April 2023

ComConsult GmbH
Beratung + Planung + Schulung

Der Netzwerk Insider

Migration von ISDN zu SIP-Trunk

von Leonie Herden

Sprechen Sie schon SIP? Zumindest im Bereich der Sprachkommunikation geht kein Weg am Session Initiation Protocol (SIP) vorbei. Einerseits wird SIP als Signalisierungsprotokoll bei IP-basierten Telefonanlagen und UC-Lösungen sowie bei SIP-Trunks zwischen verschiedenen, IP-basierten Anlagen eingesetzt. Zum anderen stellen die Provider seit Jahren die Amtsanschlüsse von klassischen, ISDN-basierten Anschlüssen auf IP-basierte Anschlüsse um. Diese Umstellung ist zwar schon sehr weit fortgeschritten, jedoch sind noch längst nicht alle Amtsanbindungen als SIP-Trunk realisiert. Daher stehen einige Unternehmen auch heute noch vor einer Migration der ISDN-basierten Amtsanbindungen.

Seite 10

Anycast, das unbekannte Verfahren

von Dr. Behrooz Moayeri

Im Januar 2023 bin ich zuletzt auf die Vor- und Nachteile von Layer-2-Ethernet-Verbindungen zwischen verschiedenen Rechenzentren (RZ) eingegangen. Ich habe die 20 Jahre alte Diskussion darüber erwähnt, ob Hochverfügbarkeit für Cluster, deren Knoten auf verschiedene RZ verteilt sind, Layer-2-Netze erfordern, die sich über die verschiedenen RZ-Standorte erstrecken.

Seite 2

WiFi Calling als Ersatz für Mobilfunk?

von David Feuser

WLAN Interworking, WLAN Call oder WiFi Calling – die Funktionsweise, Mobilfunktelefonate (Sprache) oder SMS (Text) von einer WLAN-Infrastruktur aus über ein Mobilfunknetz zu einem Teilnehmer der Wahl zu übertragen, trägt unterschiedliche Bezeichnungen. Selbst die deutschen Provider konnten sich nicht auf einen Namen einigen, ...

Seite 30

Webinar der Woche

BAIT-Anforderungen an die Banken-IT und ihre Auslagerungspartner

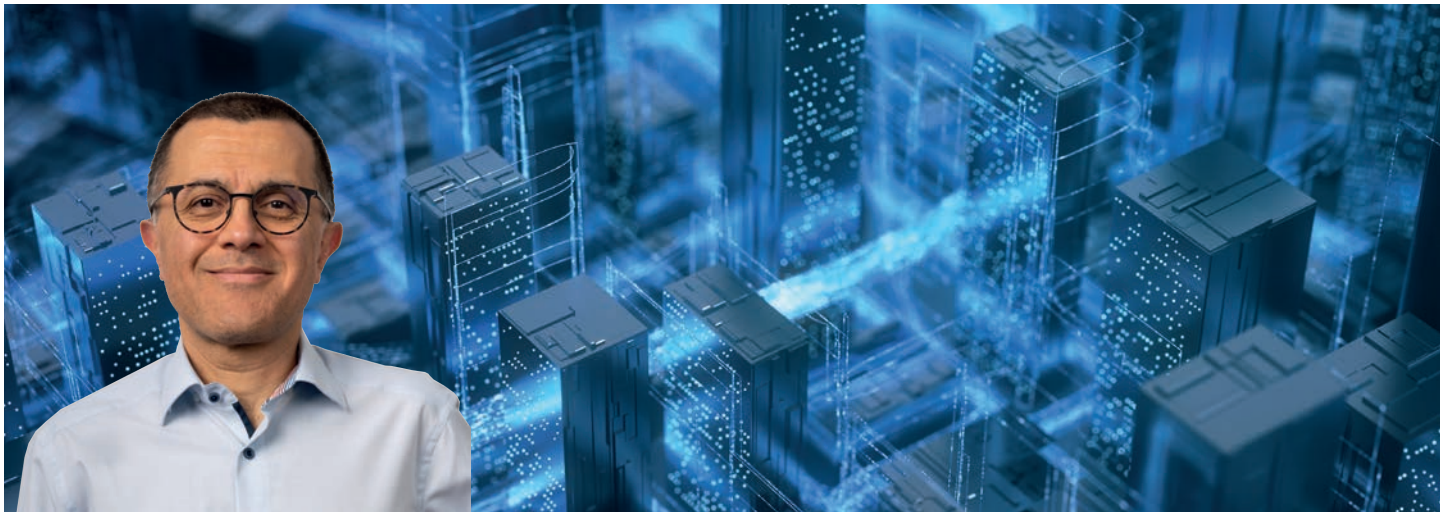
Seite 28

L4S – ein Booster für ECN?

von Dr. Joachim Wetzlar

Zugegeben, die Überschrift liest sich etwa so wie die meisten Standards von IEEE, IETF oder 3GPP. Offensichtlich ist man im angelsächsischen Raum Abkürzungen gewohnt; mir fällt es nach wie vor schwer, mich an solche Sätze zu gewöhnen. Wie dem auch sei, worum geht es?

Seite 26



Anycast, das unbekannte Verfahren

von Dr. Behrooz Moayeri

Im Januar 2023 bin ich zuletzt auf die Vor- und Nachteile von Layer-2-Ethernet-Verbindungen zwischen verschiedenen Rechenzentren (RZ) eingegangen. Ich habe die 20 Jahre alte Diskussion darüber erwähnt, ob Hochverfügbarkeit für Cluster, deren Knoten auf verschiedene RZ verteilt sind, Layer-2-Netze erfordern, die sich über die verschiedenen RZ-Standorte erstrecken. Im Rahmen von Projekten mit dem Schwerpunkt Standort-Redundanz für Rechenzentren wird diese Frage oft gestellt. Im Folgenden möchte ich in diesem Zusammenhang auf ein weitgehend unbekanntes Verfahren näher eingehen, nämlich Internet Protocol (IP) Anycast.

Anycast ist wichtiger, als man denkt

Im Vergleich zu den Modi Unicast, Multicast und Broadcast ist das Verfahren Anycast weniger bekannt. Dabei handelt es sich um eine unverzichtbare Methode. Ein Beispiel: Es gibt im weltweiten Internet nur 13 IPv4- und 13 IPv6-Adressen, unter denen die sogenannten Root-Server des Domain Name System (DNS) erreichbar sind. Wenn ein Name Server im iterativen Verfahren die passende IP-Adresse zu einem ihm unbekannten Fully Qualified Domain Name (FQDN) sucht, fragt er zuerst immer einen Root-Server. Man kann sich vorstellen, wie oft sich dieses Verfahren wiederholt, etwa immer, wenn auf irgendeinen Link im Internet geklickt wird, der einen dem Endgerät und dem von ihm beauftragten Name Server bisher unbekannten Hostnamen enthält. „Bisher unbekannt“ heißt konkret: nicht im temporären Zwischenspeicher vorhanden. Einträge im Zwischenspeicher für DNS (DNS Cache) sind recht kurzlebig, ein paar Stunden oder Minuten. Dann werden sie entfernt. Deshalb müssen die Root-Server im Internet insgesamt viele Milliarden Anfragen pro Stunde beantworten.

Reichen dafür 13 + 13 = 26 Server? Definitiv nicht. Hunderte physische Server beherbergen die identische sogenannte Root-Zone-Datei mit den für die Beantwortung der Root-Fragen notwendigen Informationen. Daraus folgt:

- Mehrere Server sind über dieselbe IP-Adresse erreichbar.
- Änderungen der Root-Zone-Datei werden zu allen Root-Servern repliziert.

Die erste Eigenschaft wird mittels IP Anycast realisiert. Ohne Anycast geht also im Internet nichts, und das schon seit Jahrzehnten. Dafür, dass es sich um einen so kritischen Dienst handelt, ist das Verfahren Anycast relativ unbekannt.

Neben Root-Adressen wird Anycast für viele andere Zwecke genutzt. Zum Beispiel verbergen sich hinter dns.google. zwei IPv6- und zwei IPv4-Adressen (8.8.8.8 und 8.8.4.4). Das sind sogenannte rekursive Resolver. Sie kümmern sich um den ganzen Prozess der Bearbeitung von DNS-Anfragen, angefangen mit der Root-Anfrage bis zur Anfrage beim autoritativen Name Server, der die Frage abschließend beantwortet. Auch der Google-Resolver nutzt viele Server, die über lediglich vier Adressen erreichbar sind.

Wie Anycast funktioniert

Das Anycast-Prinzip ist recht einfach. Die Anycast-Adresse wird verschiedenen Instanzen zugeordnet. Dies gilt auch für die Sicht der Router auf das Netz. Der Router 1 in einem RZ des Providers A ist direkt mit einer Instanz mit der Anycast-Adresse 202.12.27.33 im selben RZ verbunden, während der Router 2 in einem RZ des Providers B eine andere Instanz mit derselben IP-Adresse 202.12.27.33 im eigenen

Migration von ISDN auf SIP-Trunk

von Leonie Herden

Sprechen Sie schon SIP? Zumindest im Bereich der Sprachkommunikation geht kein Weg am Session Initiation Protocol (SIP) vorbei. Einerseits wird SIP als Signalisierungsprotokoll bei IP-basierten Telefonanlagen und UC-Lösungen sowie bei SIP-Trunks zwischen verschiedenen, IP-basierten Anlagen eingesetzt. Zum anderen stellen die Provider seit Jahren die Amtsanschlüsse von klassischen, ISDN-basierten Anschlüssen auf IP-basierte Anschlüsse um. Diese Umstellung ist zwar schon sehr weit fortgeschritten, jedoch sind noch längst nicht alle Amtsanbindungen als SIP-Trunk realisiert. Daher stehen einige Unternehmen auch heute noch vor einer Migration der ISDN-basierten Amtsanbindungen. Hierbei gibt es einige Punkte zu beachten: angefangen von der grundsätzlichen Architektur, also der Frage, ob ein zentraler SIP-Trunk oder mehrere, dezentrale SIP-Trunks genutzt werden sollen, über die Absicherung mittels Session Border Controler (SBC) bis hin zum physikalischen Anschluss an das Providernetz. Diese und weitere Themen rund um das SIP-Trunking wollen wir im folgenden Artikel genauer betrachten.

Änderungen bei Umstellung von ISDN auf SIP-Trunks

Zunächst schauen wir auf typische Architekturen, die bei ISDN-basierten Amtsanschlüssen bei Unternehmen mit verteilten Standorten anzutreffen sind. Hier ist jeder Standort mit einem dedizierten ISDN-basierten Anschluss an das öffentliche Telefonnetz angebunden. Am Hauptstandort ist eine zentrale Telefonanlage (PBX, Private Branch Exchange) vorhanden, die sämtliche Teilnehmer mit den entsprechenden Leistungsmerkmalen versorgt. Die weiteren Standorte sind über ein Weitverkehrsnetz (WAN, Wide Area Network) mit dem Hauptstandort verbunden. Jeder Standort hat in der Regel eine lokale Rufnummer mit eigenem Rufnummernblock. Die Anzahl der Sprachkanäle ist abhängig von der Anschlussart, angefangen mit kleinen ISDN-Basisanschlüssen und ISDN-Mehrgeräteanschlüssen, die in der Regel 2 ISDN-Kanäle bereitstellen, bis hin zum Primärmultiplex-Anschluss (PMX-Anschluss), dessen Kanalanzahl ein Vielfaches von 30 ist. Die Abbildung 1 zeigt ein Beispielunternehmen mit mehreren dezentralen Standorten. Die Telefonanlage ist hier schon eine IP-basierte Anlage, die somit über ein ISDN-IP-Gateway an den ISDN-Trunk angeschlossen ist. Als ISDN-Trunk wird hier die Anbindung an den Provider bezeichnet.

Mit der Umstellung auf IP-basierte Anschlüsse ergeben sich für das Beispielszenario Änderungen in Bezug auf folgende Themen:

- Realisierung der Provider-Anbindung
- Verteilung der SIP-Trunks
- Dimensionierung des SIP-Trunks
- Notwendigkeit eines SBC im eigenen Netz

Realisierung der Provider-Anbindung

Zuerst schauen wir uns den grundsätzlichen Aufbau eines SIP-Trunks an (siehe Abbildung 2). Die Provider haben jeweils lokale Points of Presence (POP) sowie eigene SBCs, die jedoch für die Absicherung des eigenen Netzes sorgen. Aufseiten des SIP-Providers erfolgt der Übergang ins öffentliche Te-

Best-Practice-Erfahrungen aus Planungsprojekten von Smart Buildings

Mit Dr. Andreas Kaup sprach Christiane Zweipfennig

Der Markt für Smart Buildings erlebt derzeit ein großes Wachstum. Intelligente Gebäude nutzten moderne Technologien aus unterschiedlichen Bereichen, um Immobilien effizienter und nachhaltiger zu machen. Durch die Mehrung an Netzwerkkommunikationen in intelligenten Gebäuden steigen auch die IT-Security-Anforderungen im Gebäude. Ist ein Smart Building von Anfang an vorausschauend geplant und werden alle relevanten Gewerke von vornherein mit in die Planung einbezogen, spart man Zeit und verhindert nachhaltig unnötige Ausgaben und Planungsänderungen.

Dr. Andreas Kaup hat an der RWTH Aachen sein Masterstudium in Bauingenieurwesen abgeschlossen. Für seine Doktorarbeit forschte er in Kooperation mit der Tsinghua University in Peking im Erdbebeningenieurwesen und beschäftigte sich mit dem Einsatz von Smart Materials als Erdbebendämpfer. Nach seiner Promotion verlagerte sich sein Interesse auf die Energieeffizienz von Gebäuden sowie deren umweltschonenden Betrieb und so stieg er in die Smart-Building-Thematik ein. Seit 2022 ist er als Berater für Smart Technologies und Smart Buildings bei ComConsult tätig. In diesem Interview berichtet er darüber, welche Vorgehensweise sich bei der Planung von Smart Buildings in den Projekten von ComConsult bewährt hat.

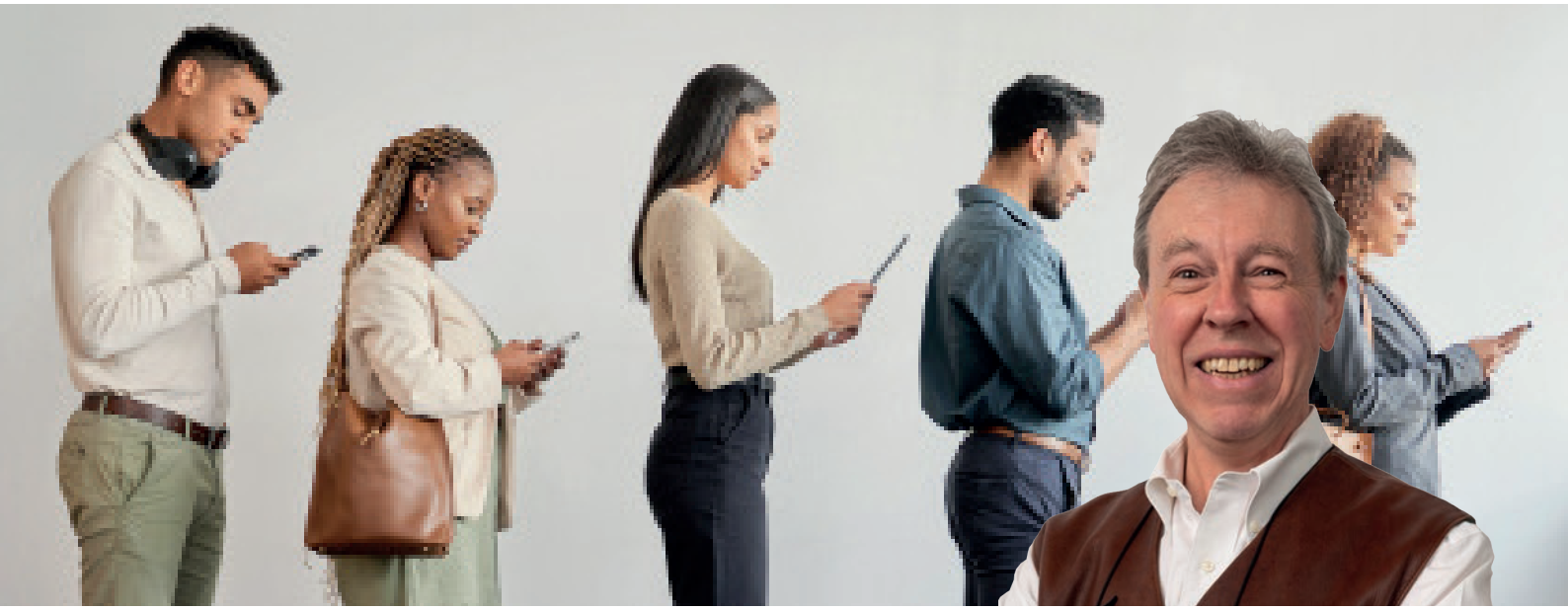
Das Competence Center Smart Buildings ist ein relativ junger Unternehmensbereich bei ComConsult. Das Thema Smart Building gewinnt zunehmend an Bedeutung. Was sind die Treiber und die Beweggründe der wachsenden Gebäudedigitalisierung?

Die Treiber für die zunehmende Digitalisierung von Gebäuden sind vielschichtig. Zum einen ist in den letzten Jahren durch die Pandemie die Homeoffice-Thematik in den Fokus geraten. In dieser Zeit standen viele Büroflächen leer, doch gab es durch die laufenden Kosten keine Einsparungen. Den Gebäudeinhabern wurde bewusst, dass sie kaum Daten darüber hatten, wie viele Personen sich wann in ihren Räumen aufgehalten haben. Es entstand der Wunsch nach Belegungsstatistiken und Flächenauswertungen mit der Motivation, die Gebäude auf dieser Grundlage energie- und kosteneffizienter zu nutzen. Ein weiterer Beweggrund war und ist, den Mitarbeitern durch die Gebäudedigitalisierung einen Anreiz zu schaffen, an ihre Arbeitsplätze zurückzukehren. Ein Wellbeing-Faktor ist zum Beispiel, dass durch Messungen der Raumluftqualität über Multisensoren für optimale CO2-Werte und eine konstante Raumtemperatur oder Luftfeuchtigkeit gesorgt werden kann. Die Hauptmotivation für die zunehmende Smartifizierung von Gebäuden liegt jedoch aus meiner Sicht ganz klar darin, Energie einzusparen. Ohne eine intelligente Gebäudeautomation ist es kaum möglich, gesetzliche Anforderungen zur Energieeffizienz und die ESG-Gebäudevorgaben zu erfüllen. ESG steht für Environmen-

> Energie- und kosteneffiziente Nutzung durch Belegunsstatistiken und Flächenauswertung

L4S – ein Booster für ECN?

von Dr. Joachim Wetzlar



Zugegeben, die Überschrift liest sich etwa so wie die meisten Standards von IEEE, IETF oder 3GPP. Offensichtlich ist man im angelsächsischen Raum Abkürzungen gewohnt; mir fällt es nach wie vor schwer, mich an solche Sätze zu gewöhnen. Wie dem auch sei, worum geht es?

L4S steht für “Low Latency, Low Loss, Scalable Throughput”. Der “L4S Internet Service” basiert auf dem Verfahren der Explicit Congestion Notification (ECN). Mit letzterem quäle ich regelmäßig die Teilnehmer meines Seminars „Fehlersuche in lokalen Netzen“. ECN funktioniert im Prinzip wie folgt:

- Sobald ein Router in einer seiner Warteschlangen eine hohe Auslastung feststellt, markiert er die entsprechenden IP-Pakete mit „Congestion Experience“.
- Der Empfänger erkennt diese Markierung und markiert seinerseits die Quittung an den Absender mit „ECN Echo“.
- Daraufhin wird der Absender seine Paketrate vermindern.

Das Verfahren erfordert nicht nur die Unterstützung durch Endgeräte und Server. Vielmehr müssen auch alle Netzkomponenten mitspielen. Wahrscheinlich ist das die Ursache dafür, dass ECN bisher kaum zum Einsatz kommt. Die deutschsprachige Wikipedia [1] schreibt:

„Wer ECN einsetzt, sollte sich bewusst sein, dass manche Administratoren die geänderte Semantik des TOS-Bytes durch den RFC 3168 im September 2001 noch nicht realisiert haben. Auch gehen Router und Firewalls selbst namhafter Unternehmen teilweise unvorhersehbar mit den ECN-Bits um. Es besteht daher die Gefahr, dass eine Verbindung mit eingeschaltetem ECN nicht zustande kommt.“

Ich selbst habe ECN an meinem Client aktiviert und beobachte keinerlei Einschränkungen. Protokollanalyse zeigt, dass es im Internet zahlreiche Sites gibt, bei denen ECN ebenfalls aktiviert ist. Einen Nutzen konnte ich bislang jedoch nicht nachweisen. Wahrscheinlich liegt das auch daran, dass die bisherige Art der Auslastungs-Regelung bei TCP, die im Wesentlichen auf Paketverlusten basiert, ganz gut funktioniert, und das wie folgt:

Aus Sicht der meisten TCP-Varianten besteht das Optimum darin, dass die Zahl unbestätigt gesendeter Pakete (das Congestion Window, CWND) dem Produkt aus Bandbreite und Antwortzeit (Round Trip Time, RTT) entspricht. An diesem Punkt ist das Medium vollständig ausgelastet, und es gehen noch keine Pakete verloren.

Um das Optimum zu erreichen, erhöht der Sender die Paketrate so lange, bis erste Pakete verloren gehen. Daraufhin vermindert er seine Sendetätigkeit schlagartig, um sich nachfolgend wieder an das vermeintliche Optimum heranzutasten, an dem Paketverluste einsetzen, und so fort.

Für die meisten Anwendungen ist das mehr als ausreichend. Stellt man jedoch erhöhte Anforderungen an die Übertragungsqualität, erkennt man die folgenden Nachteile:

- Die tatsächlich erzielte Bitrate folgt einer Art Sägezahn-Funktion, ist also nicht konstant.
- Verlorene Pakete müssen wiederholt werden („Retransmissions“), wodurch sich die Antwortzeit verlängert.
- Im Bereich des Optimums sind die Warteschlangen an den „Engstellen“ der Netze gefüllt, was ebenfalls die Antwortzeit erhöht.

Besser wäre es, frühzeitig die Paketrate zu begrenzen. Dann erreichte man dauerhaft geringe Antwortzeiten bei gleichmäßiger Bitrate. Dieses Ziel hat L4S im Auge. Scalable Congestion Control bedeutet, dass der Sender frühzeitig die Paketrate begrenzt, sodass keine Paketverluste auftreten. Dafür benötigt er die Infor-

WiFi Calling als Ersatz für Mobilfunk?

von David Feuser

WLAN Interworking, WLAN Call oder WiFi Calling – die Funktionsweise, Mobilfunktelefonate (Sprache) oder SMS (Text) von einer WLAN-Infrastruktur aus über ein Mobilfunknetz zu einem Teilnehmer der Wahl zu übertragen, trägt unterschiedliche Bezeichnungen. Selbst die deutschen Provider konnten sich nicht auf einen Namen einigen, sodass Telekom und Telefonica diese Funktion WLAN Call und Vodafone WiFi Calling nennt. Seit 2016 wird diese Technologie von allen deutschen Providern angeboten. Daher ist sie zwar nicht gerade die neueste, doch gewinnt sie immer mehr an Bedeutung, wenn es darum geht, eine allgemeine Erreichbarkeit für mobile Endgeräte kostengünstig dort zu schaffen, wo kein Mobilfunk existiert – was typischerweise in Gebäuden der Fall ist. Der Begriff Voice over WiFi (VoWiFi) sollte für diese Technologie als weltweit verständlich gelten und findet daher in diesem Artikel Anwendung.

Zu Beginn der Smartphone-Ära standen WLAN und die Mobilfunktechnologie noch konkurrierend gegenüber. WLAN wurde hauptsächlich für den reinen Datenverkehr genutzt, während Mobilfunk für die Telefonie, also Sprachübertragungen, und SMS zuständig war bzw. immer noch ist. Es war schlichtweg nicht möglich, Mobilfunkdienste über WLAN zu übertragen. Dies hat sich 2004 mit dem Unlicensed-Mobile-Access-(UMA-)Standard geändert, der von der GSMA (Groupe Speciale Mobile Association) veröffentlicht wurde. Das Ziel dieses Standards war es, Mobilfunkdienste an IP-Netze heranzuführen, sodass ein Wechsel zwischen den beiden Netzen möglich wurde. Mit der Einführung der IP-Technologie in der vierten Mobilfunkgeneration (4G) war der erste Schritt hin zu einer gemeinsamen Nutzung der beiden Technologien getan. Der UMA-Standard wurde dadurch in VoWi-Fi (WiFi Calling) umbenannt und an den heutigen Stand der Technik angepasst.

Architektur und Funktionsweise von VoWiFi

Schauen wir uns die Architektur und Funktionsweise von VoWiFi etwas genauer an. Abbildung 1 zeigt den klassischen Aufbau eines Anrufs mittels Voice over LTE (VoLTE) (in Grün dargestellt) und einem Teilnehmer, der VoWiFi nutzt (in Rot dargestellt). Als Erstes betrachten wir, wie Sprache in LTE-Mobilfunknetzen übertragen wird.

In 2010 haben die deutschen Provider begonnen, LTE in ihren Mobilfunknetzen zu implementieren. Was Ihnen vielleicht noch nicht bekannt ist: Zunächst ist keine Sprachlösung im LTE-Standard implementiert worden, da die Hauptziele höhere Datenraten, niedrige Latenzen und die Einführung der IP-Technologie waren. Die eigentliche Sprachübertragung wurde erst vier Jahre später mit der Veröffentlichung von LTE-Advanced (Release 10) eingeführt. Voice over LTE ermöglicht eine paketbasierte Telefonie, nämlich Voice over IP (VoIP), vom Endgerät (User Equipment, UE) verschlüsselt und über das Serving Gateway (S-GW) und das Packet Data Network Gateway (P-GW) im LTE Core hin zum IP Multimedia Subsystem (IMS). Das IMS ist quasi der Session Border Controller (SBC) des LTE-Netzes, dient als Vermittlungsstelle für IP-basierte Multimediaanwendungen und basiert auf dem Protokoll Session Initiation Protocol (SIP), dem Signalisierungsprotokoll von VoIP. Seit Mitte 2015 stellen die deutschen Provider den VoLTE-Service ihren Kunden zur Verfügung, der im Vergleich zu den vorherigen Mobilfunkgenerationen einen extrem kurzen Rufaufbau (innerhalb weniger Sekunden) und eine bessere Sprachqualität durch Nutzung von breitbandigen Codecs bietet. Heute wird VoLTE großflächig in Deutschland angeboten und von den Endanwendern genutzt.