepackt und als native IPv6 Paket ins IPv6-Netzwerk zum IPv6-fähigen Zielhost weitergeleitet. Der Rückweg funktioniert auf dieselbe Weise.

Der Betreiber des IPv4 Netzwerks kann bei einem so genannten Tunnel Broker (RFC 3053) eine IPv6 Gegenstelle beantragen, die fix ist und über den Tunnel immer denselben IPv6-Adressbereich zur Verfügung stellt.

Ein 6in4 Tunnel benutzt den Protokolltyp 41, um IPv6 in IPv4 „direkt“ einzupacken. Der 6to4 Tunnel benutzt well known IPv4 Anycast-Adressen, die im Internet mehrfach vergeben sind. Die getunnelten Pakete werden zum nächstgelegenen Router mit einer Anycast Adresse weitergeleitet und dort bearbeitet. Dieser Router hat einen IPv6 Adressbereich, der sich aus seiner öffentlichen IPv4 Adresse berechnet. Ein solcher Tunnel ließe sich auch auf einer Linux-Maschine mit öffentlicher IPv4 Adresse einrichten.

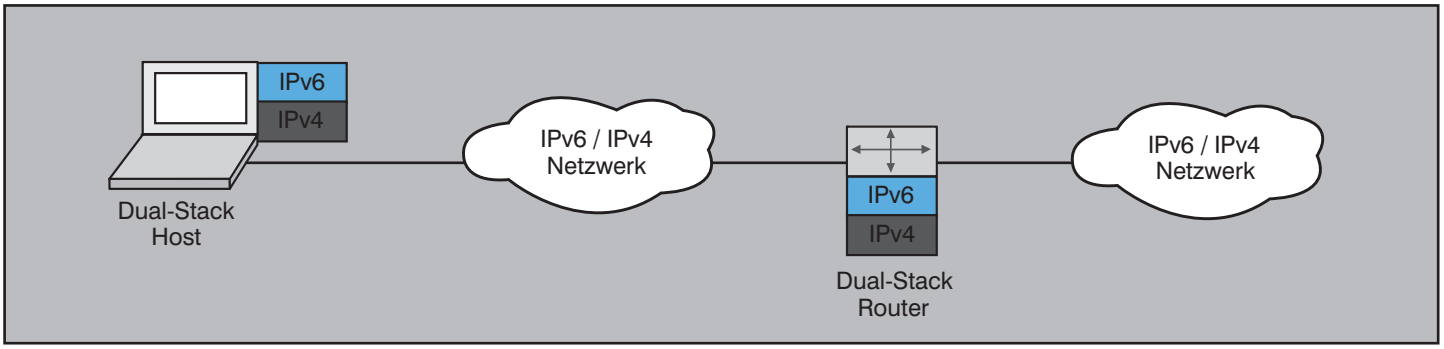


Abbildung 4.5: Einsatzszenario mit durchgehendem Mischbetrieb IPv4 und IPv6

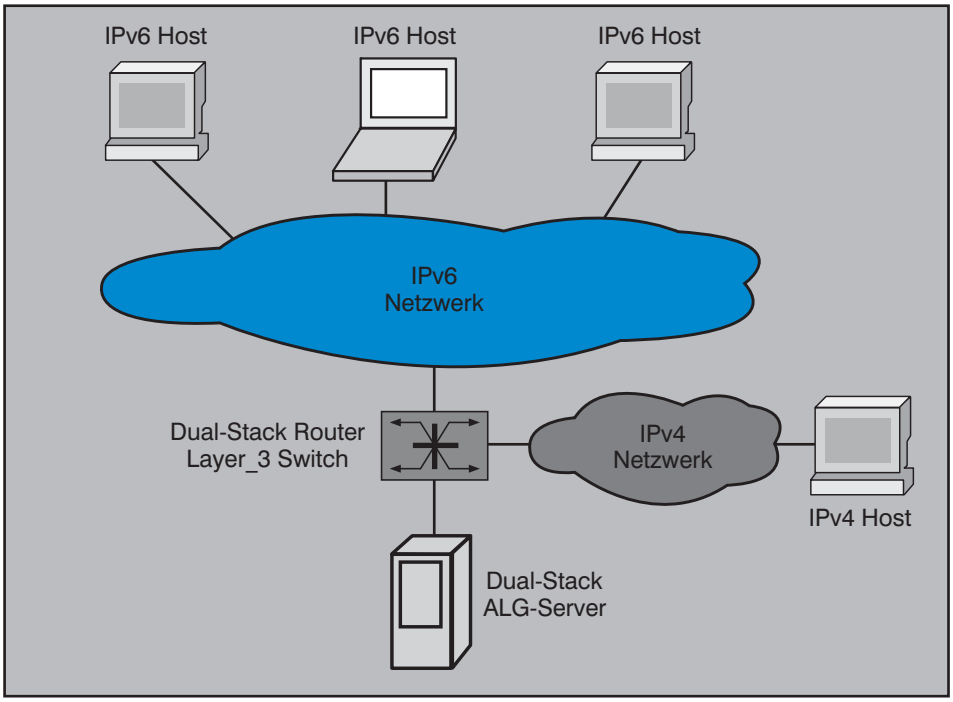


Abbildung 4.6: Einsatzszenario mit Dual Stack Implementierung für Router und Server

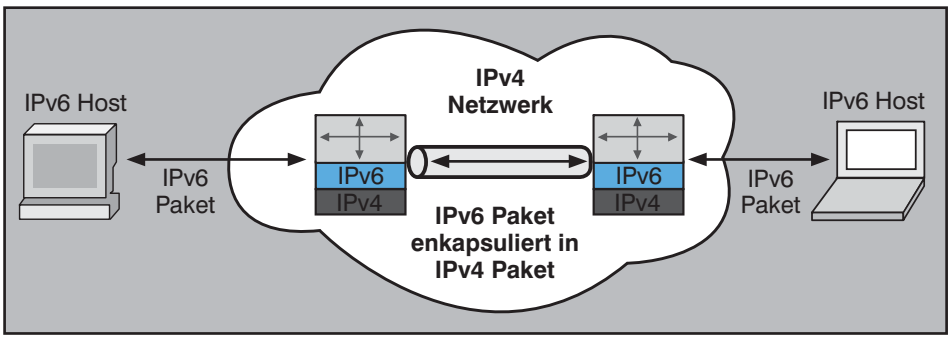


Abbildung 4.7: Verbindung von IPv6 Teilnetzen über IPv4 Tunneling

Manuell konfigurierte Tunnel
Sollen beispielsweise zwei IPv6-only Teilnetze über ein dazwischen liegenden IPv4-only Backbone verbunden werden, der noch nicht aufgerüstet ist oder mangels Funktionalität gar nicht nach IPv6 migriert werden kann, so werden die IPv6-Pakete im IPv4-Backbone in IPv4 enkapsuliert und über einen Tunnel zwischen den Übergangsroutern übertragen, wie in Abbildung 4.8 dargestellt. IPv4 Pakete werden weitergeleitet wie bisher. Die Übergangsrouter benötigen dann eine Dual Stack Funktionalität zur Handhabung beider Paketypen und zusätzlich die Funktion für En-/Dekapsulierung. Manuelle Tunnelkonfiguration ist eine von mehreren Tunnel-Möglichkeiten, die hauptsächlich eingesetzt wird, wenn eine stabile Verbindung zwischen zwei oder wenigen Peer-Punkten betrieben werden soll, die darüber hinaus mit IPsec zusätzlich gesichert und auch gegen Man-in-the-Middle Eingriffe geschützt werden kann. Manuelle Tunnel werden überwiegend zwischen Routern / Layer-3 Switches konfiguriert. Als Tunnelein- und -ausgang werden manuell IPv4 Adressen an den beteiligten Routern konfiguriert, von denen jeder am Interface in das jeweils angebundene IPv6 Netzwerk zusätzlich eine IPv6 Adresse erhält. Diese Methode ist für wenige Tunnel relativ leicht durchführbar, bedingt aber mit steigender Anzahl von Tunneln sowohl einen erhöhten Konfigurations-Aufwand als auch zunehmende Unübersichtlichkeit.

ISATAP Tunnel
Eine automatisierte Tunneltechnik ist das Intrasite Automatic Tunnel Addressing Protocol (ISATAP, RFC 4214), bei dem die Tunnel nicht statisch konfiguriert werden müssen. ISATAP Tunnel werden vorrangig zwischen IPv6-fähigen Endgeräten und Routern / Layer-3 Switches, seltener zu Endgeräten konfiguriert und unterstützen Unicast Anwendungen; ein Einsatzszenario zeigt Abbildung 4.9.

Der ISATAP Tunnel nutzt IPv4 Adressen am Endgerät und am ISATAP-fähigen Router. Das „Automatische“ an ISATAP ist, dass das Endgerät den Tunnel dynamisch einrichtet, wenn es ihn benötigt. Es kann zusätzlich die IPv4-Adresse des Routers dynamisch suchen und finden (z.B. durch DNS oder einen lokalen Eintrag). Ein ISATAP Tunnel transportiert IPv6 Pakete über eine mehr oder weniger ausgedehnte IPv4-only Netzwerk-Infrastruktur bis hin zu einem IPv6-fähigen Router oder Server/Endgerät mit Dual Stack. Innerhalb der IPv4 Netzwerk-Infrastruktur können IPv4 Anwendungen weiterhin IPv4 nutzen, während andere Anwendungen, die

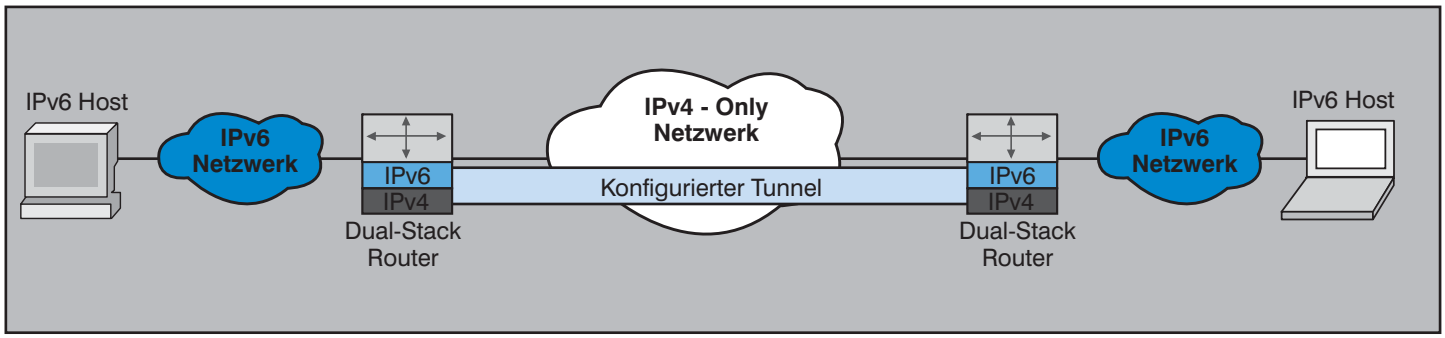


Abbildung 4.8: Verbindung von IPv6 Teilnetzen über einen IPv4 Backbone

IP Version 6 - das Internet der nächsten Generation (Teil 2)

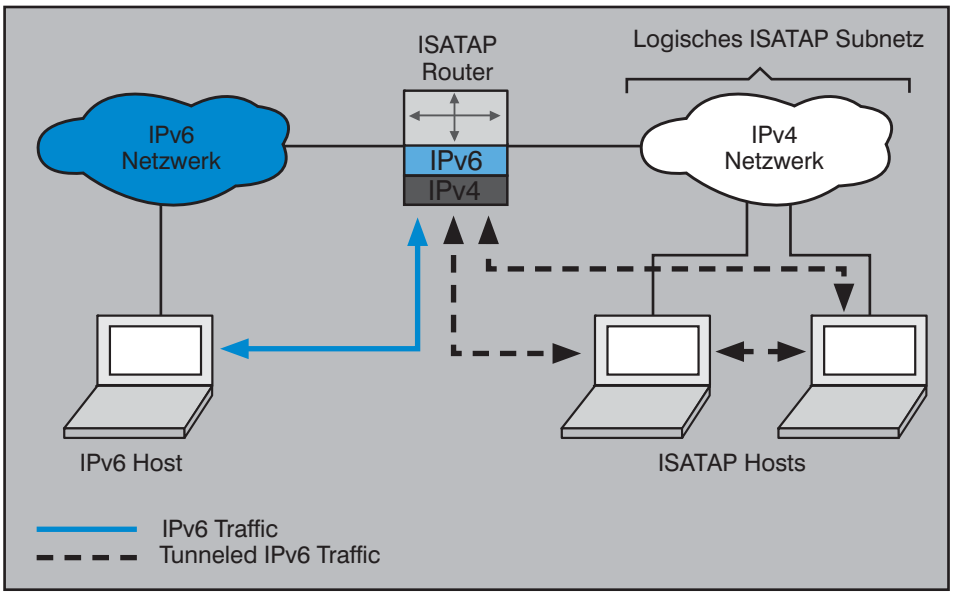


Abbildung 4.9: Nutzung von ISATAP Tunneln über eine IPv4 Netzwerk-Infrastruktur

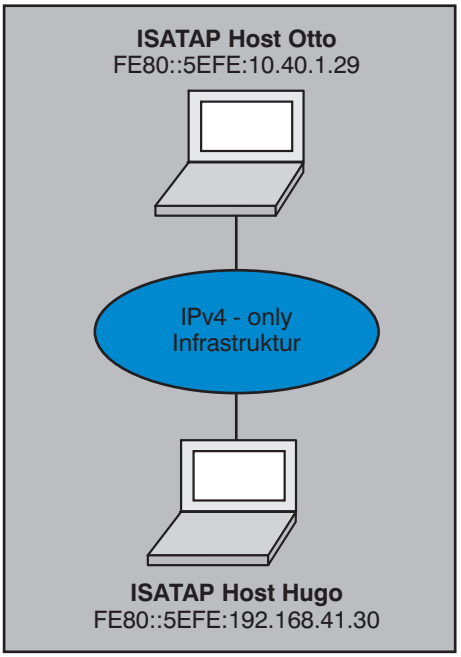


Abbildung 4.10: ISATAP Tunnel und Adressierung der Endgeräte

in - möglicherweise IPv6-only - Teilnetzen „hinter“ dem Dual Stack Router erreichbar sind, schon IPv6 verwenden. Anstelle mehrerer manueller Tunnel über die IPv4 Infrastruktur hinweg können ein einzelner oder besser zwei redundante ISATAP Router als zentraler Übergangspunkt zwischen IPv4- und IPv6-Netzwerk zum Einsatz kommen.

ISATAP Adressen nutzen die lokal administrierte Kennung ::0:5EFE:w.x.y.z, wobei w.x.y.z eine private IPv4 Unicast Adresse ist, oder ::200:5EFE:w.x.y.z, wenn w.x.y.z eine öffentliche IPv4 Unicast Adresse ist. Abbildung 4.10 zeigt ein ISATAP Szenario mit zwei IPv6 Endgeräten und entsprechenden Adressen. Die Tabelle in Abbildung 4.11 zeigt die dazu gehörigen und in IPv4- bzw. IPv6-Paketen verwendeten Adressen, in diesem Beispiel die Windows Default Einstellung mit dem Präfix FE80:: anstelle der ::0.

Ein ISATAP Einsatzszenario mit ISATAP-fähigem Router (siehe Abbildung 4.12) könnte so aussehen: Das ISATAP Endgerät schickt eine DNS Anfrage an den Namen ISATAP und erhält die Adresse eines ISATAP-fähigen Routers als Antwort. Es sendet nun eine Router Solicitation Nachricht an den ISATAP Router, der mit einer IPv4-enkapsulierten Unicast Router Advertisement Nachricht antwortet. Die Antwort enthält die Präfixe, die das Endgerät für die Autokonfiguration nutzen muss. Optional kann der Router natürlich sich selbst als Default Router bekanntgeben.

Beispiel: IPv4 und IPv6 Adressen für Link-lokale ISATAP Konnektivität	
Feld	**Wert**
IPv6 Source Adresse	FE80::5EFE:10.40.1.29
IPv6 Destination Adresse	FE80::5EFE:192.168.41.30
IPv4 Source Adresse	10.40.1.29
IPv4 Destination Adresse	192.168.41.30

Abbildung 4.11: ISATAP Mapping von IPv4 auf IPv6 Adressen

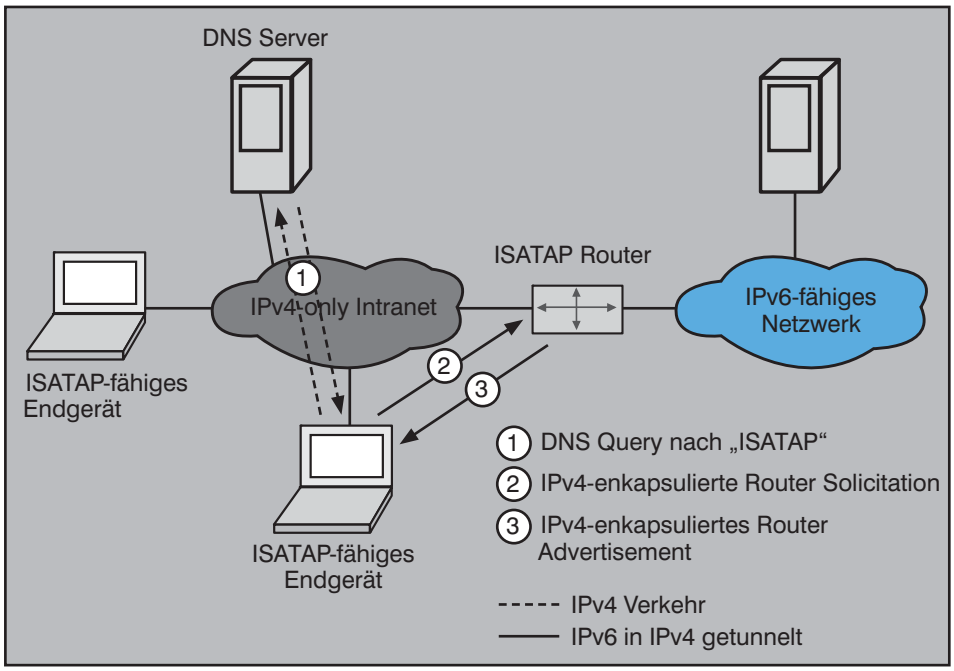


Abbildung 4.12: Aufbau eines ISATAP Tunnels

IP Version 6 - das Internet der nächsten Generation (Teil 2)

Translation (Gateway)
Unterstützt einer von beiden Kommunikationspartnern ausschließlich IPv4 und der andere ausschließlich IPv6, so funktioniert dies nur über eine Komponente in der Mitte, die IPv4 nach IPv6 übersetzt und umgekehrt (siehe Abbildung 4.13). Hierbei werden die Paketformate ineinander konvertiert (v4←→v6), darüber hinaus sind zusätzliche Aktionen wie SIIT zur Header-Konvertierung (Stateless IP-ICMP Translation) und NAT-PT (RFC 4966 Network Address Translation – Protocol Translation) erforderlich. Eine NAT-PT Komponente (im Regelfall ein Router / Layer-3 Switch) hält zu beiden Seiten eine eigene Verbindung inklusive der jeweiligen Zustandsinformationen und führt für jedes Paket eine Header- und Adresskonvertierung durch. Für die Paket-Konvertierung wird SIIT genutzt.

Der Transport Relay Translator arbeitet ähnlich wie NAT-PT, nur führt er die Konvertierung auf der Transportschicht durch.

Translation ist eine sehr aufwändige Technik, unterstützt nicht alle Funktionen von IPv6 und wird nicht von allen Netzwerk-Komponenten unterstützt. Diese Technik sollte daher nur als „last resort“ genutzt werden.

6to4
6to4 (RFC 3056) ist eine automatische Tunneltechnik, um IPv6 Teilnetze über eine IPv4 Infrastruktur miteinander zu verbinden. 6to4 behandelt das komplette IPv4 Netzwerk wie einen singulären Link. Es nutzt das globale Präfix 2002:WWXX:YYZZ:/48, bei dem WWXX:YYZZ die Hexadezimale Codierung einer öffentlichen IPv4 Adresse (w.x.y.z) eines Standorts oder eines Endgeräts ist. 6to4 Endgeräte bilden selbst keine IPv4 Tunnel für IPv6, dies ist Aufgabe der 6to4 Router. Sie sind die Schnittstelle zur IPv4 Infrastruktur, packen den native IPv6 Verkehr in IPv4/UDP ein, senden ihn bis zum 6to4 Zielrouter, der strippt IPv4/UDP ab, lässt das IPv6 Paket übrig und leitet es ins IPv6 Zielnetz weiter. Windows Server 2008 und Windows Vista unterstützen 6to4.

Teredo (Microsoft)
Teredo ist auch als IPv4 NAT Traversal (NAT-T) für IPv6 Hosts bekannt. Es leistet Adresszuweisung und automatische Tunnelbildung für IPv6 Endgeräte über öffentliche IPv4-Netzwerke hinweg, auch wenn die Verbindung ein oder mehrere NAT-Komponenten durchläuft. Um IPv4 NATs zu überwinden, sind die IPv6 Pakete als IPv4/UDP Datagramme verpackt. Teredo ist als „last resort“ für NAT Traversal gedacht und wird mehr und mehr durch 6to4 abgelöst werden.

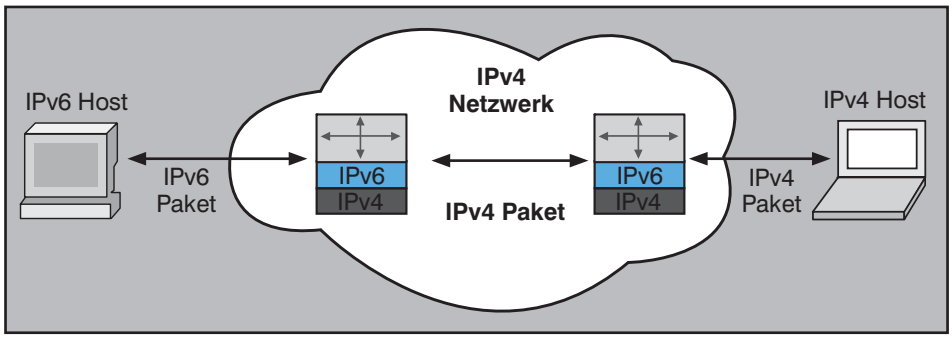


Abbildung 4.13: Verbindung von IPv4 und IPv6 Hosts mittels Translation

In Teil 3 dieses Artikels lesen Sie:
- was die Migration für Server, Endgeräte und Router bedeutet
- welche Alternativen für Standort-Designs möglich sind
- welche Kernfunktionen und Tools unterstützt werden sollten
- wo es mögliche mit IPv6 Probleme gibt
- wie sich der IPv6 Markt darstellt
- welches abschließende Fazit zu ziehen ist

Abkürzungen

ARP	Address Resolution Protocol
ARPA	Advanced Research Projects Agency
CPU	Central Processing Unit
DAD	Duplicate Address Detection
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
DoD	Department of Defense (USA)
FQDN	Fully Qualified Domain Name
ICMP	Internet Control Message Protocol (v4)
ICMPv6	Internet Control Message Protocol Version 6
IP	Internet Protocol
IPng	Next Generation Internet Protocol
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol
LAN	Local Area Network
MAC	Media Access Control
MLD	Multicast Listener Discovery
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NAT-PT	NAT Protocol Translator
NAT-T	NAT Traversal
NDP	Neighbor Discovery Protocol
NTP	Network Time Protocol
PIM-DM	PIM Dense Mode
PIM-SM	PIM Sparse Mode
PMTU	Path MTU
PTR	Pointer
RFC	Request for Comments
RIPE	Réseaux IP Européens
RR	Resource Record
SIIT	Stateless IP/ICMP Translator
SOHO	Small Office Home Office
Telnet	Teletype Network
TFTP	Trivial File Transfer Protocol (TCP/IP)
UDP	User Datagram Protocol
UNH	University of New Hampshire

Wenn Wissen für Sie wichtig ist

Effizienter und besser Lernen mit ComConsult-Study.tv!

Bis zum 15. April startet ComConsult-Study.tv eine Sonderaktion für Käufer des Jahresabos.

ComConsult-Study.tv basiert auf den neuesten Erkenntnissen der Lernforschung. Es macht Lernen effizienter und erhöht den Lernerfolg:

- Es ist auf den Bedarf ausgewählter Zielgruppen optimiert
- Es ist individuell, selektiv und zeitoptimiert
- Es vermittelt Wissen bis zu 30% schneller und bis zu 40% besser

Wer gewinnt durch ComConsult-Study.tv?
ComConsult-Study.tv hat als Kernzielgruppen Führungskräfte, IT-Spezialisten und IT-Einsteiger. Für jede dieser Zielgruppen wird eigenes und optimiertes Lernmaterial angeboten.

Welchen speziellen Bedarf haben diese Zielgruppen?
Führungskräfte und IT-Spezialisten sind häufig in der Situation, dass sie selektiv und in möglichst kurzer Zeit Informationen zu Detailthemen benötigen. Einsteiger brauchen die Möglichkeit, sich auf Schulungen vorbereiten und nach einem Seminar Themen gezielt und effizient wiederholen zu können.

Was macht ComConsult-Study.tv?
ComConsult-Study.tv basiert im Kern auf einer Bibliothek von HD-Schulungsvideos, die mit anderen Lernmedien kombiniert werden. Diese HD-Videos sind in der Regel 20 bis 30 Minuten lang und decken einzeln oder in Kombination mehrerer Videos wichtige Themen ab. Die Teilnehmer wählen die Themen nach Bedarf und Umfang.

Was bedeutet individuelles, selektives und zeitoptimiertes Lernen?
Die Teilnehmer bauen ihr Lernprogramm aus den angebotenen HD-Video-Modulen individuell und selektiv nach ihrem aktuellen Bedarf zusammen. Die Videos werden auf den Arbeitsplatz-PC geladen und sind lokal verfügbar, wann und wie lange die Teilnehmer Zeit haben.

Warum ist der Lernerfolg bis zu 30% schneller und 40% besser?
Die Lernoptimierung entsteht durch die Kombination verschiedener Lernmedien

und durch die Selektivität. ComConsult-Study.tv ist so aufgebaut, dass die Module sowohl eigenständig sind als auch die Standard-Veranstaltungen der ComConsult Akademie ergänzen. Die ComConsult Akademie baut deshalb ihre Seminare und Kongresse stufenweise so um, dass eine optimal gestaltete Kombination aus HD-Videos, Seminaren/Kongressen und Textmaterialien gegeben ist. Die Teilnehmer haben damit die Möglichkeit, sich gezielt auf die Veranstaltungen vorzubereiten und nach den Seminaren und Kongressen das Gelernte selektiv und bedarfsorientiert mit HD-Videos nachzubearbeiten. Diese Lernphasen in Kombination mit dem Mix aus Medien sind die Basis für einen deutlich erhöhten Lernerfolg. Sie lernen schneller und behalten den Stoff besser.

Kommen auch neue Kommunikations-Technologien zum Einsatz?
Traditionelle eLearning-Konzepte bieten häufig keinen persönlichen Kontakt zum Trainer und auch keine Möglichkeit, Fragen zu stellen und zu diskutieren. ComConsult-Study.tv beinhaltet deshalb „Meet the trainer“ Webkonferenzen und ein eigenes Diskussions-Forum.

Wo finde ich ComConsult-Study.tv?
Auf dem Webserver www.comconsult-study.tv werden die HD-Videos ausgewählt. Eine von uns bereitgestellt Software wird auf dem Arbeitsplatz-PC installiert und verwaltet die zu bearbeitenden Videos. Die Teilnehmer können Bookmarks in die Videos setzen, Notizen machen und ihre individuelle Lernbibliothek zusammenstellen.

Was kostet ComConsult-Study.tv?
Die einzelnen Elemente von ComConsult-Study.tv sind unterschiedlich gepreist. Die HD-Videobibliothek kostet im Abo für alle Module pro Jahr 398 Euro für die Einzelbenutzer-Lizenz. Daneben werden komplette HD-Seminare zu Themen angeboten, die besonders für diese Art von Training geeignet sind (zum Beispiel Software-Schulungen). Diese werden getrennt gepreist. Die Kombination aus HD-Material und den Veranstaltungen der ComConsult Akademie wird durch die ComConsult Akademie angeboten.

Wie erfahre ich noch mehr?
Auf www.comconsult-study.tv liegt unser kostenloses Informations-Video „Wenn Wissen für Sie wichtig ist“, das das gesamte Konzept inklusive der angebotenen Lernmodelle noch einmal im Detail erläutert. Weitere Informationen für die Spezialisten in den Weiterbildungsabteilungen finden sich in unserem White-Paper: „Effizienter und besser Lernen in der IT“, das Sie unter folgendem Link finden:
www.comconsult-study.tv/de/bonusmaterial/whitepaper/index.html

Kennenlern-Aktion
bis zum
15.04.2010

Bei Buchung eines Jahres-Abos (398,-- € zzgl. MwSt.) erhalten Sie den brandneuen Technologie-Report von Dr. Franz-Joachim Kauffels „Netzwerk-Redesign 2010: Neue Anforderungen, Technologien und Strukturen“ (Listenpreis 249,-- Euro) kostenlos!

Registrieren Sie sich jetzt!
www.comconsult-study.tv

Schwerpunktthema

Virtualisierung: Virtual Desktop Infrastructure - steht das Rechenzentrum vor dem Kollaps?

Dipl.-Inform. Matthias Egerland hat an der RWTH Aachen Informatik studiert und ist seit 2005 Mitarbeiter der ComConsult Beratung und Planung GmbH. Er ist Leiter des Competence Centers Virtuelle IT und arbeitet als Berater in den Competence Centern IT-Sicherheit und Netze. Neben den Schwerpunkten Desktop-, Server- und Infrastruktur-Virtualisierung beschäftigt sich Herr Egerland insbesondere mit der Sicherheit in virtualisierten Umgebungen.

Jonas Goede ist Berater bei der ComConsult Beratung und Planung GmbH. Dort ist er in den Bereichen Virtuelle IT und Data Center tätig. Neben diesbezüglichen Praxiserfahrungen ist er spezialisiert auf die Planung und Durchführung von Testszenarien im Bereich Virtual Desktop Infrastructure Lösungen.

Fortsetzung von Seite 1

1. Einführung in die Desktopvirtualisierung

Nachdem in den letzten Jahren viele Firmen und Anwender die Servervirtualisierung erfolgreich eingesetzt haben, verstärkt sich zunehmend der Trend, auch andere Bereiche der IT in den Fokus der Virtualisierung zu nehmen. Bei der Desktopvirtualisierung sollen bekannte Konzepte der Virtualisierung von Servern und Speicher, auf Arbeitsplatzrechner (Clients) übertragen werden. Arbeitsplatzrechner werden traditionell mit lokal installiertem Betriebssystem und lokal installierten Anwendungen betrieben. Oftmals haben große Teile der Anwender in einer Firma neben dem identischen Betriebssystem auch noch viele ähnliche Anwendungen im Einsatz. Hierin liegt das Optimierungspotential: Zusammenfassen gleichartiger Bestandteile zu einer gemeinsam genutzten Ressource. Da aber Arbeitsplatzrechner (Desktops) - je nach Arbeitsanforderung - höchst individuell gestaltet sein können, liegt in der Wahrung dieser Einzigartigkeit die zusätzliche Herausforderung der Desktopvirtualisierung.

1.1 Komponenten einer Virtual Desktop Infrastructure

Der Grundaufbau einer Virtual Desktop Infrastructure ist bei allen marktüblichen Lösungen gleich. Auf der einen Seite stehen Server, die für den Betrieb der virtuellen Desktop Hard- und Software sorgen, die so genannte „Hosting-Infrastruktur“. Auf der anderen Seite stellen Server die Inhalte (Betriebssystem und Anwendungs-Software) den virtuellen Desktops dynamisch bereit. Daneben gibt es noch Komponenten, die den Zugriff auf die virtuellen und physischen Maschinen steuern. Auf diesen Servern laufen spezielle Tools, die für vorbereitende Maßnahmen und den laufenden Betrieb notwendig sind. Außerdem ermöglichen Konsolen und Managementwerkzeuge in zentralen Bereichen die Administration der Komponenten.

Für das grundlegende Hosting von virtuellen Desktops kann ein sogenannter Hypervisor eingesetzt werden, wie er auch aus der Servervirtualisierung bekannt ist. Jeder virtuelle Desktop arbeitet damit genau wie jede andere virtuelle Maschine in einer für ihn abgeschlossenen Umgebung, ohne dabei in Konflikt mit den Hardwarezugriffen der anderen virtuellen Maschinen zu geraten.

Um die virtuellen Desktops, die auf dem Hypervisor laufen, dynamisch mit Software zu versorgen, wird ein so genannter Provisionierungsserver eingesetzt. Dieser sorgt für die Bereitstellung des Betriebssystems und der Applikationen, indem er diese aus vorkonfektionierten Images bezieht. Eine Imagedatei dient dann als Softwarebasis für eine Vielzahl von virtuell laufenden Desktops auf dem Hypervisor.

Wenn ein Endgerät Zugriff auf einen solchen virtuellen Desktop benötigt, stellt es eine Anfrage an einen speziellen Server, den so genannten „Connection Broker“. Dieser Server fragt seinerseits beim Hypervisor nach, ob eine passende virtuelle Maschine für diesen Zweck zur Verfügung gestellt werden kann. Ist eine entsprechende VM vorrätig, stellt der Hypervisor eine direkte Verbindung zwischen anfragendem Endgerät und der virtuellen Maschine her, auf die dann der Provisionierungsserver das passende Betriebssystem-Image lädt. Ist eine solche VM nicht verfügbar, veranlasst der Connection Broker den Hypervisor, eine solche zu starten. Die Übertragung zwischen Client und virtuellem Desktop wird anschließend über spezielle Protokolle (RDP, ICA, PCoIP) abgewickelt und läuft ohne die Zwischenschaltung des Connection Brokers. Abbildung 1 zeigt die schematische Darstellung einer Virtual Desktop Infrastructure.

1.2 Hardwareszenarien

Die Anforderungen auf Nutzerseite sowie die Implementierungsvariante haben Auswirkungen auf die Hardware sowohl Server- als auch Endgeräte-seitig.

Bei ThinClient-Lösungen greift eine leistungsreduzierte Hardware auf die Server der Virtual Desktop Infrastruktur zu. Diese

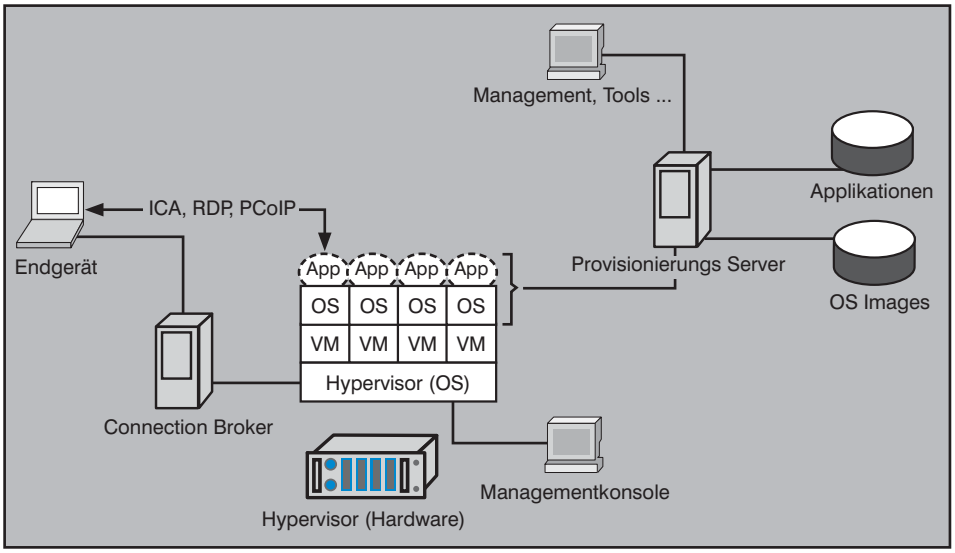


Abbildung 1: Schematische Darstellung einer Virtual Desktop Infrastructure

senden dann meist nur den Bildschirminhalt an eben diesen ThinClient, welcher wiederum die Benutzereingaben zurückgibt. Alternativ können je nach Hardwareausstattung auch Software/Betriebssystem Pakete an diese Geräte gestreamt werden, um sie lokal auf dem Desktop auszuführen und damit die Server im Rechenzentrum zu entlasten und mobiles Arbeiten zu ermöglichen (s. Modelle zur Desktopbereitstellung in Abschnitt 1.3).

Anstelle von ThinClients können BladePCs eingesetzt werden, die über eine Bildschirm- und Eingabe-Verlängerung mit dem Benutzer verbunden sind. Ein BladePC wird im Rechenzentrum auf eigener Hardware betrieben und fungiert dort als eigenständige Maschine. Somit ist diese Lösung physikalisch unabhängig von anderen Systemen und kann gezielt für einen Benutzer seine komplette Rechenleistung zur Verfügung stellen. Diese Art der Desktopbereitstellung wird oft dann gewählt, wenn ein User (oder eine kleine Gruppe von Usern) im Gegensatz zum überwiegenden Anteil der sonstigen Benutzer eine außergewöhnlich hohe Rechenleistung für sich allein beansprucht. Hier wären z.B. CAD Arbeitsplätze zu nennen, die mit hohen Anforderungen an die Grafikleistungen alle „normalen“ Arbeitsplätze übersteigen. Ohne weitere Mechanismen findet eine Virtualisierung im eigentlichen Sinne somit nicht statt. Der Desktop-PC wurde lediglich in Form des Blade-PCs in das Rechenzentrum verlagert.

Im folgenden Abschnitt werden die verschiedenen Möglichkeiten aufgezeigt, diese Virtuellen Umgebungen mit dem Benutzer zu verbinden, sprich die Desktops bereitzustellen.

1.3 Modelle zur Desktopbereitstellung

Generell ist es bei allen Benutzertypen das vorrangige Ziel, den Desktop nicht mehr auf lokalen Maschinen zu betreiben, sondern den Betrieb ins zentrale Rechenzentrum zu verlagern. Welche Konzepte zur Virtualisierung dort eingesetzt werden und wie der Benutzer Zugriff auf seinen Desktop erhält, ist je nach Anforderung unterschiedlich lösbar.

Bei der Applikationsvirtualisierung – auch Anwendungs- oder Softwarevirtualisierung genannt, handelt es sich nicht um eine komplette Virtualisierung des Desktops. Es werden lediglich einzelne Anwendungen virtualisiert. Diese Software läuft dann entweder auf einem entfernten Server und kann dort von mehreren Clients gleichzeitig genutzt werden (Terminal Server). Alternativ erhält jeder Benutzer seine Anwendungen zur lokalen Ausführung per Netzwerkstream auf seinen Client. Hierbei kann entweder die gesamte Anwendung übertragen werden, oder nur der Teil der Software, der gerade genutzt wird. Bei der Komplettübertragung der Software entsteht zunächst zwar eine höhere Netzwerklast als bei einer Teilübertragung, jedoch kann die Applikation danach komplett ohne Netzwerkanbindung betrieben werden (Offline-Fähigkeit).

Ähnlich wird auch die Verbindung zu einem komplett virtualisierten Desktop bereitgestellt. Entweder erhält der Anwender einen Netzwerkstream mit einem (Teil)Paket zur lokalen Ausführung oder ihm wird nur der Bildschirminhalt übertragen und er sendet seinerseits die Benutzereingaben zurück. Je nach Methode muss das Endgerät des Benutzers unterschiedliche Fähigkeiten beherrschen. Reicht bei einer reinen Bildübertragung eine relativ geringe Rechenleistung aus, werden bei der Streaming-Methode dem Client wortwörtlich mehr Aufgaben „übertragen“. Abbildung 2 zeigt das Modell eines gestreamten Desktops.

Um neben der reinen Bildübertragung weitere Interaktionen zwischen Client und Server vornehmen zu können, spielt das Übertragungsprotokoll eine sehr große Rolle. Es muss beispielsweise zusätzlich für die Verbindung von Druckern mit PCs Methoden bereitstellen, damit diese Geräte nicht nur dem lokalen Gerät bekannt sind, sondern auch bis zur virtuellen Maschine „durchgereicht“ werden. Ähnlich verhält es sich z.B. bei USB Geräten. Der folgende Abschnitt gibt einen Einblick in die Leistungsfähigkeit solcher Protokolle.

1.4 Übertragungsprotokolle

1.4.1 Remote Desktop Protocol (RDP)

Das Remote Desktop Protocol (RDP) wurde von Microsoft mit dem Ziel entwickelt, die Grafikausgabe eines entfernten Computers auf dem lokalen Bildschirm darzustellen und so beispielsweise entfernte Server im Rechenzentrum zu administrieren. Mit fast jedem neuen Microsoft Desktop- oder Serverbetriebssystem wurde RDP weiterentwickelt und mit neuen

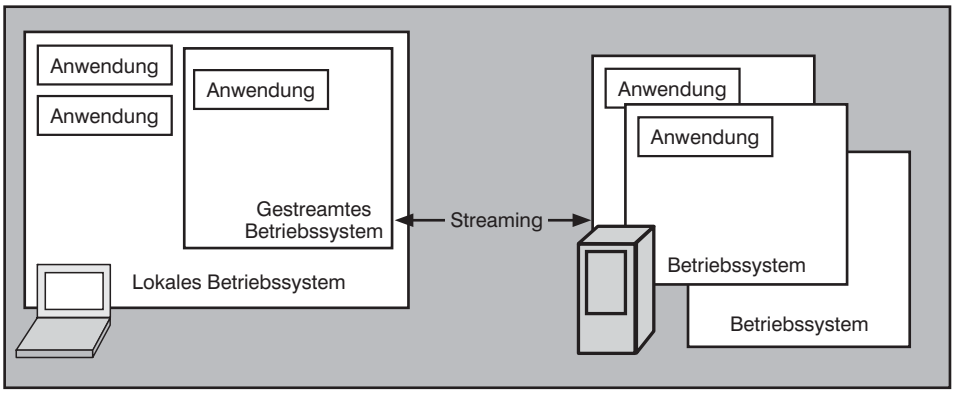


Abbildung 2: Modell Desktopstreaming

Funktionen ausgestattet. Je nach Funktionsumfang lassen sich lokale Drucker und lokale Laufwerke in die Session einbinden. Auch die Audioausgabe kann vom entfernten Host per RDP zum Client durchgereicht werden. Die neueste RDP-Version (7.0) unterstützt auch bidirektionale Audioübertragung, also auch den Soundeingang von Endgerät an den Host, was für Softphone-Applikationen essentiell ist.

Da RDP für Remotezugriff in lokalen Netzen konzipiert wurde, wird jedoch auch mit der aktuellen Version keine Technik für den Ausgleich von geringer Bandbreite oder Bandbreitenschwankungen implementiert, wie es für WAN Umgebungen typisch ist.

Für den Einsatz einer vollständig funktionalen Desktopvirtualisierung reicht es jedoch nicht mehr aus, nur den Bildschirminhalt leistungsgerecht zu übertragen und eine gleichbleibende Qualität der Darstellung zu bieten. Die viel zitierte „User Experience“ im Zusammenhang mit dieser neuen Art, Computerarbeitsplätze bereitzustellen, hängt von der Zusammensetzung vieler Faktoren ab. Das Übertragungsprotokoll muss weitere Funktionen übernehmen, wie z.B. die Verarbeitung von Multimediainhalten oder die Unterstützung spezieller Peripheriegeräte wie SmartCard-Reader. So selbstverständlich, wie diese Hardware bei lokalen Endgeräten erkannt und verwendet werden kann, so schwierig kann deren Bereitstellung bei virtuellen Desktops ausfallen. Schließlich muss jegliche Kommunikation zwischen der Hardware und den Gerätetreibern über das Netzwerkprotokoll transportiert werden. Sowohl die Anbieter von VDI-Lösungen als auch die Hersteller von ThinClients arbeiten mit Hochdruck an der Anpassung und Erweiterung ihrer Software in diesem Bereich.

1.4.2 Independent Computing Architecture (ICA)

Die Independent Computing Architecture (ICA) von Citrix spezifiziert eine Datenübertragung zwischen Server und Client, die im Gegensatz zu RDP auch über WAN-Verbindungen gute Ergebnisse liefert. Mit dem Einstieg von Citrix in die Desktopvirtualisierung wurde das ICA Protokoll durch HDX-Funktionen (High Definition user eXperience) erweitert. Diese Erweiterung besteht aus mehreren einzelnen Bausteinen, die einerseits den Problemen schwankender Bandbreite begegnen und anderseits Funktionalitäten für eine bessere Integration von lokalen Peripheriegeräten sowie zur Darstellung von Multimediainhalten in eine Virtual Desktop Infrastructure liefern.

Das ICA-Protokoll bietet außerdem die Option, die Qualität des Bildschirminhaltes stufenweise herunterzusetzen, vergleichbar mit der Kompression bei einem Video durch einen entsprechenden Codec. Als zusätzliche Qualitätssicherungsmaßnahme bietet HDX ein sogenanntes „client-side bitmap caching“. Hierbei werden Bildschirminhalte eine gewisse Zeit lang auf dem Endgerät gepuffert, wodurch beispielsweise ein schnelleres Zurückscrollen in Dokumenten ermöglicht wird.

Speziell bei der Übertragung von Flash(videos) wirbt Citrix massiv mit einer Funktion, die so nicht bei anderen Herstellern zu finden ist: Das Protokoll erkennt die Flashinhalte im Backend und sendet den Flash-Inhalt als Datei über das Netz an den Client, damit dieser die Inhalte mit seiner Rechenleistung lokal berechnet. Da es sich hier aber ausschließlich um die Sonderbehandlung von Flash handelt, fällt dieses Alleinstellungsmerkmal nur bei eben diesen Inhalten ins Gewicht. Außerdem gibt es zu bedenken, dass hierfür der Client über den entsprechenden Software-Codec und die Hardware-Leistung verfügen muss, um diesen Vorteil gegenüber anderen Protokollen auch wirklich ausspielen zu können. Webanwendungen setzen eine Vielzahl unterschiedlicher Medienformate ein, so dass die Sonderbehandlung von Flash nicht für eine generelle Beschleunigung von Multimediainhalten führen muss.

1.4.3 PC-over-IP (PCoIP)

VMware hat in seine VDI Lösung View 4 eine zugekaufte Übertragungstechnik integriert, die das ursprüngliche RDP ersetzt: PC-over-IP (PCoIP). PCoIP der Firma Terradici war zunächst eine Übertragungstechnik, die in Form von Hardware-Chips implementiert war. In VMware View 4 steht nun eine Softwarelösung von PCoIP bereit, die laut VMware eine vergleichbare Performance wie die Chip-Variante bieten soll.

VMware verfolgt bei der Bildschirmübertragung im Gegensatz zu Citrix den Ansatz, stets eine verlustfreie Darstellung des Bildschirminhaltes zu gewährleisten. Bei niedriger Bandbreite wird das Bild in einzelnen Auflösungsstufen verbessert, um letztendlich verlustfrei dargestellt zu werden. Es wird ganz bewusst mit dieser Art der Darstellung gearbeitet, da VMware laut eigenen Angaben die verlustfreie Darstellung als ein wesentliches Merkmal einer positiven „User Experience“ betrachtet.

Es wird deutlich, dass bei beiden Herangehensweisen die verfügbare Bandbreite eine Rolle spielt. Sollte die Bandbreite zu gering für den Citrix-Ansatz werden, wird entsprechend an der Bildqualität gespart. Bei VMware bzw. PCoIP wird in einer solchen Situation die Iteration der Bildschirmqualität entsprechend langsamer.

2. Netzwerkbandbreite

Einerseits muss für eine maximale Nutzerakzeptanz der komplette Desktop inklusive aller Funktionalitäten und Schnittstellen bereitgestellt werden. Andererseits führen die hierfür erforderlichen Ergänzungen im Übertragungsprotokoll auf der Netzwerkseite zu einer nicht unerheblich höheren Auslastung. Werden ThinClients, wie oben beschrieben, mit Teilen ihres Betriebssystems und ihrer Software per Netzwerkstreaming versorgt, sind hiermit hohe Übertragungsvolumina verbunden. Selbst eine Anbindung der Desktops per Bildübertragung von den virtuellen Maschinen, wo per Definition eben keine komplette Software durch das Netz gestreamt werden muss, bedeutet während der Verbindungszeit nicht unbedingt eine geringere Auslastung. Letztlich ist der Bildschirminhalt und seine Änderungsfrequenz dafür maßgeblich, welche Bandbreite für seine Übertragung zur Verfügung stehen muss, um überhaupt sinnvoll arbeiten zu können.

In heutigen lokalen Netzwerken liegen die Standardbandbreiten bei mind. 1 Gbit/s im Backbone und 100 Mbit/s bis zu den Endgeräten, was für die Desktopvirtualisierung völlig ausreicht. Im WAN liegen die Bandbreiten mit wenigen Mbit/s jedoch deutlich niedriger, so dass die Anbindung von externen Niederlassungen über eine WAN-Verbindung eine nicht zu unterschätzende Herausforderung bei der Umstellung auf VDI bedeuten kann. Neben der Bandbreite die im WAN nicht zuletzt einen wesentlichen, Kostenfaktor darstellt, spielt hier auch das Übertragungsvolumen eine Rolle.

Diesen Herausforderungen begegnen die VDI-Anbieter, wie in Abschnitt 1.4 dargestellt, in unterschiedlicher Weise mit den Mechanismen der von ihnen verwendeten Übertragungsprotokolle. Für die Dimensionierung einer VDI und der ihr zugrunde liegenden Netzwerkinfrastruktur ist die resultierende Bandbreite pro virtuellem Desktop unter Berücksichtigung eines passenden Lastprofils relevant. Die folgenden Abschnitte zeigen die Ergebnisse der Bandbreitenmessungen unter den Lastprofilen „Geschäftsanwendungen“ und „Multimedia-Inhalte“.

2.1 Lastprofil: Geschäftsanwendungen

In den folgenden Messungen, die vom Testcenter Miercom stammen, wird deutlich, in welcher Form Citrix XenDesktop 4 und VMware View 4 Bandbreite beanspruchen. Beim Start der Session wird von beiden Lösungen die höchste Netzwerklast erzeugt. Im Verlauf der Übertragung wird im Vergleich dazu das Netz nur noch sehr geringfügig belastet. Die dargestellten Bandbreiten basieren auf einem Standard Desktop Nutzungsprofil für Office-Anwendungen, welches mit beiden Übertragungstechniken (ICA und PCoIP) transportiert wurde. (siehe Abbildung 3)

In diesen Messungen wird ein unterschiedlicher, durchschnittlicher Bandbreitenbedarf deutlich. Citrix benötigt mit dem ICA Protokoll im Testzeitraum von 10 Minuten durchschnittlich 0,377 Mbps. Die höhere Anfangsnetzlast von PCoIP hingegen wirkt sich auch auf den Mittelwert über den gesamten Testzeitraum aus. So ergibt sich hier ein Wert von 1,029 Mbps im Durchschnitt. Hieraus resultiert der von Miercom plakativ vermittelte Unterschied von 64%.

Auf den ersten Blick scheint dies gewaltig, doch ob aus diesen Mittelwerten aus einer Testumgebung eine generelle Aussage über den „Bandbreitenhunger“ in natürlichen Netzwerkumgebungen ableitbar ist, kann anhand dieser Werte nur gemutmaßt werden. Die Studie kommt zu dem Ergebnis, dass durch die geringere Belastung des Netzes durch das ICA Protokoll mehr Platz für zusätzliche Benutzer (über die gleiche Leitung) bleibt, als dies bei View 4 mit PCoIP der Fall wäre.

Die genauen in diesem Szenario von den einzelnen Protokollen erforderlichen Bandbreiten können jedoch nicht pauschalisiert werden, da sie stark vom Nutzungsprofil auf dem virtuellen Desktop abhängt. Für eine Grobeinschätzung der „Verbrauchswerte“ und vor allem dem Lastprofil dieser beiden Protokolle liefern die Grafiken aber einen ersten Eindruck. Es zeigt sich, dass Lastspitzen beim Verbindungsaufbau auftreten. Diese sind mit geeigneten Übertragungstechniken im Netzwerkbereich bzw. im Backend sicherzustellen. Insbesondere für Spitzenzeiten, in denen sich viele Benutzer an der VDI anmelden, müssen entsprechende Leistungen vorgehalten bzw. eingeplant werden.

2.2 Lastprofil: Multimedia-Inhalte

Eine weitere Messung veranschaulicht den unterschiedlichen Ansatz der beiden Hersteller speziell bei Flashinhalten, die über die Leitung zum Endgerät gesendet werden müssen. Wie bereits erwähnt, überträgt ICA mittels HDX den Flashinhalt als Datei zum Client, wo er dann lokal gerendert wird. Dies bedingt natürlich eine entsprechende Hardware Unterstützung auf der Client-Seite, was im Extremfall einen ThinClient mit FatClient-Eigenschaften erfordert. Dies würde mindestens die Energieeffizienz am Front-End stark in Frage stellen.

Der Ansatz von VMware mit PCoIP führt hingegen zu einer konstanten Netzwerkbelastung: Alle Inhalte werden im Backend gerendert und der aktuelle Bildschirminhalt wird zum Endgerät übertragen - unabhängig davon, ob es sich um einfache Bildschirmseiten oder Multimediainhalte handelt. Die Auswirkungen auf den Bandbreitenbedarf dieser beiden Lösungsansätze ist in Abbildung 4 dargestellt.

Wie zu erwarten war, kann der Ansatz von Citrix auf die gesamte Messdauer zwar den besseren Durchschnittswert liefern (3,008 Mbps), jedoch benötigen beide Protokolle zu Beginn der Übertragung in etwa die gleiche Bandbreite (ca. 50 Mbps). Natürlich führt PCoIP mit der Methode, jeden neuen Bildschirminhalt - wenn auch komprimiert - über das Netz zu senden, zu einem deutlich höheren Durchschnittswert von 29,04 Mbps.

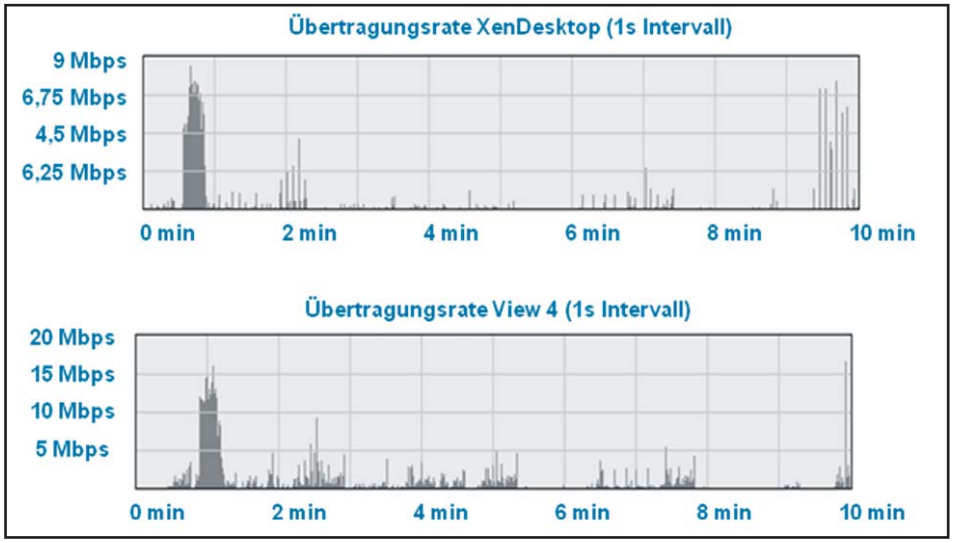


Abbildung 3: Bandbreitenbedarf eines einzelnen virtuellen Desktops mit dem Workload-Profil von Geschäftsanwendungen
Quelle: Miercom

[1] Miercom „Lab Testing Summary Report, VDI: Citrix XenDesktop 4 vs. VMware View 4“; http://www.miercom.com/dl.html?fid=20100207&type=report

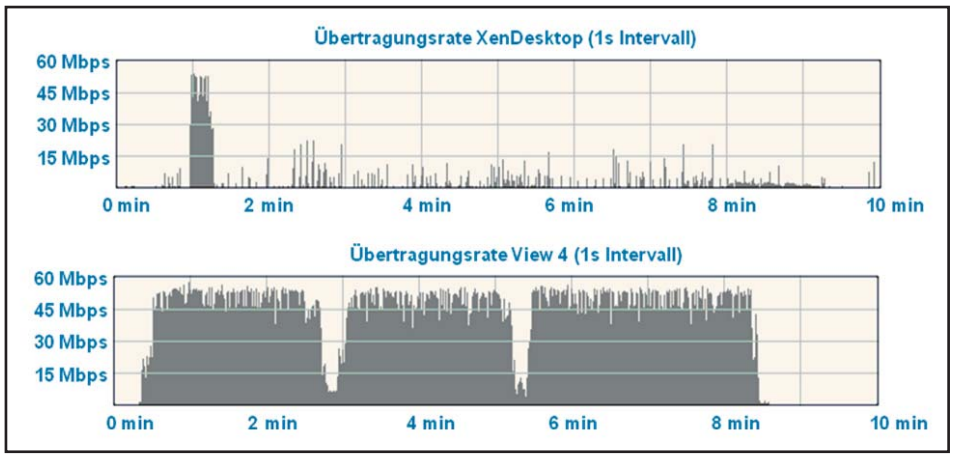


Abbildung 4: Bandbreitenbedarf eines einzelnen virtuellen Desktops mit dem Workload-Profil von Multimediaanwendungen in Form von Flash-Animationen Quelle: Miercom

Es wäre jedoch fatal, diesen Unterschied von beinahe einem Faktor 10 in die Dimensionierung der Infrastruktur einfließen zu lassen:

Einerseits fällt der gemessene Durchschnittswert besser für das Citrix ICA-Protokoll aus, je länger der Messzeitraum dauert. Andererseits ist der Konstruktionsvorteil des ICA-Protokolls auf die Übertragung von Flash-Inhalten begrenzt. Sobald auf dem Desktop ein anderes Multimedia-Format (z.B. Quicktime o.ä.) eingesetzt wird, sieht die Lastkurve des ICA-Protokolls genauso aus, wie diejenige von PCoIP. Ist darauf die Infrastruktur nicht vorbereitet, bricht sie zusammen.

3. Auswirkungen im Rechenzentrum

Das Rechenzentrum stellt den Kern einer Virtual Desktop Infrastruktur dar: Hier laufen alle Kommunikationswege zusammen. Im Speichersystem liegen die Master-Images der virtualisierten Betriebssysteme und Anwendungen. Die aus der Servervirtualisierung bekannten Hypervisor Citrix XenServer, Microsoft Hyper-V oder VMware ESX hosten im Rechenzentrum die virtuellen Desktops. Die Virtualisierung sorgt dafür, dass die Hardware-Ressourcen eines solchen Serversystems von allen gehosteten Desktops gemeinsam genutzt werden.

3.1 Anzahl virtueller Desktops pro Host-System

Entscheidend für die Auswirkung der Desktop-Virtualisierung auf die RZ-Infrastruktur ist daher die Frage, wie viele virtuelle Desktops auf einem einzelnen Serversystem gehostet werden. Hier überbieten sich die Hersteller in regelmäßigen Abständen mit neuen Rekorden. Waren es Anfang 2009 noch 30 virtuelle Desktops pro Host, wurden bald Tests mit 130 Desktops veröffentlicht. Zuletzt wurde das Gerücht von „5000 virtuellen Desktops auf einem physischen System“[2] gestreut.

Diese letzte Ankündigung kann jedoch schnell als Marketing-Blase entlarvt werden. Schaut man sich das dazugehörige Whitepaper von Citrix an, erkennt man „nur“ 3312 virtuelle Desktops und mit dem „einen physischen System“ ist lediglich der Provisionierungsserver gemeint. Die Desktop-Hosting-Infrastruktur besteht in Wirklichkeit aus insgesamt 93 Blade-Servern!

Der Erfolg eines jeden Virtualisierungsvorhabens hängt maßgeblich von der Akzeptanz der Benutzer ab. So ist es weniger entscheidend, immer neue Rekorde auf einer Teilkomponente der VDI aufzustellen. Dass diese Rekorde stets unter einem als „typisch“ definierten Lastprofil erzielt werden, steigert die Praxistauglichkeit solcher Tests dabei nur bedingt. Letztlich ist für die Benutzerzufriedenheit das Verhalten des Gesamtsystems im Vergleich zu seinem ursprünglichen lokalen Desktop der Bewertungsmaßstab. Wenn der ThinClient zum Booten seines lokalen Betriebssystems schon länger braucht als früher der Startvorgang des kompletten Windows-Systems dauerte, wird schon einiges an Überzeugungskraft erforderlich sein, diesen Benutzer von den Vorzügen der neuen Technologie zu überzeugen.

Citrix hat in einem Whitepaper Anfang 2009 die Anzahl virtueller Desktops auf einem Host-System mit der Benutzerzufriedenheit korreliert. Auf der Basis eines HP ProLiant DL585 Servers mit 4 Dual-Core 2.80 GHz AMD Opteron Prozessoren und 64 GB RAM sank die Benutzerzufriedenheit spätestens nach 30 virtuellen Desktops pro Host in den inakzeptablen Bereich[3].

In einem aktuelleren Citrix Whitepaper[4] vom Anfang 2010 dient ein Dell PowerEdge r710 Server mit 2 Quad-Core 2.93 GHz Intel Xeon 5570 Prozessoren und 72 GB RAM dem Nachweis, bis zu 130 virtuelle Desktops auf einem Citrix XenServer 5.5 Host betreiben zu können. Betrachtet man die Antwortzeiten der virtuellen Desktops unter dem als typisch definierten Workload bei steigender Anzahl gleichzeitiger Sessions, so fangen ab ca. 50 virtuellen Desktops die maximalen Antwortzeiten an, in Höhe mehrerer Sekunden zu liegen (siehe Abbildung 5).

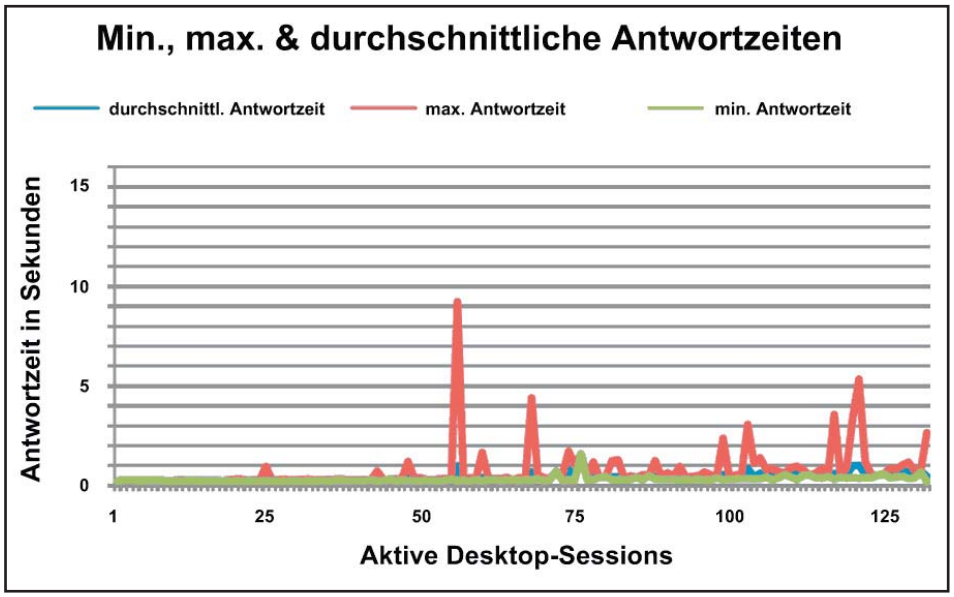


Abbildung 5: Ab ca. 50 aktiven Desktop-Sessions steigen die max. Antwortzeiten der Desktops rapide an. [Quelle: Citrix Whitepaper „Citrix XenDesktop 4 Single Server Scalability Test Results on Citrix XenServer 5.5“]

[2] http://www.citrix.de/unternehmen/presse/pressemeldungen/2010/02/02_22/
[3] Citrix Whitepaper „XenDesktop 2.1 Scalability Analysis“
[4] Citrix Whitepaper „Citrix XenDesktop 4 Single Server Scalability Test Results on Citrix XenServer 5.5“

Spätestens hier wird jeder Benutzer zum Telefonhörer greifen, um beim Helpdesk ein technisches Problem zu melden (sofern das Telefon nicht als Softphone auf seinem unerreichbaren virtuellen Desktop liegt...). Auch mit den Vorteilen moderner Hochleistungs-CPUs sollten also in einem realistischen Szenario nicht mehr als 50 virtuelle Desktops auf einem physischen Host betrieben werden.

3.2 Erforderliche Bandbreiten

Zusammen mit den in Abschnitt 2 besprochenen Durchsatzraten, die ein einzelner Desktop hervorruft, ergibt sich für die erforderlichen Netzwerkbandbreiten folgendes Bild:

Beim Start eines Desktops für Geschäftsanwendungen werden bis zu 15 Mbit/s Bandbreite belegt. Bei 50 gleichzeitigen Desktops in einem Server sind dies 750 Mbit/s Bandbreite, sofern alle diese Desktops gleichzeitig gestartet werden. Eine 1 Gigabit-Verbindung wird hierfür demnach ausreichen. Entscheidend ist, dass diese Bandbreite bei mehreren Virtualisierungshosts ohne Überbuchung durch die weitere Infrastruktur geführt wird.

Beim Starten eines Desktops mit Multimedia-Anwendungen (Flash-Animationen etc.) sind je nach eingesetztem Protokoll bis zu 60 Mbit/s und dies teilweise über die gesamte Verbindungsdauer erforderlich. Bei 50 gleichzeitigen Desktops dieser Art sind dies 3 Gbit/s Bandbreite insgesamt. Ob dieser Anwendungsfall die Notwendigkeit von 10 Gigabit-Ethernet-Schnittstellen jedoch rechtfertigt, möge jeder Service-Dienstleister selbst entscheiden.

Erst wenn die Anzahl virtueller Desktops für Geschäftsanwendungen pro Host die Größenordnung von 50 überschreitet, ist eine Bündelung mehrerer Gigabit-Schnittstellen oder die Verwendung einer 10GE-Schnittstelle erforderlich, um die angeforderten Bandbreiten aus den Servern heraus transportieren zu können.

3.3 „Viele kleine“ versus „wenige große“ Server

Theoretisch wäre eine Erhöhung der virtuellen Desktops pro Host durch die Verwendung von Serversystemen mit vervielfachter CPU-Anzahl und Hauptspeichergröße realisierbar. Doch hier stellt sich die in der Virtualisierung ganz grundsätzliche Frage, ob besser viele kleine oder wenige große Serversysteme zur Virtualisierung eingesetzt werden sollten.

Die Serverbranche misst die Virtualisierungsfähigkeit und den Konsolidierungsgrad ihrer Server in VMmarks, die im folgenden Abschnitt näher dargestellt werden.

3.3.1 VMmark

VMmark ist der Ansatz von VMware, ein objektives Benchmarking-Tool für die Virtualisierungsleistung von Servern zur Verfügung zu stellen. Bei diesem Tool wird ein vordefiniertes Lastprofil - ein so genannter „Tile“ -, das aus 6 VMs mit unterschiedlichen Betriebssystemen und Applikationen besteht, auf dem Server ausgeführt und deren Performance ausgewertet.

Diese sechs virtuellen Server setzen sich aus je drei VMs mit Microsoft Windows Server 2003 Enterprise Edition und SUSE Linux Enterprise Server 10 zusammen.

Jeweils eine Windows-VM bearbeitet einen dieser Workloads:

- Mail-Server mit Microsoft Exchange 2003
- Java-Server mit SPECjbb2005
- Standby-Server im Leerlauf ohne Last

Auf den drei Linux-VMs werden drei weitere Workloads verarbeitet:

- Web-Server mit SPECweb2005
- Datenbank-Server mit MySQL
- File-Server mit dbench

Die virtuellen Maschinen eines Tiles erfordern insgesamt ca. 6 GByte Arbeitsspeicher und 80 GByte Storage. Abbildung 6 zeigt diese 6 virtuellen Maschinen auf einem Virtualisierungshost.

Zum Erzeugen und Steuern der Last in den virtuellen Maschinen sorgen unterschiedliche Applikationen. Für jedes VMmark-Tile wird ein dedizierter Windows Server 2003 Enterprise Edition Client eingesetzt, auf dem die folgenden Applikationen laufen:

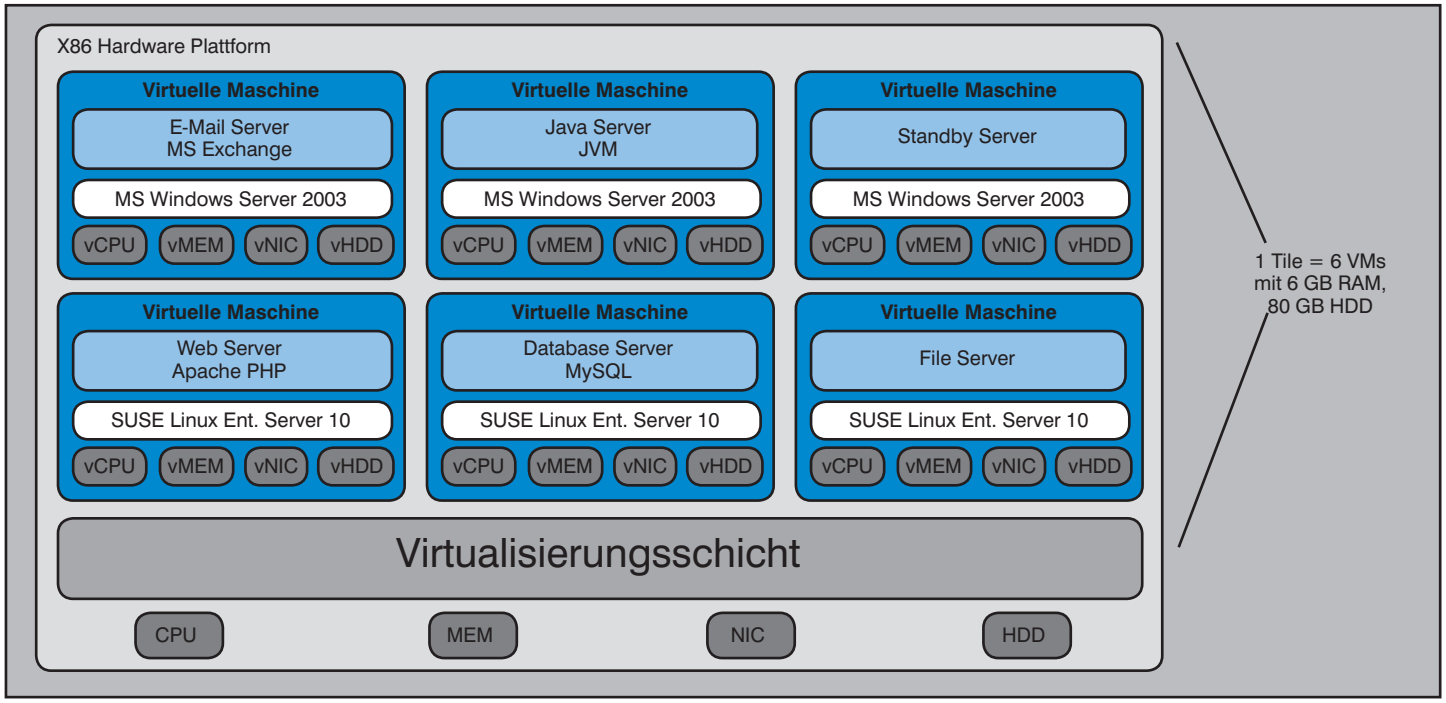


Abbildung 6: Lastmessung mittels „VMmark“ und 6 virtuellen Maschinen, die einen sog. „Tile“ ergeben

- VMmark harness
- STAF Framework und STAX Execution Engine
- LoadSim 2003
- Microsoft Outlook 2003
- BEA JRockit 5.0 JVM JDK
- SPECweb-Client von SPECweb2005
- MySQL Database Server
- SysBench Database Benchmark
- SPECjbb-Monitor von SPECjbb2005

Ist der Server mit diesen 6 VMs nicht vollständig ausgelastet, wird ein zweiter Tile – ebenfalls aus solchen 6 VMs – gestartet, usw. bis das Starten eines weiteren Tiles auf Kosten der bereits laufenden Tiles ginge, also zu keinem weiteren Leistungsanstieg des Gesamtsystems führen würde. Abbildung 7 zeigt einen Virtualisierungshost, auf dem mehrere Tiles gleichzeitig gestartet wurden, die jeweils über einen eigenen Client gesteuert und ausgewertet werden.

Der VMmark-Wert ist die Summe der Leistung der einzelnen Tiles und gibt damit Aufschluss über die Gesamtperformance des Servers und mit wie vielen Tiles diese Performance erreicht wurde. Das bedeutet, dass zwei Server, die beide einen VMmark von 20 erreichen, der erste dies jedoch mit 10 Tiles tut („VMmark=20@10Tiles“) und der zweite mit 5 Tiles („VMmark=20@5Tiles“) unterschiedliche Konsolidierungsgrade und Leistungswerte innerhalb der Tiles aufweisen:

- Der erste Server kann doppelt so viele VMs konsolidieren wie der zweite (10 Tiles versus 5 Tiles)

- Die Leistung des zweiten Servers innerhalb eines Tiles ist doppelt so hoch, wie die des ersten. D.h. die Performance der Applikationen im zweiten Tile ist doppelt so schnell wie im ersten Server. (Erklärung: Würde man im ersten Server nur 5 Tiles betreiben, wäre eine Leistung von VMmark=10@5Tiles zu erwarten. Dies ist nur die Hälfte der Leistung, die der zweite Server mit VMmark=20@5Tiles in der gleichen Anzahl virtueller Maschinen erreicht.)

Hier ist also in die Strategie mit einzubeziehen, ob die Zielsetzung ein hoher Konsolidierungsgrad oder eine hohe Leistung der einzelnen VMs ist.

3.3.2 Serverleistung in der Praxis

In der Praxis ist es allerdings bei modernen CPUs, die in etwa dem gleichen Entwicklungsstand entsprechen, so, dass die Performance unterschiedlicher Server pro Tile ungefähr gleich ist und sich zwischen 1,35 und 1,5 VMmark bewegt. Entscheidend ist daher für die Gesamtbewertung des Servers sein Konsolidierungsgrad, also die Anzahl der Tiles. Da ein Tile gemäß Definition der 6 VMs ca. 6GB Hauptspeicher benötigt, hängt der Konsolidierungsgrad i.W. vom Hauptspeicherausbau ab.

Vergleicht man beispielsweise einen HP ProLiant BL490c G6 - 8 Core Server mit 96 GB RAM mit einem IBM x3850 M2 - 24 Core Server, der nur 80 GB RAM zur Verfügung hat, kann der HP Server 3 zusätzliche Tiles starten. Beim Vergleich der Benchmark-Ergebnisse fällt auf, dass der „kleinere“ HP Server mit einem VMmark-Wert von 24.54@17 Tiles eine höhere Leistung erzielt als die „große“ IBM Maschine mit 19,1@14 Tiles. Bei dem IBM Server handelt es sich also nur vermeintlich um das größere System, da dieser Server aufgrund des kleineren Hauptspeichers die Leistung seiner 24 CPU Kerne gar nicht ausspielen kann.

Um die Virtualisierungsleistung zweier Serversysteme miteinander objektiv vergleichen zu können, müssen diese daher mit dem gleichen Hauptspeicher ausgestattet sein. Alternativ vergleicht man die VMmarks pro Tile. Diese sind beim HP Modell mit 1,44 gegenüber 1,36 bei IBM auch etwas höher, allerdings nicht so eklatant, wie es die Gesamtwerte suggerieren (der VMmwark von HP liegt pro Tile nur 5% über dem von IBM).

3.3.3 Serververgleich unter gleichen Randbedingungen

Der Vergleich in Tabelle 1 stellt tatsächlich gleiche Randbedingungen zwischen kleinen und großen Serversystemen her, da CPU-Typ und Anzahl sowie relativer Speicherausbau (pro CPU) gleich sind.

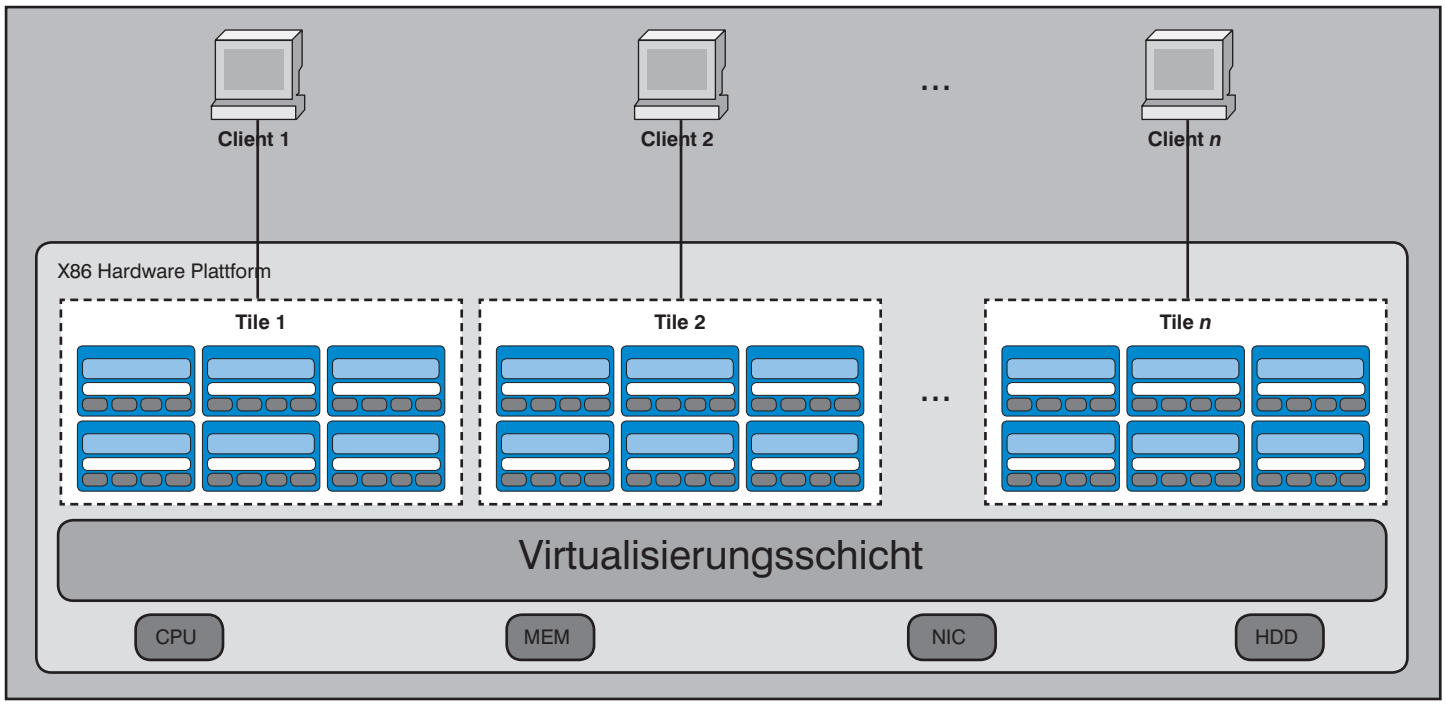


Abbildung 7: Auf dem Server werden so viele Tiles parallel gestartet, bis eine Leistungssättigung eintritt. Das Lastprofil jedes einzelnen Tiles wird durch einen eigenen Client gesteuert und ausgewertet.

Server-Modell	Prozessor	Taktrate	Sockel	Kerne	Speicher	VMmark	Listenpreis
HP ProLiant DL785 G6	AMD Opteron 8439SE	2.8 GHz	8	48	256 GB	53,73@ 35 Tiles	106.720$
HP ProLiant DL585 G6	AMD Opteron 8439SE	2.8 GHz	4	24	128 GB	29,95@ 20 Tiles	46.269$
HP ProLiant DL385 G6	AMD Opteron 2435	2.6 GHz	2	12	64 GB	15,54@ 11 Tiles	15.711$

Tabelle 1: Vergleich von HP ProLiant Rack-Servern mit AMD Opteron CPUs

Server-Modell	Prozessor	Taktrate	Sockel	Kerne	Speicher	VMmark	Listenpreis
IBM System x3950 M2	Intel Xeon X7350	2.93 GHz	8	32	128 GB	24,62@ 18 Tiles	56.875$
IBM System x3850 M2	Intel Xeon X7350	2.93 GHz	4	16	64 GB	13,16@ 9 Tiles	25.092$

Tabelle 2: Vergleich von IBM System-x Rack-Servern mit Intel Xeon CPUs

Man erkennt, dass mehrere kleine DL385 eine höhere VMmark-Performance und einen höheren Konsolidierungsgrad haben, als entsprechend weniger DL585 bzw. DL785, obwohl Anzahl und Typ CPU sowie Hauptspeicher in Summe gleich sind.

Das gleiche Bild ergibt sich beim Vergleich zweier auf Intel-Prozessoren basierender IBM Server, wie aus Tabelle 2 hervorgeht.

Weitere Aspekte bei diesen Betrachtungen sind die Invest- und Betriebskosten der Server. Die Listenpreise mehrerer kleiner Server liegen ebenfalls unter den Kosten für wenige große Server. Dieser Kostenvorteil kann sich durch unterschiedliche Herstellerrabatte auf kleine und große Server natürlich noch umdrehen.

3.3.4 Sprungfixe Kosten

Verfolgt das Serversizing das Konzept „viele kleine, anstatt wenige große Systeme“, so werden einerseits die Einstiegskosten reduziert und andererseits sind die sprungfixen Kosten niedriger. Dies sind die Kosten, die bei der Beschaffung eines zusätzlichen Servers für ein weiteres virtuelles System - etwa einen weiteren virtuellen Desktop - entstehen, wenn die vorhandene Hosting-Leistung nicht mehr ausreicht.

3.4 Ergebnis

Weder die Gesamtperformance noch die Konsolidierungsfähigkeit sprechen für den Einsatz von großen, d.h. besonders leistungsfähigen Servern gegenüber mehreren kleinen Systemen. Auch kostenseitig besteht bei großen Servern erst bei einem gegenüber kleinen Servern höheren Rabattsatz auf die Listenpreise des Herstellers ein Vorteil.

Der Einsatz mehrerer „kleiner“ Server, die also maximal bis zu 50 virtuelle Desktops gleichzeitig hosten, hat den positiven Nebeneffekt, dass sich die erforderlichen Netzwerkbandbreiten besser verteilen und im Standard-Office-Profil der Einsatz von einer oder wenigen gebündelten Gigabit-Ethernet-Links in der Regel ausreicht.

4. Fazit

Virtual Desktop Infrastructure ist die aktuell einflussreichste Entwicklung auf dem Virtualisierungsmarkt. Die Komplexität der Konfiguration und des Betriebs einer solchen Infrastruktur wird vielfach noch unterschätzt. Getrieben von den Software- und Hardware-Herstellern, die hier ihr neues, großes Geschäft wittern, besteht die Versuchung, die auf den ersten Blick schwer überschaubaren Hardware-Anforderungen mit Systemen der höchsten Leistungsstufe zu „erschlagen“.

In der Praxis ist es jedoch empfehlenswerter, den unbestritten hohen Lastanforderungen durch ein ausgewogenes Gesamtkonzept zu begegnen. Dabei ist die Verteilung der Last auf eine angemessen Anzahl von Systemen ein entscheidender Erfolgsfaktor. Bei der Dimensionierung der Server ist nicht allein die Performance und ihr Konsolidierungsvermögen entscheidend, sondern auch die Ausstattung mit Hauptspeicher und Netzwerkschnittstellen. Hier muss insbesondere darauf geachtet werden, dass die Netzanbindung nicht zum Flaschenhals wird, sondern durch eine ausgewogene Verteilung der Verkehrsströme der Erfolg des Virtualisierungsvorhabens gewährleistet wird.

ComConsult Veranstaltungskalender

Aktuelle Veranstaltungen

Aktuelle VPN-Technik, 14.04. - 16.04.10 in Aachen

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

Preis: € 1.690,-- zzgl. MwSt.

Projektmanagement II: Sitzungen moderieren, Projekte präsentieren, erfolgreich verhandeln und Teams führen, 19.04. - 23.04.10 in Aachen

In diesem 5-tägigen Intensiv-Seminar steht das Führungsverhalten des Projektleiters eindeutig im Mittelpunkt. Professionelles Moderieren, Präsentieren, Verhandeln und Teamleiten ist eine Kunst, die trainierbar ist. Durch aktives Training werden die für die Projektarbeit relevanten Führungseigenschaften signifikant verbessert.

Preis: € 2.290,-- zzgl. MwSt.

Sicherer Internetzugang, 19.04. - 21.04.10 in Aachen

Das Internet hat sich zu der entscheidenden Plattform für moderne Kommunikation und Geschäftsfelder entwickelt – trotz aller mit der damit verbundenen weitgehend unkontrollierten globalen Vernetzung einhergehenden Bedrohungen für IT-Infrastruktur und Daten. Der Anschluss an dieses Kommunikationsmedium muss daher so gestaltet sein, dass unkalkulierbare Risiken vermieden werden, ohne Nutzungspotenziale zu verschenken. Dieses Seminar identifiziert die wesentlichen Gefahrenbereiche und zeigt effiziente und wirtschaftliche Maßnahmen zur Umsetzung einer erfolgreichen Lösung auf. Alle wichtigen Bausteine werden detailliert erklärt und anhand praktischer Projektbeispiele und Übungen wird der Weg zu einer erfolgreichen Sicherheits-Lösung aufgezeigt.

Preis: € 1.690,-- zzgl. MwSt.

Lokale Netze für Einsteiger, 19.04. - 23.04.10 in Aachen

Dieses Seminar vermittelt kompakt und intensiv innerhalb von 5 Tagen die Grundprinzipien des Aufbaus und der Arbeitsweise Lokaler Netzwerke. Dabei werden sowohl die notwendigen theoretischen Hintergrundkenntnisse vermittelt als auch der praktische Aufbau und der Betrieb eines LANs erläutert. Ausgehend von einer Darstellung von Themen der Verkabelung und der grundlegenden Übertragungsprotokolle werden die wichtigen Zusammenhänge zwischen der Arbeitsweise von Switch-Systemen, den darauf aufsetzenden Verfahren und der Anbindung von PCs und Servern systematisch erklärt.

Preis: € 2.290,-- zzgl. MwSt.

IP-Wissen für TK-Mitarbeiter, 03.05. - 04.05.10 in Bonn

Dieses Seminar vermittelt kompakt und effizient das IP-Wissen, das TK-Mitarbeiter ohne Vorkenntnisse zur Planung und zum Betrieb von IP-basierten Telefonie-Lösungen benötigen. Alle Seminarinhalte werden von einem Referenten mit hoher Praxiserfahrung betreut. Ziel ist dabei bewusst, statt einer umfassenden Theorieschulung gezielt die Aspekte vorzustellen und unter Praxis-relevanten Gesichtspunkten zu beleuchten, die erfahrungsgemäß aus Sicht einer IP-basierten Telefonielösung wichtig sind.

Preis: € 1.390,-- zzgl. MwSt.

TCP/IP und SNMP, 03.05. - 07.05.10 in Bonn

LAN-, WLAN- und WAN-Netzwerke sind heutzutage IP-Netze, und ein Verzicht auf Nutzung des IP-basierten Internet undenkbar. Auch für früher nur mit herstellerspezifischen Protokollen in Verbindung gebrachte Anwendungsgebiete wie Telefonie oder Produktionsumgebungen gibt es mittlerweile geeignete IP-basierte Lösungen. Hersteller und Dienstanbieter versuchen den Eindruck zu vermitteln, die Nutzung sei kinderleicht, fast schon plug and play - man trägt ein paar Adressen ein (wenn überhaupt), und es kann losgehen. Falsch!

Preis: € 2.290,-- zzgl. MwSt.

Interne Absicherung der IT-Infrastruktur, 10.05. - 12.05.10 in Köln

Bedingt durch Netzkonvergenz, Mobilität und Virtualisierung hat die interne Absicherung der IT-Infrastruktur in den letzten Jahren enorm an Bedeutung gewonnen. Heterogene Nutzergruppen mit unterschiedlichstem Sicherheitsniveau teilen sich eine gemeinsame IP-basierte Infrastruktur und in vielen Fällen ist der Aufbau sicherer, mandantenfähiger Netze notwendig. Dieses Seminar identifiziert die wesentlichen Gefahrenbereiche und zeigt effiziente und wirtschaftliche Maßnahmen zur Umsetzung einer erfolgreichen Lösung auf. Alle wichtigen Bausteine zur Absicherung von LAN, WAN, Endgeräten, RZ-Bereichen, Servern und SAN werden detailliert erklärt und anhand konkreter Projektbeispiele wird der Weg zu einer erfolgreichen Sicherheits-Lösung aufgezeigt.

Preis: € 1.690,-- zzgl. MwSt.

Internetworking: optimales Netzwerk-Design mit Switching und Routing, 17.05. - 21.05.10 in Bonn

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

Preis: € 2.290,-- zzgl. MwSt.

Zertifizierungen

ComConsult Certified Network Engineer

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

TCP/IP und SNMP
03.05. - 07.05.10 in Bonn
27.09. - 01.10.10 in Stuttgart

Internetworking
17.05. - 21.05.10 in Bonn
25.10. - 29.10.10 in Aachen

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

ComConsult Certified Trouble Shooter

Trouble Shooting 1
18.05. - 21.05.10 in Aachen
21.09. - 24.09.10 in Aachen

Trouble Shooting 2
22.06. - 25.06.10 in Aachen
26.10. - 29.10.10 in Aachen

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

ComConsult Certified Voice Engineer

Session Initiation Protocol-Basis-Technologie der IP-Telefonie
28.06. - 30.06.10 in Bonn
22.11. - 24.11.10 in Hamburg

Sicherheitsmechanismen für Voice over IP
21.06. - 22.06.10 in Bonn
03.11. - 04.11.10 in Bonn

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen
07.06. - 09.06.10 in Königswinter
04.10. - 06.10.10 in Bonn
13.12. - 15.12.10 in Stuttgart

Optionales Einsteiger-Seminar: IP-Wissen für TK-Mitarbeiter
03.05. - 04.05.10 in Bonn
27.09. - 28.09.10 in Stuttgart
15.11. - 16.11.10 in Königswinter

Basis-Paket: Beinhaltet die drei Basis-Seminare
Grundpreis: € 4.250,-- zzgl. MwSt. statt € 4.770,-- zzgl. MwSt.

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

ComConsult Zertifizierter Projektleiter

Projektmanagement I: Projekte aus IT und Kommunikationstechnik leiten und organisieren
08.11. - 12.11.10 in Aachen

Projektmanagement II: Sitzungen moderieren, Projekte präsentieren, erfolgreich verhandeln und Teams führen
19.04. - 23.04.10 in Aachen
29.11. - 03.12.10 in Aachen

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

Impressum

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

E-Mail: insider@comconsult-akademie.de
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