ComConsult GmbH
Beratung + Planung + Schulung

Der Netzwerk Insider

Januar 2020

Systematische Weiterbildung für Netzwerk- und IT-Professionals

5G-Netze sind anders als WLAN

von Dr. Joachim Wetzlar

Der 5G-Mobilfunk kann nun auch im Unternehmensumfeld ausgerollt werden, angebunden an lokale Netze. Das lokale 5G-Netz tritt also quasi in Konkurrenz zu WLAN. Zwei Funknetze auf demselben Campus – warum sollten Sie das tun? Aufbau und Betrieb zweier Infrastrukturen ist wahrscheinlich weniger wirtschaftlich als sich auf eine zu beschränken. Sollte man also nicht WLAN gänzlich durch 5G-Mobilfunk ersetzen? 5G-Netze scheinen schließlich die Lösung für alle Probleme dieser Welt zu sein, glaubt man den vollmundigen Versprechungen von Industrie und Providern.

Ich werde mit diesem Artikel versuchen, etwas Licht in das „5G-Dunkel“ zu bringen. Was macht den 5G-Mobilfunk so besonders? Was unterscheidet ihn von bisherigen Mobilfunk-Generationen? Welche technischen „Features“ zeichnen ihn aus, und welchen technischen Aufwand muss man für den Aufbau eines eigenen Mobilfunknetzes treiben? Und – last but not least – wofür ist WLAN nach wie vor die geeignete Lösung?

weiter auf Seite 7

Sicherung und Wiederherstellung von iOS-Geräten im Unternehmensumfeld

von Mark Zimmermann

Sicherungs- und Wiederherstellungsfunktionen gehören zu den wichtigsten Funktionen mobiler Geräte. Apple bietet entsprechende Funktionen, sowohl in der iCloud als auch direkt auf einem Computer. Im privaten Umfeld funktionieren diese weitgehend zuverlässig. In Unternehmen führen diese Funktionen häufig zu Herausforderungen durch ein scheinbar inkonsistentes Verhalten.

Seit iOS 5 können Anwender auf dem iPhone gespeicherte Daten auf einem Computer oder auf iCloud sichern. Diese auf den Einsatz beim Endanwender konzipierte Funktion (siehe auch: https://support.apple.com/de-de/HT203977) setzt Administratoren immer wieder vor neue Herausforderungen. Aufgrund mangelnder Dokumente ist dieser Artikel eine Sammlung diverser Erfahrungen bezüglich dieser Herausforderungen.

weiter auf Seite 19

Geleit

Wie groß muss die Ausdehnung von Layer-2-Netzen sein?

auf Seite 2

Standpunkt

DSGVO: Erste hohe Strafen, neue Fälle

auf Seite 17

Aktueller Kongress

ComConsult Netzwerk Kongress

ab Seite 6

Neu im Programm

Container-Orchestrierung mit Kubernetes On-Premises und in der Cloud

ab Seite 6

Geleit

Wie groß muss die Ausdehnung von Layer-2-Netzen sein?

Das Internet Protocol (IP) wird für die meisten heutigen Anwendungen genutzt. IP-Verkehr ist Layer-3-Verkehr. Dieser Verkehr ist daher auch über Router möglich. Router segmentieren Layer-2-Netze. Diese Segmentierung strukturiert und ordnet unsere Netze. Große Clouds wie zum Beispiel AWS und Azure orientieren sich an dieser Strukturierung. In den Unternehmensnetzen gibt es aber immer noch ausgedehnte Layer-2-Netze, teilweise sogar standortübergreifend. Solche Strukturen machen unsere Netze komplexer. Die Frage ist berechtigt, wie groß die Ausdehnung von Layer-2-Netzen sein muss.

Motivation für Layer-2-Netze

Die Nutzung von Layer-2-Kommunikation ohne Router als Vermittler kann verschiedene Gründe haben, darunter die folgenden:

- Einige Anwendungen nutzen nicht IP, sondern Ethernet ohne IP. Eine solche Anwendung benötigt eine Layer-2-Verbindung von Ende zu Ende. Beispiele gibt es in verschiedenen Bereichen. Fiber Channel over Ethernet (FCoE) ist als eine der Varianten für Storage-Kommunikation nicht IP-basierend. Gleiches gilt für einige Protokolle im Bereich industrieller Steuerung und Regelung einschließlich Gebäudeautomation.

- Manche IP-Applikationen nutzen Multicast IP statt Unicast IP. Die meisten IP-Netze (zum Beispiel das Internet) unterstützen keine Multicast-IP-Kommunikation. Es gibt daher Szenarien, in denen für Multicast-IP Layer-2-Netze genutzt werden.

- Der vielleicht häufigste Fall der Nutzung ausgedehnter Layer-2-Netze ist in Rechenzentren von Unternehmen zu finden. Seit ca. 20 Jahren sind in diesen RZs Cluster bzw. virtualisierte Umgebungen im Einsatz, die Layer-2-Kommunikation erfordern. Der Grund ist der Einsatz sogenannter virtueller IP-Adressen (VIP) für Server. Eine VIP ist von einzelnen physischen Servern unabhängig. Cluster- und Virtualisierungsmechanismen sorgen dafür, dass eine VIP von Hardware zu Hardware „wandern“ kann. Die „VIP-Mobilität“ löst das Problem, dass einige Anwendungen zusammenbrechen, wenn die IP-Adresse des zugehörigen Servers nicht mehr erreichbar ist.

- Eine weitere Motivation für ausgedehnte Layer-2-Netze ist organisatorischer Natur. Zum Beispiel wollen einige Unternehmen ihr Wide Area Network (WAN) einschließlich der Routing-Instanzen selbst betreiben. Sie mieten daher ein Layer-2-WAN. Ähnlich ist es bei einigen „Gewerken“ der Gebäudeautomation. Manche Betreiber in diesem Bereich fordern ausgedehnte Layer-2-Netze, weil sie diese schon immer für ihre Zwecke eingesetzt haben.

Es mag zusätzlich zu den oben genannten Fällen weitere Gründe für den Einsatz ausgedehnter Layer-2-Netze geben.

Die Cloud setzt Maßstäbe

Die aufgezählten Fälle der Nutzung ausgedehnter Layer-2-Netze gehen auf die Zeiten vor Cloud-Computing zurück. Mittlerweile hat die Cloud Maßstäbe gesetzt. Wir wissen, dass die Kommunikation in und mit großen Clouds auf IP basiert. Ferner wissen wir, dass der Standardweg für den Zugriff auf Software as a Service (SaaS) das Internet ist. Was Clouds als „Verlängerung des eigenen RZs“ (IaaS – Infrastructure as a Service) betrifft, kennen wir die Cloud-Standards auch: IP-Subnetze in großen Clouds erstrecken sich nicht über verschiedene Rechenzentren, sondern bleiben in aller Regel auf eine Availability Zone (AZ), d.h. ein RZ beschränkt. Damit kann eine VIP in der Cloud nicht vom RZ zum RZ „wandern“.

Kann man unter solchen Bedingungen überhaupt Hochverfügbarkeit realisieren? Ja, das ist möglich, indem die Anwendungen nicht mehr auf sogenannte feste „Sockets“ (Kombination aus TCP/UDP-Portnummer und IP-Adresse) aufsetzen. Ein prominentes Beispiel für die Unabhängigkeit von festen „Sockets“ sind moderne Webanwendungen. Der Web-Client, zum Beispiel ein Webbrowser, kommuniziert nicht mit einem festen „Socket“. Stattdessen nutzt der Web Client einen Uniform Resource Locator (URL), um die Webanwendung zu erreichen. Ein URL kann zwar als Server Locator eine IP-Adresse enthalten, sollte aber stattdessen lieber einen Fully Qualified Domaine Name (FQDN) nutzen, zum Beispiel www.comconsult.com. Im Rahmen des Domain Name System (DNS) führt das Gerät, auf dem der Browser läuft, eine sogenannte „Auflösung“ durch und erfährt, dass zu www.comconsult.com die IP-Adresse 185.21.102.156 gehört. Ändert sich die IP-Adresse von www.comconsult.com, stürzt der Browser nicht ab, sondern veranlasst nach einem Time-out eine neue DNS-Auflösung. Eine Protokollschicht oberhalb der Transport Layer sorgt dafür, dass der „Kontext“ für die Webanwendung erhalten bleibt. Diese Schicht wäre nach der Terminologie des Open Systems Interconnection

Wie groß muss die Ausdehnung von Layer-2-Netzen sein?

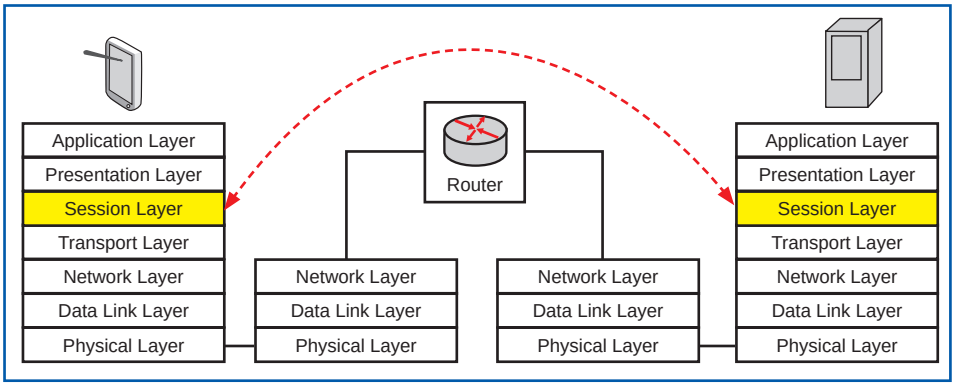

Abbildung 1: Session Layer

(OSI) die „Session Layer“. Die „Sitzung“ geht nicht verloren, wenn die IP-Adressen der Endgeräte sich ändern, wie in der Abbildung 1 dargestellt.

Das gilt mittlerweile sogar auch für UC-Anwendungen. Im Zuge der Vorbereitung dieses Geleits habe ich das bei einer Microsoft-Teams-Session ausprobiert. Ich habe die Teams-Session unter Nutzung eines VPN-Tunnels aufgebaut und daran teilgenommen. Dann habe ich mitten in der Session den VPN-Tunnel abgebaut. Teams hat mir die Möglichkeit gegeben, wieder an der Session teilzunehmen, und dieses Mal ohne VPN-Tunnel, d.h. mit einer anderen IP-Adresse und über ganz andere Wege durch das Internet.

Die großen Cloud-Anbieter müssen keine Rücksicht auf alte Socket-basierende Applikationen nehmen. Sie gehen davon aus, dass eine moderne Anwendung eine Webapplikation ist. Dies bedeutet, dass auf der User-Seite immer ein Web-Client zum Einsatz kommt. Das muss nicht unbedingt ein normaler Web Browser sein. Auch ein UC-Client kann im Netz ausschließlich als Web-Client in Erscheinung treten. Ein moderner Client verhält sich so wie ein moderner Webbrowser, d.h. er „hält“ den Kontext von Anwendungen, auch wenn sich die eigene oder die IP-Adresse des Web-Servers ändert.

In einer modernen Cloud erfolgt der Schwenk von einem zum anderen RZ nicht dadurch, dass die VIP wandert. Stattdessen gibt es Load-Balancing-Mechanismen, die Last auf verschiedene Instanzen verteilen. Diese Instanzen können auf verschiedene Rechenzentren (Availability Zones) verteilt werden.

Werden Layer-2-Netze durch Layer-3-Netze abgelöst?

Sobald ein RZ nur noch moderne Webanwendungen bedienen muss, kann die RZ-Infrastruktur so konzipiert werden wie in der Cloud. Damit entfällt eine der Hauptmotivationen für ausgedehnte Layer-2-Netze in Rechenzentren.

VIP-Wanderung ist aber wie erwähnt nicht die einzige Motivation für ausgedehnte Layer-2-Netze in RZs. Es bleibt noch die Frage, ob man für die Kommunikation zwischen Server und Storage etwas anderes als ein IP-Netz braucht:

- Fiber Channel (FC) in nativer Form nutzt nicht Ethernet, sondern separate Switches und Verbindungen. Insofern kommt FC ohne ausgedehntes Layer-2-Ethernet aus.
- FCoE benötigt Layer-2-Ethernet. Wer sich für FCoE entscheidet, braucht aber nicht nur ausgedehnte Layer-2-Netze, sondern auch besondere Switches. Diese müssen nicht nur Layer-2-Redundanzmechanismen, sondern auch verlustfreie Ethernet-Kommunikation unterstützen.

FC und FCoE sind aber nicht die einzigen nutzbaren Protokolle für die Kommunikation zwischen Server und Storage. Neben den IP-Protokollen iSCSI und NFS gibt es noch verteilte Storage-Ansätze, die Speicherobjekte auf verschiedene Virtualisierungshosts verteilen. Die Instanz, die für Speichervirtualisierung zuständig ist, unterstützt dabei Hochverfügbarkeit dadurch, dass ein RAID-1-ähnlicher Mechanismus für die Datenreplikation sorgt. Fällt ein physischer Host oder eine Speichereinheit aus, erfolgt eine automatische Umschaltung auf einen anderen Knoten. Die gesamte Speicherkommunikation ist dabei IP-basierend.

Wenn eine Anwendung IP nicht nutzen kann, müssen dafür Layer-2-Verbindungen genutzt werden. Auch wenn dies in der RZ-Infrastruktur nicht notwendig sein sollte, kann es außerhalb von Rechenzentren Nicht-IP-Anwendungen geben. Ein Beispiel ist Building Automation and Control Networks (BACnet). Wenn Komponenten in einem Gebäude nicht die IP-Variante, sondern nur die auf Ethernet basierende Version von BACnet nutzen, benötigen sie Layer-2-Verbindungen.

Layer-2-Verbindungen können auch über Layer-3-Netze vermittelt werden. Das dafür genutzte Verfahren heißt „Tunneling“ bzw. „Encapsulation“. Dabei versieht ein Tunnelende einen Layer-2-Rahmen mit einem IP-Header und sendet ihn zum anderen Tunnelende.

Eine Herausforderung dabei sind Redundanzmechanismen. Diese sind in reinen Layer-3-Netzen in Form von Routing-Mechanismen standardisiert und haben sich bewährt. In Layer-2-Netzen benötigt man eigene Redundanzmechanismen, die im Vergleich zu Layer-3-Mechanismen weniger skalierbar und robust sind. Sie werden mit Layer-2-Tunneling durch Layer-3-Netze auch noch komplexer.

Insofern sollte man jede Anforderung, aus der die Notwendigkeit von Layer-2-Verbindungen resultiert, auf den Prüfstand stellen. Dies gilt insbesondere für Fälle der rein organisatorisch motivierten Bildung von Layer-2-Netzen. Oft stellt es sich heraus, dass eine bestimmte Anwendung auch über ein Layer-3-Netz funktioniert, wenn man sie anders konfiguriert. Natürlich lässt sich ein IP-Endgerät einfacher konfigurieren, wenn man nur die IP-Adresse konfiguriert und durch eine entsprechende Subnetzmaske dafür sorgt, dass die Endgeräte alle direkt miteinander kommunizieren. Dann entfällt eben die Einstellung der Default-Router-Adresse auf dem Endgerät. Aber diese Vereinfachung der Konfiguration an einer Stelle kann Probleme für das gesamte Netz verursachen:

- Kombinierte Layer-3- und Layer-2-Netze sind komplexer als reine Layer-3-Netze.
- Layer-2-Redundanzmechanismen sind in der Regel nicht so robust wie ihre Layer-3-Pendants.
- Layer-2-Netze sind nicht so skalierbar wie IP-Netze.
- Weitere Nachteile können dadurch entstehen, dass im Netz herstellerspezifische Layer-2-Mechanismen zum Einsatz kommen und damit Abhängigkeit von einzelnen Herstellern verursachen.

Die Abwägung von Layer-2- gegen Layer-3-Netze ist im RZ, Campus und Gebäude erforderlich. Deshalb haben wir diese Gegenüberstellung auf die Agenda unseres Netzwerk Kongresses im März 2020 gesetzt.

Ihr Dr. Behrooz Moayeri

LESERBRIEF

Gerne können Sie mir Ihre Meinung und Kommentare zu diesem Artikel schicken.

Sie erreichen mich unter moayeri@comconsult.com

5G-Netze sind anders als WLAN

Fortsetzung von Seite 1

Dr. Joachim Wetzlar ist seit mehr denn 25 Jahren Senior Consultant der ComConsult 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. Weiterhin führt er als Projektleiter und Senior Consultant regelmäßig Netzwerk- WLAN- und RZ-Redesigns durch.

Abbildung 1 lässt erahnen, dass ein Funkgerät mit allem Zubehör ohne Weiteres in den Kofferraum eines Autos passt. Das war Ende der 1950er Jahre. 1958 wurde das sogenannte A-Netz eröffnet (das „A“ stand meines Wissens zunächst für „Autotelefon“). Es handelte sich um ein analoges Sprechfunkverfahren auf Frequenzen des 2-Meter-Bandes, etwas oberhalb von 150 MHz. Es waren zunächst 17 Frequenzen (Kanäle) dafür reserviert. Sende- und Empfangsfrequenzen eines Kanals lagen 4,5 MHz auseinander, und über eine entsprechende Antennenweiche wurde gleichzeitig gesendet und empfangen (voll-duplex). Für den telefonierenden Autofahrer entsprach das Erlebnis also dem des heimischen Telefons.

Die Vermittlung erfolgte von Hand. Man musste „dem Fräulein vom Amt“ also die anzurufende Telefonnummer diktieren. Umgekehrt musste der Anrufer wissen, in welcher Gegend der A-Netz-Teilnehmer gerade herumfuhr, damit der Anruf zum richtigen Funkmast (Basisstation) weitergeleitet wurde. Es wurde ein Selektivrufverfahren auf Basis von vier parallel ausgesandten Tonfrequenzen implementiert, so dass Anrufe im Fahrzeug signalisiert wurden. In den 70ern führte man zusätzlich eine automatische Kanalwahl ein. Ein elektromechanisches (!) Schrittschaltwerk scannte regelmäßig alle 17 Kanäle und suchte nach empfangbaren Basisstationen. Eine solche Anlage (Bosch OF2-B) landete Ende der 70er Jahre, nachdem das A-Netz endgültig abgeschaltet war, auf meinem Basteltisch, und ich konnte ihre Funktion eingehend studieren.

Die erste Generation des Mobilfunks (1G) war damit geboren. Es folge Anfang der 70er das B-Netz mit bis zu 75 Duplex-Kanälen im 2-Meter-Band. Nun konnten die Teilnehmer, wie vom Festnetz gewohnt, selbst wählen. Das C-Netz wurde ab 1985 eingeführt. Die Geräte wurden tragbar (z.B. Phillips Porty, Siemens C5) und hatten am Ende sogar „Handy-Format“ (Nokia C6). Es handelte sich um ein hybrides Verfahren. Während die Sprache nach wie vor analog übertragen wurde, hatte man erstmals ein digitales Verfahren für die Vermittlung implementiert.

Damit wurde das erste zellulare Netz möglich: Man konnte sich telefonierend von Funkzelle zu Funkzelle bewegen, ohne dass das Gespräch abriss. Angeblich funktionierte das sogar zuverlässiger als beim heutigen Mobilfunk. Umgekehrt konnte man unter seiner Nummer erreicht werden, wo auch immer man sich in Deutschland befand. Und überdies war die Nummer nicht mehr im Telefon selbst gespeichert, sondern auf einer persönlichen C-Netz-Teilnehmerkarte, die man ins Mobiltelefon einsteckte. Es handelte sich um den Vorläufer des Subscriber Identity Module (SIM), das seit der zweiten Generation des Mobilfunks (2G) allgemein bekannt ist.

Der 2G-Mobilfunk war vollständig digital. Sprache wurde wie bei ISDN („ich sehe Deine Nummer“) digital kodiert

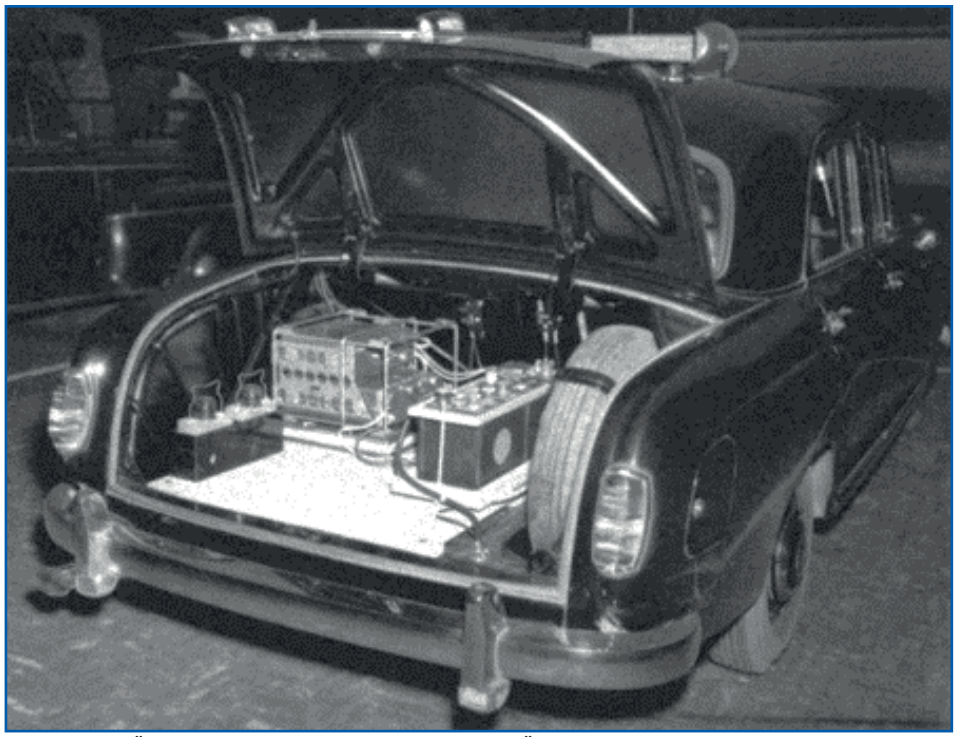

Abbildung 1: Öffentlicher beweglicher Landfunkdienst (ÖbL) (Bildquelle [1])

und übertragen. Nach erfolgreichem Gesprächsaufbau wurde für das Endgerät eine feste Bitrate reserviert, die zur Übertragung der ISDN-Sprachdaten in komprimierter Form genutzt wurden. Es handelt sich um eine leitungsvermittelte Technik, auch wenn das Medium drahtlos ist.

Der 2G zugrunde liegende Standard wurde von der Groupe Spécial Mobile (GSM) in den 80er Jahren entwickelt. Inzwischen steht GSM für das Global System for Mobile Communications. Ab 1990 wurden in Deutschland die D- und E-Netze gemäß GSM-Standard aufgebaut. Das erste D-Netz-Telefon, das ich in den Händen meines Chefs sah, war der „Knochen" (Motorola International 3200). Aber schon bald schrumpften die Geräte zum „Handy" (z.B. Siemens S3com, Ericsson T39M [2]).

GSM wurde – neben dem Kurznachrichtendienst (Short Message Service, SMS) – schon bald um die Möglichkeit erweitert, IP-Pakete zu übertragen. Neben der reinen Telefonie konnten nun beispielsweise E-Mails übertragen und Websites abgerufen werden. Es entstanden die ersten Smartphones (z.B. Nokia Communicator). Der damit einhergehende Bedarf nach höherer Bitrate wurde durch die dritte Mobilfunkgeneration zunächst gedeckt.

Das 3rd Generation Partnership Project (3GPP) gründete sich Ende der 90er Jahre und machte GSM zum weltweiten Standard. Gleichzeitig übernahm die International Telecommunications Union – Radiocommunications Sector (ITU-R) die Aufgabe, für eine weltweite Harmonisierung von Mobilfunkfrequenzen zu sorgen und Vorgaben für die Mobilkommunikation zu formulieren (International Mobile Telecommunications, IMT, vgl. [3]).

Die Parallelität zwischen leitungsvermittelter Sprachübertragung und der paketbasierten Übertragung im General Packet Radio Service (GPRS) ist in heutigen Mobilfunknetzen immer noch vorherrschend. Mit anderen Worten: während Sie telefonieren, können Sie weder E-Mails empfangen noch Websites aufrufen. Diese hybride Struktur wird letztlich erst mit der vierten Mobilfunkgeneration überwunden.

4G, oder auch Long Term Evolution (LTE), bringt neben einer weiteren Erhöhung der Bitrate die Möglichkeit der paketvermittelten Telefonie mit sich. Wie in modernen Telefonsystemen üblich, wird Sprache digitalisiert, paketiert und mittels IP übertragen (Voice over IP, VoIP). Entsprechend heißt es hier VoLTE. In der Praxis ist VoLTE noch nicht in allen Mobilfunknetzen implementiert. Sie merken das, wenn Sie im Gebäude über WLAN telefonieren („WLAN Call" bzw. „Wi-Fi Calling") und sich dann ins Freie bewegen. Wahrscheinlich reißt Ihr Gespräch dann ab. WLAN Call wurde nämlich ebenfalls in 4G spezifiziert und ist quasi VoLTE über WLAN. Ein nahtloses Handover zum Mobilfunk ist nur möglich, wenn das Mobilfunknetz VoLTE unterstützt. Tut es das nicht, bricht das Gespräch ab und muss anschließend leitungsvermittelt neu aufgebaut werden. Mit anderen Worten, die Telefonie ist in vielen Mobilfunknetzen bis zum heutigen Tag 2G.

Die fünfte Mobilfunkgeneration bringt nun eine weitere Leistungssteigerung. Das Smartphone spricht nun „Gigabit" – so jedenfalls wird es dem unbedarften Anwender verkauft. Und in der Tat werden die ersten 5G-Netze auch nicht mehr als das können. Dazu später mehr. Die ITU-R jedenfalls hat weitergehende Ideen zum 5G-Mobilfunk und diese in IMT-2020 spezifiziert [3]. Abbildung 2 zeigt eine Grafik daraus, die Sie so oder so ähnlich auch in anderen Publikationen über 5G finden werden. Demnach wird der zukünftige Mobilfunk drei grundsätzliche Anwendungsszenarien unterstützen:

- Enhanced Mobile Broadband (eMBB): Hierunter versteht man noch schnelleres Internet für Smartphones, als LTE es zu bieten vermag. eMBB ist also im Grunde nichts Neues, und das ist es, was Ihnen heute als „5G" verkauft wird.
- Massive Machine Type Communications (mMTC): Dieses Szenario zielt auf das Internet der Dinge ab. Bis 50.000 Endgeräte (!) pro Funkzelle sollen unterstützt werden. Diese Endgeräte senden natürlich nur sehr selten und nur geringste Datenmengen. Da man also nur geringe Bitraten benötigt, kann die Übertragung sehr langsam erfolgen, was hohe Reichweiten zur Folge hat. mMTC ist also die Technik, mit der sich die inzwischen sprichwörtliche „letzte Milchkanne" ans Internet anbinden lässt.
- Ultra-reliable and Low Latency Communications (uRLLC): Darauf schielen alle Unternehmen, die Automatisierungstechnik nutzen oder entwickeln. Endlich soll es mit Mobilfunk möglich werden, Daten mit kürzester Latenz und höchst verlässlich übertragen zu können. Dies ist eine Voraussetzung für Anwendungen in der Industrie-Automation oder auch beim autonomen Fahren, im weitesten Sinne also Anwendungen mit Echtzeitdatenverarbeitung.

Damit diese Szenarien möglich werden, hat das 3GPP im Rahmen der 5G-Standardisierung verschiedene Techniken definiert (bzw. ist noch dabei). Einerseits ist dies eine gegenüber LTE noch einmal verfeinerte Luftschnittstelle, also die Technik, mit der Daten ausgesendet und empfangen werden.

Andererseits ist dies die Struktur des Mobilfunk-Core. Gegenüber der bisherigen Spielart, bei der sich die Core-Komponenten in zentralen Rechenzentren der Provider befinden, wird nun Edge Computing unterstützt, bei dem Core-Komponenten unmittelbar an der An-

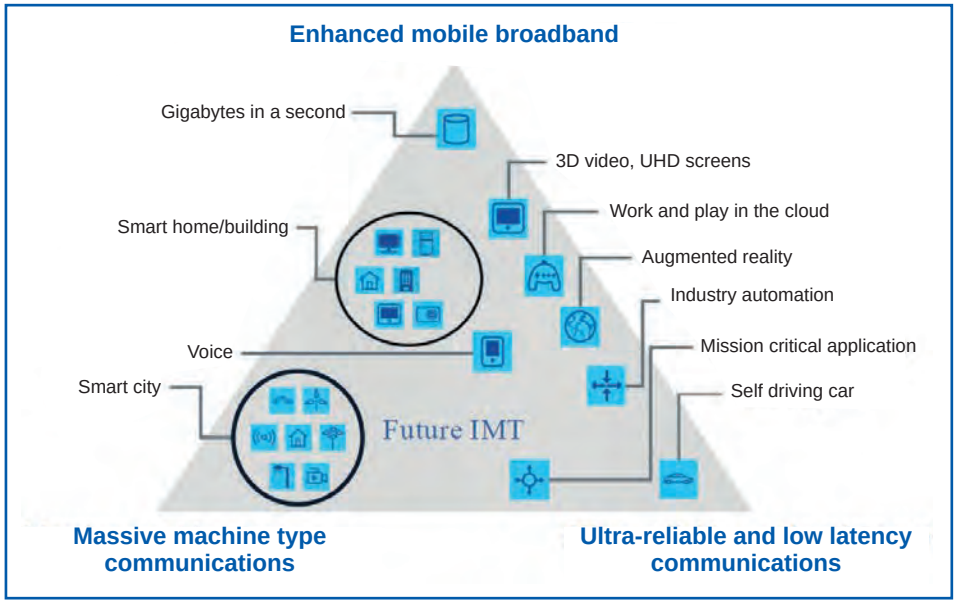

Abbildung 2: Anwendungs-Szenarien für IMT im Jahr 2020 und danach (Bildquelle [3])

Sicherung und Wiederherstellung von iOS-Geräten im Unternehmensumfeld

Fortsetzung von Seite 1

Mark Zimmermann weist mehrere Jahre Erfahrung in den Bereichen Mobile Sicherheit, Mobile Lösungserstellung, Digitalisierung und Wearables auf. 2009 hat er ein Team zur mobilen Lösungsentwicklung für einen der großen Energieversorger Deutschlands aufgebaut. Dieses Team hat über die Zeit sowohl Endkunden-Apps als auch Apps für den internen Einsatz agil gemeinsam mit dem Fachbereich entwickelt. Für eine dieser Lösungen wurde im Jahr 2013 der Best-Practice-Award 2013 des Bensberger Kreises vergeben. Er versteht es, mobile Themen aus den unterschiedlichen Herausforderungen darzustellen. Hierzu ist er auf nationaler Ebene mit Vorträgen und als freier Autor für Fachpublikationen tätig.

Backup auf einem lokalen Computer

Auf einem Mac oder PC können Anwender ein Backup ihres Geräts direkt erstellen. Ein solches lokales Backup (siehe Abbildung 1) enthält dann eine Kopie von den auf dem Gerät befindlichen Daten wie Kontakte, App-Inhalte, Fotos, Kalender und (MDM-)Konfigurationsdateien. Es sind auch Informationen wie Seriennummer, UDID, SIM-Hardware-Nummer und Telefonnummer enthalten.

Ein derartiges standardmäßig unverschlüsseltes Backup enthält allerdings nicht alle Daten eines Gerätes. Folgende Daten sind in einem solchen lokalen unverschlüsselten Backup nicht enthalten:

- Inhalte aus dem iTunes- und App-Store
- PDF-Dateien aus Apple Books
- iTunes-synchronisierte Inhalte
- bereits in iCloud gespeicherte Daten (z. B. iCloud-Fotos, iMessage-Nachrichten)
- Face-ID- oder Touch-ID-Einstellungen
- dienstlich per MDM-System installierte (managed) Apps
- per User-Enrollment verteilte Daten
- Apple Pay-Daten und -Einstellungen
- Apple Mail-Daten
- Aktivitäts-, Gesundheits- und Schlüsselbunddaten
- App-Daten, die der Entwickler aktiv von einem Backup ausgeschlossen hat

Optional lässt sich dieses lokale Backup auch verschlüsselt erstellen. Verschlüsselte Backups enthalten zusätzliche Daten. Aber auch hier sind einige Daten des Geräts nicht enthalten. Hierzu gehören:

- Aktivitäts-, Gesundheits- und Schlüsselbunddaten (z.B. Gesundheitsdaten, gesicherten Passwörter)
- WLAN-Einstellungen
- Website-Verlauf
- dienstlich per MDM-System installierte (managed) Apps
- per User-Enrollment verteilte Daten

Für KeyChain (Schlüsselbund) gelten hier einige Besonderheiten. Standardmäßig ist die KeyChain ein sicherer Ablageort von Apple zur Verwaltung von Kennwörtern und digitalen Zertifikaten. Die Verschlüsselung bzw. die Negierung dieser Option in einem Backup wirken sich direkt auf den Umgang mit diesen KeyChain-Einträgen aus.

Unverschlüsselte Backups können standardmäßig die KeyChain-Einträge nur auf dem gleichen Gerät wiederherstellten, von dem aus sie auch gesichert wurden. Der Grund liegt in der Art und Weise, wie KeyChain-Einträge in ein Backupfile transferiert werden. Diese werden dabei standardmäßig mit einem von der Geräte-UID abgeleiteten Schlüssel chiffriert. Dies erlaubt eine Wiederherstellung nur auf dem Gerät, von dem diese „gezogen“ wurden, da nur dieses Gerät die besagte UID zur Entschlüsselung besitzt.

Verschlüsselte Backups ermöglichen es dem Benutzer, eine Passphrase auszuwählen, mit der er seine Backup-Daten verschlüsseln kann. Es wird hier ein sogenannter Backup-Keybag erstellt. Dieser wird durch die zur Verschlüsselung genutzte Passphrase geschützt. Diese Passphrase wird mit 10 Millionen Interaktionen per PBKDF2 verarbeitet. In dieser neuen Backup-Keybag werden die Datenschutzklassen-Schlüssel neu erstellt,

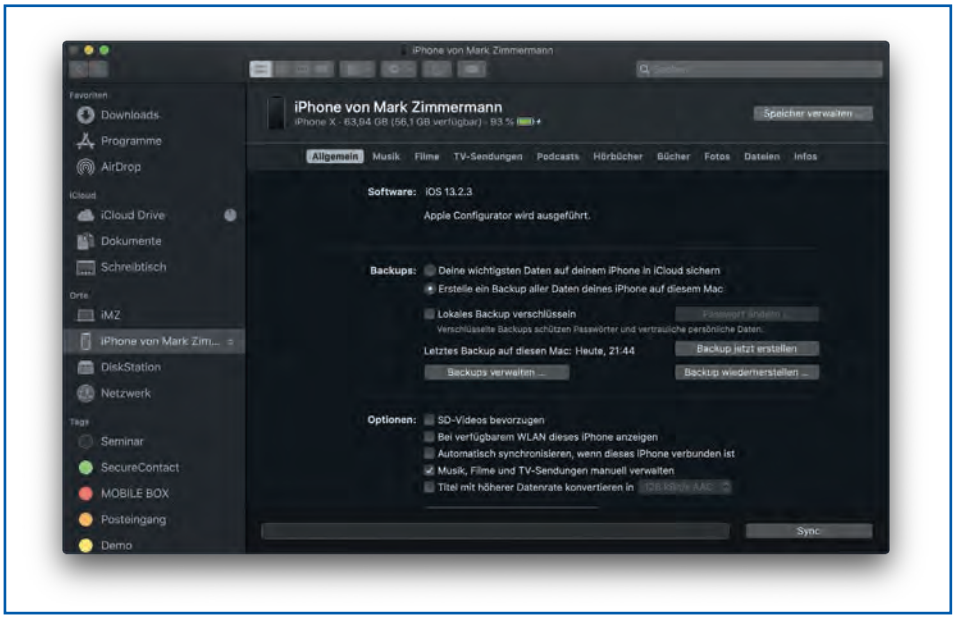

Abbildung 1: Lokale Backups an einem Computer

um die KeyChain-Daten mit diesen neuen Schlüsseln erneut zu chiffrieren - statt mit der UID des Gerätes. KeyChain-Objekte, die nicht in einem Backup vorgehalten werden dürfen, bleiben hingegen mit der Geräte-UID verschlüsselt. Wenn Entwickler möchten, dass die Keychain-Objekte ihrer App in einer Sicherung gespeichert werden, können diese die Keychain-Datenschutzattribute (thisDeviceOnly) verwenden.

Dies hat zur Folge, dass sich diese Werte - auch bei einem verschlüsselten Backup - nur auf dem gleichen Gerät wiederherstellen lassen. Für die restlichen KeyChain-Einträge gilt, dass sie sich auf jedem Gerät wiederherstellen lassen.

Exkurs: Was enthält dieser KeyBag und warum ist dieser so wichtig?

Der in iOS 4 eingeführte Datenschutzmechanismus auf iOS-Geräten schützt die (sensiblen) Daten im Dateisystem und die Elemente im Schlüsselbund durch Hinzufügen einer weiteren Verschlüsselungsebene. Hierzu verwendet iOS den Geräte-Passcode und einen gerätespezifischen Hardwareschlüssel, um einen Satz von Klassenschlüsseln zu erzeugen. Entwickler verwenden die Datenschutz-API von iOS, um den Dateien und den Einträgen in der Keychain ein Schutzklassenkennzeichen - basierend auf den Klassenschlüsseln - hinzuzufügen. Auf dem iOS-Gerät sind die Schutzartenschlüssel in dem System Keybag gespeichert. Während des Backups generiert das System einen neuen Satz von Schutzklassenschlüsseln und speichert diesen in der Backup-Keybag. Die in der System-Keybag gespeicherten Klassenschlüssel unterscheiden sich dabei nicht von den Schlüsseln in der Backup-Keybag. Geschützte Dateien und Daten im Backup werden mit den Klassenschlüsseln verschlüsselt, die im Backup-Keybag gespeichert sind. In unverschlüsselten Backups ist der Backup-Keybag mit einem von der iPhone-Hardware generierten Schlüssel (Key 0x835) und in verschlüsselten Backups mit der Passphrase, die der Anwender definiert hat, geschützt.

Übersicht möglicher Tools für lokale Backups

Nachdem wir nun die unterschiedlichen Verfahren zur lokalen Backup-Erzeugung besprochen haben, möchte ich Ihnen noch die Tools an die Hand geben, mit denen Sie ein solches Backup erzeugen und ggf. weiterverarbeiten können.

Aus dem Hause Apple gibt es hierfür zum einen die Software iTunes. Mit macOS Catalia wurde diese abgelöst und die Funktionen im Finder von macOS (siehe Abbildung 1) überführt. Wenn Sie den kostenlosen Apple Configurator aus dem macAppStore herunterladen, können Sie auch hier ein Backup von Geräten erzeugen. Die erzeugten Backups entsprechen 1:1 einem iTunes-Backup (siehe Abbildung 2).

Im Folgenden werfen wir einen kurzen Blick auf die Inhalte und den Aufbau eines solchen lokalen Backups. In dem Ordner des Backups ist eine Liste von Dateien in einem nicht direkt lesbaren Format angelegt. Dabei entspricht der Dateiname einem 40-stelligen alphanumerischen Hex-Wert ohne Dateiendung. So ist cd6702cea29fe89cf280a76794405adb17f9a0ee ein Beispiel für einen Dateinamen. Dieser 40-stellige Hex-Dateiname im Sicherungsordner ist der SHA1-Hash-Wert des Dateipfades, der an den jeweiligen Domänennamen mit dem Symbol "-" angehängt wird. Der Hash von DomainName-Dateipfad stimmt also mit der richtigen Datei im Backup überein. Die Liste der Systemdomänen kann aus der Datei /System/Library/Backup/Domains.plist auf dem iPhone eingesehen werden.

So entspricht das Backup des Adressbuchs dem SHA1-Hash-Wert “cd6702cea29fe89cf280a76794405adb17f9a0ee”. Wer den Hash-Wert einer spezifischen Datei ermitteln will, kann sich auch eines Online Hash Calculator (http://www.fileformat.info/tool/hash.htm) bedienen (z.B. HomeDomain-Library/AddressBook/AddressBookImages.sqlitedb -> cd6702cea29fe89cf280a76794405adb17f9a0ee).

Jedes iOS-Backup enthält außerdem die folgenden vier Meta-Dateien:

- Info.plist: Diese Datei enthält unter anderem Gerätedetails wie Gerätename, Build-Version, IMEI, Telefonnummer, letztes Sicherungsdatum, Seriennummer, Synchronisierungseinstellungen und eine Liste der Anwendungsnamen, die auf dem Gerät installiert wurde.
- Manifest.plist: Diese Datei enthält beispielsweise Details zu Drittanbieter-Apps, ein Flag zur Identifizierung, ob das Gerät eine Geräte-PIN hat (wasPasscodeSet).
- Status.plist: Diese Datei enthält unter anderem den Backup-Status, ein Kennzeichen zur Identifizierung der Vollsicherung (isFullBackup).
- Manifest.mbdb: Diese Binärdatei enthält Informationen über alle anderen Dateien in dem Backup. Wenn Sie Werkzeuge zur Extraktion von Daten aus Backups einsetzen, wird genau diese mbdb-Datei auf die enthaltene Dateistruktur geprüft. Damit werden die Kauderwelsch-Backup-Dateien in ein lesbares Format überführt.

All das hört sich eventuell kompliziert an. Es gibt allerdings Tools am Markt, die den Umgang mit Backups - auch aus Anwendersicht - stark vereinfachen (Beispiel siehe Bild 3). Dabei nutzen diese Tools die gleichen Schnittstellen, die Apple bereithält. Das heißt die Backup-Dateien enthalten nicht mehr und nicht weniger als die Standardwerkzeuge. Allerdings bieten die-

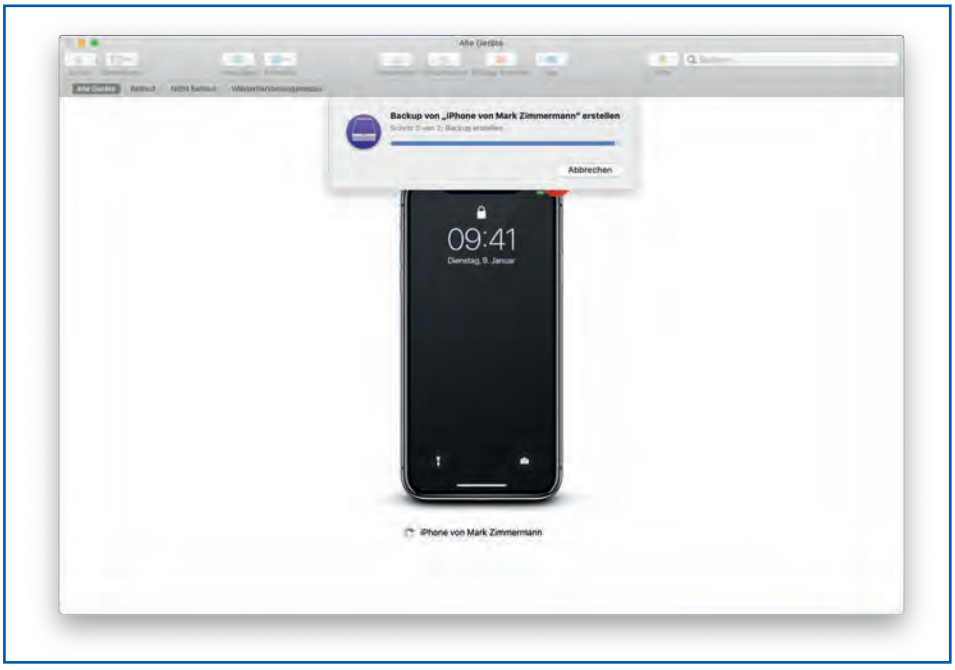

Abbildung 2: Backup per Apple Configurator