ComConsult Research

Der Netzwerk Insider

Juni 2013

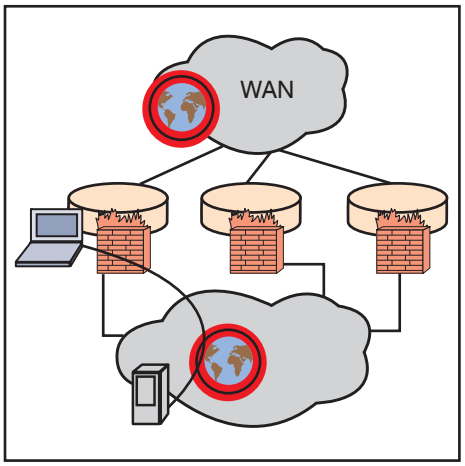
Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

Aktuelle Trends im WAN-Bereich

von Dr. Behrooz Moayeri

Der vorliegende Beitrag befasst sich mit den aktuellen Entwicklungen bei Wide Area Networks (WANs). Dabei handelt es sich um mehrere Trends in verschiedenen Aspekten der WAN-Technologien und des WAN-Marktes. Einige dieser Trends hängen miteinander zusammen, einige sind völlig unabhängig voneinander. Die Trends haben teilweise globalen und teilweise nur regionalen Charakter oder sind in verschiedenen Regionen unterschiedlich stark. Daher ist die Reihenfolge der Behandlung aktueller WAN-Trends nicht als eine Indikation der allgemeinen Bedeutung der Trends oder der Bedeutung für ein spezifisches Unternehmen zu sehen.



Steigender Kapazitätsbedarf durch RZ-Konsolidierung, Video etc.

Ein Trend, der seit Jahrzehnten anhält und sich in seiner Intensität über lange Zeit nicht geändert hat, ist der steigende Kapazitätsbedarf im WAN-Bereich. Die Zentralisierung von IT-Ressourcen von Unternehmen zusammen mit der Konsolidierung der Unternehmen selbst durch Fusionen und Akquisitionen haben seit über zehn Jahren zur Folge, dass der WAN-Kapazitätsbedarf fast jedes Unternehmens kontinuierlich steigt.

weiter auf Seite 10

Zweitthema

Neue Anwendungsformen im WLAN: 60-GHz-WLAN gemäß IEEE 802.11ad

von Dr. Joachim Wetzlar

Wozu braucht man ein WLAN, das nur wenige Meter weit reicht? Sie erinnern sich an meinen Artikel aus dem Netzwerk Insider im Oktober 2012. Mein Fazit damals war, dass die vom WLAN aufgespannten Versorgungsbereiche mit größerer Bitrate immer weiter schrumpfen werden. Die gilt insbesondere für das WLAN im „neuen“ Frequenzbereich bei 60 GHz. Diese ultrakurzen Wellen mit 5 Millimeter Wellenlänge sind kaum in der Lage, Wände zu durchdringen. Ein Nutzen für Endgeräte, die von einem WLAN hohe Bitrate und uneingeschränkte Mobilität erwarten, entsteht mit dieser Technik wohl kaum – oder doch?

Inzwischen sind einige Monate ins Land gegangen und die aktuelle Marktentwicklung lässt erste Ideen für einen praktischen Einsatz dieser Technik erkennen. Die „Task Group ad” (TGad) des IEEE 802.11 hat ihren Anhang zum gleichnamigen Standard wie erwartet zum Jahresende 2012 fertiggestellt; er hat alle Hürden des Standardisierungsprozesses genommen. Produktentwickler können sich also nun auf eine stabile Grundlage verlassen. Mit dem vorliegenden Artikel möchte ich zunächst einige technische Details des Standards erläutern, bevor ich auf die heute sichtbaren Produktentwicklungen eingehe.

weiter Seite 19

Geleit

Software Defined Networking in der Analyse

von Dr. Jürgen Suppan

ab Seite 2

Standpunkt

Sprengstoff im Internet of Things

ab Seite 16

Report-Neuerscheinung

Moderne Wireless-Technologien

ab Seite 18

Aktuelle Veranstaltungen

ComConsult SDN-Forum 2013 Sommerschule 2013

ab Seite 5

Zum Geleit

Software Defined Networking in der Analyse

So langsam klären sich die Fragezeichen und es wird immer deutlicher, dass SDN die Zukunft der Netzwerke bestimmen wird. Es wird ein Prozess sein, der über viele Jahre in mehreren Stufen gehen wird. Dabei wird es sehr unterschiedliche Auslegungen geben, aber die Tragweite ist erheblich:

- Switches werden austauschbare Commodity, die Preisentwicklung wird über 10 Jahre der der heutigen PC-Hardware ähneln
- Aus dem Hardware-Markt wird ein Software-Markt
- Es wird eine neue Anbieter-Struktur geben, da die Entwicklung der Software erhebliche Investitionen erfordern wird und nicht alle der bestehenden Hersteller die Reserven für diese Entwicklung haben
- In der ersten Entwicklungsstufe der nächsten drei Jahre werden Netzwerke dynamischer und programmierbar

Das Grundprinzip ist auf den ersten Blick einfach: in den Switches bleibt nur noch die Data-Plane - also die Paketweiterleitung – und die Control Plane - die die Weiterleitung steuert - wandert in einen zentralen Controller. OSPF, Link Aggregierung, Spanning Tree, TRILL, SPB, MPLS ... werden Software-Applikationen in diesem Controller. Aus einem Hardware-Markt wird ein Software Markt.

Schaut man tiefer in dieses scheinbar einfache Grundprinzip, dann wird die Tragweite klar. Gehen wir dazu noch einmal zurück zu einem heutigen Switch. Dieser empfängt ein eingehendes Paket und muss je nach Arbeitsweise das Paketformat des Pakets verstehen. Bei einem Layer-2-Switch waren das früher die Absender und Ziel-MAC-Adresse, aus denen dann die MAC-Weiterleitungs-Tabellen aufgebaut wurden. Bei einem Layer-3-Switch waren das die Absender und die Ziel-IP-Adressen, die zusammen mit den aus den Routing-Verfahren bestimmten Routing-Tabellen die Weiterleitung bestimmen. Einfach formuliert bestimmen in einem traditionellen Switch diese Tabellen die Grundarbeitsweise in der Weiterleitung.

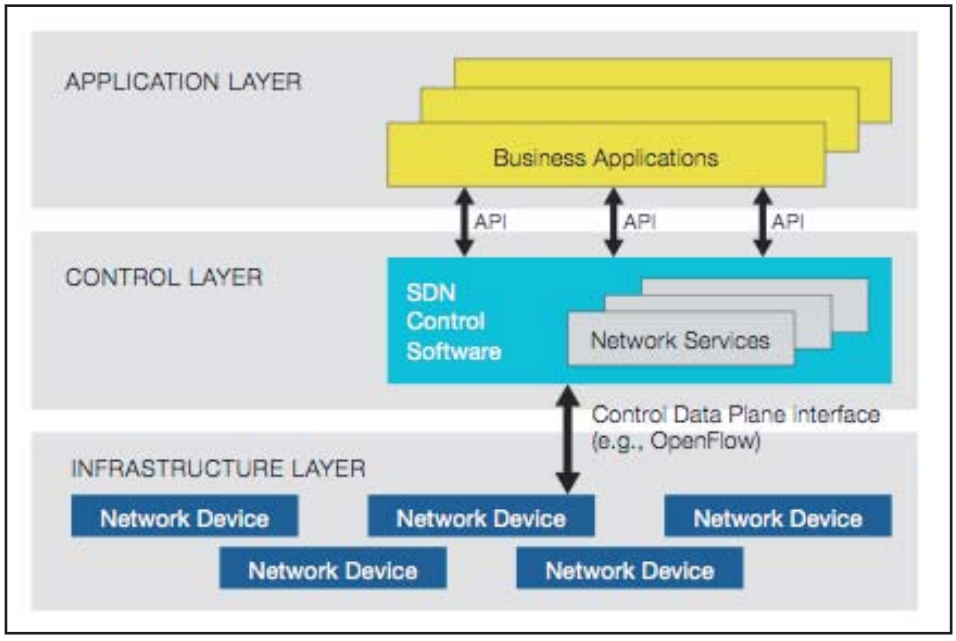


Abbildung 1: SDN-Grundarchitektur Quelle: Whitepaper Open Network Foundation

Wo ist jetzt das Problem? Nun, das Paketformat, die Weiterleitungstabellen und die ausgeführten Switching-Anwendungen gehören untrennbar zusammen. Das betrifft nicht nur Adressen, sondern auch Zusatzinformation wie VLAN-ID und QoS. Und aus den einfachen Paketformaten der Vergangenheit sind inzwischen gewaltige Gebilde geworden, hinter denen sich zum Teil komplexe Verfahren verbergen. Anders formuliert legen neue und fortschrittliche Verfahren wie TRILL oder SPB neue Paketformate fest. Alleine in den letzten 3 Jahren haben sich diese Formate drastisch verändert. Und die aktuelle Diskussion um Overlays und Netzwerk-Virtualisierung zeigt, dass wir hier noch nicht am Ende sind. Auch neue Protokolle wie IPv6 tragen ihren Teil dazu bei, dass es neue Formate gibt.

Layer-2 und Layer-3-Switches gewinnen ihre Fähigkeit, Pakete im Terabit-Bereich weiterleiten zu können, aus den eingesetzten ASICs. Und die ASICs müssen die gesamte Bearbeitungs-Pipeline im Switch vom Eintreffen des Pakets über die Analyse des Formats, die Verwaltung der Tabellen und die letztendliche Weiterleitung abdecken. Und hier liegt die Tücke. Kommt ein neues Verfahren auf den Markt und ändert sich das Rahmenformat, dann besteht die Gefahr, dass die Switch-Hardware das nicht kann. Das typischste Beispiel der letzten Jahre dafür sind TRILL und DCB. Derartige Veränderungen erfordern bisher Investitionen in neue Hardware und sind somit nur langsam und teuer umsetzbar.

Was ist mit SDN anders? SDN basiert auf der Idee, dass ein Switch im Empfang eines Pakets jedes beliebige Bitmuster im Paket bearbeiten kann. Das kann er in mehreren Schritten. So kann er im ersten Schritt die Adressen, im zweiten weiterführende Parameter wie VLAN-ID oder QoS, im dritten Protokollinformationen und soweiter und sofort bearbeiten. In jedem Schritt kann er Aktionen im Sinne der Veränderung des Pakets ausführen. Also zum Beispiel eine neue Zieladresse einfügen oder ein Paket an den Sender zurücksenden (im Falle von IPv6 zum Beispiel). Diese Fähigkeit der Verarbeitung jedes beliebigen Bitmusters geht einher mit einer zentralen Flow-Tabelle, die im Prinzip angibt, welche Teile des Pakets gelesen und wie darauf reagiert werden soll. Diese Flow-Tabellen werden durch den zentralen Controller generiert.

Was bedeutet das? Heute haben wir Layer-2-Switches, Layer-3-Switches, Router, Load Balancer, Firewalls, Proxies, modulare Switches, nicht modulare Switches, Spezial-Module in den Switches. Würden wir versuchen eine Kategorisierung und Auflistung über die Hersteller hinweg zu machen, wäre die Gestaltungsbreite erheblich.

Wie sieht der Switch der Zukunft aus? Im Prinzip gibt es diese Unterteilung nicht mehr. Jeder Switch ist im Kern identisch, wird zur Commodity, zu einem Allgemeingut ohne besonderen Wert. Layer-2- und Layer-3-Arbeitsweise sind einfach unterschiedlich ausgefüllte Flow-Tabellen. Die Nutzungsdauer der Switches geht ins Unendliche, da sie neue Verfahren per Definition können. Neue Verfahren sind eben einfach nur neue Flow-Tabellen. Damit entsteht eine ganz neue Form der Wirtschaftlichkeit, die die Nutzung von Hardware über sehr lange Zeiträume gestattet.

Gibt es dann nur noch einen Switch? Zumindest würde das den Produkt-Katalog von Cisco doch sehr übersichtlich gestalten. Nun, natürlich müssen Switches weiterhin unterschiedliche Schnittstellen und Bandbreiten unterstützen. Dies könnte durch austauschbare Media-Interfaces erfolgen. Von der Logik her spricht einiges dafür, dass modulare Switches so wie wir sie kennen, dann nicht mehr existieren. Wird es unterschiedliche Performance-Klassen geben? Jein. Betrachtet man die aktuelle ASIC-Entwicklung, dann haben die neuen ASICs eine bahnbrechende Performance. Reicht diese nicht, kann durch Maschenbildung der ASICs fast jede beliebige Leistung erreicht werden.

Ist das das Ende der heutigen Switch-Hersteller? Nun, Intel hat vor drei Wochen bereits eine Referenz-Architektur für einen offenen Switch auf der Basis von Standard-Hardware vorgestellt. Und natürlich wird sich der Hardware-Markt massiv ändern. Im Prinzip deutet alles darauf hin, dass die Entwicklung der Netzwerke der Entwicklung der PCs folgen wird. Hardware wird Allgemeingut und austauschbar. Als solches wird sie auch immer preiswerter. Es erfolgt eine Marktverschiebung von der Hardware zur Software.

Also schnell alle Cisco-Aktien verkaufen? Besser nicht. Aus dem heutigen Hardware-Markt wird einfach ein gewaltiger neuer Software-Markt werden. OSPF und TRILL sind dann kaufbare Apps auf einem SDN-Controller. Themen wie Management und weitergehende Intelligenz werden weiterhin die Hersteller-Bindung sichern. Und der Marktvorsprung der großen Anbieter ist hier riesig. Sie sind die einzigen, die über

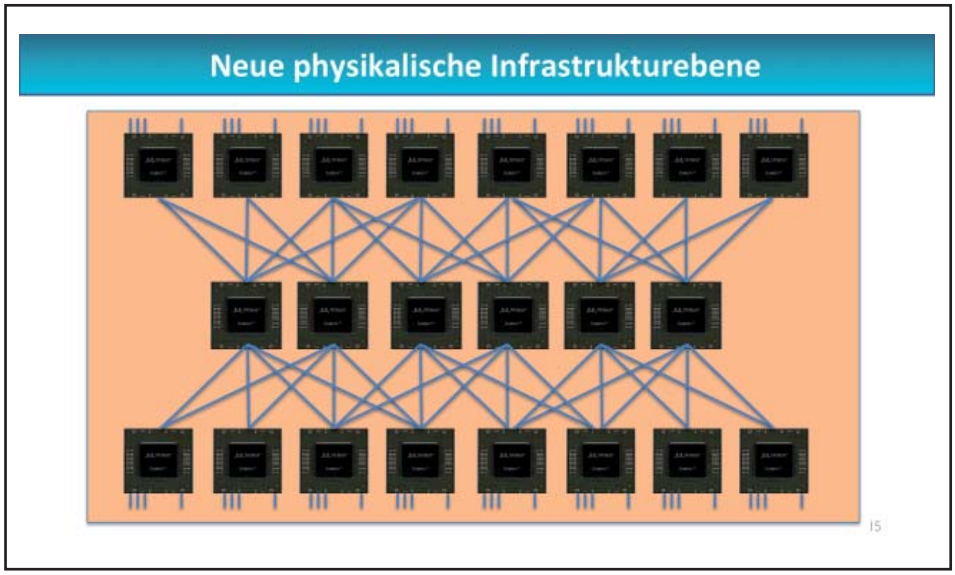


Abbildung 2: Maschenbildung mit zukünftigen ASICs, hier Mellanox als Beispiel
Quelle: Die Zukunft der LANs, Vortrag Dr. Kauffels auf dem ComConsult Netzwerk-Redesign Forum

ausreichendes Know How und auch das Kapital für diese neue Software-Welt verfügen. Was sich ändern kann und vermutlich wird sind die Margen, mit denen die Hersteller arbeiten. 60% sind im Software-Markt nicht haltbar. Also vielleicht doch besser rechtzeitig die Aktien verkaufen.

Wie realistisch ist dieses Szenario? Nun, als erstes muss klargestellt werden, dass kein einziger verfügbarer Switch die notwendigen Eigenschaften für dieses Szenario hat. HP hat zwar beispielsweise im Moment 29 Switches mit Open Flow Unterstützung im Programm. Aber das sind hybride Geräte in dem Sinne, dass sie zusätzlich zu der bisherigen traditionellen Arbeitsweise Flow-Tabellen unterstützen. Diese hybriden Geräte von allen Anbietern sind im Sinne des dargestellten Szenarios unbrauchbar. SDN erfordert einen auf performante Flow-Verarbeitung ausgelegten und optimierten Switch. Jeder andere Versuch wird in einem Performance-Desaster enden.

Wird es den richtigen SDN-Switch geben? Auf der ONS 2013 wurde vor 3 Wochen ein Referenz-Design für einen SDN-ASIC vorgestellt, das in Kooperation zwischen der Stanford University und Texas Instruments entwickelt wurde. Wir werden auf dieses Design auf unserem SDN-Forum kurz eingehen, weil es die Unterschiede

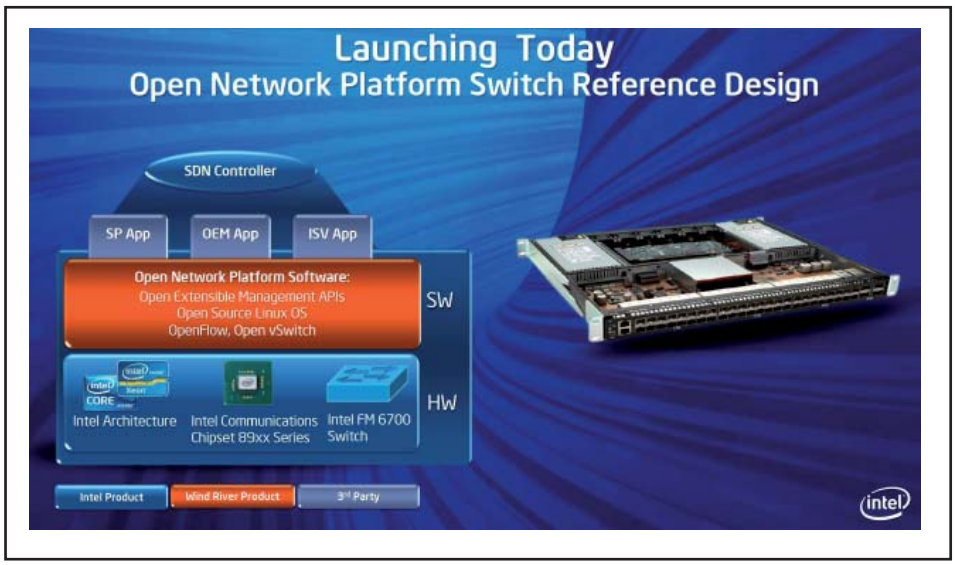


Abbildung 3: Switches als Hardware-Allgemeingut zu Massenpreisen, Intel-Referenzarchitektur vorgestellt von Rose Schooler VP Architecture

Software Defined Networking in der Analyse

zur heutigen Welt sehr klar macht. Aber es ist bekannt, dass Hersteller wie Fulcrum/ Intel massiv an diesem Thema arbeiten. So gibt es bereits erste reine SDN-Switches, die aber in der Leistung noch limitiert sind.

Ist die Verfügbarkeit der Hardware die einzige Tücke? Nein, es gibt vier weitere Großbaustellen:

- Open Flow
- Der SDN-Controller
- Das Northbound-Interface
- Die Verfügbarkeit von Apps

Open Flow unterstützt die Bearbeitung beliebiger Bitmuster im aktuellen Standard nicht. Überhaupt ist es von der wirklich benötigten Zukunftsfunktionalität vermutlich noch mindestens 3 Jahre entfernt. Und je weiter die Normung geht, desto langsamer wird sie in der Regel.

Wir brauchen einen Marktstandard für einen SDN-Controller. Es macht keinen Sinn, dass es 20 oder 30 davon gibt. Das Open Daylight Konsortium arbeitet an einem Open Source Controller, der diese Anforderungen erfüllen soll. Die Arbeit wird relativ schnell erste Ergebnisse zeigen, aber danach liegt die Tücke im Detail. Auch hier ist mit mindestens drei Jahren zu rechnen, bis wir wirklich einen großen Schritt weiter sind.

Die Zukunft von SDN wird durch die Software der Apps bestimmt. Damit diese Apps funktionieren, muss eine sauber definierte Schnittstelle zum Controller existieren. Dies ist momentan nicht der Fall, sollte aber bis Ende 2014 zu schaffen sein.

Und damit sind wir beim Schlüssel: den Apps. Die Intelligenz der heutigen Switches und Router wird in Zukunft in den zentralen Software-Apps liegen. Das ist der Markt der Zukunft, auf den sich auch Hunderte von Startups stürzen werden, sobald der OpenDaylight-Controller verfügbar ist.

Wie muss man sich die Apps der Zukunft vorstellen? Wird es eine TRILL und eine OSPF-Apps geben? Vermutlich nicht. Beide Verfahren realisieren Shortest-Multipath-Lösungen und haben ihren jeweiligen Mechanismus, um die Topologie des Netzwerkes erkennen zu können. Das wird aber in Zukunft nicht mehr notwendig sein, da die Topologie vom Controller ermittelt und als Datenstruktur bereitgestellt wird. Die Apps der Zukunft werden eine ähnliche Funktionalität wie heute bieten, aber anders arbeiten.

Was bedeutet das für Planung und Design von Netzen. Nun, da es die heutige Unterscheidung zwischen L2 und L3 nicht mehr

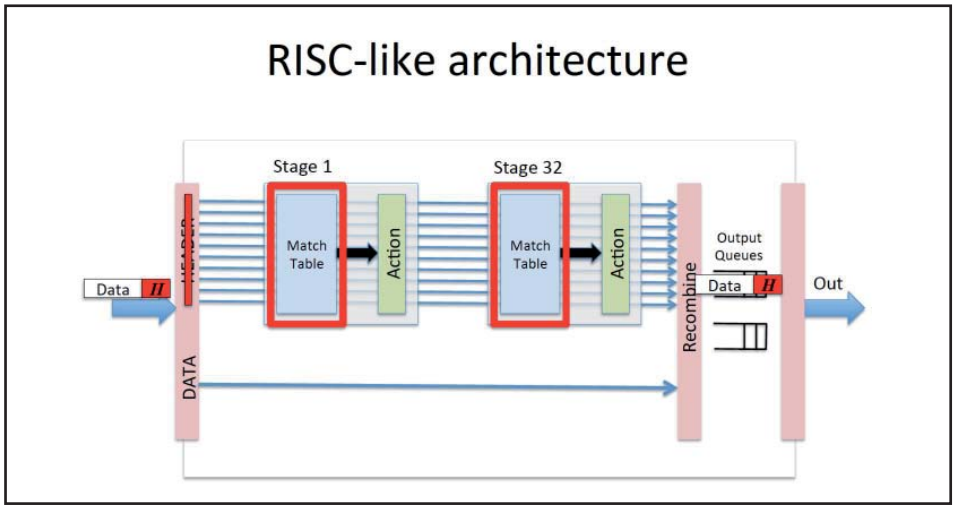


Abbildung 4: Muster-Design für einen Protokoll-unabhängigen und unlimitierten SDN-Switch, Nick McKweon, Stanford University in Kooperation mit Texas Instrument

gibt und in der ersten Aufbaustufe alles mit einem L2-Netzwerk beginnt, ist der Gestaltungs- und Design-Spielraum viel größer als heute. Es wird weiterhin L2 und L3 geben, aber vermutlich wird es viel mehr Auslegungsvarianten als heute geben. Das Netz der Zukunft wird unvergleichbar viel mehr flexibel sein als heute.

Also: fantastische Zukunft, aber leider noch nicht verfügbar? Tatsächlich wird die Entwicklung in Phasen erfolgen. Die heutigen hybriden Switches sind nicht in der Lage, diese Zukunfts-Vision zu erfüllen. Aber sie haben bereits ihre Einsatzbereiche. Ein Beispiel wäre eine Sicherheits-App (und davon wird es bis Ende 2014 viele geben), die einzelne Flows gezielt umleitet, wenn ein Risiko gesehen wird oder ein höherer Sicherheitsgrad für eine Applikation erreicht werden will. Der andere bereits in 2013 nutzbare Anwendungsbereich ist „Dynamic Provisioning". Ein Beispiel dafür die die Bandbreitensteuerung von Lync-Videokonferenzen, die HP gerade vorgestellt hat. Cisco stellt diesen Anwendungsbereich unter den Oberbegriff „Programmierbare Netzwerke" und hat entsprechende APIs für seine Switches offen gelegt. Damit sind weitreichende Dynamik-Funktionen schon heute möglich.

Zu welchem Fazit führt das? Netzwerke werden in 10 Jahren anderes aussehen als heute. Die Hardware wird durch eine ziemlich einheitliche Weiterleitungs-Maschine abgelöst werden und der Markt der Zukunft liegt in der Software. Da Software sehr dynamisch ist, wird dies viele neue und spannende Netzwerk-Nutzungen möglich machen. Erste Beispiele davon sind bereits in 2013 verfügbar.

Wir diskutieren diese bahnbrechenden Entwicklungen mit Ihnen auf dem ComConsult SDN-Forum 2013. Kein Netzwerk-Planer und Verantwortlicher sollte diese Veranstaltung verpassen. Die Tragweite der angesprochenen Entwicklungen ist zu groß.

Ihr
Dr. Jürgen Suppan

Aktueller Kongress

ComConsult SDN-Forum 2013

Software-Defined-Netzwerke - die Zukunft der Netwerke

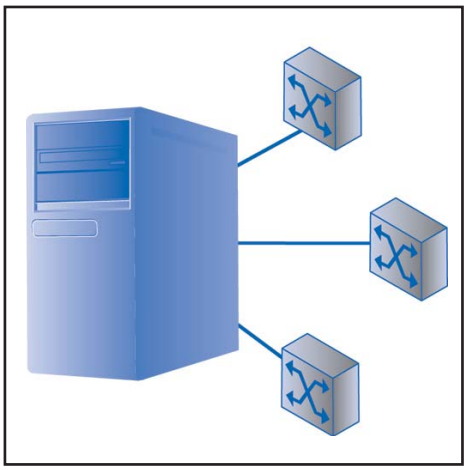
17.06. - 18.06.13 in Euskirchen

Die ComConsult Akademie veranstaltet vom 17.06. bis 18.06.13 ihr "ComConsult SDN-Forum 2013" in Euskirchen.

Software Defined Networking SDN wird die Netzwerk-Industrie in den nächsten Jahren deutlich verändern. Eine zentrale Software-Architektur wird die heutigen dezentral konfigurierten Switches ablösen. In spätestens fünf Jahren werden Switches generell programmierbar sein. Alle Anbieter passen ihre bestehenden Produkte im Moment entsprechend an oder bringen völlig neue und auf SDN optimierte auf den Markt.

Die Hersteller haben sich in Position gebracht:

- Cisco verteidigt seine Marktposition durch ein neues Automatisierungs-Konzept für das Rechenzentrum mit einer Kombination aus offenen APIs, zentraler SDN-Software und automatischer Provisionierung durch OpenStack. Gleichzeitig wird der Versuch gemacht, mit einer OpenSource Initiative „Open Daylight“ unter dem Dach der Linux Foundation die vielen neuen Start Ups in diesem Bereich zu blockieren.
- Intel wagt den Totalangriff mit einer neuen Hardware-Generation für SDN-Server und Fulcrum-Chips für eine neue Generation von Switches.



- HP hat SDN groß auf seine Fahnen geschrieben und sieht seine Chance zum Angriff auf Cisco.
- Extreme kooperiert mit BigSwitch und bringt eine neue Serie von reinen SDN-Switches auf den Markt.
- Brocade sieht generell in Software-Architekturen ein wesentliches Standbein für seine Zukunft und hat mit der Übernahme von Vyatta auch seinen Hut in den Ring geworfen.

Gleichzeitig sind viele Hersteller in der Situation, dass ihre bestehende Switch-Software überarbeitet werden muss. Altlasten, Komplexität und die Anpassung an neue Chipgenerationen erfordern nicht unerhebliche Neuprogrammierungen. SDN ist damit für viele Anbieter eine echte Alternative, die sowieso notwendige Erneuerung mit dem Angriff auf den Marktführer zu verbinden.

Das ComConsult SDN-Forum 2013 nimmt diese komplexe Situation aus Technologie, Hersteller-Interessen und Produktansätzen auseinander und analysiert:

- Welche Formen von SDN gibt es?
- Welche Rolle wird Software in Netzwerken in Zukunft spielen?
- Wie sehen die technischen Architekturen aus?
- Welche Vorteile entstehen wirklich?
- Wie reif sind Produkte und Technologien?
- Was machen die führenden Hersteller?
- Wie hängen SDN und OpenStack zusammen?

Wie immer man SDN betrachtet, egal mit welcher Ausprägung, hier entsteht eine völlig neue Technologie, die das Potenzial hat, unsere gesamte Netzwerk- und auch Rechenzentrums-Welt zu verändern.

Versäumen Sie nicht, sich einen Platz in dieser herausragenden Sonderveranstaltung zu sichern. Dieses Forum ist ein Muss für jeden Netzwerk-Planer und -Betreiber. Es geht um die Zukunft der Netzwerke.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

ComConsult SDN-Forum 2013

Ich buche den Kongress
ComConsult SDN-Forum 2013

☐ vom 17.06. - 18.06.13 in Euskirchen
zum Preis € 1.890,-- netto

☐ Bitte reservieren Sie mir ein Zimmer

vom _____ bis_____ 13

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

_____ Vorname

_____ Nachname

_____ Firma

_____ Telefon/Fax

_____ Straße

_____ PLZ,Ort

_____ eMail

_____ Unterschrift

Programmübersicht - ComConsult SDN-Forum 2013

Montag den 17.06.2013

9:30 bis 10:45 Uhr
Software Defined Networking in der Analyse:
Welche Rolle wird es spielen, wie verändert es den Markt, wann ist es für wen nutzbar?
- Zielmärkte und Relevanz
- Architektur-Elemente
- Programmierbarkeit von Netzwerken durch Anwendungen: wie muss man sich das vorstellen?
- Beispiele für den Mehrwert:
  - Dynamische Provisionierung
  - Desaster Recovery
  - Dynamische Sicherheits-Lösungen
- Reine Lehre kontra Hybrid: was bedeutet das eigentlich?
- Offenheit, Interoperabilität und Skalierbarkeit: Wunschdenken?
- Was passiert im Markt
  - Open Daylight und die Bedeutung für den Markt
  - ONF und ONS
  - Cisco OnePK: wie ist das zu bewerten?
- Roadmap für die nächsten Jahre

Dr. Jürgen Suppan, ComConsult Research GmbH

10:45 bis 11:15 Uhr Kaffeepause

11:15 bis 12:30 Uhr
SDN: viel mehr als Open Flow
- Ein SDN-Architekturmodell:SDNORM
- SDN-fähige Hardware: Switch- und Tunnel-ASICs
- SDN-Einbindung in Virtualisierungssoftware
- SDN-Herstellerstrategien im Überblick

Dr. Franz-Joachim Kauffels, unabhängiger Unternehmensberater

12:30 bis 14:00 Mittagspause

14:00 Uhr bis 14:45 Uhr
Wird alles virtuell: das Ende der Hardware?
- Virtuelle Switches und Router
- Virtuelle Firewalls und Service-Module (Load Balancer, IPS, …)
- Unterschiedliche Architekturmodelle durch Trennung von Control und Data Plane
- Auswirkung auf die Infrastruktur
- Auswirkung auf die Planung
- Monitoring und Trouble Shooting
- Sicherheit und Zuverlässigkeit

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

14:45 bis 15:45 Uhr
SDN und die Bedeutung für Cisco
- Überblick und Positionierung
- Segmentierung des Marktes
  - Unternehmen
  - Service Provider
  - MSDC
- Klassischer Ansatz versus Hybrid versus Controller
- OpenStack, OpenFlow, OnePK
- Open Daylight
- Use Cases

Gerd Pflüger, Cisco Systems GmbH

15:45 bis 16:00 Uhr Kaffeepause

16:00 bis 17:00 Uhr
SDN im Unternehmensnetz, was ist heute möglich?
- Möglichkeiten durch SDN
- Vergleich unterschiedlicher Architekturen
- Standardisierung und die Realität
- Hardware-Abhängigkeiten bei Software-Defined Networking

Dipl.-Ing. Markus Nispel, Enterasys Networks Deutschland GmbH

17:00 bis 17:30 Uhr
Offene Diskussion und Fragen der Teilnehmer,
auf dem Podium voraussichtlich:
Dr. Suppan, Dr. Kauffels, Cisco, Enterasys, Extreme, HP

ab 18:00 Uhr Happy Hour

Dienstag, den 18.06.2013

9:00 bis 10:30 Uhr
Vertiefungsvortrag:
SDN in der technischen Analyse: kann es halten was es verspricht?
- Die Architektur und die Schnittstellen
- Was macht ein Controller eigentlich?
- Was leistet Open Flow, was leistet es nicht?
  - Architektur
  - Funktions-Übersicht
- Was ist das Northbound Interface und warum ist es wichtig
- Brauchen wir mehr? Vergleich von Herstellerlösungen und OpenFlow
- Offenheit und Interoperabilität: aber wie?
- Offene Probleme
  - Controller
  - Overlays
  - Open Flow
- Bewertungskriterien zur Einschätzung von SDN

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

10:30 bis 11:00 Uhr Kaffeepause

11:00 bis 12:00 Uhr
SDN: eine Technologie verändert die Netzwerk-Welt
1. Software Defined Networking, ein Blick hinter die Kulissen
2. SDN Architektur und deren Elemente
- Infrastruktur
  - Openflow quo vadis, weitere Protokolle oder hybrid?
  - Physikalische und virtuelle Switches
- SDN Controller
  - Funktionalitäten (RZ, Campus, Zweigstelle) und der Rest der IT-Welt
- Applikationen und Netzwerkfunktionen
  - Loadbalancing, Security, UC&C

3. HP Software Defined Datacenter, mehr als nur ein Slogan
- Software Defined Server / Software Defined Storage

4. Ausblick
- Wohin entwickeln sich Prozessoren und Speicher und was können wir davon heute wie nutzen?

Dipl.-Ing. Andreas Hausmann, Dipl.-Ing. Axel Simon, Hewlett-Packard GmbH

12:00 bis 13:00 Uhr
SDN: die reine Lehre heute schon verfügbar?
- Was geht heute mit SDN?
- BigSwitch, NEC und Floodlight
- Hybride Lösung kontra reine Lehre
- Link Aggregation: geht das?
- QoS und Bandbreiten-Management mit Open Flow
- Automatisches Flow Management mit dynamischen ACLs

Dipl.-Ing. Olaf Hagemann, Extreme Networks GmbH

13:00 bis 14:00 Mittagspause

14:00 bis 15:00 Uhr
Overlays: Anbindung virtueller Maschinen im Rechenzentrum der Zukunft
- Hintergrund: Martin Casado und Nicira, VMware, Microsoft
- Anforderung der Netzwerk-Anbindung virtueller Maschinen
- Unterschiedliche Lösungen im Vergleich
- Overlays: die Hype-Technologie
- Overlay und SDN
- Ausblick: Bedeutung von Software

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

15:00 bis 16:00 Uhr
Ist SDN die Lösung für dringende Betriebsprobleme?
- Wichtige Anforderungen von Netzbetreibern
- Was bedeuten verschiedene Modi der Verteilung der Intelligenz im Netz für den Betrieb?
- Sind WLAN Controller ein Vorbild für LAN?
- Dürfen Controller und Switches von verschiedenen Herstellern sein?

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

16:00 bis 16:15 Uhr
Abschluss-Diskussion und Zusammenfassung

16:15 Ende der Veranstaltung

Intensiv-Seminar

Sommerschule 2013

Intensiv-Update auf den neuesten Stand der Netzwerktechnik

01.07. - 05.07.13 in Aachen

Die ComConsult Akademie veranstaltet vom 01.07. - 05.07.13 ihre "Sommerschule 2013" in Aachen.

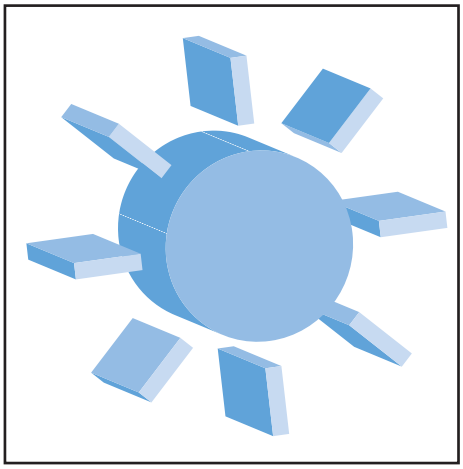
Netzwerke unterliegen einer permanenten Weiterentwicklung. Das technologische Umfeld von Netzwerken befindet sich in einem der intensivsten Änderungsprozesse der letzten 20 Jahre. Das betrifft das Rechenzentrum, neue IT-Architekturen, neue Client-Technologien bis hin zu Unified Communications. Hand in Hand mit dem Bedarf ändern sich Netzwerk-Technologien selber. Neue Standards zur Gestaltung von Netzwerken im Rechenzentrum und im Backbone sind gute Beispiele dafür. Zukunftsorientiertes und wirtschaftlich optimales Design muss dieses Gesamtbild berücksichtigen.

Die ComConsult Sommerschule 2013 analysiert und diskutiert diese Änderungen und ihre Auswirkungen speziell auf die Netzwerk-Infrastrukturen.

Die Veranstalltung bietet Ihnen 5 Tage geballtes IT-Know-how zu folgenden Themenschwerpunkten:

1. Tag: Aktuelle IT-Architekturen und ihre Auswirkung auf Netzwerke

- Entwicklungen der IT-Architekturen und Auswirkungen auf Netzwerke
  Dr. Franz-Joachim Kauffels



- Update Basistechnologie: Übertragungstechnik und Switch-ASICs
  Dr. Franz-Joachim Kauffels
- Wide Area Networks: Stand der Technik
  Dr.-Ing. Behrooz Moayeri

2. Tag: IPv6

- Aktueller Stand - Warten oder Starten?
- Adress-Design
- Sicherheit
  Markus Schaub

3. Tag: LAN-Technologien: aktuelle Entwicklungen

- Fabric-Konzepte im Vergleich
- Quo vadis VLAN-Technik? Overlays und Edge Provisionierung verändern die Netzwerkwelt
- Ein neuer LAN Standard etabliert sich: AVB
- Software-Defined Networking
  Dipl.-Inform. Petra Borwoka-Gatzweiler

4. Tag: RZ-Technik

- Server
- Virtualisierung - Marktstudie Server-Virtualisierung
- Storage
  Dipl.-Inform. Matthias Egerland

5. Tag: Wireless LAN und LTE

- Analyse neuer Übertragungstechniken, Infrastrukturkonzepte und Anwendungen im WLAN
  Dr. Simon Hoff
- LTE: die neue Mobilfunkgeneration
  Dr. Franz-Joachim Kauffels

Top Experten haben das Programm der Sommerschule gestaltet und systematisch die Erfahrungen laufender Projekte und neuester Technologie-Entwicklungen eingearbeitet. Treffen Sie einige der besten Experten, die die deutsche Netzwerk-Landschaft zu bieten hat.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Sommerschule 2013

Ich buche das Intensiv-Seminar
Sommerschule 2013

☐ vom 01.07. - 05.07.13 in Aachen
zum Preis € 2.490,-- netto

☐ Bitte reservieren Sie mir ein Zimmer

vom _____ bis_____ 13

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

_____ Vorname

_____ Nachname

_____ Firma

_____ Telefon/Fax

_____ Straße

_____ PLZ,Ort

_____ eMail

_____ Unterschrift

Programmübersicht - Sommerschule 2013

Montag, der 01.07.13 - Aktuelle IT-Architekturen und ihre Auswirkung auf Netzwerke — 09:00 - 17:00 Uhr

Entwicklungen der IT-Architekturen und Auswirkungen auf Netzwerke
- Dynamische, skalierende Web-Architekturen
- Virtualisierung • Cloud Computing
- BYOD • Speicher-Konsolidierung und –Zentralisierung
- Konzentration und Konsolidierung im WAN/Campus-Bereich

Dr. Franz-Joachim Kauffels, unabhängiger Technologie- und Industrie-Analyst

Update Basistechnologie: Übertragungstechnik und Switch-ASICs
- Status bei 40/100/400 G Ethernet
- 40 GBASE-T und NGBASE-T
- Speicherbasierende Switch-ASICs
- Hybride ASIC-Konstruktionen, Ausblick

Dr. Franz-Joachim Kauffels, unabhängiger Technologie- und Industrie-Analyst

Wide Area Networks: Stand der Technik
- MPLS als internationaler WAN-Standard
- Mit MPLS konkurrierende Plattformen
- Öffentliche Plattform Internet
- WAN-Zugangstechnologien
- WAN-Plattformen: Vergleich
- Unterschiedliches Verhalten von Anwendungen im WAN • Prüfung von Anwendungen auf WAN-Tauglichkeit
- Verkehrsprofile gängiger Anwendungen
- Wie die Übertragungsparameter im Internet zu verbessern sind
- Übertragung von Voice und Video über das WAN

Dr.-Ing. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

Dienstag, der 02.07.13 - IPv6 — 09:00 - 16:30 Uhr

Aktueller Stand - Warten oder Starten?
- Wie reif sind Protokolle, Netzkomponenten und Anwendungen in Bezug auf IPv6?
- In welchen Bereichen sollte man beginnen, in welchen kann man warten?

Adress-Design
- Welche Präfix-Variante ist für welchen Einsatzzweck geeignet?
- Wie sieht ein zukunftssicheres IPv6-Adresskonzept aus?
- DHCP vs. SLAAC vs. privacy Extention vs. manueller Konfiguration: wann setzt man welches Konzept für die Adressverteilung ein?

Sicherheit
- Neue Gefahren durch IPv6 oder alles beim Alten?
- Alte Bekannte in neuem Gewand: wie bekannte - und gelöste - Probleme von IPv4 Implementierungen bei IPv6 wieder auftauchen.
- First-Hop-Security: wie man typischen Angriffen wie bösartigen Router Advertisements begegnet.
- Worauf man bei Betriebssystemen achten muss, weil sich die Default Werte geändert haben.
- Kurzer Ausblick zum aktuellen Stand von Unternehmensfirewalls und deren IPv6-Tauglichkeit

Markus Schaub, ComConsult Study-tv

Mittwoch, der 03.07.13 - LAN-Technologien: aktuelle Entwicklungen — 09:00 - 17:00 Uhr

Fabric-Konzepte im Vergleich
- Merkmale herkömmlicher RZ-Netze
- Bedarf für Fabrics
- Anforderungskriterien für Fabrics
- Standard-Fabric: Multi-Chassis Link Aggregierung
- Standard-Fabric: Layer-2 Multipath
- Aggregierung: modular oder nicht-modular ?
- Proprietäre Fabrics
- SDN Fabrics
- Skalierung von Fabrics
- LAN-SAN Konvergenz
- Design- und Preis-Beispiele
- Bewertung der Konzepte

Quo vadis VLAN-Technik? Overlays und Edge Provisionierung verändern die Netzwerkwelt
- VLANs zur Trennung von Benutzergruppen
- Wo sollten VLANs vermieden werden?
- Handhabung von VLAN Gruppen
- Warum man immer mehr VLANs braucht
- Reduzierung von VLANs: Edge Provisionierung
- Wo endet das RZ-Netz?
- Overlay Protokolle: SPBM
- Overlay Protokolle : VXLAN
- Overlay Protokolle : LISP
- Hat MPLS ausgedient?
- Bewertungsübersicht: Overlay Protokolle
- Neue Perspektive: IETF NVO3

Ein neuer LAN Standard etabliert sich: AVB
- IEEE 802.1BA: Audio- / Video-Bridging
- IEEE 802.1AS: Timing & Synchronization
- IEEE 802.1Qav: Forwarding & Queueing
- IEEE 802.1Qat: Stream Reservation
- Wie passt AVB zu DCB (Data Center Bridging)?

Software-Defined Networking
- Aktuelle Probleme und Motivation für SDN und OpenFlow
- Wie hängen ONF, SDN und OpenFlow zusammen?
- OpenFlow Architektur
- OpenFlow Protokoll und Arbeitsweise
- Versionsunterschiede
- Offene Fragen und Probleme mit OpenFlow
- Markt und Hersteller: Aktuelle Produktbeispiele zu SDN / OpenFlow

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

Donnerstag, der 04.07.13 - RZ-Technik — 09:00 - 17:00 Uhr

Server
- Welche Hardware-Plattformen sind am Markt verfügbar (klassische Server vs. Blades)?
- Wie kann der hohe Bedarf an Netzwerk-Schnittstellen für eine virtualisierte Umgebung durch Hardware-Virtualisierung in Blade-Architekturen befriedigt werden (Physical Functions, Virtual Functions, SR-IOV, etc.)?
- Wie trägt „Fabric I/O Virtualization“ zur Flexibilität bei der Netzanbindung von Blade-Architekturen bei?
- Welche Rollen spielen VEB, VEPA und proprietäre Verfahren?

Virtualisierung

Marktstudie Server-Virtualisierung:
- Aus welchen Komponenten bestehen Citrix XenServer 6.1, Microsoft Hyper-V 2012, VMware vSphere 5.1?
- Welche Lizenzen sind für ein komplexes, repräsentatives Virtualisierungsszenario, das gemeinsam mit den Teilnehmern entwickelt wird, erforderlich?
- Welche Kosten entstehen hierbei?
- Wie ist die Leistungsfähigkeit der Hypervisor zu beurteilen? Wie kann dies in ein neutrales Bewertungsschema überführt werden?
- Wie ist die Wirtschaftlichkeit der 3 Anbieter in dem repräsentativen Szenario zu beurteilen?

Storage
- Welche generellen Anforderungen und Einsatzszenarien gibt es für Speichersysteme? Wie sehen aktuelle Entwicklungen aus?
- Skalierbarkeit: Speicherarchitekturen, traditionelle Speichersysteme, Scale-Out-Systeme, verteilte Systeme.
- Hochverfügbarkeit/Ausfallsicherheit: RAID-Systeme, Redundanzmechanismen, Replikation.
- Storage-Technologien: welche Rollen spielen ThinProvisioning, Deduplizierung, Auto-Tiering?

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

Freitag, der 05.07.13 - Wireless LAN und LTE — 09:00 - 15:30 Uhr

Analyse neuer Übertragungstechniken, Infrastrukturkonzepte und Anwendungen im WLAN
- Stand der Technik mit IEEE 802.11n
- Gigabit WLANs nach IEEE 802.11ac und IEEE 802.11ad
- Auswirkungen auf Ausleuchtung und WLAN-Planung, bzw. WLAN-Migration
- Neue Konzepte mit Beamforming und Multiuser
- In welchem Szenarien macht IEEE 802.11ad Sinn
- Ist das das Ende der normalen Endgeräte-Verkabelung?
- Konsequenzen von Gigabit WLAN auf Controller-Architekturen
- Trennung von Control und Data Plane: Neue Cotroller-Architekturen und Integration von WLAN Controllern und LAN Switches
- Sind IEEE 802.1X und WPA2 noch sicher?
- Umgang mit den Fallstricken bei der Absicherung von WLANs
- BYOD und Co.: Sichere Integration Smartphones und Tablets im WLAN
- Lokalisierung und Profiling von Endgeräten

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

Wireless beyond 11ac
- Eigenheiten des Millimeterwellenbereiches
- IEEE 802.11ad und WiGig
- Stromversorgung von Multi-Gigabit Controllern
- LTE

LTE: die neue Mobilfunkgeneration
- Struktur und Beziehung zu bestehenden Generationen • Beamforming, Diversity und MIMO-OFDMA
- Leistung, Vergleich mit 11m, ac und ad
- Kann LTE WLANs ersetzen, Szenarien, Hybride Ansätze

Dr. Franz-Joachim Kauffels, unabhängiger Technologie- und Industrie-Analyst

ComConsult-Study.tv

Meine persönliche Auswahl:

Lernvideos, die den Unterschied machen!

Wir sind bekannt für die Qualität unserer Vorträge und Referenten. Aber immer mal wieder gelingt eine Präsentation, die außergewöhnlich ist. So außergewöhnlich und bedeutend, dass sie jeder gesehen haben sollte.

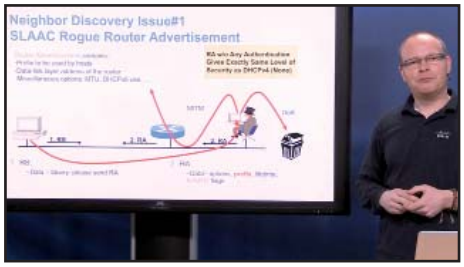
Dies ist meine persönliche – subjektive – Liste unserer außergewöhnlichen Videos.
Ihr Dr. Jürgen Suppan

Konzepte zur Anbindung virtueller Systeme

Das ist ein komplexes Thema. Viele Technologien wurden in den letzten Jahren entwickelt, aber nur wenige setzen sich in der Praxis durch. Gerade bei diesem Thema ist es wichtig, die Nachteile der einzelnen Lösungsansätze zu kennen. Dieses Video liefert beides: Information zu den Alternativen und eine klare Bewertung der Stärken und Schwächen.

Referent: Dipl.-Math. Cornelius Höchel-Winter
Zeit: 00:47:40 gesamt

Einzelpreis: 59,00 € netto
Im Abo: kostenlos

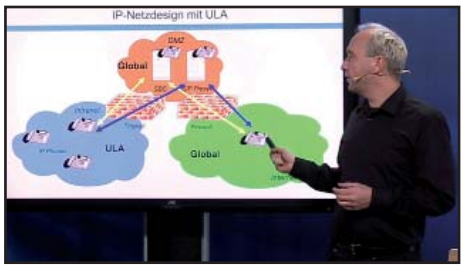


IPv6: Sicherheit am LAN-Zugang

Ein Herstellervideo, aber zu 90% herstellerneutral präsentiert. Sicherheit ist ein Mega-Thema mit IPv6. Vor allem betrifft es auch IPv4-Installationen, da der IPv6-Stack in modernen Betriebssystemen von Hause aus aktiv ist. Dieses Video zeigt beeindruckend, welche Probleme es gibt und wie bekannte und bewährte Mechanismen helfen, diese Sicherheitsprobleme zu lösen.

Referent: Markus Harbeck
Zeit: 00:54:08 gesamt

Einzelpreis: 59,00 € netto
Im Abo: kostenlos



IPv6 Grundlagen

IPv6 wird eines der Themen, die die komplette IT-Landschaft der nächsten Jahre bestimmen werden. Und das Thema ist spannend, da mit wesentlichen Design-Annahmen der Vergangenheit gebrochen wird. Auf einmal haben Endgeräte mehrere Adressen, Router bekommen eine neue Rolle, DHCP wird in Frage gestellt, Broadcasts verschwinden, aber Multicasts bekommen eine neue Bedeutung. Es ist absolut wichtig, die einzelnen Aspekte von IPv6 zu verstehen. Und diese Grundlagenserie von Markus Schaub macht dies in herausragender Weise.

Referent: Markus Schaub
Zeit: 02:24:49 gesamt

Einzelpreis: 59,00 € netto
Im Abo: kostenlos

Besser und erfolgreich präsentieren

Die Fähigkeit Projekte, Produkte und Technologien erfolgreich präsentieren zu können, ist entscheidend für den beruflichen Erfolg. Und in diesem Bereich hat sich in den letzten 5 bis 10 Jahren vieles geändert. Und es gibt klare Rezepte für den Erfolg von Präsentationen. Lars Sudmann ist europäischer Champion von Toastmaster International und seine klaren und für jeden umsetzbaren Empfehlungen sind ein erprobtes Erfolgsrezept. Viele der anerkannten ComConsult-Referenten sind durch seine Schule gegangen.

Referent: Markus Schaub
Zeit: 02:24:49 gesamt

Einzelpreis: 59,00 € netto
Im Abo: kostenlos

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

Schwerpunktthema

Aktuelle Trends im WAN-Bereich

Fortsetzung von Seite 1

Der Autor gehört der Geschäftsleitung der ComConsult Beratung und Planung GmbH an. Er blickt auf langjährige Erfahrungen bei der Konzeption und Ausschreibung von Wide Area Networks zurück.

In den letzten Jahren hat die zunehmende Videoübertragung zu diesem Trend wesentlich beigetragen. Sowohl Videokonferenzen als auch Video Streaming, Videoüberwachung und die Einbindung von Videoinhalten in Dokumenten und Anwendungen werden zunehmend auch über WAN genutzt. Beispiel Videokonferenzen: Über viele Jahre ist es in vielen Unternehmen nicht gelungen, die Amortisierung von Videokonferenzanlagen durch Einsparung von Reisekosten und Reisezeiten als Türöffner für die stärkere Nutzung von Videokonferenzen zu nutzen. In den letzten Jahren hat jedoch ein anderer Faktor die Nutzung von Collaboration Tools inkl. Video geradezu erzwungen, nämlich der Druck, Vorhaben, Projekte, Abstimmungen und andere Aufgaben in wesentlich kürzeren Fristen erledigen zu müssen. Eine Telefon-, Web- oder Videokonferenz ist wesentlich schneller geplant und durchgeführt als ein Präsenzmeeting.

Die Folge für standortübergreifende Netze ist klar: mehr übertragenes Volumen. Allerdings ist in diesem Zusammenhang zu berücksichtigen, dass im Zusammenhang mit Collaboration Tools das Gesetz von Metcalfe gilt: der Wert einer Kommunikationslösung steigt quadratisch mit der Anzahl der darüber erreichbaren Benutzer. Angewandt auf Collaboration Tools inkl. Web- und Videokonferenzen bedeutet dies, dass der Wert der Lösungen, mit denen man auch über Firmengrenzen hinweg kooperieren kann, den Wert rein unternehmensinterner Lösungen bei weitem übersteigt. Dies bedeutet: In den nächsten Jahren wird die Videoübertragung über den Internetanschluss der Unternehmen wesentlich stärker zunehmen als die Videoübertragung über das private WAN.

Local Internet Break-out

Mittlerweile ist es für den Autor keine Überraschung mehr festzustellen, dass der Internet-Verkehr in vielen privaten WANs den größten Volumenanteil ausmacht. Insbesondere die Bestrebung, die Zahl der Administrationspunkte für Perimetersicherheit zu minimieren, war die Motivation dafür, in den 2000er Jahren den Internet-Verkehr auf zentrale Zugänge zum weltweiten öffentlichen Netz zu konzentrieren. (siehe Abbildung 1)

Die Zentralisierung des Internetzugangs half, den Aufwand für die Administration von Firewalls, Proxies und sonstigen Elementen der Infrastruktursicherheit zu optimieren, führt jedoch mittlerweile zu einigen nicht zu übersehenden Nachteilen:

- Insbesondere in global agierenden Unternehmen kann die Zentralisierung des Internetzugangs bedeuten, dass bedingt durch lange Paketlaufzeiten von einem Benutzerstandort zum weit entfernten RZ und von dort zu wiederum weit entfernten Zielen im Internet die Antwortzeiten beim ausgehenden Web-

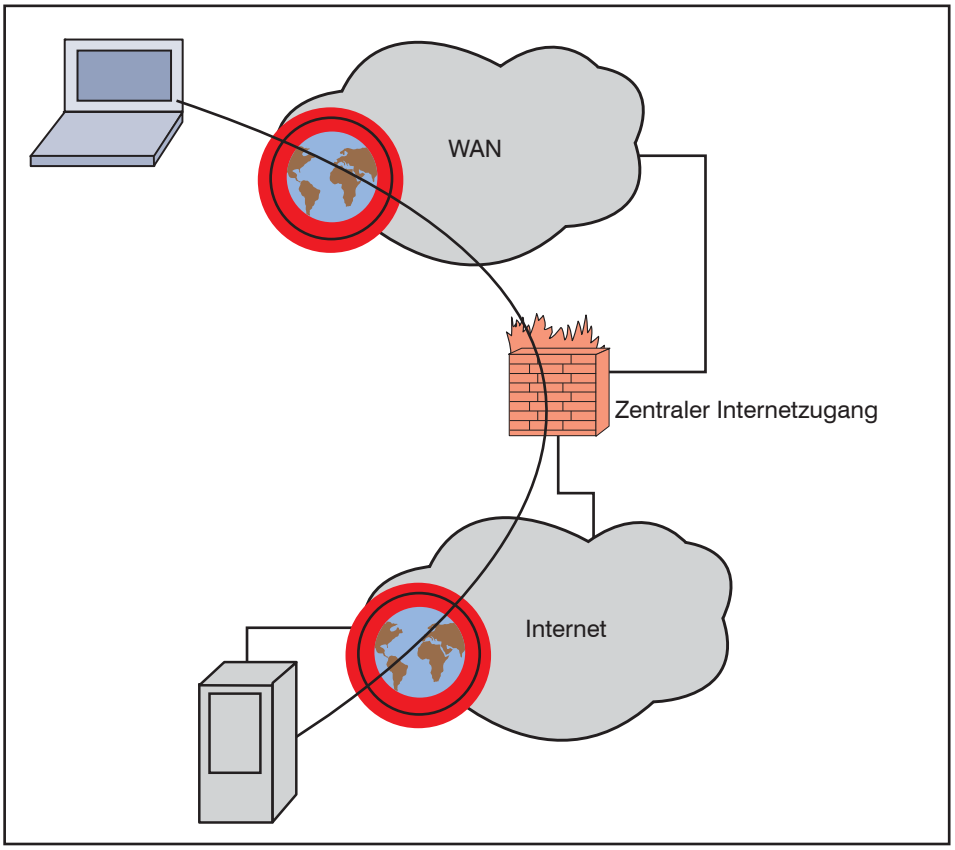


Abbildung 1: Zentraler Internetzugang

zugriff wesentlich länger sind als Benutzer zum Beispiel bei der Internetnutzung zuhause gewohnt sind. Dabei kann die Internetnutzung im Zeitalter öffentlicher Clouds für viele Unternehmen geschäftskritisch oder zumindest geschäftsrelevant sein.

- Der im Vergleich zu anderen Anwendungen überdurchschnittlich steigende Webverkehr belastet beim zentralen Zugriff auf das Internet das private WAN immer stärker.

- Die Regionalisierung von Webinhalten externer Anbieter (Anpassungen für Sprache, Location Services) wird durch die Umleitung des Zugriffs auf das weit entfernte RZ erschwert.

Daher ist ein immer häufiger festgestellter Trend insbesondere in weltweit agierenden Unternehmen die Dezentralisierung von Internetzugängen. Sogenannte Local Internet Break-outs werden zunehmend entweder für alle Standorte oder zumindest für lokale Gruppen von Standorten (zum Beispiel für nationale Gesellschaften) vorgesehen.

Zunehmende Bedeutung von lokalen Appliances

Local Internet Break-outs erfordern dezentrale Sicherheitskomponenten, wie aus der Abbildung 2 hervorgeht. Die Reduzierung der IT-Ausrüstung der dezentralen Standorte auf Arbeitsplatzendgeräte, Drucker und WAN Router ist dann nicht mehr möglich. Mindestens eine Sicherheitsinstanz ist an jedem direkt mit dem Internet verbundenen Standort erforderlich.

Die Abneigung zentraler IT-Abteilungen gegen dezentrale Ausrüstung, die installiert, überwacht und gewartet werden muss, kann relativiert werden, wenn Produkte eingesetzt werden, die trotz dezentraler Installation ein zentrales Management und die Verteilung einheitlicher Richtlinien erlauben.

Eine bereits seit Jahren eingesetzte Kategorie dezentraler Ausrüstung bilden WAN Optimisation Controller (WOCs). Die ursprüngliche Motivation für den Einsatz von WOCs war, wie der Name schon aussagt, die Optimierung der Verkehrsströme und deren Anpassung an WAN-Bedingungen. Diese Optimierung besteht im Wesentlichen darin, die über das WAN übertragene Datenmenge zu reduzieren (geläufige Bezeichnungen dafür sind Kompression bzw. Deduplizierung) und die Zahl der WAN-Durchläufe für einen bestimmten Anwendungsschritt zu minimieren. (siehe Abbildung 3).

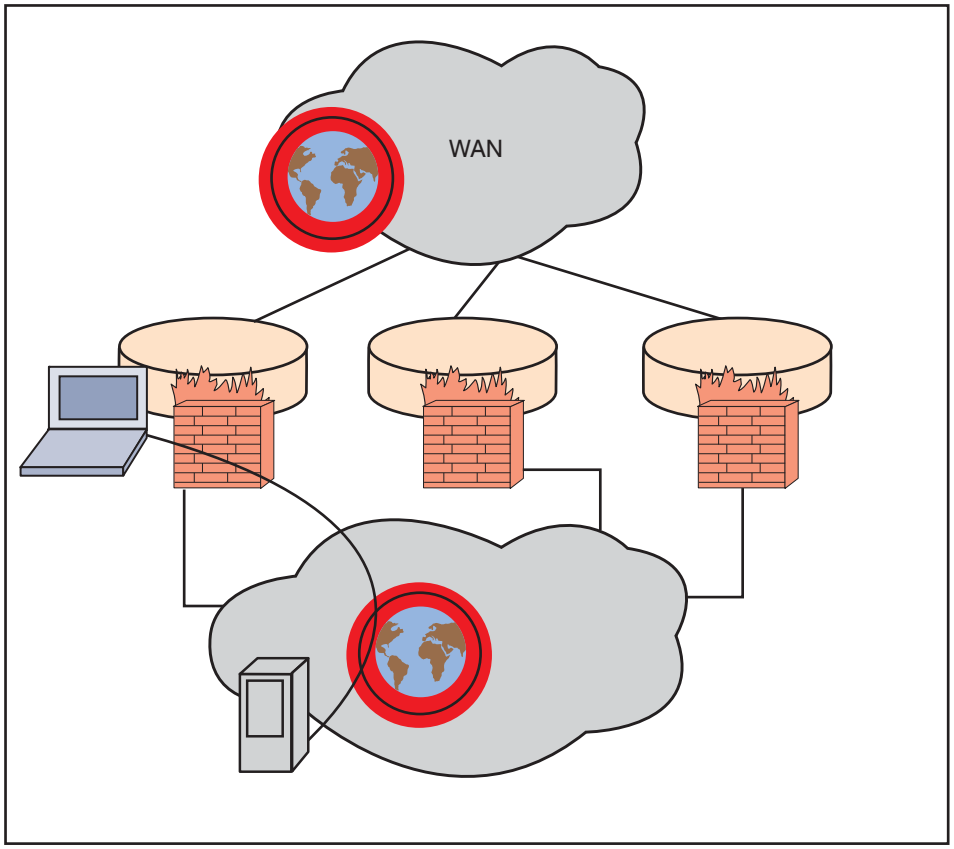


Abbildung 2: Dezentraler Internetzugang

Somit bekommt der WAN Router am dezentralen Standort Gesellschaft. Wenn aber eine lokale Intelligenz in Gestalt des WOCs pro Standort erforderlich ist, kann die zugehörige Appliance auch andere Aufgaben übernehmen: Name Server, DHCP-Server, Print Server, Domain Controller etc. Auch Sicherheitsfunktionen können die Appliance bereichern und damit die pro Standort erforderliche Hardware minimieren, wenn die Standorte mit lokalen Internetanschlüssen versehen werden sollen.

Virtuelle Appliances

Die ganze Netzbranche spricht über Software Defined Networking (SDN). SDN soll die Kosten für Anschaffung und Betrieb von Netzkomponenten reduzieren und ihre Flexibilität erhöhen. Auch Appliances für dezentrale Standorte können von Spezialhardware auf Standardhardware umgestellt werden. Appliances werden damit virtualisiert und können dadurch von den Vorteilen der Virtualisierung profitieren:

- Standard-Hardware lässt sich wesentlich einfacher warten und pflegen. Ein x86-Rechner kann auch an dezentralen Standorten binnen kurzer Zeit installiert bzw. ersetzt werden.

- Hochverfügbarkeitslösungen lassen sich mit virtuellen Appliances wesentlich einfacher realisieren. In der Regel können für die Realisierung von Hochverfügbarkeit die Standardverfahren der Virtualisierungslösung genutzt werden.

- Patch Management und Updates sind mit virtuellen Appliances wesentlich einfacher zu gestalten.

Kurzum, dieselben Vorteile wie für virtuelle Serverfarmen gelten auch für virtuelle Appliances, seien sie virtualisierte Firewalls, WOCs oder Router.

Internet Overlays

Das Konzept von Internet Overlays ist nichts Neues und geht in die Zeit um die Jahrtausendwende zurück. Mit der Internet-Wirtschaft entstand ein Wettbewerb um die schnellsten Webseiten. Webinhalte gelangen am schnellsten zum Benutzer, wenn sie schon vorher in die Nähe des Benutzers verlagert worden sind. (siehe Abbildung 4)

Die in der Abbildung 4 dargestellte Verkürzung des Wegs des Benutzers zu den Webinhalten ist prinzipiell mit der WAN-Optimierung vergleichbar. Auch die WAN-Optimierung basiert zum Teil auf die Verkürzung des Weges zwischen Benutzern und Inhalten.

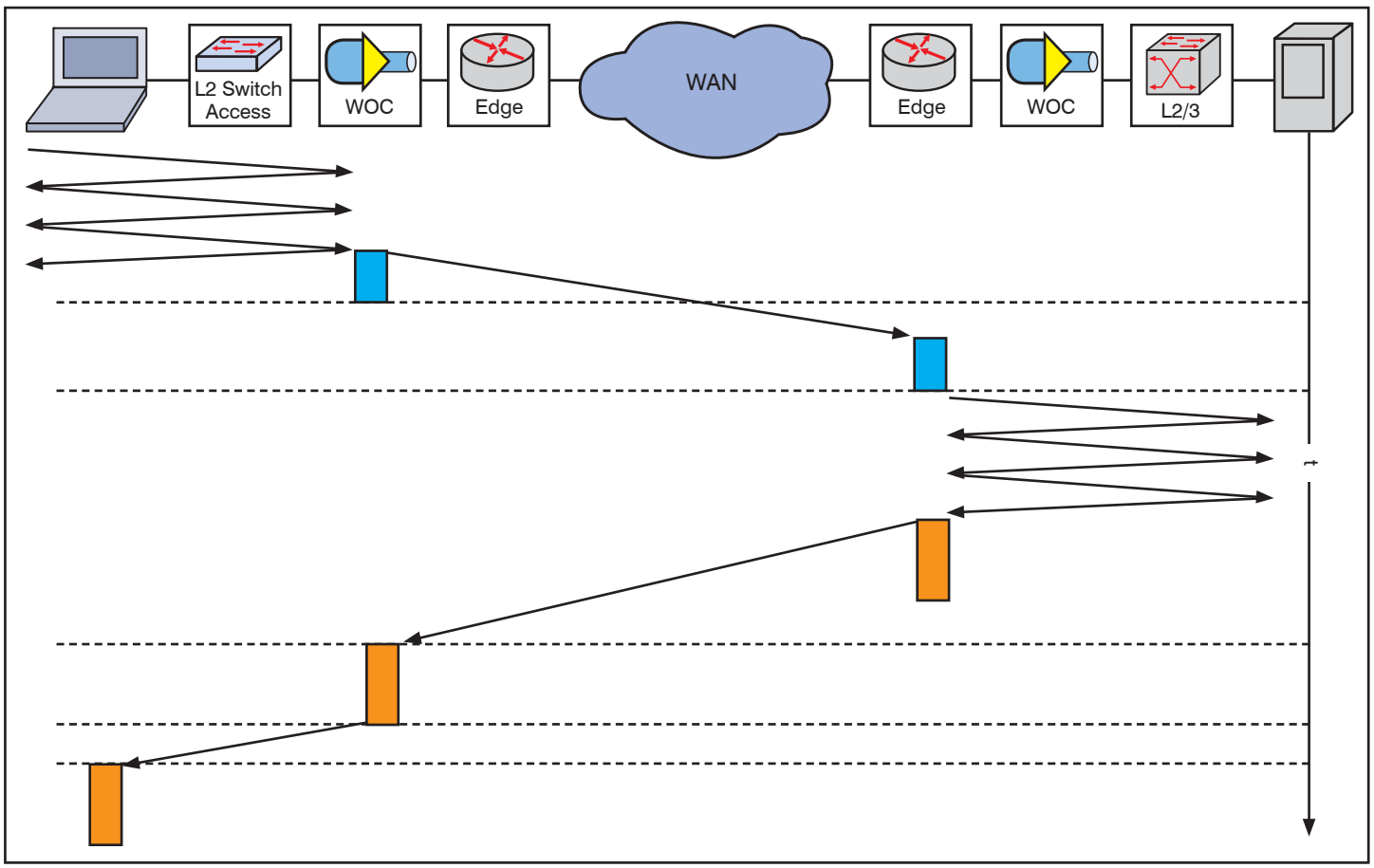


Abbildung 3: Reduzierung der Zahl der WAN-Durchläufe

Der Mechanismus für die Verlagerung oder vielmehr die Replikation der Daten in Richtung Benutzer kann zum Beispiel darin bestehen, dass im Domain Name System (DNS) verschiedene Einträge für denselben Webserver geführt und je nach Ursprung der DNS Requests die Clients zu den ihnen am nächsten stehenden Server gelotst werden.

Das über zehn Jahre alte Prinzip kann nun so erweitert werden, dass nicht nur weltweit verteilte Kunden von einem schnellen Webzugriff profitieren, sondern mittels Internet Overlays auch die weltweit verteilten Standorte und Mitarbeiter eines Unternehmens in den Genuss kürzerer Antwortzeiten kommen. Zum Beispiel können unternehmensinterne Anwendungen auf der Basis von HTTPS im Internet bereitgestellt werden. Für die Sicherheit dieser Applikationen können eine starke Benutzerauthentisierung beispielsweise mittels Tokens und die verschlüsselte Übertragung sorgen, für kurze Antwortzeiten Internet Overlays. Anbieter solcher Dienste verfügen über eine global verteilte Infrastruktur.

Multi-Provider-Umgebungen

Aus verschiedenen Gründen entscheidet sich eine Reihe von Unternehmen dafür, für standortübergreifende Kommunikation die Dienste von mehr als nur von einem Provider zu nutzen. Üblich ist zum Beispiel ein Dual Homing des Internetanschlusses bei zwei Providern zu Zwecken der Ausfallsicherheit, aber auch der Lastverteilung.

Multi-Provider-Umgebungen sind auch im WAN-Bereich durchaus gängig. Das liegt vor allem daran, dass ein einzelner Provider nicht in allen Weltregionen in Sachen Wirtschaftlichkeit, schnelle Bereitstellung von Diensten, Ausfallsicherheit und kurzen Wegen zu Standorten der Kunden

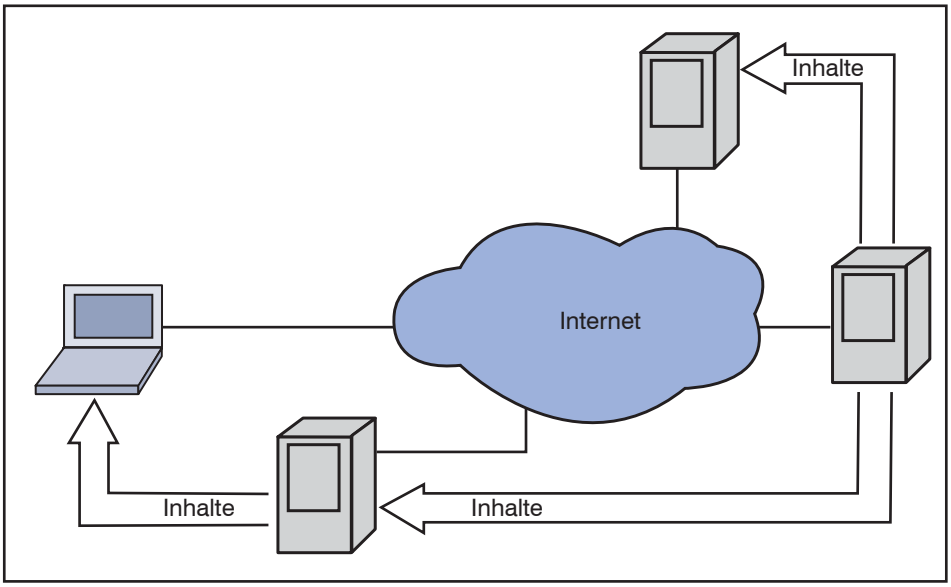


Abbildung 4: Verlagerung der Inhalte in die Nähe der Benutzer

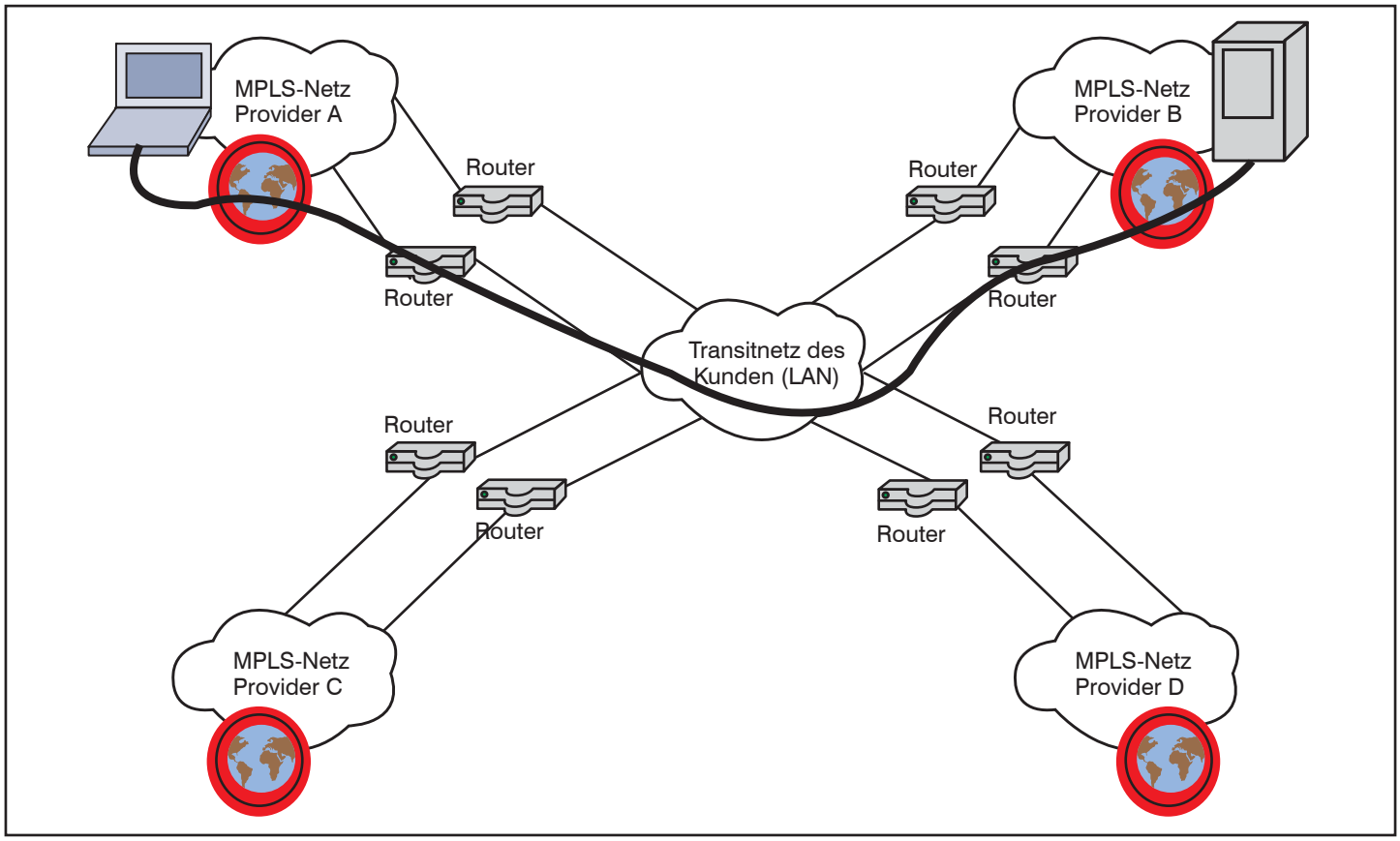


Abbildung 5: Multi-Provider-WAN

führend sein kann. Alle Provider haben regionale Schwerpunkte und entsprechend Schwächen in anderen Regionen.

So wurden in den letzten zehn Jahren viele private WANs unter Nutzung der Plattformen mehrerer Provider aufgebaut, wie anhand eines Beispiels in der Abbildung 5 dargestellt. In diesem Beispiel nutzt das Unternehmen die Dienste von vier Providern, zu deren Plattformen an einem Standort des Kunden (typischerweise im RZ) Zugänge bestehen.

Wie aus der Abbildung 5 hervorgeht, hat die dargestellte Multi-Provider-Lösung den Nachteil, dass die Kommunikation zwischen zwei Kundenstandorten in ungünstigen Fällen zweimal über ein weltweites Netz (des Providers A und des Providers B) geführt wird und somit unter langen Paketlaufzeiten leiden kann.

Unterhalten die Provider aber sogenannte Network-to-Network Interfaces (NNIs), dann erübrigen sich ungünstige Wege über Standorte des Kunden. Somit gehört die Prüfung der Verfügbarkeit und Nutzbarkeit von NNIs zwischen Providern mittlerweile zum WAN-Anforderungskatalog vieler Firmen, die für WAN eine Multi-Provider-Lösung in Erwägung ziehen.

Differenzierung zwischen nationalen und internationalen WAN-Verfahren

Eine Besonderheit des WAN-Marktes (anders als viele andere Marktsegmente der IT) ist die Differenzierung zwischen WAN-Verfahren, die in globalen und internationalen Netzen eingesetzt werden, und solchen, die nur nationale Relevanz haben. Länder unterscheiden sich in der Historie der Telekommunikation, in Regulierungsrichtlinien und in ihren geografischen Randbedingungen. Der WAN-Markt in Deutschland ist ein völlig anderer als der in den fast dreißig Mal größeren USA. Netze, die von den Providern in Deutschland unter relativ niedrigem Aufwand eingeführt werden können, scheitern in einem riesigen Land wie den USA möglicherweise an den Dimensionen des Landes.

Andererseits brauchen viele Unternehmen internationale WAN-Dienste. In den letzten 15 Jahren haben sich das Internet und MPLS klar als DIE beiden Plattformen für internationale Netze durchgesetzt. Eine dritte international weit verbreitete WAN-Technologie wird sich nicht kurzfristig durchsetzen.

Die Situation in nationalen WAN-Märkten ist jedoch eine andere. Zum Beispiel muss MPLS nicht die Basis jedes nationalen WAN in Deutschland sein. Viele Unternehmen nutzen noch WAN-Dienste auf der Basis von älteren Provider-Plattformen wie SDH (Synchrone Digitale Hierarchie). Dazu zählen nicht nur die klassischen Festverbindungen, sondern auch Ethernet über SDH, entweder in Form von Punkt-zu-Punkt-Verbindungen oder als Any-to-Any-Dienst mit Ethernet-Zugängen. In letzter Zeit sind auch modernere Dienste auf der Basis des Optical Transport Network (OTN) hinzugekommen, das als Nachfolger von SDH mit wesentlich höherer Leistungsfähigkeit gilt.

Access-Diversifizierung

Zu den nationalen Besonderheiten gehört der Access-Bereich. Je nach dem, wie sich die Telekommunikations-, Mobilfunk-, TV-Netz- und Internet-Access-Märkte in einem Land in den letzten Jahren entwickelt haben, sind dort mehr oder weniger WAN-Zugangstechnologien verfügbar. Daher ist die jeweilige Situation im Access-Bereich sehr landesspezifisch. Der Diversifizierungsgrad von WAN-Access-Verfahren (auch als Local Loop oder letzte Meile bekannt) unterscheidet sich von Land zu Land sehr stark.

In Deutschland dominiert zum Beispiel der Zugangstyp Digital Subscriber Line

(DSL) den Verbrauchermarkt. Im Zuge der „Consumerisation“ profitierten in den letzten Jahren viele Unternehmen von DSL-Angeboten der Provider, die im Vergleich mit den klassischen Festverbindungen wesentlich günstiger sind (der DSL-Markt ist sehr groß und damit die einzelne Leitung relativ günstig). Daher hat in Deutschland (aber natürlich nicht nur hier) in den letzten Jahren die Zahl privater WANs mit DSL-Zugängen stark zugenommen. Dies gilt sowohl für asymmetrische als auch für symmetrische DSL-Varianten.

Aber neben DSL haben hier auch andere Access-Technologien signifikante Anteile am WAN-Markt. Aktuelle Erhebungen bei unseren Kunden zeigen zum Beispiel, dass rund 50 % der Standorte über Lichtwellenleiter (LWL) angebunden sind (unsere Kunden sind jedoch für den Gesamtmarkt nicht unbedingt repräsentativ, weil es sich bei unseren Kunden überwiegend um große und mittlere Unternehmen handelt; der Anteil von LWL am deutschen Gesamtmarkt für WAN Access dürfte wesentlich kleiner sein). Eine zunehmende Zahl von Gebäuden und Liegenschaften kann LWL-Zugänge nutzen, verbunden mit wesentlich höherer Skalierbarkeit der Bitrate als mit DSL möglich (Angebote auf der Basis von Kupferleitungen hören bei ein- bis zweistelligen Megabit-Werten auf, während es für LWL bereits Standardangebote bis 10 Gbit/s gibt).

Aber LWL ist nicht die einzige Alternative zu DSL. Nach wie vor sind viele Unternehmensstandorte über (immer symmetrische) Standardfestverbindungen angebunden, zum Beispiel über Leitungen des Typs E1 mit 2 Mbit/s. Dagegen sind Anbindungen mit E3 (34 Mbit/s) in der Regel mittlerweile aus dem Angebot der Provider verschwunden bzw. wirtschaftlich uninteressant.

Ethernet kommt auf der letzten Meile immer häufiger zum Einsatz, entweder auf Kupfer- oder auf LWL-Basis, und zwar unabhängig davon, welche Technologie die Backbone-Plattform nutzt, mit denen die Unternehmensstandorte über Ethernet verbunden werden. Als Schnittstelle zwischen dem Kunden und dem Provider wird in Deutschland ohnehin meistens Ethernet genutzt, sei es weil die Access-Leitung selbst auf Ethernet basiert oder weil eine am Standort des Kunden eingesetzte Komponente des Providers (Customer Premises Equipment, CPE) als Schnittstelle zum Kundennetz Ethernet Interfaces bereit stellt.

Layer-2-WAN

Ebenfalls zu den nationalen Besonderheiten gehört der Verbreitungsgrad von Layer-2-WAN. Der Autor gehört nicht zu den Verfechtern der „freien Fahrt für freie VMs“ über das WAN, weil ungehemmt bewegliche VMs (Virtuelle Maschinen) nur dann sinnvoll sind, wenn nicht nur die Serverinstanzen, sondern auch die Daten unverändert überall verfügbar sind. Insbesondere über WAN-Entfernungen ist es aber schwierig, alle Datenkopien synchron zu halten[1]. Insofern ist die Motivation, mittels Layer-2-WAN-Strukturen die Beweglichkeit von VMs auch im WAN zu ermöglichen, zu relativieren. Aber dies ist nicht die einzige Motivation für Layer-2-WANs. Einige Unternehmen legen zum Beispiel Wert auf ein aus Layer-3-Sicht transparentes WAN, damit sie die Layer-3-Hoheit ausschließlich bei sich behalten und keine statischen Routen oder Routing-Protokolle als Schnittstellen zum Provider unterhalten müssen, was eine potenzielle Quelle von Fehlern oder Sicherheitsproblemen sein kann.

Die technologische Basis für Layer-2-WAN kann unterschiedlich sein. Hier einige Varianten:

- Der Kunde mietet nur Punkt-zu-Punkt-Verbindungen beim Provider und gestaltet die WAN-Topologie selbst. Die Punkt-zu-Punkt-Verbindungen können Ethernet- oder andere Verbindungen (zum Beispiel E1) sein und auf verschiedenen Plattformen basieren (SDH, OTN, Dark Fiber, Ethernet over MPLS, Richtfunk etc.)

- Virtual Private LAN Service (VPLS) setzt auf die MPLS-Plattform des Providers auf. VPLS ist eine Mehrpunkt-any-any-Plattform auf Layer-2-Basis.

- Mehrpunkt-Ethernet ist mittlerweile auch über neue Plattformen wie OTN möglich.

Insgesamt ist festzustellen, dass die meisten Unternehmen zwischen WAN und RZ-RZ-Kopplung unterscheiden. Während über letztere Layer-2- und in der Regel auch SAN-Verbindungen realisiert werden, bleibt man meistens bei einem Layer-3-WAN.

Hybrid-WAN

Auf nur eine WAN-Technologie zu setzen kann nachteilig sein. Beispielsweise kann es in vielen Regionen der Welt Monate dauern, bis ein Provider an einem Standort den Zugang zu seiner MPLS-Plattform realisiert. Solche Verzögerungen sind für immer kurzfristiger entscheidende und agierende Unternehmen nicht akzeptabel. Auch können die Kosten für MPLS das WAN-Budget vieler Unternehmen sprengen.

Daher werden internationale WAN oft als Hybrid-WAN mit einer Mischung aus MPLS und Internet (den beiden weltweit etablierten WAN-Plattformen) aufgebaut. Die klassische Ausprägung eines Hybrid-WAN ist die MPLS-Plattform eines Providers zuzüglich eines auf IPsec basierenden Virtual Private Network (VPN) über das Internet. Viele Unternehmen haben Letzteres selbst aufgebaut und betrieben. Dies kann jedoch aus verschiedenen Gründen überholt sein:

- Einige Unternehmen sind überfordert, wenn es um die logistischen und rechtlichen Herausforderungen des Betriebs von Internet-VPN insbesondere in den Ländern geht, die restriktiv mit verschlüsselten VPNs bzw. mit Internet-Zugängen außerhalb des nationalen Hoheitsbereichs umgehen (zum Beispiel könnten sonst die chinesischen Mitarbeiter eines deutschen Unternehmens über das Unternehmensnetz einen nicht durch den chinesischen Staat regulierten, über Deutschland realisierten Internetanschluss nutzen). Provider haben dagegen etablierte Prozesse für solche Aufgaben, die sie für mehrere Firmen wahrnehmen.

- Zentrale VPN-Zugänge wirken sich hinsichtlich der Laufzeiten negativ aus, wenn das VPN die typische Hub&Spoke-Topologie nutzt.

- An entfernten Standorten gibt es oft keine geeigneten Mitarbeiter, die Arbeiten im Zusammenhang mit den VPN Appliances übernehmen könnten.

Daher bieten einige Provider hybride WAN-Lösungen an, in denen Kombinationen von MPLS und Internet-VPN eingesetzt werden. Diese Provider können in der Regel schneller die Verbindung zu einem neuen Standort herstellen, weil sie die langen Bereitstellungszeiten für MPLS durch einen Internet-basierenden Dienst überbrücken können. Ferner verfügen Provider über verteilte Standorte, sodass die Laufzeiten zwischen zwei Punkten in einem hybriden WAN verkürzt werden können.

XaaS

Zu den RZ-spezifischen Cloud-Diensten wie Software as a Service (SaaS) und Infrastructure as a Service (IaaS) sind in letzter Zeit weitere Dienste der Kategorie XaaS hinzu gekommen, die insbesondere auf die Bedienung verteilter Standorte von Unternehmen abzielen.

Ein Beispiel ist Security as a Service. Werden verteilte Standorte direkt an das Inter-

[1] siehe Artikel von Moayeri, Behrooz: Synchron oder asynchron? Insider RZ-Magazin, ComConsult Research, April 2013.

net angeschlossen, muss die IT an diesen Standorten vor den Gefahren aus dem Internet geschützt werden. Werden selbst beschaffte und betriebene Sicherheitskomponenten wie Web Security Gateways (Kombination aus Content Filter, Proxy, Schutz vor schadenstiftender Software und anderen Sicherheitskomponenten) eingesetzt, ist dies in der Regel mit hohen Kosten für Beschaffung und Betrieb verbunden. Mittlerweile kann Web Security auch als externer Service eingekauft werden. Local Internet Break-out dient, wie der Name bereits andeutet, vor allem dem ausgehenden Internet-Zugriff. Die Netzkomponente an einem Standort kann zum Beispiel sämtliche Kommunikation über das Internet bis auf zwei Ausnahmen unterbinden: VPN-Verbindung zu den zentralen unternehmensinternen IT-Ressourcen und Webzugriff über die Web Security Cloud. Sämtlicher ausgehender Internetzugriff aus diesem Standort wird dann statt über das firmeninterne VPN über die Web Security Cloud geführt.

Auch Network as a Service (NaaS) wird neuerdings als Begriff verwendet. Darunter wird in der Regel ein Dienst verstanden, in dessen Mittelpunkt ein Netz aus verteilten Points of Presence (PoPs) steht. Diese PoPs vermitteln nicht nur die schnelle und zuverlässige Paketübertragung zu jedem anderen verbunden PoP, sondern darüber hinaus direkte Internet-Zugänge zur Aufnahme der Verbindungen zu Standorten, die in kurzer Zeit vernetzt werden können, indem sie einen lokalen Standardanschluss an das Internet erhalten. Ferner kann ein PoP zum Beispiel typische WAN-nahe Funktionen wie WOC aufnehmen.

RZ-Replikation über WAN

Im Zusammenhang mit Layer-2-WANs wurde bereits erwähnt, dass die Synchronisation von Daten über WAN-Entfernungen nicht immer möglich ist. In diesen Fällen bietet sich eine asynchrone Replikation an, die bei Ausfällen des aktiven RZ-Standorts zwar nicht ohne Datenverluste und Ausfallzeiten, aber mit einem begrenzten Maß an Datenverlusten und Ausfallzeiten einen Weiterbetrieb der IT im Backup-RZ ermöglicht. Regelmäßige asynchrone Replikationen von Daten sind auch über WAN-typische Entfernungen realisierbar. Somit können überregionale oder gar internationale RZ-Backup-Konzepte realisiert werden.

Für das „Überleben“ eines Katastrophenszenarios (Disaster Recovery) im Zusammenhang mit einem RZ müssen drei Bedingungen erfüllt werden:

- An einem anderen, vom Ausfall nicht betroffenen Standort sind die erforderlichen Rechen- und Speicherressourcen verfügbar oder können binnen der tolerierbaren Ausfallzeit bereit gestellt werden.
- Der Backup-Standort ist über eine WAN-Plattform (MPLS, Internet etc.) mit dem RZ-Hauptstandort und mit Standorten und Netzen der betroffenen Benutzer verbunden.
- Die Daten werden in der geforderten Regelmäßigkeit vom Haupt- zum Backupstandort repliziert.

Ein solches Konzept kommt ohne besondere RZ-Kopplung aus und benötigt nur einen Standard-WAN-Dienst. Es ist aus Netzsicht nur dafür zu sorgen, dass der Backup-Standort mit der ausreichenden Kapazität an das WAN angeschlossen wird.

Zusammenfassung

Die in diesem Beitrag behandelten Trends sind wie folgt zusammenzufassen:

- Der standortübergreifende Verkehr steigt weiter an. Insbesondere ist mit der überdurchschnittlichen Zunahme des Volumens der Internet-Kommunikation zu rechnen.
- Das Pendel der Zentralisierung des Internetzugangs schlägt bei immer mehr Unternehmen zurück. Viele Standorte brauchen Local Internet Break-out, vor allem für ausgehenden Webzugriff.
- Appliances für WAN-Optimierung, Security und andere lokale Dienste gewinnen an Bedeutung.
- Die Virtualisierung umfasst auch WAN-Router und andere Appliances.
- Mit Internet Overlays können Antwortzeiten von Anwendungen verbessert werden.
- Multi-Provider-Umgebungen erfordern Network-to-Network Interfaces zwischen Providern, deren Verfügbarkeit in der Beschaffung von WAN-Diensten zu beachten ist.
- International sind Internet und MPLS de facto Standards für WAN. National kommen andere Varianten wie Ethernet-Dienste hinzu.
- Zumindest in Deutschland sind mittlerweile verschiedene WAN-Access-Verfahren auf der Basis von Kupfer, LWL und drahtlosen Verbindungen verfügbar.
- Layer-2-WAN haben sich gegen Layer-3-WAN nicht durchgesetzt.
- Provider bieten mittlerweile hybride Lösungen für WAN an, die meistens aus der Kombination einer privaten Plattform (in der Regel MPLS) mit dem Internet bestehen.
- Verschiedene Dienste wie WAN-Optimierung und Web Security sind mittlerweile als Service aus der Cloud verfügbar.
- Es ist mit der Zunahme der RZ-Replikation über das WAN zu rechnen.

Standpunkt Sicherheit

Sprengstoff im Internet of Things

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

Im sogenannten Internet of Things erfassen Dinge (Things) – nicht Menschen wie im „Internet of Humans" – Informationen, sind per IP vernetzt und stellen Informationen für andere Dinge oder Menschen zur Verfügung. Dahinter stecken natürlich unterschiedlichste Systeme und Anwendungen.

Beispiele sind Sensoren und Steuerungen in der Automatisierungs- und Gebäudetechnik oder aber das vernetzte Fahrzeug, das mit anderen Fahrzeugen (Car2Car) oder mit der Infrastruktur (Car2Infrastructure) kommuniziert[1]. Über drahtlose Kommunikationstechniken werden dabei Informationen über das Umfeld des Fahrzeugs ermittelt, um z.B. das Sichtfeld des Fahrers zu erhöhen („Vorsicht: Glatteis hinter der nächsten Kurve") oder sogar autonomes Fahren (beispielsweise Kolonnenfahrt / Platooning von mehreren Fahrzeugen, bei denen der erste Fahrer der Kolonne lenkt und die anderen Fahrer sich anderweitig beschäftigen können) zu unterstützen.

Dass solche Anwendungen vernetzter Fahrzeuge keine akademischen Hirngespinste mehr sind, sondern inzwischen sogar praxistauglich sind, haben die Ergebnisse der Arbeiten der verschiedenen Forschungs- und Entwicklungsabteilungen der Automobilhersteller (und auch Google) in den letzten zwei Jahren eindrucksvoll gezeigt[2].

Erwähnenswert ist, dass man weltweit seit mehr als 20 Jahren in der Verkehrs-Telematik an der Vernetzung von Fahrzeugen und deren Anwendung arbeitet[3]. Dabei sind durchaus Anwendungen entstanden, die längst Gebrauchsgegenstände geworden sind, die wir kaum noch bewusst wahrnehmen, wie die dynamische Zielführung. Nur hatten vor 20 Jahren höchstens kühne Visionäre mit dem Internet of

Things auch nur ansatzweise gerechnet. Dasselbe gilt allerdings auch für die Feststellung, dass IT-Innovation heutzutage vom Consumer-Markt getrieben wird und wir munter Consumer-Produkte in der IT (und im Internet of Things) verbauen.

Nehmen wir etwa an, dass in Fahrzeugen der nächsten Zukunft (oder sogar schon heute) als Schnittstelle zum Menschen konventionelle Tablets mit iOS, Android oder Windows verbaut werden. Nehmen wir außerdem noch an, dass über Smartphones gewisse elementare Funktionen eines Fahrzeugs per Bluetooth, ZigBee, WLAN oder Mobilfunk gesteuert werden könnten, wie z.B. Vorheizen im Winter, Auf- und Abschließen[4] des Fahrzeugs. Dann ist es nicht abwegig, dass solche Standardplattformen sogar als Basis für einen Bord-Computer dienen könnten (wie wäre es mit „Realtime Android" oder „Embedded Android").

Es ist nun keine Frage, ob oder wann das Internet of Things sich materialisiert, es ist längst da, und es ist leider auch gefährlich. Erstens vererben sich auf das Internet of Things auf triviale Weise viele der Gefahren, die wir im Internet of Humans kennen. Einem Virus ist es prinzipiell egal, ob ein Android Tablet in der Hand eines Menschen liegt oder im Armaturen-Brett eines Fahrzeugs verbaut ist. Zweitens ist das schadenstiftende Potential von Malware im Internet of Things von besonderer Qualität. Was passiert bei systematischer Fälschung von Sensorwerten, was passiert bei zielgerichteter Sabotage von Standard-IT-Komponenten im Internet of Things, z.B. in einem Fahrzeug? Bei Malware haben wir oft noch den Menschen, der eine ungewöhnliche Anfrage aus dem Internet sinnvollerweise nicht beantwortet. Würde auch ein Thing diese Intelligenz haben? Hier hat Malware eine ganz neue Dimension bekommen! Haben wir aus Stuxnet und Co. für das Internet of Things gelernt?

Der Ruf nach striktester Trennung von allen kritischen Systemen im Internet of Things wird dann schnell laut, und wenn wir ehrlich sind, wird er höchstens Firewall-Hersteller freuen. Wir müssen uns hier eher vergegenwärtigen, dass sich nicht nur Gefahren vom Internet of Humans auf das Internet of Things vererben. Es können und müssen sich auch die Sicherheitsmaßnahmen vererben. Die Hersteller der Things im Internet of Things sind hier in der Verantwortung. Hier geht es um so (scheinbar) triviale Dinge wie den Eigenschutz von Things. Wir sind es gewohnt, dass PCs und Server, die über das Internet kommunizieren, auf eine angemessene Art gehärtet werden müssen und dass auf Ebene der Anwendung (und damit auch der Softwareentwicklung) gewisse Regeln einzuhalten sind, um nicht Angriffen ausgeliefert zu werden. Das sollte auch für Things im Internet of Things der Fall sein. Es ist leider nur anzunehmen, dass die Entwickler und Nutzer der Things diese Themen schon wieder bis zum bösen Erwachen verdrängen werden.

Es gibt außerdem Aspekte, die für das Internet of Things eine besondere Bedeutung haben. Hierzu gehören speziell sichere Identitäten im Netz. Spoofing von Identitäten kann im Internet of Things zu Katastrophen führen. Wir benötigen also Instrumente, um zu prüfen, ob ein empfangenes Paket auch tatsächlich von der im Paket angegebenen Quelle stammt:

- Wir könnten das Identitätsproblem auf Ebene der Anwendungen lösen (dann ist Spoofing auf Layer 3 und 4 immer noch möglich, stört aber nicht weiter). Eine Vielzahl unterschiedlicher, heterogener Lösungen wäre hier jedoch die natürliche Konsequenz.

[1] Siehe z.B. http://de.wikipedia.org/wiki/Car2Car_Communication und http://vector.com/vi_car2x_de.html
[2] Siehe z.B. http://www.zeit.de/zeit-wissen/2013/03/autonomes-auto-google-fahrzeugindustrie
[3] Siehe z.B. O. Spaniol, S. Hoff, „Anwendung von Informatik-Methoden auf Probleme des Straßenverkehrs", in „Telematik im Straßenverkehr", Springer, 1995
[4] Hier hat Apple beispielsweise Patente angemeldet, siehe http://www.spiegel.de/auto/aktuell/apple-patent-auto-per-iphone-finden-oeffnen-und-starten-a-896916.html

- Auf Layer 3 würde man natürlich sofort an so etwas wie den Authentication Header in IPsec denken. Nur, wer verwaltet all die sich ergebenden Security Associations im Internet of Things? In Einzelfällen ist so etwas möglich, als generelle, stets zu verwendende Lösung sicherlich nicht.

- Auf Layer 2 stolpert man über IEEE 802.1AE MACsec. Hier würden sogar MAC-Adressen zu vertrauenswürdigen Identitäten. Nur gibt es auch über 6 Jahre nach Verabschiedung des Standards kaum Produkte, und nur Cisco bietet bisher Switches mit MACsec-Unterstützung an. Außerdem bleibt MACsec konstruktionsbedingt eine lokale und damit punktuelle Lösung des Problems.

Es bleibt insgesamt wünschenswert, das Problem auf Layer 3, also im Rahmen von IP zu lösen. Wir benötigen hierzu ein Mittel, dass nach Zuweisung einer IP-Adresse an ein Endgerät automatisch die IP-Pakete mit einer kryptographischen Prüfsumme versieht, mit der (ohne unangenehmen Zusatzaufwand) geprüft werden kann, ob das Paket auch wirklich von der Station stammt, die das Paket ursprünglich gesendet hat. Mit IPsec drehen wir uns hier im Kreis. Es ist daher nicht überraschend, dass die IETF bereits seit ca. 5 Jahren an diesem Problem unter dem Titel „Source Address Validation Improvements“ arbeitet[5]. Lösungen materialisieren sich zwar langsam, nur wird wahrscheinlich niemand eine Prognose hinsichtlich der Beständigkeit wagen. Egal: Für das Internet der Things benötigen wir zwingend vertrauenswürdige Identitäten der Things, die auf einer einheitlichen, in IP nativ und per Default vorhandenen und nutzbaren Technik basieren. Andernfalls droht ein GAU, bei dem der Phantasie kaum Grenzen gesetzt sind.

Last but not least, es gibt interessante Korrelationen zwischen dem Internet of Things und dem Internet of Humans, die Datenschützer erschrecken und Big Data um höchst spannende Dimensionen erweitern, nämlich die Korrelation der Daten eines Dings und der Daten eines Menschen. Hier kann man sich sofort eine Vielzahl von Beispielen denken. Stellen wir uns etwa vor, dass ein Fahrzeug gewisse Messwerte wie Beschleunigungs-, Brems- und Lenkverhalten erfasst. Dann könnten Rückschlüsse auf den Typ des Fahrers möglich sein („aggressiv“ oder „ruhig“). Wie wäre es nun mit einer Versicherung, deren Kosten adaptiv zum Fahrerverhalten sind? Hier sind Datenschützer und Gesetzgeber gefragt, jedoch ohne in den ebenso gefährlichen Reflex zu verfallen die technische Innovation zu blockieren. Außerdem: Wer haftet bei einem (Sicherheits-)Vorfall im Internet of Things?

[5] Siehe http://datatracker.ietf.org/wg/savi/charter/

Report Neuerscheinung

Moderne Wireless-Technologien

Im Mai 2013 ist bei ComConsult Research die Neuauflage des Report "Moderne Wireless-Technologien" von Dr. Franz-Joachim Kauffels erschienen.

Die Entwicklung der Endgeräte wie Smartphones und Tablets scheint in immer schnellerem Takt zu erfolgen. Dass diese Geräte am Nabel der Cloud hängen, zieht sofort höhere Anforderungen an die Leistung der Infrastruktur nach sich.

In den letzten 2-3 Jahren haben Provider eine einzigartige Aufrüstungswelle vorgenommen und die 3G-Mobilfunknetze auf 4G umgestellt, in Europa meist mit LTE. Die Kernfrage ist jetzt, ob und wie die Wireless-Infrastrukturen in Unternehmen und Organisationen sinnvoll aufgerüstet werden können. Dafür gibt es aktuell zwei Kandidaten:

- IEEE 802.11ac als unmittelbare Weiterentwicklung von 11n im 5 GHz-Band
- IEEE 802.11ad als neuer Standard für die Kommunikation im 50 GHz-Band

Beide versprechen in der Werbung bis zu 7 Mbit/s. pro Zelle, bei 11ac wird die Leistung in der Praxis erheblich geringer sein. 11ad ist konstruktiv deutlich besser und könnte tatsächlich eine Leistung in der Größenordnung einiger Gigabit/s. pro Zelle erreichen. Consumer-Markt-Komponenten nach IEEE 802.11ac werden ab Mitte 2012 ausgeliefert. Die Frage ist, ob es für ein Unternehmen überhaupt sinnvoll ist, WLANs nach 11n durch WLANs nach 11ac abzulösen. Der Unterschied zwischen der höchsten Leistungsstufe von 11n (nominal 540 Mbps/Zelle) und der Leistungsstufe der ersten Produktgenerationen von 11ac (real 700 -1200

Mbps/Zelle) ist in realen Szenarien nämlich gar nicht so groß.

Denkt man etwas weiter, liegen die Kosten für eine Erweiterung nämlich bei den neuen Access Points, sondern vielmehr in der Infrastruktur. Spätere Generationen von 11ac und schon die erste Generation von 11ad haben eine Datenrate von deutlich mehr als 1 Gbps/Zelle. Daher muss die gesamte Infrastruktur, die die APs versorgt, auf 10 GbE umgestellt werden !!! Mit 11ad verschärft sich diese Situation noch weiter, denn die Eigenschaften der Wellenausbreitung im Millimeterwellenbereich führt zu Zellen, deren Größe selbst unter optimistischen Annahmen 50 – 70 qm kaum überschreiten wird.

Um die Markteinführung von 11ac nicht zu behindern, ist trotz vorhandener Muster für alle Komponenten die Weiterentwicklung von 11ad für etwa zwei Jahre auf Eis gelegt worden. Diesen Zeitraum können Unternehmen und Organisationen dazu nutzen, zu entscheiden, welche Technik sie denn in Zukunft einsetzen möchten. In der Zwischenzeit wird sich aber noch eine weitere Diskussion entwickeln, nämlich die Frage, ob man überhaupt die eigene WLAN-Infrastruktur noch weiterentwickelt oder sie lieber durch LTE ergänzt oder ganz ersetzt. Denn LTE ist verfügbar und letztlich ist es nur ein Rechenexempel.

In einer solch verfahrenen Situation hilft nur umfassendes Grundlagenwissen. Genau dazu dient dieser Report. Abgesehen von einer grundsätzlichen Einführung in die Möglichkeiten der Implementierung von Multi-Gigabit-WLANs in den bekannten Frequenzbereichen und Bändern werden die Technologien von 11n, 11ac und 11ad vorgestellt und untereinander verglichen. Zusätzlich werden wesentliche Grundeigenschaften von LTE erläutert und die Möglichkeit der Schaffung hybrider Umgebungen erläutert.

Die Erweiterungen der zweiten Auflage dieses erfolgreichen Reports betreffen die für die neuen Gigabit-Wireless-Infrastrukturen dringend benötigten Controller-Architekturen sowie Fragen der elektromagnetischen Belastung durch den Einsatz der neuen Technologien in einem größeren Maßstab. Im Gegensatz zu LTE sind WLANs nach den Standards 11ac und 11ad primär für die Versorgung privater Haushalte gedacht. Um im Umfeld eines Unternehmens oder einer Organisation erfolgreich eingesetzt werden zu können, bedürfen sie genau wie ihre Vorgänger umfangreicher technischer und organisatorischer Ergänzungen. In 2013 reagieren die einschlägigen Hersteller darauf angemessen mit neuen Architekturen und Geräten.

Fax-Antwort an ComConsult 02408/955-399

Bestellung

Moderne Wireless-Technologien

☐ Ich bestelle den Report
Moderne Wireless-Technologien
zum Preis von € 349,-- netto
zzgl. Versandkosten

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

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

Zweitthema

Neue Anwendungsformen im WLAN: 60-GHz-WLAN gemäß IEEE 802.11ad

Fortsetzung von Seite 1

Dr.-Ing. Joachim Wetzlar ist seit fast 20 Jahren Senior Consultant der ComConsult Beratung und Planung GmbH. Er leitet dort das Competence Center „Tests und Analysen“ und ist maßgeblich an seinem Aufbau beteiligt. Er blickt auf einen erheblichen Erfahrungsschatz mit Messgeräten und den Details der Kommunikations-Protokolle zurück. Neben seiner Tätigkeit als Trouble-Shooter führt Herr Dr. Wetzlar als Projektleiter und Senior Consultant regelmäßig Netz-Redesigns und WLAN-Planungen durch. Besucher von Seminaren und Kongressen schätzen ihn als kompetenten Referenten mit hohem Praxisbezug.

Das 60-GHz-Band bietet im Vergleich zu den althergebrachten WLAN-Frequenzen ungeahnten „Platz“. Ein einzelner Kanal belegt 2000 MHz. Zum Vergleich: Die WLAN gemäß IEEE 802.11a/b/g belegen pro Kanal 20 MHz, 11n bis zu 40 MHz und 11ac bis zu 160 MHz. Die Abbildung 1 zeigt das Kanalschema. In Europa sind demnach vier Kanäle nutzbar, in den USA und Japan je drei Kanäle.

So viel Bandbreite pro Kanal und doch „nur“ eine maximale Bitrate von 7 Gbit/s – das klingt komisch. Wieso schafft der neue WLAN-Standard für das 5-GHz-Band IEEE 802.11ac dieselbe Bitrate mit nur 160 MHz Bandbreite? Sie erinnern sich: Die Entwickler von 11ac haben allerlei technische Tricks angewandt, um das zu erreichen. Der weitreichendste ist das Verfahren „Multiple Input Multiple Output“ (MIMO), bei dem auf derselben Frequenz mehrere Datenströme – dort „Spatial Streams“ genannt – von mehreren Sendern ausgesandt und von mehreren Empfängern empfangen werden. 11ac wird seine maximale Bitrate erst erreichen, wenn es den Chip-Herstellern gelungen ist, 8 Spatial Streams zu erzeugen und zu verarbeiten. Derzeit sind Produkte mit 3 Spatial Streams verfügbar. Damit erzielt man im 5-GHz-Band Bitraten von 1,3 Gbit/s bei 80 kHz Bandbreite. Erste Chipsätze mit 4 Spatial Streams wurden vorgestellt, z.B. von Quantenna. Der Weg zu 8 Spatial Streams wird also noch einige Jahre Entwicklungszeit verschlingen.

Demgegenüber hat es das 60-GHz-WLAN einfacher. MIMO wird nicht benötigt! 2000 MHz Bandbreite reichen aus, um 7 Gbit/s mit Hilfe einfacher Techniken erreichen zu können. Wie bei WLAN üblich wählt der Sender das für die jeweilige Übertragungssituation optimale Verfahren. Er hat dabei die Auswahl aus einem Strauß verschiedener Parameter:

- Physikalische Schicht (PHY): Das Ein-Träger-Verfahren (Single Carrier PHY) muss von allen Stationen unterstützt werden. Hierbei wird eine einzelne Trägerfrequenz – d.h. eine der vier Frequenzen aus Abbildung 1 – mit der Information moduliert, so wie wir das aus den Anfängen der Radiotechnik kennen. Die Morsetelegraphie funktioniert im Prinzip genau so, nur mit etwas geringerer Bitrate. Daneben gibt es das Verfahren der orthogonalen Frequenzmodulation (Orthogonal Frequency Division Multiplex, OFDM). Das OFDM PHY sendet mehrere so genannte Unterträger parallel aus und moduliert sie mit unterschiedlicher Information. Das entspricht im Prinzip der guten alten Druckerschnittstelle („Centronix“), bei der mehrere Drähte parallel unterschiedliche Informationen übertragen. OFDM braucht nicht von allen Stationen unterstützt zu werden. Allerdings werden die versprochenen 7 Gbit/s nur mit OFDM erreicht. Die Single Carrier Modulation ist für maximal 4,6 Gbit/s gut.

- Modulationsverfahren: Es können vier verschiedene Verfahren gewählt werden. Das „langsamste“ und somit störunempfindlichste ist die binäre Phasenmodulation (Binary Phase-shift Keying, BPSK), mit der sich ein Bit pro Zeiteinheit übertragen lässt. Daneben gibt es die vierwertige Phasenmodulation (Quadrature Phase-shift Keying, QPSK) mit zwei Bits pro Zeiteinheit sowie je eine 16- und 64-wertige Quadratur-Amplitudenmodulation (QAM), mit denen sich 4 bzw. 6 Bits pro Zeiteinheit kodieren lassen.

- Faltungscode: Dabei handelt es sich um ein Verfahren, das Redundanz in den Datenstrom hineincodiert. Wenn einzelne Bits durch Störungen verloren gehen, kann der Empfänger sie dank Redundanz wiederherstellen. Es ist offensichtlich, dass diese Redundanz zusätzliche Information ist, die übertragen werden muss. Als Code-Rate bezeichnet man nun den Anteil der Nutzdaten am Gesamt-Datenaufkommen. Code-Rate 3/4 bedeutet also, dass 75% des übertragenen Datenvolumens Nutzdaten sind, und die Redundanz also die verbleibenden 25% ausmacht. IEEE 802.1ad sieht Code-Raten im Bereich von 1/2 bis 13/16 vor.

Die Kombination aus diesen Parametern ergibt letztlich die erzielbare Brutto-Daten-

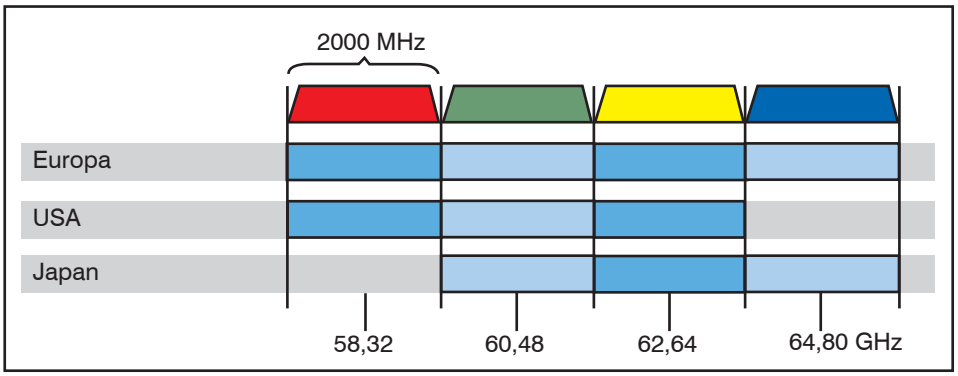


Abbildung 1: Kanäle im 60-GHz-Band

rate. Abbildung 2 ist ein kleiner Auszug. Daneben gibt es übrigens noch ein Low Power Single Carrier PHY mit geringfügig anderen Datenraten, das offensichtlich weniger Prozessorleistung benötigt und somit für Geräte mit geringer Stromaufnahme geeignet ist.

Zuletzt soll noch das Control PHY erwähnt werden. Es basiert auf dem Single Carrier PHY, überträgt jedoch nur 27,5 Mbit/s. Es dient zur Übertragung bestimmter Steuerungsinformationen, wie z.B. dem Einstellen der Antennen-Richtcharakteristik (Beamforming). Warum hierfür eine derart geringe Bitrate verwendet wird, sollen Sie gleich erfahren.

Der von mir verwendete Begriff „60-GHz-Band“ taucht in der IEEE 802.11ad eigentlich nur in der Überschrift auf. Dort heißt es “Enhancements for Very High Throughput in the 60 GHz Band”, also etwa “Erweiterung für sehr hohen Durchsatz im 60-GHz-Band“. Im Standard selbst ist dann nur noch vom „DBand“ die Rede. Das „D“ steht für „directional“, zu Deutsch „gerichtet“. Im DBand ist eine gerichtete Übertragung vorherrschend. Sender und Empfänger nutzen die Richtwirkung ihrer Antennen aus, um miteinander zu kommunizieren. Erst durch die Verwendung von Richtantennen entsteht am Empfänger eine so hohe Signalstärke, dass sich die störanfällige Modulation der hohen Bitraten einsetzen lässt. Mit anderen Worten, die Richtwirkung der Antennen ist eine Voraussetzung dafür, dass sich Giga-Bitraten über erträgliche Entfernungen übertragen lassen. Ohne Richtwirkung, also mit einem Rundstrahler, lassen sich bei gleicher Entfernung nur wesentlich geringere Bitraten erzielen.

Das ist der Grund für die Einführung des Control PHY mit 27,5 Mbit/s. Es dient unter anderem zur Verbindungsherstellung, macht also eine Kommunikation bereits möglich, bevor beide Stationen ihre Antennen aufeinander ausgerichtet haben. Nebenbei bemerkt: Die WLANs im 2,4- und 5-GHz-Band werden im Standard 11ad übrigens als „OBand“ bezeichnet. Das „O“ steht für „omnidirectional“, also „in alle Richtungen“. Das meint die Tatsache, dass die meisten Stationen, insbesondere die Clients in diesen Bändern Rundstrahlantennen einsetzen.

Wie richten nun die Stationen ihre Antennen aufeinander aus? Das Verfahren kennen Sie bereits und auch die dazu passende Abbildung 3. Sie zeigt, was passiert, wenn man mehrere in einer Reihe aufgestellte Antennen mit phasenverschobenen Signalen ansteuert („Phased Array“). Es entsteht dann eine Wellenfront, die sich

PHY	Modulation	Code-Rate	Datenrate (Mbit/s)
Single Carrier	BPSK	1/2	385
Single Carrier	BPSK	5/8	962,5
OFDM	QPSK	5/8	1732,5
Single Carrier	QPSK	13/16	2502,5
OFDM	16-QAM	3/4	4158
Single Carrier	16-QAM	3/4	4620
OFDM	64-QAM	13/16	6756

Abbildung 2: Brutto-Datenraten bei IEEE 802.11ad (Ausschnitt)

schräg von der Antennengrundlinie fortbewegt. Der WLAN Access Point kann für jedes Datenpaket eine individuelle Senderichtung wählen, je nachdem, wo sich die Station gerade befindet. Die beste Antennenrichtung lernt er, indem er die zuvor von der Station empfangenen Signale und deren Phasenlage an den einzelnen Antennen auswertet und eine so genannte Steuer-Matrix berechnet. Access Point und Station tauschen Inhalte dieser Steuer-Matrizen aus; zu diesem Zweck stehen Felder in den Paket-Headern zur Verfügung.

Das Verfahren des Beamforming funktioniert bei 60 GHz viel besser als bei 2,4 oder 5 GHz. Das liegt an der gegenüber den typischen Abmessungen von WLAN-Komponenten verringerten Wellenlänge. Während die Wellen bei 5 GHz noch ca. 6 cm lang sind, sind es bei 60 GHz nur noch 5 mm. Das „Taschenbuch der Hochfrequenztechnik“ von Meinke und Gundlach behauptet in der Ausgabe von 1957, dass der Gewinn einer Dipolzeile proportional zum Verhältnis ihrer Ausdehnung zur Wellenlänge sei. Der Gewinn gegenüber einem einfachen Dipol lässt sich mit der folgenden Formel berechnen, dabei bezeichnet L die Ausdehnung der Dipolzeile und λ die Wellenlänge. Der Gewinn GDZ ist in dieser Formel auf die eine fiktivge Antenne bezogen, die in alle Richtungen des Raumes gleichmäßig abstrahlt. Diese so genannte isotrope Antenne hat also ein kugelförmiges Richtdiagramm. Der Bezug auf den isotropen Strahler wird bei der Angabe des Gewinns durch den Index i gekennzeichnet (dBi).

$$G_{DZ} = 2{,}2\ dB + 10 \cdot \log\left(1 + \frac{8}{3}\frac{L}{\lambda}\right) dB$$

Die Ausdehnung L der Dipolzeile ist natürlich durch die Abmessung der WLAN-Endgeräte begrenzt. Die Formel scheint also indirekt zu sagen, dass sich bei gleichen Abmessungen und einem Zehntel der Wellenlänge (5 mm zu 6 cm ist etwa ein Zehntel) der zehnfache Antennengewinn erzielen lässt. Eine wichtige Vorausset-

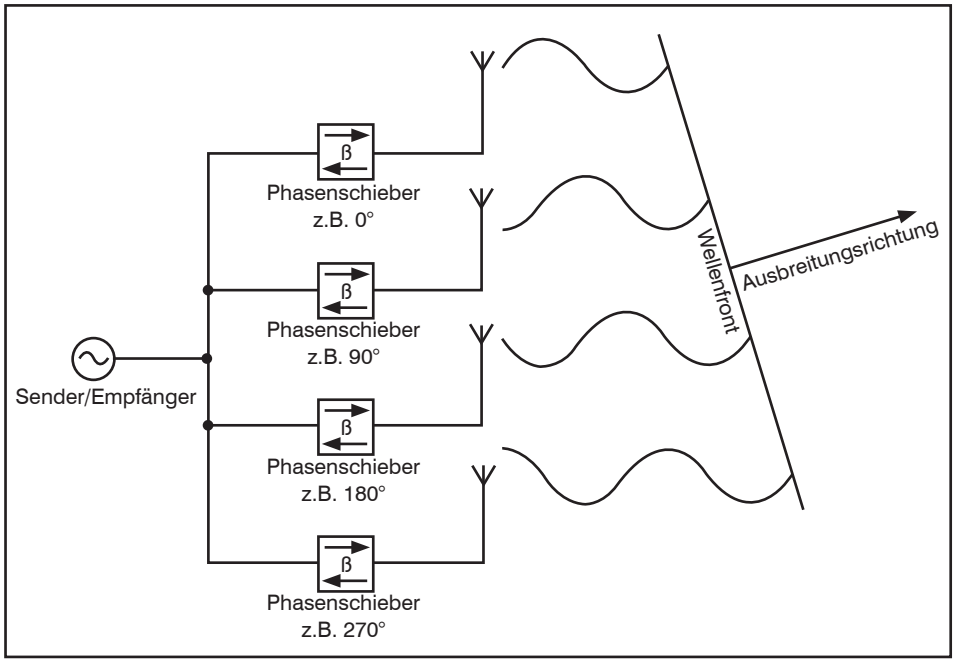


Abbildung 3: Prinzip des Beamforming

zung für die Gültigkeit der Formel ist laut Meinke und Gundlach, dass die einzelnen Dipole der Dipolzeile etwa 3/4λ voneinander entfernt sind.

Zur Verdeutlichung habe ich mich einer Software bedient, mit der man das Verhalten von Antennen simulieren und deren Richtwirkung graphisch darstellen kann. Stellen Sie sich zu diesem Zweck einen Access Point vor, an dem vier Antennen in einer Reihe angebracht sind. Die Antennen zeigen senkrecht nach oben und haben einen Abstand von je 4,5 cm, entsprechend 3/4λ bei 5 GHz. Die gesamte Ausdehnung der Dipolreihe beträgt somit 18 cm. Abbildung 4 zeigt die Sicht von oben auf die Dipolreihe und das sich ergebende Richtdiagramm. Als Gewinn wird von der Software ein Wert von 10,7 dBi angegeben, das ist etwas weniger als sich mit der oben angegebenen Formel errechnen lässt.

Zum Vergleich nehmen wir an, dass dieselbe Dipolreihe nun mit 60 GHz betrieben wird. Es ergibt sich ein Richtdiagramm gemäß Abbildung 5. Hier erkennt man keine ausgeprägte Richtwirkung, stattdessen verteilt sich die Abstrahlung auf zahlreiche „Nebenzipfel“. Als Gewinn wird sogar nur 8,3 dBi errechnet. Wirklich gut wird die Richtwirkung erst, wenn man ein paar mehr Dipole nimmt und diese mit dem optimalen Abstand 3/4λ anordnet (Abbildung 6). Die Gesamtlänge L beträgt in diesem Beispiel mit 8 Antennen 3 cm, und es ergibt sich ein Gewinn von ca. 14 dBi.

Welche Antennenformen die Entwickler für das DBand letztlich wählen werden, deutet sich bereits an. Der Hersteller Wilocity hat anlässlich der Consumer Electronics Show (CES) in Las Vegas im Januar dieses Jahres erste Muster solcher Antennen vorgestellt und zeigt auch ein Bild auf seiner Webseite (Abbildung 7). Man erkennt nicht mehr als eine Leiterplatte, auf der zwei Reihen à 8 Quadrate metallisch aufgebracht sind. Offensichtlich befindet sich auf der Rückseite die Elektronik, die diese 16 Antennen phasenrichtig anregen kann. Die von mir anhand einer anderen Abbildung geschätzte Breite ergibt sich etwa zu 3 cm. Das ist einerseits die bezüglich der Richtwirkung optimale Abmessung (s.o.). Andererseits ist 3 cm das Maß der Mini-PCI-Karten, auf denen WLAN-Adapter für Notebooks derzeit angeboten werden. Damit wird klar, dass sich Clients im 60-GHz-Band unter vertretbarem Aufwand mit Richtantennen werden ausstatten lassen, die eine gute Bündelung der Wellen aufweisen, wie in Abbildung 6 dargestellt.

Mit dieser Erkenntnis bekommt der Begriff der Funkzelle eine ganz andere Bedeutung. Dehnt sich die Funkzelle auf 2,4

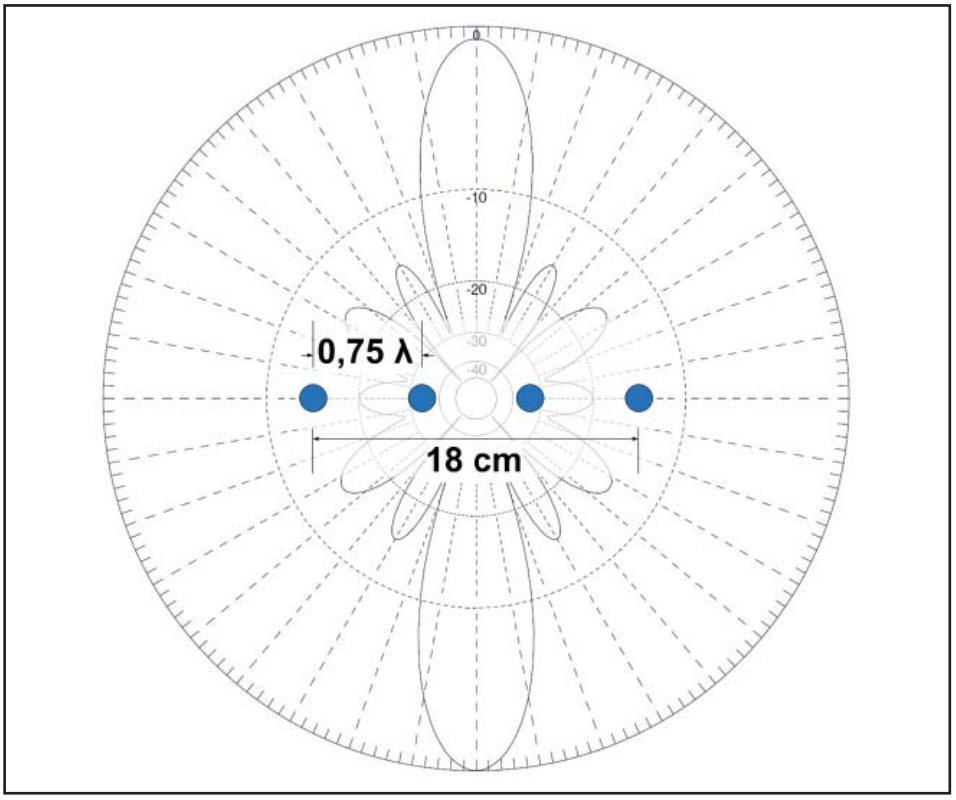


Abbildung 4: Richtdiagramm der Dipolreihe bei 5 GHz

und 5 GHz in erster Näherung kreisförmig um den Access Point aus, so haben wir es nun mit keulenförmiger Funkabdeckung zu tun. Zu jeder Station, die sich im Bereich des Access Points befindet, baut dieser eine entsprechend gerichtete Über-

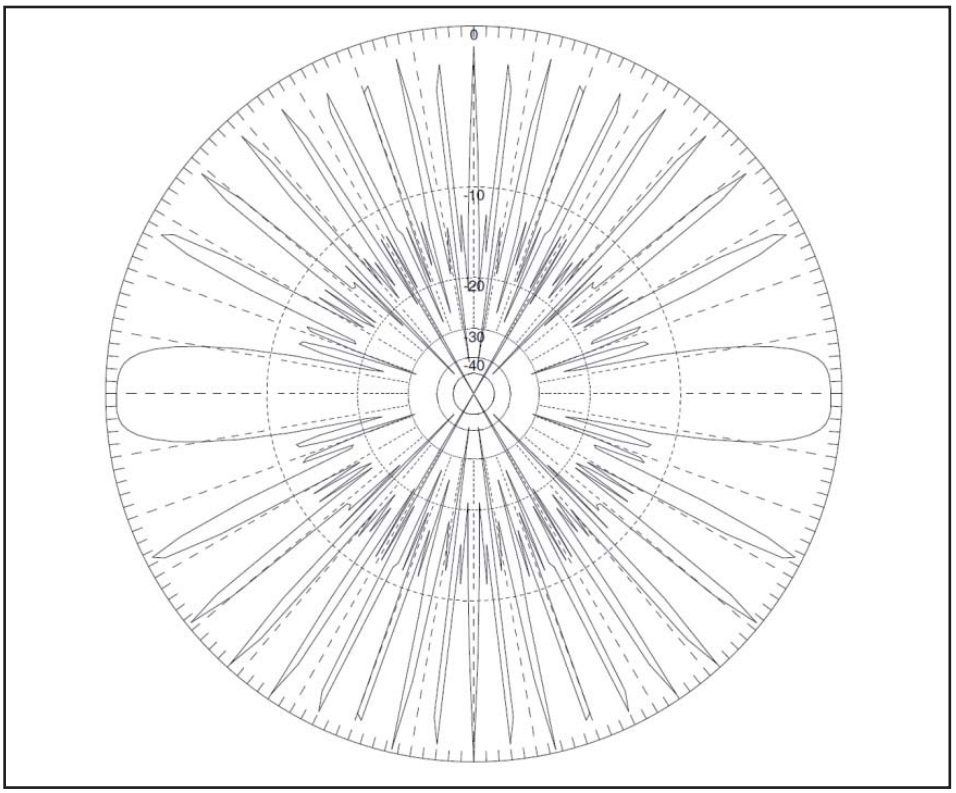


Abbildung 5: Richtdiagramm der Dipolreihe aus Abbildung 4 bei 60 GHz

Neue Anwendungsformen im WLAN: 60-GHz-WLAN gemäß IEEE 802.11ad

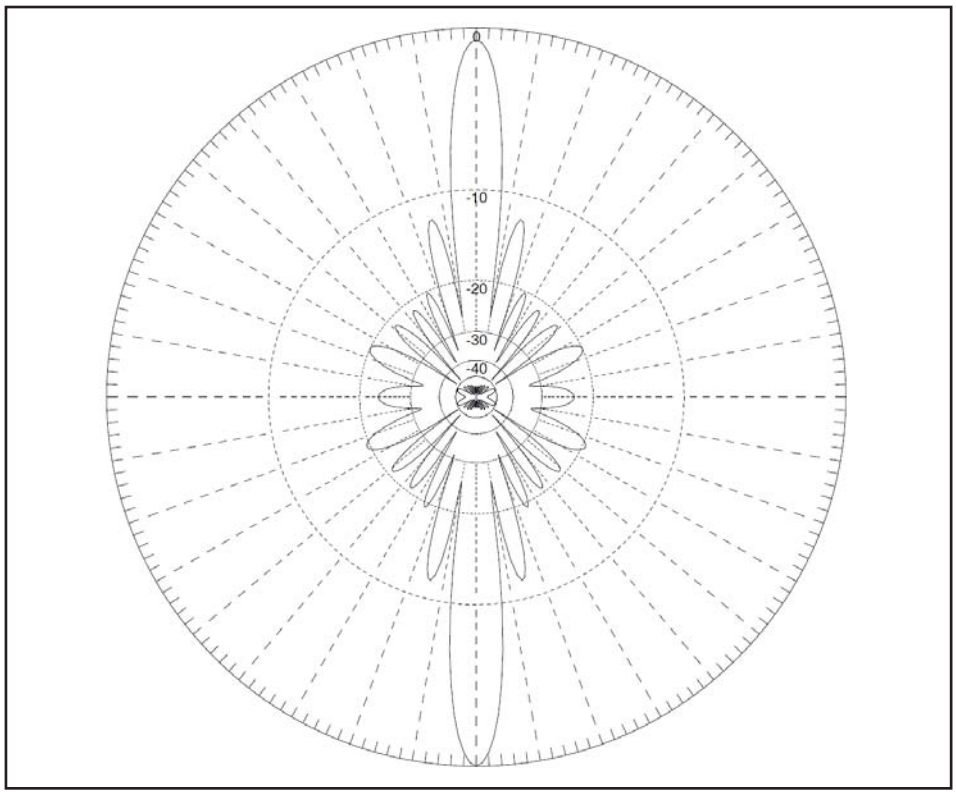


Abbildung 6: Richtdiagramm einer Dipolreihe aus 8 Dipolen

tragung auf. Und die Stationen tun dies genauso zum Access Point („Beam Combining“). Der Bereich, in dem die Stationen per Beam Combining miteinander kommunizieren können, wird zur besseren Unterscheidung nun Basic Service Area (BSA) genannt. Sie erinnern sich, die Funkzelle im 2,4 und 5 GHz WLAN wird im Standard als Basic Service Set (BSS) bezeichnet.

Die gerichtete Übertragung führt, das ist Ihnen wahrscheinlich aufgefallen, zu einem Effekt, den man eigentlich vermeiden möchte. Die Stationen im Bereich einer BSA hören sich nämlich gegenseitig nicht mehr, da sie ihre Richtantennen auf den Access Point ausgerichtet haben. Dieser so genannte Hidden-Station-Effekt führt normalerweise zu Kollisionen, die sich nur mittels RTS/CTS verhindern lassen. Die sendewillige Station schickt dabei zunächst eine Bitte um Sendeerlaubnis (Request to Send, RTS) an den Access Point und erhält von diesem eine Freigabe (Clear to Send, CTS) zurück. Mindestens das CTS wird von allen übrigen Stationen gehört, die dann für eine im CTS angegebene Zeitspanne schweigen müssen.

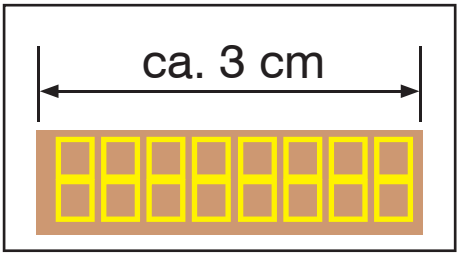


Abbildung 7: Antennen-Array mit 16 Antennen in zwei Reihen

Grundsätzlich funktioniert dieses Verfahren im DBand ebenfalls, jedoch bremst das RTS/CTS die schnelle Datenübertragung aus, unter anderem weil hierfür das Control PHY verwendet werden müsste. Die Erfinder haben aus der Not eine Tugend gemacht. Wenn die Stationen nun schon Beam Combining beherrschen, dann kann man sie auch gleichzeitig paarweise miteinander kommunizieren lassen. In Abbildung 8 ist ein derartiges Szenario dargestellt. Oberes und unteres Stationspaar kommunizieren gleichzeitig miteinander, obwohl sie derselben BSA angehören. Ein Notebook erhält Daten von einem Server über den Access Point (AP), während ein anderes Notebook sich mit einem Tablett PC synchronisiert. Eine fünfte Station ist gerade untätig, sie hat ihre Antenne auf Rundstrahlcharakteristik eingestellt.

Der Standard führt für diese parallele Nutzung des Mediums innerhalb einer BSA den Begriff „Spatial Sharing“ ein, also etwa „geteilte Nutzung des Raumes“. Sie werden bemerkt haben, dass in meinem Beispiel das untere Stationspaar ohne Nutzung des Access Points miteinander kommuniziert. Das ginge in einem BSS des OBand WLAN überhaupt nicht. Hier müsste man zu diesem Zweck ein so genanntes ad-hoc WLAN zwischen Notebook und Tablett aufbauen. Auch die-

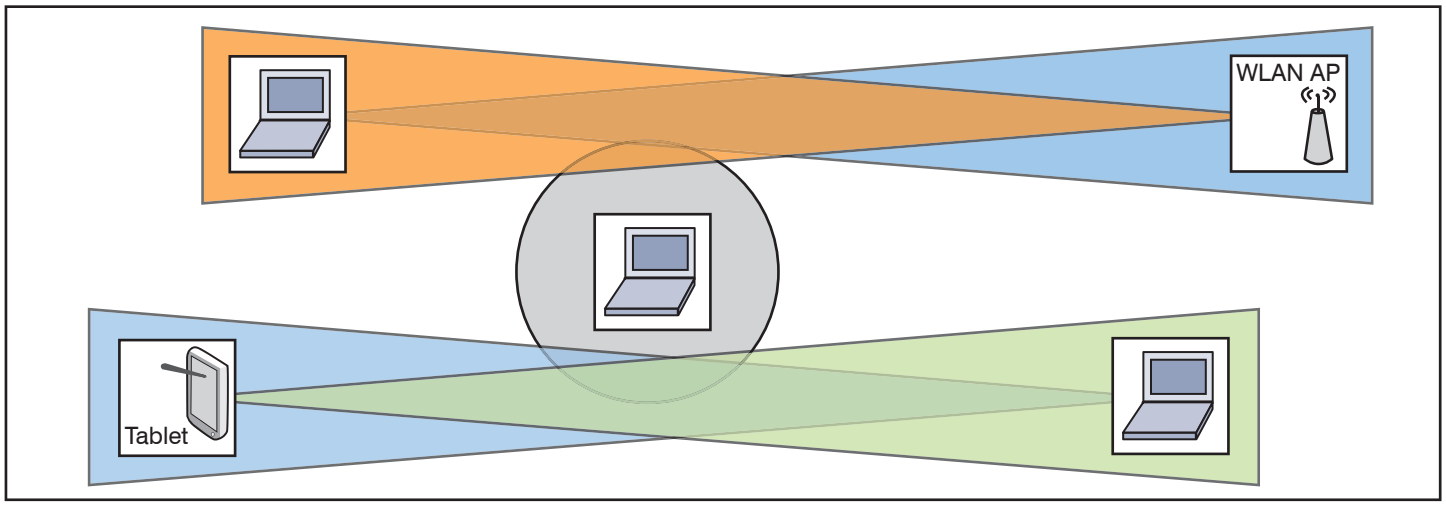


Abbildung 8: Spatial Sharing im DBand WLAN

Neue Anwendungsformen im WLAN: 60-GHz-WLAN gemäß IEEE 802.11ad

Abbildung 9: Mini-PCI-Karte für 2,4/5/60-GHz-WLAN (gesehen bei http://electronicdesign.com)

ses Konzept wurde vom neuen Standard 11ad erweitert. Es heißt nun Private BSS (PBSS) und erweitert das herkömmliche ad-hoc WLAN insbesondere um moderne Sicherheitskonzepte. Außerdem kann eine Station nun gleichzeitig Mitglied in einem PBSS und einer BSA sein. Erst dadurch wird das Konzept des Spatial Sharing sinnvoll umsetzbar.

Kommen wir nun zur Anwendung der Technik von IEEE 802.11ad. Zunächst stellt sich die Frage, was denn die Deutsche Bundesnetzagentur zur Verwendung des 60-GHz-Bandes sagt. Schließlich gab es in den Anfängen der WLANs erhebliche Einschränkungen, was die Nutzung des 5-GHz-Bandes betraf. Das sieht heute allerdings anders aus. Bereits in 2011 hat die BNetzA in ihrer Verfügung 8/2011 spezifiziert, dass WLAN-Geräte (die heißen bei der BNetzA „Wireless Access Systems / Radio LAN“) im Frequenzbereich von 57 bis 66 GHz eine maximale äquivalente Strahlungsleistung (EIRP) von 40 dBm nutzen dürfen. Das entspricht 10 Watt. Die EIRP bezieht bekanntermaßen den Antennengewinn mit ein. Das Gesamtsystem aus Sender, Kabel, Verbindern und Antennen darf in Hauptstrahlungsrichtung (!) keine höhere Leistung abstrahlen als eine isotrope Antenne, die mit 10 Watt gespeist wird. Access Points dürften also Leistungen von 100 Milliwatt kaum überschreiten, um die Vorgaben der BNetzA nicht zu verletzen.

Im Zusammenhang mit den Antennen hatte ich bereits den Hersteller Wilocity erwähnt. Dieser Hersteller – nein, ausnahmsweise nicht aus dem Silicon Valley sondern aus Israel – arbeitet bereits seit 2007 an Chips für die 60-GHz-Technik. Wilocity ist überdies ein führendes Mitglied der Wireless Gigabit Alliance (WiGig Alliance, http://wirelessgigabitalliance.org), die es sich zur Aufgabe gemacht hat, die 60-GHz-Technik voranzutreiben, ähnlich wie die WiFi Alliance beim 2,4/5-GHz-WLAN. Liest man die von der WiGig Alliance veröffentlichten Papiere, so stößt man schnell auf deren Vision: WiGig ist die universelle Lösung zur Vernetzung von PCs, Handhelds und Consumer-Elektronik.

Netzwerke – also WLAN und Client-/Server-Kommunikation auf Basis von TCP/IP – spielen dabei nicht die Hauptrolle. Vielmehr geht es um eine „Verdrahtlosung“ der High-Speed-Schnittstellen zu Peripheriegeräten, die heute mangels entsprechender Funktechnik noch nicht ohne das Kabel auskommen. Ich spreche von USB 3.0 und von Graphikschnittstellen wie dem High Definition Multimedia Interface (HDMI) oder Display Port. Bluetooth ist für derlei Zwecke einfach zu langsam. Die WiGig Alliance hat bereits passende Protokollspezifikationen vorgestellt. Es gibt insbesondere die WiGig Bus Extension (WBE), ein Protokollstack für die drahtlose Anbindung von Peripherie, sowie die WiGig Display Extension (WDE) als Ersatz für drahtgebundene Graphikschnittstellen.

Und man lese und staune: Diese Technik können Sie heute bereits kaufen! Die Firma Dell bietet als Zubehör zum „Latitude 6430u Ultrabook“ gegen einen geringen Aufpreis die „Dell Wireless 1601 Kombikarte, 802.11a/b/g/n 2x2, Bluetooth 4.0 LE + WiGig (60 GHz)“ an. Passend zum derart ausgestatteten Notebook gibt es von Dell eine drahtlose Docking Station, die „Wireless Dock D5000“. Daran werden wie üblich Monitor, Maus, Tastatur, Ethernet und Lautsprecher angeschlossen. Das Notebook selber können Sie getrost in eine Ecke legen, in der es einen Stromanschluss zum Laden gibt, denn das geht mit der 60-GHz-Technik leider noch nicht. Dell weist darauf hin, dass zwischen der Wireless Dock und dem Notebook eine Sichtverbindung bestehen soll. Der maximale Abstand zwischen Notebook und Dock wird mit 10 Metern vorgegeben.

Wilocity brüstet sich in einer Pressemitteilung vom Februar 2013 damit, die 60-GHz-Technik für Dell zu liefern. Im Internet kursieren Abbildungen der entsprechenden Mini-PCI-Karte (Abbildung 9). Sie erkennen einen Chip von Wilocity (Wil6120) neben einem AR9462 von Qualcomm/Atheros. Letzterer beherrscht WLAN gem. IEEE 802.11a/b/g/n. Der Wil6120 erreicht nach Aussage von Wilocity eine Brutto-Bitrate von 4,6 Gbit/s, er unterstützt also offensichtlich nur das Single Carrier PHY. Das Antennen-Array aus Abbildung 7 finden Sie auf der Karte nicht, es wird offensichtlich über Kabel angeschlossen.

10 Meter Radius für eine Funkzelle ist nicht viel – wenn man in den herkömmlichen Kategorien flächendeckender WLANs denkt. Aber Sie erkennen, dass mit der 60-GHz-Technik etwas anderes gewollt wird. Netzwerk ist nicht das Hauptaugenmerk. Es geht stattdessen um die vollständige Befreiung vom Kabel am Arbeitsplatz. Endgeräte, die ab Werk schon fast ohne Steckverbinder geliefert werden – ich spreche von Tablett PCs – bieten heute bereits eine Rechenleistung, die für die meisten Arbeiten des Büroalltages vollkommen ausreichend ist. Und wenn ich dieses Endgerät an meinem Arbeitsplatz mit Tastatur, Maus und großem Bildschirm bedienen kann, hat es seinen wesentlichen Nachteil verloren. Am Ende des Tages stecke ich das Endgerät dann in die Tasche und nehme es samt Daten mit.

Vielleicht läuten wir mit dieser Revolution gar das Ende der „Cloud“ ein. Es wird gar nicht mehr erforderlich sein, die Daten auf einer Vielzahl von Endgeräten zu synchronisieren. Nein, es gibt nur noch ein Endgerät, das an verschiedenen Orten die jeweils passende Peripherie drahtlos nutzt, inklusive Netzwerk.

Aber glauben Sie nicht, dass wir mit dieser Revolution auch das Ende des Kabels einläuten. Nein, denn jede dieser drahtlosen Docking Stations benötigt natürlich Strom und Ethernet, wie auch jeder herkömmliche WLAN Access Point. Nur wird die Dichte jetzt viel höher. In einem Artikel der April-Ausgabe des „Netzwerk-Insider“ sprach Dr. Jürgen Suppan von der „Arbeitsplatz-Zelle“. Ich habe dafür den Begriff der „Attozelle“ erfunden. Unter Femtozellen verstehen die Provider bekanntlich die Versorgung von Wohnungen oder Büros mit Mobilfunk. Die darunter liegende Stufe ist der einzelne Arbeitsplatz. Und jeder Arbeitsplatz benötigt Strom und ein Ethernet-Kabel. Wie gut, dass unsere Infrastruktur bereits heute darauf vorbereitet ist!

ComConsult Veranstaltungskalender

Aktuelle Veranstaltungen

Trouble Shooting in vernetzten Infrastrukturen, 11.06. - 14.06.13 in Aachen

Dieses Seminar vermittelt, welche Methoden und Werkzeuge die Basis für eine erfolgreiche Fehlersuche sind. Es zeigt typische Fehler, erklärt deren Erscheinungsformen im laufenden Betrieb und trainiert ihre systematische Diagnose und die zielgerichtete Beseitigung. Dabei wird das für eine erfolgreiche Analyse erforderliche Hintergrundwissen vermittelt und mit praktischen Übungen und Fallbeispielen in einem Trainings-Netzwerk kombiniert. Die Teilnehmer werden durch dieses kombinierte Training in die Lage versetzt, das Gelernte sofort in der Praxis umzusetzen. Als Protokoll-Analysator-Software kommt Wireshark zum Einsatz. Einer Verwendung selbst mitgebrachter Analyse-Software, mit deren Bedienung der Teilnehmer vertraut ist, steht nichts im Wege.

Preis: € 2.290,-- netto

Service-Offerierung - Von Service-Spezifizierung bis Service-Katalogisierung, 11.06. - 12.06.13 in Aachen

Der Service-Katalog mit seinen Offerten zur Service-Erbringung ist für jeden Service Provider die wesentliche Präsentationsplattform gegenüber seinen Service-Kunden. Für alle Beteiligten kommt es darauf an, dass die Service-Angebote klar und kompakt formuliert sind, so dass sie gut verstanden und angenommen werden. Gleichzeitig müssen die Katalogeinträge einfach und effizient zu verwalten sein.

Preis: € 1.590,-- netto

Intensiv-Tag Video: Markttrends und Technologien, 12.06.13 in Bonn

Auf dieser eintägigen Sonder-Veranstaltung unter Moderation von Petra Borowka-Gatzweiler wird der aktuelle Markt für Video und Videokonferenzen sowie deren Integration in UC-Lösungen analysiert. Es erfolgt eine Einführung in den aktuellen Technologiestand und Neuentwicklungen, insbesondere neue Standards für die Videotechnologie.

Preis: € 990,-- netto

Consult SDN-Forum 2013, 17.06. - 18.06.13 in Euskirchen

Software Defined Networking SDN wird die Netzwerk-Industrie in den nächsten Jahren deutlich verändern. Eine zentrale Software-Architektur wird die heutigen dezentral konfigurierten Switches ablösen. In spätestens fünf Jahren werden Switches generell programmierbar sein. Alle Anbieter passen ihre bestehenden Produkte im Moment entsprechend an oder bringen völlig neue und auf SDN optimierte auf den Markt.

Preis: € 1.890,-- netto

SIP (Session Initiation Protocol) - Basis-Technologie der IP-Telefonie, 24.06. - 26.06.13 in Köln

Dieses 3-tägige Seminar vermittelt Planern, Betreibern und Administratoren Anforderungen und Technologien für den Einsatz von Telefonie und Mehrwertdiensten auf Basis des SIP-Standards. Chancen und Risiken werden anhand von Einsatzszenarien bewertet und kontrovers diskutiert. Der größte Nachteil der bisher realisierten VoIP- und Unified Communications- (UC) Lösungen ist, dass sie mit hersteller-spezifischen Protokollen arbeiten. Doch dies ist ein Übergangs-Zustand. Das Session Initiation Protocol wird in Zukunft der gemeinsame Standard für IP-Telefonie und alle Echtzeit-Anwendungen werden. Schon jetzt sind signifikante Anbieter wie Cisco, Microsoft und Siemens auf diesen Standard umgeschwenkt, die verbleibenden Anbieter werden das kurz- bis mittelfristig nachholen.

Preis: € 1.890,-- netto

Sicherheitsmanagement mit BSI-Grundschutzmethodik/ ISO 27001, 24.06. - 26.06.13 in Köln

Informationssicherheit ist heutzutage ein Muss, sei es aus rechtlichen oder wettbewerbstechnischen Gründen. Den vielfältigen „Compliance"-Ansprüchen gesellt sich der Aspekt einer Konformität zu BSI-Methodik bzw. ISO 27001 hinzu und die Anforderung, sich an den zugehörigen Kontrollfragen und Maßnahmenkatalogen erfolgreich messen zu können. Längst sind ISO 27001 und BSI-IT-Grundschutz nicht mehr nur eine Möglichkeit, sich „werbewirksam" zertifizieren zu lassen. Vielfach liefert ihre Anwendung die erwartet plausible Antwort auf die Frage nach Erreichung eines „best-practice"-Mindest-Sicherheitsniveaus oder nach angemessenem (!) Sicherheitsaufwand bei erhöhtem Sicherheitsbedarf. So nützlich diese Hilfestellung bei Aufbau und Aufrechterhaltung der nötigen Sicherheit sind, so sehr kann bei mangels Erfahrung „ungeschickter" Anwendung ein enormer, vermeidbarer Arbeitsaufwand entstehen. Erfahrungen aus ComConsult-Projekten zur Anwendung der Methoden und Werkzeuge, mit und ohne abschließender Zertifizierung, können und sollen hier helfen.

Preis: € 1.890,-- netto

Rechenzentrumsdesign - Technologien neuester Stand, 24.06. - 26.06.13 in Köln

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

Preis: € 1.890,-- netto

Sommerschule 2013, 01.07. - 05.07.13 in Aachen

Netzwerke unterliegen einer permanenten Weiterentwicklung. Das technologische Umfeld von Netzwerken befindet sich in einem der intensivsten Änderungsprozesse der letzten 20 Jahre. Das betrifft das Rechenzentrum, neue IT-Architekturen, neue Client-Technologien bis hin zu Unified Communications. Hand in Hand mit dem Bedarf ändern sich Netzwerk-Technologien selber. Neue Standards zur Gestaltung von Netzwerken im Rechenzentrum und im Backbone sind gute Beispiele dafür. Zukunftsorientiertes und wirtschaftlich optimales Design muss dieses Gesamtbild berücksichtigen. Die ComConsult Sommerschule 2013 analysiert und diskutiert diese Änderungen und ihre Auswirkungen speziell auf die Netzwerk-Infrastrukturen.

Preis: € 2.490,-- netto

Zertifizierungen

ComConsult Certified Network Engineer

Lokale Netze
09.09. - 13.09.13 in Aachen
25.11. - 29.11.13 in Aachen

TCP/IP intensiv und kompakt
07.10. - 11.10.13 in Stuttgart

Internetworking
17.06. - 21.06.13 in Aachen
14.10. - 18.10.13 in Aachen

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

ComConsult Certified Trouble Shooter

Trouble Shooting in vernetzten Infrastrukturen
11.06. - 14.06.13 in Aachen
24.09. - 27.09.13 in Aachen

Trouble Shooting für Netzwerk-Anwendungen
09.07. - 12.07.13 in Aachen
05.11. - 08.11.13 in Aachen

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

ComConsult Certified Voice Engineer

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen
16.09. - 18.09.13 in Berlin
09.12. - 11.12.13 in Köln

Session Initiation Protocol Basis-Technologie der IP-Telefonie
24.06. - 26.06.13 in Köln
07.10. - 09.10.13 in Stuttgart

Umfassende Absicherung von Voice over IP und Unified Communications
18.07. - 19.07.13 in Bonn
04.11. - 05.11.13 in Bonn

Optionales Einsteiger-Seminar: IP-Wissen für TK-Mitarbeiter
30.09. - 01.10.13 in Düsseldorf

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

ComConsult Certified Service Catalogue Manager

Servicialisierung - Leitkonzept für verlässliche Service-Erbringung
07.11. - 08.11.13 in Bonn

Service-Identifizierung - Von Service-Begriff bis Service-Konsumentennutzen
18.11. - 19.11.13 in Siegburg

Service-Offerierung - Von Service-Spezifizierung bis Service-Katalogisierung
02.12. - 03.12.13 in Düsseldorf

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

Impressum

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

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

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

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

Für unverlangte eingesandte Manuskripte
wird keine Haftung übernommen