ComConsult Research

Der Netzwerk Insider

März 15

Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

IPv6: Fundamente richtig legen

von Dr. Behrooz Moayeri

Die Welt der Netze steht vor der nächsten großen Umstellung. Das Internet Protocol der Version 6 (IPv6) wird kommen. Daran zweifelt niemand mehr ernsthaft. IPv6 wird an den Grenzen keines Unternehmens halt machen. Jedes Unternehmen muss sich auf IPv6 vorbereiten. Wenn die Fundamente richtig gelegt werden, wird die Umstellung auf IPv6 weitgehend schmerzfrei verlaufen. Anderenfalls drohen instabile Zustände und ein großer Migrationsaufwand.

Aber welche sind die richtigen Fundamente? Die ersten Erfahrungen aus der Praxis liegen vor. Alle Unternehmen können von diesen Erfahrungen lernen. Und sie sollten das tun. Die Zeit dafür ist jetzt. Bevor äußere Zwänge zum überstürzten Handeln zwingen, müssen die Verantwortlichen für die IT-Infrastruktur die geplante und gut durchdachte Einführung von IPv6 im eigenen Unternehmensnetz vorbereiten. Der erste Schritt ist der Aufbau von Know-how über IPv6. Einiges bei IPv6 unterscheidet sich vom Pendant unter IPv4. Und da ist noch die lange Phase des Nebeneinanders der beiden Protokolle. Dieselben Systeme und Anwendungen können beide Protokolle nutzen. Dies sollte kontrolliert und gesteuert erfolgen. Alles dem Zufall zu überlassen kann heilloses Durcheinander, Ausfälle und viel Arbeit bedeuten.

weiter auf Seite 7

Die Zeit des Zurücklehnens ist vorbei

Zweitthema

SDN, NFV, OpenFlow und Virtualisierungs-Protokolle – Zusammenhänge, Perspektiven, Marktrelevanz

von Dipl.-Inform. Petra Borowka-Gatzweiler

SDN und NFV scheinen zur Zeit ganz oben im Hypecycle der Netzbetreiber zu stehen. Sind SDN und NFV dasselbe oder sind es unterschiedliche Technologien? Welche Märkte bedienen sie? Wohin gehören OpenFlow, Controller, Northbound, Southbound, East-Wetbound API, Network Function Virtualisation Infrastructure sowie Virtualisierungs-Protokolle wie VXLAN, GENEVE und NSH? Welche Relevanz haben diese Technologien für Enterprise Netzwerke? Der nachfolgende Beitrag beleuchtet diese Themen, ihre technologischen Hintergründe und ihre praktische Marktrelevanz.

1. SDN – Software Defined Networking

Heutige Netzwerke bestehen vielfach aus proprietärer Hardware, die mittels Hersteller-Software konfiguriert und administriert wird. Somit sind Hardware und Control Plane herstellerspezifisch. SDN ist eine aufkommende Netzwerk-Technologie auf Basis einer standardisierten Netzwerk-Architektur, die den bislang proprietären Control Plane Konzepten etablierter Netzwerk-Komponenten ein Ende bereiten will: Die Control Plane wird aus den Netzkomponenten auf eine zentrale standardisierte Steuerung ausgelagert. Hierdurch wird sie für den Betreiber (mittels remote Steuerung standardisierter Clients / Agenten) zugreifbar und programmierbar.

weiter auf Seite 18

Geleit

Branded Whites Box-Switches: was soll das und was bedeutet das für die Branche?

auf Seite 2

Aktueller Kongress

ComConsult Netzwerk- und IT-Infrastruktur Forum 2015

ab Seite 4

Standpunkt

WLAN: Wird 5 GHz zum neuen 2,4-GHz-Band?

auf Seite 16

Neues Seminar

Strategien für Unternehmen zur richtigen Positionierung im Internet

auf Seite 17

Zum Geleit

Branded Whites Box-Switches: was soll das und was bedeutet das für die Branche?

Die Zeit proprietärer Netzwerk-Hardware könnte sich bald dem Ende nähern. Nicht in dem Sinne, dass normale Switches wie wir sie von den üblichen Anbietern kennen, komplett verschwinden sondern mehr in dem Sinne, dass eine neue Produktkategorie zunehmend an Bedeutung gewinnt. So beobachten wir in den großen Cloud-Rechenzentren seit Jahren eine zunehmende Ablehnung von Standard-Produkten, sowohl auf der Netzwerk als auch auf der Server-Seite. Dabei werden interessanterweise nicht nur die Anschaffungskosten kritisiert, sondern vor allem die Betriebskosten, die mit den bisherigen proprietären Lösungen einher gehen. Betrachtet man speziell das Open Compute Projekt von Facebook, dann wird durchaus deutlich, dass ein großer Markt, der bisher auf wenige starke Anbieter reduziert war, wichtige Verbesserungen und Veränderungen im Produktdesign total verschlafen hat. Es war ja auch nicht notwendig, die Kunden kauften ja auch so. In letzter Konsequenz sind so Lösungen entstanden, die den Kunden deutlich zu hohe Betriebskosten zumuten (stark abhängig von der Zahl der eingesetzten Switches und Server).

So ist in den letzten Jahren die White-Box-Bewegung entstanden, die sich vor allem an die sehr großen Rechenzentren dieser Welt wendet. Dabei werden Hardware und Software entkoppelt. Ein Anbieter konzentriert sich auf Hardware-Massenware, ein anderer auf die Software. Hardware-Massenware ist dabei durchaus naheliegend und liegt im Trend der letzten Jahre. Mehr und mehr Hersteller von Netzwerk-Komponenten haben die eigene ASIC-Entwicklung entweder eingestellt oder reduziert. Viele der heute angebotenen Switches sind bereits verkappte OEM-Boxen, die nur durch die Software des Anbieters und die Art des Gehäuses eine gewisse Eigenständigkeit bekommen. Das mag nicht unbedingt für die Top 10% der Hochleistung-Switches gelten, aber für die Massenware im RZ oder im Access-Bereich ist dies definitiv der Fall. Access-Switches sind bereits weitestgehend austauschbar und die Hersteller gehen lange Wege um diese Austauschbarkeit durch Software-Eigenschaften zu kaschieren (manchmal durchaus mit Sinn, zum Beispiel wenn es um die Rechts- und Zugangsverwaltung für Endgeräte geht oder um die Vereinheitlichung eines Wi-

red und Wireless Access). Für den RZ-Betreiber bedeutet der neue Trend vor allem, dass er sich betriebsseitig für eine Software entscheiden kann und nach Bedarf die Hardware zukaufen kann, die am besten zu seinem Betrieb passt. Der Betrieb wird einfacher, und natürlich sind die Einkaufspreise deutlich günstiger.

Der hier angesprochene Markt ist so groß, dass ihn die traditionellen Anbieter nicht einfach ignorieren können. Trotzdem überrascht Hewlett Packard den Markt mit seiner Zusammenarbeit mit Accton und Cumulus. HP wird in den nächsten Wochen zwei Typen von Switch-Systemen zur Vermarktung durch Accton bereit stellen. Damit entsteht eine branded White-Box, die vor allem die Eigenschaft haben wird, mehrere unterschiedliche Betriebssysteme zu betreiben. Um dem Kunden die Entscheidung zu erleichtern, hat HP gleichzeitig mit Cumulus einen Vertrag geschlossen und stellt die Cumulus-Software als Betriebssystem für die Accton-Switches-Switches zur Verfügung (ein Linux-basiertes Netzwerk-Betriebssystem). Was auf den ersten Blick vielleicht etwas paradox wirkt, kann sich bei näherer Betrachtung zu einem gewinnbringenden Geschäftsmodell für HP entwickeln. Die bisherigen White-Box-Lösungen haben ihren typischen Nachtei im Bereich des Services. Die Kunden müssen die Integration und mögliche Probleme selber bearbeiten. HP steigt mit seinen neuen Kooperationen in diesen Markt ein und will sich als das führende Service-Unternehmen für branded White-Ware positionieren. Es bleibt abzuwarten, ob das gelingt, aber der Schritt ist sicher interessant.

Die im Moment von HP und Accton geplanten Produkte sind 10/40-Gigabit Massenprodukte, wie wir sie in RZs in großen Stückzahlen sehen. Sie werden später im Jahr ergänzt durch die neuen 25/50/100G Switches.

HP ist mit dieser Vorgehensweise nicht allein, reduziert seine Kooperationen aber auf genau definierte und somit eingeschränkte Produkte. Vermutlich will man auch abwarten, ob das angestrebte Ser-

Branded Whites Box-Switches: was soll das und was bedeutet das für die Branche?

vice-Geschäftsmodell überhaupt zum Tragen kommt. Der andere Hersteller, der diesen Weg schon früher gegangen ist, ist DELL. DELL hatte bereits im Januar 2014 angekündigt, seine Switch-Produkte mit Cumulus-Software auszuliefern und ließ dieser Kooperation im April eine weitergehende Kooperation mit BigSwitch folgen.

Was bedeutet diese Entwicklung jetzt für Unternehmen, die nach neuer Netzwerk-Hardware suchen und vor neuen Investitionen stehen?

Erst einmal muss festgestellt werden, dass diese neue White-Box-Bewegung, branded oder auch nicht, in einem Wettbewerb mit SDN steht. Tatsächlich könnte sich hier auch eine interessante Überlappung ergeben, indem Spezialanbieter zum Beispiel aus dem Sicherheitsmarkt Access-Lösungen durch eine Kombination von White-Box-Hardware mit ihrer SDN-basierten Zugangs-Software erzeugen. Der entscheidende Punkt bei White-Box-Lösungen ist die Entkopplung von Hardware und Software. Das war aber genau der Punkt, den SDN auch angehen wollte: der Aufbau eines Hardware-unabhängigen Software-Marktes. Branded White-Box-Lösungen könnten in diesem Sinne den SDN-Markt erheblich beschleunigen und für Unternehmen wie Big Switch Networks der finale Rettungsanker sein.

Genau diese Frage deuten aber auch darauf hin, dass wir in einer zu frühen Phase des Marktes sind, um wirklich einen Einstieg in diese Welt empfehlen zu können. Schon mit SDN war und ist klar, dass sich erhebliche Veränderungen ergeben werden. Aber die Frage ist weiterhin offen wie diese im Detail aussehen werden.

Tatsächlich kann der Anwender sich aber in einem erheblichen Umfang auf diese Entwicklung vorbereiten. Aus unserer Sicht (ComConsult Research) hat sich im Design von Netzwerken sowohl im RZ als auch im Access-Bereich in den letzten drei Jahren doch eine deutliche Veränderung ergeben. Diese Veränderung ist Teil eines Prozesses, der noch mehrere Jahre andauern wird und auch die Server- und Speicher-Systeme betreffen wird. Der Anwender muss diese Trends kennen und seine Architektur und konkrete Projektplanung auf die neueste Entwicklungen abstellen. Dann hat er eine gute Chance, mit auf den Zug aufzuspringen, wenn die Zeit nur reif genug dafür ist. Die Anbieter werden nämlich nicht bei den Speziallösungen einsteigen sondern bei Massen-Lösungen, die einem neuen und gängigen Design unterliegen. Hier ist der größte Markt außerhalb der großen Cloud-Rechenzentren. Also ist unsere klare Empfehlung: vermeiden Sie Sonderlocken und folgen Sie dem aktuellen Design-Trend.

Wir helfen Ihnen dabei speziell mit zwei Veranstaltungen: zum einem unser **ComConsult Netzwerk- und Infrastruktur Forum 2015** und zum anderen mit einer ganz besonderen Sonderveranstaltung, die sich hochaktuell die neuen Designsätze vornimmt und diskutiert (**Netzwerk-Design für Enterprise Netzwerke**).

Es ist wieder einmal spannend im Netzwerk-Markt und unser Team von Comconsult Research wird sich zusammen mit ausgewählten Top-Referenten dieser Entwicklung mit interessanten Diskussionen auf dem **ComConsult Netzwerk- und Infrastruktur-Forum 2015** stellen.

Ihr
Dr. Jürgen Suppan

Kongress

ComConsult Netzwerk- und IT-Infrastruktur Forum 2015
20.04. - 22.04.15 in Königswinter

Das ComConsult Netzwerk- und IT-Infrastruktur-Forum 2015 stellt die drei momentan dominantesten Netzwerk-Themen in den Mittelpunkt der Veranstaltung:
- Netzwerke und Infrastrukturen im Rechenzentrum
- Netzwerk-Planung und Design
- Betrieb, Verfügbarkeit und Wirtschaftlichkeit von Netzwerken

Dabei beobachten wir in allen drei Bereichen momentan herausragende Entwicklungen, die sowohl die Leistung als auch die Wirtschaftlichkeit von Netzwerken in den nächsten Jahren stark beeinflussen werden. Drei Beispiele aus dem Programm des Forums sollen das verdeutlichen.

Der Netzwerk-Markt ist in Bewegung wie diese Beispiele zeigen. Das ComConsult Netzwerk- und IT-Infrastruktur-Forum 2015 ist das richtige Forum zur richtigen Zeit. Wir analysieren exklusiv für Sie:
- was passiert im Rechenzentrum und wie können Sie Ihr Netzwerk darauf optimal vorbereiten
- wie verändert sich Netzwerk-Design und wie können Sie die Vorteile zu Ihren Gunsten nutzen ohne das gesamte Netzwerk ablösen zu müssen
- wie können Sie die Komplexität des Netzwerkes im Betrieb reduzieren und dabei gleichzeitig besser werden

Wie in jedem Jahr hat auch dieses Forum einen Vertiefungstag, an dem wir ein ausgewähltes Thema ausgiebig analysieren und mit Ihnen diskutieren. Dieser Tag ist optional buchbar, aber wir empfehlen ihn allen Teilnehmern.

Moderation: Dr. Jürgen Suppan
Preis: € 2.390,-- netto

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

Aktueller Kongress

ComConsult Netzwerk- und IT-Infrastruktur Forum 2015

20.04. - 22.04.15 in Königswinter

Das ComConsult Netzwerk- und IT-Infrastruktur-Forum 2015 stellt die drei momentan dominanten Netzwerk-Themen in den Mittelpunkt der Veranstaltung:

- Netzwerke und Infrastrukturen im Rechenzentrum
- Netzwerk-Planung und Design
- Betrieb, Verfügbarkeit und Wirtschaftlichkeit von Netzwerken

Dabei beobachten wir in allen drei Bereichen herausragende Entwicklungen, die sowohl die Leistung als auch die Wirtschaftlichkeit von Netzwerken in den nächsten Jahren stark beeinflussen werden. Drei Beispiele aus dem Programm des Forums sollen das verdeutlichen.

Im Rechenzentrum führen die Anforderungen von Virtualisierung, dem Aufbau von Private Clouds und der performanten Integration von Speicher-Systemen dazu, dass wir unsere bisherigen Architekturen mehr und mehr in Frage stellen. Statt dessen drängen neue Themen in die Diskussion:

- die Rolle von Software-Switches in den Architekturen und als Teil von Lösungen wie VMware NSX
- die Rolle von virtuellen Appliances, um ganze Anwendungsbereiche über mehrere Server hinweg mobil zu gestalten und zwischen Standorten verlagern zu können (wesentlicher Teil für Notfall-Szenarien, das ging so bisher nicht)
- SDN gewinnt in diesem Umfeld rapide an Bedeutung, zwar nicht wie ursprünglich als Technologie vorgestellt, sondern mehr als Speziallösung zur Steuerung von Software-Switches und virtuellen Appliances, aber dafür hat es in diesem Bereich den Status einer unreifen Technologie längst verlassen

Im Bereich Netzwerk Design dominiert die Kombination aus einer besseren Anpassung von Netzwerken an den Bedarf und nach flexibleren Lösungen. So sehen wir:

- neue Ethernet-Bandbreiten, die auf den ersten Blick überraschen, aber bei näherer Analyse sehr viel Sinn machen
- neue Design-Konzepte zur Verbesserung von Skalierung und Provisionierung, zum Beispiel als Edge/Core-Design
- die erste große Welle der IPv6-Projekte

Im Bereich Betrieb geht es sehr viel um die Optimierung bekannter Technologien und die dynamische Anpassung an einen sich permanent verändernden Bedarf:

- im Bereich WLAN haben wir zwar mit 802.11ac eine neue Technologie und müssen Planung und Design daran anpassen. Aber die eigentlichen Anforderungen liegen in vielen Projekten mehr und mehr im Betrieb. Und Bandbreiten-Management in Kombination mit Sicherheits-Aspekten und einer Integration in ein sehr leistungsfähiges Monitoring sind hier die Schlüssel-Funktionen
- wir haben im Betrieb ein zunehmendes Problem mit der Komplexität des Netzwerk-Aufbaus und der daraus resultierenden Destabilisierung des Netzwerks an sich. Eine der wesentlichen Ursachen für die Destabilisierung liegt in der Explosion der Anzahl von Middleboxes im Netzwerk (Firewalls, IDS, Load Balancer, …). Wir beobachten eine zunehmende Zahl von Netzwerken, die im Core mehr MiddleBox-Systeme als Switches haben
- das Thema Sicherheit nimmt noch weiter an Bedeutung zu. In den Projekten ist es in vielen Fällen inzwischen das Thema Nummer 1 für die Gestaltung des Betriebs. Das Problem liegt hier nicht in der Auswahl einer Lösung, sondern in der Gestaltung der Lösung in einer Form, dass sie mit überschaubarem Aufwand betrieben werden kann.

Der Netzwerk-Markt ist in Bewegung wie diese Beispiele zeigen. Das ComConsult Netzwerk- und IT-Infrastruktur-Forum 2015 ist das richtige Forum zur richtigen Zeit. Wir analysieren für Sie:

- was passiert im Rechenzentrum und wie können Sie Ihr Netzwerk darauf optimal vorbereiten
- wie verändert sich Netzwerk-Design und wie können Sie die Vorteile zu Ihren Gunsten nutzen ohne das gesamte Netzwerk ablösen zu müssen
- wie können Sie die Komplexität des Netzwerkes im Betrieb reduzieren und dabei gleichzeitig besser werden

Wie in jedem Jahr hat auch dieses Forum einen Vertiefungstag, in diesem Jahr dreht er sich komplett um IPv6 und die aktuellen Projekterfahrungen in diesem Bereich.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

ComConsult Netzwerk- und IT-Infrastruktur Forum 2015

Ich buche den Kongress
ComConsult Netzwerk- und IT-Infrastruktur Forum 2015

☐ vom 20.04. - 22.04.15 in Königswinter zum Preis € 2.390,-- netto

☐ vom 20.04. - 21.04.15 in Königswinter zum Preis € 1.990,-- netto

☐ am 22.04.15 in Königswinter zum Preis € 990,-- netto

Zum Kongressportal
www.comconsult-research.de

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

Programmübersicht ComConsult Netzwerk- und IT-Infrastruktur Forum 2015

Montag, 20.04.2015

9:30 - 10:15 Uhr
Keynote: Netzwerk- und IT-Infrastruktur-Trends 2015: wohin geht der Weg?
- Bedarfsanalyse
- Die Top 5 Zukunfts-Technologien in der Bewertung von ComConsult Research
- Investitions-Alternativen im Vergleich

Dr. Jürgen Suppan, ComConsult Research Ltd.

Netzwerke und Infrastrukturen im Rechenzentrum

10:15 - 11:00 Uhr
Das tatsächliche Potential von SDN
- Wo steht SDN heute?
- SDN ist nicht gleich SDN - eine Klarstellung
- Was macht SDN denn so attraktiv?
- Anwendungsbeispiele mit SDN, die traditionell nicht oder nur mit hohem Aufwand umsetzbar sind
- Empfehlungen

Dipl.-Ing. Markus Nispel, Extreme Networks GmbH

11:00 - 11:30 Uhr Kaffeepause in der Ausstellung

11:30 - 12:15 Uhr
Neue Lösungsansätze für RZ-Netze
- Unterschiede zu klassischen Netzwerktechnologien
- Was ist der Kern von SDN?
- OpenFlow-SDN vs. Netzwerkvirtualisierung
- NV und SDN als Bausteine für das Software-Defined Datacenter von VMware (NSX)
- Wo bleiben die Anwendungen: Cisco ACI und QoS im Rechenzentrum

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

12:15 - 13:00 Uhr
Private Clouds und die Auswirkung auf IT-Infrastrukturen
- Was eine Private Cloud als solche qualifiziert
- Software-Defined Data Center: Voraussetzung für die Cloud
- Virtualisierte Server als Kernbestandteil
- Elemente einer modernen Speicherstrategie
- Das passende RZ-Zonenkonzept zur Cloud
- Organisatorische Herausforderungen

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

13:00 - 14:15 Uhr Mittagspause

14:15 - 15:00 Uhr
Application Centric Infrastructure: Die Basis für eine Policy-Definierte RZ, LAN und WAN-Infrastruktur
- ACI als Basis für die Policy-Definierte RZ-Infrastruktur (Bausteine der ACI-Architektur, Grundlage für Automation im RZ, Policy-Modell: wie Anwendungen abgesichert werden können)
- Wie APIC-EM den LAN- und WAN-Betriebsprozess optimiert (Vorteile der Controller gemanagten Infrastruktur, Abstraktion als Basis für Automatisierung, QoS, ACL, Richtlinien auf der Basis abstrahierter Topologie, die Rolle des Controllers)

Dipl.-Inform. Matthias Wessendorf, Markus Harbeck, Cisco Systems GmbH

Netzwerk-Planung und Design

15:00 - 15:45 Uhr
Neue Datenraten für Ethernet
- 2,5GbE und 5GbE zur Unterstützung flächendeckender WLAN-Inrastrukturen
- 25GbE und 50GbE als skalierbare Alternative zum unseligen 40GbE
- Die neue Generation der 25/50/100G Switch ASICS wie Broadcom Tomahawk
- 40G am Scheideweg: kommt 40 GBASE-T oder doch nicht?

Dr. Franz-Joachim Kauffels, unabhängiger Unternehmensberater

15:45 - 16:15 Uhr Kaffeepause in der Ausstellung

16:15 - 17:00 Uhr
IPv6: Wo wir stehen, was wir noch brauchen
- Aktueller Stand bei Unternehmen, Providern und Herstellern
- Mit welchen Schwierigkeiten müssen Unternehmen rechnen?
- Welche ungeklärten Problemfelder müssen noch angegangen werden?

Markus Schaub, ComConsult-Study.tv

17:00 - 17:45 Uhr
The New IP – welche Rolle wird NFV in heutigen Netzen spielen?
- Warum Software und wie sehen typische Lösungen aus?
- Vergleich mit Hardware-Lösungen: Vor- und Nachteile
- Kosten-Vergleich: wie viel Geld lässt sich sparen
- Einsatz-Szenerien und Empfehlungen

Christopher Feussner, Brocade Communications GmbH

ab 18:00 Uhr Happy Hour

Dienstag, 21.04.2015

9:00 - 9:45 Uhr
Neue Designkonzepte im Vergleich: Verbesserung von Skalierung und Provisionierung
- Trennung in Edge und Core / Backbone
- Erhöhte Skalierbarkeit
- Verbesserte Provisionierung (Virtualisierung, Quality of Service, Zugangskontrolle/NAC, Mobilität)
- Anforderungen für den Edge: RZ, Access
- Anforderungen für den Core: RZ, Campus
- Technologien: Tunnelverfahren und Markierung
- Migrations-Aufwand
- Multivendor-Unterstützung
- Einheitlichkeit für Campus, RZ und Access

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

Betrieb, Verfügbarkeit und Wirtschaftlichkeit von Netzwerken

9:45 - 10:30 Uhr
WLAN-Netzwerke mit 802.11ac: Methoden zur Bandbreiten-Optimierung und zuverlässigen Versorgung mobiler Teilnehmer
- Analyse: wie viel Bandbreite hat 11ac wirklich und wo liegen Probleme
- Warum Bandbreiten-Management erforderlich ist
- Einfache Prioritäten-Schemata versagen, wie kann eine intelligente und adaptive Lösung genau auf den Bedarf zugeschnitten werden
- Wahl eines optimierten 802.11 ac Channel Design
- Intelligente Steuerung der Clients um optimale Bandbreite für die gesamte WLAN Infrastruktur zu gewährleisten.

Reinhard Lichte, Aruba Networks GmbH

10:30 - 11:00 Uhr Kaffeepause in der Ausstellung

Programmübersicht ComConsult Netzwerk- und IT-Infrastruktur Forum 2015

Dienstag, 21.04.2015

11:00 - 11:45 Uhr
Quality of Service im WLAN: Grenzen und Möglichkeiten der Technologie
- QoS auf der Luftschnittstelle: IEEE 802.11e und WiFi Multimedia (WMM)
- Übertragungs-Kapazität, der Schlüssel für hohe Dienstegüte: Wie plant man leistungsfähige WLAN?
- Multi-User MIMO wird verfügbar, nützt es der QoS?
- QoS zum „Nulltarif", wie funktionieren Anwendungs-sensitive WLANs?
- Software Defined Networking (SDN), ein alternativer Ansatz zur Umsetzung von QoS

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

11:45 - 12:30 Uhr
Problematik und Zukunft von Middleboxes
- Firewalls, IPS, Proxies, Load Balancer, WAN-Optimierer & Co.: warum sie immer mehr Aufwand verursachen
- Ist SDN die Zukunft für Middleboxes?
- Bestehende vielversprechende Ansätze

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

12:30 - 14:00 Uhr Mittagspause

14:00 - 14:45 Uhr
Neue Herausforderungen für die Netzwerksicherheit
- Abwehr von Lauschangriffen und Advanced Persistent Threats: Anforderungen an die Netzwerk-sicherheit und resultierende Sicherheitsarchitekturen
- Netzzugangskontrolle, Verschlüsselung auf Ebene des Netzwerks, Zonenkonzepte: Aufwand vs. Sicherheitsgewinn
- Virtualisierung und Vertikal integrierte Systeme: Evolution zu Plattform-integrierten Sicherheitskomponenten
- SDN, ACI und Co.: Notwendigkeit Anwendungs-zentrierter Sicherheitskonzepte im modernen RZ

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

14:45 - 15:30 Uhr
Vom klassischen Infrastruktur Monitoring zum Ende zu Ende Business Applikations Monitoring
- Proaktive Überwachung und Root-Cause Analyse von Applikationsproblemen
- Überwachung der Business Transaktionen auf dem Weg durch die IT Infrastruktur
- Business Impact Analyse
- End Benutzer Monitoring
- Applikations und Datenbank Decodierung (L2-L7 Decodierung)
- Automatische Erkennung von Anomalien

Peter Rehle, ICS GmbH

15:30 - 16:15 Uhr
Technologien, die die nächsten Jahre beeinflussen werden und unsere Netzwerke und Infrastrukturen verändern werden
- Die Top-Technologien der nächsten Jahre
- Auswirkung auf Infrastrukturen
- Empfehlungen für die Vorbereitung, Planung und Investition sowie die zukünftige Nutzung

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

16:15 Uhr Abschließende Kaffeepause

Mittwoch, 22.04.2015

IPv6 Migration: Projekterfahrungen und -empfehlungen
- Organisation eines IPv6 Rollouts (Planung des Vorgehens, was muss wann entschieden werden, welche Abteilungen sind in welcher Projektphase gefordert, wo existiert Schulungsbedarf)
- Adresskonzept (Welche Alternativen stehen zur Verfügung, was sind die Vor- und Nachteile)
- Zuweisung von IPv6 Adressen (Welche Verfahren stehen zur Verfügung, wie integriert man Komponenten, die kein DHCPv6 unterstützen)
- Anforderungen an Netzwerk- und Infrastrukturkomponenten (Erstellung von Anforderungsprofilen für einzelne Komponenten, Testdurchführung, ausgewählte Testergebnisse)
- LAN-Archtitektur (Redundanzverfahren: VRRP, HSRP, Routing von IPv6, Umgang mit QoS bei IPv6)
- Migration der Internetpräsenz
- Migration von Anwendungen und Appliances
- Erstellung eines Anforderungskataloges für die Anschaffung von Hard- und Software
- Externe Anbindungen (WAN, Internet, Internet-VPN, Externe Partnerunternehmen)
- Security (Ergebnisse von Proxy-Tests, Firewalls & IDS, First-Hop-Security)

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH
Markus Schaub, ComConsult Study.tv

10:30 - 11:00 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause
15:30 Uhr Ende der Veranstaltung

Folgende Aussteller nehmen an der Veranstaltung teil

AixpertSoft, Alcatel·Lucent, ARUBA networks, AVAYA The Power of We, BROCADE, CISCO, ComConsult Beratung + Planung, ComConsult Research, ComConsult Study.tv, controlware communicationssysteme, Extreme networks, FLUKE networks, ics, MICROSENS, NETWORK INSTRUMENTS JDSU Performance Management, psiber, semonit service monitoring IT, TELONIC, WÜRTHPHOENIX

Schwerpunktthema

IPv6: Fundamente richtig legen

Fortsetzung von Seite 1

Dr.-Ing. Behrooz Moayeri hat viele Großprojekte mit dem Schwerpunkt standortübergreifende Kommunikation geleitet. Er gehört der Geschäftsleitung der ComConsult Beratung und Planung GmbH an und betätigt sich als Berater, Autor und Seminarleiter.

Deshalb ist es wichtig, dass die Experten im Unternehmen die Unterschiede zwischen IPv4 und IPv6 kennen. Ferner ist es von Bedeutung zu wissen, welche Probleme und Unwägbarkeiten es in einer dualen Umgebung mit beiden Protokollen geben kann.

Die letzten Zweifler überzeugen

Noch sind nicht alle, auf deren Stimme und Einfluss es in der IT ankommt, davon überzeugt, dass man sich mit IPv6 befassen muss. Immer seltener, aber häufig genug hört man das Argument, dass ein Protokoll, von dem schon seit fast 20 Jahren gesprochen wird, noch lange auf sich warten lassen wird. Vor allem weil viele Anwendungen und Systeme IPv6 noch nicht unterstützen, brauche man sich mit diesem Protokoll gar nicht zu befassen. So das Argument der Zweifler. Zu diesen gehören leider auch viele, die über IT-Budgets entscheiden und die Prioritäten in Unternehmen setzen. Diese Zweifler sind der Meinung, die Unternehmens-IT habe dringendere Aufgaben zu bewältigen. Die dringenden Probleme seien wichtiger als ein Protokoll einzuführen, das zurzeit von den meisten Applikationen und Geräten noch gar nicht unterstützt werde.

Wahrscheinlich lassen sich diese Zweifler von der rhetorischen Frage kaum beeindrucken, die lautet: Warum muss eine Aufgabe erst zu einer dringenden werden, bevor sie angepackt wird? Es gilt nun man: Dringenderes zuerst.

Was vielleicht überzeugender auf die Zweifler wirkt, ist der Hinweis, dass die IPv6-Einführung insgesamt nicht als „Big Bang“ durchgeführt werden muss. Das Stichwort heißt „Lifecycle“. Die IPv6-Umstellung betrifft die Gesamtheit der IT-Systeme: Switches, Router, Sicherheitskomponenten, Server, Endgeräte, Betriebssysteme, Middleware und Anwendungssoftware. Es ist unvorstellbar, dass die Umstellung all dieser Komponenten auf IPv6 nach einem Stichtagsprinzip gelingen kann. Deshalb ist mit einer langen Umstellungsphase zu rechnen. Vor diesem Hintergrund ist es geschickter, die IPv6-Umstellung nicht losgelöst, sondern im Zuge vom normalen Lebenszyklus der Komponenten vorzusehen. Konkret bedeutet dies: Ist die Ablösung einer Anwendung, eines Systems, einer Middleware zu einem bestimmten Termin ohnehin vorgesehen, ist dieser Termin der geeignetste Zeitpunkt der Umstellung auf den dualen Betrieb mit IPv4 und IPv6 bzw. auf reinen Betrieb mit IPv6.

Auf diese Weise wird die Hemmschwelle gesenkt, die viele Unternehmen bisher von der Beschäftigung mit IPv6 abgehalten hat. IPv6-Einführung als Begleiterscheinung des normalen Lifecycles der IT-Komponenten lässt sich einfacher durchsetzen als ein Umstellungsprojekt mit eigenem hohem Budget.

Aber die Dringlichkeits- und Budgetüberlegungen sind nicht die einzigen Argumente gegen IPv6. Auch technische Argumente werden manchmal bemüht. So wird behauptet, die Adressknappheit als Hauptmotivation für die Einführung von IPv6 sei ein Phantom. Das Argument lautet konkret, global gültige IPv4-Adressen seien schon seit den 1990er Jahren knapp, und man habe gelernt, damit umzugehen. Diese Position weist auf die Abhilfe durch Network Address Translation (NAT) hin, die angeblich das Problem der Adressknappheit eliminiere. (siehe Abbildung 1)

In ihrer Not haben sogar die Service Provider für die eigenen Netze NAT eingeführt. Wer die IPv4-Adresse seines mobilen Gerätes im öffentlichen Netz überprüft, stellt oft fest, dass die Adresse einem privaten Adressraum wie 10.0.0.0/8 oder 100.64.0.0/10 entstammt. Im Umkehrschluss bedeutet dies, dass die heutigen Applikationen auf eine global eindeutige Adresse nicht angewiesen sind.

Diese Argumentation lässt außer Acht, dass die Service Provider mit Skalierbarkeits- und Betriebsproblemen im Zusammenhang mit NAT kämpfen. Der Verkehr im Netz explodiert. Dies gilt auch für die Anzahl paralleler Verbindungen. NAT-Komponenten, die die rapide steigende Zahl der Verbindungen in Tabellen verwalten, werden zu Nadelöhren im Netz. Immer mehr solche Komponenten müssen betrieben werden. Dies bedeutet mehr Aufwand für die Service Provider und oft auch Ärgernis für ihre Kunden.

Ferner legt IPv4 der Cloud Ketten an.

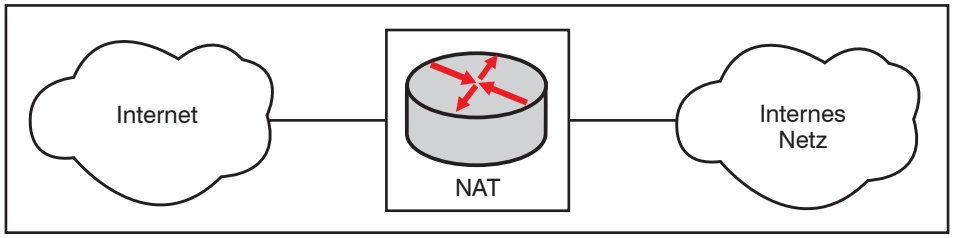

Abbildung 1: Network Address Translation

IPv6: Fundamente richtig legen

Eine Cloud lebt von der Skalierbarkeit, auch was die Anzahl der in der Cloud realisierbaren Server betrifft. Jede, auch jede virtuelle, Maschine in der Cloud braucht mindestens eine IP-Adresse, über die sie erreichbar ist. Diese Adresse sollte eine öffentliche sein. Hinter NAT verborgen kann ein Server nur ca. 60.000 gleichzeitige Verbindungen unterstützen, weil die zur Indizierung genutzte Portnummer nur 2**16 Werte ermöglicht. Nicht von ungefähr zahlte Microsoft 7,5 Millionen Dollar für ca. 666.000 IPv4-Adressen aus der Konkursmasse von Nortel. Jeder Cloud-Betreiber braucht eine schnell wachsende Zahl von öffentlichen Adressen.

Übrigens gibt es die NAT-Restriktion auch beim ausgehenden Zugriff aus einem Unternehmensnetz auf einen öffentlichen Server. Eine öffentliche IP-Adresse kann per NAT nur ca. 60.000 gleichzeitige Verbindungen mit demselben Server erlauben.

Es gibt auch Sicherheitsbedenken gegen IPv6. Hier lautet das Argument, die Nutzung privater IPv4-Adressen sei ein Sicherheitsvorteil. Eine private Adresse sei von außen nicht erreichbar, und das könne nur gut sein. Wer so argumentiert, verkennt, dass die direkte IP Connectivity für die meisten der heutigen Angriffsmuster nicht erforderlich ist. Oder anders formuliert: Es ist um die Sicherheit des Unternehmens nicht gut bestellt, wenn sich das Unternehmen nur auf private Adressen im internen Netz setzt. Dem Autor sind Unternehmen bekannt, die seit über zwei Jahrzehnten keine anderen als global gültige IPv4-Adressen einsetzen. Die Netze dieser Unternehmen gehören zu den sichersten, die der Autor kennt. Den IP-Durchgriff ins Unternehmensnetz hinein zu verhindern gehört zu den leichtesten Sicherheitsaufgaben und ist auch ohne NAT zu lösen. Heutige Angriffe sind viel komplexer und nutzen erlaubte Kanäle, um selbst bei Anwendung von NAT in das Unternehmensnetz zu gelangen. (siehe Abbildung 2)

Eine weitere Argumentationslinie gegen die Einführung von IPv6 im Unternehmensnetz besteht darin, IPv6 als eine reine Internet-Angelegenheit zu bezeichnen. Wer so argumentiert, sieht die Notwendigkeit des neuen Protokolls im öffentlichen Netz ein, um im gleichen Atemzug diese Notwendigkeit in Unternehmensnetzen abzustreiten. Man könne doch im internen Netz ein anderes Protokoll nutzen als im Internet, wo sei das Problem? Diese Argumentation baut darauf, dass die Anbieter von Hardware und Software IPv4 unbegrenzt unterstützen

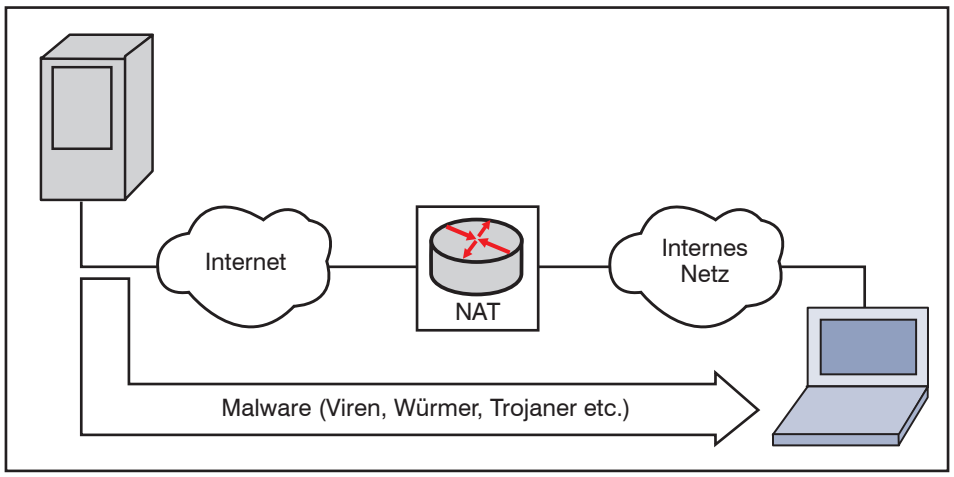

Abbildung 2: Bedrohungen, für die NAT keine ernste Barriere darstellt

werden. Die Erfahrung der letzten Jahrzehnte spricht aber dagegen. Sobald die seit einigen Jahren schnell wachsende IPv6-Nutzung im Internet IPv4 überflügelt, wird die duale Welt infrage gestellt. Viele Entwicklungen in der IT greifen vom Verbraucher- auf den Unternehmensmarkt über. So war das bei PCs, Smartphones, Tablets, und so wird es bei IPv6 sein. Das Leben auf der IPv4-Insel der Glückseligen, während ringsherum Milliarden von Geräten über IPv6 kommunizieren und das Internet of Things alles erfasst, was mit Strom oder Batterie arbeitet, wird irgendwann nicht mehr möglich sein. Es werden Systeme und Applikationen kommen, die nur IPv6 und kein IPv4 mehr unterstützen. Erste Anzeichen dafür gibt es schon. Microsoft schränkt den Support für Windows-Systeme ein, auf denen IPv6 abgeschaltet ist.

IPv6-Adresskonzept ausarbeiten

Ist es gelungen, die letzten Zweifler im eigenen Unternehmen zu überzeugen, muss man zur Vorbereitung der IPv6-Einführung zunächst konzeptionelle Arbeit leisten. Dazu gehört die Ausarbeitung eines Plans für die im Unternehmen zu nutzenden IPv6-Adressen.

IPv6 wird an einigen Prinzipien des Netzdesigns nichts ändern. Zu diesen Prinzipien gehört die Einteilung der Netze in Subnetze. Auch IPv6-Subnetze müssen über Router miteinander kommunizieren. Deshalb werden automatisch generierte Link-Local Addresses (LLAs) nicht ausreichen. LLAs erlauben nur die Kommunikation in einem Subnetz.

Geroutete IPv6-Adressen sind entweder Global Addresses (GAs) oder Unique Lo-

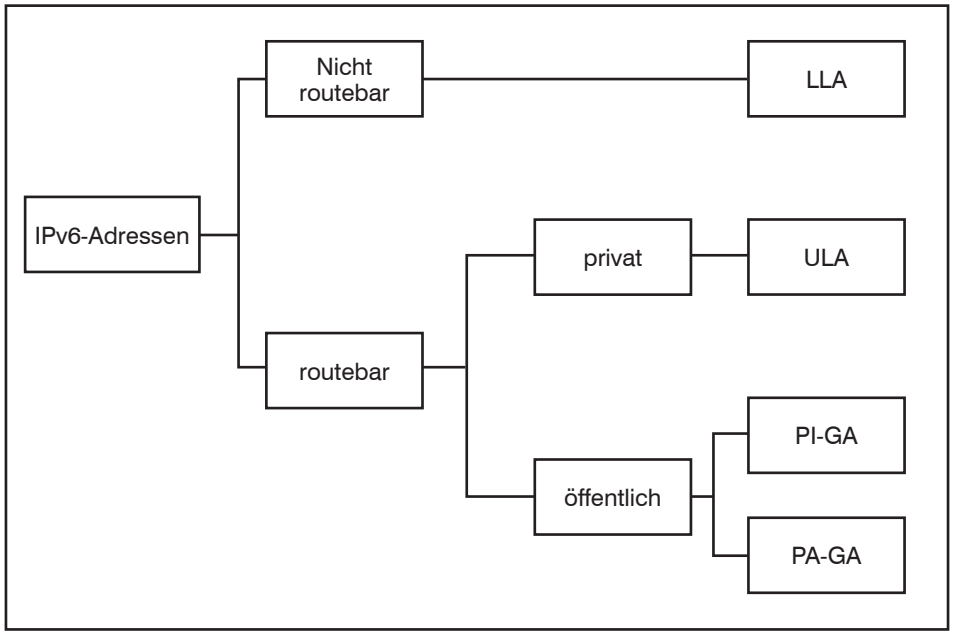

Abbildung 3: Kategorisierung von IPv6-Adressen

cal Addresses (ULAs), wie aus der Abbildung 3 hervorgeht. GAs sind mit öffentlichen IPv4-Adressen vergleichbar. Sie sind weltweit gültig. Ein Gerät mit einer GA kann direkt auf der IP-Ebene mit jedem anderen Gerät im Internet kommunizieren. ULAs sind mit privaten IPv4-Adressen vergleichbar. Sie werden im Internet nicht geroutet. ULAs sind nur innerhalb der Grenzen eines Unternehmens eindeutig.

Das IPv6-Adresskonzept muss die Entscheidung für den Einsatz von GAs oder ULAs im Unternehmensnetz fällen und begründen. Diese Entscheidung kann nur unternehmensspezifisch gefällt werden. Wer die Notwendigkeit der direkten IP-Verbindung eines Gerätes mit externen Netzen ausschließt, kann für dieses Gerät eine ULA vorsehen. Proxies auf Transport- oder Applikationsebene ermöglichen bekanntlich Geräten ohne direkte IP-Verbindung den Zugriff auf das Internet. Es ist aber zu bedenken, dass die heutige Middlebox-Architektur, zu denen Firewalls und Proxies gehören, nicht von Ewigkeit sein muss. Sie skaliert nicht und ist schwer zu betreiben. Aus diesem Grund gibt es zurzeit Überlegungen, Middlebox-Funktionalität mit einer anderen Architektur zu erreichen. Dies könnte im Sicherheitsbereich zum Beispiel darin bestehen, dass die Sicherheitsregeln von einer Vielzahl Netzkomponenten durchgesetzt werden. Eine denkbare Sicherheitsarchitektur kann die heutige Praxis, am Perimeter innere und äußere Sessions zu entkoppeln, durch eine andere ersetzen. Es ist denkbar, dass für die Durchsetzung der Sicherheitsregeln die Entkopplung der Sessions am Perimeter und damit die Verhinderung der direkten IP-Kommunikation nicht erforderlich sein werden. Private Adressen erzwingen jedoch eine solche Entkopplung. Ein Adresskonzept mit global gültigen Adressen ist damit flexibler und zusammen mit jeder denkbaren Sicherheitsarchitektur einsetzbar.

Globale Adressen sind entweder providerunabhängig (Provider Independent, PI) oder aus dem zusammenhängenden Block eines Providers (Provider Aggregatable, PA). PA-Adressen haben den Nachteil, dass beim Providerwechsel die Adressen geändert werden müssen. Dies klingt aufwändiger als es vielleicht sein wird. IPv6 erlaubt aufgrund der vierfachen Zahl der Bits pro IPv6-Adresse eine strikte Trennung des vom Provider zugewiesenen Präfixes von den Bestandteilen der Adresse, die für die interne Strukturierung des Netzes und unter Umständen auch für die Klassifizierung von Gerätetypen und für Sicherheitsregeln verwendet werden. Das providerspezifische Präfix kann sich ändern, ohne dass man die

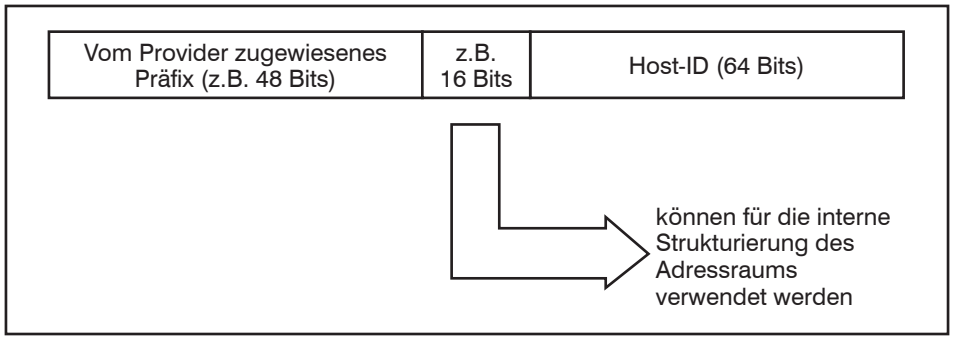

Abbildung 4: Beispiel für die Aufteilung des IPv6-Adressfelds

weiteren Bits antasten muss. Zum Beispiel kann man ein 48 Bit langes, vom Provider A zugewiesenes Präfix durch ein gleich langes (oder kürzeres, in diesem Fall bis zum 48. Bit beliebig auffüllbares) Präfix ersetzen, das von einem Provider B zugewiesen wird. (siehe Abbildung 4)

Dabei kann man die restlichen 80 Bits auf allen Endgeräten, Routern, Firewalls etc. unverändert lassen. Das Ersetzen des Präfixes beschränkt sich auf Änderungen an Systemen, auf denen das Präfix eingestellt wird. Im Falle der Nutzung des Dynamic Host Configuration Protocol (DHCP) sind dies die DHCP-Server, im Falle von Stateless Address Autoconfiguration (SLAAC) die Router. Ein Unterschied zu IPv4 besteht darin, dass es mit IPv6 realistisch wird, von jedem Provider eine auch für die interne Verwendung genügende Zahl von Adressen zu bekommen. Unter IPv4 kann man wegen der mittlerweile herrschenden akuten Adressknappheit bei einem Providerwechsel nie sicher sein, einen zusammenhängenden Adressblock durch einen anderen mindestens gleich großen ersetzen zu können.

Auch wenn beim Wechsel von einem zum anderen Provider nur das Providerpräfix von PA-Adressen geändert werden muss, kann das Vermeiden des damit verbundenen Aufwands und Betriebsrisikos eine Motivation für den Einsatz von PI-Adressen sein. Für global agierende Unternehmen sind PI- besser als PA-Adressen geeignet. Man stelle sich den Aufwand vor, der im globalen Netz eines Unternehmens entsteht, auch wenn sich nur in einer Region ein Präfix ändert. Möglicherweise muss auch einiges in anderen Regionen geändert werden. Auch wenn durch konsequente Nutzung des Domain Name System (DNS) alles außer der Einstellung des Präfixes selbst auf DHCP-Servern und Routern automatisch gehen sollte, sind zumindest die Planung des Wechsels und die entsprechenden Vorkehrungen gegen die damit verbundenen Risiken ziemlich aufwändig.

Woher bekommt man PI-Adressen? In der Regel sind die Regional Internet Registries (RIRs) für die Vergabe von PI-Adressen zuständig. Réseaux IP Européens (RIPE) ist die RIR für Europa. Andere Regionen wie Nordamerika, Lateinameri-

ka, Afrika und Asien haben ihre eigenen RIRs. Für ein global agierendes Unternehmen stellt sich die Frage, ob es pro Region einen eigenen Adressbereich beantragt oder PI-Adressblöcke überregional einsetzt. Wenn das Unternehmen in einer Region einen eigenen Internet-Anschluss nutzt, müssen die dafür genutzten PI-Adressen im Internet geroutet werden. Es ist nicht selbstverständlich, dass Provider Adressen abweichend vom weltweiten regionalen Schema routen. Denn angesichts der potenziell sehr hohen Anzahl von IPv6-Netzen kann ein Provider anstreben, ganze Weltregionen jeweils über aggregierte Adressen zu erreichen. Wenn Abweichungen von diesem Schema zur Regel werden, können die Routing-Tabellen Dimensionen annehmen, die die heute für IPv4 eingesetzten Tabellen um Größenordnungen übertreffen.

Vor diesem Hintergrund besteht die zukunftssicherste Variante für ein global agierendes Unternehmen darin, jeden regionalen Internetanschluss mit Adressen aus der betreffenden Region zu betreiben (Abbildung 5). Dies erhöht zwar den Aufwand für die Beantragung von Adressen, stellt aber sicher, dass die Erreichbarkeit der Internetanschlüsse des Unternehmens nicht von der Routing-Politik der Provider abhängt. Ferner stehen dem Unternehmen mit mehreren regionalen Blöcken insgesamt mehr Adressen zur Verfügung.

Was die Größe der den Unternehmen zugewiesenen Adressblöcke betrifft, gibt es eine gute Nachricht. Unternehmen erhalten in der Regel maximal 48 Bits lange Präfixe. Zieht man von den verbliebenen 80 Bits den standardmäßig 64 langen Host Identifier ab, verbleiben zwischen dem zugewiesenen Präfix und dem Host Identifier 16 Bits. Diese 16 Bits ermöglichen die Bildung von 65536 Subnetzen. Der Luxus, eine solche Anzahl von Subnetzen jeweils mit einem Maximum von beispielsweise 256 Adressen bilden zu können, ist unter IPv4 nur wenigen Unternehmen vorenthalten, die Class-A-Adressen zur Verfügung haben. RIRs vergeben darüber hinaus auch größere Adressblöcke, d.h. kleinere Präfixe als /48, wenn das Unternehmen den Bedarf begründen kann. Je nach Branche, in der das Unternehmen tätig ist, sind verschiedene Szenarien denkbar, in denen der Bedarf an Adressen in den nächsten Jahren um Größenordnungen steigen kann. Im Produktionsbereich ist dieser Trend bereits seit Jahren feststellbar. Als vierte industrielle Revolution wird die Einführung des Internet of Things (IoT) in der Fertigung bezeichnet. Nicht nur die Produktionsmaschinen, sondern auch die Produkte sollen kommunikationsfähig werden.

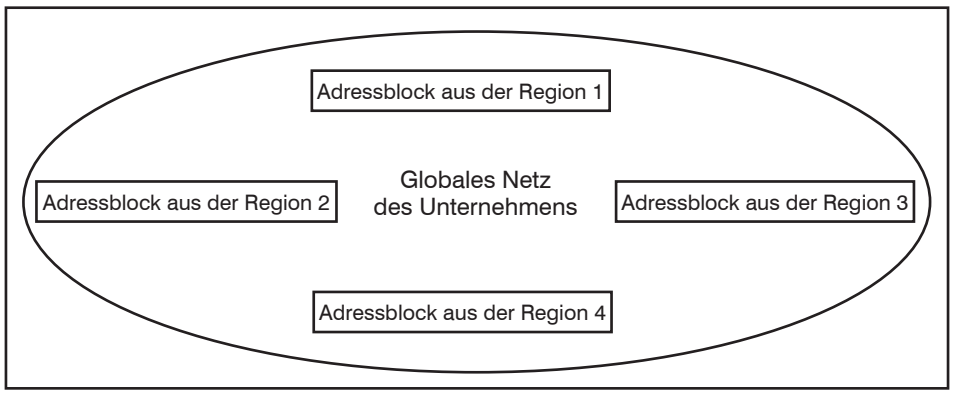

Abbildung 5: Nutzung verschiedener Adressblöcke im globalen Netz

Kommunikation wurde dabei in den letzten Jahrzehnten immer mehr zur IP-Kommunikation.

Die interne Strukturierung des verfügbaren IPv6-Adressraums ist von der Größe des verfügbaren IPv6-Adressraums sowie der Anzahl und der Größe der Standorte des Unternehmens abhängig. Eine konsequentere Zusammenfassung von Subnetzen ist unter IPv6 möglich. Damit lassen sich die Routing-Tabellen mit den unhandlicheren IPv6-Adressen verkleinern.

Die interne Strukturierung des Adressraums kann nach rein geografischen Aspekten erfolgen. Ergänzend können einige Bits für eine Kodierung des Gerätetyps verwendet werden. Die Notwendigkeit der Kodierung von Gerätetypen wird nicht einheitlich bewertet. Einige Unternehmen gehen davon aus, dass die heute unterscheidbaren Gerätetypen langfristig nicht unbedingt Bestand haben werden. Aus dieser Ungewissheit leiten diese Unternehmen ab, dass eine Verwendung einiger Bits der IPv6-Adresse als Gerätecode nicht sinnvoll ist. Andere Unternehmen erwarten zum Beispiel eine dauerhafte Unterscheidung zwischen dem Client- und dem Server-Bereich. Ein Code, der die Unterscheidung zwischen Client und Servern auf sehr einfache Art ermöglicht, kann manche Sicherheitsregel übersichtlicher machen.

Festlegung der Methoden der Konfiguration von Hosts

Unter IPv6 ist DHCP nicht die einzige Methode für die automatische Zuweisung von Adressen. DHCP-Unterstützung ist nicht einmal zwingender Bestandteil des von Endgeräten zu unterstützenden IPv6-Funktionsumfangs. Dafür müssen alle Endgeräte SLAAC unterstützen.

Einige Unternehmen haben unter IPv4 die Vorteile der zentralen Verwaltung der Adressen schätzen gelernt. Diese Unternehmen legen Wert darauf, auch IPv6-Adressen in einer zentralen Datenbank zu dokumentieren. Gegen die 1:1-Übertragung der Methoden der Konfiguration der Endgeräte von IPv4 auf IPv6 spräche nichts, wenn alle Endgeräte die DHCP-Methode unterstützten. Dies ist leider nicht der Fall. Vor allem die Entwickler von Android sträuben sich immer noch gegen die Implementierung von DHCPv6 für Android. Da viele mobile Endgeräte auf Android basieren, müssen Unternehmen, die solche Endgeräte einsetzen, diese entweder manuell konfigurieren oder SLAAC einsetzen. Eine gemischte Adresszuweisung über DHCP und

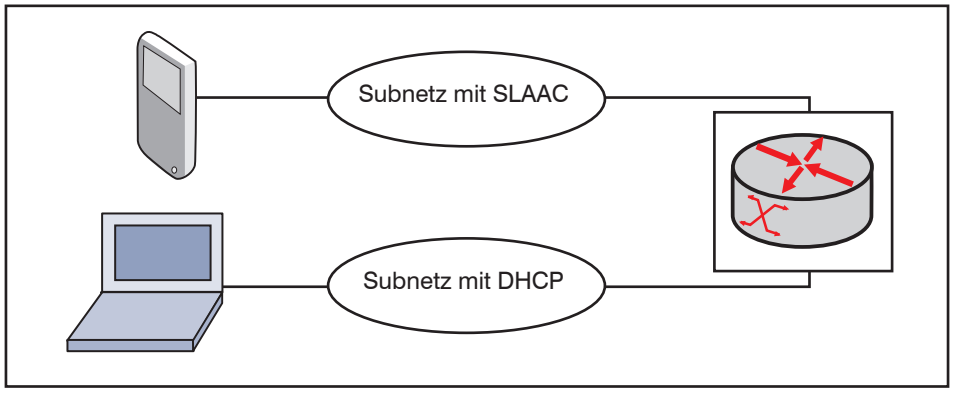

Abbildung 6: Subnetz mit SLAAC und Subnetz mit DHCP

SLAAC im selben Subnetz ist nicht möglich, weil die Steuerung der Nutzung eines dieser Verfahren durch ein Endgerät anhand von Router Advertisments (RAs) erfolgt, die pro Subnetz die eine oder andere Methode vorgeben. (siehe Abbildung 6)

Die Nutzung von SLAAC ist mit oder ohne Security Extensions möglich. Ohne Security Extensions wird die MAC-Adresse eines Endgeräts als Teil des 64 Bits langen Host Identifier übernommen. Das Bewegungsprofil des Gerätes ist somit für alle seiner Kommunikationspartner sichtbar. Ein solches Bewegungsprofil verrät vielleicht mehr als von manchen Unternehmen toleriert werden kann. Security Extensions für SLAAC ermöglichen statt der Übernahme der MAC-Adresse die Nutzung wechselnder, nichts über das Gerät verratender Werte im Host Identifier.

IP-Adressen sind nicht die einzigen Parameter, die auf Geräten eingestellt werden müssen. Eine funktionierende IP-Konfiguration muss auf jeden Fall auch die Information enthalten, unter welcher oder welchen Adressen das Gerät den Domain Name Service erreichen kann. Je nach Funktionsumfang von Geräten ist die Einstellung der DNS-Adresse über DHCP oder über Informationen in RAs möglich. Alternativ können Geräte Anycast nutzen, um DNS zu erreichen.

Festlegungen der Methoden für die IPv6-Konfiguration von Endgeräten müssen die Besonderheiten der eingesetzten Endgeräte berücksichtigen.

Was ändert sich im LAN Design?

Da die Umstellung von IPv6 auf IPv4 nicht über Nacht, sondern möglichst im Zuge des normalen Lebenszyklus von Systemen und Applikationen erfolgen wird, ist mit einem langen Nebeneinander der beiden Protokolle zu rechnen. Diese Situation ist nicht unbekannt. Bis in die 1990er Jahre wurden Netze im Multiprotokollmodus betrieben. Neben IP gab es noch Systems Network Architecture (SNA) für die Kommunikation mit Großrechnern, Internetwork Packet Exchange (IPX) für den Zugriff auf Netware File Server des Herstellers Novell, DECnet von Digital Equipment Corporation und noch ein paar andere Protokolle, die mittlerweile fast in Vergessenheit geraten sind. Nach und nach stellten die Hersteller ihre Systeme auf IP um. Der Multiprotokollbetrieb wich dem einfacheren reinen IP-Betrieb.

Wenn nun IPv6 eingeführt wird, während IPv4 weiter zu nutzen ist, ersetzt der Modus mit zwei Protokollen die bisherige Monokultur mit IPv4. Zumindest die Netzkomponenten, vor allem die Routing-Instanzen, müssen auf den dualen Modus umgestellt werden. Auf Routern und Layer-3-Switches erfolgt dies dadurch, dass jede Netzschnittstelle neben der IPv4-Adresse noch eine IPv6-Adresse erhält (siehe Abbildung 7). Zusätzlich müssen Routing-Mechanismen für IPv6 eingestellt werden.

Im internen Netz wird sich der Zuschnitt der Subnetze für IPv6 gegenüber dem für IPv4 dort ändern, wo IPv4-Adressknappheit Entscheidungen diktiert haben, die man mit mehr verfügbaren Adressen anders gefällt hätte. Solange aber die ersten reinen IPv6-Endgeräte auf sich warten lassen, wird es keine reinen IPv6-Subnetze geben. So muss das IPv6-Adresskonzept auf die bestehende Unterteilung in Subnetze abgebildet werden. Die Größe der IPv6-Subnetze wird sich auf jeden Fall gegenüber IPv4 ändern, denn kein IPv4-Subnetz stellt 64 Bits für die Endgeräteadressierung zur Verfügung. 64 Bits stehen nämlich unter IPv6 standardmäßig für Host-IDs zur Verfügung. Aber die Unternehmen werden schon aus Gründen der Sicherheit und Robustheit der Netze in der Regel die Zahl der Geräte pro Subnetz unter 1.000 halten.

Dort wo es keine Endgeräte gibt, zum Beispiel bei Links zwischen zwei Layer-3 Switches, kann man theoretisch auch die 64 Bits, die der Host-ID vorenthalten sind, für die Aufteilung in verschiedene Subnetze nutzen. Dies ist davon abhängig, ob die Layer-3-Switches eine solche Aufteilung unterstützen.

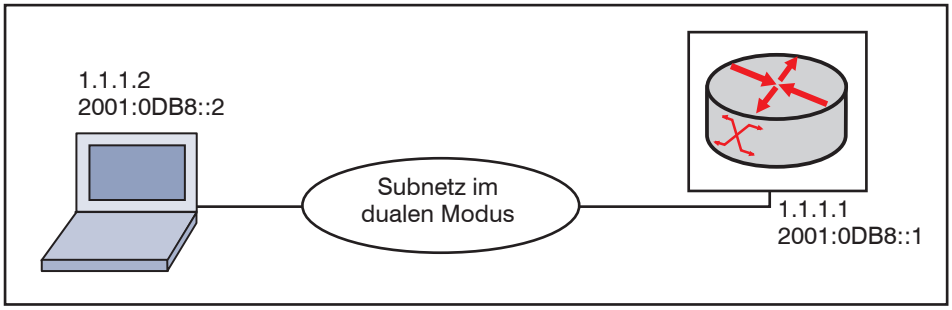

Abbildung 7: Subnetz im dualen Modus

Theoretisch kann man auf Punkt-zu-Punkt-Verbindungen (P2P Links) zwischen zwei Routing-Instanzen auf routebare Adressen verzichten und LLAs einsetzen. Aber LLAs können von außerhalb eines Subnetzes nicht erreicht werden. Damit kann man zum Beispiel die Erreichbarkeit der beiden Enden eines P2P Links nicht über das Netz überprüfen. Deshalb ist es üblicher, wie unter IPv4 routebare IPv6-Adressen auch für P2P Links vorzusehen.

Auf den ersten Blick mag es als Verschwendung erscheinen, auf P2P Links ganze Subnetze mit bis zu 2**64 Adressen zu konfigurieren. Die eigentliche Frage muss aber lauten, wie viele Subnetze man einsparen würde, wenn man dies nicht täte. Das Beispiel in der Abbildung 8 soll der Klärung dieser Frage dienen.

Wenn man vereinfachend davon ausgeht, dass die Zahl der P2P Links zweimal so hoch ist wie die Zahl der Layer-3-Instanzen, kann man die Größenordnung der Anzahl der P2P Links berechnen. Bei Anwendung einer weiteren Vereinfachung könnte man für die Zahl der Layer-3-Instanzen 25 % der Zahl der Layer-2 Switches annehmen. Und wenn man annimmt, dass die Zahl der Layer-2 Switches gleich 10 % der Anzahl der Endgeräte ist, kann man die Zahl der P2P Links berechnen:

Zahl der P2P Links =
2 * 25 % * 10 % * Anzahl Endgeräte =
5 % * Anzahl Endgeräte

Wenn ein Subnetz durchschnittlich 10 Endgeräte aufnimmt, also die Anzahl der Endgerätesubnetze 10 % der Anzahl der Endgeräte beträgt, ist der Overhead der P2P-Subnetze wie folgt zu berechnen:

Overhead der P2P Links =
5 % * Anzahl Endgeräte / (10 % * Anzahl Endgeräte) =
50 %

Die P2P Links fügen also 50 % Overhead zur Anzahl der Subnetze hinzu. Das klingt viel, ist aber auf den zweiten Blick nur gleichbedeutend damit, dass man von den mindestens 16 Bits, die man zur internen Strukturierung zur Verfügung hat, ein Bit verliert. Dann hätte man sogar so viele Subnetze für P2P Links zur Verfügung wie für Endgeräte, also 100 % statt 50 %.

Der Vorteil, den man dadurch bekommt, ist die Verkleinerung der Anzahl der Einträge in Routing-Tabellen. Schon auf der ersten übergeordneten Layer-3-Instanz kann man nämlich alle Endgeräte- und P2P-Subnetze zusammenfassen und als aggregierte Route behandeln. Die lästigen Einträge für P2P Links, die schon unter IPv4 unangenehm auffallen, verschwinden.

Nun kann es auch Kompromisse geben, wieder vorausgesetzt, die Layer-3-Instanzen unterstützen längere Präfixes als /64. Man könnte zum Beispiel alle P2P Links an einem Standort zusammenfassen, und pro Standort erscheint in den Routing-Tabellen der WAN-Router eine zusätzliche Route für P2P Links. Der ganze Adressraum für P2P Links kann dann wesentlich kleiner sein als der für Endgeräte genutzte Adressraum.

Das im Vergleich zu IPv4 viel größere Reservoir an Adressen ist nicht der einzige Aspekt, unter dem Design-Unterschiede zwischen IPv4 und IPv6 denkbar sind. Man kann zum Beispiel auch darüber nachdenken, für IPv6 ein anderes Routing-Protokoll einzusetzen als für IPv4. Allerdings ist dies zumindest bei den Anwendern von OSPF (Open Shortest Path First) als dem de facto Standard für unternehmensinternes Routing nicht üblich. Da OSPF für IPv6 seit Jahren verfügbar und stabil ist, gibt es oft keinen Grund, verschiedene Routing-Protokolle für IPv4 und IPv6 einzusetzen. In der Regel setzt man zwei verschiedene Instanzen bzw. Prozesse desselben Routing-Protokolls für IPv4 und IPv6 ein. Die beiden Instanzen sind unabhängig voneinander und können auch unterschiedlich eingestellt werden, wenn es sein muss, zum Beispiel was die Metriken betrifft. Wenn es aber keinen zwingenden Grund für Abweichungen gibt, übernimmt man für IPv6 die Einstellungen unter IPv4.

Das gilt auch für das First Hop Redundancy Protocol (FHRP), das für die redundante Gestaltung von Routern in einem Subnetz verwendet wird. (siehe Abbildung 9)

Theoretisch können zwei redundante Router unabhängig voneinander RAs in Endgerätesubnetze senden, sodass jedes Endgerät beide Router kennt. Dann kann ein Endgerät von einem zum anderen Router wechseln, wenn ein Router nicht erreichbar ist. Aber die meisten Netzbetreiber wollen sich nicht auf Mechanismen der Endgeräte für die Realisierung von redundantem Routing verlassen. Das bleibt auch bei IPv6 so. Deshalb gibt es auch unter IPv6 die üblichen Mechanismen für die redundante Auslegung des First Hop für Endgeräte:

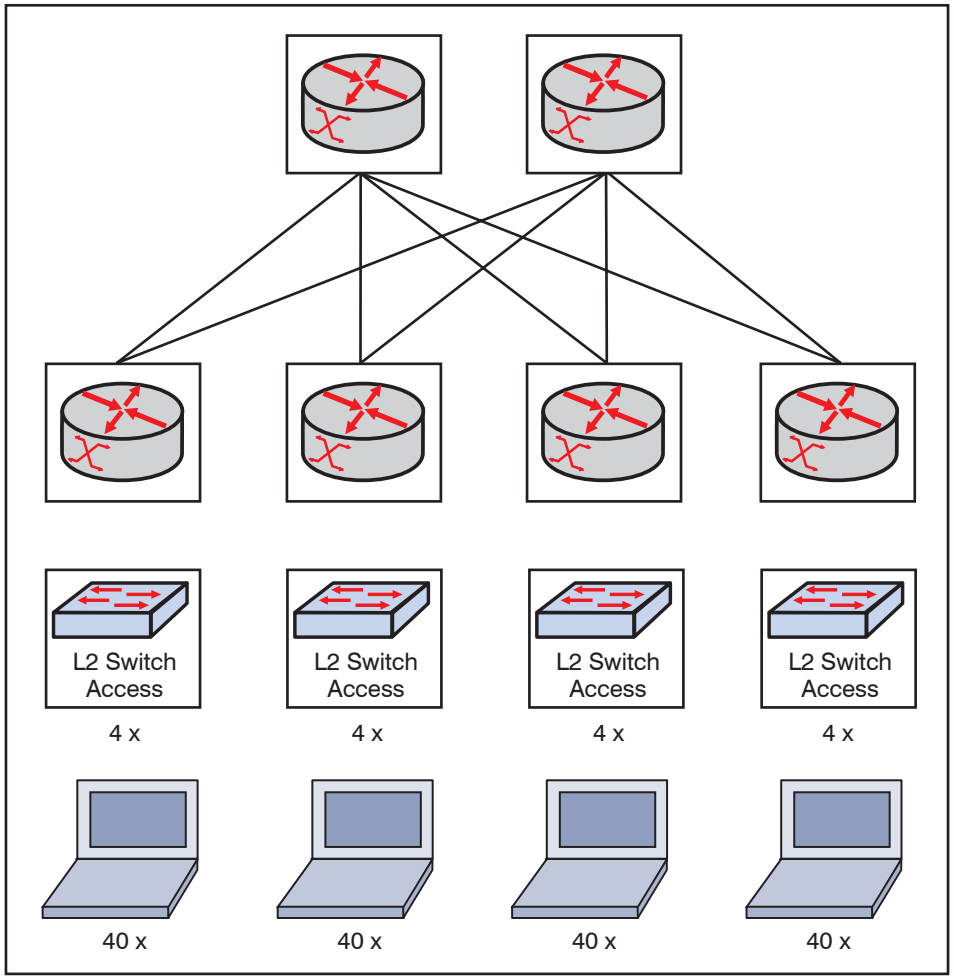

Abbildung 8: Beispiel für die Berechnung der Zahl der P2P-Links

- Virtuelle Switches: Zwei Layer-3-Switches bilden einen virtuellen Switch und stellen aus der Sicht der Endgeräte logisch eine Instanz dar bzw. sind über dieselbe MAC- und IP-Adresse erreichbar. Diese virtuellen Adressen werden automatisch vom zweiten Switch übernommen, wenn der erste ausfällt.
- FHRP: Die beiden Layer-3-Switches sind unabhängig voneinander und haben auch eigene IP Interfaces pro Subnetz, aber als First Hop bzw. Default Router wird auf den Endgeräten eine Adresse eingestellt, die zu jedem Zeitpunkt von einem der beiden Router bedient wird. Fällt er aus, übernimmt der zweite die Adresse. Diese Umschaltung wird von einem FHRP gesteuert. Es gibt das standardisierte Virtual Router Redundancy Protocol (VRRP) und proprietäre FHRPs. Diese Protokolle sind für IPv6 ebenfalls nutzbar.

IPv6 Routing im WAN

Während LANs in der Regel exklusiv von einem Unternehmen genutzt werden und

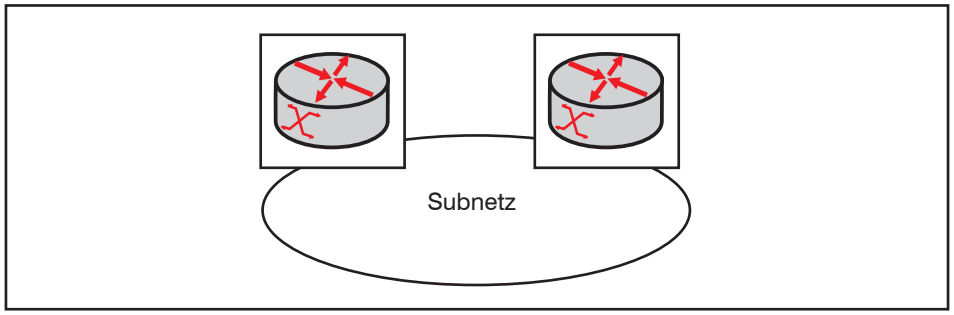

Abbildung 9: Subnetz mit zwei redundanten Routern

daher entsprechend dem Bedarf und den Präferenzen des Unternehmens konfiguriert werden können, gibt es im Wide Area Network (WAN) häufig eine Abhängigkeit vom WAN Provider. Bekanntlich bedienen WAN Provider verschiedene Kunden mit derselben Plattform. Diese Plattform muss sehr stabil und robust funktionieren, denn ein Ausfall würde alle mit der Plattform bedienten Kunden des Providers betreffen. Deshalb testen und verifizieren die WAN Provider jeden neuen Mechanismus eingehend und intensiv, bevor sie ihn einsetzen. Wenn die Einführung des Mechanismus den laufenden Betrieb auch nur kurzzeitig unterbrechen kann, dauert es lange, bis man einen geeigneten Zeitpunkt für die Änderung gefunden hat.

Dieser langen Test- und Integrationsphase geschuldet sind einige WAN Provider noch nicht so weit, dass sie zum Beispiel Multi-Protocol Label Switching wirklich im Modus „Multi-Protocol" betreiben. Bis diese Provider neben IPv4 auch IPv6 über ihre MPLS-Plattform übertragen, kann noch einige Zeit vergehen.

Einem Kunden, der bei der Einführung von IPv6 nicht so lange warten will, bieten sich zwei Optionen:

- Er nutzt weiterhin den IPv4 Routing Service des Providers. Dann muss IPv6 in IPv4 getunnelt werden. Die Tunnelendpunkte können zum Beispiel Router sein, die die entsprechende Tunnelfunktion unterstützen.

- Er nutzt einen Layer 2 Service im WAN. Dann ist das Routing unabhängig vom Provider. Die Routing-Instanzen werden im dualen Modus vom Kunden betrieben.

In einem internationalen WAN kann die Beschränkung auf Layer 2 im WAN den Kreis der potenziellen Anbieter im Provider-Markt verkleinern. Herkömmlicher Routing Service auf MPLS-Basis ist immer noch der de facto Standard für internationale WANs.

Internet-Anbindung

Die Internet-Anbindung ist für viele Unternehmen der erste Bereich, der IPv6 unterstützen soll. Dies ist vor allem darauf zurückzuführen, dass sich IPv6 im Moment stärker im Internet als in internen Netzen ausbreitet. Die Internet-Anbindung soll die Kommunikation mit jedem Ziel im Internet ermöglichen. Eine Beschränkung auf IPv4 bei der Internet-Anbindung birgt nicht nur das Risiko, dass irgendwann in Zukunft einige externe Kommunikationsbeziehungen nicht möglich sind. Auch wenn

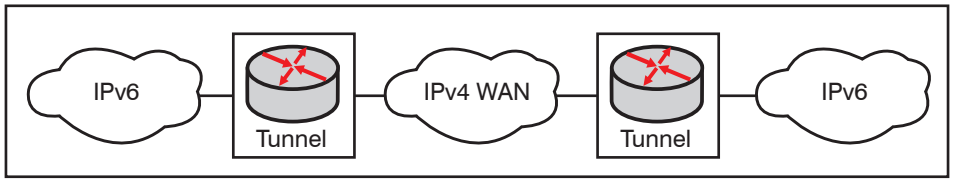

Abbildung 10: IPv6-in-IPv4-Tunnel im WAN

heute jeder eingehende und jeder ausgehende Zugriff über das Internet IPv4 nutzen kann, verzichtet man mit einer eigenen IPv6-Anbindung auf alternative neue Wege und Übertragungspfade, die im Internet auf IPv6-Basis entstehen.

Ferner kann es für einige Unternehmen eine Frage des innovativen Images sein, auch unter IPv6 im Internet Präsenz zu zeigen.

Zunächst muss der Internet Service Provider IPv6-Übertragung unterstützen. Hier ist es ähnlich wie bei WAN-Providern: nicht alle sind so weit, dass sie IPv6 übertragen können. Hier helfen aber auch keine Workarounds wie Tunnels. Wenn man auf eine IPv6-Anbindung an das Internet Wert legt, muss man einen Provider finden, der dazu in der Lage ist.

Je nach IPv6-Adresskonzept übernimmt der Provider über das reine IPv6 Routing auch noch andere Aufgaben in diesem Zusammenhang. Er kann zum Beispiel als Sponsoring Local Internet Registry (LIR) agieren und die Einträge über die Zuordnung eines IPv6-Adressbereichs zum Unternehmen bei der zuständigen RIR pflegen. Wie bei IPv4 auch kann der ISP ferner der Inhaber des Autonomen Systems (AS) sein, über das der Internet-Zugang des Unternehmens geführt wird. Dies ist nicht zuletzt von der Art der Gestaltung der Internet-Anbindung abhängig. Legt ein Unternehmen darauf Wert, über zwei verschiedene ISPs mit dem Internet verbunden sein, besteht eine Option darin ein eigenes AS zu betreiben. Zwischen verschiedenen Autonomen Systemen im Internet wird bekanntlich das Border Gateway Protocol als Routing-Mechanismus verwendet. Das ist unter IPv6 nicht anders als unter IPv4, wie aus der Abbildung 11 hervorgeht.

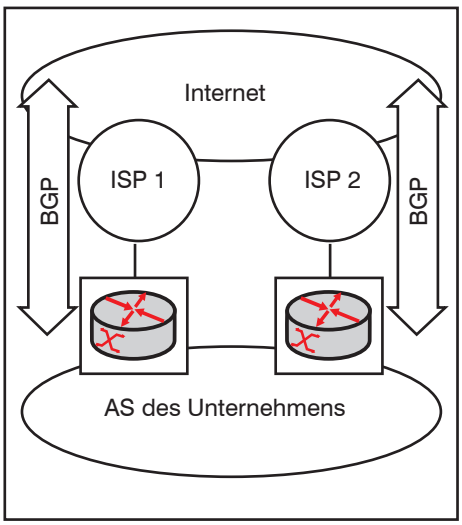

Abbildung 11: Nutzung von BGP

Aber reines Routing macht noch keinen Internet-Zugang. Es ist noch zu entscheiden, welche Systeme über IPv6 extern kommunizieren. Hier ist zwischen eingehendem und ausgehendem Zugriff zu unterscheiden.

Für den ausgehenden Zugriff kann man zum Beispiel Web Proxies so konfigurieren, dass sie auch IPv6 nutzen. Gute Web Proxies erlauben die Einstellung von Richtlinien für den Umgang mit zwei Protokollen. Zum Beispiel kann es sinnvoll sein, in der ersten Phase IPv4 zu favorisieren und bei Verfügbarkeit von DNS-Einträgen für beide Protokolle (A Records für IPv4 und AAAA Records für IPv6) IPv4 vorzuziehen. Die Motivation für eine solche Richtlinie kann sein, eventuelle Probleme mit der IPv6-Erreichbarkeit des Zielsystems zu umgehen. Sind IPv6-Routen mittlerweile so stabil, dass man sie von Anfang an gegenüber IPv4 bevorzugt? Leider fällt die Antwort auf diese Frage so differenziert aus wie es denkbare Ziele im Internet gibt. Große Content-Anbieter wie Google haben schon seit Jahren Erfahrungen mit IPv6 und bieten eine weitgehend stabile IPv6-Präsenz. Das kann bei kleineren Anbietern ganz anders aussehen. Es mag sein, dass ein Anbieter über A und AAAA Records bekannt ist, aber noch Probleme mit IPv6 Routing im externen oder internen Netz hat. Hier kann nur die Praxis aufschlussreich sein. In den letzten Jahren haben uns immer weniger Berichte von instabilen IPv6-Routen erreicht.

Auf jeden Fall sollte ein Web Proxy die Möglichkeit unterstützen, bei Nichtverfügbarkeit der Verbindung über ein Protokoll auf das andere umzusteigen. Die Möglichkeit der Feineinstellung entsprechender Time-out-Werte wäre ebenfalls hilfreich.

Bei eingehenden Zugriffen stellt sich umgekehrt die Frage, ob man sowohl der ei-

genen internen Infrastruktur als auch der externen IPv6-Anbindung so weit vertraut, dass man unter Nutzung von IPv6 Inhalte im Internet präsentiert. Auch hier sind die in den Anfangsjahren hin und wieder vernehmbaren Berichte über nicht erreichbare Inhalte aufgrund instabiler IPv6-Routen einem Status gewichen, in dem man solche Berichte selten zu hören bekommt. Die interne Infrastruktur hat man ohnehin im eigenen Einflussbereich. Das reine IPv6 Routing ist mittlerweile als sehr stabil einzustufen. Problematisch können die Middleboxes werden: Firewalls, Reverse Proxies und Load Balancer. Und am Ende der Kette steht noch ein Endsystem mit einer Anwendung, zum Beispiel ein Web Server, wie in der Abbildung 12 dargestellt.

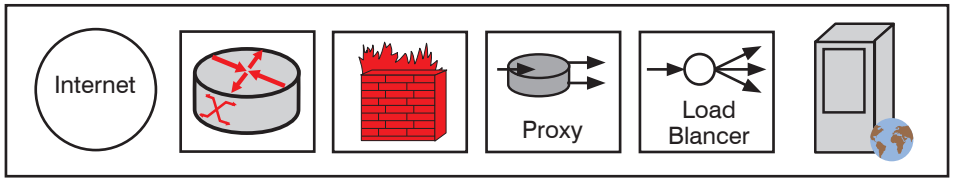

Abbildung 12: Typische Kette beim eingehenden Zugriff aus dem Internet

Die einfachste Lösung ist eine Translation-Lösung direkt am Internet-Übergang. Dabei werden alle eingehenden IPv6-Verbindungen über das Internet auf einem Gerät, das NAT64 (NAT zwischen IPv6 und IPv4) unterstützt, terminiert und intern als IPv4-Verbindung neu aufgebaut. In weiteren Schritten kann man IPv6 tiefer in das interne Netz hereinlassen. Wann und wie weit, ist davon abhängig, ob die betreffenden Middleboxes unter IPv6 dieselben Funktionen unterstützen wie unter IPv4, und ob sie im dualen Modus stabil und ohne unangenehme Nebenwirkungen betreibbar sind.

Interessant könnte die IPv6-Präsenz im Internet für Virtual Private Networks werden. Mein Kollege Dr. Wetzlar berichtete mir vor Jahren von einem Hotel in der Schweiz, in dem der IPv6-Zugang zum Internet kostenlos und der IPv4-Zugang kostenpflichtig ist. Auf solche Ideen können Provider kommen, wenn sie an der zunehmenden Verlagerung des Verkehrs von IPv4 auf IPv6 interessiert sind.

Nicht nur solche Promotion-Angebote der Provider, sondern auch die Vermeidung von NAT in Providernetzen kann eine Motivation dafür sein, über IPv6 auf das VPN des eigenen Unternehmens zuzugreifen. Voraussetzung ist natürlich die Verfügbarkeit eines IPv6-Zugangs. Ist ein solcher vorhanden, kann man davon ausgehen, dass man ohne NAT bis zum VPN durchkommt. Das kann unter Umständen schneller und leistungsfähiger sein als der IPv4-Weg, der vielleicht Carrier-Grade NAT beim Provider durchläuft.

Eine andere Frage als das im Internet genutzte Medium ist, ob man im VPN-Tunnel IPv4 oder IPv6 überträgt. Das ist von der IPv6-Ertüchtigung der Endgeräte und Systeme auf beiden Seiten abhängig. Es ist erwägenswert, mit der Client-Seite anzufangen und auf dem Client die duale Protokollunterstützung einzuführen. Handelt es sich beim Betriebssystem auf dem Client um eine aktuelle Windows-Version, braucht man nur über den VPN-Tunnel (bei Client-to-Site) oder mittels der Layer-3-Instanzen am Client-Standort (bei Site-to-Site) dem Client die IPv6-Konfiguration zu vermitteln. Dann kann der Client über IPv6 auf jede interne Anwendung und jedes interne System zugreifen, das mit der Zeit verfügbar wird. Nur nach getesteter Verfügbarkeit eines solchen IPv6-Weges sollte auch ein entsprechender Eintrag im DNS angelegt werden, denn sonst läuft der Verbindungsversuch des Clients ins Leere.

Besonderheiten bei Extranets

Einige Unternehmen nutzen neben dem Internet und dem internen Netz noch Extranets. Ein Extranet ist ein nichtöffentliches Netz, das verschiedene Organisationen miteinander verbindet. Es gibt verschiedene Ausprägungen von Extranets. Eine Ausprägung kann vorsehen, dass Systeme des Unternehmens A nie direkt mit Systemen des Unternehmens B kommunizieren, sondern nur über ein bestimmtes System C, das zum Beispiel eine Collaboration Suite bereitstellt. Eine andere Ausprägung kann den direkten Zugriff der Systeme eines Unternehmens auf die Systeme eines anderen Unternehmens vorsehen.

In beiden Fällen ist das IP Routing zu klären. Zwei Unternehmen können zum Beispiel vereinbaren, dass ein gemeinsam genutztes System mit einer Adresse konfiguriert wird, die mit keiner internen Adresse in den beiden Unternehmensnetzen kollidiert. Das ist bei IPv6 einfacher als bei IPv4, weil IPv6 viel mehr Adressen zur Verfügung stellt. Prinzipiell kann sowohl bei IPv4 als auch bei IPv6 eine private wie eine öffentliche Adresse dem gemeinsam genutzten System zugeordnet werden. Im ersten Fall muss die private Adresse so gewählt werden, dass sie in keinem der beiden internen Netze genutzt wird.

Sollen Systeme in den beiden internen Netzen direkt miteinander kommunizieren, stellt sich die Frage, wie tief in das eigene interne Netz die Route zum fremden Netz bekannt gegeben wird. Die einfachste Lösung ist die Nutzung der Default-Route, die es sowohl bei IPv4 als auch bei IPv6 geben kann. Da aber die Default-Route eventuell auch für Ziele im Internet verwendet wird, muss es mindestens ein System geben, das die IP-Adressen des Partnerunternehmens kennt und Pakete an diese Adressen nicht zum Internet, sondern zum Extranet weiter leitet. Wichtig ist auf jeden Fall, dass dies koordiniert passiert. Sendet Organisation A die an Organisation B gerichteten Pakete über das Extranet, darf B die An A gerichteten Pakete nicht über das Internet routen. Denn sonst können Firewalls, die es im Übertragungspfad zwischen zwei Organisationen höchstwahrscheinlich geben wird, mit den Paketen nichts anfan-

gen. Firewalls, die stateful arbeiten, führen Informationen über den Status einer Verbindung. Eine solche Firewall blockiert alle Pakete von Verbindungen, deren Aufbau sie nicht vollständig kennt. (siehe Abbildung 13)

Komplexer wird es, wenn das Extranet nicht zwei, sondern mehrere Unternehmen miteinander verbindet. Die Koordination mit dem Ziel, das bei jeder Kommunikationsbeziehung die Pakete in beiden Richtungen über dasselbe Extranet gesendet werden, muss dann immer zwischen zwei Unternehmen erfolgen, die das Extranet für die Kommunikation nutzen wollen. Eine andere Möglichkeit besteht darin, dass ein zentraler Koordinator die Liste der über das Extranet erreichbaren Routen pflegt. Jedes Unternehmen, das eines der eigenen Systeme über das Extranet erreichbar machen will, teilt die IP-Adresse des Systems dem zentralen Koordinator mit, der die Adresse im Extranet routet.

IPv6 bedeutet eine große Erleichterung der Kooperation zwischen verschiedenen Unternehmen. Unter IPv4 wird es bei steigender Anzahl der Extranet-Teilnehmer schwieriger, ohne NAT auszukommen, denn die meisten Unternehmen belegen intern denselben privaten Adressraum (in der Regel 10.0.0.0/8) vollständig. Unter IPv6 braucht man nur die Festlegung, dass die unternehmensübergreifende Kommunikation unter Nutzung von GAs erfolgt. Selbst wenn es im Verbund Unternehmen gibt, die ULAs verwenden, kann der zentrale Koordinator dafür sorgen, dass es zu keiner Adresskollision kommt. Es ist ohnehin ratsam, dass jedes Unternehmen, das ULAs nutzen möchte, unter Nutzung von **https://www.sixxs.net/tools/grh/ula/** den eigenen ULA-Bereich registriert. Wenn alle Kooperationspartner diesen Schritt durchgeführt haben, kommt es zu keiner Kollision.

Was sich in Sachen Security ändert

Auch wenn viele Mechanismen unter IPv4 und IPv6 ähnlich sind, weisen die beiden Protokolle Unterschiede auf, die zum Teil sicherheitsrelevant sind.

Ein Sicherheitsaspekt betrifft die Konfiguration von Endgeräten. Hier gibt es eine gemeinsame Schwachstelle von IPv4 und IPv6. In der Regel wird DHCP nicht kryptografisch abgesichert. So ist es möglich, dass ein Angreifer mit direktem oder indirektem Zugriff auf ein IP-Subnetz DHCP missbraucht, um die Konfiguration von Endgeräten zu manipulieren. Eine solche Manipulation kann dem Ziel dienen, einen Man-in-the-Middle(MitM)-Angriff durchzuführen. Der MitM kann zum Beispiel sämtliche Kommunikation eines Endgeräts aufzeichnen.

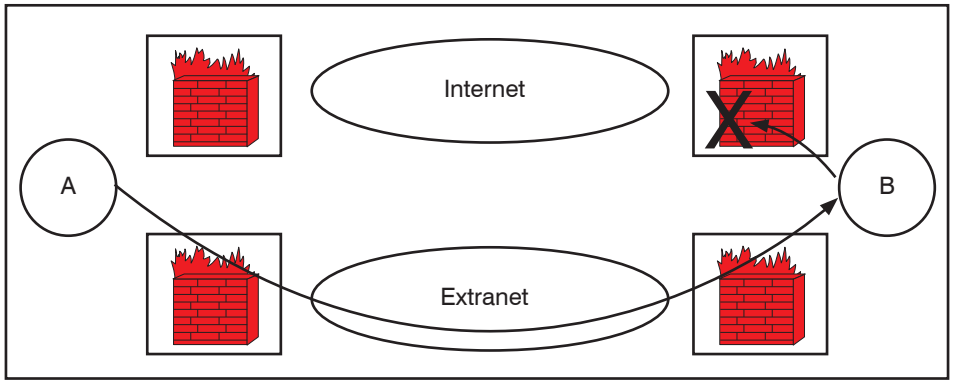

Abbildung 13: Problematik beim asymmetrischen Routing

Einige Layer-2 Switches bieten sowohl unter IPv4 als auch IPv6 Sicherheitsmechanismen gegen solche Spoofing-Attacken. Ein Switch kann so eingestellt werden, dass DHCP Responses nur dann weiter geleitet werden, wenn sie über bestimmte Schnittstellen empfangen werden. Typischerweise sind das die Uplinks des Switches.

Bei IPv6 kommt die Möglichkeit hinzu, Endgeräte über RAs und SLAAC zu konfigurieren. Hier können ähnliche Mechanismen greifen. Ein Layer-2 Switch kann so eingestellt werden, dass nur RAs weiter geleitet werden, die über bestimmte Ports empfangen worden sind. (siehe Abbildung 14)

Im Zusammenhang mit SLAAC wurden in diesem Beitrag die Security Extensions bereits erwähnt. Ihre Einschaltung nimmt nicht nur Angreifern die Möglichkeit, Geräte an deren IP-Adressen leicht zu erkennen. Insbesondere in drahtlosen Netzen, wo Endgeräte nicht mit Switch-Ports verbunden und daran zu erkennen sind, schwirren dann Pakete herum, deren IP-Adressen keinen Aufschluss über die Identität des Gerätes zulassen.

Wenn ein Gerät, das mangels DHCP-Aktivierung in einem Subnetz SLAAC nutzen muss, zwischen dem internen und öffentlichen Netzen wechselt, empfiehlt sich, SLAAC Security Extensions zu nutzen. Dann muss man den Verzicht auf einen Teil der Tracking- und Trace-Möglichkeit im internen Netz in Kauf nehmen.

Erfahrungen austauschen

Die Fortsetzung der Erläuterung der richtigen IPv6-Fundamente würde den Rahmen dieses Beitrages sprengen. Es ist wichtig, dass es bei der Einführung von IPv6 zum Erfahrungsaustausch zwischen Unternehmen kommt. ComConsult leistet dazu ihren Beitrag auf dem diesjährigen Netzwerk- und IT-Infrastruktur Forum. Wir freuen uns auf die Diskussion mit Ihnen!

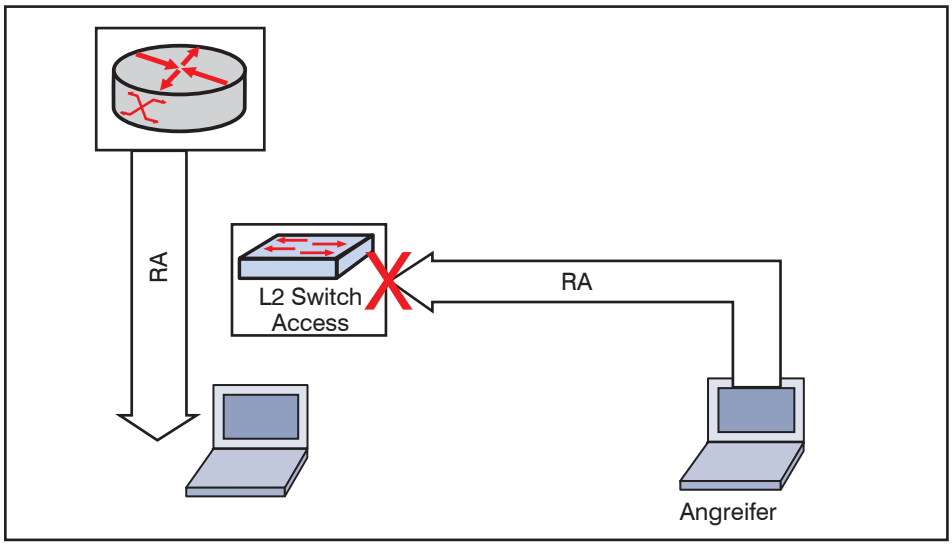

Abbildung 14: Schutz vor böswilligem Router Advertisement

Standpunkt

WLAN: Wird 5 GHz zum neuen 2,4-GHz-Band?

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

WLAN gibt es bekanntlich für zwei unterschiedliche Frequenzbereiche. Da ist zum einen das ISM-Band (ISM = Industrial, Scientific, Medical) von 2,4 bis 2,5 GHz. Es ist quasi das traditionelle WLAN. Wohl alle heute verfügbaren Endgeräte unterstützen es und bei der Planung gilt es außer einer geschickten Kanalplanung kaum Hürden zu nehmen.

Allerdings steht dieses Band auch für allerlei Nachteile. Bekanntlich dürfen ISM-Bereiche von den verschiedensten Funkdiensten verwendet werden, solange diese die Vorgaben der Regulierungsbehörden einhalten. Die aktuell gültige „Allgemeinzuteilung von Frequenzen für die Nutzung in lokalen Netzwerken“ der Bundesnetzagentur (Verfügung 10/2013) umfasst nach wie vor den Hinweis „Es besteht kein Schutz vor Beeinträchtigungen durch andere bestimmungsgemäße Frequenznutzungen“. Solche bestimmungsgemäße Frequenznutzungen können Bluetooth-Anwendungen, Mikrowellenherde, drahtlose Videokameras und vieles mehr sein.

Das Schreckgespenst des durch Funkstörungen lahmgelegten WLAN hat viele Unternehmen dazu ermutigt, Anwendungen in das 5-GHz-Band zu verlagern. Ursprünglich in Europa gar nicht zugelassen, haftete diesem Frequenzbereich lange der Makel des technisch Komplizierten an. Die Regulierungsbehörden verlangen nämlich technische Maßnahmen, die eine Störung des Primärnutzers im 5-HGz-Band verhindern. Und das sind Radarsysteme, die insbesondere an Flugplätzen und auf Flugzeugen zum Einsatz kommen. Der zugehörige Standard EN 301893 hat in der Vergangenheit zahlreiche Überarbeitungen erfahren, und die Hersteller mussten ihre WLAN Access Points immer wieder entsprechend anpassen.

Auf der anderen Seite erstrahlt das 5-GHz-Band inzwischen als das moderne und zukunftsweisende. Das neue Gigabit-WLAN gemäß IEEE 802.11ac ist sogar ausschließlich für 5 GHz spezifiziert. Nur hier gibt es eine ausreichende Anzahl von Kanälen, um kraft Bündelung hohe Bitraten zu erzielen. Radar ist für die meisten Standorte erfahrungsgemäß kein Thema, andere Störquellen gibt es kaum.

Das ist inzwischen bei den Anwendern angekommen. Ein jeder möchte „seinen“ Endgeräten die beste Performance spendieren – „latest and greatest“. Ich erlebe bei meinen Kunden einen wahren „Run“ auf das 5-GHz-Band. Es werden alle Endgeräte auf 5 GHz umgestellt, die das irgendwie zulassen. Die WLAN-Hersteller bieten sogar Features an, mit deren Hilfe Dual-Band-Endgeräte auf 5 GHz gezwungen werden sollen.

Mal abgesehen davon, dass solche Features bisweilen unangenehme Seiteneffekte haben, erscheint mir das Vorgehen an sich nicht zielführend zu sein. Denn – man kann es nicht oft genug wiederholen – WLAN ist und bleibt ein Shared Medium, allen „Performance Boosts“ zum Trotz. Schon beim Ethernet Yellow Cable (erinnern Sie sich noch an dieses frühe Shared Medium?) führte beispielsweise das Nebeneinander von Terminals und Datei-Transfers zu erhöhten Kollisionsraten. Nicht anders ist es im WLAN: Hand-Scanner, Diagnosegeräte, Akkuschrauber und Office Notebooks konkurrieren miteinander, leider meist ohne einen Gewinner.

Nutzen Sie doch alle Möglichkeiten des WLAN aus! Die beiden Frequenzbänder, die man uns zugesteht, bieten die Chance für eine Homogenisierung des Datenverkehrs. Packen Sie gleiches zu gleichem! Den Akkuschrauber neben die Handscanner; beide übertragen häufig kurze Datenblöcke. Das Office Notebook neben das Diagnosegerät; letzteres wird vielleicht regelmäßig mit einem Megabyte-großen Programm betankt und passt daher gut zur Dateiverarbeitung des Notebooks.

Wenn Sie so vorgehen, werden wahrscheinlich die neueren Geräte im 5-GHz-Band landen. Das ist gut so, denn „Legacy Devices“ sind besser im 2,4-GHz-Band aufgehoben. Nicht aus Performance-Erwägungen (s.o.) sondern auch weil die Gesetzeslage bei 2,4 GHz seit den Anfängen unverändert geblieben ist. Vergleichen Sie dagegen einmal die Länder-spezifischen Kanalschemata im 5-GHz-Band! Zu allem Überfluss sind erst in 2007 in den USA große Bereiche hinzugekommen. Gerade international tätige Unternehmen werden also Schwierigkeiten haben, eine Kanalplanung für das 5-GHz-Band vorzulegen, die auf der einen Seite „Legacy Devices“ unterstützt und auf der anderen Seite Raum für hohe Performance bietet. Entscheiden Sie sich für die Performance!

Neues Seminar

Strategien für Unternehmen zur richtigen Positionierung im Internet

18.05.15 in Köln

Die ComConsult Akademie veranstaltet am 18.05.15 ihr neues Seminar "Strategien für Unternehmen zur richtigen Positionierung im Internet" in Köln.

Kein Unternehmen kann es sich heute wirklich noch leisten, das Internet nicht optimal zu nutzen. Die rechtlichen Rahmenbedingungen werden jedoch zunehmend komplexer und deren Einhaltung immer wichtiger, um rechtlichen Nachteile für die Präsenz am Markt und gegenüber Mitbewerbern zu vermeiden.

Ziel des Seminars ist es, den Teilnehmern einen einführenden Überblick über die aktuelle rechtliche Situation für Unternehmen im Bereich der Nutzung des Internets insbesondere für Unternehmensinternetseiten, Social Media und E-Commerce zu verschaffen und für die Risiken für Unternehmen im Umgang mit Internet und Neuen Medien zu sensibilisieren.

Dieses Seminar zeigt die Vor- und Nachteile der Nutzung des Internets für Unternehmen auf und gibt den Teilnehmern einen Überblick über typische und kostenintensive Fehlerquellen im Bereich des Wettbewerbsrechts, Urheberrechts und Markenrechts.

Im Seminar werden unter anderem Offensiv- und Defensivstrategien aufgezeigt,

insbesondere im Umgang von Abmahnungen und strategische Möglichkeiten für Unternehmen in diesen Bereichen.

In diesem Seminar lernen Sie

- Strategien zur Erkennung von rechtlichen Risiken und Gefahrenpotentialen im Internet anhand der Darstellung typischer Problembereiche
- Strategien zur Problemvermeidung und Risikominimierung
- Strategien zur Erkennung von Handlungsnotwendigkeiten
- Strategien zur Schadensvermeidung bzw. Minimierung unter Berücksichtigung von Rückstellungen für potentielle Gefahren
- Strategien zum Umgang mit wettbewerbsrechtlichen, Urheberrechtlichen und markenrechtlichen Abmahnungen im Unternehmen
- Strategien zum Umgang mit Folgen von Rechtsverletzungen im Internet
- Intelligente Strategien zur Absicherung für Unternehmen im Internet

Das Seminar richtet sich an Nichtjuristen aus dem Bereich der Wirtschaft, vorrangig an die Verantwortlichen der Geschäftsleitung, insbesondere Geschäftsführer und Vorstand und Inhaber von Unternehmen und Betrieben, Verantwortliche von Marketingabteilungen, Verantwortliche des Vertriebs sowie Verantwortliche für Inhalte im Internet und Betreiber von Internetseiten.

Der Referent Dr. Tobias Beltle ist als Rechtsanwalt und Mediator in der Kanzlei Dury in Saarbrücken tätig. Er ist Fachanwalt für gewerblichen Rechtsschutz und in seiner anwaltlichen Tätigkeit schwerpunktmäßig auf dem Gebiet des gewerblichen Rechtsschutzes sowie des IT-Rechts und im Bereich der Vertragsgestaltung tätig. Er berät und vertritt überwiegend Unternehmen.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Ich buche das Seminar
Strategien für Unternehmen zur richtigen Positionierung im Internet

☐ am 18.05.15 in Köln
zum Preis von € 1.090,-- netto

☐ Bitte buchen Sie mir ein Hotelzimmer

vom_____ bis_____15

Buchen Sie über unsere Web-Seite

www.comconsult-akademie.de

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

Zweitthema

SDN, NFV, OpenFlow und Virtualisierungs-Protokolle – Zusammenhänge, Perspektiven, Marktrelevanz

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.

Fortsetzung von Seite 1

SDN soll somit herstellerübergreifend in Multivendor-Umgebungen einsetzbar sein. Um dies für alle Produkte zu erreichen, wird die Control Plane offengelegt, es werden offene, standardisierte Protokolle entwickelt, die Control Plane setzt auf einem Standard-Server und Standard-Betriebssystem auf.

SDN will die Netzwerk-Kontrolle (Lernen, Weiterleitungs-Entscheidungen und Policies) von der Netzwerk-Hardware, -Topologie und Paketweiterleitung (physikalische Verbindungen, Interfaces und deren Beziehung zueinander) entkoppeln.

Da die Control Plane ausgelagert ist, kann sie verschiedenste Arten von Netzkomponenten steuern: vSwitches, Hardware-Switches, Router, WLAN Access Points, Load Balancer, Traffic Shaper, Firewalls etc. Somit kann eine Gesamtsteuerung der kompletten verkabelten und kabellosen Netzwerk-Infrastruktur aus einer gemeinsamen Topologie-Sicht heraus implementiert werden. In diesem Sinn zielt SDN auf eine übergeordnete Orchestrierung des Netzwerks und der Netzwerk-Dienste hin, bei der die Netzwerk-Dienste von den physikalischen Netzwerk-Interfaces und physikalischen Netzwerk-Infrastrukturen losgelöst sind.

Globale Service-Definitionen müssen nicht mehr auf die physikalischen Interfaces gemappt werden, Service-Einheiten (zum Beispiel eine Applikation, eine VM) können über verschiedene Interfaces hinweg migrieren, ohne ihre Identität zu ändern oder getroffene Spezifikationen zu verletzen. In dem Maß, wie globale Service-Definitionen nicht mehr auf alle Interfaces und alle Interface-Lokationen gemappt werden müssen, soll eine Vereinfachung des Netzwerk-Betriebs erreicht werden.

Die SDN Control Plane nutzt zur Kommunikation zwischen Controller und Netzkomponente typischerweise ein spezielles Kontroll-Protokoll, vergleichbar der Signalisierung in Kommunikations-Lösungen.

Die Vision ist nun: Netzwerk-Administratoren können anhand der logischen Netzwerk-Abstraktion das Verhalten des Gesamt-Netzwerks programmieren, anstatt die Konfiguration vieler einzelner Netzwerk-Komponenten anfassen zu müssen. Über den SDN Controller mit seiner zentralen Intelligenz könnte das Netzwerk-Verhalten in Echtzeit geändert werden und könnten neue Netzwerk-Dienste / -Applikationen innerhalb von Stunden oder Tagen anstelle von Wochen oder Monaten ausgerollt werden. Die logische Gesamtsicht soll zudem die effiziente Ausnutzung aller möglichen denkbaren Netzwerk-Ressourcen ermöglichen. (siehe Abbildung 1)

Eine weitergehende Sichtweise setzt auf die Applikationsschicht der ONF-Archi-

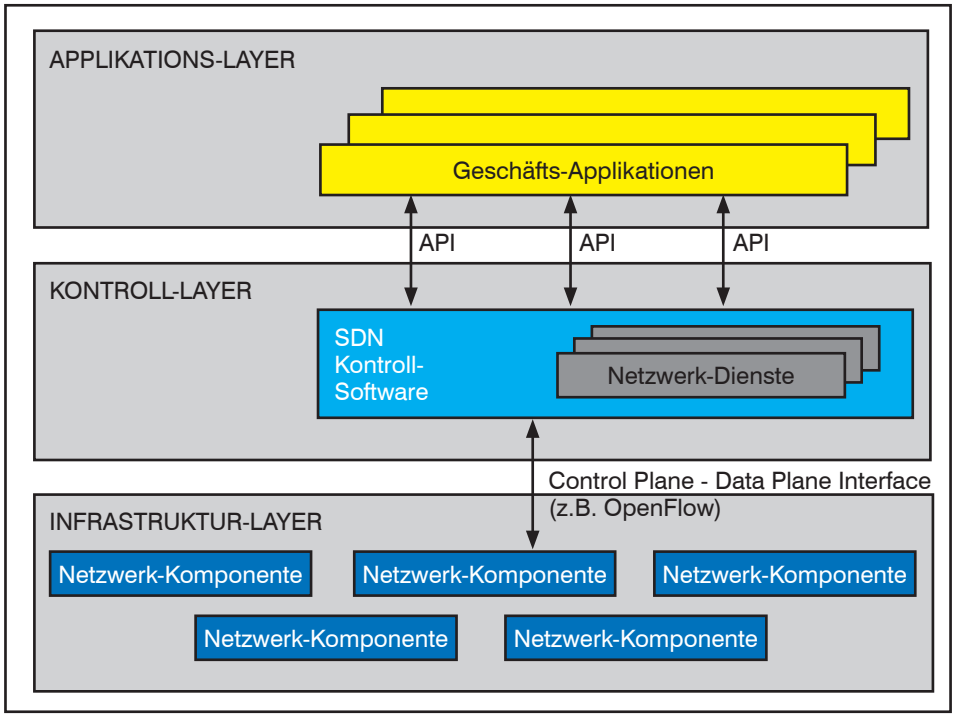

Abbildung 1: Logische Übersicht der SDN-Architektur gemäß ONF

tektur noch eine Orchestrierungs-Ebene auf, die der übergeordneten Administration und Automatisierung der verschiedenen SDN-Applikationen gilt. (siehe Abbildung 2)

SDN und ONF

Anfang 2011 gründeten die Deutsche Telekom, Facebook, Google, Microsoft, Verizon und Yahoo die Open Networking Foundation als non-Profit Konsortium mit dem Ziel, Software Defined Networking (SDN) nach vorne zu treiben. Später erfolgte der Beitritt von Broadcom, Brocade, Ciena, Cisco, Citrix, Dell, Ericsson, Force10, HP, IBM, Juniper, Marvell, Microsoft, NEC, Netgear, NTT, Oracle, Riverbed Technology und VMware. Aktuell hat die ONF viele Mitglieder aus verschiedenen marktrelevanten Technologiebereichen: Provider, Netzwerk-Komponenten-Hersteller, Chip-Hersteller, Software- und System-Hersteller. Die ONF führt auch Studien zur Entwicklung offener APIs für entsprechende übergreifende Management Tools durch.

Einsatzbereiche von SDN

SDN Openflow kann ein Standard zur Handhabung aller virtualisierten Netzwerk-Lösungen werden, insbesondere auch für OpenVirtual Switch (OVS) und OpenStack. Der gesamte Komplex "komponentenübergreifendes Management" ist ein potenzieller SDN-Kandidat, da weder OSI-Management noch SNMP noch http hier umfassende Lösungen gebracht haben (ketzerische Frage: Trauen wir SDN dies nunmehr zu?). Insbesondere Automation von Management und Provisionierung stehen ganz oben auf der Liste von Providern, Data Center und Netzwerkbetreibern.

Der Service-Bereich AaaS, IaaS, Konsolidierung von Überkapazität sowie Cloudlösungen würde von übergreifenden SDN-Lösungen profitieren. Bei Einsatz von Overlay-Verfahren könnte SDN/OpenFlow Ende-zu-Ende konsistent die erforderlichen Frame- und Paket-Änderungen steuern (NAT, Tunnel-Header, Tag Rewriting etc.).

Die Entwicklung neuer Routing Protokolle als "Open Source Routing" wird zwar von den SDN-Vätern immer wieder gerne herangezogen, steht aber aktuell wohl nicht wirklich im Fokus der Problemlösung. OSPF und MPLS gut funktionierende Verfahren.

Aber selbst wenn die etablierten Layer-2 und Layer-3 Standards nicht ersetzt werden sollen, gibt es auch im Enterprise

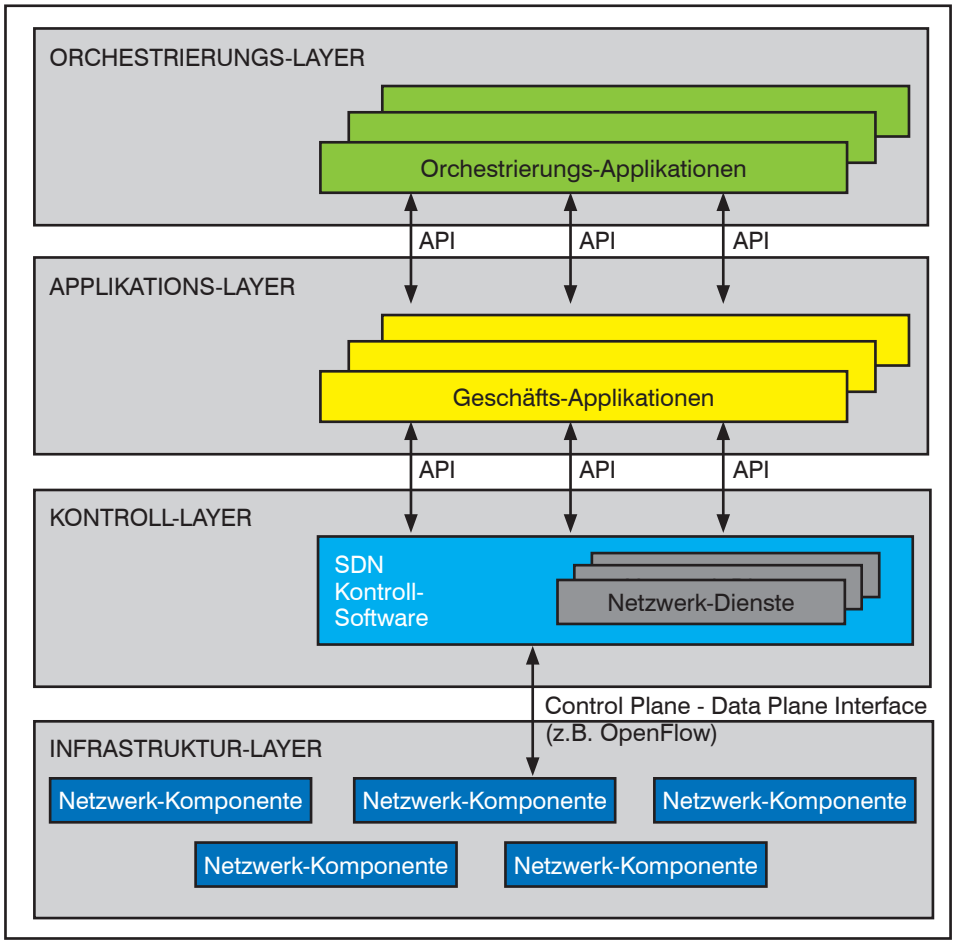

Abbildung 2: Erweiterte SDN-Architektur

Netzwerkbereich Mehrwert-Möglichkeiten mit SDN/OpenFlow: Übergreifende Lastverteilung / Traffic Engineering / netzweite QoS-Regeln als Erweiterung der L2/L3-Standardnetzwerksteuerung.

Ebenso sind Mandantentrennung und Zugangssteuerung mit netzweiten Sicherheits-Regeln und NAC, dynamische Umleitung von Flows für jede Art von IPS / IDS-Überprüfung und Erkennung von Sicherheits-Incidents sehr spannende SDN-Anwendungsbereiche. Gleiches gilt auch für netzweites Monitoring und Statistiken als Funktionserweiterungen der Netzwerksteuerung, die mit SDN/OpenFlow unterstütz werden könnten.

Abschließend ist eine Zusammenfassung von Einsatzszenarios aufgeführt, teilweise sind dies auch schon Applikationsmodule auf verfügbaren Controllern:

- Management
  - Management von OpenVirtual Switch (OVS), OpenStack
  - zentrales komponentenübergreifendes Management
  - Gemeinsame Management-Domäne für physische und virtuelle Switch-Infrastruktur
  - Programmierbarkeit von Netzkomponenten
  - Automation von Management und Provisionierung
  - Monitoring, Reporting, insbesondere
    - dynamische und selektive Flows bei Last-Peaks und außergewöhnlichen Lasten
    - dynamische und selektive Flows zur Fehlerdiagnose
- Mandanten
- IaaS (Infrastruktur)
- AaaS (Applikationen)
- Konsolidierung von Überkapazität (Cloud)
- Zugangs-Dienste (Carrier, dynamisch)
- Sicherheit
  - Enterprise NAC
  - Enterprise Security-Regeln
  - Triggern von Security-Incidents
  - dynamische und selektive Flow-Umleitungen zur Überprüfung, an ein IDS / IPS
- Traffic Engineering
  - Kontrolle des Überbuchungsverhältnisses
  - Bandwidth on Demand
  - Flow Klassifizierung
  - Forward zentraler Netzwerksteue-

rungsregeln
  - Flowbasierendes aktives LB
  - Ende-zu-Ende QoS
  - Load Balancing über alle Verbindungen hinweg
  - LB entsprechend einer SD Heuristik
- Frame Änderung (NAT, Tunnel, Tag Rewrite)
- OpenSource Routing
- Schnelles Failover bei Port-/Switchausfall
- WAN Optimierung
- SLA im WAN Ende-Ende per OpenFlow am Provider Edge und Client Ingress
- verschiedene Service Level

1.1 SDN Schnittstellen (APIs)

Da das Wohl und Wehe des Netzwerks vom Controller abhängt, haben der Controller und seine Schnittstellen im SDN-Konzept natürlich eine ganz zentrale Bedeutung. Es gibt vier fundamentale Punkte, die bei jedem Controller benötigt werden und zum SDN-Stack gehören. (siehe auch Abbildung 3):

1. Einrichtung des Datenpfades für die Netzwerk-Infrastruktur (z.B. OpenFlow Switches), zum Beispiel mit dem OpenFlow Protokoll

2. Ein Southbound-API, um Netzwerkkomponenten standardisiert in das ICT Ecosystem zu integrieren

3. Ein Northbound-API, um Applikationen standardisiert in das ICT Ecosystem zu integrieren

4. East-Westbound-APIs für Controller-Verbunde, zur Kommunikation mit anderen Controllern

Northbound API (NBI)

Das Northbound-API des Controllers erlaubt – im Prinzip beliebigen – Applikationen, mit dem SDN-Controller zu interagieren. Dies können Basis-Applikationen zum Ersatz der gängigen Standards für Layer-2 Wegberechnung, Redundanz und Lastverteilung oder Layer-3 Wegberechnung, Redundanz und Lastverteilung sein, es können aber auch weiterführende Applikationen für Traffic Engineering, Monitoring, Reporting, Sicherheit oder Mandantentrennung sein.

Leider gibt es in der ONF keine stringenten Bemühungen, ein Northbound API zu standardisieren und zu forcieren. Zwar gibt es unter der Rubrik "Services" eine Arbeitsgruppe "NBI", diese ist aber über ein einleitendes 8-Seiten WG-Charter Papier mit einem sehr vagen Umriss des North-Bound Interfaces im Oktober 2013 bis dato nicht hinausgekommen. Auch in der WG "Architektur und Framework", die alibimäßig mit der Betrachtung des NBI beauftragt wurde, ist nicht wirklich Brauchbares zu finden.

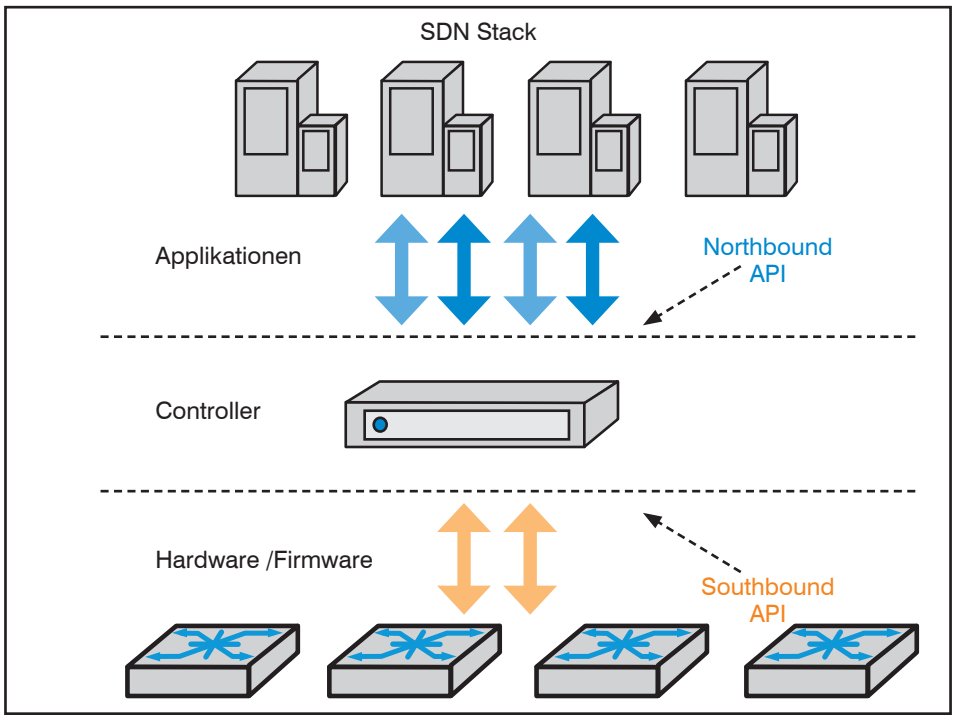

Abbildung 3: SDN-Schnittstellen – Southbound und Northbound API

Ketzerische Geister könnten hieraus den Schluss ziehen, dass die ONF kein wirkliches Interesse am Northbound API hat, sondern sich mit der Ausarbeitung des Southbound API zufrieden gibt.

Southbound API, OpenFlow

Der SDN-Controller interagiert mit den Netzwerk-Ressourcen respektive der Netzwerk-Infrastruktur über das Southbound-API: Über diese Schnittstelle manipuliert der Controller die Flow-Tabellen und Weiterleitungs-Instruktionen der unterliegenden Netzwerk-Infrastruktur, des so genannten Netzwerk Substrats. Zum Netzwerk-Substrat gehören in letzter Konsequenz nicht nur Hardware-Komponenten (falls es die dann noch gibt) wie Layer-2 und Layer-3 Switches, sondern auch Router, Load Balancer, Firewalls, VPN-Gateways, WLAN Access Points, WLAN-Controller, PSTN-Gateways, Media Gateways, SBCs, sondern auch alle virtuellen Instanzen der genannten Netzwerkkomponenten (virtuelle Switches, Router, Firewalls, Load Balancer etc.) kurz alle Hardware- und virtualisierten Software-Komponenten der Netzwerk-Infrastruktur.

Das Southbound API wird von der ONF mit dem OpenFlow Protokoll standardisiert, denkbar sind jedoch auch andere Protokolle. Die ONF-Aktivitäten hier sind virulent, etwa jedes halbe Jahr wird ein neues OpenFlow Switch Protokoll Release verabschiedet. Das aktuelle Release hat die Version OpenFlow 1.5.0 und datiert vom Dezember 2014. Hierauf ist bei der Produkt-Betrachtung ein Augenmerk zu richten, denn die unterstützte OpenFlow Version bestimmt die erreichbare Funktionalität. Version 1.1 bis 1.3 ist aktuell als veraltet einzustufen, zwischen Version 1.1 und 1.5.0 gibt es deutliche Funktions-Erweiterungen. Aktuelle Switch ASICs können erfahrungsgemäß nie die neueste OpenFlow Release unterstützen, sondern liegen immer etwa zwei bis drei Releases zurück. OpenFlow und seine Arbeitsweise wurde in früheren Insidern ausführlich beschrieben, daher erfolgt in diesem Beitrag keine weitere Detaillierung mehr.

Alternativen zu OpenFlow werden beispielsweise im OpenDaylight Projekt aufgezeigt, auf das später noch eingegangen wird.

East-Westbound API

Eine vollständige SDN-Architektur kann sich nicht mit einem einzelnen Controller oder Controller-Cluster zufrieden geben. Partitionierungen werden in jedem Fall erforderlich sein, sei es zur logischen Aufteilung in verschiedene Providerbereiche oder zur Verbindung von physischen Netzwerkbereichen, die jeweils durch einen eigenen Controller gehandhabt werden. Gründe hierfür sind sowohl weltweite Skalierbarkeit und schrittweises Wachstum

als auch Managebarkeit, Schutzzonen und Mandantenkonzepte.

Um solche Partitionierungen zu ermöglichen, muss über das Southbound und Northbound Interface hinausgehend auch die Ost-West-Kommunikation verschiedener Controller als so genannter SDNi (SDN Interconnect) definiert werden (wie in Abbildung 4 dargestellt). Soll diese standardkonform oder zumindest kompatibel stattfinden, muss ein herstellerübergreifendes East-Westbound Controller Interface spezifiziert werden (je nach Literaturquelle auch Eastbound-Westbound oder East-Westbound Interface genannt)

Das East-Westbound Interface regelt die Verteilung der Control Plane auf mehrere voneinander prinzipiell unabhängige Controller, die sich dann über ihre jeweiligen SDN-Domänen und hierfür erforderlichen Routing Informationen miteinander austauschen (siehe auch Abbildung 4). Einsatz-Szenarien sind zum Beispiel:

- Cloud Federations
- Optimierung provider-übergreifender Netze
- Übergabe-Punkt zwischen Provider-Netzen für Kontroll-Informationen
- Austausch von Kontroll-Informationen zwischen Enterprise-SDN und Provider-SDN

Auch für dieses Interface gibt es bisher keinen verabschiedeten Standard, aber mehrere Gremien und Hersteller, die daran arbeiten. Interessanterweise ist auf der ONF-Webseite hierzu gar nichts zu finden. Einzelne Hinweise sind bei folgenden Institutionen zu finden:

- ITU-T SG 13: "Future Networks including Cloud Computing, mobile and NGN"
- ETSI ISG AF (ETSI Industry Specification Group on Autonomic network engineering for self-managing Future Internet): "Relationships between SDN and Autonomic Management & Control"
- IETF ALTO WG: ALTO zur Orchestrierung von SDN (Telefonica Präsentation: "The (Multiple) Connection between ALTO and SDN"; Oktober 2012)

1.2 SDN und Management

Netzwerk-Management im Rahmen einer SDN-Lösung bietet einerseits Verbesserungspotenzial im Vergleich zum heutigen Betrieb, andererseits bringt es eine Reihe neuer Herausforderungen, die für eine erfolgreiche Implementierung von SDN zu lösen sind. Eine Umfrage von Webtorials (Dr. Jim Metzler e.a., 2014) zeigt auf, dass zwar 53% der Unternehmen glauben, dass SDN Konfiguration und Provisionierung erleichtern wird; gleichzeitig geben

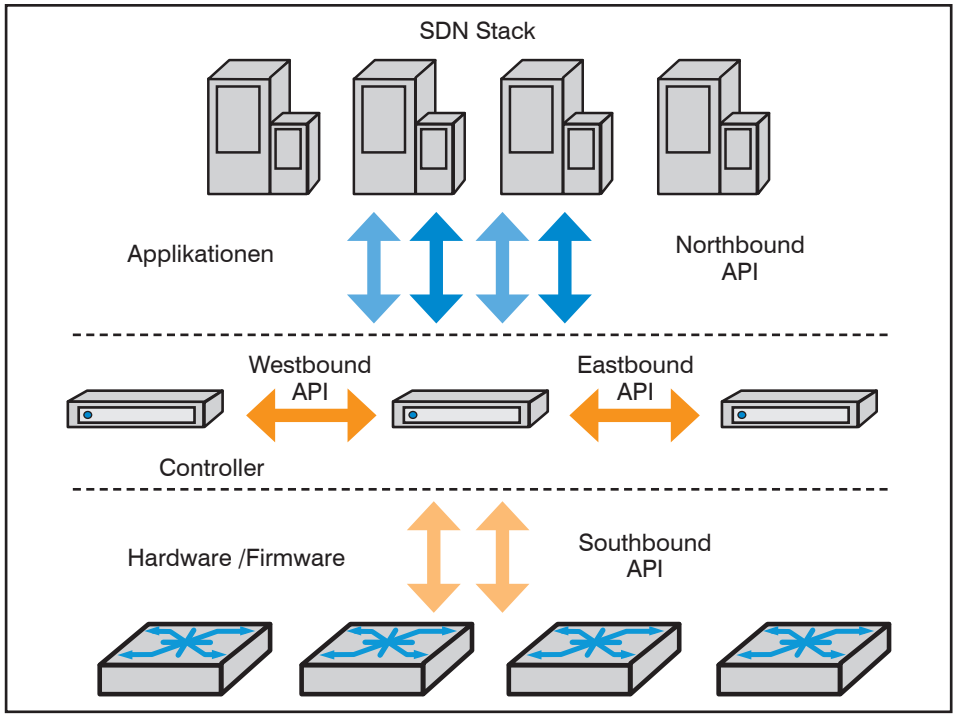

Abbildung 4: SDN-Schnittstellen – East-Westbound API

aber 13% der Befragten an, dass Bedenken hinsichtlich der Management-Möglichkeiten einer SDN-Lösung ein signifikantes Hindernis für den Einsatz von SDN darstellen – Janus lässt grüßen…

Eine Übersicht der ONF (SDN Architecture Overview 1.0, 12/2013) gibt einen Eindruck über die Komplexität, die beim Thema SDN Netzwerk-Management zu lösen ist (siehe Abbildung 5): Die Anforderungen an ein Ende-zu-Ende Service Level und Performance Management sind deutlich höher als in einem traditionellen Netzwerk: SDN muss zusätzliche Komponenten überwachen, nämlich den Controller sowie eine Ende-zu-Ende Kombination aus virtuellen und physischen Netzkomponenten und Ressourcen, die noch dazu nicht statisch sind, sondern sich dynamisch än-

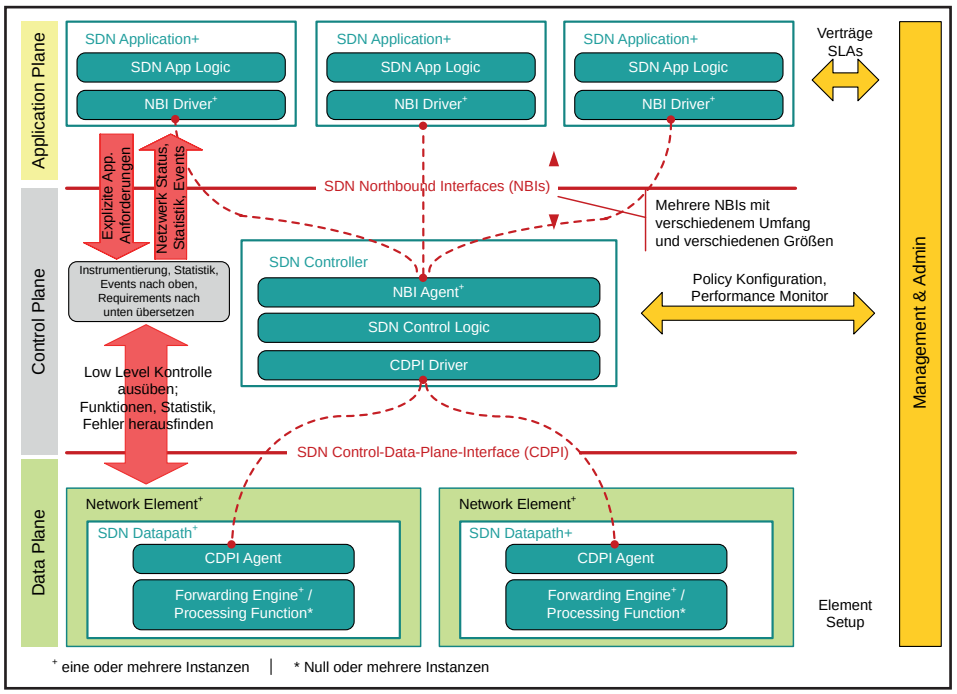

Abbildung 5: SDN Management Herausforderung

dern. Zudem muss auch das Control Plane Protokoll (z.B. OpenFlow) überwacht werden.

Abbildung 5 zeigt, dass in der untersten SDN-Ebene die Data Plane aus verschiedensten Netzwerk Elementen zusammengesetzt ist, deren SDN Datenwege ihre Funktionalität durch den Agenten des Control-Data-Plane Interface (CDPI-Agent) zugreifbar machen und (dem SDN Controller) offenlegen. In der obersten SDN-Ebene teilen SDN Applikationen über die Northbound-Schnittstelle, respektive ihre NBI-Treiber, ihre Anforderungen (dem SDN-Controller) mit. Der Controller seinerseits übersetzt die Applikations-Anforderungen in Anforderungen an die SDN-Datenwege.

Diese 3-Tier Architektur stellt schon alleine an die Handhabung von Anforderungs- und Kontrollnachrichten hohe Anforderungen. Darüber hinaus ist es einigermaßen anspruchsvoll, über Applikations-, Controller- und Data Path-Ebene hinweg konsistentes Leistungs-, SLA-, und Konfigurationsmanagement zu implementieren. In der ONF-Übersicht wird dies recht lapidar auf der rechten Seite als eine schichtenübergreifende Vertikalfunktion "Management & Admin" dargestellt.

Eine weitere Herausforderung liegt darin, dass der SDN Controller bei neuen Flows im Datenpfad liegt. Das bedeutet: wenn viele neue Flows generiert werden, wird der Controller selbst ein möglicher Bottleneck und trägt signifikant zur Erhöhung der Latenzzeit bei.

In der aktuellen Version der Architektur-Übersicht (SDN Architecture Overview 1.1, 11/2014) ist bezeichnenderweise der Management-Bereich in verschiedene OSS für Applikation und Controller/Netzwerk unterteilt und die Schnittstellen sind wesentlich grober dargestellt. (siehe Abbildung 6)

SDN hat das Potenzial, Verbesserungen für Netzwerkmanagement und –betrieb zu bewirken, bringt jedoch auch neue Anforderungen und Herausforderungen für eine funktionierende Management-Umgebung mit sich.

1.3 SDN und Overlay / Underlay Modell

SDN hat in den letzten Jahren einige Veränderungen durchlaufen – was für eine junge Technologie typisch ist. Wurde im letzten Jahr noch diskutiert, ob Virtualisierung mittels Overlay Netzen tatsächlich eine SDN-Lösung ist, so sind Virtualisierungs-Overlays in diesem Jahr von den meisten Fachleuten als eine Form von SDN anerkannt. Somit haben wir es bei

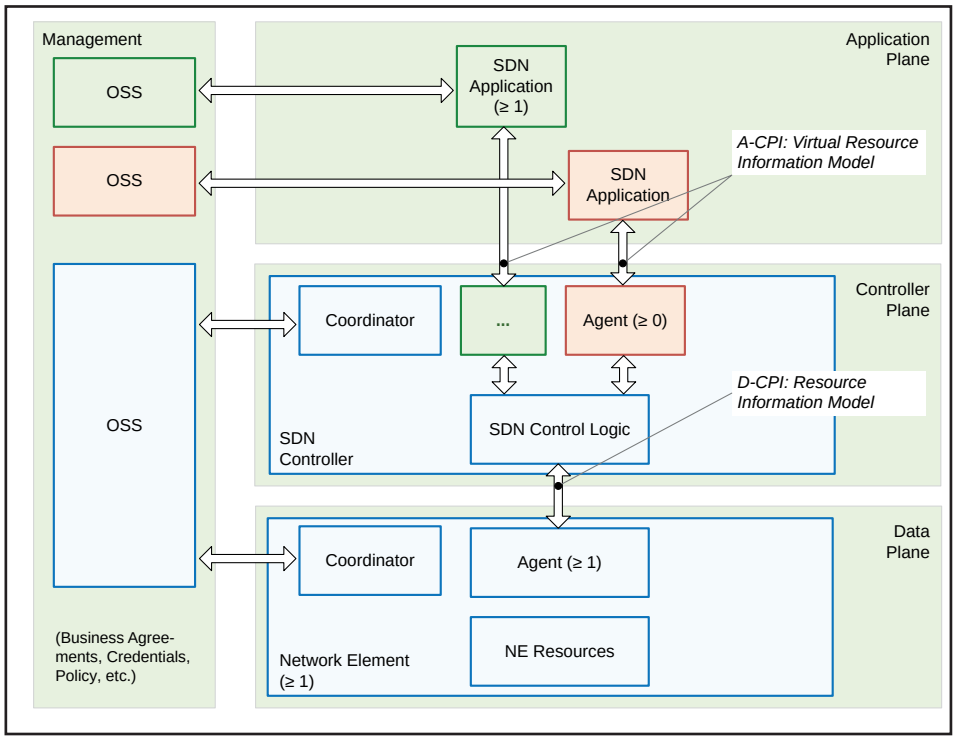

Abbildung 6: SDN Architektur Überblick v1.1

SDN teilweise mit einem Overlay Modell, teilweise mit Underlay Modell zu tun.

Das Overlay Modell fokussiert sich hinsichtlich Virtualisierung auf die Hypervisor-Ebene und nutzt Enkapsulierungs-Tunnel. Somit bewegen sich die entsprechenden Einsatz-Szenarien, Mehrwerte und Herausforderungen im Umfeld virtualisierter Server. Zu den Virtualisierungs-Overlay Verfahren zählen z.B. VXLAN, NVGRE, STT, GENEVE, NSH und SPBM. Das virtuelle Netz kann Layer-2 (SPBM, MAC in MAC) oder Layer-3 (VXLAN und ähnliche, UDP/IP/Ethernet Tunnel) sein und ist unabhängig von der unterliegenden physischen Netzwerk-Infrastruktur. Der Tunnel Header enthält dann ein ID-Feld, das in der Regel 24 Bit oder größer ist und das virtuelle Ziel-Netzwerk eindeutig identifiziert.

Das Netzwerk-Virtualisierungs-Overlay Modell beinhaltet nicht zwingend einen Controller.

Netzwerk-Virtualisierungs-Overlays (NV-Overlays) bieten einige Vorteile:

- Netzwerk-Virtualisierung (NV) findet am Netzwerk Edge statt, das unterliegende physische Netzwerk bleibt davon unberührt
- Die Anzahl erreichbarer IDs ist mit 16 Millionen erheblich höher als bei 4000 VLANs, auch wenn praktische Limitierungen vielfach im Bereich von 16.000 bis 32.000 virtuellen Netzen liegen.
- Die Entkopplung der virtuellen von der physischen Infrastruktur, respektive MAC und IP Adressen beseitigt netzwerkseitige Limitierungen wie Adress-Tabellengrößen in Switches.
- VM Mobilität wird unabhängig vom unterliegenden Netzwerk, die entsprechenden Netze für VMs können rein am Edge provisioniert werden.
- Überlappende Adressräume verschiedener Mandanten sind möglich.
- Multipath Lastverteilung wird auch "innerhalb" eines virtuellen Netzes möglich (über die darunterliegende physische Netzwerk-Infrastruktur)
- Virtuelle Appliances, für die mehrere Netzwerk-Dienste nacheinander erforderlich sind (z.B. Authentisierung, DPI, NAC-Policy-Zuweisung, QoS-Profil), die auf verschiedenen VMs residieren, können mittels Service Chaining durch "Point-and-Click" über das NV-Management bereitgestellt werden.
- Sofern eine NV-Lösung (zusätzlich) controller-basiert ist, liegt der Controller nicht im Datenpfad und stellt somit keinen Bottleneck dar.

NV-Overlays haben jedoch auch einige Nachteile:

- Virtuelle und physische Netze sind separate Einheiten, die separate Service Level Agreements, Policy Management, Provisionierung und Kontrollpunkte haben. Alle diese Parameter müssen korreliert, aufeinander abgestimmt und überwacht werden.

- Wachstum der virtuellen Netze geht nicht zwingend mit einem Wachstum der physischen Netze einher, was zu einer Überbuchung der unterliegenden Netzwerk-Infrastruktur führen kann. Auch hier ist konsistente Abstimmung erforderlich.

- Für die Kommunikation zwischen virtueller und physischer Netzwerk-Infrastruktur oder zwischen verschiedenen virtuellen Netzen (z.B. VXLAN und NVGRE) sind Gateways erforderlich, die als Datenübergangs-Punkt einen potenziellen Bottleneck darstellen, egal ob sie tatsächlich als ASIC oder als Appliance-Hardware oder wiederum als VM realisiert sind.

- Einige hochwertige Netzwerk-Funktionen können aufgrund der Enkapsulierung von den virtualisierten Netzen nicht genutzt werden (z.B. Differentiated Services).

Das Underlay-Modell ist eher als "klassische" SDN-Technologie bekannt und fokussiert sich darauf, dass eine Reihe von virtuellen und physischen Netzkomponenten (NE, Netzwerk Elemente) durch einen SDN Controller gesteuert werden, der die Flow Tabellen der NEs manipulieren und somit das Netzwerk-Verhalten kontrollieren kann (eine Übersicht zeigt Abbildung 7). Die denkbaren Einsatzfälle sind somit breiter angelegt, sie betreffen alle Netzbereiche wie RZ, Campus, Edge und MAN/WAN. Da der Header, der in Flow Tabellen mittels Paket-Lookup geprüft wird, meistens auf Schicht 1 bis 4 limitiert ist, bedienen Underlay-Modelle über die Flow-Tabellen-Steuerung vielfach die Funktionen der Schichten 1 bis 4, insbesondere gilt dies für OpenFlow.

Eine ONF-konforme SDN-Architektur enthält stets einen Controller und basiert somit stets auf dem Underlay-Modell.

Die SDN Umfrage von Webtorials (Dr. Jim Metzler e.a., 2014) kommt zu dem Ergebnis, dass aktuell eine (wenn auch geringe) Mehrheit der SDN-Anwender den höheren Mehrwert im Underlay Modell sieht.

Auch eine Kombination von beiden Modellen, das sogenannte Overlay/Underlay Modell, ist denkbar. Hierbei wird die Virtualisierung im Edge Bereich mit der zentralen Kontrolle der Netzwerk-Elemente durch einen SDN-Controller kombiniert. Die Management-Herausforderungen beider Modelle addieren sich dann.

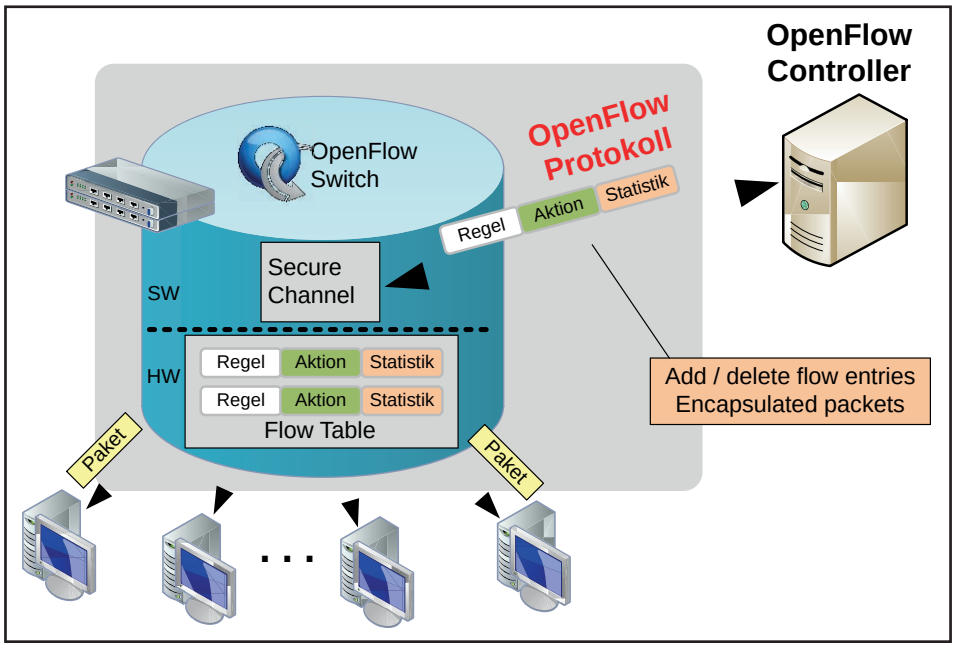

Abbildung 7: SDN Underlay Modell mit OpenFlow

Im nächsten Teil lesen Sie:
- OpenDaylight Projekt
- Network Function Virtualization
- NFV Einsatzszenarien
- NFV und SDN
- Marktrelevanz von SDN und NFV und Fazit

Abkürzungen

3GPP	3rd Generation Partnership Project
AaaS	Application as a Service
ALTO	Application-Layer Traffic Optimization
API	Application Programming Interface
ASIC	Application Specific Integrated Circuit
BGP	Border Gateway Protocol
BSS	Business Support System
CDN	Content Delivery Network
CDPI	Control-Data-Plane Interface
COTS	Commercial-Off-The-Shelf
CPU	Central Processing Unit
DAS	Direct Attached Storage
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
DPI	Deep Packet Inspection
EM	Element Manager
EMS	Element Management System
EPC	Evolved Packet Core
ETSI	European Telecommunications Standards Institute
ESX	Elastic Sky X (VMware)
ESXi	Elastic Sky X Integrated (VMware)
FG	Forwarding Graph
GENEVE	Generic Network Virtualization Encapsulation
GPE	Generic Protocol Extension
IaaS	Infrastructure as a Service
ICT	Information and Communications Technology
ID	Identifikator
IDC	International Data Corporation
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IF	Interface
IMS	IP Multimedia Subsystem
IP	Internet Protocol
IPS	Intrusion Protection System
ISG	Industry Specification Group
IT	Informations-Technologie
ITU-T	International Telecommunications Union for Telecommunication Standards
KVM	Kernel-based Virtual Machine
LAN	Local Area Network
LB	Load Balancer
LISP	Locator / ID Separation Protocol
M&O	Management and Orchestration
MAC	Media Access Control
MAN	Metropolitan Area Network
MANO	Management and Orchestration
MME	Mobility Mangement Entity
MPLS	Multi Protocol Label Switching
NAC	Network Access Control
NAS	Network Attached Storage
NAT	Network Address Translation
NBI	Northbound API
NE	Network Element
NF	Network Function
NFV	Network Function Virtualisation
NFVI	NFV Infrastruktur

NGN	Next Generation Network
NSH	Network Service Header
NV	Netzwerk-Virtualisierung, Network Virtualisation
NVGRE	Network Virtualization using Generic Routing Encapsulation
ODL	OpenDaylight
OEM	Open Equipment Manufacturer
OF	OpenFlow
ONF	Open Networking Foundation
OPNFV	Open Platform for NFV Projekt
OSPF	Open Shortest Path First
OSS	Operations Support System
OVS	Open Virtual Switch
PGW	Packet Data Network Gateway
POC	Proof of Concept
PoP	Point of Presence
PSTN	Public Switched Telephone Network
QoS	Quality of Service
REST	Representational State Transfer
RGW	Residental Gateway
RTP	Real Time Protocol
RZ	Rechenzentrum
SBC	Session Border Controller
SBI	Southbound Interface
SDK	Software Development Kit
SDN	Software-Defined Networking
SDNi	SDN Interconnect
SFC	Service Function Chaining
SGW	Serving Gateway
SLA	Service Level Agreement
SNMP	Simple Network Monitoring Protocol
SPBM	Shortest Path Bridging Mac
STT	Stateless Tunneling Protocol
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VM	Virtual Machine
VNF	Virtualized Network Function
VNF-FG	VNF Forwarding Graph
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
VRRP	Virtual Router Redundancy Protocol
vSwitch	virtueller Switch
VXLAN	Virtual Extensible LAN
WAN	Wide Area Network
WG	Working Group
WLAN	Wireless LAN

Links

www.etsi.org/technologies-clusters/technologies/nfv
www.opendaylight.org/project/technical-overview
www.opennetworking.org

Literatur

- ETSI: Network Functions Virtualisation (NFV) White Paper 3, 10/2014
- ETSI: Network Functions Virtualisation (NFV) White Paper 2, 10/2013
- ETSI: GS NFV 001 (10/2013) Network Functions Virtualisation (NFV); Use Cases
- ETSI: GS NFV 002 (12/2014) Network Functions Virtualisation (NFV); Architectural Framework
- ETSI: GS NFV-INF 001 (01/2015) Network Functions Virtualisation (NFV); Infrastructure Overwiew
- ETSI: GS NFV-INF 005 (12/2014) Network Functions Virtualisation (NFV); Infrastructure; Network Domain
- ONF: OpenFlow Switch Specification 1.5.0, Dezember 2014
- ONF: OpenFlow Switch Specification 1.3.0, April 2012
- ONF: North Bound Interface Working Group (NBI-WG) Charter (06/2013)
- ONF: OF-CONFIG 1.1 OpenFlow Management and Configuration Protocol
- OpenDayligt: Hydrogen Diagramm
- OpenDayligt: Helium Diagramm
- SDxCentral: What ist NFV – Network Functions Virtualization?

Lesen Sie auch den Artikel aus dem Netzwerk Insider Oktober 2012 "Werden SDN und OpenFlow herkömmliche Netzwerke verdrängen?" von Petra Borowka-Gatzweiler.

ComConsult Veranstaltungskalender

RZ-RZ-Kopplung - alles nur eine Frage der Bandbreite?, 09.03.15 in Bonn

fast ausgebucht

Rechenzentren in entfernten Standorten zu betreiben erfordert sich mit IT-Sicherheit, Desaster Recovery, Service Level Agreements und Hochverfügbarkeit auseinander zu setzen. Dabei sind zum Teil Vorgaben bspw. vom BSI zu beachten. In dieser Schulung werden die aktuellen Techniken erläutert und für die richtige strategische Entscheidung zu einem Gesamtkonzept zusammengeführt.

Preis: € 990,-- netto

Die neue EU-Datenschutzgrundverordnung, 09.03.15 in Bonn

Garantietermin

2015 wird ein neues einheitliches Datenschutzrecht in der Europäischen Union in Kraft treten. Die Verordnung ist noch nicht endgültig verabschiedet, aber die wichtigsten Regelungen sind bereits jetzt weitgehend klar. So wird es gravierende Änderungen bei der Verarbeitung von sensiblen Daten und bei der grenzüberschreitenden Datenverarbeitung geben. Informieren Sie sich frühzeitig über die geplanten Regelungen, damit Sie bei Inkrafttreten der Richtlinie wissen, was auf Ihr Unternehmen zukommt.

Preis: € 990,-- netto

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen, 09.03. - 11.03.15 in Hamburg

Garantietermin

Dieses Seminar vermittelt alle notwendigen Projektschritte zu einer erfolgreichen Umsetzung von VoIP Projekten. Diese erstrecken sich über die Einsatz- und Migrations-Szenarien, die einsetzbaren Basis-Technologien und Komponenten und die erweiterten TK-Anwendungen wie IVR, UM oder UC. Es werden Bewertungskriterien für eine TK-Lösung und eine Übersicht über den bestehenden TK-Markt mit allen etablierten Hersteller vorgestellt.

Preis: € 1.890,-- netto

Interne Absicherung der IT-Infrastruktur, 09.03. - 10.03.15 in Hamburg

Garantietermin

In diesem Seminar lernen Sie wie man die Sicherheit von LAN, WAN, Endgeräten, RZ-Bereichen, Servern und SAN erreicht. Konkrete Beispiele aus der Praxis zeigen den Weg zu einer erfolgreichen IT-Sicherheits-Lösung.

Preis: € 1.590,-- netto

WAN: Konzept, Planung und Ausschreibung, 09.03. - 10.03.15 in Hamburg

Garantietermin

Seminar über die erfolgreiche Konzeption, Planung und Betrieb von WAN-Netzwerken. Lernen Sie wie Sie mit modernsten Technologien und erprobten Architekturen wirtschaftliche, verfügbare und leistungsfähige WAN-Lösungen aufbauen können. Erfahren Sie wie Sie sinnvoll SLAs für die Praxis aufsetzen können, die auch im Tagesbetrieb standhalten. Mit vielen Tipps und Tricks aus der Praxis.

Preis: € 1.590,-- netto

Wireless LAN professionell, 09.03. - 11.03.15 in Hamburg

Garantietermin

Lernen Sie in diesem Seminar wie Sie eine WLAN-Lösung zukunftsorientiert und investitionssicher für die verschiedensten Endgerätetypen und Dichten aufbauen. Lernen Sie wie Sie Verfügbarkeit und Bandbreite optimieren. Verbessern Sie Ihr WLAN mit den verschiedensten Struktur-Elementen vom Access-Point bis zum WLAN-Controller. Erfahren Sie worin sich Produkte und Technologien führender Anbieter unterscheiden. Berücksichtigen Sie die neusten Entwicklungen zur Gestaltung einer WLAN-Lösung, die langfristig tragfähig und wirtschaftlich ist. Lernen Sie Vor- und Nachteile aller aktuellen Technologien kennen und vermeiden Sie Planungs-Fehler.

Preis: € 1.890,-- netto

Internetworking: optimales Netzwerk-Design mit Switching und Routing, 23.03. - 27.03.15 in Aachen

Garantietermin

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

Preis: € 2.490,-- netto

IPv6 Grundlagen - SeminarPlus, 23.03. - 24.03.15 in Berlin

Garantietermin

IPv6 betreiben, bedingt IPv6 verstehen. In diesem Seminar werden die Grundlagen des neuen IP Protokolles verständlich und praxisnah vermittelt. Die Schulung richtet sich gleichermaßen an Planer, Betreiber, Administratoren und Software-Entwickler.

Preis: € 1.790,-- netto

Rechenzentrumsdesign - Technologien neuester Stand, 23.03. - 25.03.15 in Berlin

fast ausgebucht

Dieses Seminar analysiert die neuesten Technologie-Trends im Rechenzentrum. Sie lernen von der Verkabelung über die Stromversorgung, die Klimatisierung und den Schrankaufbau, wie ein ausfallsicheres und energieeffizientes Rechenzentrum heute strukturiert wird. Mechanismen für Redundanz im Netzwerk, Lastverteilung und Standort-übergreifende Hochverfügbarkeit werden diskutiert und es wird untersucht wie diese mit dem fortwährenden Trend zur Virtualisierung zusammenspielen. Abschließend werden aktuelle Speichersysteme, deren Anbindung über die am Markt verfügbaren Übertragungsprotokolle sowie Aspekte zur Datensicherung und Disaster Recovery diskutiert.

Preis: € 1.890,-- netto

Netzzugangskontrolle: Technik, Planung und Betrieb, 23.03. - 25.03.15 in Berlin

Garantietermin

Dieses 3-tägige Seminar vermittelt den aktuellen Stand der Technik der Netzzugangskontrolle (Network Access Control, NAC) und zeigt die Möglichkeiten aber auch die Grenzen für den Aufbau einer professionellen NAC-Lösung auf. Schwerpunkt bildet die detaillierte Betrachtung der Standards IEEE 802.1X, EAP und RADIUS. Dabei wird mit IEEE 802.1X in der Fassung von 2010 und mit IEEE 802.1AE (MACsec) auch auf neueste Entwicklungen eingegangen.

Preis: € 1.890,-- netto

Zertifizierungen

ComConsult Certified Network Engineer

Lokale Netze
18.05. - 22.05.15 in Aachen
28.09. - 02.10.15 in Aachen

TCP/IP-Netze erfolgreich betreiben
13.04. - 15.04.15 in Düsseldorf
15.06. - 17.06.15 in Nürnberg
09.11. - 11.11.15 in Köln

Internetworking
23.03. - 27.03.15 in Aachen
08.06. - 12.06.15 in Aachen
19.10. - 23.10.15 in Aachen

Paketpreis für zwei 5-tägige und ein 3-tägiges Intensiv-Seminar € 6.180,-- netto (Einzelpreise: € 2.490,-- netto bzw. 1.890,-- netto)

ComConsult Certified Trouble Shooter

Trouble Shooting in vernetzten Infrastrukturen
05.05. - 08.05.15 in Aachen
27.10. - 30.10.15 in Aachen

Trouble Shooting für Netzwerk-Anwendungen
09.06. - 12.06.15 in Aachen
17.11. - 20.11.15 in Aachen

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

ComConsult Certified Voice Engineer

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen
09.03. - 11.03.15 in Hamburg
04.05. - 06.05.15 in Bonn
28.09. - 30.09.15 in Köln

Session Initiation Protocol Basis-Technologie der IP-Telefonie
13.04. - 15.04.15 in Düsseldorf
15.06. - 17.06.15 in Nürnberg
09.11. - 11.11.15 in Köln

Umfassende Absicherung von Voice over IP und Unified Communications
23.03. - 24.03.15 in Berlin
08.06. - 09.06.15 in Stuttgart
19.10. - 20.10.15 in Bonn

Optionales Einsteiger-Seminar: IP-Wissen für TK-Mitarbeiter
27.04. - 28.04.15 in Nürnberg
14.09. - 15.09.15 in Bonn

Wir empfehlen die Teilnahme an diesem Seminar **"IP-Wissen für TK-Mitarbeiter"** all jenen, die die Prüfung zum ComConsult Certified Voice Engineer anstreben, ganz besonders aber den Teilnehmern, die bisher wenig bis kein Netzwerk Know How, insbesondere TCP/IP, DNS, SIP usw., vorweisen können.

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

Impressum

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

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

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

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

Für unverlangte eingesandte Manuskripte
wird keine Haftung übernommen