ComConsult Research

Der Netzwerk Insider

Januar 2017

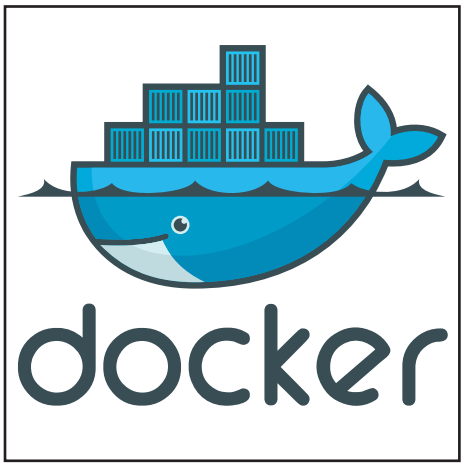
Systematische Weiterbildung für Netzwerk- und IT-Professionals

Data Center

Container-Networking

von Markus Schaub

Schon die Bezeichnung „Container“ legt einen Vergleich mit den 12,192 m langen, 2,438 m breiten und 2,591 m hohen ISO 668 Containern nahe. Dabei würde sich ein Kuchen als Analogie viel eher eignen. Warum? Dazu später mehr. Aber auch diese Analogie hat natürlich ihre Grenzen. Weder aus der einen noch aus der anderen lässt sich ableiten, was Container eigentlich sind, wofür man sie nutzt und warum sie nicht nur zunehmend auf die Entwicklung und den Betrieb von Software Auswirkungen haben, sondern auch für Netzwerke nicht ohne Konsequenzen sind.



Die Kernidee

Um die Idee von Containern zu verstehen, zäumt man das Pferd am besten von hinten auf und betrachtet das fertige Produkt, den Container selbst. Diese werden gerne mit virtuellen Maschinen verglichen. Abbildung 1 zeigt den strukturellen Aufbau von Containern und stellt diesen dem der virtuellen Maschinen gegenüber. Im Großen und Ganzen scheinen beide sehr ähnlich zu sein, da sie bis auf eine Schicht identisch sind: dem Guest-OS, also dem Betriebssystem, das in einer VM läuft. Dieses fehlt bei Containern.

weiter auf Seite 7

Wireless LAN

Was bringt der neue WLAN-Standard?

von Dr. Joachim Wetzlar

Kurz vor Weihnachten hat das IEEE den neuen WLAN-Standard IEEE 802.11-2016 veröffentlicht. Was? Schon wieder neue WLAN-Techniken? Gehören damit unsere WLAN-Komponenten, die teilweise noch aus dem letzten Jahrzehnt stammen, endgültig aufs Abstellgleis, sprich in den Elektroschrott? Keine Sorge: Der genannte Standard bringt eigentlich nichts Neues. Und dennoch gibt es neue Ideen und Entwicklungen im WLAN-Umfeld, die ich in diesem Artikel etwas beleuchten möchte.

Die letzte Ausgabe des WLAN-Standards – IEEE 802.11-2012 – war schon gewaltig: Insgesamt knapp 2.800 Seiten. Selbst auf Bibeldruckpapier wäre das noch ziemlich unhandlich. Immerhin kann man sich das Dokument als PDF beim IEEE herunterladen. Die Regel ist, dass ca. ein halbes Jahr nach der Veröffentlichung der Download kostenlos wird. Hierzu hat das IEEE das „Get Program“ eingerichtet, dessen Website sich unter dem Link **http://standards.ieee.org/about/get/** aufrufen lässt.

weiter auf Seite 17

Geleit

RZ kontra Cloud:

vergessen Sie IaaS, vergessen Sie Kosten, es geht um die Zukunft unserer Anwendungen:

naht das Ende von Client-Server?

auf Seite 2

Standpunkt

WLAN Clients senden weiter als man denkt!

auf Seite 15

Aktueller Kongress

ComConsult Netzwerk-Forum 2017

ab Seite 4

Aktuelles Seminar

Leistungsfähige, skalierbare, hochverfügbare, sichere und wirtschaftliche Speicherlösungen

auf Seite 16

Geleit

RZ kontra Cloud:

vergessen Sie IaaS, vergessen Sie Kosten, es geht um die Zukunft unserer Anwendungen:

naht das Ende von Client-Server?

ComConsult Research hat eine aktuelle Untersuchung abgeschlossen, deren Ergebnisse exklusiv auf dem Netzwerk Forum 2017 diskutiert wird. Dabei geht es um die Frage, warum und wie auch große Unternehmen Teile ihrer IT in die Cloud verlagern. Die Untersuchung hat wieder einmal unterstrichen, dass speziell bei der Diskussion „Cloud kontra Rechenzentrum“ einige zentrale Fakten nicht übersehen werden dürfen. Gleichzeitig wurden aber auch zentrale IT-Architekturen der Vergangenheit in Frage gestellt.

Bei der Diskussion der Cloud, speziell hier der Aspekt PaaS, darf nie übersehen werden, dass wir hier über einen klar definierten Typ von Anwendung sprechen:

- Es geht in der Regel um Web-Applikationen
- Mikro-Service-Architekturen lösen dabei monolithische Anwendungs-Architekturen ab
- Automatische Skalierung (Elastizität) spielt dabei eine große Rolle (siehe AWS Lambda)

Diese Rahmenparameter sind die Basis für eine Reihe von Folgeproblemen. Der Übergang zu Mikro-Services ist in der Anwendungsentwicklung der Status-Quo, da er die Voraussetzung für eine deutlich agilere Pflege von Anwendungen ist und die Ausfallzeiten durch Wartung pro Jahr dramatisch reduziert. Kombiniert man dies mit speziellen Diensten der Cloud-Plattformen wie zum Beispiel die automatische Migration auf neue Versionen, dann erreichen auch große Applikations-Betreiber heute Ausfallzeiten, die nur noch im Bereich weniger Minuten pro Jahr liegen. Leider haben Mikro-Services aber auch Nachteile. Einer der Kernnachteile liegt in der Lizenzierung. Die Anbieter von Software müssen bereit sein, sich auf diese Art von Architektur mit ihren Preis-Modellen einzulassen. Das ist nicht immer der Fall und im Zweifel erfordert dies den Wechsel des Software-Produkts. Gleiches gilt für die Eignung von Datenbanken in diesem Umfeld. Es gibt sicher Gründe warum dominante Anbieter wie Oracle in den Cloud-Datenbanken zum Beispiel von Amazon eine Gefahr sehen.

Damit ist aber auch klar, dass bei der Diskussion der Cloud eine 1:1 Migration bestehender Altanwendungen in der Regel ausgeschlossen werden kann. Unsere Untersuchung hat gezeigt, dass selbst im Fall von neuen Anwendungen, die bereits Mikroservice-Architekturen haben, erhebliche Anpassungen an die Cloud-Plattform erforderlich sind (diese sind aber bei bereits vorliegenden Mikroservice-Architekturen in der Regel schnell umsetzbar).

In unserer Untersuchung hat es damit auch eine sehr naheliegende Diskussion gegeben, die wir auch auf ComConsult Netzwerk Forum 2017 vertiefen wollen: wo stehen Client-Server-Architekturen. Die Aufteilung von Anwendungen in einen Client- und einen Server-Teil erfolgte historisch, um die Server zu entlasten und speziell x86-Server einer breiteren Nutzung zuzuführen. Diese Art von Architektur war dann auch über die letzten 15 Jahre gesehen sehr erfolgreich. Sie hat naturgemäß einen gravierenden Nachteil: sie erfordert die Installation und Pflege eines Clients. Dies kann je nach Gast-Betriebssystem, Typ des Clients und Art der Kommunikation zum Server zu erheblichen Aufwendungen im Betrieb führen. So kann man klar feststellen, dass die Betriebskosten von Client-Server-Lösungen deutlich höher sind als die Betriebskosten zentralistischer Lösungen (speziell wenn man wirklich alle Aufwendungen auf der Client-Seite erfasst. Sie kennen die typischen Probleme: neue Windows-Version erfordert zuerst den umfangreichen Test auf Kompatibilität, dann gibt es Widersprüche im Bedarf verschiedenerer Clients, dann gibt es Probleme mit Treibern usw).

Damit kommen wir zu einer ganz zentralen These: Client-Server-Architekturen sind tot. Sie sind nicht mehr erforderlich, da wir durch Mikroservice-Architekturen und Parallelisieren auf der Server-Seite eine quasi unendliche Kapazität haben. Das mag nicht für alle Anwendungen gelten, es gibt sicher Ausnahmen, aber es gilt für mehr als 90% aller Anwendungen.

Logischerweise wird man dann auch gar nicht erst versuchen eine Client-Server-Anwendung in die Cloud zu verlagern. Auch wären die Verluste durch die Verzögerung in der Kommunikation zwischen Client und Server so hoch, dass mit hoher Wahrscheinlichkeit keine akzeptable Anwendungs-Performance erreicht werden kann.

Damit ist aber auch klar: die Diskussion über die Cloud setzt an der völlig falschen Stelle an. In Wirklichkeit geht es um die Anwendungs-Architektur der Zukunft. Es geht um die komplette Ablösung aller bestehenden Alt-Anwendungen durch moderne Software-Architekturen. Die Frage, ob diese dann in der Cloud laufen oder nicht ist dabei gar nicht so spannend wie diese zentrale Frage.

Unabhängig von bestehenden Anwendungen gibt es dabei einen zunehmenden Bedarf für neue Anwendungen, die spezielle Dienste für Kunden bereitstellen. Zum Beispiel wird die Zukunft der Banken und Versicherungen durch diese neuen Anwendungen geprägt sein. Die Zeit von Internet-Banking aus der Steinzeit nähert sich dem Ende. Wir sprechen in Zukunft über hochintelligente Finanz-Assistenten, die die gesamte Spannbreite von Kreditaufnahme bis hin zur Anlage von Geld abdecken werden. Dies wird eine sehr dynamische und agile Entwicklung voraussetzen. Die große

RZ kontra Cloud: naht das Ende von Client-Server?

Frage ist nun wo speziell diese Anwendungen angeordnet werden. Diese Art von Anwendung wird aber vermehr erhebliche KI-Dienste integrieren müssen. Die im Moment zentrale Frage ist: was macht eine Bank, wenn sie KI im neuen Kunden-Client will, aber diese Dienste nur in der Cloud findet?

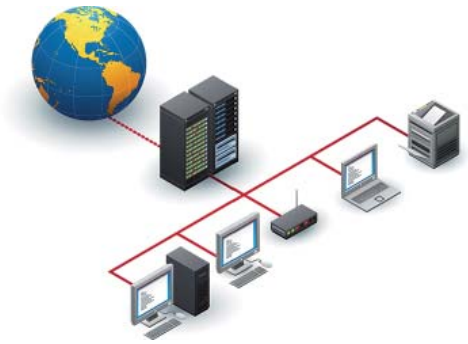
Dr. Hoff diskutierte in der Ausgabe vom November 2016 des Netzwerk Insiders die Umsetzung einer DMZ-Lösung in der Cloud. Dies ist zumindest international ein Megatrend. Und unsere Untersuchung hat gezeigt, dass es dafür sehr ernst zu nehmende Gründe gibt. Wer Anwendungen für Kunden in einem extrem Wettbewerbs-intensiven Umfeld entwickelt, der braucht Anwendungs-Agilität. Neue Funktionen müssen im Tagesrhythmus umsetzbar sein. Dies geht mit alten Anwendungs-Architekturen nicht. Hier stellt sich die Frage: wenn nicht ein Cloud-PaaS eingesetzt werden soll, wie sieht die lokale Alternative aus? Viele speziell kleinere Kunden werden schlicht nicht die Mittel haben solche extrem weit gehenden Entwicklungs-Umgebungen selber bereitzustellen und zu pflegen. Natürlich wird das die Auswahl der Plattform beeinflussen. Microsoft unterstützt lokale Entwicklungen deutlich besser als Amazon AWS. Auch Oracle geht in die Richtung der Unterstützung hybrider Szenarien. Allerdings hat dies auch Amazon erkannt. So weicht die neue Kooperation mit VMware die klare Cloud-Grenze bei Amazon auf. Allerdings werden dabei keinerlei Plattform-Dienste lokal angeboten, so dass der Vorteil weiterhin auf der Microsoft-Seite bleibt.

Dies wird uns noch eine ganze Weile beschäftigen, da es weitgehende Veränderungen der lokalen Infrastrukturen erfordert. Dies ist wiederum eine der Diskussionen des ComConsult Netzwerk Forums 2017.

Es ist und bleibt spannend.

Ihr
Dr. Jürgen Suppan

Kongress



ComConsult Netzwerk Forum 2017
27.03. - 30.03.2017 in Köln

Das ComConsult Netzwerk-Forum 2017 stellt die vier momentan dominantesten Netzwerk-Themen in den Mittelpunkt der Veranstaltung: Anwendungs-Architekturen und Kommunikation im Rechenzentrum, Netzwerk-Design und Optimierung des Betriebs, WLAN-Design und die Herausforderungen neuer Standards, Netzwerk-Sicherheit in einem Cloud-Umfeld.

Am ersten Tag analysieren wir die Auswirkungen aktueller Anwendungs-Architekturen auf die schnelle Bereitstellung, die Gestaltung und die Leistung von Netzwerken. Anwendungs-Architekturen werden immer dynamischer und in Kombination mit der Forderung nach einer sehr schnellen Bereitstellung von Kapazitäten ergibt sich eine komplexe Orchestrierungs-Aufgabe. Die Dynamik ergibt sich dabei nicht nur beim Start einer Mikroservice-Architektur, sondern auch bei Lastveränderungen im laufenden Betrieb.

Am zweiten Tag stellen wir uns den aktuellen Veränderungen im Netzwerkdesign in Kombination mit der Frage, wie wir in einer immer komplexeren Situation zu einem optimalen Betrieb kommen können.

Am dritten Tag diskutieren wir die neuesten WLAN-Standards und zum Abschluss des Tages die Frage, wie eine umfassende Sicherheits-Lösung unter Berücksichtigung der Cloud aussehen kann.

Der vierte Tag des ComConsult Netzwerk Forums widmet sich traditionell einem Schwerpunktthema, welches wir gemeinsam mit Ihnen intensiv beleuchten möchten. In diesem Jahr steht das Thema „Netzwerksicherheit: Bedrohungen, Herausforderungen, Trends und Best Practice“ im Fokus.

Wie in jedem Jahr so wird auch 2017 das ComConsult Netzwerk-Forum der Treffpunkt der Branche sein. Top-Referenten, die Analyse der neuesten Entwicklungen, praxisnahe Empfehlungen, mehr Sicherheit für Ihre Entscheidungen und viele, viele Diskussionen prägen diese Veranstaltung. Versäumen Sie nicht sich rechtzeitig einen Platz zu sichern.

Top-Referenten, die Analyse der neuesten Entwicklungen, praxisnahe Empfehlungen, mehr Sicherheit für Ihre Entscheidungen und viele, viele Diskussionen prägen diese Veranstaltung.

Preise: € 2.790,- netto - 4-tägige Veranstaltung mit Thementag
€ 2.390,- netto - 3-tägige Veranstaltung ohne Thementag

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

Aktueller Kongress

ComConsult Netzwerk Forum 2017 27.03. - 30.03.17 in Köln

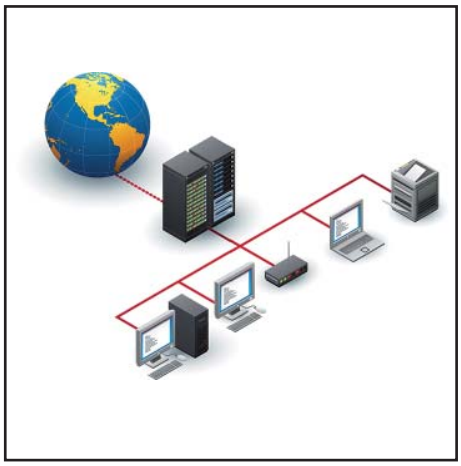
Die ComConsult Akademie veranstaltet vom 27.03. bis 30.03.2017 ihren Kongress "ComConsult Netzwerk Forum 2017" in Köln.

Das ComConsult Netzwerk-Forum 2017 stellt die vier momentan dominantesten Netzwerk-Themen in den Mittelpunkt der Veranstaltung:

- Anwendungs-Architekturen und Kommunikation im Rechenzentrum
- Netzwerk-Design und Optimierung des Betriebs
- WLAN-Design und die Herausforderungen neuer Standards
- Netzwerk-Sicherheit in einem Cloud-Umfeld

Am ersten Tag analysieren wir die Auswirkungen aktueller Anwendungs-Architekturen auf die schnelle Bereitstellung, die Gestaltung und die Leistung von Netzwerken. Anwendungs-Architekturen werden immer dynamischer und in Kombination mit der Forderung nach einer sehr schnellen Bereitstellung von Kapazitäten ergibt sich eine komplexe Orchestrierungs-Aufgabe. Die Dynamik ergibt sich dabei nicht nur beim Start einer Mikroservice-Architektur, sondern auch bei Lastveränderungen im laufenden Betrieb.

Wir stellen uns dementsprechend den Fragen:



- wie sieht die Schnittstelle zwischen Anwendung und Netzwerk aus?
- schnelle Bereitstellung und dynamische Kapazitätsanforderungen: wie geht das?
- welche Basis-Technologien sind auf der Netzwerkseite erforderlich?
- was muss Orchestrierung leisten?

Am zweiten Tag stellen wir uns den aktuellen Veränderungen im Netzwerkdesign in Kombination mit der Frage, wie wir in einer immer komplexeren Situation zu einem optimalen Betrieb kommen können.

Wir analysieren:

- wie sehen die aktuellen Design-Entwicklungen aus?
- Software Defined WAN: Hype oder bringt es wirklich etwas?
- Künstliche Intelligenz als Basis des Netzwerk-Betriebs: ist Machine Learning die Zukunft des Betriebs?

Am dritten Tag diskutieren wir die neuesten WLAN-Standards und zum Abschluss des Tages die Frage, wie eine umfassende Sicherheits-Lösung unter Berücksichtigung der Cloud aussehen kann.

Im Detail stellen wir vor:

- die neuen WLAN-Standards mit immer mehr Leistung: kommen wir an die Grenzen des Planbaren? wie viel Leistung können wir in Zukunft in welchen Szenerien liefern?
- WLAN und 5G: wie sieht in Zukunft das Zusammenspiel von WLAN und Mobilfunk aus?
- Kommunikation mobiler Endgeräte: wie integrieren wir welches Gerät wann und an welchem Ort optimal?
- Netzwerke und die Cloud: ein unlösbarer Widerspruch in der Gestaltung von Sicherheit?

Wie in jedem Jahr so wird auch 2017 das ComConsult Netzwerk-Forum der Treffpunkt der Branche sein. Top-Referenten, die Analyse der neuesten Entwicklungen, praxisnahe Empfehlungen, mehr Sicherheit für Ihre Entscheidungen und viele, viele Diskussionen prägen diese Veranstaltung. Versäumen Sie nicht sich rechtzeitig einen Platz zu sichern.

Anmeldung an kundenservice@comconsult-research.de

ComConsult Netzwerk Forum 2017

Ich buche den Kongress
ComConsult Netzwerk Forum 2017
27.03. – 30.03.17 in Köln

☐ zum Preis von € 2.790,-- netto (4 Tage)
☐ zum Preis von € 2.390,-- netto (3 Tage)

☐ Bitte buchen Sie mir ein Hotelzimmer

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

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

Programmübersicht ComConsult Netzwerk Forum 2017

Montag 27.03.17
Anwendungs-Architekturen und Kommunikation im RZ

9:30 Uhr 60 Minuten
Netzwerke zukunftssicher positionieren: welche Anforderungen generiert die IT der Zukunft? Ergebnisse einer Analyse von ComConsult Research
Dr. Jürgen Suppan, ComConsult Reserarch GmbH

10:30 Uhr 60 Minuten
Underlay / Overlay-Design für RZ-Netze
- Underlay Design
- VXLAN als De-facto-Standard für Overlay Data Plane
- Overlay Control Plane: Varianten
- BGP als De-facto-Standard für Overlay Control Plane
- Teufel im Detail: redundante Anbindung von Servern

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

11:30 Uhr Kaffeepause

12:00 Uhr 45 Minuten
Das Software-Defined Data Center - Der Paradigmenwechsel in der IT
- Was bedeutet „Software-Defined“?
- NFV statt OpenFlow: Die Virtualisierung des Netzwerks
- Virtualisierung von Sicherheitsfunktionen
- Unterstützung von Anwendungen: Die Anwendung definiert ihre Umgebung
- Integration von Cloud- und Fog-Computing
- SDDC = Private Cloud?
- Wie ändern sich Berufsbilder?

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

12:45 Uhr Mittagspause

14:15 Uhr 45 Minuten
Sind echte Router und Switches nicht mehr gut genug? Brauchen Netzwerker die Virtualisierung wirklich?
- Software Defined Everything: das Ende der Netzwerk-Abteilung?
- Server-, Speicher-, Firewall- und Netzwerk-Virtualisierung und ihre Integration: was bedeutet das eigentlich
- Die Rolle des Netzwerk- und Security-Spezialisten in der Zukunft
- Aktuelle Entwicklung und Planung von Datacenter-Lösungen der Zukunft

Gerd Pflüger, VMware Global Inc.

15:00 Uhr 45 Minuten
Private Cloud für die Berliner Verwaltung
Axel Freiberg, Frank Dornheim, IT-Dienstleistungszentrum Berlin

15:45 Uhr Kaffeepause

16:15 Uhr 45 Minuten
Analytics im Netzwerk
- Welche Daten können erfasst werden?
- Was kann damit erreicht werden?

Markus Harbeck, Cisco Systems GmbH

17:00 Uhr 45 Minuten
Netzwerk-Gestaltung in und mit der Cloud
- Wie werden Netzwerke in und mit der Cloud gestaltet? • Welche Alternativen gibt es?
- Gibt es Funktions-Nachteile?
- Projektbericht: was haben wir gelernt?

Markus Schaub, ComConsult Study.tv

ab 18:00 Uhr Happy Hour

Dienstag, 28.03.17
Netzwerk-Design und Optimierung des Betriebs

9:00 Uhr 60 Minuten
Modernes Campus Design
- Warum Verfahren wie STP, RSTP und LACP unzureichend sind (Neue Anwendungen in bekannten Protokollen, warum Echtzeit zunehmend unsere Netze dominiert)
- Vorteile moderner Designs mit TRILL, SPB und MC-LAG (Funktionsweise der Verfahren, Standardisierung)
- Warum QoS auch im LAN zu einem Thema wird (Designaspekte bei der QoS Umsetzung)
- Was spricht für ein Design das IP bis in den Accessbereich nutzt?

Markus Geller, ComConsult Research GmbH

10:00 Uhr 60 Minuten
Software-Defined WAN
- Active/Active-Nutzung des privaten WAN und des Internet • Nutzung physischer und virtueller CPE-Komponenten
- Zero-Touch Provisioning
- Erfahrungen aus Ausschreibungen

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

11:00 Uhr Kaffeepause

11:30 Uhr 60 Minuten
Software Defined - wie entwickelt sich die Technologie in den nächsten Jahren
- Netzwerk Automatisierung und Orchestrierung, wo stehen wir heute
- Automatisierung ohne SDN, Comeback der Fabrics • Künstliche Intelligenz und Netze – das Comeback von „SDN“?
- Intent based Networking: Der Weg von Analytics und ITOA zur Automatischen Netzsteuerung
- Big Data hält Einzug in die Netzsteuerung: Machine Learning als Control Plane des Netzes

Dipl.-Ing. Markus Nispel, Extreme Networks GmbH

12:30 Uhr Mittagspause

14:00 Uhr 45 Minuten
Ethernet und Photonics: neue Entwicklungen für das RZ
- Neue Anforderungen durch Cloud-Dynamik und exponentielle Technologien
- 25,50,100, 200 und 400 GbEthernet und mögliche Alternativen
- Gibt es überhaupt noch Unterschiede in der Switch-Hardware?
- Silicon Photonics: Durchbruch nach schwierigem Start • Konsequenzen für Betreiber privater RZ-Infrastrukturen

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

14:45 Uhr 45 Minuten
Vortragsslot
N.N.

15:30 Uhr Kaffeepause

16:00 Uhr 45 Minuten
IPv6: Projekterfahrung nutzen!
- Erfahrungen aus Kundenprojekten und der Stand von IPv6
- Klare Tendenzen und Treiber für IPv6 beim Kunden
- Ein klassisches Beispiel für die IPv6-Einführung im Mittelstand: ComConsult Beratung und Planung
- Erfahrungen Nutzen und Herausforderungen der Zukunft erkennen

Dr. Johannes Dams, ComConsult Beratung und Planung GmbH

Programmübersicht ComConsult Netzwerk Forum 2017

Mittwoch 29.03.17
WLAN und Security

9:00 Uhr
60 Minuten

5G: Infrastruktur der Disruptiven Digitalisierung

- Anforderungen durch Disruption, IoT und neue Arbeitsmodelle
- Grundlegende Technologien
- Ergebnisse der ersten größeren Testumgebungen
- Von LTE zu 5G: Weg der Standardisierung

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

10:00 Uhr
60 Minuten

Enterprise WLANs - ein Sammelbecken aus Zukunft und Altlasten

- Erfahrungsbericht: Anforderungen und Fallstricke aus der Praxis
- In welche Richtung entwickelt sich WLAN weiter?
- Stand der Dinge bei 802.11ax und 11ay
- Der Dual-Band AP – eigentlich ein Auslaufmodell!
- Sind Gäste-WLANs noch zeitgemäß?
- Wie sehen zukunftsträchtige WLAN-Konzepte aus?

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

11:00 Uhr Kaffeepause

11:30 Uhr
60 Minuten

Gestaltung und Betrieb moderner WLANs

- Flexible Controller Gestaltung
- Multi-Tenant-Betrieb
- Überwachung in Echtzeit: welche Information gibt es, wie kann sie an andere Systeme weitergegeben werden
- Wo geht es hin?

Reinhard Lichte, Aruba - a Hewlett Packard Enterprise Company

12:30 Uhr Mittagspause

14:00 Uhr
45 Minuten

Sicherheit aus der Cloud: Vorteile und Herausforderungen

Dipl.-Inform. Claus Vaupel, Zscaler Germany GmbH

14:45 Uhr
45 Minuten

Informationssicherheit in und aus der Cloud

- Herausforderung sicheres Cloud Computing in Public Cloud, (virtual) Private Cloud und Hybrid Cloud
- Integration Private Cloud und Provider Cloud
- Standardisierte und zertifizierte Cloud-Sicherheit
- Virtuelle Sicherheits-Gateways und virtuelle Internet DMZ in der Cloud: Mehr als ein Trend!
- Management von WLAN und LAN-Komponenten aus der Cloud
- Rolle der Cloud bei der Abwehr von Distributed Denial of Service (DDoS)
- Data Loss Prevention in der Cloud
- Abwehr zielgerichteter Angriffe durch Cloud-Dienste

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

15:30 Uhr Kaffeepause

16:00 Uhr
45 Minuten

Bessere Netzanbindung, bessere Funktechnik - wozu das alles?

- Mobilität am Arbeitsplatz 2021
- Netzanbindung mobiler Endgeräte
- Sichere Kommunikation für mobile Clients

Dipl.-Ing. Dominik Zöller, ComConsult Beratung und Planung GmbH

16:45 Uhr Ende der 3-tägigen Veranstaltung

Donnerstag 30.03.17
Netzwerksicherheit: Bedrohungen, Herausforderungen, Trends und Best Practice

9:00 Uhr
90 Minuten

Abwehr zielgerichteter Angriffe

- Angriffsmethoden und Werkzeugkasten
- Notwendigkeit system-und anwendungsübergreifender Strategien
- Erkennung von Symptomen
- Sandboxing
- Protokollierung, 2nd Generation SIEM und Big Data
- Bedeutung eines Information Security System für die Abwehr zielgerichteter Angriffe
- Systematisches Schwachstellenmanagement, Behandlung von Sicherheitsvorfällen
- Vulnerability Scanning: Techniken und Werkzeuge
- Sensibilisierung der Nutzer und Administratoren
- Demonstration

10:30 Uhr Kaffeepause

11:00 Uhr
90 Minuten

NAC in der Praxis

- Warum IEEE 802.1X immer noch ein Alptraum sein kann
- Best Practice NAC: Wie NAC erfolgreich umgesetzt und betrieben werden kann
- Der Teufel steckt im Detail: Wo sich die Hersteller unterscheiden • Projektbeispiele
- Typische Fehler in der Praxis
- Evolution von NAC: Von Advanced Monitoring über Profiling bis hin zur Abwehr zielgerichteter Angriffe

12:30 Uhr Mittagspause

13:30 Uhr
120 Minuten

Zonenkonzepte als Standardinstrument zur Absicherung der IT

- Warum Zonenkonzepte zu einem Standardinstrument geworden sind
- Best Practice für den Aufbau von Zonen
- Zonen im Campusbereich und NAC
- Zonen im Rechenzentrum, zwischen Rechenzentren und über WAN
- Zonen in der Cloud, zwischen Private Cloud und Provider Cloud
- Zonen in der virtualisierten Welt: Wie sehen Zonenkonzepte für Network Overlays aus?
- Virtualisierte Firewalls, Hypervisor-Integration von Firewalls • Welche Zonen braucht man?
- Staging-Umgebungen: Trennung von Entwicklung/Test und produktiver Umgebung
- Zonenkonzepte in der Industrial IT
- Prozesse für den Betrieb einer Zonenarchitektur
- Notwendigkeit der Trennung von Managementverkehr und produktivem / funktionalen Verkehr
- Sichere Administration und Überwachung braucht ein eigenes Zonenkonzept
- Management von Systemen über Management-Ports, Lights-out Management oder über produktive Interfaces
- Entkopplung administrativer Zugriffe durch Sprungserver, Terminal Server, virtuelle Admin-Clients
- Protokollierung administrativer Zugriffe
- Storage und Datensicherung
- Projektbeispiele

Dr. Simon Hoff, Dipl.-Math. Simon Oberem, Dipl.-Inform. Daniel Prinzen, Sebastian Wefers, ComConsult Beratung und Planung GmbH

15:30 Uhr Ende der 4-tägigen Veranstaltung

Der Veranstalter behält sich Änderungen im Programm vor.

Data Center

Container-Networking

Fortsetzung von Seite 1

Markus Schaub ist seit 2009 Leiter von ComConsult-Study.tv. Er verfügt über umfangreiche Berufserfahrung in den Bereichen Netzwerken und VoIP und ist seit mehr als 13 Jahren bei ComConsult beschäftigt. Seine Schwerpunkte liegen im Netzwerk-Design, IP-Infrastrukturdiensten und SIP, zu denen er viele Vorträge auf Kongressen hielt, erfolgreich Seminare durchführte und zahlreiche Veröffentlichungen schrieb.

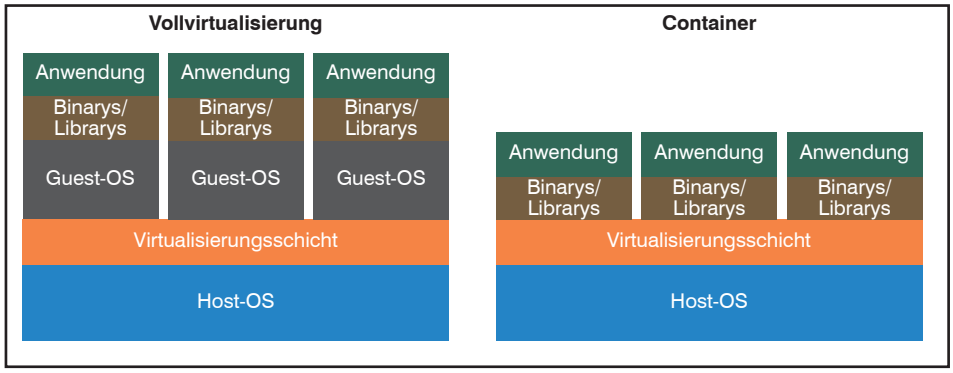


Abbildung 1: Vergleich virtuelle Maschine und Container

Viele betrachten Container deshalb als eine Art von lightweighted VMs, abgespeckten Virtuellen Maschinen. Das ist allerdings der falsche Ansatz. Denn dann stößt man auf eine ganze Reihe von unerträglichen Unzulänglichkeiten, wie die Abhängigkeit vom Betriebssystem des Hosts, die fehlenden virtuellen Netzwerkkarten, ein Fehlen von Funktionen wie vMotion und vieles mehr. Container erscheinen bei diesem Vergleich wie ein Rückschritt von einer ausgereiften Technologie zurück zu Virtualisierung aus der Steinzeit.

Man versteht Container besser, wenn man sie nicht als eine Form abgespeckter VMs betrachtet, sondern als eine neue Art der Softwareverteilung. Musste man bislang immer darauf achten, ob ein System die benötigte Umgebung für eine Anwendung bereitstellt, so bringen Container ihre Wohlfühlumgebung bereits mit. Da Container in sich gekapselt sind, braucht man auch bei der Installation nicht darauf achten, ob ggf. andere Anwendungen auf einem System laufen, die inkompatible Libraries benötigen.

Um ein Beispiel zu bringen: ein Entwickler programmiert ein neues Modul für eine Webseite. Da das Modul von Grund auf neu entwickelt wird, setzt er dabei auf PHP 7.0. Allerdings werden auch andere Module von der Webanwendung genutzt, die älteren Datums sind und deshalb maximal mit PHP 5.x zurechtkommen. Nach der Entwicklung muss also ein Web-Server gesucht werden, der bereits PHP 7.0 hat. Diese Information muss zwischen Entwicklern und Betreibern ausgetauscht und sauber dokumentiert werden.

Bei Containern ist das nicht nötig: jeder Container bringt seine Abhängigkeiten mit und läuft in seiner eigenen Laufzeitumgebung. Abbildung 2 zeigt schematisch das Innenleben eines Containers.

Laufen mehrere Container auf einem Host-System, so sind sie – und hier klappt der Vergleich mit Virtuellen Ma-

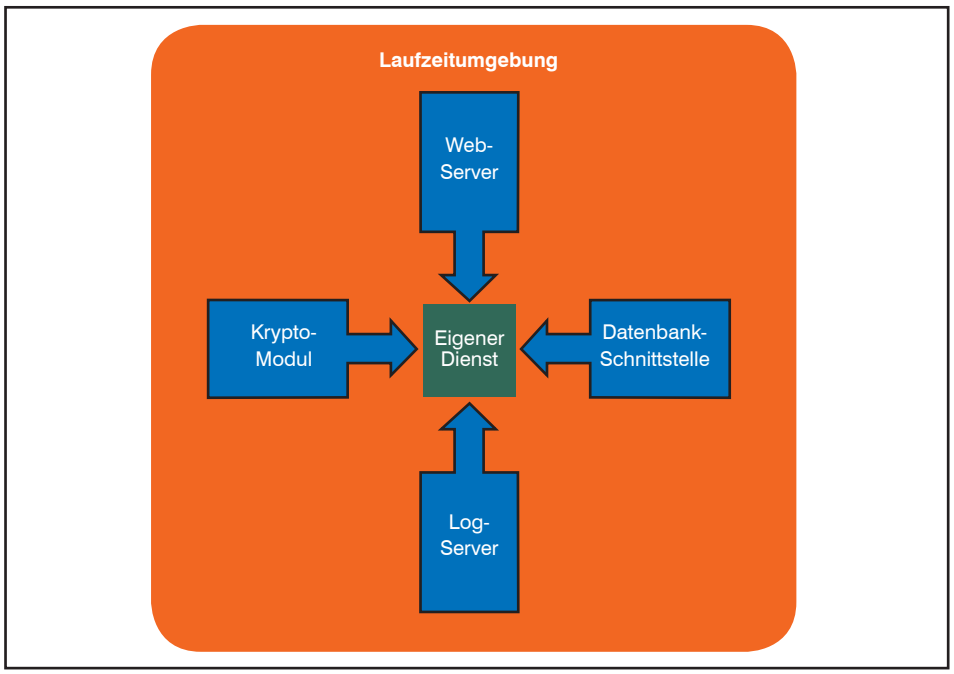


Abbildung 2: Innenleben eines Containers

schinen – gegeneinander abgeschirmt. D.h. im obigen Beispiel kann ein Container als Library PHP 5.x ein anderer PHP 7.x als Library mitbringen. Innerhalb des Containers können auch beide Webserver Port 80 nutzen. Problematisch wird letzteres erst, wenn man Ports für die externe Kommunikation, also außerhalb der Laufzeitumgebung des Containers freigeben möchte. Dazu später mehr.
Halten wir fest:

Eine Kernkomponente eines Containers ist es, einen Dienst inkl. seiner Abhängigkeiten und seiner Laufzeitumgebung isoliert zu betreiben.

Das alleine ist weder sonderlich neu noch ein Alleinstellungsmerkmal dieser vergleichsweise neuen Technologie. Es muss also noch mehr dahinter stecken. Dazu reicht es nicht einen laufenden Container zu betrachten, sondern vielmehr muss man verstehen, wie Container gebaut, verteilt und betrieben werden. Damit wären wir bei der Analogie des Kuchens.

Betrachtet man den Container als fertigen Kuchen, fehlen einige Dinge, die man benötigt, einen Kuchen zu backen: das Rezept, die Zutaten und die Geschäfte, wo man letztere erwerben kann.
Wenn man in dem Bild bleibt, so gibt es das alles auch für Container:

- Das Rezept ist die Anleitung, wie ein Container gebaut werden soll. Dieses Rezept heißt bei Docker bspw. Dockerfile.

- Die Zutaten sind die Libraries, Programme und Dienste, die alle zusammengefasst den Teig ergeben. Diesen Teig könnte man als Image bezeichnen. Der Teig muss noch gebacken werden, dem Image fehlt noch die Laufzeitumgebung.

- Die Geschäfte heißen Hub, dort kann man die notwendigen Zutaten beziehen, die im Rezept stehen.

- Fügt man dem Teig noch Hitze hinzu, hat man den Kuchen. Analog: das Image zzgl. einer Laufzeitumgebung ergibt einen Container.

Schauen wir uns die einzelnen Schritte im Detail an:

Der Dockerfile

Der Dockerfile ist eine Textdatei, die in der Programmiersprache Go geschrieben wird.

Der Dockerfile ist eine Anleitung, das Rezept, wie ein Image erstellt werden soll. Das Image, der Teig, ist die Vorstufe zum Container, zum Image später mehr.

Abbildung 3 zeigt beispielhaft einen solchen Dockerfile. Images können auf anderen Images beruhen, so wie man Fertigprodukte im Supermarkt kaufen kann, bspw. Blätterteig. Im Beispiel wird ein MySQL Server aufgesetzt. Die Basis „FROM“ ist eine bereits existente Ubuntu-Umgebung. Wichtig ist, nicht Ubuntu als komplettes Betriebssystem, sondern die Standard-Ubuntu-Umgebung ohne Kernel, denn der wird ja später vom Hosts-System bereitgestellt.

Als nächstes wird derjenige angegeben, der sich um dieses Image kümmert, der MAINTAINER.

Dann folgen eine Reihe von Befehlen, die die MySQL-Umgebung so aufsetzen wie der Maintainer es braucht: mysql wird installiert, konfiguriert, User werden angelegt, der Speicherort wird festgelegt, ein TCP-Port für die externe Kommunikation wird auf dem Host-System geöffnet etc.

```
FROM ubuntu:latest
MAINTAINER Markus Schaub

# Get MySQLRUN apt-get update
RUN apt-get install -y mysql-server-5.5

# Open MySQL to a world
RUN sed -i -e"s/^bind-addresss*=s*127.0.0.1/bind-address = 0.0.0.0/" /etc/mysql/my.cnf
# Script to pass MySQL
ADD startup.sh /
RUN chmod 755 /*.sh
#define access data
ENV DB_USER tagesschaub
ENV DB_PASSWORD shadow
ENV DB_NAME wp
ENV VOLUME_HOME "/var/lib/mysql"
# expose MySQL port to a network
EXPOSE 3306
# open to mount
VOLUME ["/var/lib/mysql", "/var/log/mysql"]
# start container
CMD ["/bin/bash", "/startup.sh"]
```

Abbildung 3: Beispiel eines Dockerfiles

Wer schon mal auf einem Linux-System Programme installiert hat, findet sich schnell zurecht, denn die Befehle entsprechen denen, die zu dem Linux-System gehören, hier eben Ubuntu. Denen werden nur entsprechende Go-Befehle vorangestellt. Hinzu kommen noch einige leicht zu erlernende Befehle, für die Definition der Schnittstellen zwischen dem Host und dem späteren Container, wie PORT (offener TCP-Port) oder VOLUME (Speicherplatz außerhalb der Laufzeitumgebung).

Hat man den Dockerfile fertig geschrieben, kann man das Image erstellen.

Das Image

Mittels des „build“ Befehles wird das Image erzeugt, indem die Befehle im File abgearbeitet werden. Im Beispiel aus Abbildung 3 geht die Containersoftware, bspw. Docker, nun hin und lädt zunächst vom Hub das aktuelle („latest“) Ubuntu-Image herunter. Danach werden die restlichen Befehle ausgeführt, also MySQL wird geladen und im Image installiert, die User erzeugt, etc.

In der Kuchenanalogie: es wird eingekauft und der Teig wird angesetzt. Und so ist das Resultat des Build-Prozesses auch kein Kuchen, also kein Container. Vielmehr wird eine Datei erzeugt, in der nun alles vorhanden ist, was der Container später benötigt, außer der Laufzeitumgebung, also beispielsweise temporären Verzeichnissen und natürlich dem Kernel selbst.

Der Container

Um nun vom Teig zum Kuchen zu kommen, muss man ihn noch backen. Das geschieht mit dem „run“ Befehl. Damit startet man ein Image und es wird zum Container. D.h. die Laufzeitumgebung wird erzeugt, und, wenn gewünscht, werden Schnittstellen bereitgestellt. Typisch sind Netzwerkschnittstellen und Speicher außerhalb des Containers.

Letzteres ist wichtig, denn wenn man einen Container löscht, so verschwindet auch seine Laufzeitumgebung und damit alle Daten, die nur im Container vorliegen. Hat man jedoch ein Programm „containerisiert“, das Daten erzeugt, die auch außerhalb des Containers verfügbar sein sollen, so muss man diese irgendwohin schreiben. Oder aber der Dienst im Container soll Dateien bearbeiten, die bereits vorhanden sind, dann muss dieser Speicherort natürlich gemountet werden.

Wichtig ist zu verstehen, dass nicht das eigentliche Image gestartet wird, sondern beim „run“ Befehl wird eine Kopie des originalen Images erzeugt und dieses wird dann gestartet.

Das hat Konsequenzen:

- Was immer man also mit dem Container anstellt, es hat keine Konsequenz für das ursprüngliche Image.
- Löscht man den Container, so verliert man zwar alles, was in seiner Laufzeitumgebung gespeichert wurde, das Image existiert aber immer noch. Man kann also dieselbe Umgebung erneut in ihrem ursprünglichen Zustand starten.
- Da das Image nur eine Datei ist, können natürlich mehrere Kopien auf verschiedenen Systemen zur selben Zeit existieren. Anderes formuliert: legt man das fertige Image an einem zentralen Platz ab, dem Hub, dann kann es sehr einfach verteilt werden.

Der letzte Punkt ist das Herz der Conainter-Idee: hat man ein Programm oder einen Dienst geschrieben, so kann man ihn mittels des Images problemlos verteilen und doch zentral pflegen. Da vom Host-System nur wenige Ressourcen direkt benötigt werden, sind die Anforderungen an das Host-System relativ gering. Es sei denn, man hat einen Dienst geschrieben, der bestimmte Funktionen des Kernels benötigt und somit Mindestanforderungen an das Kernelrelease stellt. Ist dem nicht so, kann man problemlos z.B. unter Ubuntu entwickeln und das Image auf CentOS Host ausführen. Bei Docker geht das mittlerweile sogar zwischen Linux und macOS – bedingt sogar mit Windows.

Abbildung 4 zeigt die Verteilung von Images mittels zentralem Speicherort, dem Hub.

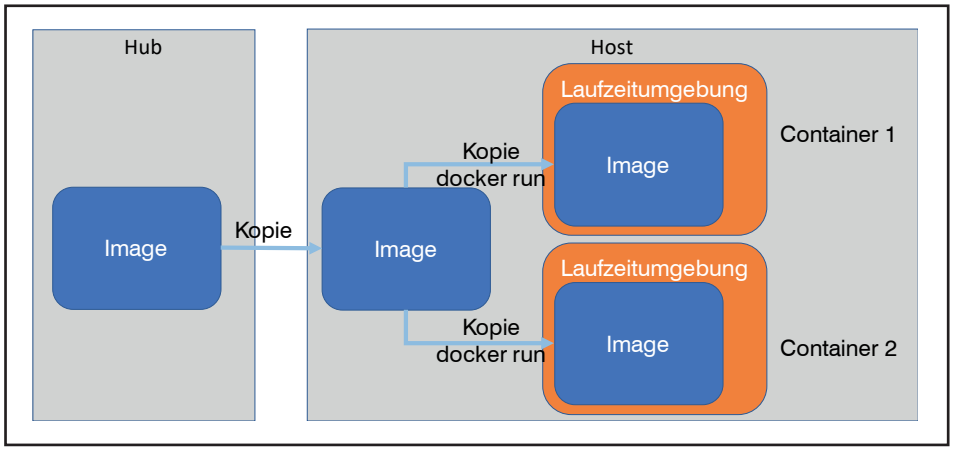


Abbildung 4: Zentrale Verteilung von Images

Image ohne Dockerfile

Der Vollständigkeit halber muss erwähnt werden, dass ein Dockerfile für die Erstellung von Images nicht zwingend nötig ist. Man kann Rezepte ja auch spontan erfinden.

Alternativ zum beschriebenen Vorgehen mit Dockerfile ist es auch möglich einen Container in ein Image umzuwandeln. Man kann bspw. dasselbe Resultat wie das Beispiel aus Abbildung 3 auch dadurch erzeugen, dass man zunächst das Ubuntu-Image lädt, startet und sich dann mittels „attach“ Befehles mit der Kommandozeile des so erzeugten Containers verbindet. Dann kann man alle Installationsbefehle des Dockerfiles dort genauso ausführen, als wäre der Container eine Virtuelle Maschine, auf deren Terminal man zugreift. Läuft alles zufriedenstellend, stoppt man den Container und wandelt ihn in ein Image um.

Wichtig dabei ist zu bedenken, dass man auf der Kommandozeile zwar alle internen Container-Befehle ausführen kann, jedoch keine Möglichkeit hat, die Schnittstellen zwischen Host und Container zu beeinflussen, denn der Container ist ja gegen das Hostsystem abgeschirmt. Will man also einen Port öffnen oder ein Laufwerk mounten, wie das im Beispiel der Fall ist, so muss man das später machen. Dafür stehen Parameter zur Verfügung, die man beim Starten eines Containers mit angibt.

Grundsätzlich ist der Weg über Dockerfiles vorzuziehen, da das implizit eine Dokumentation liefert, was gemacht wurde. Das ist bei Images, die aus Containern erzeugt wurde, nicht der Fall.

Jedoch hat auch das Vorgehen ohne Dockerfiles seine Berechtigung: für Quick-n-Dirty-Lösungen. Manchmal braucht man ein System nur „mal eben“. Beispielsweise wenn man nur mal testen will, ob das eigene Programm auch läuft, wenn man die PHP Version ändert. Dann startet man einen neuen Container mit seinem Programm, macht das Upgrade der PHP Version und schaut, ob alles klappt. Wenn ja, passt man seinen Dockerfile an, wenn nein, kann man „herumbasteln“ um herauszufinden woran es liegt.

Warum Docker-Container so beliebt sind

Linux-Container gibt es schon länger. Allerdings waren sie eher etwas für Nerds als für die breite Masse. Das gilt insb. für die breite Masse der Entwickler. Docker erfand nicht die Container selbst, sondern schuf darum herum eine Reihe von Tools, die die Erstellung, Verteilung und den Betrieb dergestalt vereinfachten, dass Container leicht zu händeln waren. Dadurch können sich Programmierer und Administratoren nun auf ihre eigentliche Aufgabe konzentrieren, ohne viel Aufwand in das Erlernen des Umgangs mit Containern zu stecken oder Zeit in die Verwaltung der Container zu investieren.

Doch reicht der einfache Umgang nicht aus, eine Technologie muss natürlich auch Vorteile gegenüber dem bisherigen bringen, damit sie attraktiv wird. Die Vorteile der Container-Technik liegen in zwei Kernbereichen der IT: der Entwicklung und dem Betrieb, auf Englisch: Development and Operation. Container passen ideal zur DevOp-Philosopie, die einen schnellen Zyklus von der Entwicklung zum Betrieb vorsieht. Traditionell muss neue Software intensiv getestet werden. Auch wenn nur einzelne Module neu geschrieben wurden, muss das gesamte Paket getestet werden, ob es nicht „neue“ Fehler in alten Modulen gibt, weil sich Abhängigkeiten geändert haben. Hier versprechen Container Abhilfe, da sie ihre eigenen Abhängigkeiten mitbringen und von anderen Prozessen isoliert laufen.

Allein die Container-Technik ist aber nicht die Lösung: auch die Gesamtanwendung muss Anforderungen erfüllen, wenn man die Vorteile wirklich ausnutzen möchte. Die wichtigste Voraussetzung ist dabei, dass die Anwendung nicht mehr monolithisch programmiert werden darf, sondern sich aus einer Reihe von kleineren Prozessen, so genannten Microprozessen, zusammensetzt. Diese Microprozesse können nun alle in ihren eigenen Containern laufen, so dass ggf. inkompatible Abhängigkeiten kein Problem mehr darstellen. Das reduziert den Zeitaufwand für Tests dramatisch. Auch kann der Aufwand für die Abstimmung zwischen Entwicklern und Betreibern minimiert wer-

den, da nur noch wenige Anforderungen miteinander abgesprochen werden müssen. Schließlich liefert der Entwickler nun nicht nur das Modul, sondern das Modul in einer lauffähigen Umgebung.

Wem das zu abstrakt ist, kann sich das Ganze am Beispiel einer Webseite vorstellen: statt die Webseite komplett zu gestalten und mit Inhalten zu füllen, wird die Seite nun in Bereiche, bspw. iFrames, unterteilt und gestaltet. Der Inhalt dieser iFrames kann nun von verschiedenen Webservern geliefert werden, die so unterschiedlich sein können, wie sie es müssen, bspw. ein Tomcat, ein nginx und ein apache, PHP 5 und PHP 7 in buntem Mix. Auch die Infrastruktur, aus der die Daten kommen, kann auf verschiedenen Datenbanken beruhen. Und so weiter. Wird nun ein iFrame-Inhalt geändert, sind die anderen nicht davon betroffen.

Fassen wir die Vorteile nach Lebenszyklen seiner Software zusammen:

- Entwicklung
  - Eigene Entwicklung wird mit Abhängigkeiten ausgeliefert
  - Versionierung ist einfach durch das Kopieren angehaltener Container
  - Zugriff auf bereits existierende und gepflegte Images
- Verteilung
  - Hosts werden ohne Anwendungsanforderungen bereitgestellt
  - Zentrale Bereitstellung der Images
  - Container werden durch Filter passenden Hosts zugeordnet
    Dazu später mehr.
- Betrieb
  - Bei Bedarf schnelle Bereitstellung von Containern
  - Notwendige Anpassungen an den Host sind durch Parameter einfach zu realisieren
  - Standardisierte Schnittstellen für den Containerbetrieb und die Containerverwaltung

Container im Netz

Bisher wurde nur die Basisidee von Containern erläutert. Ein wesentlicher Aspekt war, dass sie isoliert vom Rest der Welt agieren um Inkonsistenzen zu anderen Containern auf demselben Host oder gar dem Mutter-OS zu verhindern. Isolierte Prozesse bringen jedoch nur selten etwas, schließlich will man Daten verarbeiten, die irgendwo liegen und Ergebnisse wiederum abspeichern oder präsentieren. Container brauchen also Schnittstellen zum Rest der Welt, über die sie Daten abrufen und schreiben können bzw. über die die Prozesse in den Containern erreicht werden können.

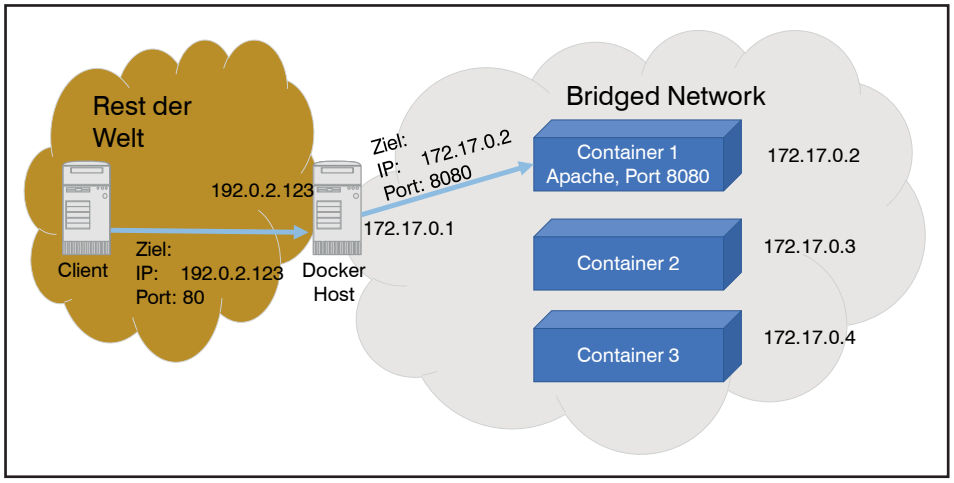


Abbildung 5: Standardschnittstelle Bridged Network mit NAT

Für diese Schnittstellen stehen je nach Anforderung zwei Varianten zur Verfügung. Zum einen kann einem Container beim Starten Zugriff auf externen Speicher gewährt werden. Dieser wird im Container dann ganz „normal“ gemountet. Die Prozesse innerhalb des Containers können auf diesen Speicher lesend und schreibend zugreifen. Anders als bei Container-internen Verzeichnissen bleiben diese Verzeichnisse jedoch erhalten, wenn man den Container löscht.

Die andere Art des Zugriffs ist über IP. Zum einen können die Prozesse innerhalb des Containers per IP auf externe Quellen zugreifen, zum anderen ist es aber auch möglich interne Prozesse über Portfreigaben für den Rest der Welt erreichbar zu machen. Letzteres ist meist aber nicht so uneingeschränkt möglich wie das bei Virtuellen Maschinen der Fall ist. Da Container sich die Kernel-Funktionen mit dem Mutter-OS teilen, verfügen sie nicht, wie VMs über unabhängige, virtuelle Netzwerkkarten, sondern das Host-OS stellt die Netzwerkverbindungen zur Verfügung.

Das klang jetzt etwas abstrakt, was daran liegt, dass es verschiedene Varianten gibt, wie das Host-OS den Netzwerkzugang der Container realisieren kann. Diese schauen wir uns im Folgenden an.

Default: Bridged Network

Wird auf einem Host ein Container gestartet, so bekommt er vom Host-OS eine IP Adresse zugewiesen. Diese kommt standardmäßig aus dem privaten IP Bereich 172.17.X.X. Das Host-OS achtet dabei darauf, dass IP Adressen nicht doppelt vergeben werden. Die Container auf dem-

selben Host können untereinander per IP kommunizieren, wenn sie die IP-Adressen oder den Host-internen Namen der anderen Container kennen. Daher der Name: Bridged Network, die Container agieren wie eine Gruppe gebridgder Hosts. Einen Zugang zum Rest der Welt haben sie zunächst einmal nicht.

Um diesen herzustellen, nutzt Docker ein Portforwarding und NAT. Abbildung 5 zeigt das am Beispiel eines Web-Servers, der intern auf Port 8080 läuft, extern aber über die IP-Adresse des Host-OS über Port 80 erreicht werden kann.

Dieses Verfahren ist schnell und einfach. Vor allem können die Host-Systeme unabhängig voneinander die IP-Adressen der Container vergeben, ohne dass es zu Konflikten mit doppelten IP-Adressen kommt.

Aber natürlich hat dieses Verfahren auch die üblichen Nachteile, die NAT nun einmal mit sich bringt. Dazu gehört insbesondere, dass keine zwei Container auf demselben Host-System über denselben Port erreichbar sind. Im obigen Beispiel bedeutet das, dass kein zweiter Webserver in einem Container laufen kann, der über den Standard-Port 80 zu erreichen wäre.

Ein weiterer Nachteil ist, dass die Container auf zwei verschiedenen Hosts ebenfalls nur per Portforwarding miteinander kommunizieren könnten, auch wenn sie zur selben Anwendung gehören.

Last-but-not-Least können Container, die nicht zur selben Anwendung gehören, jedoch auf demselben Host laufen, sich untereinander per IP erreichen. Insbesondere wenn man über Container in Clouds nachdenkt, ist das ein großes Sicherheitsrisiko.

Um dieses Risiko aus dem Weg zu räumen, gibt es neben der Standard-Bridge auch die User-defined Bridge.

User-defined Bridge

Bei einer User-definded Bridge werden die Container in Gruppen unterteilt, wie das beispielhaft in Abbildung 6 dargestellt ist:

Auf einem Host wurden zwei Gruppen definiert: die Gruppe „Entwicklung“ und die Gruppe „Betrieb“. Beim Start eines Containers wird dieser der einen oder anderen Gruppe zugewiesen. Die Kommunikation untereinander ist nur innerhalb einer Gruppe möglich, nicht jedoch Gruppenübergreifend.

Dieses Verfahren ermöglicht es dem Betrieb unterschiedlichen Anwendern Ressourcen auf derselben Hardware zur Verfügung zu stellen, ohne dass die Anwender sich in die Quere kommen können. Wie bereits erwähnt ist dies für den Betrieb einer Cloud unerlässlich, um ein Mindestmaß an Sicherheit zu gewährleisten. Dabei ist egal, ob es sich um eine private oder public Cloud handelt.

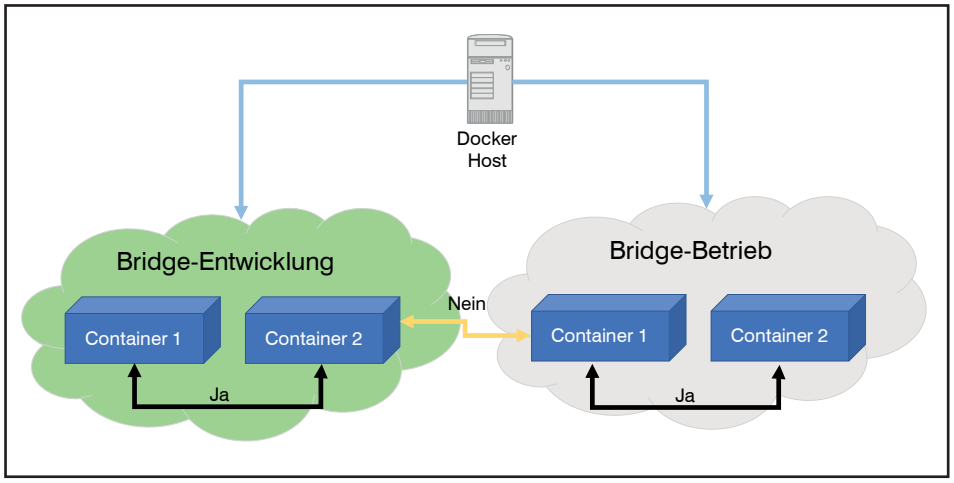


Abbildung 6: Beispiel einer User-defined Bridge

Allerdings ist damit das Problem verteilter Anwendungen noch nicht gelöst, deren Microprozesse auf unterschiedlichen Hosts gelandet sind. Denn selbst wenn auf zwei Hosts dieselben Gruppen existieren, so können diese noch nicht untereinander kommunizieren. Dafür benötigt man ein Overlay Network.

Overlay Network

Als Overlay Network kommt prinzipiell jede Overlay Technologie in Frage, die einem gerade einfällt. In Abbildung 7 ist es beispielsweise VXLAN. GRE wäre ebenso möglich. Nicht alle Overlay-Technologie haben bereits Einzug in die Tools von Docker gefunden, jedoch kommen hin und wieder neue hinzu, so dass ein Blick in die Dokumentation hilfreich ist, wenn man wissen möchte, ob die von einem bevorzugte Technik bereits realisiert wurde.

Das Overlay Network wird zwischen den Host-Systemen aufgespannt. Die Docker-Software sorgt nun automatisch dafür, dass IP-Adressen bei verbundenen Hosts an Container nicht doppelt vergeben werden. Auf die Weise ist sichergestellt, dass es zu keinen Konflikten kommen kann. Die Overlay Technik ist selbstverständlich mit dem User-defined Bridging-Verfahren kombinierbar. Anders als im Beispiel könnten die Container also noch unterschiedlichen Gruppen zugewiesen werden.

Die bislang vorgestellten Techniken lösen jedoch noch nicht die NAT Probleme: Ports müssen explizit geforwarded werden und extern steht jeder Port nur einmal zu Verfügung, auch wenn mehrere Container diesen gerne nutzen würden.

Um auch diesen Nachteil anzugehen,

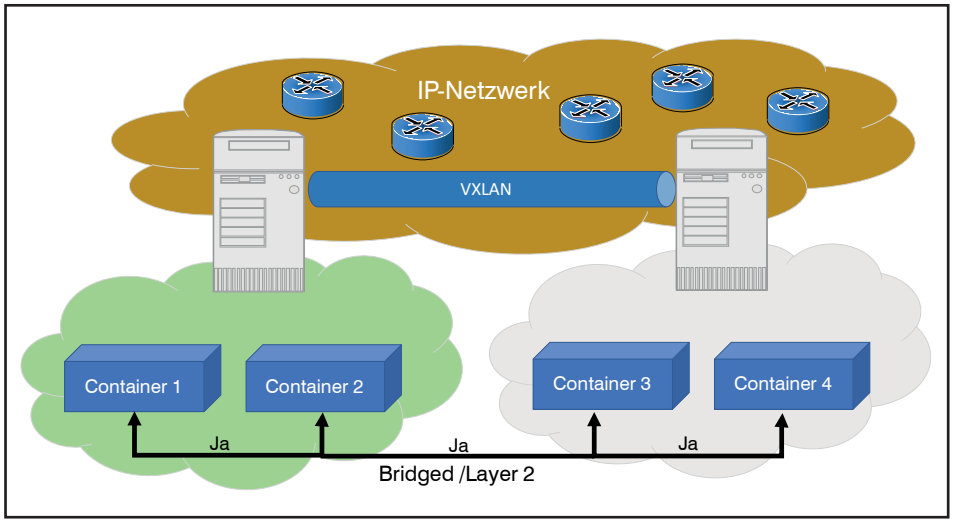


Abbildung 7: Docker Hosts mit Overlay Network

gibt weitere Verfahren, die genutzt werden können. Diese werden nun beispielhaft anhand von IPv6 vorgestellt.

IPv6 mit NDP Proxy

Der ein oder andere Leser wird sich noch an den Proxy-ARP bei IPv4 erinnern, der vor der Einführung von VRRP und dessen proprietären Verwandten als Redundanzverfahren genutzt wurde. In IPv6 gibt es eine Entsprechung, den NDP Proxy.

Gemäß dem Standardvorgehen von IPv6 bekommt ein Host eine IPv6 Adresse und das /64 Präfix zugewiesen. Auf dem Host wird nun ein zu seiner Adresse passender Teil als kleineres Präfix definiert, aus dem er seinen Containern IP Adressen geben kann. Im Beispiel von Abbildung 8 wird dem Host 1 die IP Adresse 2001:db8::a001 zugewiesen und als „Sub-Präfix“ verteilt er Adressen von 2001:db8::a008 bis 2001:db8::a00f und vergibt den Containern ein Präfix von /125. So können die Container untereinander auf demselben Host wieder bridged miteinander kommunizieren, wollen sie jedoch mit Containern auf anderen Hostes reden, so müssen sie den eigenen Host als default Router nutzen.

Der eigentliche Router bekommt davon nichts mit, denn wenn er einen SNMA-Request (den ARP-Nachfolger bei IPv6) ausführt, so antwortet der Host stellvertretend für den Container, also als Proxy.

Haben Sie jetzt einen Knoten im Gehirn? Macht nichts, ich auch. Das Verfahren benötigt einiges an Konzentration, um es zu verstehen und auch um es zu betreiben. Eingeführt wurde es von Docker, um von der Konfiguration des eigentlichen Routers unabhängig zu sein.

Es geht nämlich auch deutlich eleganter, indem man die Hosts als Router einsetzt:

Routed IPv6

Da bei IPv6 kein Adressmangel herrscht, kann man, wie in Abbildung 9 dargestellt, jedem Host-System ein komplettes /64 Präfix zuweisen. Dazu muss dann allerdings auf dem eigentlichen Router eine entsprechende Hostroute zu dem System angelegt werden. Die Container bekommen nun IPv6 Adressen aus diesem Bereich mit kleineren Präfixen zugewiesen (im Beispiel /80er). Außerdem muss der Host nun als Router für die Container agieren.

In diesem Fall sind weder Proxy-Funktionen, noch NAT noch Portforwarding vonnöten. Die Container können aus Sicht des Netzes als vollwertige Hosts angeschlossen werden. Mit all den dazugehörigen Vorteilen wie Erreichbarkeit, und Nachteilen wie Sicherheit.

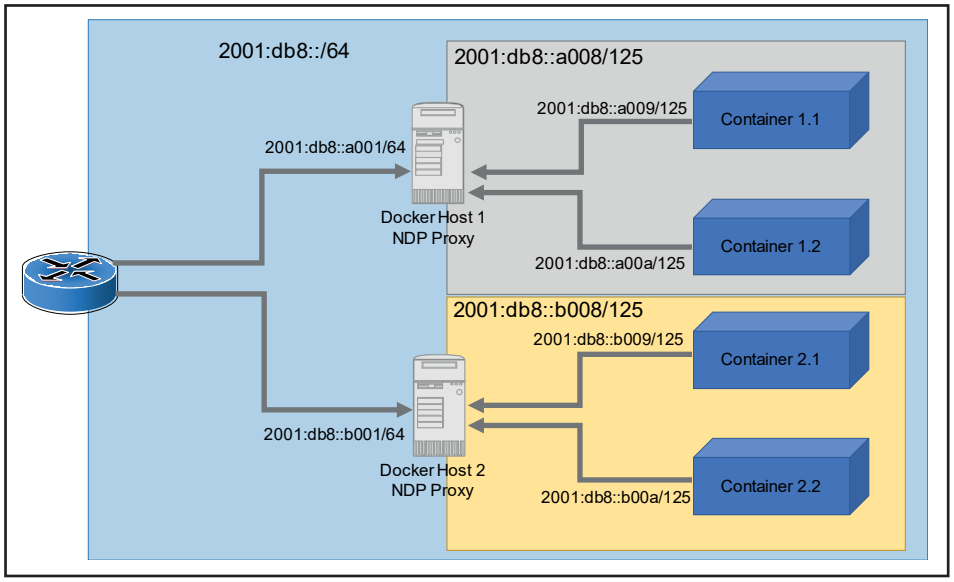


Abbildung 8: Docker Hosts mit NDP Proxy

Stehen einem ausreichend IPv4 Adressen zur Verfügung, ist dieses Verfahren prinzipiell auch auf dieses Protokoll übertragbar.

Schnittstellen und kein Ende

Die Schnittstellen zum Netz und auf Speicher sind für Container elementar wichtig, da sie die Verbindung zu Welt herstellen. Darum wird hier auch viel daran gearbeitet und es lohnt sich immer ein Blick in die Dokumentation, welche aktuell zur Verfügung stehen und wie diese eingebunden werden.

Da die Wahl der Schnittstelle von der Anwendung im Container abhängt, kann an dieser Stelle keine generelle Empfehlung gegeben werden. Was allerdings ein wenig traurig stimmt, ist, dass IPv4 und IPv6 unterschiedlich behandelt werden müssen, wenn man beides parallel betreiben möchte. Das erhöht den planerischen und auch den betrieblichen Aufwand und führt zu einer unübersichtlichen Gesamtsituation. Es steht zu hoffen, dass hierfür eine Lösung gefunden wird.

Verteilung und Orchestrierung

Bislang wurden Container und ihre Schnittstellen zum Rest der Welt vorgestellt. Für die Betrachtung aus Sicht des Netzes fehlt noch ein wesentliches Element: die Verteilung der Container auf die verschiedenen Hosts.

Dafür stehen heute verschiedene Tools zur Verfügung. Teils sind diese an einen speziellen Container-Typ gebunden,

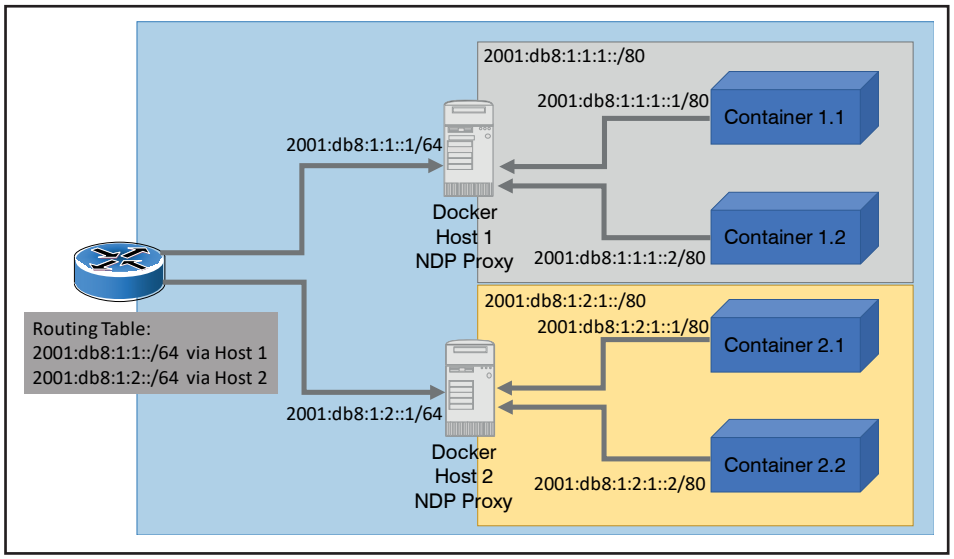


Abbildung 9: Docker mit Routed IPv6

teils nicht. Docker Swarm zum Beispiel ist eine Orchestrierungstool für Docker Container, wohingegen Kubernetes da sehr viel offener ist. Auch verschiedene Cloud-Provider bieten eigene Orchestrierungstools für Container an, dazu gehören bspw. Amazon, Microsoft oder Google. Oft beruhen diese jedoch auf anderen Tools und wurden „nur“ für die spezielle Cloud optimiert. Neben der Frage, für welche Container-Typen sie geeignet sind, unterscheiden sich diese Tools auch im Funktionsumfang und damit in der Komplexität der Bedienung. So gilt Kubernetes als sehr umfangreich aber auch als hochkomplex, wohingegen Docker Swarm eher (noch) eine vergleichsweise einfach zu handelnde Variante ist.

Da Orchestrierungstools nicht im Fokus dieses Artikels stehen und es in Hinblick auf die Konsequenzen für den Netzwerktraffic ausreicht, das generelle Konzept zu erklären, wird im Folgenden nur auf die Funktionsweise von Docker Swarm eingegangen.

Bei der Orchestrierung geht es darum, die Container möglichst optimal auf die vorhandenen Host-Systeme zu verteilen. Das Problem dabei liegt im Wort „optimal“. Da durchaus mehrere Tausend oder gar Millionen Container gleichzeitig in einem Rechenzentrum bzw. in einer Cloud laufen können, müssen sie mehr oder weniger automatisch nach einem vordefinierten Regelwerk verteilt werden. Es ist nicht denkbar händisch ein Design zu entwerfen, das wirklich optimal wäre. Neben der Anzahl laufender Container steht dem auch die hohe Dynamik entgegen, die mit der Technologie einhergeht.

Stellt sich also die Frage: welche Möglichkeiten stehen zur Verfügung ein Regelwerk zu erstellen, nach dem Container automatisch verteilt werden können? Im Falle von Docker Swarm gibt es dafür drei Oberklassen, die sich wiederum in Unterklassen aufteilen lassen:

1. Klassifizierung von Hosts-Systemen
2. Klassifizierung von Containern
3. Verteilungsalgorithmus

Klassifizierung der Hosts

Die Hosts können nach verschiedenen Eigenschaften klassifiziert werden. Docker nennt das „Node-Filter“. Per default gibt es drei Node-Filter:

1. Betriebssystem
2. Kernelversion
3. Storage-Driver

Da es Docker-Container mittlerweile nicht nur für Linux, sondern auch für macOS und Windows gibt, kann es notwendig sein, dass ein bestimmter Container auf einem Host läuft, der ein bestimmtes Betriebssystem hat. Der Grund ist, dass sich Container und Host den Kernel teilen. Das ist auch der Grund, warum Hosts nach Kernelversionen klassifiziert werden können. Benötigt ein Container eine Mindestversion des Linux Kernels, kann das über diesen Filter definiert werden.

Neben diesen Default-Filtern ist es möglich eigene Filter zu definieren. So können Hosts beispielsweise auch mit Länder- oder Regions-Tags versehen werden, die als Filter dienen können. Will man z.B. sicherstellen, dass ein Container später auf jeden Fall im EU-Raum gestartet wird, muss man die Hosts entsprechen taggen und kann bei der Container Verteilung auf diesen Tag zurück greifen. Ebenso wäre es möglich nach Entwicklung, Test und Betrieb zu unterscheiden, um sicher zu stellen, dass ein Host, auf dem eine kritische Betriebsanwendung läuft, nicht plötzlich durch einen Performance-Test blockiert wird, nur weil ein Test-Container darauf gelandet ist.

Health-Filter

Ein spezieller Node-Filter ist der Health-Filter. Anders als die anderen Node-Filter wird dieser automatisch vom Swarm gepflegt und soll gewährleisten, dass „gesunde“ Hosts von solchen mit Problemen unterschieden werden können.

Generell gilt zunächst einmal jeder Host in einem Swarm als gesund. Um den Health-Status auf „krank“ zu ändern gibt es zwei Kriterien:

1. Der Host ist gar nicht mehr vom Swarm zu erreichen
   In diesem Fall wird er als „tot“ betrachtet. Da der Swarm ihn nicht erreichen kann, ist es offensichtlich nicht möglich dort Container zu starten oder dort laufende zu verwalten.

2. Erreichbarkeitsprobleme
   Jeder Host muss sich regelmäßig im Swarm melden. Wenn diese Meldung nicht regelmäßig erfolgt – aber auch nicht ausbleibt – gilt er als „krank“. Da er grundsätzlich erreicht werden kann, ist er nicht „tot“ aber offensichtlich hat er Probleme.

Das Health-Kriterium kann für die Verteilung von Containern herangezogen werden. So kann man festlegen, dass be-

stimmte Container nur auf gesunden Hosts laufen und andere, die nur für Tests von Praktikanten gedacht sind, auch auf ungesunden laufen dürfen.

Container-Filter

Es reicht nicht, nur die Hosts zu klassifizieren, natürlich muss das auch für die Container selbst möglich sein. Wie bei den Hosts stehen auch hier verschiedene Varianten zur Verfügung:

1. Port-Filter
   Port-Filter bedeutet, dass ein Container nur auf einem Host laufen darf, auf dem bestimmte Ports für das Portforwarding noch zur Verfügung stehen.
   Beispielsweise ist es nicht sinnvoll zwei Webserver auf ein und demselben Host laufen zu lassen, wenn beide Port 80 zur Verfügung stellen wollen.

2. Dependency-Filter
   Dieser Filter gibt an, dass es Abhängigkeiten gibt, die der Host erfüllen muss, damit der Container arbeiten kann. Das kann eine Netzwerkverbindung sein oder Zugriff auf bestimmten freigegebenen Speicher.

3. Affinity-Filter
   Wie schon bei den Nodes gibt es auch bei den Containern einen relativ frei nutzbaren Filter. Bei den Containern heißt dieser „Affinity“. Die einfachste Form des Affinity Filters ist eine „Affinität“ zu einem bestimmten Host. Damit kann man festlegen, dass ein Container nur auf einem ganz bestimmten Host laufen darf, oder auch nur auf einer speziellen Gruppe.

   Ein weiterer Affinity-Filter wäre, dass ein Container nur auf einem Host gestartet werden soll, auf dem das dazugehörige Image bereits vorhanden ist. Das macht dann Sinn, wenn man unnötigen Netzwerktraffic verhindern will, der durch die Übertragung der Images zwangsläufig entsteht.

Der freieste Filtermechansimus ist aber wie schon bei Hosts, die eigene Klassifizierung, dazu können die Container gelabeld werden. Das kann man beispielsweise einsetzen um sicher zu stellen, dass eine Webanwendung nur dann gestartet werden kann, wenn auf dem Host die dazugehörige Datenbankanwendung bereits läuft.

Beispiel eines Filters

Abbildung 10 zeigt ein Beispiel für eine automatisierte Verteilung von Containern:
Eine Webanwendung wurde in diesem Fall containerisiert und soll nun produktiv in Betrieb gehen. Die Bedingungen sind: Port 80 muss frei sein (Container-Filter: Port) und der Host muss aus rechtlichen Gründen innerhalb der EU sein (Node-Filter: freie Gruppierung, hier „region=eu“). In diesem Fall kommen von den vorhandenen 9 Hosts noch 3 in Frage.

Verteil-Algorithmus

Und damit wären wir beim Verteil-Algorithmus, also der Frage: wie verteilt der Swarm die Container, wenn die Filter mehr als eine Option überlassen.

Dafür stehen wiederum verschieden Ansätze zur Verfügung:

- Spread
  Gleichmäßige Auslastung aller Hosts anhand der RAM- und CPU-Kenndaten (nicht Netzwerk oder andere I/O Schnittstellen)

- BinPack
  Der Versuch möglichst dichte Packung unter Berücksichtigung von CPU und RAM zu erzeugen

- Random
  Zufällige Verteilung ohne Beachtung von CPU und RAM

Jedes dieser Verfahren hat seine Vor- und Nachteile. Spread versucht durch die Verteilung die vorhandenen Ressourcen möglichst optimal auszulasten, um so die bestmögliche Performance zu erreichen. Das Problem bei Spread ist, dass es passieren kann, dass bestimmte Container nicht mehr gestartet werden können, weil nirgends ausreichen Platz ist, obwohl bei anderer Zuordnung der laufenden Container zu den Hosts das durchaus noch der Fall wäre.

Bei BinPack ist es im Grunde umgekehrt: Platz geht hier vor Performance. Solange ein Container noch auf einen Host passt, wird er auch dort gestartet.

Random wiederum ist die Hoffnung, dass der Zufall für die bestmögliche Verteilung sorgen wird.

Bedeutung für das Netz

Als VMware mit Motion kam, befürchteten einige „wild wandernde virtuelle Maschinen“ würde bald die Gigabitleitungen der Rechenzentren blockieren. Letztlich haben sich die Virtuellen Maschinen jedoch als sesshafter erwiesen als es die Germanen zur Zeit der Völkerwanderung waren.

Stellt sich die Frage, ob das bei Containern nicht genauso sein wird und man sich als Netzwerker zurücklehnen und das Spektakel aus sicherer Entfernung betrachten kann.

Die Antwort lautet schlicht: Nein! Virtuelle Maschinen sind (zumeist) mehr Maschine als virtuell, soll heißen: sie sind wo sie sind und da bleiben sie auch. Container sind hingegen keine vollständigen Anwendungen, sondern „nur“ Teile davon, Microprozesse eben. Und von daher sind sie darauf angewiesen mit anderen Microprozessen zu kommunizieren, um gemeinsam die Anwendung zu erzeugen. Diese Kommunikation läuft über IP und anders als bei klassischen Anwendungen nicht über eine Hostinterne IP-Kommunikation, sondern zu anderen Containern. Diese können je nach Orchestrierung „ganz woanders“ sein. Somit entsteht Netzwerktraffic, den es bislang in dieser Häufigkeit nicht gab. Dabei steht zu befürchten, dass nicht die Bandbreite, sondern das Delay zu einem Problem wird.

Netzwerker sind also gut beraten, sich frühzeitig mit dieser Technik vertraut zu machen und bei dem Entwurf der Orchestrierungsregeln aktiv mit zu arbeiten.

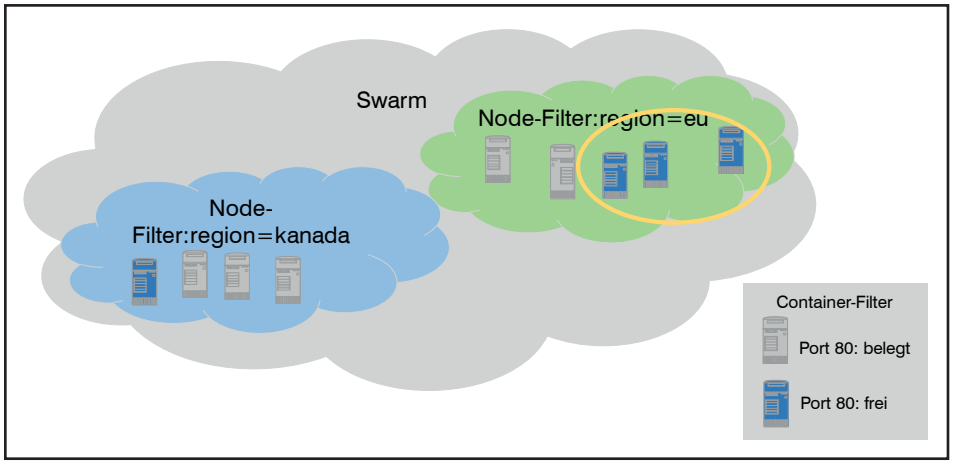


Abbildung 10: Beispiel für die Verteilung von Containern

Standpunkt

WLAN Clients senden weiter als man denkt!

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

Ein fahrerloses Transportfahrzeug (FTF) im Testbetrieb bei einem meiner Kunden: Regelmäßig kommt es zu Störungen und das FTF bleibt unvermittelt stehen. Das Fahrzeug verfügt über allerhand Sensoren, um seinen Weg zu bestimmen. Es fährt also eigentlich autonom. Aber zur Einbindung in eine Fertigungsumgebung ist eine WLAN-Anbindung vonnöten. Und hierfür macht der Hersteller genaue Vorgaben: 95% aller Anfragen müssen spätestens nach 200 Millisekunden beantwortet werden. Und 99% aller Anfragen spätestens nach einer halben Sekunde. Aufregend, wenn man dieses FTF in ein vorhandenes WLAN integrieren möchte, in dem es hunderte Clients und zig Anwendungen gibt…

Wie dem auch sei, ich habe mir die Sache genauer angesehen. Was passiert im WLAN, wenn das FTF stehen bleibt? Hierzu habe ich Pakete sowohl im WLAN, d.h. auf der Luftschnittstelle, als auch im LAN zwischen Access Point und WLAN Controller aufgezeichnet. Die Analyse ergab:

- Es traten immer wieder Paketverluste auf. Dabei gingen ausschließlich Pakete verloren, die vom Access Point zum FTF gesendet wurden. Der Access Point hat dagegen alle Pakete des FTF empfangen.
- Der WLAN-Adapter des FTF „klebte“ immer am selben Access Point. Mit anderen Worten, obwohl offensichtlich die Empfangsqualität schlecht war, hat der WLAN-Adapter des FTF nicht versucht, ein Handover (Roaming) zu einem anderen Access Point zu initiieren.
- Das WLAN (2,4 GHz) ist so eingerichtet, dass Bitraten von 11 Mbit/s und darüber zugelassen sind. Langsamere Bitraten sind nicht erlaubt. Dennoch sendete der WLAN-Adapter des FTF teilweise mit der langsamsten Rate, d.h. mit 1 Mbit/s. Diese Pakete wurden vom Access Point ebenfalls mit 1 Mbit/s beantwortet (ACK).

Letzteres kam mir zunächst komisch vor. Wie kann der Access Point dem FTF mit 1 Mbit/s antworten, wo seine Mindest-Rate doch 11 Mbit/s ist? Ich habe daraufhin den WLAN-Standard IEEE 802.11-2012 gewälzt und folgendes herausgefunden: ACK Frames müssen mit einer Datenrate gesendet werden, die kleiner oder gleich der Rate des zu bestätigenden Frame ist. Klingt logisch. Aber warum sendet das FTF überhaupt mit 1 Mbit/s? Denn im Standard steht auch, dass eine Station nur die Bitraten verwenden soll, die ihm vom Empfänger – hier dem Access Point – mitgeteilt werden.

Die Frage habe ich (bisher) nicht beantworten können. Hierfür ist wohl ein Gespräch mit dem Entwickler des WLAN-Adapters nötig, was sich im Einzelfall kaum organisieren lässt. Ungeachtet dessen haben wir hier eine Erklärung für das „Kleben“ des FTF am WLAN. Aus Sicht des FTF ist alles in Ordnung, denn seine Pakete werden vom Access Point bestätigt. Nur die Gegenrichtung scheitert, weil hohe Bitraten nicht so weit reichen wie niedrige.

Und noch etwas hat sich bei der Untersuchung herausgestellt. Die Access Points werden in der Standardeinstellung mit automatischer Leistungsregelung betrieben. Da sie sich gegenseitig sehr gut hören, haben sie die Leistung sehr weit heruntergedreht: bis auf 1 Milliwatt. Die Client-Adapter senden aber nach wie vor mit voller Sendeleistung, also sicher mit mehr als 10 Milliwatt. Auch dies wäre eine Erklärung für die asymmetrische Kommunikation.

Was folgt daraus? Unsere generelle Empfehlung, die Bitraten im WLAN zu homogenisieren, also die langsamen Raten abzuschalten, greift zu kurz, wenn die Clients nicht mitspielen. Im geschilderten Fall besteht der Workaround darin, bei den FTF nur noch IEEE 802.11g/n zuzulassen. Immerhin senden sie dann mit mindestens 6 Mbit/s. Und die Sendeleistung der Access Points muss in derselben Größenordnung liegen wie die der Clients.

Und noch ein Fazit ziehe ich: Sie sollten sich trauen, Ihren Lieferanten Vorgaben bezüglich der Eigenschaften und des Verhaltens von WLAN-Endgeräten machen. Man könnte sich einen Anforderungskatalog für WLAN Clients ausdenken!

Aktuelles Seminar

Leistungsfähige, skalierbare, hochverfügbare, sichere und wirtschaftliche Speicherlösungen 29.05. - 30.05.2017 in Frankfurt

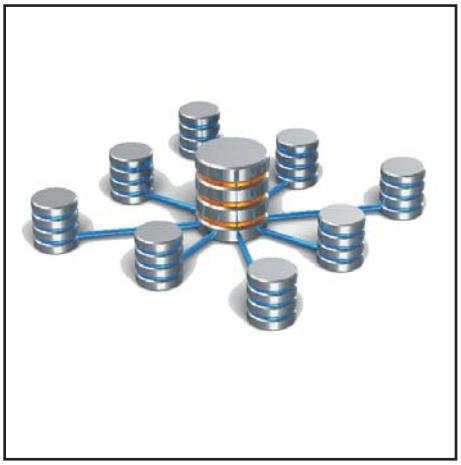
Die ComConsult Akademie veranstaltet vom 29.05. bis 30.05.2017 ihr Seminar "Leistungsfähige, skalierbare, hochverfügbare, sichere und wirtschaftliche Speicherlösungen" in Frankfurt.

Der Speichermarkt befindet sich im Umbruch: Neue Flash-Speicher bieten bisher unerreichte Leistungsfähigkeit bei stetig sinkenden Investitions- und Betriebskosten. Durch die Virtualisierung von Direct Attached Storage steht mittlerweile eine ausgereifte Technologie zur Verfügung, die zu traditionellen Storage Area Networks konkurrenzfähig ist. Außerdem nimmt die Nutzung von Public-Cloud-Speicher aufgrund verbesserter Sicherheit und optimierter Möglichkeiten zur Anbindung rapide zu.

Im Seminar werden die unterschiedlichen Technologien vorgestellt und, basierend auf einem pragmatischen Best-Practice-Ansatz, Szenarien beschrieben um für jede Organisation das Optimum zu erreichen.

In diesem Seminar lernen Sie

- Speichertechnologien – Hochleistungs-NV-RAM und SSD und moderne HDDs: Lösungen passend für jedes Einsatzgebiet
- Virtualisierter Direct Attached Storage: Ist eine Effizienzsteigerung bei fallenden Kosten möglich? Werden traditionelle SANs langfristig überflüssig?



- Speicher in der Cloud: leistungsfähige und sichere Übertragung der Daten, Möglichkeiten zur sicheren Speicherung, Diskussion verschiedener Einsatzszenarien
- Skalierbarkeit von Speichersystemen: die optimalen Lösungen für Scale-Up- und Scale-Out Ansätze
- Methoden zur effektiven Datenhaltung im Überblick: Thin Provisioning, Storage Tiering, Kompression, Deduplizierung
- Hochverfügbarkeit und Ausfallsicherheit: Möglichkeiten und Grenzen bei der (geo-)redundanten Verteilung von Daten
- Migration: Bewährte Ansätze für die Einführung neuer Server- und Speicherstrukturen, revisionssichere Datenlöschung bei der Ablösung von Speichersystemen
- Das passende Transportprotokoll für jedes Anwendungsgebiet: Fibre-Channel, Fibre Channel over Ethernet, iSCSI, Network File System und Server Message Block im Vergleich
- Datensicherheit: Mechanismen zum sicheren Betrieb von Speichernetzen und Network Attached Storage, Verschlüsselte Datenhaltung und -Übertragung
- Management- und Analysewerkzeuge für Speicherumgebungen
- Datensicherung: Sicherungsmedien Disk und Tape, Sicherungsverfahren

Das Seminar wendet sich an Planer und Betreiber von Speicherlösungen, die einen detaillierten Einblick in aktuelle Speichertechnologien bekommen möchten. Ziel ist es, den Teilnehmern eine Informationsgrundlage zu vermitteln, die es ihnen ermöglicht bestehende Speicherinfrastrukturen zu optimieren und neue Systeme zukunftssicher aufzubauen. Grundlegende Kenntnisse über Speicherlösungen werden dabei vorausgesetzt. Anhand von Praxis-Beispielen aus dem Planungsalltag werden die technischen Details zusammen mit den Erfahrungen der Teilnehmer diskutiert.

Anmeldung an kundenservice@comonsult-research.de

Leistungsfähige, skalierbare, hochverfügbare, sichere und wirtschaftliche Speicherlösungen

Ich buche das Seminar
Leistungsfähige, skalierbare, hochverfügbare, sichere und wirtschaftliche Speicherlösungen
29.05. - 30.05.2017 in Frankfurt

☐ zum Preis von € 1.590,-- netto

☐ Bitte buchen Sie mir ein Hotelzimmer

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

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

WLAN

Was bringt der neue WLAN-Standard?

Fortsetzung von Seite 1

Dr.-Ing. Joachim Wetzlar ist seit mehr denn 20 Jahren Senior Consultant der ComConsult Beratung und Planung GmbH und leitet dort das Competence Center „Data Center“. Er verfügt über einen erheblichen Erfahrungsschatz im praktischen Umgang mit Netzkomponenten und Serversystemen. Seine tiefen Detailkenntnisse der Kommunikations-Protokolle und entsprechender Messtechnik haben ihn in den zurückliegenden Jahren zahlreiche komplexe Fehlersituationen erfolgreich lösen lassen. Neben seiner Tätigkeit als Trouble-Shooter führt Herr Dr. Wetzlar als Projektleiter und Senior Consultant regelmäßig Netzwerk- WLAN- und RZ-Redesigns durch. Besucher von Seminaren und Kongressen schätzen ihn als kompetenten und lebendigen Referenten mit hohem Praxisbezug.

Der neue Standard wurde am 14. Dezember 2016 veröffentlicht. Er umfasst nun 3.237 Seiten. Glaubt man der Inhaltsangabe, wurden verschiedene Berichtigungen eingebracht und einiges klarer dargestellt. Es wurden verschiedene nicht näher spezifizierte Erweiterungen des Medienzugangsverfahrens (MAC Layer) und der Übertragungsverfahren (PHY Layer) eingebracht. Insbesondere aber hat man die „Amendments“ 1 bis 5 in den Standard eingearbeitet.

Was sind „Amendments“? Zu Deutsch Änderungen oder Berichtigungen. In der Tat werden viele der Neuerungen, die von den Arbeitsgruppen des IEEE – den Task Groups – eingebracht werden, als Änderungen des bestehenden Standards formuliert. Die entsprechenden Dokumente enthalten zusätzliche Kapitel und darüber hinaus Änderungen an bestehenden Abschnitten. Diese Änderungen werden tatsächlich so dargestellt, als hätte man im Textprogramm die Überarbeitungsmarkierungen aktiviert. Man findet durchgestrichene Passagen und hinzugefügte.

Somit ist also das Zusammenstellen eines neuen IEEE-Standards eher eine redaktionelle Tätigkeit als eine inhaltliche. Die folgenden fünf Amendments aus den Jahren 2012 und 2013 wurden jetzt eingearbeitet:

- Amendment 1: Prioritization of Management Frames (IEEE 802.11ae) stellt sicher, dass die Anmeldung am WLAN, das Handover und weitere Vorgänge mit höherer Betriebssicherheit als bisher erfolgen können. Hierfür wird Quality of Service (QoS) für die entsprechenden Management Frames eingeführt.

- Amendment 2: MAC Enhancements for Robust Audio Video Streaming (IEEE 802.11aa). Dieses Dokument führt spezielle Multicast-Modi ein, um die Übertragung von Videos an mobile Endgeräte zu verbessern. Ein Element ist der „Trick“, Multicasts mehrfach auszusenden, um die Wahrscheinlichkeit für einen fehlerfreien Empfang zu erhöhen. Hierüber haben wir im Januar 2015 an dieser Stelle berichtet.

- Amendment 3: Enhancements for Very High Throughput in the 60 GHz Band (IEEE 802.11ad). Hierbei handelt es sich um das WLAN im Millimeterwellenbereich, über das wir an dieser Stelle bereits mehrfach berichtet haben.

- Amendment 4: Enhancements for Very High Throughput for Operation in Bands below 6 GHz (IEEE 802.11ac). Damit ist die inzwischen allseits bekannte und verfügbare Technik der hohen Bitraten im 5-GHz-Band gemeint.

- Amendment 5: Television White Spaces (TVWS) Operation (IEEE 802.11af). Ähnlich wie Wi-Fi HaLow (IEEE 802.11ah) handelt es sich um eine Technik für Frequenzen unterhalb von 1 GHz. Es werden schmalere Bandbreiten und entsprechend geringere Bitraten spezifiziert.

Aus Sicht eines Betreibers eines Enterprise WLAN bringt der Standard also tatsächlich nichts neues. Insbesondere Very High Throughput (VHT) von 11ac ist ja bereits verfügbar. Und der Rest ist nicht wirklich relevant. Viel interessanter ist, an welchen Amendments das IEEE derzeit arbeitet. In der Folge möchte ich auf die Arbeit der Task Groups 11ax und 11ay eingehen. Und ich wage einen Ausblick auf die Beziehung zwischen WLAN und Mobilfunk.

IEEE 802.11ax: High Efficiency WLAN (HEW)

HEW wird vom IEEE als der Nachfolger für IEEE 802.11n und 11ac gesehen. Man erwartet, dass der Standard (bzw. das Amendment) in 2019 veröffentlicht wird. Derzeit arbeitet man an der ersten Version, dem Draft 1.0, der leider noch nicht verfügbar ist. Daher habe ich verschiedene andere Quellen zu Rate gezogen, insbesondere Artikel von Personen bzw. Unternehmen, die in irgendeiner Form an der Entwicklung des Standards beteiligt sind. Auf Basis dieser Informationen lässt sich inzwischen ein ziemlich klares Bild der neuen Techniken zeichnen, die mit HEW ins WLAN einziehen werden.

„Efficiency“, also Effizienz ist es, was die Entwickler des Standards erreichen wollen. Effizienz bedeutet, dass vor allem aus der Sicht des Anwenders die Effizienz größer werden soll. Sie können sich vorstellen, dass Bitrate alleine wahrscheinlich nicht der Schlüssel zum Erfolg ist. Darüber hinaus wissen Sie, dass die Möglichkeiten mit dem VHT WLAN (IEEE 802.11ac) bereits ziemlich weit ausgereizt wurden. In früheren Artikeln habe ich gezeigt, dass man mit VHT nicht besonders weit kommt. Ein Access Point pro Büro ist die Richtschnur.

Und nun stellen Sie sich ein Fußballstadion mit einer fünfstelligen Anzahl von Zuschauern vor! Fast alle haben ein Smartphone und möchten darüber während des Spiels online und in Echtzeit informiert werden. Wofür man das braucht, kann ich mir nicht wirklich vorstellen, aber das tut hier nichts zur Sache. Jedenfalls muss das WLAN dergestalt sein, dass der einzelne Anwender eine brauchbare Reaktionszeit beim Zugriff auf Inhalte erlebt.

Ein wesentliches Problem bei allen bisherigen WLAN-Varianten ist, dass Stationen sich das Medium „Luft“ teilen. Es muss also nacheinander gesendet werden. Im besagten Stadion, wo Anwender so dicht stehen, dass sie sich gegenseitig berühren, bleibt für den einzelnen nicht viel Bi-

trate übrig. Eigentlich stören sich alle Endgeräte und die Access Points nur gegenseitig. Man braucht also Techniken, um mehr Stationen ungestört parallel nebeneinander betreiben zu können. 3 Kanäle im 2,4-GHz-Band und 16 auf 5 GHz reichen dazu ganz sicher nicht.

Multi-User MIMO

Erste Ansätze für Parallelisierung gab es bereits im VHT WLAN. Das Schlüsselwort lautet „Multi-User". Multi-User MIMO ermöglicht es einem Access Point (auf wundersame Weise) gleichzeitig Daten an mehrere Stationen zu senden. Ein Access Point, der MIMO mit beispielsweise vier Spatial Streams unterstützt, kann diese vier Streams auf zwei Stationen aufteilen. Darüber hinaus kann er die Streams in unterschiedliche Richtungen aussenden, um jede der Stationen optimal zu erreichen. IEEE 802.11ac nennt das „Downlink Multi-User MIMO (DL-MU-MIMO) Beamforming". Das Verfahren wird bekanntlich ab Produkten mit 11ac „Wave 2" unterstützt.

Grundsätzlich ist das eine gute Idee. Denn wahrscheinlich unterstützen die wenigsten WLAN-Stationen so viele Spatial Streams wie der Access Point. Das gilt vor allem im Stadion. Smartphones bieten zum einen zu wenig Platz, um viele Antennen unterbringen zu können. Zum anderen sparen weniger Sender und geringere Bitraten Strom, denn Batteriekapazität ist bei Smartphones ein teures Gut.

Der Downlink, also die Richtung vom Access Point zur Station, ist natürlich nur die „halbe Miete". IEEE 802.11ax wird zusätzlich MIMO für den Uplink ermöglichen. Damit die Stationen gleichzeitig senden können, müssen sie vom Access Point koordiniert werden. Zu diesem Zweck sendet der Access Point so genannte Trigger Frames an die Stationen, die daraufhin mit den jeweiligen Daten antworten (vgl. Abbildung 1).

Modifiziertes OFDM

Bekanntlich wird bereits seit fast 20 Jahren im WLAN das Verfahren „Orthogonal Frequency-Division Multiplexing" (OFDM) eingesetzt. Hierbei werden die Bits nicht nacheinander auf einen einzigen Träger aufmoduliert sondern das Signal besteht aus mehreren „Unterträgern", die parallel mit Bits moduliert werden. Das Verfahren entspricht im Prinzip der Parallelschnittstelle, die Sie von Ihren alten PCs kennen (der 25polige Subminiatur-D-Stecker). Dort gab es 8 Datenleitungen, über die sich gleichzeitig ein ganzes Byte übertragen ließ.

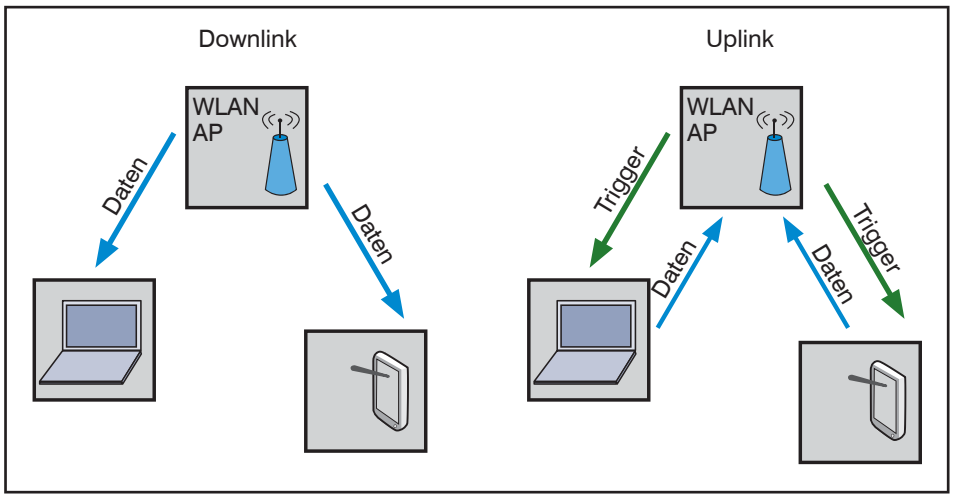


Abbildung 1: MU-MIMO im Downlink und Uplink

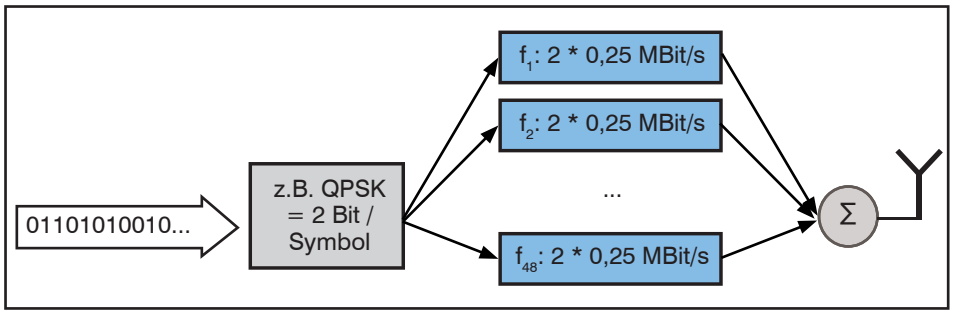


Abbildung 2: Zum Prinzip von OFDM

Bereits in IEEE 802.11a wurde OFDM mit 48 Unterträgern realisiert. Die Gruppe aus Bits, die sich mittels OFDM gleichzeitig übertragen lässt, nennt man „Symbol". Bei 11a besteht ein Symbol somit aus Vielfachen von 48 Bits, je nach Modulation des Unterträgers. Abbildung 2 illustriert dieses Konzept. Setzt man eine zweiwertige Modulation ein (binäre Phasenmodulation, BPSK), sind es genau 48. Setzt man eine vierwertige ein (quaternäre Phasenmodulation, QPSK), sind es 96 und so fort. Bekanntlich hat man die Wertigkeit der Modulation im Laufe der Zeit immer weiter gesteigert. Bei IEEE 802.11a und 11n war das Maximum die 64wertige Quadratur-Amplitudenmodulation (64-QAM). Mit 11ac kam eine 256wertige hinzu und 11ax wird sogar die 1024-QAM unterstützen.

Bei allen OFDM-Varianten ist bisher eines gleich geblieben: Der Abstand der Unterträger. Er beträgt genau 312,5 kHz. Daraus ergibt sich eine Symboldauer von 3,2 μs. Tatsächlich wird diese Zeit nicht vollständig für die Datenübertragung ausgenutzt sondern es gibt zwischen den Symbolen eine kurze Pause, den so genannten Schutzabstand (bzw. Guard Interval). Ursprünglich beträgt der Schutzabstand 0,8 μs, wodurch sich die nutzbare Symbolrate zu 250.000 pro Sekunde ergibt (der in Abbildung 2 dargestellte Wert). Mit 11n hat man einen kürzeren Schutzabstand eingeführt (0,4 μs), und man konnte dadurch die nutzbare Symbolrate um 20% erhöhen.

Wozu ist der Schutzabstand gut? In der Tat steckt im Schutzabstand der bahnbrechende Vorteil des OFDM gegenüber anderen Modulationstechniken. Funksignale gelangen meist auf mehreren Wegen zum Empfänger, da sie zwischenzeitlich an allerlei leitenden Elementen reflektiert werden. die Wege sind unterschiedlich lang, die reflektierten Signale erreichen also den Empfänger zu unterschiedlichen Zeiten. Der Schutzabstand sorgt dafür, dass sich zwei aufeinanderfolgende Symbole trotz Mehrwegeempfang nicht gegenseitig überlagern und stören. 0,4 μs entsprechen einem Weg von ca. 120 Metern. In normalen WLAN-Umgebungen sind Wegeunterschiede deutlich kürzer. OFDM ist also gegenüber Mehrwegeempfang sehr robust. Zum Vergleich: In WLAN gemäß IEEE 802.11b mit 11 Mbit/s beträgt die Symboldauer nur 0,25 μs, weniger als ein Zehntel der OFDM-Symboldauer. Trotz ihrer geringen Datenrate sind diese WLANs wesentlich anfälliger auf Mehrwegeempfang.

Betrachten wir noch einmal das Fußball-

stadion: Sie erkennen sofort, dass hier die genannten 120 Meter eine vergleichsweise kurze Strecke sind. Ein größerer Schutzabstand wäre also wünschenswert und nützlich. Und genau dort setzt HEW an: Die Symboldauer wird auf 12,8 µs vervierfacht. Gleichzeitig wächst das Schutzintervall auf 3,2 µs an. Das entspricht fast 1000 Meter Wegeunterschied, ohne dass sich aufeinanderfolgende Symbole überlagern. Es sind aber auch 0,8 und 1,6 µs Schutzabstand erlaubt, was im Gegenzug die nutzbare Bitrate etwas erhöht.

Die Vervierfachung der Symboldauer hat einen weiteren Nebeneffekt, den ich mit Abbildung 3 zu erklären versuche. Der Abstand der Unterträger schrumpft auf ein Viertel. Gleichzeitig hat der einzelne Unterträger eine geringere Bandbreite. Die Unterträger können dadurch näher an die Grenze des Funkkanals heranrücken, ohne Störungen im Nachbarkanal hervorzurufen. Im oberen Diagramm der Abbildung 3 erkennen Sie 7 Unterträger, im unteren sind es 31, also mehr als das Vierfache. Die Abbildung dient nur der Illustration. In Wirklichkeit nutzt VHT bei 40 MHz Kanalbandbreite 108 Unterträger, bei 160 MHz sind es 468. Die entsprechenden Anzahlen bei HEW sind 468 respektive 1960 Unterträger.

Beides – der im Vergleich zur Symboldauer geringere mögliche Schutzabstand und die höhere Anzahl nutzbarer Unterträger des OFDM – ergibt bei HEW etwas höhere Brutto-Bitraten als bei VHT. Abbildung 4 stellt das für die Kanalbandbreiten 40 und 160 MHz bei einem Spatial Stream gegenüber. Berücksichtigt man außerdem, dass HEW mit der 1024-QAM 10 Bit pro Unterträger und Symbol übertragen kann, ergibt sich als maximale Bitrate pro Stream 1,2 Gbit/s. Mit 8 Spatial Streams werden somit sagenhafte 10 Gbit/s fast erreicht.

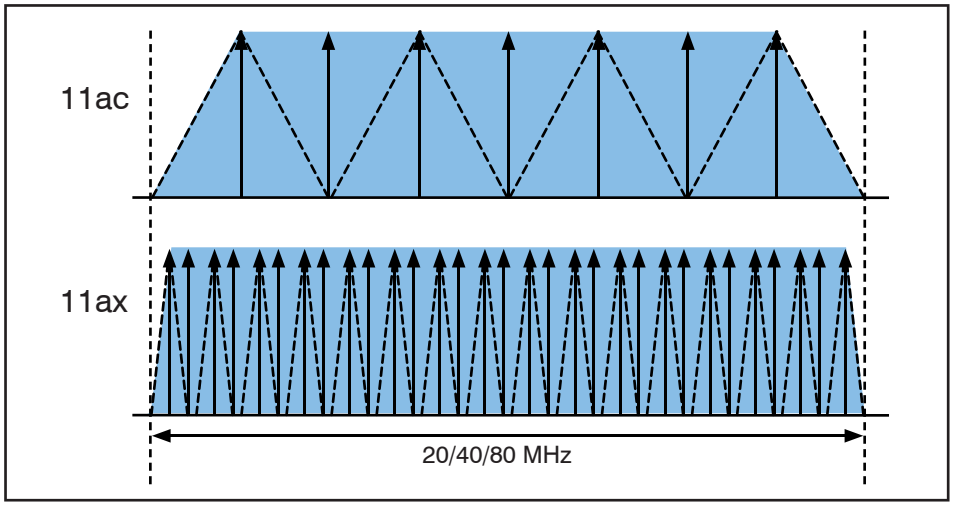


Abbildung 3: Unterträger bei 11ac und 11ax (schematisch)

MCS	Modulation	Code-Rate	802.11ac 40 MHz (MBit/s)	802.11ax 40 MHz (MBit/s)	802.11ac 160 MHz (MBit/s)	802.11ax 160 MHz (MBit/s)
0	BPSK	1/2	15,0	17,2	65,0	72,1
1	QPSK	1/2	30,0	34,4	130,0	144,1
2	QPSK	3/3	45,0	51,6	195,0	216,2
3	16-QAM	1/2	60,0	68,8	260,0	288,2
4	16-QAM	2/3	90,0	103,2	390,0	432,2
5	64-QAM	2/3	120,0	137,7	520,0	576,5
6	64-QAM	3/4	135,0	154,9	585,0	648,5
7	64-QAM	5/6	150,0	172,0	650,0	720,6
8	256-QAM	3/4	180,0	206,5	780,0	864,7
9	256-QAM	5/6	200,0	229,4	866,7	960,8
10	1024-QAM	3/4	-	258,1	-	1080,9
11	1024-QAM	5/6	-	286,7	-	1201,0

Abbildung 4: Brutto-Bitraten bei einem Spatial Stream IEEE 802.11ac und 11ax im Vergleich

OFDMA

Das zusätzliche „A“ hinter OFDM hat es in sich. Die Abkürzung bedeutet „Orthogonal Frequency-Division Multiple Access”. Vergleichbar zu MU-MIMO wird nun von HEW die Möglichkeit vorgesehen, dass mehrere Stationen gleichzeitig in einem OFDM-System senden können. Dazu teilt man die Unterträger in mehrere Gruppen auf, so genannte Resource Units (RU). Das ist in Abbildung 5 dargestellt. In Wirklichkeit kann eine RU 24, 48, 102, 234, 468 oder 980 Unterträger umfassen.

Damit ist offensichtlich eine sinnvolle Verteilung der Unterträger auf die Stationen entsprechend der zu übertragenen Paketgrößen möglich. Ziel ist es, dass alle gleichzeitig übertragenen Pakete etwa gleich lange dauern, um Verschnitt zu vermeiden. Ein kurzes Paket würde also weniger Unterträger erhalten, damit es etwa genauso lange dauert, wie ein längeres Paket, welches über viele Unterträger übertragen wird. Diese Verteilung kann pro Paket erfolgen. In jedem OFDMA-Paket (IEEE 802.11ax bezeichnet solche Pakete als HE_MU_PPDU) ist eine Information enthalten, welche Station welcher RU zugewiesen wurde und welche Modulation (z.B. QPSK, 256-QAM) und Code-Rate einzusetzen ist.

Auch in Gegenrichtung soll das Verfahren funktionieren. Ein Trigger Frame weist Stationen die RU, Modulation und Code-Rate zu. Stationen senden dann gleichzeitig mit den zugewiesenen Parametern. Woher der Access Point weiß, wie viele Daten die Stationen in ihre Pakete packen möchten, so dass eine möglichst effiziente Verteilung der Ressourcen möglich ist, habe ich noch nicht herausfinden können.

Spatial Re-Use

WLAN in Fußballstadien haben sicher ein ähnliches Problem wie WLAN in Hallen: Die Stationen hören sich zu gut. Selbst mit einer ausgeklügelten Zellplanung wird sich nicht verhindern lassen, dass mehrere Access Points auf demselben Kanal senden. Und dann ist es wahrscheinlich, dass sich deren Zellen überlappen, so wie ich es immer wieder in großen Hallen erlebe, insbesondere im 2,4-GHz-Band. Nehmen wir also eine Situation an, die in Abbildung 6 dargestellt ist. Zwei Access Points haben den selben Arbeitskanal und ihre Zellen überlappen sich. Eine Station „B“ befindet sich im Überlappungsbereich. „B“ ist an Access Point „2“ assoziiert.

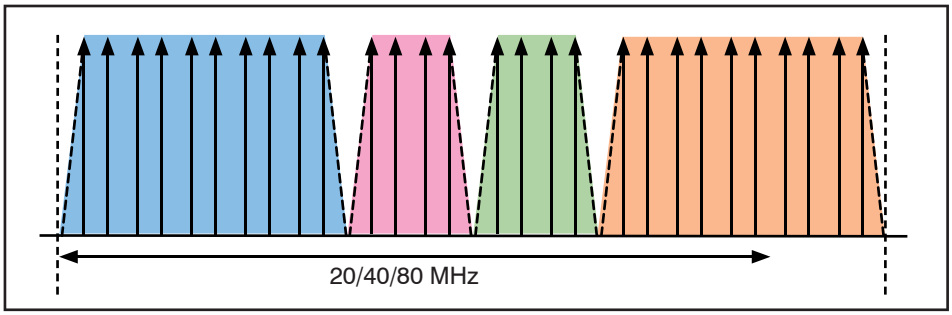


Abbildung 5: Aufteilung der Unterträger auf Endgeräte bei OFDMA (schematisch)

Access Point „1“ sendet gerade Daten an Station „A“. Das hören alle Stationen in der Funkzelle. Selbstverständlich hört auch „B“ diese Aussendung und muss daher warten, bis die Aussendung beendet ist, bevor sie ihre Daten an Access Point „2“ senden kann.

Spatial Re-Use ermöglicht nun etwas ungewohnt Neues: „B“ erkennt, dass die Aussendung von Access Point „1“ stammt und somit aus einer fremden Zelle kommt. Dann braucht „B“ nicht zu warten, bis das Medium frei ist, sondern kann direkt mit seiner Aussendung an Access Point „2“ beginnen. Die Hoffnung ist, dass beide Pakete ihr Ziel erreichen. Je nach Situation wird das sogar recht wahrscheinlich sein.

Zusammenfassung IEEE 802.11ax

High Efficiency WLAN (HEW) ist eine Sammlung verschiedener Ideen zur Optimierung von WLAN. Dabei tritt erstmals die reine Steigerung von Übertragungsbitrate in den Hintergrund. Dennoch, ein wenig mehr Bitrate fällt als Nebeneffekt ab: Statt 7 Gbit/s können unter optimalen Bedingungen nun knapp 10 erreicht werden.

Viel wichtiger sind die Mechanismen zur Effizienzsteigerung, die allesamt auf eine gleichzeitige Nutzung des Mediums Luft durch mehrere Stationen zielen. „Multi-User“ ist das Zauberwort. Folgende Ideen werden vorgebracht:

- Multi-User MIMO nicht nur im Download sondern auch im Upload, also von der mobilen Station zum Access Point.
- OFDMA, also Aufteilung der Unterkanäle eines OFDM-Systems auf mehrere Stationen, die dann gleichzeitig senden bzw. empfangen.
- Spatial Re-Use mit dem Ziel, dass sich überlappende Zellen desselben Kanals nicht mehr gegenseitig blockieren.

Und die gute Neuigkeit zum Schluss ist, dass IEEE 802.11ax – im Gegensatz zum Vorgänger 11ac – nicht nur auf das 5-GHz-Band beschränkt ist sondern auch auf 2,4 GHz wirken kann. Dort sind natürlich weder 80 noch 160 MHz Kanalbandbreite möglich.

IEEE 802.11ay: Enhanced Throughput for Operation in License-Exempt Bands above 45 GHz

Ein komplizierter Titel! Aber eigentlich handelt es sich „nur“ um eine Erweiterung des bestehenden „Amendment 3“ (siehe oben), besser bekannt als IEEE 802.11ad. Mit den License-Exempt Bands sind die lizenzfreien Bereiche oberhalb 45 GHz gemeint. In Deutschland ist das der Bereich von 57 bis 66 GHz, der laut Verfügung 8/2011 von der Bundesnetzagentur dafür freigegeben wurde.

Der Standard IEEE 802.11ad spezifiziert Datenübertrag bis knapp 7 GHz; Details wurden bereits im Juni 2013 an dieser Stelle beschrieben. Ich fasse daher die Funktionsweise nur kurz zusammen:

- Es werden zwei Übertragungsverfahren definiert. Eines nutzt herkömmliche Modulation eines einzelnen Trägers, das andere das OFDM. Chipsätze unterstützten bisher ausschließlich die Ein-Träger-Modulation und erzielten damit einen Brutto-Durchsatz von bis zu 4,6 Gbit/s.
- Die kurze Wellenlänge (ca. 5 mm) macht es möglich, Richtantennen auf kleinstem Raum zu implementieren. Damit wird Beamforming zur bestimmenden Technik dieser WLANs. Stationen und Access Points können ihre Antennen aufeinander ausrichten und kommunizieren dann ungestört von anderen Stationen in der Nachbarschaft. Wegen der großen Bedeutung der Richtwirkung bezeichnet der Standard das Frequenzband auch als „Directional Band“ (DBand).
- Neben der Übertragung von IP-Daten von und zu LANs werden auch andere Datenarten unterstützt. Das sind beispielsweise Display-Inhalte, Audio und USB-Schnittstellen.

Eine typische Anwendung für diese Technik ist die Wireless Docking Station. Inzwischen konnten wir das bei ComConsult in Form der Lenovo ThinkPad® WiGig Dockingstation testen. Ein schwarzer Würfel von ca. 8 cm Kantenlänge, der in der Nähe des Laptops positioniert wird. Hält man allerdings die Hand zwischen beide Geräte, ist es mit der Konnektivität schon vorbei.

Die WiGig Alliance, die sich zum Ziel gesetzt hatte, die Technik zu verbreiten, ist inzwischen in der Wi-Fi Alliance aufgegangen, meines Erachtens ein logischer Schritt. Auf der Website der Wi-Fi Alliance findet man derzeit 5 Geräte, die das Zer-

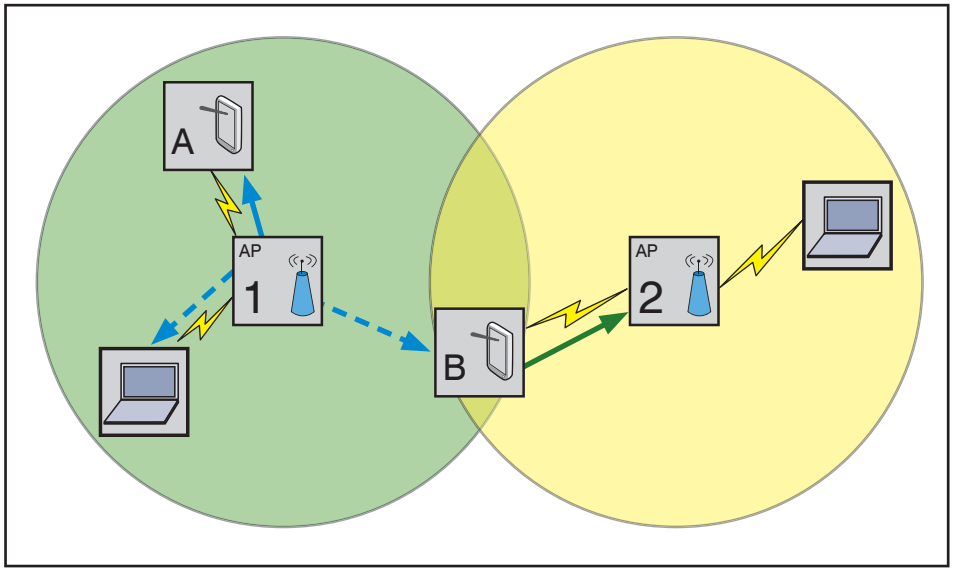


Abbildung 6: Illustration des Spatial Re-Use

tifikat Wi-Fi CERTIFIED WiGig™ tragen: Ein Laptop und vier Chipsätze verschiedener Hersteller. Die genannte Docking Station ist nicht darunter. Inzwischen gibt es sogar einen Heimrouter von TP-Link mit 60-GHz-WLAN.

Die IEEE Task Group 802.11ay will nun die Technik für Bitraten von bis zu 20 Gbit/s weiterentwickeln. Ein Draft 1.0 wird für Sommer 2017 erwartet, der fertige Standard Ende 2019. Einige technische Details konnte ich bereits herausfinden:

- Channel Bonding: Der alte Trick, mit dem auch die „niederfrequenten“ WLANs höhere Bitrate erzielen, ist das Zusammenfassen von Kanälen. Auf 60 GHz wird es die Möglichkeit geben, zwei, drei oder vier Kanäle zusammenzufassen, wodurch sich in Europa die Möglichkeiten gemäß Abbildung 7 ergeben.

- MIMO: Bisher war die Mehrantennentechnik des Multiple Input Multiple Output im DBand nicht vorgesehen. Jetzt kommt es doch. Bekanntlich setzt MIMO Mehrwegeempfang voraus. Richtantennen unterbinden das jedoch. Daher will man einerseits Antennen mit unterschiedlichen Polarisationsebenen einsetzen, um Spatial Streams parallel übertragen zu können. Andererseits soll mittels Beamforming gezielt ein Mehrwegeempfang herbeigeführt werden. Abbildung 8 illustriert das Prinzip.

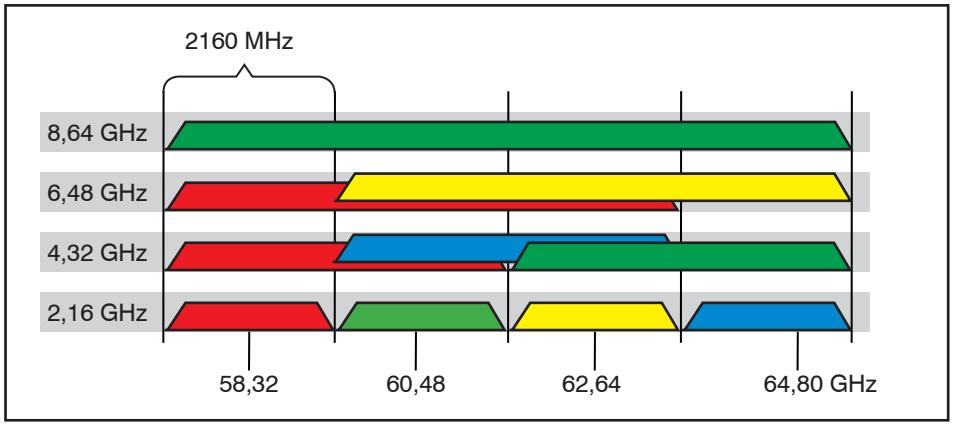


Abbildung 7: Channel Bonding bei IEEE 802.11ay

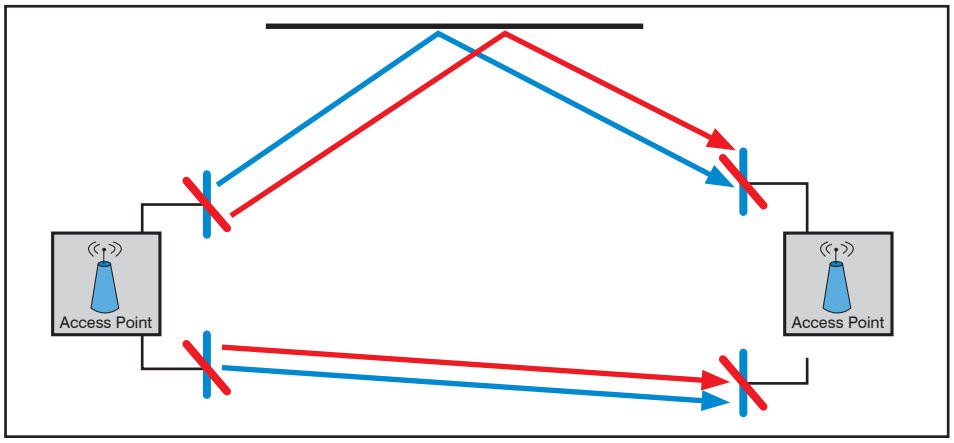


Abbildung 8: MIMO und Beamforming bei IEEE 802.11ay

Einige Anwendungsbeispiele für das aufgebohrte 60-GHz-WLAN werden von Autoren der Task Group genannt. Neben den bereits realisierten Docking Stations stellt man sich unter anderem den Einsatz für Video Streaming im heimischen Wohnzimmer vor. Interessant ist auch die Möglichkeit, Brillen für Augmented bzw. Virtual Reality über diese Technik zu vernetzen. Verschiedene Hersteller haben auf der gerade zu Ende gegangenen Consumer Electronics Show (CES) in Las Vegas Prototypen für diesen Anwendungsfall gezeigt.

Daneben könnte die neue Technik dank der hohen Bitrate auch herkömmliche Netzwerk-Schnittstellen ersetzen. Der Einsatz als Backhaul für Mesh WLAN erscheint naheliegend. Bisher hat man dabei das Problem, dass die Verbindung zwischen den Access Points meist auf 5 GHz realisiert wird. Sie konkurriert also mit den Endgeräten, die sich im selben Band mit den Access Points verbinden möchten. Unerwartet finde ich aber den Vorschlag, dass man sogar Glasfasern in Rechenzentren einsparen könnte. Redundanzen werden stattdessen mit dem neuen WLAN realisiert, die Bitrate sollte für die meisten Server-Anwendungen ausreichen.

Zuletzt wird der Einsatz im Zusammenhang mit Mobilfunk erwähnt. Die Provider treiben einen großen Aufwand, hohe Bitraten an die neuen Basisstationen für LTE (4G) heranzuführen. Und das wird mit 5G-Mobilfunk nicht einfacher. IEEE 802.11ay könnte auch hier die Glasfaser ersetzen. Man rechnet damit, auf 60 GHz Entfernungen von bis zu 1 km überbrücken zu können (!).

LTE/WLAN Offload

Eine Anwendung für IEEE 802.11ax habe ich noch nicht genannt. Der WLAN-„Offload“. Damit ist gemeint, dass Mobilfunknetze entlastet werden, wenn man Daten stattdessen über WLAN austauscht. Das kennen Sie wahrscheinlich schon aus Lounges an Flughäfen und Bahnhöfen. Dort stellt man Ihnen ein – häufig kostenfreies – WLAN zur Verfügung. Und Sie buchen Ihr Smartphone oder den Laptop dort ein, obwohl sie eigentlich über eine Mobilfunkverbindung verfügen. WLAN ist oft schneller und die Antwortzeiten sind kürzer als bei Mobilfunk – zumindest, wenn nur 2G oder 3G zur Verfügung stehen. Und außerdem belastet WLAN das meist begrenzte Datenvolumen im Mobilfunk nicht.

Mobilfunk-Provider finden das natürlich interessant. Gerade erst haben Ericsson und Cisco bekanntgegeben, ihre strategische Partnerschaft auf WLAN-Komponenten auszudehnen (herzlichen Dank an Herrn Dr. Kauffels für diesen Hinweis!). Es soll eine neue WLAN-Lösung mit Namen „Evolved Wi-Fi Networks“ (EWN) angeboten werden. In EWN werden die Mobilfunklösungen von Ericsson mit WLAN-Komponenten von Cisco kombiniert. Man möchte den Kunden von Ericsson leistungsfähige WLAN-Lösungen anbieten.

Der Deal zeigt genau in die geschilderte Richtung: WLAN als Ergänzung zum Mobilfunk. Wie kann das technisch funktionieren? Nein, dieses Mal brauche ich keine neuen Techniken zu erläutern, denn es ist eigentlich schon alles vorhanden:

- Im Mobilfunk gibt es die „3GPP Access Network Discovery and Selection Function“ (ANDSF). Deren Aufgabe ist es, den Standort des mobilen Endgeräts zu ermitteln. Auf Grund dessen teilt die ANDSF dem Endgerät alternative Zugangs-

netze mit, wenn diese am Standort des Endgeräts zur Verfügung stehen. Ein alternatives Zugangsnetz ist insbesondere WLAN. Umgekehrt lernt die ANDSF vom Endgerät, welche Netze es empfängt. Schließlich teilt die ANDSF dem Endgerät mit, welche Daten über welches Netz zu schicken sind. So könnten Telefonate (VoIP) weiterhin über das Mobilfunknetz erfolgen, während Web Browsing über WLAN erfolgt.

- Im WLAN gibt es den Standard IEEE 802.11u „Interworking with External Networks“, der bereits in IEEE 802.11-2012 enthalten ist. Das darin spezifizierte „Access Network Query Protocol“ (ANQP) ähnelt dem ANDSF. Das WLAN-Endgerät erfährt bereits vor der Assoziation an einem WLAN, welche Mobilfunk-Roaming-Partner darüber erreicht werden können. Die erforderlichen Authentisierungsverfahren (EAP-Methoden) werden dem Endgerät mitgeteilt. Und selbst wenn man keinen Vertrag mit einem entsprechenden Provider hat, besteht die Möglichkeit, Notrufe zu signalisieren.

Letztlich lassen sich mit Hilfe der beiden Techniken WLAN und Mobilfunk miteinander verbinden, wie es in Abbildung 9 skizziert ist. Man erkennt in der oberen Hälfte das Controller-basierte WLAN und unten das Mobilfunknetz. Wie üblich, ist das mit Abkürzungen gespickt. Die Basisstation heißt „eNodeB“. Sie steht in Verbindung zum „Serving Gateway“ (S-GW) und zur „Mobility Management Entity“ (MME). Daten fließen vom S-GW weiter über den „Packet Data Network Gateway“ (P-GW) in das öffentliche Netz. Weitere Elemente sind der „Home Subscriber Server“ (HSS), in dem die Kundendaten verwaltet werden. Ein „Authentication, Authorization, Accounting“ (AAA) Server ermöglicht dem WLAN die Authentisierung von Endgeräten über das Protokoll RADIUS. Bindeglied ist der „Evolved Packet Data Gateway“ (ePDG) und das ganze Gebilde wird als „Evolved Packet Core“ (EPC) bezeichnet.

Man erkennt in Abbildung 9 das Zusammenwirken des Endgerätes mit ANDSF und WLAN. Letztlich authentisiert sich das Endgerät über das WLAN mit dem Mobilfunknetz. Die dafür erforderlichen Zugangsdaten stecken in der SIM-Karte des Endgerätes. Nachdem die Verbindung zum WLAN hergestellt ist, baut das Endgerät einen gesicherten Tunnel (IPsec) zum ePDG des Mobilfunknetzes auf (vgl. Abbildung 10). Ziel ist es, dass die vom Mobilfunknetz an das Endgerät vergebene IP-Adresse sowohl über dieses als auch über das WLAN erreichbar ist. Die Daten werden nun Anwendungs-abhängig entweder über das Mobilfunknetz oder WLAN geroutet.

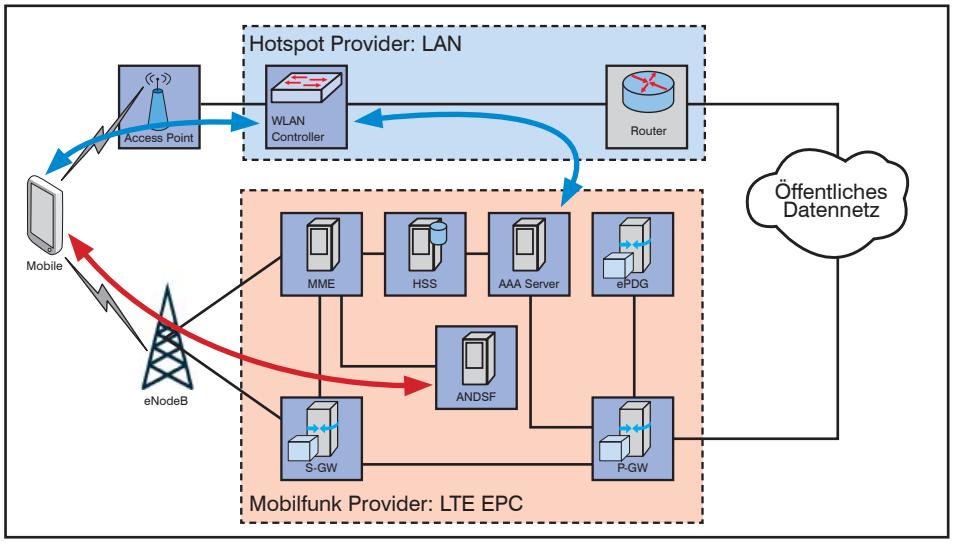


Abbildung 9: Signalisierung bei LTE/WLAN Offload

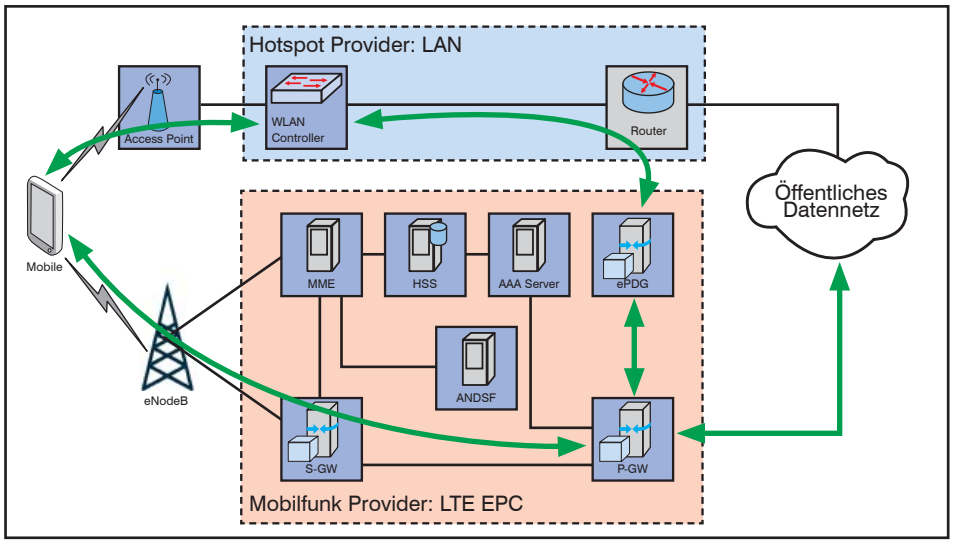


Abbildung 10: Datenflüsse bei LTE/WLAN Offload

Erste Implementierungen habe ich bereits bei meinem Mobilfunkprovider in manchen Lounges entdecken können. Ein Test steht noch aus.

Zusammenfassung

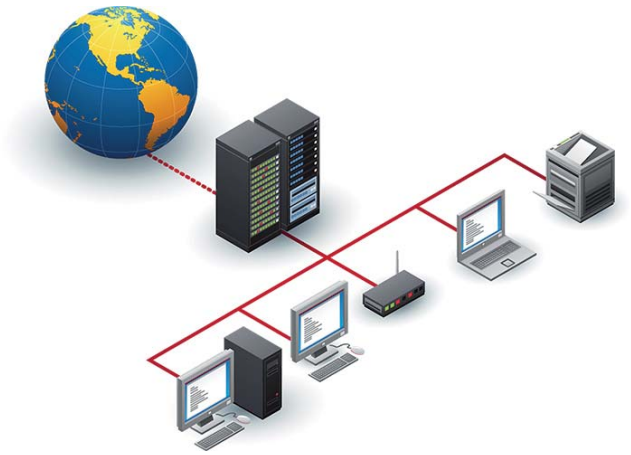
Das Jahr 2017 wird keine bahnbrechend neuen WLAN-Produkte bringen. Aber es ist jetzt absehbar, wohin die Reise bis zum Ende dieses Jahrzehnts gehen wird. WLAN in den traditionellen Frequenzbändern bei 2,4 und 5 GHz sind, was die erzielbare Bitrate angeht, mehr oder weniger ausgereizt. Das Medienzugangsverfahren jedoch bietet noch Luft nach oben. Der zukünftige Standard IEEE 802.11ax spezifiziert die Techniken OFDMA und Spatial Re-Use. Außerdem wird das mit IEEE 802.11ac „Wave 2“ eingeführte Multi-User MIMO um die Fähigkeit des Upload erweitert. Alles zusammen soll aus der Sicht des WLAN-Endgeräts eine vierfach höhere Effizienz ergeben. Aus meiner Sicht steckt die größte Chance für eine Effizienzsteigerung in OFDMA. MU-MIMO halte ich eher für eine Totgeburt, da man viel zu sehr auf die Umgebungsbedingungen angewiesen ist. Auf die Wirkung von Spatial Re-Use bin ich gespannt. Aber leider müssen wir vorher die vielen alten Endgeräte loswerden, die bei den schönen neuen Verfahren nicht mitmachen. Im Fußballstadion stehen dafür die Chancen besser als in einer Fabrik.

Daneben arbeitet das IEEE an einer Optimierung des WLAN im Millimeterwellenbereich. IEEE 802.11ay wird den Vorgänger IEEE 802.11ad um Channel Bonding und MIMO erweitern und dadurch auf Brutto-

Datenraten von 20 Gbit/s kommen. Neben den Mini-Funkzellen, die auf einen Arbeitsplatz beschränkt bleiben (in früheren Artikeln haben wir dafür den Begriff „Atto-Zelle“ erfunden) sollen diese WLAN auch Kommunikation über mehrere hundert Meter unterstützen. Wir sind gespannt, welche Produkte sich dafür in den nächsten Jahren materialisieren.

Mobilfunk und WLAN konkurrieren um die knappe Ressource „Funkfrequenz“. Im Enterprise-Bereich propagieren wir die Auslagerung nicht Produktions-relevanter Kommunikation auf den Mobilfunk. Die Provider gehen nun den umgekehrten Weg: WLANs werden an die Mobilfunknetze angebunden, damit bestimmte Anteile der Kommunikation auf WLAN abgeladen werden können. Die Standards dafür sind vorhanden und es gibt bereits erste Implementierungen. Im Enterprise-Bereich könnte man zukünftig auf Bereitstellung und Betrieb eigener Gäste-WLANs verzichten. Stattdessen meldet sich der Anwender über das Inhouse-WLAN am Netz seines Mobilfunk-Providers an, ganz ohne Voucher und Verwaltungsaufwand. Voraussetzung ist, dass die Provider uns entsprechende Schnittstellen bereitstellen – technisch wäre das kein Problem.

Kongress



ComConsult Netzwerk Forum 2017
27.03. - 30.03.2017 in Köln

Das ComConsult Netzwerk-Forum 2017 stellt die vier momentan dominantesten Netzwerk-Themen in den Mittelpunkt der Veranstaltung: Anwendungs-Architekturen und Kommunikation im Rechenzentrum, Netzwerk-Design und Optimierung des Betriebs, WLAN-Design und die Herausforderungen neuer Standards, Netzwerk-Sicherheit in einem Cloud-Umfeld.

Am ersten Tag analysieren wir die Auswirkungen aktueller Anwendungs-Architekturen auf die schnelle Bereitstellung, die Gestaltung und die Leistung von Netzwerken. Anwendungs-Architekturen werden immer dynamischer und in Kombination mit der Forderung nach einer sehr schnellen Bereitstellung von Kapazitäten ergibt sich eine komplexe Orchestrierungs-Aufgabe. Die Dynamik ergibt sich dabei nicht nur beim Start einer Mikroservice-Architektur, sondern auch bei Lastveränderungen im laufenden Betrieb.

Am zweiten Tag stellen wir uns den aktuellen Veränderungen im Netzwerkdesign in Kombination mit der Frage, wie wir in einer immer komplexeren Situation zu einem optimalen Betrieb kommen können.

Am dritten Tag diskutieren wir die neuesten WLAN-Standards und zum Abschluss des Tages die Frage, wie eine umfassende Sicherheits-Lösung unter Berücksichtigung der Cloud aussehen kann.

Der vierte Tag des ComConsult Netzwerk Forums widmet sich traditionell einem Schwerpunktthema, welches wir gemeinsam mit Ihnen intensiv beleuchten möchten. In diesem Jahr steht das Thema der „Netzwerksicherheit: Bedrohungen, Herausforderungen, Trends und Best Practice“ im Fokus.

Wie in jedem Jahr so wird auch 2017 das ComConsult Netzwerk-Forum der Treffpunkt der Branche sein. Top-Referenten, die Analyse der neuesten Entwicklungen, praxisnahe Empfehlungen, mehr Sicherheit für Ihre Entscheidungen und viele, viele Diskussionen prägen diese Veranstaltung. Versäumen Sie nicht sich rechtzeitig einen Platz zu sichern.

Top-Referenten, die Analyse der neuesten Entwicklungen, praxisnahe Empfehlungen, mehr Sicherheit für Ihre Entscheidungen und viele, viele Diskussionen prägen diese Veranstaltung.

Preise: € 2.790,- netto - 4-tägige Veranstaltung mit Thementag
€ 2.390,- netto - 3-tägige Veranstaltung ohne Thementag

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

ComConsult Veranstaltungskalender

Lokale Netze für Einsteiger, 13.02. bis 17.02.2017 in Aachen

Garantietermin

Dieses Seminar vermittelt kompakt und intensiv innerhalb von 5 Tagen die Grundprinzipien des Aufbaus und der Arbeitsweise Lokaler Netzwerke. Der Intensiv-Kurs vermittelt die notwendigen theoretischen Hintergrundkenntnisse, vermittelt den praktischen Aufbau, den Betrieb eines LANs und vertieft die Kenntnisse durch umfangreiche, gruppenbasierende Übungsbeispiele. Ausgehend von einer Darstellung von Themen der Verkabelung und Übertragungsprotokolle wird die Arbeitsweise von Switch-Systemen, drahtloser Technik, den darauf aufsetzenden Verfahren und der Anbindung von PCs und Servern systematisch erklärt.

Preis: € 2.490,-- *

IP-Wissen für TK-Mitarbeiter, 20.02. bis 21.02.2017 in Bonn

Dieses Seminar vermittelt TK-Mitarbeitern ohne Vorkenntnisse im Bereich LAN und IP das erforderliche Wissen zur Planung und zum Betrieb von VoIP-Lösungen. Die Inhalte sind so gegliedert, dass Sie die Grundlagen schnell verstehen. Es werden die wichtigsten VoIP-spezifischen Aspekte vorgestellt und unter praxisrelevanten Gesichtspunkten beleuchtet. Die Themen erstrecken sich von IP und LAN-Grundlagen hin zu praxisrelevanten Themen wie QoS, Jitter und Bandbreiten-Fragen. Ziel ist es dem IP-Unkundigen die wichtigen Grundlagen der Netzwerktechnik kompakt und praxisnah zu vermitteln.

Preis: € 1.590,-- *

RZ-Kopplung: Georedundanz für Rechenzentren, 13.03.2017 in Berlin

Rabattaktion %

Die gestiegene Bedeutung von zentralen IT-Systemen für Unternehmen und gesetzliche Vorgaben erfordern geo-redundante Standorte von Rechenzentren. Für die Bereitstellung und den Betrieb der Rechenzentrums-Kopplung wird besonderes Know-how und strategische Planung benötigt. In diesem Seminar werden die aktuellsten Technologien und Anforderungen vorgestellt und ein optimales Gesamtkonzept beschrieben.

Preis: € 1.090,-- *

Aufbau und Management von Internet-DMZ und internen Sicherheitszonen, 13.03. bis 15.03.2017 in Berlin

Die IT-Sicherheit für die Internet DMZ und internen Sicherheitszonen werden in diesem Seminar von Experten aus der Praxis vorgestellt und anschaulich erklärt. Verschiedene IT-Architekturen und Konzepte werden analysiert und auf ihre Praxistauglichkeit untersucht. Die Umsetzung anhand konkrete Projektbeispiele runden die Schulung ab.

Preis: € 1.890,-- *

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen, 13.03. bis 15.03.2017 in Köln

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

Preis: € 1.890,-- *

Netzzugangskontrolle: Technik, Planung und Betrieb, 13.03. bis 15.03.2017 in Berlin

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

Preis: € 1.890,-- *

TCP/IP-Netze erfolgreich betreiben, 13.03. bis 15.03.2017 in Aachen

Rabattaktion %

IP ist die Grundlage jeden Netzes. Die Protokolle TCP und UDP bilden die Basis jeder Anwendungskommunikation. Es werden zudem Kenntnisse über Routingprotokolle, DHCP, DNS benötigt. Dieses Seminar vermittelt praxisnah das notwendige Wissen.

Preis: € 1.890,-- *

Vertragsgestaltung und rechtssichere Organisation von Cloud Services für Nichtjuristen, 03.04. bis 04.04.2017 in Bonn

Rabattaktion %

Dieses Seminar erklärt, wie Sie die Auslagerung Ihrer Private Cloud vertraglich absichern und warum Sie das unbedingt machen sollten.

Preis: € 1.590,-- *

Virtualisierungstechnologien in der Analyse, 03.04. bis 04.04.2017 in Bonn

Im Zuge stetig zunehmender Konsolidierung ist Virtualisierung längst zum Standard in jedem Rechenzentrum geworden. Doch der Blick hinter die Kulissen offenbart einen rapide wachsenden Komplexitätsgrad, dessen Beherrschung ein tieferes Verständnis dieser Technologie erfordert. In diesem Seminar werden die Zusammenhänge zwischen Server, Netzwerk und Storage im Umfeld der Virtualisierung analysiert.

Preis: € 1.590,-- *

Kommunikation über Private WAN und Internet, 03.04. - 04.04.2017 in Bonn

Rabattaktion %

Dieses Seminar vermittelt die Erfahrungen aus den jüngsten Projekten mit dem Fokus Konzeption und Ausschreibung von WANs. Teilnehmer dieses Seminars profitieren von langjährigen Erfahrungen der Vortragenden im WAN-Bereich, kombiniert mit dem großen Erfahrungsschatz von ComConsult bei der Lösung von Problemen und der Lokalisierung von Fehlern in standortübergreifenden Netzen. Ferner werden Erfahrungen bei der Gestaltung sinnvoller Service Level Agreements (SLA) im WAN-Betrieb in diesem Seminar vermittelt.

Preis: € 1.590,-- *

* alle ausgewiesenen Preise sind netto-Preise

Zertifizierungen

ComConsult Certified Network Engineer

Lokale Netze für Einsteiger
13.02. - 17.02.17 in Aachen
08.05. - 12.05.17 in Aachen
18.09. - 22.09.17 in Aachen

TCP/IP-Netze erfolgreich betreiben
13.03. - 15.03.17 in Aachen
29.05. - 31.05.17 in Aachen
09.10. - 11.10.17 in Bremen

Internetworking
03.04. - 07.04.17 in Aachen
19.06. - 23.06.17 in Göttingen
13.11. - 17.11.17 in Aachen

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

ComConsult Certified Trouble Shooter

Trouble Shooting in vernetzten Infrastrukturen
02.05. - 05.05.17 in Aachen
26.09. - 29.09.17 in Aachen

Trouble Shooting für Netzwerk-Anwendungen
27.06. - 30.06.17 in Aachen
07.11. - 10.11.17 in Aachen

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

ComConsult Certified Voice Engineer

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen
13.03. - 15.03.17 in Köln
15.05. - 17.05.17 in Düsseldorf
16.10. - 18.10.17 in Frankfurt

Session Initiation Protocol Basis-Technologie der IP-Telefonie
05.04. - 07.04.17 in Bonn
29.05. - 31.05.17 in Frankfurt
08.11. - 10.11.17 in Stuttgart

Umfassende Absicherung von Voice over IP und Unified Communications
08.05. - 10.05.17 in Frankfurt
10.07. - 12.07.17 in Düsseldorf

Optionales Einsteiger-Seminar: IP-Wissen für TK-Mitarbeiter
20.02. - 21.02.17 in Bonn
02.05. - 03.05.17 in Düsseldorf
18.09. - 19.09.17 in Düsseldorf

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

Basis-Paket: Beinhaltet die drei Basis-Seminare
Grundpreis: € 5.100,--* statt € 5.670,--*
Optionales Einsteigerseminar: Aufpreis € 1.190,--* statt € 1.590,--*

* alle ausgewiesenen Preise sind netto-Preise

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: kundenservice@comconsult-research.de
http://www.comconsult-research.de

Herausgeber und verantwortlich
im Sinne des Presserechts:
Dr. Jürgen Suppan
Chefredakteur: Dr. Jürgen Suppan
Erscheinungsweise: 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