ComConsult Research

Der Netzwerk Insider

Juni 2016

Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

Neue WLAN-Techniken in Enterprise WLANs?

von Dr. Joachim Wetzlar

„Die Zukunft wird Wireless“ – so lasen Sie im Geleit des Netzwerk Insiders vom Januar dieses Jahres. Ja, auch ich kann diesen Trend bestätigen, wenn ich die Umgebungen meiner Enterprise-Kunden beobachte. Und das, obwohl doch an anderer Stelle des Netzwerk Insiders behauptet wurde, WLAN leide unter der „Pest“ des „unsäglichen DCF-Steuerungsverfahrens“. Wie dem auch sei, es stehen (mal wieder) neue WLAN-Chips in den Startlöchern der Netzwerkausrüster, um uns mit noch höherer Bitrate beglücken zu können. Wird das den Unternehmen helfen, die bereits heute große WLANs betreiben und wesentliche Teile ihrer Produktion darauf abstützen?

Was sind das für Anwendungen, die nun in die Enterprise-Umgebungen drängen? Ich nenne einige Beispiele, die man mir entweder im Rahmen meiner Planungstätigkeit genannt hat oder bei deren Inbetriebnahme bzw. der Fehlersuche ich unterstützen durfte.

weiter auf Seite 8

Zweitthema

Unternehmensnetze folgen nicht immer dem Beispiel der Hyperscaler

von Dr. Behrooz Moayeri

Fasziniert vom schnellen Aufstieg und explosionsartigen Wachstum der sogenannten Hyperscaler wie Google, Amazon und Facebook gehen einige Verantwortliche in Unternehmen von der Übertragbarkeit der Konzepte der großen Internetfirmen auf die eigene IT aus. Der internen IT-Abteilung wird oft vorgehalten, dass sie nicht so flexibel und schnell auf Wünsche der Kunden reagiere wie die Hyperscaler.

Typische Fragestellung dabei: „Warum kann ich bei Amazon mit wenigen Klicks Server, Massenspeicher und den Netzzugang dazu einrichten, während dies in unserer internen IT-Umgebung Tage oder gar Wochen dauern kann?“ Der vorliegende Beitrag geht darauf ein, warum die Unternehmensnetze nicht immer dem Beispiel der Hyperscaler folgen können.

weiter auf Seite 15

Geleit

Brauchen wir eine Strategie zur Nutzung der Cloud?

auf Seite 2

Standpunkt

Vorsicht mit „Roaming Profiles“!

auf Seite 14

5 Tage Intensiv-Update

ComConsult Sommerschule 2016

ab Seite 6

Aktuelles Seminar und Expertentipp

Private Cloud rechtssicher auslagern

ab Seite 4

Zum Geleit

Brauchen wir eine Strategie zur Nutzung der Cloud?

Arbeitsplätze in der Cloud sind sowohl preiswert als auch sofort verfügbar. Für komplexere Produkte wie Salesforce gibt es kostenlose Teststellungen. Ist also "try and error" der naheliegende Weg zum Einstieg in die Cloud? Oder gibt es Gründe, die eine Strategie oder ein Konzept für einen Einstieg erfordern?

Da die Cloud begrifflich alles oder nichts sein kann, nehmen wir als Ausgangspunkt der Diskussion die folgenden drei Cloud-Nutzungen:

- die Bereitstellung von Rechenleistung in Form von virtuellen Maschinen
- die Bereitstellung von Datei-Systemen (Beispiel: Box)
- die Bereitstellung einer CRM-Applikation (Beispiel: Salesforce oder SugarSync)

In der Regel gibt es im Rahmen der IT folgende in der Regel kombinierte Gründe oder Voraussetzungen für die Notwendigkeit eines Konzepts bzw. einer Strategie:

- die Anzahl betroffener Mitarbeiter: das Problem der Entscheidung für die "falsche" Lösung oder ein späterer Umstieg auf ein anderes Produkt ist abhängig von der Anzahl der betroffenen Mitarbeiter
- die Bedeutung der durch die Mitarbeiter ausgeübten Prozesse: auch eine kleinere Zahl von Mitarbeitern kann zum Problem werden, wenn das falsche Produkt gewählt wurde
- das Ziel der Nutzung und seine Auswirkung auf Mitarbeiter, Prozesse und Kosten: dies ist ohne Frage eines der Kern-Themen: warum soll ein Cloud-Service überhaupt genutzt werden
- die mit dem Projekt verbundenen Invest- und Betriebs-Kosten
- der Arbeitsaufwand und die Fähigkeit das Projekt mit vorhandenem Personal abzuwickeln: ein einfacher "try und error Test" in der Cloud mit wenigen Arbeitsplätzen mag auf den ersten Blick preiswert sein speziell im Vergleich zu Alternativen mit hohen Verlaufkosten, dies ist aber nicht generell der Fall. Eine

ganze Reihe von Cloud-Lösungen skalieren wirtschaftlich schlecht über die Anzahl der Arbeitsplätze: preiswert bei wenigen und teuer bei vielen Arbeitsplätzen

- die Sicherheit der Daten: hier geht es nicht nur um den Bedarf an Sicherheit, sondern auch und speziell um die Kosten der Umsetzung von Sicherheit. Generell unterstelle ich, dass Cloud-Lösungen in vielen Fällen sicherer sind als lokale Lösungen. Dabei darf aber der Zusatz-Aufwand, um eine Cloud-Lösung an den eigenen Sicherheits-Bedarf anzupassen oder den Sicherheits-Perimeter in die Cloud zu verschieben nicht unterschätzt werden. Eine virtuelle Maschine bei Amazon ist in Sekunden in Betrieb genommen. Soll sie aber mit einem virtuellen Netzwerk, virtuellen Firewalls, Load-Balancern und anderen NFV-Instanzen im Sinne einer Perimeter-Verschiebung kombiniert werden, dann sieht die Wirtschaftlichkeit auf einmal ganz anders aus
- die Einhaltung von Compliance-Bedingungen oder allgemeiner rechtlichen Rahmenbedingungen: wir sprechen hier über ein Minenfeld unklarer und schwammiger juristischer Rahmenbedingungen, die von ahnungslosen Laien aufgestellt und von noch ahnungsloseren Richtern umgesetzt werden. Was ein Gericht für gut erklärt, kann in einem anderen Bundesland oder einem anderen Land der EU völlig akzeptabel sein. Für Unternehmen mit mehreren internationalen Standorten oder für die Nutzung von Cloud-Lösungen in verschiedenen Ländern eine echte Barriere
- die langfristige Bindung an ein Produkt oder einen Hersteller: ähnlich wie früher bei SAP gibt es Produkte in der Cloud, die man nur schwer wieder abschaffen kann, wenn sie erst einmal in wichtigen Prozessen integriert sind. Hier stellt sich die Frage, ob potenzielle Ausstiegskosten in der Projekt-Entscheidung wirtschaftlich berücksichtigt werden sollten. Dies ist speziell interessant, wenn es um Entscheidungen wie die beispielsweise einer lokalen SugarSync-Installation kontra einer Salesforce-Nutzung geht

Es gibt bei dieser Betrachtung einen sofort erkennbaren deutlichen Unterschied zwischen der Public und der Private Cloud. Public Cloud-Lösungen haben eine niedrige Einstiegsbarriere, da mit wenigen Test-Arbeitsplätzen begonnen werden kann und damit keine Investitionen erforderlich sind. Auch können Public Cloud Projekte mit wenig Personal (ich wage nicht zu sagen quasi nebenbei) gestartet werden.

Ich unterstelle deshalb, dass die meisten Private Cloud-Projekte eine Langfrist-Strategie und ein technologisches Rahmenkonzept erfordern. Das Beispiel der Bereitstellung von Rechenleistung als Private Cloud-Projekt macht dies deutlich. Die naheliegende technologische Basis ist OpenStack. Damit sind wir sowohl von der Kosten- als auch von der Aufwandsbetrachtung in Bereichen, die wohl kaum jemand ohne einen sehr weitgehenden Projektansatz angehen würde. Von daher konzentriere ich die Betrachtungen auf die Public Cloud, da aus meiner Sicht nur dort die Gefahr eines zu einfachen Einstiegs mit schmerzhaften Folgen besteht.

Die Nutzung von Applikationen wie Salesforce oder SugarSync können wir auch per se als Projekt mit dem Bedarf einer Strategie ansehen, das liegt in der Natur dieser Applikationen, da die Prozesse, die darauf aufsetzen, zu wichtig für die Unternehmen sind. Die zentrale Frage wird bei solchen Applikationen sein: wie viel Individualisierung ist erforderlich, geht das besser in einer Public-Lösung oder in einer Private-Installation? Dies betrifft nicht nur Gesichtspunkte wie die Datensicherheit oder die Einhaltung von Compliance-Vorschriften, sondern auch beispielsweise so zentrale Fragen wie, ob ein Multi-Mandanten-

Brauchen wir eine Strategie zur Nutzung der Cloud?

Modell wie Salesforce nicht generell die Gefahr beinhaltet, individuelle Anforderungen an Funktionalität nur mit großen Einschränkungen oder Kosten erfüllen zu können. Trotzdem wird die Abwägung schwierig, wenn Betriebskosten oder einzelne Funktionen eine hohe Priorität haben.

Bleiben wir deshalb bei dem einfachsten der drei Nutzungs-Beispiele: der Nutzung eines Datei-Dienstes wie Box als Private Cloud Dienst (stellvertretend für die verschiedenen Anbieter in diesem Marktsegment wie Dropbox, Huddle, SugarSync …). So ein einfacher Dienst muss doch leicht zu evaluieren sein, oder? Nun, dann lassen sie mich ein paar sehr naheliegende Fragen zur Nutzung eines solchen Dienstes stellen:

- Was ist das primäre Ziel der Dienst-Nutzung?
  - die Abschaffung des lokalen Datei-Systems auf dem lokalen Server?
  - die Bereitstellung einheitlicher Daten auf verschiedenen Endgeräten eines Nutzers?
  - der Austausch von Daten mit externen Personen?
  - die Schaffung einer Arbeits- und Kollaborations-Umgebung für Teams?
  - die Umsetzung eines einfachen Back-up-Konzepts?
- Was bedeutet die Nutzung technisch?
  - dass der lokale Zugriff bei den Mitarbeitern auf lokale Folder erfolgt, die mit der Cloud synchronisiert werden?
  - wenn ja, sind immer alle lokalen Folder auch in der Cloud?
  - gibt es rein lokale Daten?
  - gibt es Daten, die gar nicht lokal sein dürfen und die nur über den Web-Browser bearbeitet werden sollen?
  - welche Anforderungen sind dann an die Funktionalität der Browser-Oberfläche zu stellen?
  - wie Echtzeit-fähig muss der Cloud-Service sein? Wie schnell müssen lokale Änderungen “online” sein und wie hoch ist das Risiko von Konflikten?
  - wie gehen wir mit den unvermeidlichen Konflikten um?
  - wie ist der Zusammenhang mit den Applikationen, mit denen diese Dokumente erstellt bzw. bearbeitet werden? (Microsoft Office?)
  - wie ist der Zusammenhang mit anderen Cloud-basierten Diensten, können diese direkt auf die Dokumente zugreifen oder diese integrieren?
  - benutzen alle Mitarbeiter dieselbe Version dieser Applikationen?
  - wie werden Zugriffskonflikte bei der gleichzeitigen Nutzung eines Dokuments behandelt?
  - wie authentifiziert sich ein Mitarbeiter? Ist das sicher genug?
  - betrachten wir die Verschlüsselung des Anbieters als ausreichend oder wollen wir mit einer eigenen Verschlüsselung und einem privaten Schlüssel-Management einen höheren Grad von Sicherheit erreichen? Sind die damit verbundenen erheblichen Funktions-Nachteile akzeptabel?
  - wird generell das mit diesem Cloud-Dienst verbundene Sicherheits-Niveau als ausreichend betrachtet? Wollen wir Single-Sign-On, Two-Factor-Authentication, …
- Was bedeutet die Cloud-Lösung wirtschaftlich?
  - wie hoch sind die jährlichen Lizenzkosten?
  - wie hoch sind die Ausstiegskosten?
  - welche Zusatzkosten entstehen zum Beispiel in der Nutzung weiterer Cloud-Dienste?
  - wie aufwendig ist die Ersteinrichtung und der folgende Betrieb?
  - sind funktionale individuelle Anpassungen erforderlich? Müssen Schnittstellen angepasst oder programmiert werden?
  - wie abhängig ist die Lösung von einzelnen Funktionen der Cloud und wie hoch ist das Risiko, dass der Anbieter diese Funktionen wieder abschafft oder so modifiziert, dass sie nutzlos werden?

Und es gibt ein schönes Beispiel, das wir selber in den letzten Wochen diskutiert haben: was bedeutet die Nutzung eines Cloud-basierten Datei-Dienstes unter Berücksichtigung von Viren, die die lokalen Daten verschlüsseln und unzugreifbar machen (Ransomware, siehe dazu die aktuelle Ausgabe der c´t)? Es wäre sehr naiv davon auszugehen, dass das nie passieren kann (angeblich sind 30% der deutschen Unternehmen davon betroffen) und das eigene Sicherheitskonzept so gut ist, dass man gegen externe Angreifer zu 100% geschützt ist. Naturgemäß laufen diese Viren ins Leere, wenn nur mit der Browser-Oberfläche in der Cloud gearbeitet wird. Aber sie erfassen natürlich alle lokalen Folder, die synchronisiert sind. Und damit übertragen sie die Verschlüsselung (Zerstörung) der Daten auch sofort in die Cloud und zerstören die damit verbundenen Daten eines Teams für alle Team-Mitarbeiter. Cloud-Dienste wie Box haben einen Versionsdienst. Dies bedeutet in der Theorie, dass jedes Dokument auf den Zustand von vor der Verschlüsselung zurückgesetzt werden kann. Aber dies geht nur manuell pro Dokument. Man kann hoffen, dass Box bereit ist ein Skript über alle betroffenen Dokumente laufen zu lassen, doch sicher ist das nicht. Damit sind wir automatisch bei der Frage der Datensicherung. Zumindest ältere Dokumente, die nicht mehr verändert werden, sollten ja ohne Probleme aus der Sicherung wiederhergestellt werden können. Also auf jeden Fall gibt es einen Bedarf für eine organisierte Sicherung. Aber es gibt auch die Frage: kann der Umfang der betroffenen Dokumente dadurch verkleinert werden, dass nur aktive Dokumente synchronisiert werden? Oder da ist natürlich die Extremfrage: warum überhaupt außerhalb des Browsers mit lokalen Daten arbeiten, wenn alle notwendigen Applikationen wie Microsoft Office mit dem Cloud-Dienst integriert sind und eine lokale Instanz gar nicht erforderlich ist?

Aber was zeigt die Diskussion dieses relativ einfachen Beispiels? Nun, bezogen auf die zu Beginn genannten Kriterien, können wir bei Cloud Diensten in der Mehrzahl der Fälle unterstellen:

- die Zahl der betroffenen Mitarbeiter wird hoch sein
- die Kosten pro Arbeitsplatz sind nicht niedrig bei Produkten wie Box; Wirtschaftlichkeit ist also ein Thema
- Ausstiegskosten sind ein signifikantes Thema
- Sicherheit ist ein Thema
- Compliance ist ein Thema

Die Schlussfolgerung ist dementsprechend auch unter Berücksichtigung der aufgeworfenen technischen Fragen:

- Bei der Nutzung von Cloud-Diensten geht an einem sauber aufgesetzten Projekt mit klaren Zieldefinitionen und einem schriftlich formulierten Nutzungs-Konzept im Rahmen einer Gesamt-Strategie kein Weg vorbei. Und naturgemäß spielt die Frage der Zielsetzung eine tragende Rolle dabei.
- Die niedrige Einstiegshürde unter Vermeidung von Investitionen und mit geringen Kosten für wenige Testarbeitsplätze ist eine gefährliche Verlockung, die die spätere Komplexität des Projekts unterschätzen lässt. Auch die Berechnung der Wirtschaftlichkeit ist weit komplexer als vielleicht im ersten Augenblick gedacht.

Ihr
Dr. Jürgen Suppan

Aktuelles Seminar

Private Cloud rechtssicher auslagern

Vertragsgestaltung für Nichtjuristen

15.06. - 16.06.16 in Köln

Die ComConsult Akademie veranstaltet vom 15.06. bis 16.06.16 ihr Seminar "Private Cloud rechtssicher auslagern - Vertragsgestaltung für Nichtjuristen" in Köln.

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

Der Aufbau von Private Cloud-Lösungen ist ein Megatrend. Die komplette Kontrolle über die eigenen Daten und den Zugang zu diesen ist in der Regel die Haupt-Motivation. Allerdings ist die technische Umsetzung der Private Cloud mit OpenStack oder einer ähnlichen Infrastruktur sehr komplex und für viele Unternehmen kaum wirtschaftlich zu bewältigen.

Aus diesem Grund sehen wir einen hochaktuellen Trend in der Auslagerung der Private Cloud-Infrastruktur zu einem darauf spezialisierten Betreiber. Dabei bleibt aber die komplette Installation Unternehmensspezifisch und ist abgeschottet gegenüber anderen Kunden des externen Betreibers. Für die Unternehmen und Behörden, die diesen Weg gehen, ergeben sich signifikante Vorteile:

- alle Vorteile einer Cloud-Installation können genutzt werden

- das Unternehmen/die Behörde behält die Kontrolle über die Daten und den Zugang
- das notwendige komplexe Know How kann wirtschaftlich eingekauft werden

Juristische Herausforderungen
Allerdings ist diese Art der Umsetzung mit einigen juristischen Herausforderungen verbunden, die weit über eine normale Hosting oder Outsourcing-Situation hinaus gehen.

Dazu gehören unter vielen anderen:
- der Vertrag muss die technischen Ziele konkret wiedergeben
- mögliche Probleme müssen von vornherein ausgeschlossen werden
- Skalierbarkeit und schnelle Bereitstellung müssen vertraglich abgesichert sein
- IT-Sicherheit und Datenschutz müssen jederzeit nachprüfbar sein
- der Ort der Datenverarbeitung muss aus Datenschutz-rechtlichen und steuerlichen Gründen vertraglich vereinbart sein
- die Migration zu einem anderen Dienstleister muss jederzeit möglich sein
- bei Schwierigkeiten mit der Migration müssen Vertragslaufzeit und Unterstützungsleistungen angepasst werden können

Mit der neuen EU-Datenschutzgrundverordnung kommen wichtige Änderungen auf Nutzer und vor allem Anbieter von Cloudleistungen zu: Die Haftungssummen werden drastisch erhöht und können zukünftig bis zu 1000 mal höher sein als bisher. Der Cloudanbieter haftet erstmals direkt gegenüber Dritten und nicht nur gegenüber seinem Auftraggeber. Auf die neue Haftungssituation müssen sich beide rechtzeitig vorbereiten und bereits vor Inkrafttreten der neuen Verordnung ihre Verträge anpassen.

Rechtsanwalt Ulrich Emmert führt Sie durch dieses Seminar.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Private Cloud rechtssicher auslagern

Ich buche das Seminar
Private Cloud rechtssicher auslagern

☐ 15.06. - 16.06.16 in Köln
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

Expertentipp

Private Cloud rechtssicher auslagern?

Ulrich Emmert ist Rechtsanwalt in der Kanzlei esb Rechtsanwälte. Ein Schwerpunkt seiner Tätigkeit sind Beratungen und Schulungen im Bereich des EDV-, Telekommunikations– und Online-Rechts. Dabei kommen ihm umfangreiche technische Kenntnisse im Bereich Programmierung, Datenbanken und Internet-Security zugute, die auch eine qualifizierte Beratung im Bereich Netzwerksicherheit, Softwarelizenzverträge oder Datenschutz ermöglichen.

Unternehmen greifen zunehmend auf Cloud-Dienste zurück, um Kosteneinsparungen zu realisieren und um zu vermeiden, dass für zukünftige Entwicklungen bereits unnötig Ressourcen bereitgehalten werden müssen.

Dabei werden jedoch häufig Compliance-Anforderungen vergessen oder bewusst in den Hintergrund gedrängt. Daraus entstehe erhebliche Haftungsrisiken für Unternehmen, insbesondere weil damit auch Vorschriften zu IT-Sicherheit, Datenschutz und Geheimhaltung sowie zur Aufbewahrung und Löschung von Informationen missachtet werden.

Nach einer Umfrage von Markus Vehlow und Cordula Golkowsky von PWC zum Thema „Cloud Computing, Navigation in der Wolke“ unter deutschen Unternehmen im Jahr 2013 haben 39% der Unternehmen angegeben, sie würden Cloud-Dienste aus den USA nutzen und weitere 24%, sie würden Cloud-Dienste aus anderen Ländern außerhalb der EU nutzen.

Derzeit ist es durch das Urteil des Europäischen Gerichtshofs vom 6.10.2015 nicht mehr möglich, mit Hilfe des Safe Harbor Abkommens eine rechtmäßige Verarbeitung von Daten von EU-Bürgern in den USA zu erreichen. Das geplante Nachfolgeabkommen EU-US-Privacy Shield ist derzeit noch nicht in Kraft und wird voraussichtlich auch die Kriterien des Europäischen Gerichtshofs nicht erfüllen können, so dass mit einer neuerlichen Aufhebung zu rechnen ist.

Behörden und Freiberufler haben mit den Vorschriften des Amts- bzw. Berufsgeheimnisses zu kämpfen, die die Verwendung von Cloud-Diensten einschränken können. Es ist unter Juristen heftig umstritten, welche Arten der Cloud hier genutzt werden dürfen und welche Datenverarbeitung sogar strafrechtlich relevant sein kann. Ein Cloudanbieter lässt sich kaum als Gehilfe im Sinne des Gesetzes qualifizieren. Bereits die Möglichkeit, dass Mitarbeiter des Cloudanbieters oder seines Treuhänders auf die Daten zugreifen können, kann hier zu einer Complianceverletzung führen. Zudem werden bei Überwachungsmaßnahmen und Beschlagnahmeanordnungen gegen Provider möglicherweise Zeugnisverweigerungsrechte von Behörden und Freiberuflern untergraben, die den Zugriff der Staatsanwaltschaft bei eigener Datenverarbeitung verhindert hätten. Auch dies kann zu einer unerlaubten Kenntnisnahme Dritter führen. Hier sollte geprüft werden, welche Datenverarbeitung innerhalb des öffentlichen Dienstes bzw. dem Büro des Freiberuflers stattfinden muss bzw. welche Leistungen auch durch private Unternehmen erbracht werden können.

Das Steuerrecht verlangt von Unternehmen ebenfalls erhebliche Voraussetzungen, wenn die Daten nicht in der Unternehmens-IT, sondern irgendwo in einer Rechnerwolke gespeichert werden. Bestimmte Arten von Cloud-Diensten sind hier generell unzulässig. Die revisionssichere Archivierung von Daten nach der neuen GoBD und die erheblich gestiegenen Anforderungen an Verfahrensdokumentationen wecken weitere Zweifel an einer einfachen Verlagerung in die Cloud ohne sorgfältige Planung und Complianceprüfung.

Möglicherweise verstoßen auch Mitarbeiter gegen arbeitsvertragliche Pflichten, wenn sie Cloud-Dienste zur Verarbeitung von Unternehmensinformationen nutzen. Die Consumerizaion von IT macht zumindest im Bereich online erreichbarer privater Datenspeicher von Mitarbeitern wie z.B. Microsoft Onedrive, Dropbox oder Google Drive und bei der Synchronisation von auf mobilen Endgeräten gespeicherten Daten in die Cloud wie z.B. Apple Icloud vor rechtlich unzulässigen oder zumindest problematischen Sachverhalten nicht Halt.

Das Unternehmen oder seine Mitarbeiter können hier Probleme wegen der Strafbarkeit des Verrats von Geschäftsgeheimnissen bekommen, es können durch Geheimnisverrat aber auch erhebliche Nachteile für das Unternehmen im internationalen Wettbewerb entstehen.

Neue Anforderungen gibt es durch die jetzt stufenweise in Kraft tretenden Regelungen der EIDAS-Verordnung und der EU-Datenschutzverordnung. Bestimmte IT-Dienste sind zukünftig Vertrauensdiensteanbietern vorbehalten, die dafür die Anforderungen der EIDAS-Verordnung umsetzen müssen. Die Verarbeitung sensibler Daten in Cloud-Umgebungen wird zukünftig noch stärker reglementiert, während die Anforderungen an eine wirksame Einwilligung zur Verarbeitung von Daten für bestimmte Zwecke oder zur Verarbeitung im Ausland erheblich steigen werden. Bisherige Compliance-prüfungen sind daher für die Herausforderungen der nächsten beiden Jahre bei weitem nicht mehr ausreichend.

Behörden wie Unternehmen sollten also vor der Nutzung von Clouddiensten die allgemeinen rechtlichen wie auch die jeweils branchenbezogenen Complianceanforderungen prüfen, bevor Geschäftsprozesse durch die Inanspruchnahme von Clouddiensten verändert werden.

Intensiv-Update auf den neuesten Stand der Netzwerktechnik

ComConsult Sommerschule 2016 - Intensiv-Update auf den neuesten Stand der Netzwerktechnik 27.06. - 01.07.16 in Aachen

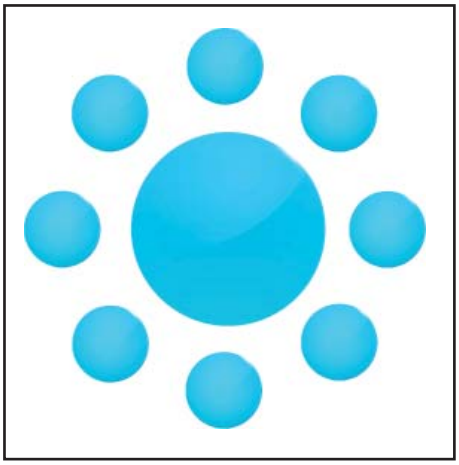
Die ComConsult Akademie veranstaltet vom 27.06. bis 01.07.16 ihre "ComConsult Sommerschule 2016" in Aachen.

Das technologische Umfeld von Netzwerken befindet sich in einem der intensivsten Änderungsprozesse der letzten 20 Jahre. Das betrifft das Rechenzentrum, neue IT-Architekturen, neue Client-Technologien bis hin zu Unified Communications. Hand in Hand mit dem Bedarf ändern sich Netzwerk-Technologien selber. Zukunftsorientiertes und wirtschaftlich optimales Design muss dieses Gesamtbild berücksichtigen.

Die Sommerschule 2016 bringt Sie in fünf Tagen auf den neuesten Stand der Netzwerk-, Kommunikations- und Infrastruktur-Technik.

Wir analysieren für Sie:

- Wie verändern sich IT-Architekturen und welche Anforderungen generiert das auf Infrastrukturen, welche neuen Anforderungen entstehen speziell im Rechenzentrum?



- Was passiert auf der WAN-Seite, wie sieht eine zukunftsorientierte WAN-Lösung aus?
- Wie sieht die Zukunft des LAN aus? Welche der neuen Technologien werden sich durchsetzen? Wie können skalierbare und sichere LAN-Infrastrukturen geschaffen werden?
- Unified Communications und das Ende von ISDN: Wie sieht die Kommunikationslösung der Zukunft aus? Was bedeutet das für Infrastrukturen?
- WLAN-Technik erreicht immer neue Leistungsklassen, aber wie sieht die Zukunft aus? Wo ist die Abgrenzung zum Mobilfunk?
- Sicherheit wird immer mehr zum Schlüssel für erfolgreiche IT-Infrastrukturen: Cloud-Computing und mobile Endgeräte, wie passt das in ein Sicherheitskonzept?

Top Experten der Branche gestalten das Programm dieser Intensiv-Schulung und bringen systematisch die Erfahrungen laufender Projekte und neuester Technologie-Entwicklungen in diesen Kurs ein. Treffen Sie einige der besten Experten, die die deutsche Netzwerk-Landschaft zu bieten hat.

Sichern Sie sich jetzt noch einen Platz auf dieser Veranstaltung!

Fax-Anmeldung an ComConsult 02408/955-399

ComConsult Sommerschule 2016

Ich buche das Seminar
ComConsult Sommerschule 2016

☐ 27.06.-01.07.16 in Aachen
zum Preis von € 2.490,--

☐ 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 Sommerschule 2016

Montag, der 27.06.16 - IT-Architekturen und Auswirkungen auf Infrastrukturen

Architekturen
IT-Architekturen sind geprägt von Endgeräten, die lokale Anwendungen ausführen und auf Applikationen auf Server zugreifen. Im Moment ändert sich hier alles. Unser Verständnis von Endgerät, Betriebssystem und Server muss auf den Prüfstand. Ohne Zweifel wird unsere IT-Landschaft in fünf Jahren dramatisch anders aussehen als heute. Und Netzwerke haben die zentrale, tragende Rolle für diese Entwicklung. Wir analysieren wo es hingeht und wie Netzwerke aussehen müssen, um diesen Weg zu unterstützen.

10:00 - 12:30 Uhr
Wir analysieren für Sie:
- Wie ändert sich IT und welche Auswirkungen hat das auf Infrastrukturen?
- Was passiert auf der Netzwerk-Seite, um diesen Anforderungen zu entsprechen?
- Welche neuen Technologien müssen speziell bei den Planungen für die nächsten Jahre beachtet werden?

Dr. Franz-Joachim Kauffels, Technologie-Analyst

14:00 - 17:00 Uhr
Rechenzentren: neue Arten von Infrastrukturen gefragt
Rechenzentren sind unter Druck:
- Die Cloud puscht das Thema Wirtschaftlichkeit, Kosten und Transparenz
- Mobile Endgeräte erfordern mindestens eine Private Cloud Infrastruktur und einen Übergang zu benutzerzentrischen Lösungen
- Server- und Speicher-Konsolidierung gehen permanent weiter, hochskalierende Infrastrukturen sind gefordert
- Virtualisierung geht in die nächste Runde und öffnet die Tür zu automatischen Lastausgleichen und Provisionierungen mit erheblichen Anforde rungen an Infrastrukturen

Wir analysieren für Sie:
Strategien für das Rechenzentrum der Zukunft:
- Software-Defined Networks SDN: Was ist der Kern von SDN? Wo unterscheidet sich SDN von klas sischen Netzwerkarchitekturen? OpenFlow, Netz werkvirtualisierung und weitere Ansätze; Ciscos Sonderweg: ACI und QoS im RZ
- Cloud Computing: Cloud Konzepte: Private, Public oder Hybrid? Was leistet die Cloud heute, welche Anforderungen entstehen bei der Anbindung? Software as a Service: Warum Cloud-Anwendungen anders sind. Hinter den Kulissen: Typische Cloud Anwendungen im Praxistest

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

11:00 - 11:15 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause
15:00 - 15:15 Uhr Kaffeepause
ab 19:00 Uhr Happy Hour

Dienstag, der 28.06.16 - Netzwerk-Technologien: aktuelle Entwicklungen

9:00 - 10:30 Uhr
Das Internet of Things: wo stehen wir?
Mehr und mehr Produkte drängen in den Markt. Daraus leitet sich die Frage ab, welche Anforderungen an Infrastrukturen hier auf uns zukommen. Dieser Vortrag zeigt wo wir stehen und was auf uns zukommt.

Sie lernen in diesem Themenblock:
• Was ist IoT? • Anwendungsbereiche und Einsatzszenarien • Infrastrukturen • Roadmap

10:45 - 12:30 Uhr
SDN und NFV in der Analyse
- Wo steht der Markt?
- Was ist NFV und wo setzen wir es wann ein?
- Welchen Stellenwert hat Hardware in den neuen Technologien?
- Wie hängen SDN und NFV zusammen?

Dipl.-Inform. Petra Borowka-Gatzweiler, UBN

14:00 - 15:30 Uhr
Netzwerk-Design-Lösungen im direkten Vergleich
Wir haben im Moment wesentliche Design-Entwicklungen, die sich direkt widersprechen. Gleichzeitig sind einige der neuen Ansätze auch sehr komplex. Hier stellt sich die Frage, wie man mit möglichst wenig Aufwand ein maximal gutes Design erreichen kann.

Wir diskutieren mit Ihnen:
- Layer 2 Design
- Layer 3/4 Design
- Sonderfälle
- Empfehlungen

Markus Geller, ComConsult Research GmbH

15:45 - 17:00 Uhr
VMware NSX: Zukunft oder Irrweg?
Immer mehr der traditionellen Anbieter integrieren NSX in ihre Lösungen, zum Teil sogar strategisch und ohne wirkliche Alternative. Cisco grenzt sich dabei klar durch einen eigenen Weg ab.

Wir analysieren:
- Was ist der Bedarf?
- Wie nutzbar ist NSX wirklich?
- Sind die vorhandenen Alternativen besser?
- Gibt es einen mindestens gleichwertigen herstellerneutralen Weg?

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

10:30 - 10:45 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause
15:30 - 15:45 Uhr Kaffeepause

Mittwoch, der 29.06.16 - UC, das Ende von ISDN: wie sieht die Kommunikations-Lösung der Zukunft aus?

UC-Projekte haben in den letzten Jahren deutlich an Komplexität gewonnen. Zwar haben sich die Produkte weiter entwickelt, doch gleichzeitig hat sich ein neues Verständnis von Kommunikation mit einer gleichzeitigen Verschiebung der Funktionsbereiche ergeben. Moderne Browser beinhalten heutzutage die komplette Funktionalität eines UC-Clients für Sprache und Video und generieren die Frage nach der Zukunft des Telefons. Gleichzeitig ist ISDN am Ende, es wird 2017 abgeschaltet. Dies erfordert eine Neubestimmung des Verständnisses von Kommunikation: was gehört dazu, wie kommunizieren wir in Zukunft mit Externen?

9:00 - 17:00 Uhr
Wir analysieren für Sie:
- Motivation: Warum All-IP? Einführung in das Thema
- SIP Trunking vs. PSTN: Was sind die wesentlichen Unterschiede?
- Standards für Enterprise- und Provider-Peering
- Session Border Controller: Funktionalität und Markt
- Provider-Marktübersicht: Geschäftsmodelle und Angebote
- Was kommt nach 2018?
- Architektur einer globalen All-IP Kommunikation

Dipl.-Inform. Petra Borowka-Gatzweiler, UBN
Markus Geller, ComConsult Research GmbH

10:30 - 10:45 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause
15:00 - 15:15 Uhr Kaffeepause

Donnerstag, der 30.06.16 - WLAN und Mobilfunk

Der funkbasierten Kommunikation gehört die Zukunft. Sie wird die kabelgebundene Alternative nicht verdrängen, aber die Zahl der kabellosen Endgeräte wird deutlich überwiegen. Dies betrifft den Bereich innerhalb der Unternehmen ebenso wie die Kommunikation außerhalb. Tatsächlich wird die jetzige klare Trennung zwischen Mobilfunk und WLAN in den nächsten 5 Jahren abgelöst werden durch einen mehr integrierten Ansatz, in dem ein Endgeräte den jeweils optimalen Zugang dynamisch wählt. In Konsequenz benötigen wir Infrastrukturen, die sowohl der Anzahl als auch den qualitativen Anforderungen mobiler Teilnehmer gewachsen sind. Und tatsächlich ermöglicht die neueste Generation von Produkten Lösungen, die so noch vor wenigen Monaten nicht möglich waren.

9:00 - 12:30 Uhr
Enterprise WLANs und ihre technologischen Grenzen
- Das Medienzugangsverfahren DCF: Ist es für eine immer größer werdende Anzahl von Teilnehmern pro Zelle geeignet oder laufen wir in ein Problem?
- Schneller, näher, höher: Wie sich WLAN-Technik in Richtung 10 Gigabit entwickelt
- MU-MIMO in der Analyse: Ist dies der Schlüssel zu höherer Performance in der Zelle?
- Wie profitieren Enterprise WLANs von den neuen Technologien?
- Wie sieht der Bedarf konkret aus, brauchen wir Multi-Gigabit und ist diese Entwicklung wirtschaftlich?

Dipl.-Ing. Michael Schneiders, ComConsult Beratung und Planung GmbH

14:00 - 17:00 Uhr
Die Analyse der neuesten Entwicklungen
- Explosives Wachstum in allen Anforderungsbereichen
- Echte Multi-Gigabit WLANs mit IEEE 802.11ad
- Die nächsten WiFi-Generationen 11ax und 11ay
- Die Entwicklung von LTE
- Problematik von LTE in lizenzfreien Bereichen
- Kommt schneller als man denkt: 5G Mobilfunk
- Anforderungen an unterstützende Infrastrukturen

Dr. Franz-Joachim Kauffels, Technologie-Analyst

10:30 - 10:45 Uhr Kaffeepause
12:30 - 14:00 Uhr Mittagspause
15:00 - 15:15 Uhr Kaffeepause

Freitag, der 01.07.16 - Sicherheit / WAN und Internet

Sicherheit in der IT wird zum dominierenden Thema der nächsten Jahre. Aber hier geht es nicht um hochfliegende Träume sondern um Informationssicherheit als integraler Bestandteil der IT-Architektur.

9:00 - 12:30 Uhr
Wir analysieren für Sie:
- Abwehr zielgerichteter Angriffe: Notwendigkeit sys tem- und anwendungsübergreifender Strategien
- Netzbasierende Sicherheit: Praxiserfahrungen aus den Bereichen Verschlüsselung, Zonenkonzepte, NAC und Testumgebungen
- Sicheres Cloud Computing und sicheres Mobile Computing: Möglichkeiten und Grenzen
- Sicherheit und UC: Immer offener und immer sicherer, ist das ein unlösbarer Widerspruch?

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

WAN und Internet wachsen untrennbar zusammen. Es gilt das beste aus den jeweils verfügbaren Lösungen zu nutzen und gleichzeitig mögliche Risiken zu vermeiden. Im Ergebnis geht es um eine schlüssige Weiterverkehrs-Architektur für alle bestehenden Anwendungsbereiche.

14:00 - 15:30 Uhr
Wir analysieren für Sie:
- Warum Internet und privates WAN beide erforderlich sind • Wie privates WAN und Internet zu einer sinnvollen Gesamtstruktur werden
- Eigene Perimeter Security versus Nutzung einer Internet Security Cloud
- Rolle von Software-Defined WAN

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

10:30 - 10:45 Uhr Kaffeepause
13:00 - 14:00 Uhr Mittagspause
15:30 Uhr Ende der Veranstaltung

Der Veranstalter behält sich Änderungen im Programm vor

Schwerpunktthema

Neue WLAN-Techniken in Enterprise WLANs?

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 „Tests und Analysen“. 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.

Da sind zum einen die Anwendungen, bei denen Mobilität wichtig, ja unabdingbar ist. Diese Anwendungen gibt es seit langem. Allerdings steigt nun der Bedarf nach hoher Bitrate. So werden im Automobilbau viele Funktionen der Fahrzeuge auf elektronischem Wege getestet. Am Band – meistens an dessen Ende – wird ein Testgerät mit der Diagnose-Steckdose des Fahrzeugs verbunden. Der Mitarbeiter prüft nun anhand eines auf dem Testgerät ablaufenden Programms allerhand Funktionen des Fahrzeugs. Bei dieser Gelegenheit erhalten zahlreiche Steuergeräte im Fahrzeug ihre Software, und die vom Kunden bestellten Funktionen werden freigeschaltet.

Es heißt, pro Fahrzeug werde ca. ein halbes Gigabyte Daten ausgetauscht. Und selbstverständlich müssen diese Daten über WLAN fließen, da sich das Fahrzeug am Band währenddessen fortbewegt. Und ebenso selbstverständlich muss der Datentransfer mit hoher Bitrate vonstattengehen, damit das Fahrzeug fahrbereit ist, wenn es am Band-Ende angekommen ist.

Um das „Betanken“ der Steuergeräte zu vereinfachen und vor allem den dabei herrschenden Zeitdruck zu entschärfen, sollen zukünftig neuartige Geräte eingesetzt werden. Diese Geräte werden bereits frühzeitig im Fahrzeug platziert und mit seiner Elektronik verbunden. Steuergeräte lassen sich auf diese Weise jederzeit mit der erforderlichen Software versehen. Der Vorteil liegt auf der Hand: Man spart Zeit am Band-Ende. Der Nachteil erschreckt die WLAN-Planer: Es werden in Summe mehrere hundert dieser Boxen unterwegs sein und Software Downloads können an beliebiger Stelle des Bandes erfolgen. Reicht es heute aus, nur im Bereich des Band-Endes eine WLAN-Verfügbarkeit mit hoher Bitrate bereitzustellen, ist dies zukünftig in der gesamten Montagehalle der Fall.

Zum zweiten drängen immer mehr drahtlose Anwendungen ins Feld, bei denen Mobilität eigentlich gar nicht gefordert ist. Es ist eben nur so wunderschön einfach, eine Netzwerk-Verbindung bereitzustellen, ohne dass man erst ein Kabel ziehen muss. Eine solche Anwendung entdeckte ich neulich in einem Logistik-Bereich, in dem Mitarbeiter damit beschäftigt sind, Teile aus Regalen zu nehmen und auf Kommissionier-Wagen abzulegen. Sicher, der Wagen ist beweglich und benötigt ein mobiles Terminal. Aber die Regale stehen fest. Dort sind Sensoren montiert, die zur Teile-Zählung verwendet werden und also mit der zentralen Logistikanwendung kommunizieren müssen. Und diese geschieht aus dem genannten Grund per WLAN!

Und zuletzt möchte ich nicht versäumen die vielen privaten WLAN-Endgeräte zu erwähnen, die heutzutage im Umlauf sind, nicht nur im Enterprise-Bereich. Mitarbeiter klagen immer wieder darüber, dass in den Arbeitsbereichen – seien es Büros mit bedampften Scheiben oder Stahlblech-beplankte Fertigungshallen – der Mobilfunkempfang schlecht sei. Dementsprechend stellen viele meiner Kunden flächendeckend spezielle WLANs für derlei Endgeräte zur Verfügung („Gäste-WLAN“). Bei einem Kunden konnte ich mit Hilfe des WLAN-Managementsystems ermitteln, dass die Zahl der innerhalb eines Monats am Gäste-WLAN angemeldeten Endgeräte die Gesamtzahl der in allen übrigen WLANs angemeldeten betrieblichen Endgeräte deutlich überstieg (!).

Was bedeutet dieser Trend zu immer mehr WLAN-Endgeräten mit immer höherem Bitratenbedarf für das WLAN? Wenden wir uns zunächst dem Medienzugangsverfahren zu.

DCF – Pest oder Segen für WLANs?

DCF bedeutet „Distributed Coordination Function“. Darunter versteht der Standard IEEE 802.11 das normale Medienzugangsverfahren im WLAN. Es basiert auf der zutiefst menschlichen Annahme, dass man nur reden sollte, wenn gerade niemand anderes spricht. WLAN-Endgeräte machen es also grundsätzlich wie die (höflichen) Menschen: Wer etwas sagen möchte, wartet bis der Vorredner ausgesprochen hat. Da hierbei eine gewisse Wahrscheinlichkeit dafür besteht, dass mehrere gleichzeitig reden („Kollision“) hat man sich eine Besonderheit ausgedacht. Wer reden möchte, nehme sich einen Würfel und werfe eine Zufallszahl. Eine dieser Zahl entsprechende Zeit muss gewartet werden, bevor man reden darf. Beim WLAN nennt man dieses Verfahren „Carrier Sense Multiple Access with Collision Avoidance“ (CSMA/CA) oder eben DCF.

Abbildung 1 illustriert dieses Verfahren. Eine Station – hier der Access Point – beendet gerade seine Aussendung, während zwei andere Stationen – B und C – darauf warten, senden zu dürfen. Zunächst lassen beide eine Pause („Distributed Inter-frame Spacing“, DIFS) verstreichen, bevor sie eine zufällige Zeit warten („Backoff“, während des „Contention Window“, CW). Station B kommt zuerst an die Reihe und sendet einen Frame. Station C muss sich gedulden und kommt erst beim nächsten Contention Window an die Rei-

he; sie kann den Rest ihrer Wartezeit „mitnehmen“, ohne eine neue Zufallszahl würfeln zu müssen. Abbildung 1 deutet auch an, dass jeder Frame vom Empfänger bestätigt wird. Diese „Acknowledges“ (ACK) dürfen ohne vorangehendes Contention Window bereits nach kurzer Wartezeit („Short Inter-frame Spacing“, SIFS) gesendet werden.

Über die Details dieses Verfahrens ließe sich noch viel mehr schreiben, z.B. dass man Quality of Service (QoS) über eine Variation der Wartezeit DIFS und des Contention Window realisiert hat. Eines ist jedoch klar: Je mehr Stationen beteiligt sind, desto schlechter wird das Verfahren funktionieren. Während meines Studiums habe ich eine Vorlesung namens Datenfernverarbeitung besucht. Darin wurden allerlei Formeln gelehrt, mit denen man derlei Zusammenhänge angeblich berechnen konnte. Zugegeben, ich habe das nicht wirklich verstanden. Aber die Analogie zur menschlichen Kommunikation finde ich anschaulich. Versuchen Sie mal, sich auf einer Fete angeregt zu unterhalten. Oder in der Diskothek. Wenn Sie CSMA dort konsequent anzuwenden versuchen, werden Sie kein Wort herausbringen, denn das Medium ist ununterbrochen belegt.

Diesen Zustand findet man häufig in großen Hallen, etwa in Logistikzentren oder Montagehallen. Dort ist einerseits eine große Menge Access Points installiert, und andererseits hören sich die Access Points gegenseitig sehr gut, da es kaum dämpfende Zwischenwände gibt. In solchen Umgebungen reichen häufig alleine die regelmäßig von den Access Points ausgesandten Beacon Frames aus, um das Medium komplett zu belegen. Den Stationen bleibt dann nur noch, zu schweigen. Dieser Zusammenhang lässt sich sehr gut mit dem „Wi-Fi Overhead Calculator“ nachvollziehen, zu finden unter **http://www.revolutionwifi.net/revolutionwifi/p/ssid-overhead-calculator.html.** Das werden Sie bereits aus meinen früheren Artikeln kennen.

Alles bisher Gesagte führt zu meinem ersten **Fazit: DCF funktioniert schlecht in WLANs mit einer großen Anzahl von Teilnehmern.**

Diesen Zusammenhang kennen wir bereits aus dem Ethernet. Nein, ich meine nicht das moderne „geswitchte“ Ethernet, sondern Ethernet über Koaxialkabel, wie ich es vor über 20 Jahren kennengelernt hatte. Die Fehlersuche in jenen Tagen offenbarte, dass es nicht auf die Zahl der angeschlossenen Stationen ankam. Vielmehr war deren Sendewahrscheinlichkeit bestimmend für Kollisionen und deren negative Auswirkungen. Eine große Zahl von Terminals, die ständig Zeichen mit einem Großrechner austauschten, war wesentlich problematischer als eine ebenso große Zahl von PCs, die beizeiten Dateien von oder zu einem Server kopierten. Besonders problematisch wurde es aber, wenn PCs und Terminals ein gemeinsames Ethernet nutzten. Diese Erkenntnis lässt sich ohne weiteres auf WLAN übertragen. **Fazit: Gleichartiger Datenverkehr aller Stationen wirkt sich positiv auf das Verhalten der DCF aus.**

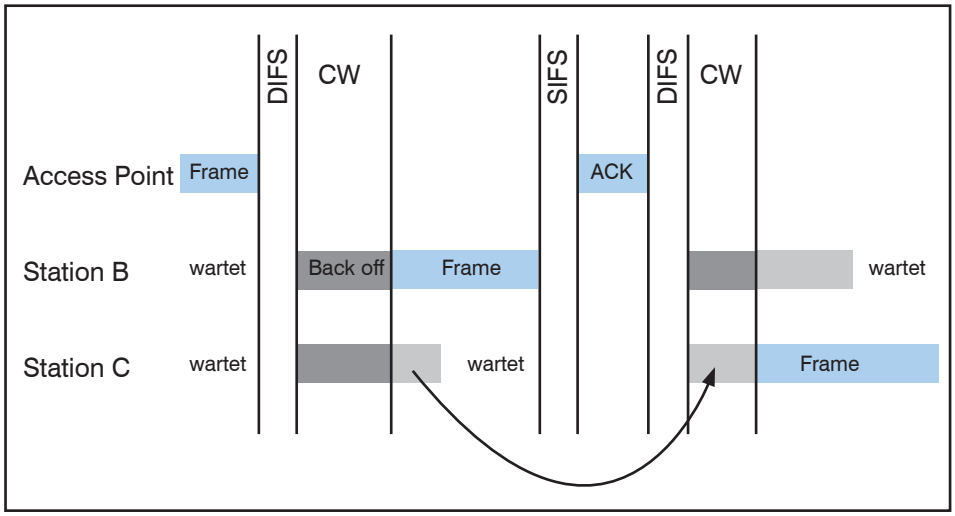


Abbildung 1: Medienzugang bei WLAN mittels DCF

Zuletzt möchte ich dennoch eine Lanze für die DCF brechen. Das Verfahren ist so einfach, dass es sich durchsetzen konnte. Erinnern Sie sich noch an den europäischen Gegenentwurf zur IEEE 802.11? Das HIPERLAN (High Performance LAN) besaß ein optimiertes Medienzugangsverfahren, das Kollisionen zu vermeiden suchte. Der Nachfolger HIPERLAN/2 wurde gar als „Wireless ATM“ bezeichnet. Der Preis dafür war eine hohe Komplexität und entsprechend hohe Entwicklungskosten. Dementsprechend verschwand diese Technik schließlich in der Schublade, ähnlich wie die ATM-LAN-Emulation. Das WLAN mit DCF hat sich dagegen durchgesetzt weil es sich so einfach implementieren ließ.

Das Problem der WLAN-Reichweite

Der „Wi-Fi Overhead Calculator“ (s.o.) zeigt sehr anschaulich, dass ein Funkkanal desto mehr belegt wird, je geringer die Bitrate ist, mit der die Beacon Frames abgestrahlt werden. Geringe Bitraten reichen weiter – auch diese Aussage kennen Sie aus meinen früheren Artikeln: In den Datenblättern der WLAN-Ausrüster findet man Angaben über Empfangsleistungen (in Milliwatt bzw. dessen Äquivalent dBm), die erforderlich sind, um WLAN-Daten einer bestimmten Modulationsart bzw. Bitrate sicher aufnehmen zu können. Ein moderner Access Point, der mit IEEE 802.11n bei 300 Mbit/s betrieben wird, benötigt demnach typischerweise eine Empfangsleistung von 72 dBm. Für die geringstmögliche Bitrate, also z.B. 6 Mbit/s bei IEEE 802.11a im 5-GHz-Band oder bei IEEE 802.11g im 2,4-GHz-Band werden nur noch 96 dBm benötigt; das ist nur noch ungefähr ein 250stel.

Die Empfangsleistung jeglicher Funkwellen nimmt im freien Raum quadratisch mit dem Abstand ab. Ein 250stel der Empfangsleistung wird also etwa beim 16fachen Abstand erreicht. Ich habe diesen Zusammenhang in Abbildung 2 dargestellt. Dieser Abbildung liegt eine Formel für die Freiraumausbreitung von Funkwellen zugrunde, und sie stellt den Zusammenhang in logarithmischem Maßstab dar. Demnach können im 5-GHz-Band ca. 180 Meter überbrückt werden, wenn man mit 300 Mbit/s sendet. Frames, die mit der langsamsten Bitrate abgestrahlt werden, reichen gar 2,8 Kilometer weit.

Nun werden die Beacon Frames nicht zufällig mit der geringstmöglichen Bitrate ausgestrahlt. Ziel ist es, alle möglichen WLAN-Endgeräte zu unterstützen. Der Handscanner aus dem Jahre 2003 soll ebenso eine Chance erhalten wie das ultramoderne Smartphone vom letzten Weihnachtsfest. Die Beacon Frames repräsentieren quasi den kleinsten gemeinsamen Nenner aller WLAN-Endgeräte.

Würde man dagegen alle Altgeräte aussondern, könnte man den kleinsten gemeinsamen Nenner anheben. Es ergäbe sich eine Homogenisierung der WLAN-

Reichweiten. Reichten die Beacon Frames nicht weiter als die Mehrzahl der WLAN Endgeräte, könnte die DCF wesentlich besser wirken. Anders ausgedrückt ließe sich auf diese Weise eine Funkzelle in ihrer Größe und Auswirkung besser begrenzen.

Fazit: Eine Homogenisierung der im WLAN möglichen Bitraten wirkt sich positiv auf das Verhalten der DCF aus.

Wie sich Fehler bei der Konfiguration erlaubter Bitraten der Access Points in der Praxis auswirken können, konnte ich neulich bei einem Kunden erleben. Ein Flurförderfahrzeug bewegt sich auf den Fahrwegen einer Fertigungshalle. Access Points sind in regelmäßigen Abständen an den Säulen der Halle montiert. Abbildung 3 zeigt beispielhaft die Konfiguration. Nun würde man erwarten, dass sich der WLAN Client, der sich auf dem Fahrzeug befindet, brav nacheinander an den Access Points 1, 2, 3 und 4 assoziiert. Etwas anderes war regelmäßig der Fall, wie wir an schlechter Performance im Bereich der Access Points 2 feststellten. Hier stockte die Kommunikation regelmäßig. Ein Test mittels PING zeigte, dass die Wartezeiten deutlich höher wurden, wenn das Fahrzeug diesen Bereich von links kommend durchquerte.

Schließlich haben wir mit Hilfe des WLAN Managements untersucht, in welcher Reihenfolge sich der Client an den Access Points assoziierte. Dabei konnten wir immer wieder eine andere als die erwartete Reihenfolge beobachten. Zunächst war der Client noch eine Weile an 1 assoziiert. Danach wechselte er zu 3, kurze Zeit später zu 2, dann wieder zu 3 und zuletzt erwartungsgemäß zu Access Point 4; diese Reihenfolge ist mit den Pfeilen in Abbildung 3 angedeutet.

Als erstes würde man eine ungünstige Lage des Access Point 2 erwarten. Vielleicht empfängt der Client den Access Point 3 zunächst stärker als 2. Immerhin lässt dessen Position an dem Querweg solches vermuten, denn hier gibt es keine Hindernisse in Richtung Fahrweg. Eine Ausleuchtungs-Messung in diesem Bereich konnte das jedoch nicht bestätigen.

Letztlich entdeckten wir, dass der Access Point 3 mit einem anderen WLAN Controller verbunden war. Und dort war die Mindest-Bitrate auf 6 Mbit/s eingestellt. Bei allen anderen Access Points betrug sie 18 Mbit/s! Damit wurde das Verhalten erklärlich. Access Point 3 präsentiert sich gegenüber den Clients als einer mit vergleichsweise hoher Reichweite. Deshalb assoziierten sie sich dort eher als beispielsweise an Access Point 2. Dass die

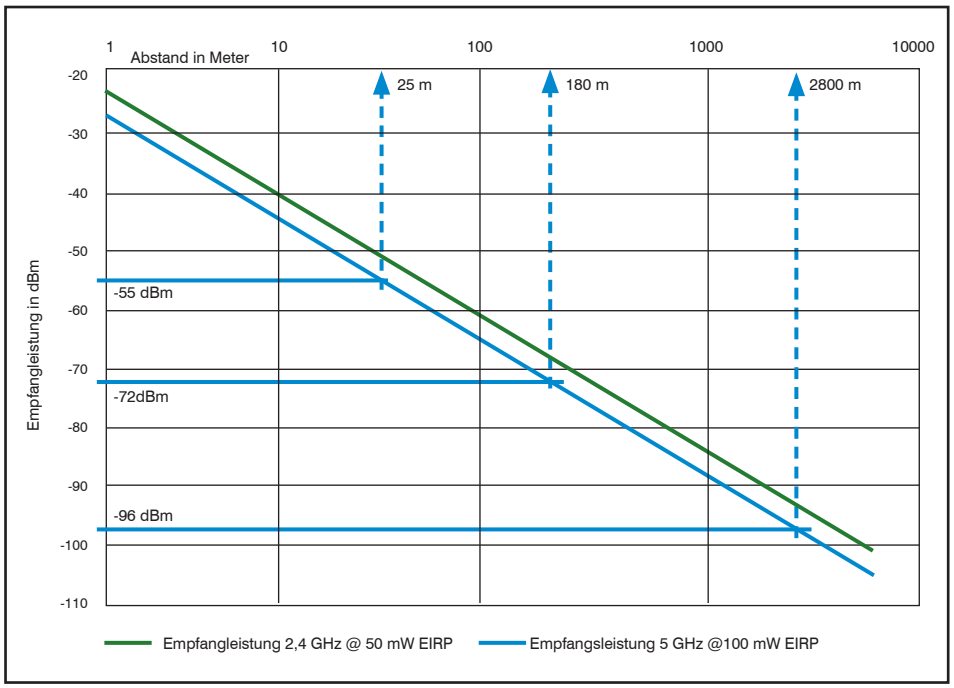


Abbildung 2: Signalstärke als Funktion des Abstandes

Datenübertragung über Access Point 3 langsamer sein würde, haben die WLAN Clients bei ihrer Handover-Entscheidung nicht berücksichtigt. **Fazit: man achte auf eine konsistente Konfiguration aller Access Points.**

IEEE 802.11ac „Wave 3“, das Multi-Gigabit-WLAN?

Bisher ging es um die Probleme am unteren Ende der WLAN-Bitratenskala. Und wie sieht es am oberen Ende aus? Bereits vor einem halben Jahr hat der Chip-Hersteller Quantenna seine „10G Wave 3“ WLAN-Produktreihe angekündigt (siehe **http://www.quantenna.com/pressrelease-09_08_15.html**) und präsentiert auf seiner Website ein wahrlich erschreckendes Aufmacherbild (Abbildung 4). Wie kommen die auf „10G“?

Hierzu sehen wir uns zunächst die Evolution des Gigabit WLAN an. Die Abbildung 5 gibt eine Übersicht. Die meisten von Ihnen werden WLAN Access Points der Technik IEEE 802.11n betreiben. Diese Technik unterstützt zwar theoretisch eine Brutto-Bitrate 600 Mbit/s. Praktisch jedoch haben die Hersteller lange Zeit Komponenten mit nur 300 Mbit/s verkauft, basierend auf der Technik des „Multiple Input Multiple Output“ (MIMO) mit zwei Daten-

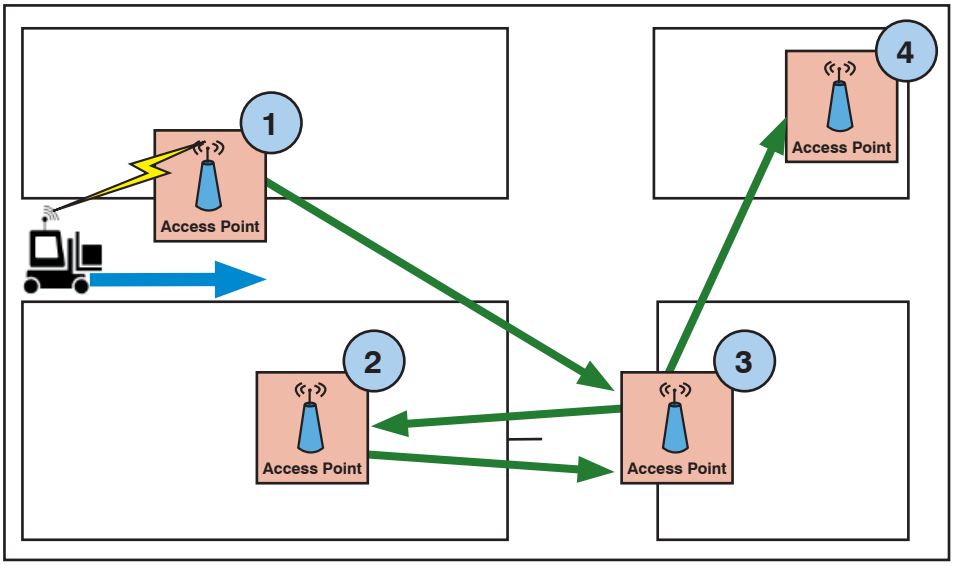


Abbildung 3: Verbindungs-Reihenfolge eines bewegten WLAN Client zu Access Points

strömen, als „Spatial Streams“ bezeichnet. Die zuletzt angebotenen Serien der 11n Access Points unterstützen drei Spatial Streams mit entsprechend 450 Mbit/s.

Wenn Sie bereits Access Points mit dem aktuellen Standard IEEE 802.11ac einsetzen, wird es sich wahrscheinlich um APs mit der ersten Generation dieser Chips handeln. Diese als „Wave 1“ bezeichnete Technik unterstützt ebenfalls nur drei Spatial Streams. Da aber der Funkkanal hier 80 MHz breit sein darf und außerdem mit der 256 QAM eine acht- anstatt sechswertige Modulation eingesetzt werden kann, steigt die Bruttobitrate auf nunmehr 1,3 Gbit/s an.

Vor ca. einem Jahr stellte der Chip-Hersteller Qualcomm seine WLAN-Chips gemäß IEEE 802.11ac „Wave 2“ vor (siehe **https://www.qualcomm.com/news/releases/2015/06/01-0**). „Wave 2“ erweitert den Funktionsumfang der bisherigen Chips um zwei Features. Erstens wird nun ein 160 MHz breiter Funkkanal unterstützt, der auch aus zwei separaten Kanälen mit je 80 MHz bestehen kann. Und zweitens gibt es nun „Multi User MIMO“ (MI-MIMO), dazu später mehr. Mit drei Spatial Streams erreicht man so 2,6 Gbit/s, mit vier Spatial Streams sogar 3,5 Gbit/s. Diese Technik gibt es bereits in Consumer-Produkten, aber auch die neuesten Access Points für den Enterprise-Bereich enthalten diese Chips. Beispiele sind Access Points der Serie 330 von HP (Aruba), Cisco Aironet 1850 und AP3935 von Extreme Networks. Interessanterweise sind diese drei Produkte nur für 80 MHz Kanalbandbreite spezifiziert. Der AP330 von Aruba beherrscht zwar auch 160 MHz, dann aber nur mit zwei Spatial Streams. Wie dem auch sei, die Brutto-Bitrate dieser Produkte beschränkt sich auf „nur“ 1,7 Gbit/s.

Und nun kommt also „Wave 3“. Dabei handelt es sich eigentlich um die vollständige Unterstützung aller in der Norm IEEE 802.11ac vorgesehenen Features. Erstmals schafft es Quantenna Communications also, 8 Spatial Streams umzusetzen; der Chipsatz trägt die Bezeichnung QSR10G.

IEEE 11ac erzielt mit 8 Spatial Streams und 160 MHz Kanalbreite knapp 7 Gbit/s. Quantenna implementiert dazu noch eine neue 10wertige Modulation (1024 QAM). Damit werden es ca. 8,6 Gbit/s. Und jetzt kommt der Trick: Parallel dazu werden im 2,4-GHz-Band noch vier Spatial Streams mit 40 MHz Bandbreite und 1024 QAM gesendet. Das gibt dann insgesamt 9,7 Gbit/s, also etwa 10G! Ein Datenblatt habe ich noch nicht gefunden und auch kein Produkt, das diesen Chipsatz enthält. Gespannt bin ich jedenfalls auf die Empfindlichkeit der Empfänger.

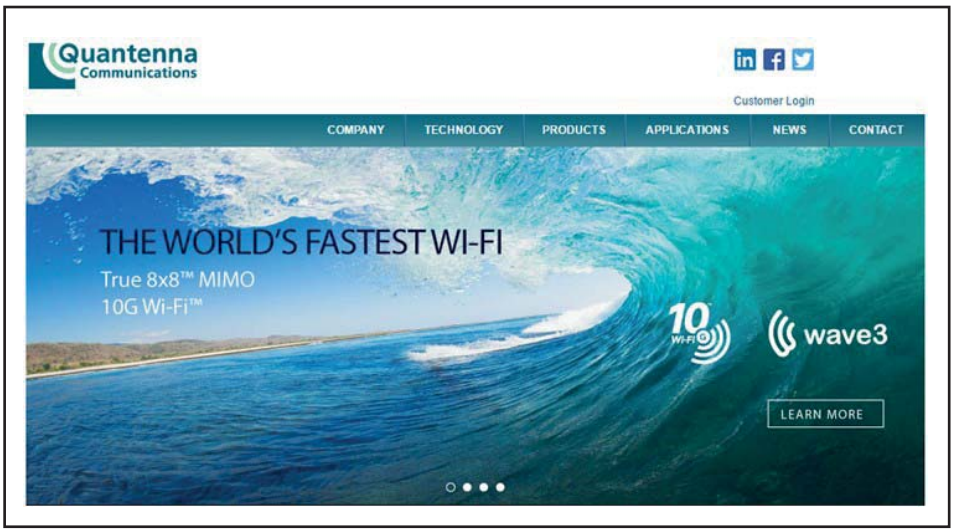


Abbildung 4: Werbung des Chip-Herstellers Quantenna Communications

Die Frage ist also, wie viele „dBm“ am Empfänger benötigt werden, um diese Übertragungsleistung zu erreichen. Schaut man in die Datenblätter aktueller Produkte, erkennt man für die höchste Bitrate Werte bei -55 dBm. In das Diagramm in Abbildung 2 eingetragen, kommt man auf einen Abstand von 25 Metern. Nehmen wir an, Quantenna sei nicht wirklich in der Lage zu zaubern, dann braucht deren QRS10G noch einmal die doppelte Leistung für die doppelte Kanalbandbreite und desgleichen für die doppelte Anzahl von Spatial Streams. Das macht also die vierfache Leistung oder -49 dBm. Für eine Vervierfachung der Leistung muss der Empfänger seinen Abstand zum Sender halbieren. Wir reden also nun von nur noch 12,5 Metern im freien Raum. Die von uns schon mehrfach aufgestellte Behauptung, eine WLAN- Zelle werde zukünftig die Grenzen eines Büros nicht überschreiten, scheint sich also zu bewahrheiten.

Aber wie macht man es in einer Industrie-Umgebung? Hier fehlt die natürliche Zellenbegrenzung der Bürowand mit ihrer zusätzlichen Dämpfung. Und dank der vielen bereits vorhandenen Endgeräte, die „nur“ 11n unterstützen und also bis zu 180 Meter weit funken (siehe nochmals Abbildung 2), werden wir es erneut mit stark frequentierten Zellen zu tun haben. Ganz abgesehen von dem praktischen Problem, alle 20 Meter einen Access Point montieren zu müssen, und zwar in der Nähe der mobilen Endgeräte, d.h. nur wenige Meter von den entsprechenden Fahrwegen entfernt. Um ehrlich zu sein: Ich weiß dafür noch keine Lösung. Wir werden es probieren müssen. Aber auch hier gilt das Fazit von oben: Es wird nur mit möglichst ähnlichen Bitraten funktionieren.

Und was bleibt am Ende vom Multi-Gigabit-WLAN übrig?

	802.11n heute	802.11 ac "Wave 1"	802.11 ac "Wave 2"	802.11 ac "Wave 3"
Band	2,4 GHz 5 GHz	5 GHz	5 GHz	5 GHz
Spatial Streams	3 (4)	3	3 (4)	8
MIMO	Single User	Single User	Multi User	Multi User
maximale Kanalbreite	40 MHz	80 MHz	160 MHz	160 MHz
Modulation	64QAM	256QAM	256QAM	256QAM
Brutto-Bitrate	450 (600) Mbit/s	1,3 Gbit/s	2,6 (3,5) Gbit/s	6,9 Gbit/s
Durchsatz max.	290 Mbit/	850 Mbit/s	1,7 (2,3) Gbit/s	4,5 Gbit/s

Abbildung 5: Übersicht der aktuellen WLAN-Standards

Seien wir realistisch:

- Eine gleichzeitige Nutzung des 2,4- und des 5-GHz-Bandes für eine WLAN-Übertragung scheidet wohl aus. Die beiden Bänder bieten ja gerade die Chance, zwei separate WLANs mit unterschiedlichen Kommunikationsprofilen aufzubauen.

- 160 MHz Kanalbandbreite belegt de facto das gesamte heute zur Verfügung stehende Spektrum bei 5 GHz. Es ist nicht absehbar, dass so viele zusätzliche Frequenzen hinzukommen werden, dass wir zukünftig 3 mal 160 MHz nutzen könnten, eine Voraussetzung für eine einigermaßen überlappungsfreie Zellenplanung.

- Mit 80 MHz Kanalbandbreite ginge es so gerade eben. Typische WLAN-Frequenzkonzepte weisen jedoch den unteren 100 MHz (Kanäle 36 bis 48) meist eine Sonderstellung zu. Damit bleibt also als realistische Kanalbandbreite im Enterprise-Bereich nur 40 MHz übrig.

- Mit 40 MHz Kanalbreite und 8 Spatial Streams lassen sich 1,6 Gbit/s brutto erzielen. Der Nettodurchsatz erreicht dann bestenfalls 1 Gbit/s. Das gilt aber nur, wenn auch das mobile Endgerät über einen WLAN-Adapter mit 8 Spatial Streams verfügt.

In der Praxis der Enterprise-WLANs wird sich also das eine Gigabit Nettodurchsatz nicht erzielen lassen. **Fazit: IEEE 802.11ac „Wave 3" ist de facto nicht einmal ein Gigabit WLAN.**

Was leistet MU-MIMO?

MU-MIMO wurde als großer Fortschritt der „Wave 2" angepriesen. Dieses Feature ermöglicht es einem Access Point, gleichzeitig Daten an mehrere Endgeräte zu senden. Dazu nutzt er die Richtwirkung seines Antennen-Arrays aus. Damit das klappt, muss der Access Point mindestens über vier Antennen verfügen. Die Abbildung 7 illustriert das Prinzip.

Mit MU-MIMO ist die Hoffnung verbunden, den Funkkanal besser ausnutzen zu können. Denn die meisten Endgeräte werden weniger Spatial Streams unterstützen als die Access Points. Typische Handheld Devices, wie z.B. Smartphones, beherrschen heutzutage sogar nur einen Spatial Stream. MU-MIMO kann mehrere solcher Endgeräte unterstützen. Aktuelle „Wave 2" Access Points (Beispiele siehe oben) unterstützen drei gleichzeitige Endgeräte. Allerdings sind dabei noch einige Einschränkungen zu beachten:

- Selbstverständlich muss auch das empfangende Endgerät über einen „Wave 2"-Adapter verfügen, selbst wenn es nur einen Spatial Stream beherrscht. Damit MU-MIMO überhaupt funktioniert, ist ein gemeinsames Protokoll zwischen Access Point und Endgerät vonnöten.

- MU-MIMO funktioniert nur im Download, also in der Richtung vom Access Point zum Endgerät. Eine Spezifikation der Gegenrichtung, also „Upload MU-MIMO" (UL MU-MIMO) ist erst Gegenstand der IEEE 802.11ax („High Efficiency WLAN"), deren Fertigstellung nicht vor Ende 2018 zu erwarten ist.

Und jetzt dürfen Sie sich fragen, wie groß die Wahrscheinlichkeit ist, dass es in Ihren Enterprise WLANs mehrere „Wave 2"-Endgeräte gibt, die gleichzeitig Daten empfangen sollen. **Fazit: Der Nutzen von MU-MIMO für Enterprise WLANs aus heutiger Sicht äußerst gering.**

Fügen wir alles zusammen!

Es führt kein Weg daran vorbei: Einerseits werden WLAN-Produkte immer schneller und leistungsfähiger. Im Rahmen des Lifecycle Managements werden diese Produkte früher oder später Einzug in unsere WLAN-Installationen halten. Andererseits wird es zukünftig vermehrt Anwendungen geben, die hohe Bitraten benötigen. Die Anforderung ist es, mehrere hundert Megabyte in einigen Sekunden übertragen zu können. Und die Entwickler dieser Anwendungen testen das zunächst in ihren eigenen Labors, die wahrscheinlich über eine optimale WLAN-Umgebung verfügen.

Die heute noch überaus heterogene Client-Landschaft in Enterprise WLANs wird mit solchen Anforderungen nicht zurechtkommen. Das belegen unsere zahlreichen Fehlersuche-Einsätze der letzten Jahre. Wie lässt sich das in den Griff bekommen? Hier ein erster Vorschlag für eine sinnvolle Vorgehensweise:

- Ordnen Sie die WLAN-Anwendungen Ihres Hauses in verschiedene Kategorien ein. Es gibt Anwendungen, bei denen nur wenige Daten ausgetauscht werden, wie beispielsweise Handscanner im Logistikbereich. Bestimmte dieser Anwendungen erfordern darüber hinaus kurze Antwortzeiten und eine unterbrechungsfreie WLAN-Verbindung, wie beispielsweise fahrerlose Transportfahrzeuge (FTF). Andere Anwendungen verlangen hohe Bitraten, wie zum Beispiel die oben erwähnten Testgeräte. Auch Büro-Umgebungen, bei denen vollständig auf eine Ethernet-Versorgung der Clients verzichtet wurde („WLAN Only"), fallen in diese Kategorie.

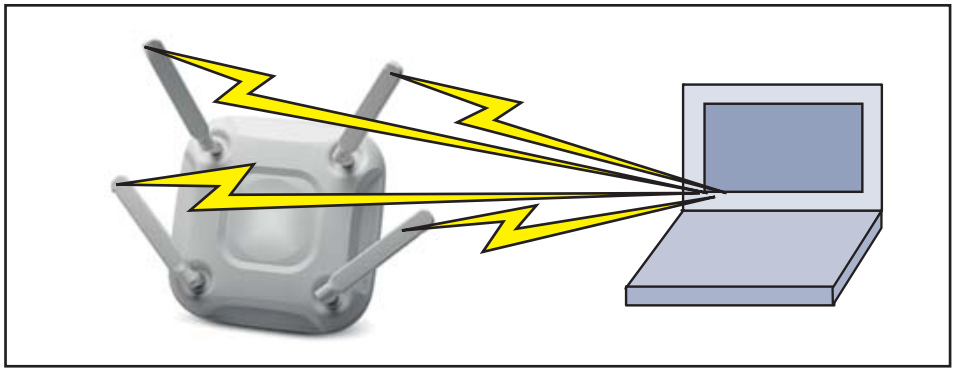


Abbildung 6: MIMO – Ein Endgerät nutzt die volle Bitrate

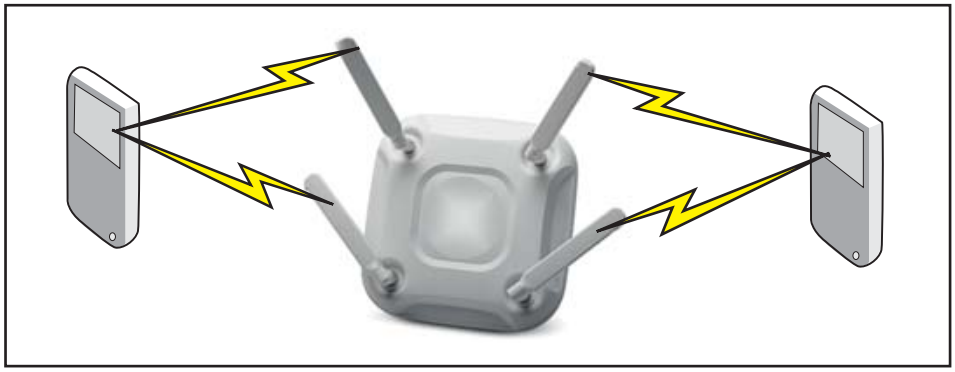


Abbildung 7: MU-MIMO – mehre Endgeräte empfangen gleichzeitig unterschiedliche Daten

- Überlegen Sie anhand Ihrer Kategorisierung, welche Anwendungen Sie in einem WLAN kombinieren können und welche nicht. Ziel ist es, so wenige WLANs – d.h. SSIDs – wie möglich einzurichten. Selbstverständlich spielen bei dieser Überlegung Sicherheitsaspekte eine Rolle.

- Legen Sie einen WLAN-Frequenzstandard für Ihr Unternehmen fest. Darin ist angegeben, welches WLAN welche Kanäle nutzen darf. Typische Frequenzstandards umfassen drei Bereiche, nämlich die Kanäle 1-11, 36-48, 52-140. Denkbar ist es, zusätzlich die Kanäle 52-64 als separaten Bereich auszuweisen.

- Weisen Sie nun die WLANs den Bereichen Ihres Frequenzstandards zu. Dabei sollten Sie beachten, dass nur der oberste Bereich die Kanalbündelung auf 40 MHz zulässt. Hier sind also die Anwendungen hoher Bitrate anzusiedeln. Und dann gibt es bestimmt noch „Altlasten“, die das 5-GHz-Band überhaupt nicht unterstützen. Die kommen dann auf die Kanäle 1-11, d.h. ins 2,4-GHz-Band.

Sie erkennen das Ziel: die **Parallelisierung mehrerer WLANs**. Um zu meinem einleitenden Beispiel der DCF zurückzukehren: Schicken Sie die Gesprächsteilnehmer Themen-bezogen in unterschiedliche Räume und schließen Sie die Türen. Das Ergebnis könnte vielleicht die folgende Aufteilung sein:

- 2,4 GHz, Kanäle 1 bis 11: „Legacy WLAN“ zur Unterstützung von Altgeräten. Es steht zu erwarten, dass sich hier die Anwendungen wiederfinden, die auf kurzen Nachrichten basieren.

- 5 GHz, Kanäle 36 bis 48: „Automation WLAN“ mit Komponenten, bei denen es auf die Übertragungssicherheit ankommt. Diese WLAN sind häufig örtlich begrenzt, beispielsweise auf eine oder mehrere Anlagen.

- 5 GHz, Kanäle 52 bis 140: „High-speed WLAN“ für alle Anwendungen, bei denen es auf die Übertragung hoher Datenmengen in kurzer Zeit ankommt.

Und in welche der drei WLANs soll man nun die große Zahl der privaten Smartphones und Tabletts einordnen? Die Antwort ist klar: In keines der drei. Diese Endgeräte besitzen normalerweise eine Mobilfunkschnittstelle, über die sie Internetverbindung erlangen, wenn sie außerhalb Ihres Unternehmens herumgetragen werden. Warum also nicht auch innerhalb Ihres Unternehmens? Es ist also eine gute Idee, für eine gute Ausleuchtung Ihrer Büros und Hallen mit WLAN **und** mit Mobilfunk zu sorgen. Diese Lösung wäre gleichzeig eine elegante Antwort auf die Frage, wie man den Gast-Geräten Internetzugang gewährt, ohne dabei die Integrität und Verfügbarkeit der unternehmenskritischen WLAN-Kommunikation zu gefährden.

Wie dem auch sei, die Zukunft der Enterprise WLAN ist in einer Parallelisierung verschiedener Funknetze mit unterschiedlichen Anwendungen zu suchen.

Standpunkt

Vorsicht mit „Roaming Profiles“!

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.

Microsoft Windows ist doch etwas tolles, wenn man es im Zusammenhang mit Windows Servern und dem Verzeichnisdienst „Active Directory“ (AD) einsetzt. Man kann sich mit seinem Benutzernamen und Kennwort an einem beliebigen Windows-PC anmelden, solange dieser Mitglied im AD des Unternehmens ist. Und besser noch: Überall blickt der Anwender auf seine gewohnte Benutzeroberfläche. Alle Icons auf dem Desktop und das Hintergrundbild erscheinen wie gewohnt. Das mühsam angepasste persönliche Startmenü enthält die gewohnten Einträge an gewohnter Stelle, Kennworte und Zertifikate wandern mit. Sogar Einstellungen in den Programmen sind überall dieselben, wie beispielsweise die „Symbolleiste für den Schnellzugriff“ in Microsoft Office.

Wie macht Microsoft das? Ganz einfach: Auf jedem Windows PC hat jeder Anwender ein „Benutzerprofil“. Das ist eigentlich nur ein Verzeichnisbaum mit allerhand Unterverzeichnissen. Da gibt es Verzeichnisse für Dokumente, Bilder und Videos. Die „Favoriten“ des Internet Explorer sind Dateien in einem speziellen Verzeichnis und auch der Desktop ist eigentlich ein Verzeichnis.

Viele Anwendungen legen Einstellungen in der so genannten Windows Registry ab. Die Registry hat einen Benutzer-spezifischen Teil. Dieser Teil ist als Datei im Benutzerprofil abgelegt. Und dann gibt es noch das Verzeichnis „AppData“, in dem sich die restlichen Einstellungen befinden, wie das Startmenü, Office-Vorlagen und Benutzer-Zertifikate. Eigentlich werden die Unterverzeichnisse von AppData von allen Anwendungen zur Ablage irgendwelcher Informationen benutzt, seien es wichtige oder auch weniger wichtige. Manches ist auch unwichtig. So verzichten viele Anwendungen darauf, die im Benutzerprofil abgelegten Daten wieder zu löschen, wenn sie offensichtlich nicht mehr benötigt werden. Das passiert regelmäßig, wenn man Anwendungen deinstalliert.

Damit der Benutzer an jedem Rechner dasselbe Profil vorfindet, kopiert Microsoft es auf einen Server im AD. Das nennt man

ein „Server-gespeichertes Profil“, oder etwas eleganter „Roaming Profile“. Meldet der Anwender sich an, synchronisiert Windows die Daten des Benutzerprofils mit der Kopie auf dem Server. Bei der Abmeldung passiert dasselbe. Leider muss Windows dazu in jedes Verzeichnis des Benutzerprofils hineinschauen und jede Datei auf Aktualität prüfen. Da Benutzerprofile mit den Jahren recht umfangreich werden (s.o.) kommen für eine Synchronisation schnell mehr als zehntausend (!) Zugriffe zusammen; das habe ich bei meinen Messungen schon oft gesehen. Wenn dann – wie bei einem meiner Kunden – das Rechenzentrum 100 km entfernt ist, dauert die Synchronisation gerne mehrere Minuten. Beim An- und beim Abmelden. Das ärgert den Anwender.

Was kann man in so einem Fall tun? Grundsätzlich gibt es zwei Möglichkeiten: Erstens bietet Microsoft inzwischen eine Alternative, oder besser Ergänzung zu den Roaming Profiles. Mittels „Folder Redirection“ werden ausgewählte Verzeichnisse des Benutzerprofils direkt auf dem Server abgelegt, brauchen also bei An- und Abmeldung nicht synchronisiert zu werden. Damit diese Verzeichnisse dennoch immer verfügbar sind, insbesondere auf Laptops, markiert Windows die umgeleiteten Verzeichnisse als „Offlinedateien“. Die werden auch synchronisiert, allerdings passiert das unbemerkt vom Anwender während er angemeldet ist.

Wer je mit Offlinedateien gearbeitet hat, weiß, dass dies nicht immer ganz unproblematisch ist. Daher kann man auf die zweite Möglichkeit verfallen: Vollständiger Verzicht auf Roaming Profiles. Vielleicht werden Sie damit Ihre Anwender gegen sich aufbringen. Aber seien wir ehrlich: Welcher Prozentsatz von Anwendern meldet sich regelmäßig (!) an unterschiedlichen Rechnern an? In der Regel passiert dies nur, wenn der Anwender einen neuen Rechner bekommt, also alle paar Jahre. Oder wenn der Anwender neben seinem Laptop ab und zu einen virtuellen Client bzw. einen Terminal Server nutzt.

Technisch gesehen, funktioniert die Arbeit ohne Roaming Profiles am besten. Um den Anwender dennoch einigermaßen zu beruhigen, können Sie Hilfe anbieten. Die Hilfe besteht in erster Linie darin, von vorneherein passend konfigurierte Clients bereitzustellen. So finden die Office-Programme von selbst alle wichtigen Vorlagen, die E-Mail-Signatur ist bereits mit dem vollen Namen des Anwenders vorkonfiguriert und das Startmenü hat schon die Ordnung, die der typischen Arbeitsweise Ihrer Mitarbeiter angepasst ist. Sicher, das erfordert einige Kreativität. Aber auch dafür stellt Microsoft allerlei nützliche Werkzeuge bereit: Das „Default Profile“ kann bereits beim „Betanken“ des neuen Rechners alle wichtigen Einstellungen samt Registry-Einträgen beinhalten. Anmelde-Scripts sorgen für Benutzer-spezifische Anpassungen und Gruppenrichtlinien erledigen den Rest.

Nicht zuletzt heißt es, den Anwender auf Ihre Seite zu bringen. Jeden Tag erst Benutzername/Kennwort eingeben und danach Kaffee holen, ist hinderlich. Am neuen Rechner erst einmal das gewohnte Hintergrundbild einzustellen, ist zu verkraften, wenn sich sonst schon einmal losarbeiten lässt. Und nicht zuletzt schaffen Sie auf diese Weise regelmäßig alle Altlasten in den Benutzerprofilen weg – Aufräumen zum Nulltarif.

Zweitthema

Unternehmensnetze folgen nicht immer dem Beispiel der Hyperscaler

Fortsetzung von Seite 1

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

Merkmale der Hyperscaler

Wie aus der Bezeichnung hervorgeht, stellt ein Hyperscaler eine Infrastruktur, eine Plattform oder Software für eine Anwenderzahl bereit, die nach oben extrem skalieren kann. Die typische Umgebung bei einem Hyperscaler ist in der Abbildung 1 dargestellt.

In der Abbildung 1 steht O() für „Order of“, d.h. „in der Größenordnung von“. Wie wir aus Pressemeldungen wissen, haben die größten Hyperscaler wie Google und Facebook für einige Dienste bereits die Grenze von einer Milliarde Anwender überschritten. Andere Dienste bei ihnen haben hunderte Millionen Nutzer, in der Abbildung 1 dargestellt als $O(10^8)$.

Wenn auch nur 1 % der Nutzer eines solchen Dienstes gleichzeitig aktiv ist, gibt es Millionen gleichzeitige Sessions. In Spitzenzeiten (zum Beispiel bei einem wichtigen Ereignis) darf aber eine solche Umgebung unter der Last nicht zusammenbrechen. Eine zweistellige Millionenzahl von Sessions darf somit zu keinem Problem führen. Wir wissen, dass Sessions in der Regel aus mehreren TCP-Verbindungen bestehen. Eine neunstellige Zahl von gleichzeitigen TCP-Verbindungen muss somit möglich sein.

Wer sogenannte statusbewusste Komponenten wie Firewalls und Load Balancer betrieben hat, weiß, dass auf dem Markt verfügbare, bezahlbare Komponenten dieser Art in der Regel bis zu einer fünf- oder sechsstelligen Zahl von gleichzeitigen TCP-Verbindungen skalierbar sind. Hyperscaler arbeiten gerne mit preiswerter Standardtechnik, wie man hört und liest. Es wäre also nicht verwunderlich, wenn es in einer solchen Umgebung zehntausende Load Balancer bzw. eine ähnliche Zahl Webserver gäbe. Diese stellen die Schnittstelle zu den Anwendern zur Verfügung. In der Regel greifen die Anwender über solche Front Ends auf Daten zu, die in Datenbanken gehalten werden. Auch die Anzahl der Datenbankserver kann bei einem Hyperscaler in die tausende gehen, allein wenn man bedenkt, wie viel Speicherplatz mittlerweile solche Firmen den Anwendern zur Verfügung stellen. Dabei wird sicherlich der verfügbare Speicherplatz überbucht. Aber wenn jeder von einer Milliarde Anwendern durchschnittlich nur 1 GB beim Hyperscaler belegen würde, kommt man auf 1 Exabyte, bzw. 1000 Petabytes. Wenn diese Daten in Datenbanken gehalten werden, braucht man dafür viele Datenbankinstanzen, zum Beispiel wie in der Abbildung 1 angenommen in der Größenordnung von 1000.

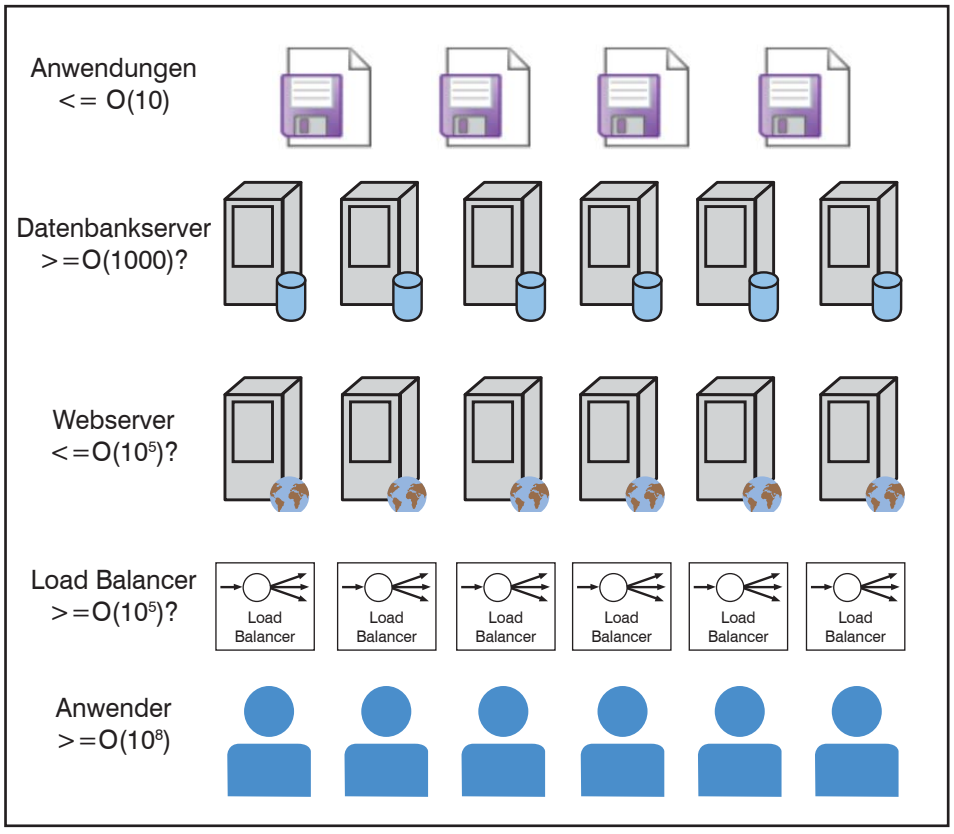


Abbildung 1: Typische Umgebung bei einem Hyperscaler

Zusammengefasst: Der Hyperscaler hat eine große Infrastruktur mit zehntausenden bzw. tausenden Instanzen. Diese hohe Zahl ist der hohen Nutzerzahl geschuldet. Alle gleichartigen Komponenten dieser großen Infrastruktur können (und sollten) ähnlich konfiguriert sein.

Betrachtet man dagegen die Anzahl verschiedener Anwendungen, ergibt sich ein ganz anderes Bild. Ein Hyperscaler betreibt in der Regel eine Handvoll bis wenige Dutzend verschiedene Applikationen. Jede dieser Anwendungen hat es hinsichtlich der Nutzerzahl in sich. Einzelne Dienste und Anwendungen (wie zum Beispiel Google Mail) können die Zahl von einer Milliarde Nutzer erreichen.

Zum Vergleich: IT-Umgebung eines typischen Unternehmens

Abbildung 2 zeigt die IT-Umgebung eines typischen mittleren bis großen Unternehmens. Dieses Unternehmen hat eine vierstellige Anzahl von IT-Benutzern. Die Anzahl der intern genutzten Load Balancer ist innerhalb der Unternehmensnetze meistens einstellig. Viele Webserver werden nicht über Load Balancer erreicht, weil die Hochverfügbarkeit durch andere Mechanismen wie Server Cluster oder Servervirtualisierung erreicht wird und die Leistung einer einzigen Serverinstanz für die gleichzeitig zugreifenden Benutzer meistens ausreicht.

Die Zahl verschiedener Datenbankinstanzen ist typischerweise zweistellig (in größeren Umgebungen dreistellig, in kleineren Umgebungen nur einstellig).

Wenn das Unternehmen konsequent auf Web Front Ends für Applikationen setzt, ist die Anzahl dieser Front Ends in derselben Größenordnung wie die Anzahl der Anwendungen. Und diese Zahl ist in einem mittleren bis großen Unternehmen in der Regel dreistellig, in sehr großen Unternehmen sogar vierstellig. Je nach Grad der Durchdringung der Geschäftsprozesse des Unternehmens mit IT kann sich eine solch hohe Anzahl ergeben.

Dies bedeutet im Vergleich zur Hyperscaler-Umgebung eine viel kleinere Anzahl von Benutzern und eine wesentlich größere Anzahl verschiedener Anwendungen.

Wie aus der Abbildung 2 hervorgeht, gibt es innerhalb von Unternehmen eine relativ hohe Zahl von Applikationen. Pro Applikation werden aber nur wenige Infrastrukturkomponenten benötigt, denn die Anzahl der Anwender pro Applikation ist viel niedriger als beim Hyperscaler.

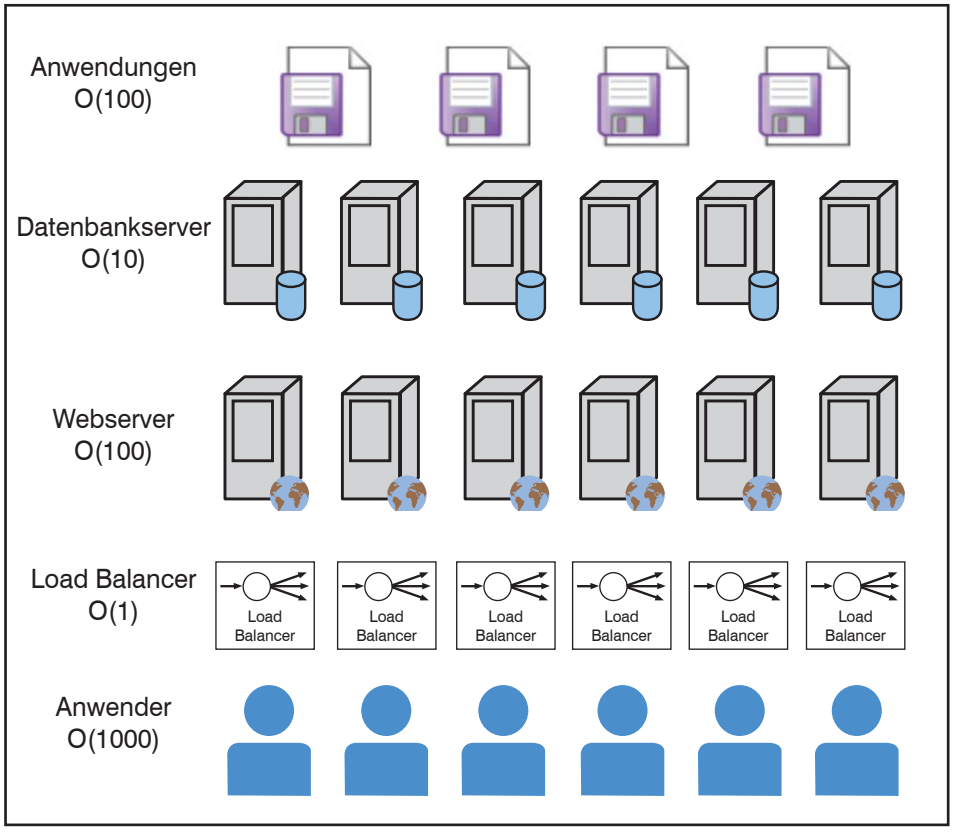


Abbildung 2: IT-Umgebung eines typischen Unternehmens

Folglich gibt es im Rechenzentrum eines typischen Unternehmens in der Regel keine sehr hohe Anzahl gleich konfigurierter Komponenten. Einen solchen Skalierungseffekt kann es in einem Unternehmen jedoch im Bereich Client Access geben.

Wo sich in Unternehmensnetzen die zentrale Steuerung lohnt

Ein Beispiel ist die Infrastruktur für Wireless Local Area Network (WLAN). In einem WLAN kommt es darauf an, dass jede Benutzergruppe unabhängig vom Ort dieselben Zugriffsprofile nutzen kann. Ein Zugriffsprofil entspricht in der Regel einem Service Set Identifier (SSID). Die Zuordnung eines Endgerätes zu einem SSID erfolgt entweder automatisch oder durch eine Aktion des Benutzers. In jedem Fall darf die Anzahl verschiedener SSIDs nicht zu hoch sein und bleibt idealerweise im einstelligen Bereich.

Dagegen kann es in einem großen Gebäude oder Gelände hunderte oder sogar tausende Access Points geben. Diese sollten möglichst einheitlich konfiguriert sein. Das zentrale Management ist aus verschiedenen Gründen wichtig:

- Die Anwender sollten überall dieselben Zugriffsprofile nutzen können.
- Die Zellenplanung sollte einem zentralen Management unterliegen.
- Eine zentrale Steuerungsebene ist für die Bildung von Overlay-Netzen erforderlich. Jedes Overlay-Netz entspricht einem Zugriffsprofil und ist überall verfügbar.

So haben sich in den letzten Jahren in den meisten großen Unternehmensnetzen WLAN-Strukturen durchgesetzt, in denen das Management und die Steuerung der WLAN-Umgebung auf zentrale Controller konzentriert sind, vereinfacht dargestellt in der Abbildung 3.

Wie aus der Abbildung 3 hervorgeht, wird eine Anzahl von hunderten Access Points auf die gleiche Weise konfiguriert, nämlich für die Bedienung einer geringen Zahl von Zugriffsprofilen bzw. SSIDs. Auch andere Parameter wie Frequenznutzung, Zuordnung der Frequenzen zu den Zugriffsprofilen und Schnittstellen zu Controllern werden gleichartig konfiguriert.

Daher lohnt sich auch hinsichtlich der Minimierung des Administrations- und des Management-Aufwands die Konzentration von Steuerung und Management (Control Plane, Management Plane) auf wenige zentrale Controller-Instanzen. In vielen Fällen werden die Controller sogar auch als zentrale Endpunkte von Tunneln genutzt, also für zentrale Hubs der Data Plane.

Unternehmensnetze folgen nicht immer dem Beispiel der Hyperscaler

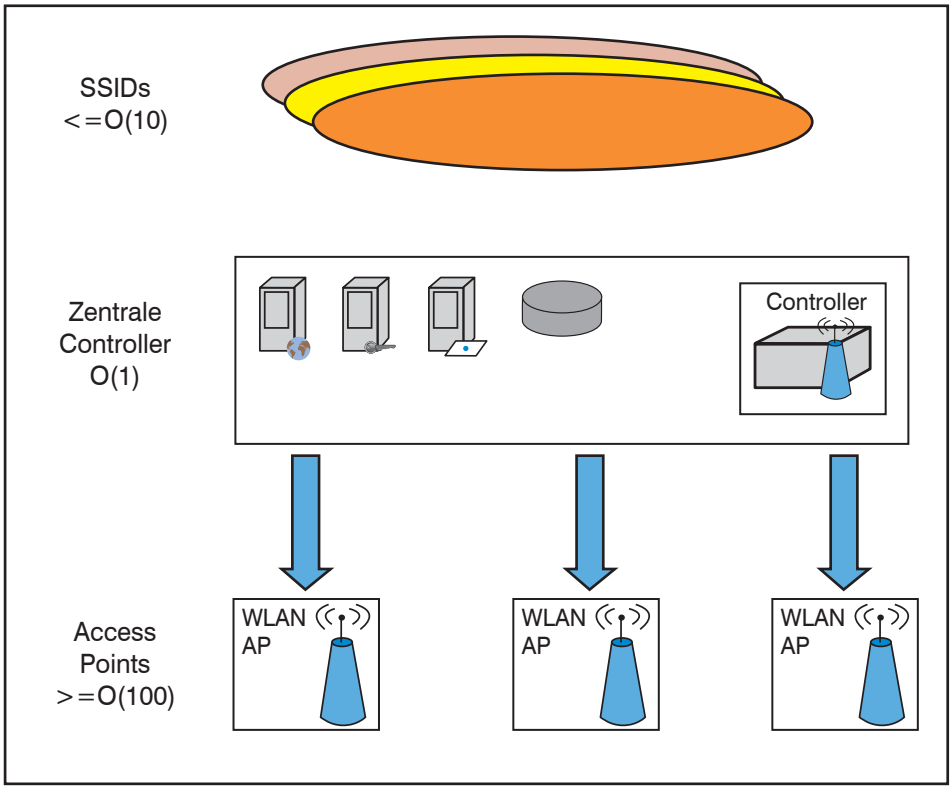


Abbildung 3: WLAN-Umgebung eines typischen großen Unternehmens

Wo die zentrale Steuerung an Grenzen stößt

Im WLAN-Design sind weder die Unternehmen noch die Service Provider dem Beispiel des jeweils anderen gefolgt. Der Bedarf an zentraler Steuerung und Administration der WLAN-Umgebung wurde von Unternehmen und Betreibern von Hot Spots ungefähr zeitgleich festgestellt. Die daraus resultierenden Designs sind sich ähnlich, auch wenn in Umgebungen der Service Provider aufgrund anderer Randbedingungen teilweise andere WLAN-Produkte eingesetzt werden als in den Unternehmensnetzen.

Aus ungefähr einem Jahrzehnt Erfahrungen beim Design und Betrieb von WLAN-Umgebungen ist einiges zu lernen. Dazu zählt die Erfahrung, dass eine extreme Konzentration von Controller-Funktionen auf ganz wenige Instanzen wie in der Abbildung 3 dargestellt bei einer sehr hohen Anzahl von Access Points (vierstellige Zahl und mehr) an Skalierbarkeitsgrenzen der Controller stoßen kann. Deshalb werden sehr große WLAN-Umgebungen so aufgebaut, dass zwar das Management möglichst zentralisiert wird, aber die Controllerebene aus einer größeren Anzahl von Instanzen besteht. Abbildung 4 stellt diesen Ansatz dar.

Das zentrale Management ist für die Zertifikats- und Schlüsselverwaltung, als Schnittstelle für die administrative Oberfläche sowie für die Verwaltung von Images und Konfigurationsdateien vom Vorteil, wie in der Abbildung 4 angedeutet.

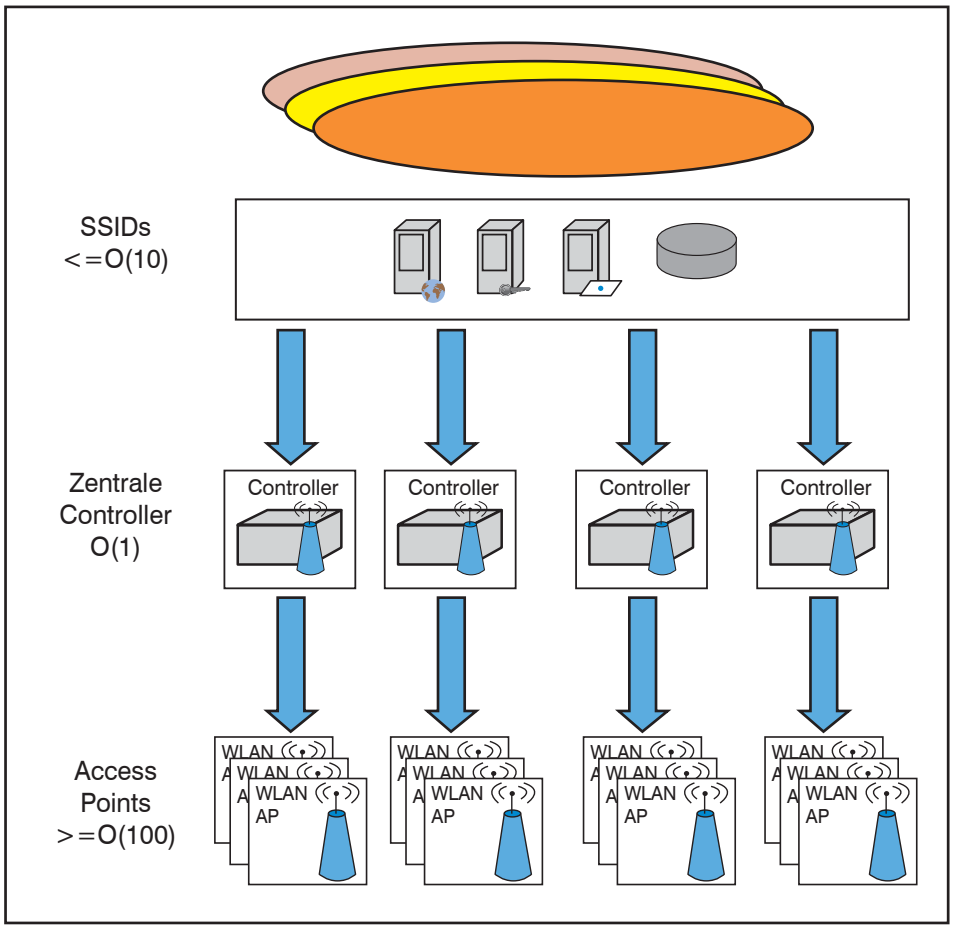


Abbildung 4: WLAN-Umgebung mit verteilter Control Plane

Zentrale Steuerung vieler gleich konfigurierten Geräte

Ähnliche Gründe, wie sie sowohl bei Betreibern von WiFi Hot Spots als auch in Unternehmen zu Controller-basierenden WLAN-Designs geführt haben, sind Anlass für Hyperscaler, in ihren Rechenzentren auf zentrale Steuerung der Vielzahl gleich konfigurierter Geräte zu setzen.

Man stelle sich vor, ein Hyperscaler führe eine Änderung in einer bestimmten Applikation ein. Nehmen wir ein Beispiel, das es in der Realität bereits gegeben hat: die Umstellung einer Webapplikation von http auf https. Dazu wäre folgendes (fiktives) Szenario denkbar:

- Auf der Vielzahl der Load Balancer oder Webserver, die bisher die http-Sessions bedient haben, ist eine Umleitung auf https-Seiten einzustellen. Dies erfolgt in der Regel durch einheitliche Umleitung auf einen Link wie https://anwendung.hyperscaler.net. Gleicher Link, zu verteilen auf tausende Komponenten.

- Setzt der Hyperscaler Global Load Balancing ein, wird die DNS-Anforderung nach der IP-Adresse passend zum Namen anwendung.hyperscaler.net abhängig vom Kontext der DNS-Anfrage beantwortet, zum Beispiel abhängig von der IP-Adresse des anfragenden Gerätes. Denkbar ist, dass die DNS-Anfrage durch Zugriff auf und Nachschlagen in einer sogenannten Geo-IP-Datenbank beantwortet wird. Auch der Zugriff auf diese Datenbank kann über einen ähnlichen Load-Balancing-Mechanismus erfolgen. In beiden Fällen ist eine größere Anzahl Komponenten (hier: Namensserver) ähnlich zu konfigurieren.

- Die vielen https-Sessions können so auf viele Load Balancer verteilt werden. Diese müssen, um den Clients den erforderlichen SSL/TLS Handshake anbieten zu können, mit Zertifikaten versehen werden. Das ist die Aufgabe einer zentralen Zertifikatsverwaltung. Die Load Balancer sind auch diesbezüglich gleich zu konfigurieren.

- Die Load Balancer terminieren die SSL-Verbindungen, und können im Hintergrund Verbindungen zu http-Servern aufbauen, die bisher auch die Applikation bedient haben. Auch dafür kann Load Balancing bzw. Global Server Load Balancing genutzt werden. Gleiches Spiel wie oben genannt: viele Komponenten, gleiche Konfiguration.

Geht die Zahl der gleich zu konfigurierenden Geräte in tausende und mehr, lohnen sich die zentrale Steuerung und das zentrale Management. Nur so sind Hyperscaler in der Lage, „auf Knopfdruck“ Änderungen in ihrer Umgebung einzuführen. Solche Änderungen haben wir in den letzten Jahren mehrfach erlebt.

Eine schematische und vereinfachte Darstellung des oben beschriebenen Szenarios gibt die Abbildung 5 wieder.

Wie in der Abbildung 5 dargestellt profitiert der Hyperscaler von der Möglichkeit, eine Vielzahl gleichartiger, gleich konfigurierter Komponenten mit einer zentralen Steuerungsebene zu betreiben. Auch wenn dies ein fiktives Szenario ist, soll es anschaulich machen, wo sich die Konzentration der Intelligenz einer Infrastruktur, zum Beispiel in der Gestalt der Control Plane, besonders lohnt, nämlich bei einer Vielzahl von gleichen Geräten mit gleicher Konfiguration.

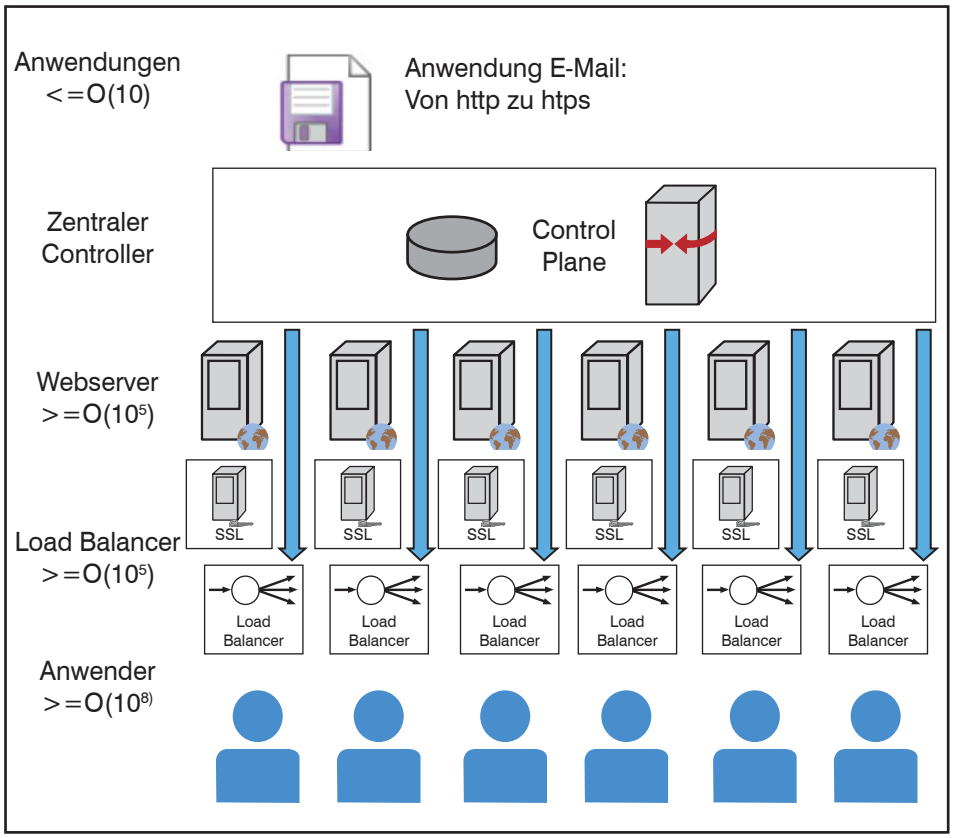


Abbildung 5: Zenrale Steuerung vieler gleich konfigurierter Geräte

Weitere Unterschiede

Software Defined Networking (SDN), wie es in engerem Sinne ausgelegt wird, heißt eben die Abstraktion der Control Plane von der Date Plane, damit die Steuerung des Netzes zentralisiert werden kann. Dies kann für Hyperscaler oder generell Service Provider mit einer Vielzahl von gleichen Komponenten mit der gleichen Konfiguration sinnvoll sein. Weitere denkbare Beispiele sind:

- Ein Internet Service Provider, der zum Beispiel eine Vielzahl Digital Subscriber Line Access Multiplexer (DSLAM) mit einer zentralisierten Control Plane betreibt

- Ein Mobilfunkbetreiber, der viele Basisstationen mit einem zentralen Controller steuert

- Ein Wide Area Network (WAN) Provider, der tausende Geräte der Kategorie Customer Premises Equipment (CPE) mit der gleichen Konfiguration versieht

Auch in Unternehmen kann es ähnliche Szenarien geben, insbesondere im Access-Bereich. Seltener sind aber Szenarien mit einer hohen Anzahl gleich konfigurierter Geräte in Rechenzentren von Unternehmen. Im RZ-Bereich trifft man insbesondere die Vielzahl und Vielfalt der Applikationen an, die manchmal auch mit einer einmaligen Konstellation von Sicherheitszonen einhergehen.

Welche Folgen hätte die Übertragung des für Hyperscaler und Service Provider möglicherweise sinnvollen SDN-Ansatzes auf das Rechenzentrum (RZ) eines Unternehmens?

Ein solches RZ ist in der Abbildung 6 dargestellt.

Wie aus der Abbildung 6 hervorgeht, unterhält der zentrale Controller zwei Typen von Schnittstellen:

- Sogenanntes Southbound Interface zu Netzkomponenten mit der Data Plane: Über diese Schnittstelle steuert der Controller die Netzkomponenten.

- Sogenanntes Northbound Interface zu Anwendungen: Über diese Schnittstelle können Anwendungen dem Controller Richtlinien übergeben bzw. von diesen Informationen über das Netz bekommen. Die Richtlinien können zum Beispiel Mechanismen wie Quality of Service (QoS) oder Zuordnung zu Sicherheitszonen betreffen.

Mittlere und große Unternehmen nutzen eine Vielzahl von Anwendungen. Würde jede Anwendung die Möglichkeit bekommen, über das Northbound Interface dem Netz Richtlinien zu übergeben, kann ein

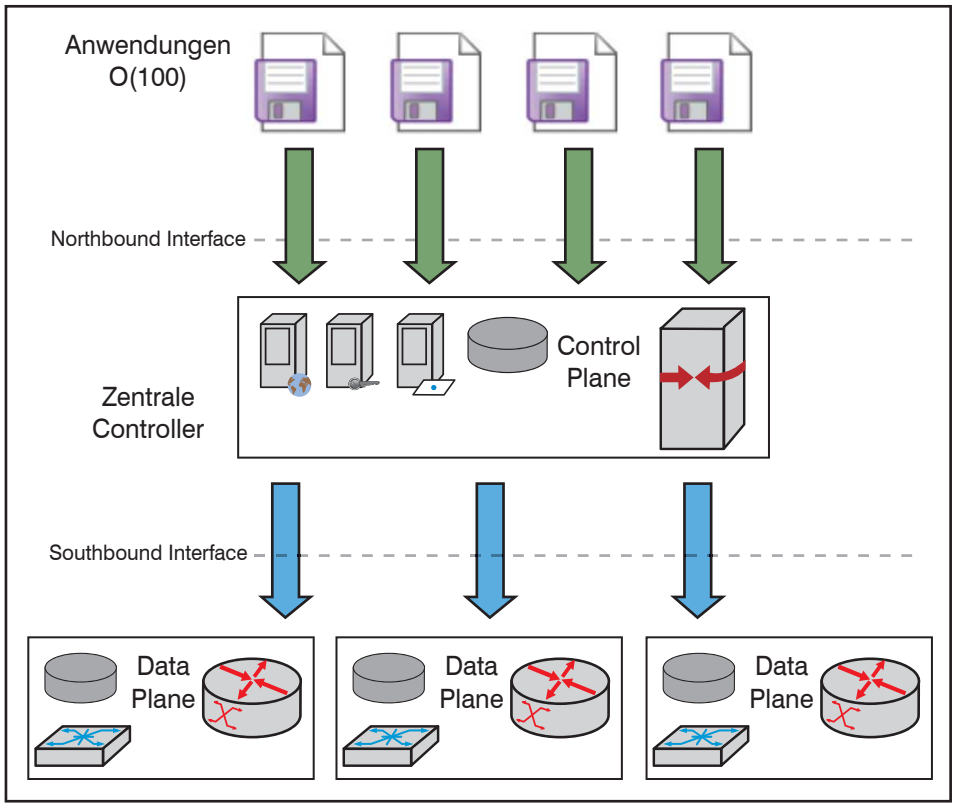


Abbildung 6: SDN im RZ eines Unternehmens

Konflikt mit dem gängigen Betriebsmodell für Infrastrukturen in Unternehmen entstehen. Gängige Betriebsmodelle der Unternehmen für Infrastrukturen sehen vor, dass diese, normalerweise bestehend aus Servern, Storage und Netz, für die Anwendungen bestimmte Garantien erfüllen müssen, zum Beispiel was die Verfügbarkeit betrifft. Diese werden in Service Level Agreements (SLA) festgehalten. Für die Einhaltung dieser SLA müssen Infrastrukturverantwortliche sorgen. Um dieser Pflicht nachzukommen, benötigen Verantwortliche für Server, Storage und Netz die Hoheit über die Subsysteme, die sie betreiben. Wer die administrative Hoheit für das Netz hat, muss dafür sorgen, dass diese Hoheit auch ausgeübt wird. Daher ist es einleuchtend, dass die Berechtigungen für die Administration von Netzkomponenten auf die Personengruppe beschränkt bleibt, welche diese Berechtigungen benötigt. Das Northbound Interface kann diese strikte Regelung unterlaufen, wie in der Abbildung 7 angedeutet ist.

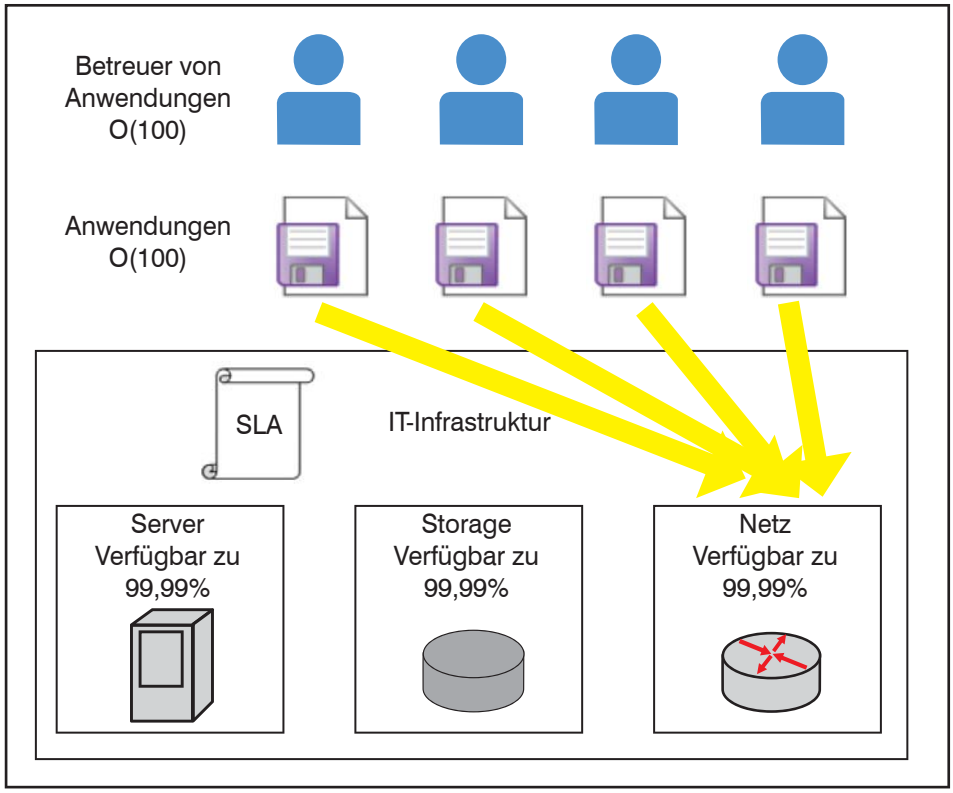


Abbildung 7: Nothboud Interface im Kontext eines gängigen Betriebsmodells für die Infrastruktur in einem Unternehmen

Daher kann das Northbound Interface nicht allen Applikationen mit den vielen für diese Applikationen zuständigen Betreuer zur Verfügung stehen. Denkbar ist nur die Nutzung dieser Schnittstelle durch Anwendungen, die der Infrastrukturbetrieb selbst nutzt, wie zum Beispiel Netzmanagement, Monitoring, Reporting, Logging-Anwendungen etc.

Fazit

Umgebungen der Hyperscaler und unternehmensinterne IT-Infrastrukturen unterscheiden sich vor allem sich im Verhältnis zwischen der Größe der Umgebung und der Anzahl der darüber zu betreibenden Anwendungen. Ein Hyperscaler muss wenige Applikationen für eine sehr hohe Zahl von Anwendern betreiben. Dagegen stehen in einem Unternehmen für eine wesentlich kleinere Zahl von Benutzern viele verschiedene Anwendungen zur Verfügung. Folglich gibt es bei einem Hyperscaler immer eine sehr hohe Zahl von Komponenten gleicher Art, die gleich konfiguriert werden. Im RZ eines Unternehmens ist das in der Regel nicht der Fall. Deshalb müssen Konzepte, die in einer Hyperscaler-Umgebung für Effizienz durch zentrale Steuerung der Infrastruktur sorgen, nicht zwangsläufig auch in einem Unternehmen sinnvoll sein.

Zu den Konzepten, die insbesondere unter Berücksichtigung der Anforderungen der Hyperscaler und Service Provider entwickelt worden sind, gehört der Ansatz der Trennung der sogenannten Control Plane von der Data Plane. Während die Control Plane in einem Netz der Steuerung der Netzfunktionen dient, werden Daten über die Data Plane übertragen. In konventionellen Netzkomponenten sind Control Plane und Data Plane eigenständig pro Netzkomponente vorhanden. Der traditionelle Ansatz des Netzbetriebs besteht darin, die Control Plane pro Netzkomponente eigenständig zu konfigurieren. Gibt es eine hohe

Unternehmensnetze folgen nicht immer dem Beispiel der Hyperscaler

Zahl gleichartiger Komponenten, die gleich konfiguriert werden müssen, kann die Zentralisierung der Control Plane und deren Konzentration auf zentrale Controller für die Erhöhung der Effizienz sorgen.

Fehlt in einem Unternehmensnetz die kritische Masse an gleichen Komponenten gleicher Konfiguration, entfällt eine wesentliche Motivation für die Zentralisierung der Control Plane.

Ein weiterer Unterschied zwischen den Umgebungen der Hyperscaler und unternehmensinternen Infrastrukturen besteht darin, dass letztere strikte Service Level Agreements erfüllen müssen. Anwendungen, die ganz verschiedene Geschäftsprozesse des Unternehmens abbilden, müssen sich auf die Infrastruktur verlassen können. Wird der zentrale Controller für die Steuerung des Netzes durch Applikationen genutzt, können Servicegarantien der Infrastruktur beeinträchtigt werden.

Die hier beschriebenen Umstände gehören zu den Gründen, weshalb sich in den meisten Rechenzentren von Unternehmen die Trennung der Control Plane von der Data Plane nicht durchgesetzt hat. Obwohl dieser Ansatz schon seit einigen Jahren diskutiert wird, folgen die meisten unternehmensinternen Rechenzentren nicht diesem Ansatz.

ComConsult Veranstaltungskalender

Messtechnik der Übertragungsphysik im Umfeld der Lokalen Netze, 13.06.16 in Bonn

Garantietermin

Die Sonderveranstaltung zeigt den aktuellen Stand der neuen aktuell verfügbaren speziellen Handheld-Scanner auf und erläutert die Messrichtlinien, die für Abnahmemessungen von Glasfaser-Kabelanlagen optimal sind. Im zweiten Schwerpunkt widmet sich die Veranstaltung den Messungen im WLAN-Umfeld.

Preis: € 1.090,-- netto

IT-Kommunikation im Umfeld von Fertigung und Automation, 13.06.-14.06.16 in Bonn

Garantietermin

Mit der aktuellen Technologie-Entwicklung stellt sich immer mehr die Frage, ob eine klare Trennung zwischen Büro und Fertigung in Zukunft noch erreichbar sein wird. Dieses Seminar analysiert wie Fertigungsnetzwerke auf diese Herausforderungen reagieren können und wie mit geeigneten Technologien Sicherheit, Leistung und Flexibilität gewährleistet werden kann.

Preis: € 1.590,-- netto

Netzzugangskontrolle: Technik, Planung und Betrieb, 13.06.-15.06.16 in Bonn

Garantietermin

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

Preis: € 1.890,-- netto

Trouble Shooting für Netzwerk-Anwendungen, 14.06.-17.06.16 in Aachen

Garantietermin

Dieses Seminar beschreibt die typischen Störsituationen im Umfeld moderner Anwendungen, gibt Einblick in bisher als Black Box benutzten Mechanismen und Abläufe und trainiert die systematische und methodische Diagnose und Fehlerbeseitigung. Dabei wird die Theorie mit praktischen Übungen und vielen Fallbeispielen in einem Trainings-Netzwerk kombiniert. Die Teilnehmer werden durch dieses kombinierte Training in die Lage versetzt, das Gelernte sofort in der Praxis umzusetzen. Als Protokoll-Analysator kommt Wireshark zum Einsatz. Einer Verwendung selbst mitgebrachter Analyse-Software, mit deren Bedienung der Teilnehmer vertraut ist, steht nichts im Wege.

Preis: € 2.470,-- netto

Private Cloud rechtssicher auslagern - Vertragsgestaltung für Nichtjuristen, 15.06.-16.06.16 in Köln

Garantietermin

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

Preis: € 1.590,-- netto

RZ-Kopplung: Georedundanz für Rechenzentren, 20.06.16 in Köln

Garantietermin

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,-- netto

TCP/IP-Netze erfolgreich betreiben, 20.06.-22.06.16 in Bonn

Garantietermin

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,-- netto

Rechenzentrumsdesign - Technologien neuester Stand, 20.06.-22.06.16 in Bonn

Garantietermin

Das Seminar liefert eine Einschätzung aktueller und neuer RZ-Technologien und bietet Ihnen auf der Basis jahrzehntelanger Erfahrung bewährte Best-Practice-Hinweise.

Preis: € 1.890,-- netto

Information Security Management mit ISO 27001 und BSI-Grundschutz, 20.06.-22.06.16 in Bonn

Garantietermin

Angemessene Sicherheit mit optimalem Aufwand: geht das? Die Antwort liegt in der Nutzung bewährter Standards und Lösungen bei gleichzeitiger Erfüllung von Compliance-Richtlinien. Anders formuliert: Das Rad muss nicht von jedem Unternehmen neu erfunden werden. Dieses Seminar stellt den Aufbau und die nachhaltige Umsetzung eines standardisierten und zertifizierbaren Information Security Management System (ISMS) auf Basis von ISO 27001 und BSI IT-Grundschutz vor. Es wird dabei aufgezeigt, wie eine praxisgerechte Sicherheitslösung mit optimalem Aufwand erreicht werden kann.

Preis: € 1.890,-- netto

SIP (Session Initiation Protocol) - Basis-Technologie der IP-Telefonie, 20.06.-22.06.16 in Bonn

Garantietermin

Ziel der Schulung ist die Erläuterung von SIP als den Schlüssel für eine offene, leistungsfähige und Kosten-optimale Kommunikations-Lösung. Es umfasst nahezu alle Dienste, die wir heute für UC benötigen: Sprache, Video, Daten und Präsenz. Lernen Sie was SIP leistet, worin sich wesentliche Hersteller-Lösungen unterscheiden und wie Sie das Beste aus beiden Welten zukunftsorientiert nach Ihrem Bedarf optimieren.

Preis: € 1.890,-- netto

Zertifizierungen

ComConsult Certified Network Engineer

Lokale Netze
19.09. - 23.09.16 in Aachen

TCP/IP-Netze erfolgreich betreiben
20.06. - 22.06.16 in Bonn
24.10. - 26.10.16 in Bonn

Internetworking
04.07. - 08.07.16 in Aachen
14.11. - 18.11.16 in Aachen

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

ComConsult Certified Trouble Shooter

Trouble Shooting in vernetzten Infrastrukturen
27.09. - 30.09.16 in Aachen

Trouble Shooting für Netzwerk-Anwendungen
14.06. - 17.06.16 in Aachen
15.11. - 18.11.16 in Aachen

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

ComConsult Certified Voice Engineer

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen
24.10. - 26.10.16 in Frankfurt

Session Initiation Protocol Basis-Technologie der IP-Telefonie
20.06. - 22.06.16 in Bonn
09.11. - 11.11.16 in Berlin

Umfassende Absicherung von Voice over IP und Unified Communications
04.07. - 06.07.16 in Stuttgart
28.11. - 30.11.16 in Bonn

Optionales Einsteiger-Seminar: IP-Wissen für TK-Mitarbeiter
19.09. - 20.09.16 in Frankfurt

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,-- netto statt € 5.670,-- netto
Optionales Einsteigerseminar: Aufpreis € 1.190,-- netto statt € 1.590,-- netto

Impressum

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

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

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

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