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-

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.**

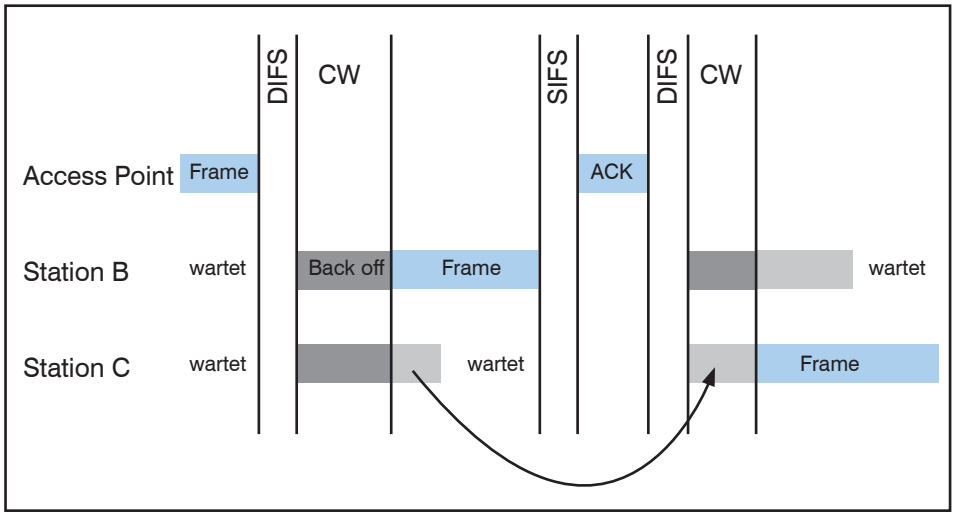

Abbildung 1: Medienzugang bei WLAN mittels DCF

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-

Zweitthema

Unternehmens-netze 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.

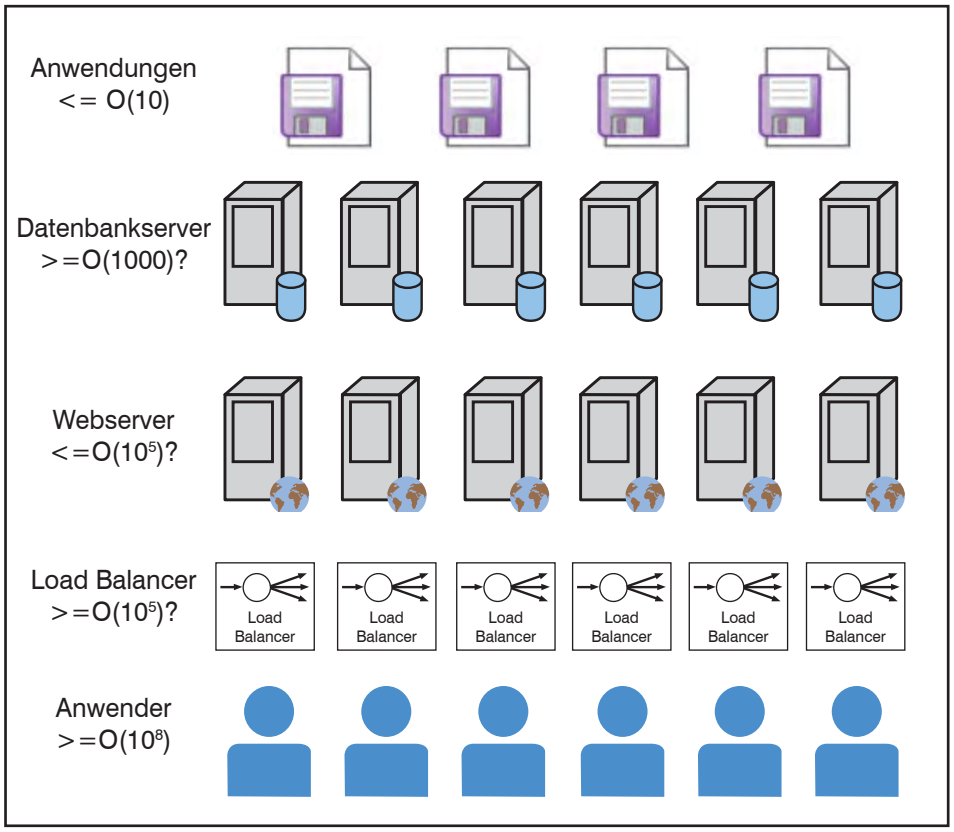

Abbildung 1: Typische Umgebung bei einem Hyperscaler

Unternehmensnetze folgen nicht immer dem Beispiel der 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.

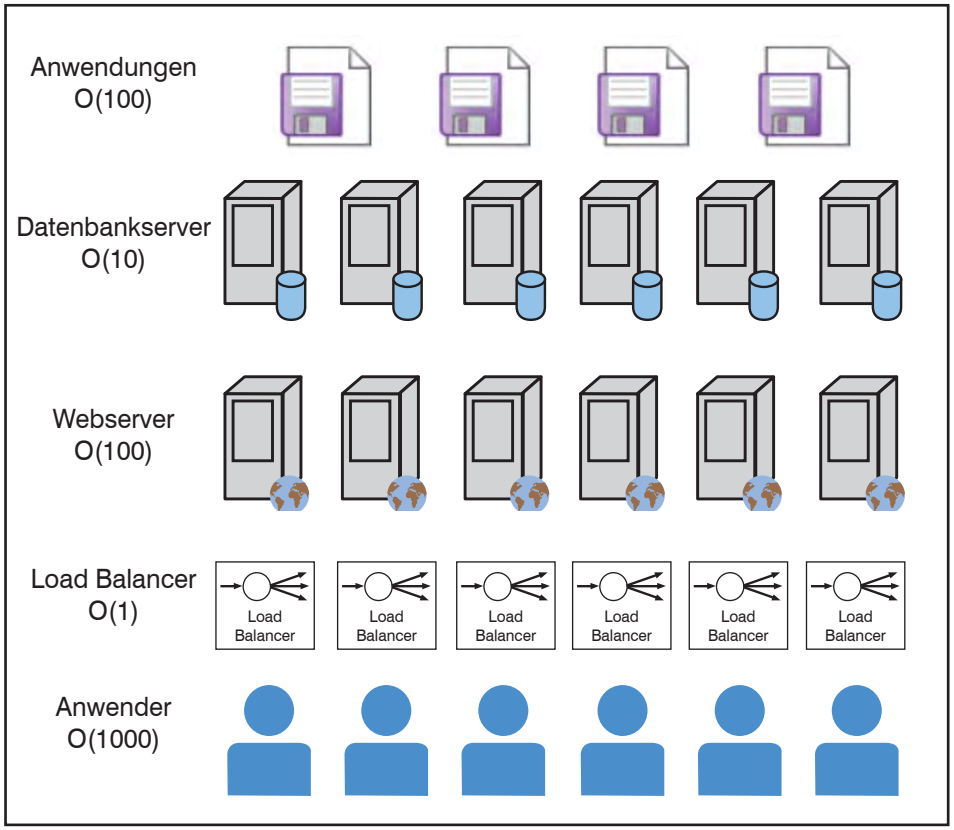

Abbildung 2: IT-Umgebung eines typischen Unternehmens

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.