ComConsult Research

Der Netzwerk Insider

Januar 2016

Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

Wireless Trends: LTE-Entwicklungen und Konsequenzen für die Betreiber privater Wireless Infrastrukturen

von Dr. Franz-Joachim Kauffels

Wie bereits im Artikel zu IEEE 802.11ac (Dezemberausgabe) geschildert wurde, wachsen die Anforderungen auch an Mobilfunksysteme in einem fast schon als ungesund zu bezeichnendem Maße. Das liegt vor allem am Video-Steaming mit den „Hauptsündern" Netflix und YouTube. Eigentlich haben interessierte Betreiber vor, neue, stark personalisierte Anwendungen in einem weiten Bereich von der Gesundheitsfürsorge über mobile Zahlungssysteme bis hin zu noch aufdringlicherer Werbung als ohnehin schon (Mobile Service Advertising Protocol MSAP, „Minority Report" lässt grüßen) zu etablieren, auch um entsprechende Big Data Projekte zu

„füttern". Derartige Pläne können aber nicht richtig umgesetzt werden, wenn es keine hinreichende Bandbreite gibt. Aktuell gibt es Begehrlichkeiten hinsichtlich der Nutzung lizenzfreier Bänder, die bislang den WLANs vorbehalten waren, auch für LTE. Sollte es dazu kommen, werden Welten aufeinanderprallen und WLANs in den entsprechenden Überlappungsbereichen deutlich den Kürzeren ziehen.

Heute stellen wir die aktuelle ntwicklung vor und kommen dann auch mit dem Wissen aus dem letzten Artikel zu abschließenden Handlungsempfehlungen.

weiter auf Seite 6

Zweitthema

Session Border Controller: Die Perimeter-Komponente für All-IP - Teil 2

von Dipl.-Inform. Petra Borowka-Gatzweiler

4.3 SLA-Sicherstellung, Verfügbarkeit

Zur Sicherstellung der Service Level Agreements (SLA) und der Verbindungsqualität gehören nicht nur die Qualitätsüberwachung und Traffic Shaping. Der Session Border Controller muss auch eine ausreichende Verfügbarkeit und Robustheit aufweisen.

Robustheit, Verfügbarkeit

Redundanzfunktionen und ein robustes Betriebssystem sind Grundvoraussetzung eines SBC.

Hierzu gehört auch die Implementierung wichtiger Funktionsmodule wie Signalisierung, Sicherheitsfunktionen, Transcoding, Traffic Engineering (TE) / Shaping, Deep Packet Inspection (DPI), Netzwerkzugang / Senden und Empfangen in separaten Prozessor-Einheiten. Separater Neustart der einzelnen Module, ISSU und gute Trouble Shooting-Möglichkeiten leisten weitere Verbesserungen der Robustheit.

weiter auf Seite 17

Geleit

Die Zukunft wird Wireless! Aber die Zeiten eines dominanten Standards sind vorbei

auf Seite 2

Aktueller Kongress

ComConsult Netzwerk Forum 2016

ab Seite 3

Standpunkt

Wenn Sicherheitskomponenten unsicher sind

auf Seite 14

Aktuelle Sonderveranstaltung

Das PSTN stirbt: Die neue Kommunikation mit SIP/IP

auf Seite 16

Zum Geleit

Die Zukunft wird Wireless! Aber die Zeiten eines dominanten Standards sind vorbei

Die Technologie-Entwicklung im Bereich WLAN folgte in den letzten Jahren ziemlich auf dem von ComConsult Research prognostizierten Pfad. Und mit IEEE 802.11ac Wave 2 erreichen wir so langsam eine Produkt-Situation, mit der viele sehr unterschiedliche Anwendungs-Szenarien abgedeckt werden können.

Trotzdem ist es an der Zeit die Grenzen dieser Technologie zu sehen und zu verstehen, dass wir mit dem bisherigen Vorgehen den zukünftigen Bedarf nicht abdecken können. Die Gründe dafür liegen in der Physik. Die Parameter:

- Abdeckung und Reichweite
- Bandbreite
- Teilnehmerzahl in einer Zelle

eines WLANs sind de facto ein Widerspruch in sich. Und tatsächlich sprechen wir von Gigabit WLAN, auch wenn wir in der Praxis die Gigabit nur mit erheblichen Einschränkungen im Design wirklich erreichen können.

Was bedeutet das und wie kann hier eine Lösung aussehen?

Die Antwort liegt ebenfalls in der Physik begründet. Wir können eben Gigabit nur auf sehr kurzen Distanzen wirklich umsetzen, speziell wenn wir die Gigabit pro Gerät und nicht pro Zelle sehen. Gleichzeitig haben wir aber für das Internet of Things den Bedarf, auch sehr große Distanzen zuverlässig abdecken zu können.

Die Lösung muss dementsprechend in einer Kombination aus verschiedenen Technologien liegen. Aus heutiger Sicht sind das u.a.

- IEEE 802.11ad für kurze Entfernungen und wirkliches Gigabit
- IEEE 802.11ac für größere Zellen mit aber immer noch einer hohen Leistung
- LTE mit 5G für alles darüber hinaus

Das Problem ist dabei, dass wir keine isolierten Technologie-Welten gebrauchen können. Wir werden Situationen haben, in denen wir Roamen wollen und ein Handover erforderlich ist. Und tatsächlich ist ein wesentlicher Teil der 5G-Entwicklung in dieser Harmonisierung der Technologien zu sehen. Für ein Endgerät muss es egal sein, über welche Funktechnik es kommuniziert. Dementsprechend muss es aber eben auch alle diese Funktechniken unterstützen.

Ein Kernproblem, in das wir dabei laufen werden, ist die Regulierung der Nutzung der “freien” Frequenzbänder. Und leider arbeiten die verschiedenen Interessen-Gruppen dabei nicht so zusammen wie man dies eigentlich erwarten sollte. Man kann sich des Eindrucks nicht erwehren, dass speziell die LTE-Fraktion keinerlei Rücksicht auf WLAN-Technologie nimmt und mehr oder weniger deutlich den Anspruch auf die entsprechenden Frequenzen erhebt. Nur damit bricht für Unternehmen die Chance einer konfliktfreien flächendeckenden Zeltplanung in den Unternehmen zusammen.

Nun wird ja gerade die Entwicklung von 5G noch mindestens 4 Jahre dauern. Die Frage ist also wie Unternehmen jetzt und heute zu einer geordneten Nutzung von Wireless Technologien kommen können. Und geordnet bedeutet aus meiner Sicht, dass wir Architekturen und Nutzungsformen finden müssen, die ein Miteinander von mindestens LTE, 11ac und 11ad ermöglichen. Zum jetzigen Zeitpunkt würde ich einige der preiswerten Funktechniken, die gerade für IoT eine Bedeutung haben können, aufgrund der Kombination aus Stromverbrauch und Kosten nicht abschreiben. Aber dies ist momentan keine Priorität. Mit dem Aufleben von 11ad - so wie wir auf der CES in Las Vegas in der letzten Woche beobachten konnten - sind wir an dem Punkt, an dem wir ein geordnetes Gesamtkonzept brauchen. Dies beinhaltet auch so simple Sachen wie Verkabelung in Integration von Access Points und Wireless Switching.

Wir haben diesen Themenbereich deshalb zu einem der Schwerpunkt-Themen auf unserem ComConsult Netzwerk Forum 2016 gemacht. Die Zukunft ist Wireless, das ist keine Frage. Was allerdings eine Frage ist, ist wie der richtige Technologie-Mix zu einem wirtschaftlichen und technischen Erfolg gebracht werden kann.

Ihr Dr. Jürgen Suppan

Kongress

ComConsult Netzwerk Forum 2016
18.04. - 21.04.16 in Königswinter

Das ComConsult Netzwerk Forum 2016 stellt die momentan dominantesten Netzwerk-Themen in den Mittelpunkt der Veranstaltung: Neue Technologien und IT-Architekturen, Netzwerk-Design, WLAN-Design und Sicherheit in Netzwerken. Drei Vortragstage und ein optionaler Vertiefungstag bilden den perfekten Rahmen um effizient und kompakt auf den neuesten Stand zu kommen. Das ComConsult Netzwerk Forum 2016 ist die herausragende Veranstaltung im Jahr 2016.

Moderatoren: Dipl.-Inform. Petra Borowka-Gatzweiler, Dipl.-Math. Cornelius Höchel-Winter, Dr.-Ing. Behrooz Moayeri
Preis: € 2.590,- netto 4 Tage / € 2.390,- netto 3 Tage / € 990,- netto 1 Tag

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

Aktueller Kongress

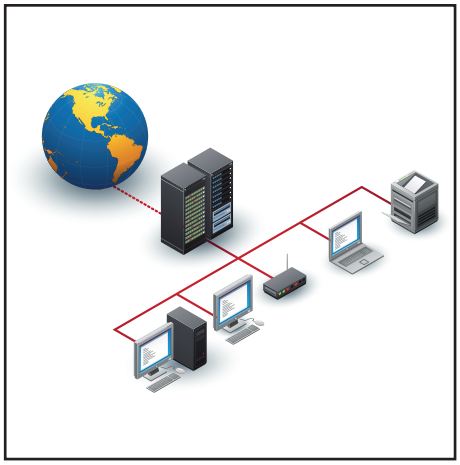
ComConsult Netzwerk Forum 2016
18.04. - 21.04.16 in Königswinter

Die ComConsult Akademie veranstaltet vom 18.04. bis 21.04.16 ihr "ComConsult Netzwerk Forum 2016" in Königswinter.

Das ComConsult Netzwerk Forum 2016 stellt die vier momentan dominantesten Netzwerk-Themen in den Mittelpunkt der Veranstaltung:

- Neue Technologien und IT-Architekturen: wie müssen sich Netzwerke ändern?
- Netzwerk-Design: skalierbare Kapazitäten, Service-orientiert und sicher
- WLAN-Design mit 802.11ac Wave 2 und die saubere Integration ins LAN-Design
- Sicherheit in Netzwerken: Zertifikate und NAC

Am ersten Tag analysieren wir u.a. ob wir zentral gesteuerte Netzwerk-Lösungen brauchen. An einer Reihe ausgewählter Anwendungsbeispiele wird untersucht, ob eine ausgelagerte Data-Plane den Betrieb, die schnelle Bereitstellung und die Gestaltung unterstützt oder ob das Ganze zu komplex wird. Hintergrund dazu ist die Frage, wie man Overlay-Netzwerke am besten konfigurieren und betreiben kann (verbunden natürlich mit der Frage, ob man sie überhaupt braucht).



Diese ergänzen wir um die praktische Frage nach der Zukunft des WAN: können sich WANs gegenüber dem Internet durchsetzen?

Am zweiten Tage steht Netzwerk-Design mit allen neuen Technologien im Vordergrund:

- Network Function Virtualization
- SDN
- 25/50/100: neue Bandbreiten für wen?
- Trill kontra Fabricpath kontra SPB kontra VXlan
- Layer 3 Design mit modernsten Technologien: wo stehen wir?

Der dritte Tag stellt zwei Sonderthemen in den Vordergrund, die in allen aktuellen Projekten eine tragende Rolle spielen und auch speziell das Jahr 2016 bestimmen werden:

- WLAN-Design nach 802.11ac Wave 2 und seine Integration in LAN-Design
- Sicherheit mit Zertifikaten und NAC

Das ComConsult Netzwerk Forum 2016 ist das richtig Forum zur richtigen Zeit.

Wir analysieren exklusiv für Sie:

- welche neuen Technologien und Produkte stehen für bessere und wirtschaftlichere Netzwerke zur Verfügung?
- wie verändern sich Anforderungen an Netzwerke?
- wie verändert sich Netzwerk-Design und wie können Sie die Vorteile zu Ihren Gunsten nutzen ohne das gesamte Netzwerk ablösen zu müssen?

Unser Vertiefungstag in diesem Jahr dreht sich komplett um IPv6 und die aktuellen Projekterfahrungen in diesem Bereich.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung
ComConsult Netzwerk Forum 2016

Ich buche den Kongress
ComConsult Netzwerk Forum 2016
18.04. - 21.04.16 in Königswinter

☐ 18.04. - 21.04.16 in Königswinter
zum Preis von € 2.590,-- netto - 4 Tage

☐ 18.04. - 20.04.16 in Königswinter
zum Preis von € 2.390,-- netto - 3 Tage

☐ Bitte buchen Sie mir ein Hotelzimmer

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

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

Programmübersicht - ComConsult Netzwerk Forum 2016

Montag, den 18.04.2016 - IT-Architekturen und neue Technologien

9:30 bis 10:30 Uhr
Die Top-Themen 2016
- Warum sich SDN in Unternehmensnetzen nicht durchsetzt (Unterschiede zwischen Unternehmens- und Hyperscaler-Netzen)
- WANs unter zunehmendem Einfluss der Entwicklungen im Internet
- Risiken des Aufschubs der IPv6-Einführung

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

10:30 bis 11:30 Uhr
Cloud Computing: Einsatz im Unternehmen
- Anspruch vs. Marketing: Was ist Cloud Computing eigentlich?
- Cloud-Produkte im Unternehmenseinsatz:
  - Nutzbarkeit: Cloud-Produkte sind „anders“
  - Anforderungen an die Netzwerke und die Infrastruktur
  - Wo liegen Nutzungsgrenzen und typische Probleme
- Erfahrungen aus konkreten Projekten

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

11:30 Uhr Kaffeepause

12:00 bis 12:45 Uhr
Internet of Things
- Was ist IoT / Industrie 4.0
- Anwendungsbereiche, Einsatz-Szenarien
- Architektur und Protokolle
- Wo steht die Standardisierung?
- IoT Roadmap der nächsten Jahre

Dipl.-Inform. Petra Borowka-Gatzweiler, UBN

12:45 Uhr Mittagspause

14:15 bis 15:00 Uhr
Wandel der Netzwerkarchitekturen in Zeiten von SDN
- Private Cloud und Hybrid Enterprise verändern die Anforderungen
- Von SDN zu SDx, sind Sie bereit dafür?
- Separierung von Underlay und Overlay Netzmanagement
- Warum Layer 3 Underlay Designs
- Für Enterprise braucht man mehr – Layer 2 over Layer 3 mit VXLAN
- VXLAN Control Plane Optionen – mit (SDN) Controller und ohne
- Wie passen VMware und OpenStack ins Bild

Dipl.-Ing. Markus Nispel, Extreme Networks GmbH

15:00 bis 15:45 Uhr
Docker: Fluten Container bald das RZ?
- Was sind Container und wie funktionieren sie?
- Wie unterscheiden sich Container von klassischen Virtualisierungstechniken?
- Was sind die Vor- und Nachteile? Was werden die typischen Anwendungsgebiete von Containern sein?
- Was sind die Konsequenzen für das Netzwerk von Rechenzentren?
- Sind Container in der Cloud?

Markus Schaub, ComConsult-Study.tv

15:45 Uhr Kaffeepause

16:15 bis 17:15 Uhr
Cloud-Computing: der rechtliche Rahmen und die Herausforderungen

Dr. Fabian Niemann, Bird & Bird LLP

ab 18:00 Uhr Happy Hour im Foyer

Dienstag, den 19.04.2016 - LAN-Design: Planung, Betrieb

9:00 bis 10:00 Uhr
SDN/NFV
- Wo steht der SDN-Markt?
- Was ist NFV? (Architektur, Einsatzszenarien, Marktbedeutung)
- Abgrenzung und Überlappung von NFV und SDN
- NFV und Network Services (Service Chaining mit NSH)

Dipl.-Inform. Petra Borowka-Gatzweiler, UBN

10:00 bis 11:00 Uhr
Netzdesign im Vergleich
- Layer 3 Design mit z.B. BGP
- Layer 2 Design mit SPB
- Layer 4 Design mit z.B. QUIC
- Lösungen wie NSX, ACI oder OpenFlow

Markus Geller, ComConsult Research GmbH

11:00 Uhr Kaffeepause

11:30 bis 12:30 Uhr
Anwender-Erfahrungsvortrag IPv6

N.N.

12:30 Uhr Mittagspause

14:00 bis 14:45 Uhr
Architektur im Rechenzentrum - 25, 50 und 100G
- Einführung in eine neue Generation von offenen und skalierbaren RZ Switchen
- 25G, die neuen 10G? • 50G, die neuen 40G für Storage?
- 100G, der neue 40G Interconnect?
- Anwendungsfälle für Rechenzentren
- Remote Direct Memory Access über Converged Ethernet (RoCE) in der Praxis

Arne Heitmann, Mellanox Technologies Ltd.

14:45 bis 15:30 Uhr
Fabrics kontra Standard-Design an Projektbeispielen

Heinz Behrens, Avaya GmbH & Co KG

15:30 Uhr Kaffeepause

16:00 bis 17:00 Uhr
40 Gigabit-Ethernet und mehr: Auswahl zukunftssicherer Schnittstellen und der optimalen Verkabelung
- Simplizität der alten und Komplexität der neuen physikalischen Schnittstellen
- Schnittstellenvielfalt der Switch-Hersteller
- Unbeachtete Abhängigkeiten zwischen Elektronik und Verkabelung
- MPO war gestern, LC ist heute! Ist das so?
- Unbekannte Modul-Inkompatibilität der verschiedenen Datenraten
- Die universelle Verkabelung für alle Datenraten

Dipl.-Ing. Hartmut Kell, ComConsult Beratung und Planung GmbH

Programmübersicht - ComConsult Netzwerk Forum 2016

Mittwoch, den 20.04.2016 - WLAN-Design: Planung und Betrieb / Sicherheit

9:00 bis 10:00 Uhr
Neue WLAN-Techniken und ihr Einfluss auf Enterprise WLANs
- DCF: „Pest“ oder Segen für die Entwicklung des WLAN?
- Die dritte Welle der WLAN Chips rollt auf uns zu! Wie profitieren Enterprise WLANs davon?
- WLAN bis 10 Gigabit/s braucht man für Ultra HD Video. Welche Anwendungen profitieren sonst noch davon?
- LTE und 5G: auch der Mobilfunk wird schneller. Warum überhaupt noch WLAN aufbauen?
- Mobilfunk im auch 5-GHz-Band? Werden WLAN nun die Frequenzen geraubt?

Dr. Joachim Wetzlar, ComConsult Beratung und Planung GmbH

10:00 bis 11:00 Uhr
Wireless Evolution: von 11ac wave 2 zu LTE-Erweiterungen
- Megatrend Mobilität, Status und Wachstum
- Professionelle WLANs mit IEEE 802.11ac wave 2
- IEEE 802.3ad reloaded: 60 GHz-Bereich, 7Gbit/s
- Die Entwicklung von LTE, auch im lizenzfreien Bereich

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

11:00 Uhr Kaffeepause

11:30 bis 12:30 Uhr
WLAN in der Praxis

N.N.

12:30 Uhr Mittagspause

14:00 bis 14:45 Uhr
Fallstricke und Best Practice bei NAC
- Warum IEEE 802.1X immer noch ein Alptraum sein kann
- Best Practice NAC: Wie NAC erfolgreich umgesetzt und betrieben werden kann
- Welches Sicherheitsniveau mit NAC überhaupt geschaffen werden kann
- Ist MACsec eine Alternative?
- Evolution von NAC: Von Advanced Monitoring über Profiling bis hin zur Abwehr zielgerichteter Angriffe

Dipl.-Inform. Daniel Prinzen, ComConsult Beratung und Planung GmbH

14:45 bis 15:30 Uhr
Sichere Kommunikation im Netz mit Zertifikaten: Alptraum oder etablierte Technik?
- Von NAC über Web-Anwendungen bis zum SSL-VPN: Anwendungen von Zertifikaten zur sicheren Kommunikation
- Fallstricke Schlüsselmanagement und Vertrauenskette: Welche Sicherheitsvorfälle es gab und was wir dagegen tun können
- Certificate Pinning und Certificate Transparency: Warum das Konzept der Vertrauenskette dringend renoviert werden musste

Dr. Simon Hoff, ComConsult Beratung und Planung GmbH

15:30 Uhr Ende der 3-tägigen Veranstaltung - Kaffeepause für Teilnehmer der 4-tägigen Veranstaltung

Donnerstag, den 21.04.2016 - Optionaler Zusatztag "IPv6"

ab 9:00 den ganzen Tag
IPv6 Migration: Projektvorbereitung und Umsetzung
- Organisation eines IPv6 Rollouts (Planung des Vorgehens, was muss wann entschieden werden, welche Abteilungen sind in welcher Projektphase gefordert, wo existiert Schulungsbedarf)
- Adresskonzept (Welche Alternativen stehen zur Verfügung, was sind die Vor- und Nachteile)
- Zuweisung von IPv6 Adressen (Welche Verfahren stehen zur Verfügung, wie integriert man Komponenten, die kein DHCPv6 unterstützen)
- Anforderungen an Netzwerk- und Infrastrukturkomponenten (Erstellung von Anforderungsprofilen für einzelne Komponenten, Testdurchführung, ausgewählte Testergebnisse)
- LAN-Archtitektur (Redundanzverfahren: VRRP, HSRP, Routing von IPv6, Umgang mit QoS bei IPv6)
- Migration der Internetpräsenz
- Migration von Anwendungen und Appliances
- Erstellung eines Anforderungskataloges für die Anschaffung von Hard- und Software
- Externe Anbindungen (WAN, Internet, Internet-VPN, Externe Partnerunternehmen)
- Security (Ergebnisse von Proxy-Tests, Firewalls & IDS, First-Hop-Security)

Markus Schaub, ComConsult Study.tv

10:30 Uhr Kaffeepause
12:45 Uhr Mittagspause
15:30 Uhr Ende der 4-tägigen Veranstaltung

Besuchen Sie auch das Kongressportal zum Netzwerk Forum 2016 mit vielen Zusatzinformationen, Artikeln und Videos exklusiv für die Teilnehmer.

http://www.comconsult-research.de/kongresse/netzwerk-2016/

Schwerpunktthema

Wireless Trends: LTE-Entwicklungen und Konsequenzen für die Betreiber privater Wireless Infrastrukturen

Dr. Franz-Joachim Kauffels ist Technologie- und Industrie-Analyst und Autor. Seit über 30 Jahren unabhängiger, kritischer und oft unbequemer Bestandteil der Netzwerkszene. Verfasser von über 20 Büchern in über 70 Ausgaben sowie über 2000 Artikeln, Videos und Reports.

Fortsetzung von Seite 1

Erinnern wir uns an die Mobilfunksysteme auf dem Weg zu LTE. Zunächst war man froh, einigermaßen ungestört telefonieren zu können. Mit UMTS entstanden die ersten Möglichkeiten zur Datenübertragung, die über GPRS schließlich zu LTE geführt haben. LTE seinerseits ist ebenfalls laufend in Entwicklung begriffen, Mitte 2015 haben die meisten privaten Nutzer Release 10, aber es gibt schon Initiativen in Richtung Release 13.

Das Kernproblem ist jedoch, dass die Mobilfunktechnik grundsätzlich anders arbeitet als ein herkömmliches Datennetz wie ein LAN oder ein WLAN. Mobilfunktechnik basiert immer auf dem Grundgedanken eines **geordneten** Funknetzes. Es gibt immer zentrale Stationen (z.B. Base Stations), die die Leistung des Netzes systematisch an die Nutzer (Subscriber) unterverteilen. Ein geordnetes Funknetz unterscheidet zwischen Up- und Downstream (Base zu Subscriber, Subscriber zu Base) und in den verschiedenen Richtungen werden meist auch unterschiedliche Steuerungsmethoden benutzt, vorzugsweise Raum und/oder Zeitmultiplexverfahren. Aktuell benutzt LTE im Uplink Single Carrier und für den Downlink OFDMA. (siehe Abbildung 12) In einem WLAN, auch in 802.11ac wave2, herrscht vergleichsweise fast das pure Chaos und ein mittlerweile über 40 Jahre altes Steuerungsverfahren sorgt unter systematisch hohen Verlusten für ein wenig Ordnung. All dies hat Vor- und Nachteile.

Ein geordnetes Funknetz kann wesentlich mehr Teilnehmer sinnvoll versorgen als ein übliches WLAN und das auch mit einer höheren Reichweite in einer Zelle. Seine Dienste sind allerdings eher schmalbandig, die Verfahren dazu optimiert, möglichst vielen Stationen ein gerechtes, kleines Teil vom Bandbreite-Kuchen abzugeben. Ein WLAN geht hingegen in die Knie, wenn zu viele Teilnehmer arbeiten wollen. Dafür kann es einem individuellen Teilnehmer aber vergleichsweise sehr viel Bandbreite geben.

Sie sehen schon, worauf es hinausläuft: um den Anforderungen in Zukunft gerecht werden zu können, muss das grobmaschige Mobilfunksystem durch eine Vielzahl kleiner Zellen ergänzt werden. Diese kleinen Zellen können WLANs sein. Das gibt es ja heute schon, aber aus der Perspektive der Mobilfunk-Entwickler wäre es wünschenswert, eine eigene Technologie für diesen Zweck zu haben, die im Kontext des Mobilfunks weiterentwickelt werden kann. (siehe Abbildung 13)

In den vergangenen Jahren gab es schon eine Reihe von Vorschlägen für solche „Pico“- oder „Femto“-Zellen, von denen sich aber keiner durchsetzen konnte, weil sich schlicht zu viele selbsternannte Stan-

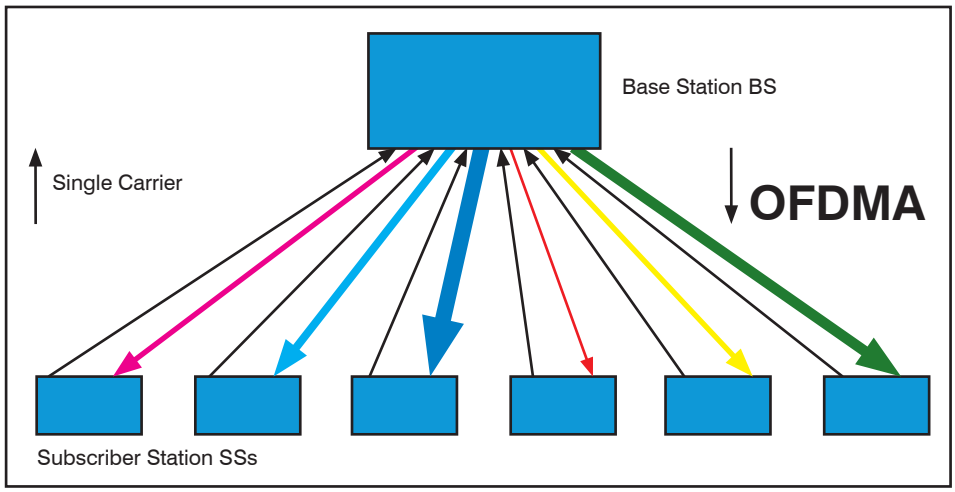


Abbildung 12: Geordnetes Funknetz

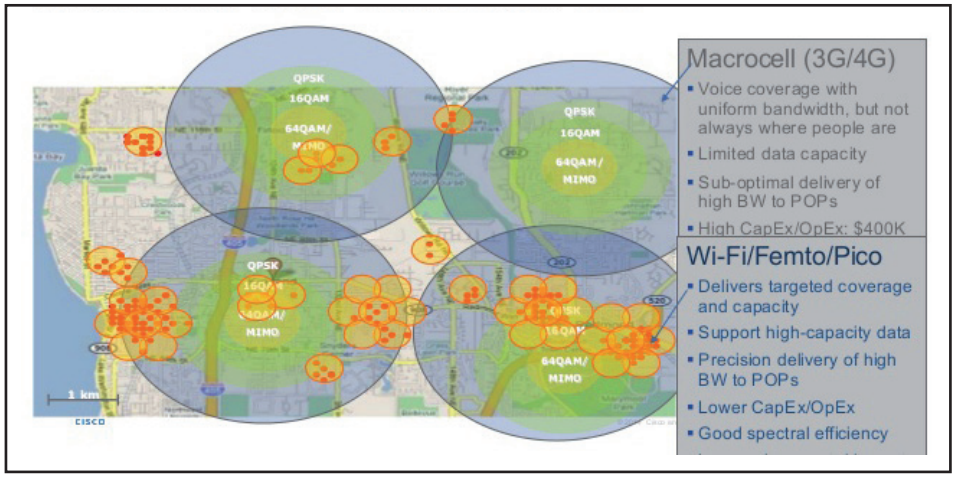


Abbildung 13: Der Charme kleiner Zellen Quelle: Cisco

dardisierungsgremien gegenseitig paralysiert hatten.

So blieb den Herstellern nichts anderes übrig, als selbst teilweise sehr komplexe Systeme zur Zusammenarbeit zwischen gängigen Mobilfunksystemen und Small Cells, meist auf WLAN-Basis zu etablieren. Ein solches System bietet für den Betreiber idealerweise natürlich den Vorzug, dass er das gesamte Gebilde mit den unterschiedlichen Funkverfahren und Bereichen einheitlich steuern und betreiben kann. Das spielt eine umso größere Rolle, desto stärker die Bedrohungen werden, denen man nur durch abgestimmte Maßnahmen auf dem gesamten Verbund erfolgreich entgegentreten kann. Als Beispiel zeigen wir das Service Provider WiFi System von Cisco. (siehe Abbildung 14)

Provider sehen die durch ein solches System entstehenden Abhängigkeiten zu einem Hersteller aus prinzipiellen Erwägungen nicht gerne. Deshalb wird es auch weiterhin auf Standards basierende Weiterentwicklungen geben, die im Zentrum dieser Betrachtungen stehen.

Um ein Verständnis darüber zu entwickeln, was sich auf dem Bereich bewegt und wie letztlich die Implikationen dieser Entwicklungen auf private Betreiber wie Unternehmen und Organisationen sein werden, müssen wir leider etwas ausholen.

2.1 LTE Advanced

LTE Advanced ist die aktuelle Entwicklungsgeneration etwa von Release 10 bis Rel. 12. Es gibt schon viele ganze oder teilweise Implementierungen und LTE Advanced ist sozusagen der Rahmen für alles, was aktuell passiert.

Es gibt vier primäre Entwicklungsbereiche bei LTE Advanced:

1. Carrier Aggregation und ihre Weiterentwicklung
2. Möglichkeit zum Aufbau hyperdichter HetNets, weitere Gewinne durch verbesserte Empfänger
3. Ausdehnung von LTE auf lizenzfreie Spektren
4. Erweiterung von LTE auf neue Funktionsbereiche wie direkte Kommunikation zwischen Endgeräten oder Video-Streaming und Erschließung neuer, breiterer Frequenzbereiche

Carrier Aggregation gibt es schon länger. Sie soll aber in Zukunft nicht nur zwischen relativ benachbarten Frequenzbereichen wie heute arbeiten, sondern auch über verschiedene Träger, verschiedene Bänder und über lizensierte und unlizensierte Bereiche hinweg ausgedehnt werden können. Damit möchte man schlicht und ergreifend höhere Datenraten unterstützen. Schon wenn man nur fünf LTE Carrier mit einer Bandbreite von je 20 MHz zu einem einzigen mit einer Bandbreite bis zu 100 MHz zusammenschließt, kann man nicht nur hinsichtlich der Übertragungsrate, sondern auch bei der Latenz deutliche Verbesserungen erzielen. (siehe Abbildung 15)

Einfach dargestellt ist es so, dass mit einem breiteren Kanal Bursts, wie sie bei bestimmten Anwendungen entstehen, zügig verarbeitet werden können und dadurch freie Zeiten entstehen, die anderen Nutzern zugeteilt werden können. Durch viele Messungen und Analysen weiß man, dass schon zwei zusammen gelegte Kanäle über das übliche Anwendungsspektrum von Mobilgeräten deutlich mehr Leistung haben als lediglich die doppelte eines individuellen Kanals.

Die Carrier Aggregation kann sehr gewinnbringend mit MIMO-Übertragungsverfahren kombiniert werden. Die spektrale Effizienz, also das, was man aus einem Kanal an Übertragungsleistung „herausholen“ kann, steigt damit deutlich.

Die HetNets (Heterogeneous Networks) beschreiben die systematische Kombination von Mobilfunkzellen mit Small Cells. Genau hier ist die Stelle, an der man einem LTE-Netz Leistungen in bislang völlig ungeahnten Dimensionen verleihen kann. Man braucht dazu zwei wichtige Zutaten: die Möglichkeit der (ggf. temporären) Vergrößerung ihres Wirkungsbereiches und schlagkräftiges Interferenz-Management.

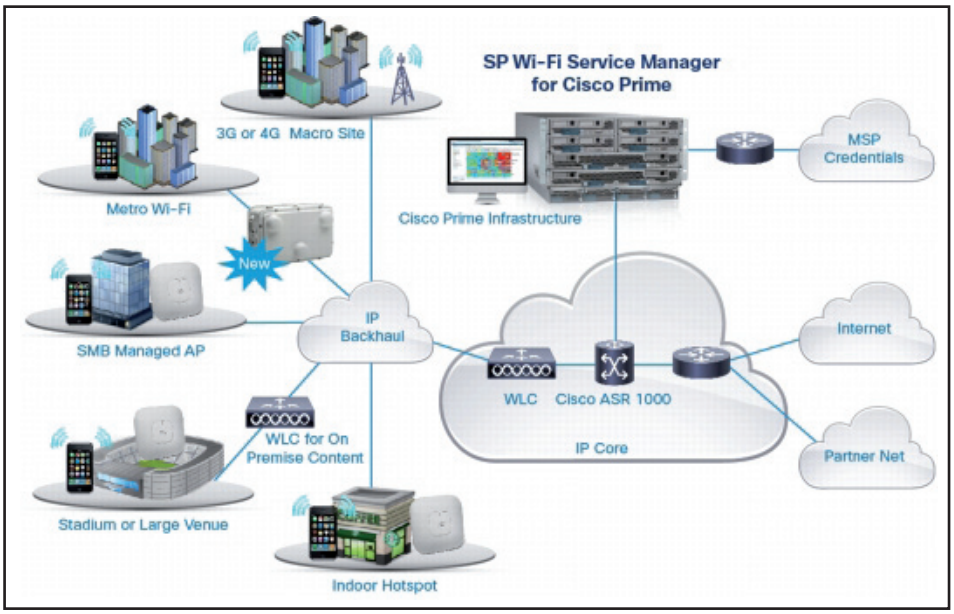


Abbildung 14: Cisco Service Provider WiFi System Quelle: Cisco

Wireless Trends: LTE-Entwicklungen und Konsequenzen für die Betreiber privater Wireless Infrastrukturen

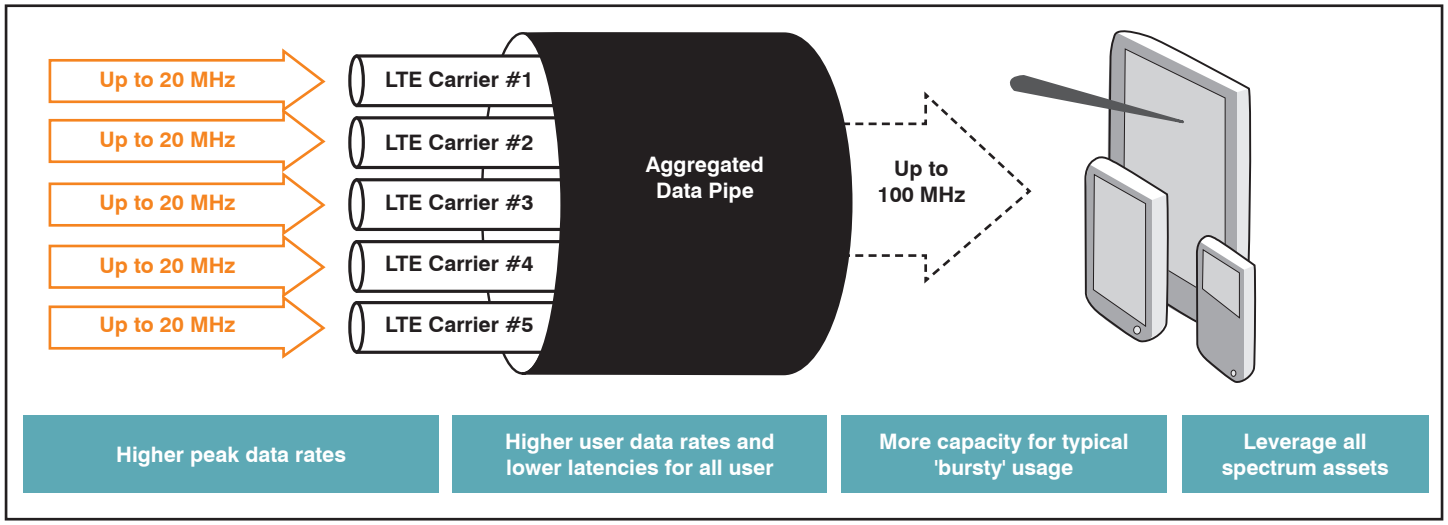


Abbildung 15: Carrier Aggregation Quelle: 3GPP

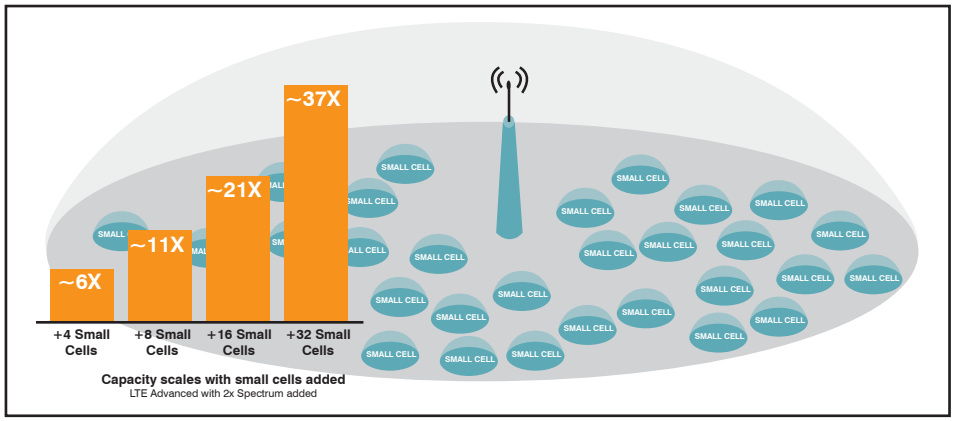


Abbildung 16: Kapazität skaliert dank umfangreichem Interferenz-Management mit der Anzahl der Small Cells Quelle: 3GPP

Letzteres ist Voraussetzung dafür, dass sich die Small Cells nicht gegenseitig stören. Eine Vergrößerung des Wirkungsbereiches kann man mit verbesserter Receiver-Technologie erzielen. Was wir dazu benötigen, haben wir schon weiter oben bei den WLANs besprochen: verbesserte Filter-Technologie zur Realisierung einer guten Nutzung der spektralen Möglichkeiten, sensible Zwischenverstärker bei Mehrantennen-Systemen und Beamforming.

Es ist tatsächlich so, dass sich die Gesamtkapazität der LTE-Zelle linear mit der Anzahl der Small Cells erhöht. Es gibt dazu zwei weitere Voraussetzungen. Die LTE Base Stations an den „Funktürmen“ benötigen einen sehr starken Glasfaser-Backbone, weil es sonst nicht zur zu Kapazitäts- sondern auch zu Latenzproblemen kommen kann. Das haben die Provider aber schon heute gut im Griff. Ein anderer Aspekt ist die letztlich zwischen Base Stations und Small Cells benötigte Bandbreite. Hier ist die Carrier Aggregation ein wichtiges Hilfsmittel. Natürlich hilft es auch, wenn von den Frequenzkontrollbehörden weitere Kanäle zur Verfügung gestellt werden. Leider ist es ja so, dass Kanäle mit niedrigeren Frequenzen eine höhere Signalreichweite erlauben und vice versa bei Kanälen mit höheren Frequenzen. Dieser ewige Tradeoff wird auch in Zukunft bestehen, weil er eng mit den physikalischen Grundlagen verwoben ist. In Abbildung 16 zeigen wir, was passiert, wenn ein LTE-Versorgungsbereich mit vielen Small Cells angereichert wird.

Stationen, die den Bereich von Small Cells verlassen, brauchen jetzt keine Ansammlung kleiner Funklöcher zu erwarten. Duale Zellen-Konnektivität macht es möglich, einen stabilen Mobilbetrieb zu gewährleisten. Schon heute unterstützen alle modernen mobilen Endgeräte wenigstens 3G/LTE und WLAN und haben auch entsprechend unabhängige Transceiver. Ein kleines Protokoll genügt, um sie immer im Netz zu halten. (siehe Abbildung 17)

Was die Small Cells angeht, haben wir bei den LTE Entwicklern eine erhebliche Be-

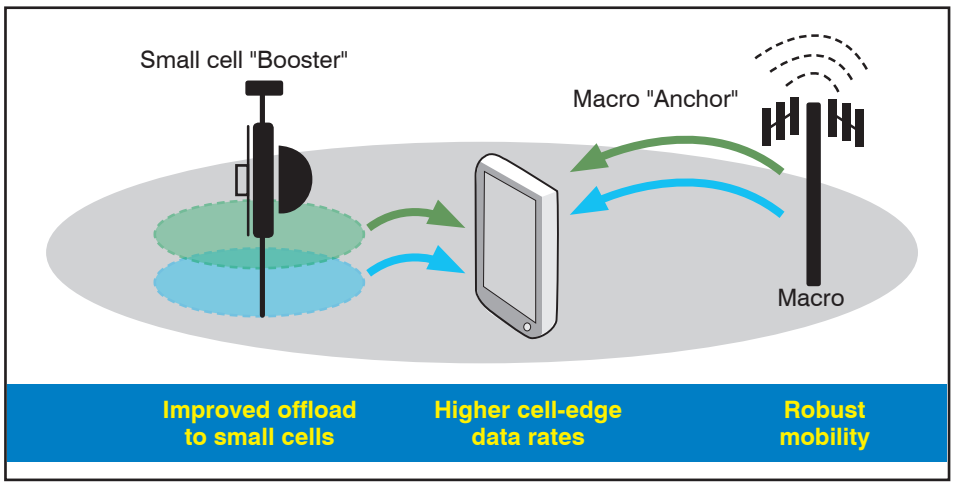


Abbildung 17: Multi-Flow: duale Zellen-Konnektivität über kleine Zellen sowie Makros und kleine Zellen Quelle: 3GPP

gehrlichkeit hinsichtlich der Erweiterung auf lizenzfreie Bänder. Der Funkraum in lizensierten Bereichen ist eigentlich immer zu klein und es gibt immer mehr Streit darum. Bei einer nicht lange zurück liegenden Versteigerung hat die US-FCC z.B. einem Unternehmen (Dish) Frequenzen verkauft, das dieses aber gar nicht nutzt, sondern hortet. Alle anderen Bieter haben sich daraufhin erheblich beschwert und das Verfahren muss nochmal neu aufgerollt werden. Die lizenzfreien Bereiche sind da schon sehr spannend und genau das ist in Zukunft ein wachsendes Problem für private Betreiber: es kann wenigstens innerhalb von Städten zu einem erheblichen Wettbewerb zwischen privaten WLANs und LTE-Verfahren kommen und ohne ein großer Prophet zu sein kann man absehen, dass dies Probleme für die privaten Betreiber darstellt. Sie müssen nämlich mit der nachrichtentechnischen Qualität, die LTE hat, auch auf ihrer Seite des lizenzfreien Bereichs mithalten. Und das wird alles andere als einfach. Zur Erweiterung von LTE auf neue Anwendungsbereiche haben wir schon genug gesagt, so dass wir uns jetzt die weitere Entwicklung genauer ansehen können.

2.2 LTE Rel. 13

Rel. 13 ist die Version, über die aktuell aktiv diskutiert wird. Nochmals zur Erinnerung: bei den Diskussionen, die wir hier betrachten, geht es um den Teil des Mobilfunknetzes, der auch als RAN (Radio Access Network) bezeichnet wird. Die Entwicklung des RANs liegt beim Gremium 3GPP. 3GPP erweitert die LTE-Plattform in Richtung neuer Services und höherer Leistung, um die zunehmenden Bedarfe der Mobil-Kommunikation abdecken zu können. Gleichzeitig arbeitet 3GPP aber auch an der nächsten Generation Mobilfunk (5G), die ca. ab 2020 kommen wird.

Das lizensierte Spektrum bleibt die erste Wahl für einen 3GPP-Betreiber, um den Kunden neue Dienstleistungen und ein verbessertes Benutzererlebnis zu liefern. Die zusätzliche Nutzung lizenzfreier Bereiche wird aber ein zunehmend wichtiges Element um auf den wachsenden Leistungshunger reagieren zu können. 3GPP-Betreiber haben letztlich zwei Möglichkeiten, lizenzfreie Bereiche zu nutzen:

- WiFi vermöge WiFi/LTE-Internetworking
- LTE im lizenzfreien Spektrum

Die Auswahl hängt von vielen verschiedenen Faktoren ab. Die Abbildung 18 zeigt die bisherige Entwicklung bei Zusammenwirken zwischen LTE und WiFi.

Das Framework wurde seit dem ersten LTE-Release entwickelt. Im Laufe der Zeit wurden immer engere Formen des Internetworkings hinzu genommen.

In Rel. 13 wird mit folgenden Methoden eine noch engere Kooperation definiert:

- Aggregation von WiFi und LTE Radio-Links
- Erweiterte, durch das Netzwerk kontrollierte Mobilität mittels erweiterter Netzwerk-Reporting-Verfahren z.B. mit Messungen des User Equipments und neuen Steuerungs-Möglichkeiten im Netz

Das Projekt studiert Themen von Änderungen in der Wellenform von LTE, um in lizenzfreien Bereichen arbeiten zu können, bis hin zu weitreichenden Diskussionen um Koexistenzfragen. Wesentliche Prioritäten sind hierbei:

- 5 GHz-Band
- Globale Lösung, die in unterschiedlichen Regionen mit unterschiedlichen Regularien arbeiten kann
- Licensed Assisted Access (LAA)-Betrieb
- Faire Koexistenz zwischen LTE, WiFi und unterschiedlichen LTE-Betreibern (kein Wort von privaten WiFi-Betreibern)

In der allgemeinen Diskussion gibt es zwei wichtige Alternativen: LAA und LTE-U (LTE unlicensed). Sie unterscheiden sich ganz erheblich im Umgang mit anderen, fremden Funksystemen in den lizenzfreien Bereichen. Die Abbildung 19 gibt einen kompakten Überblick.

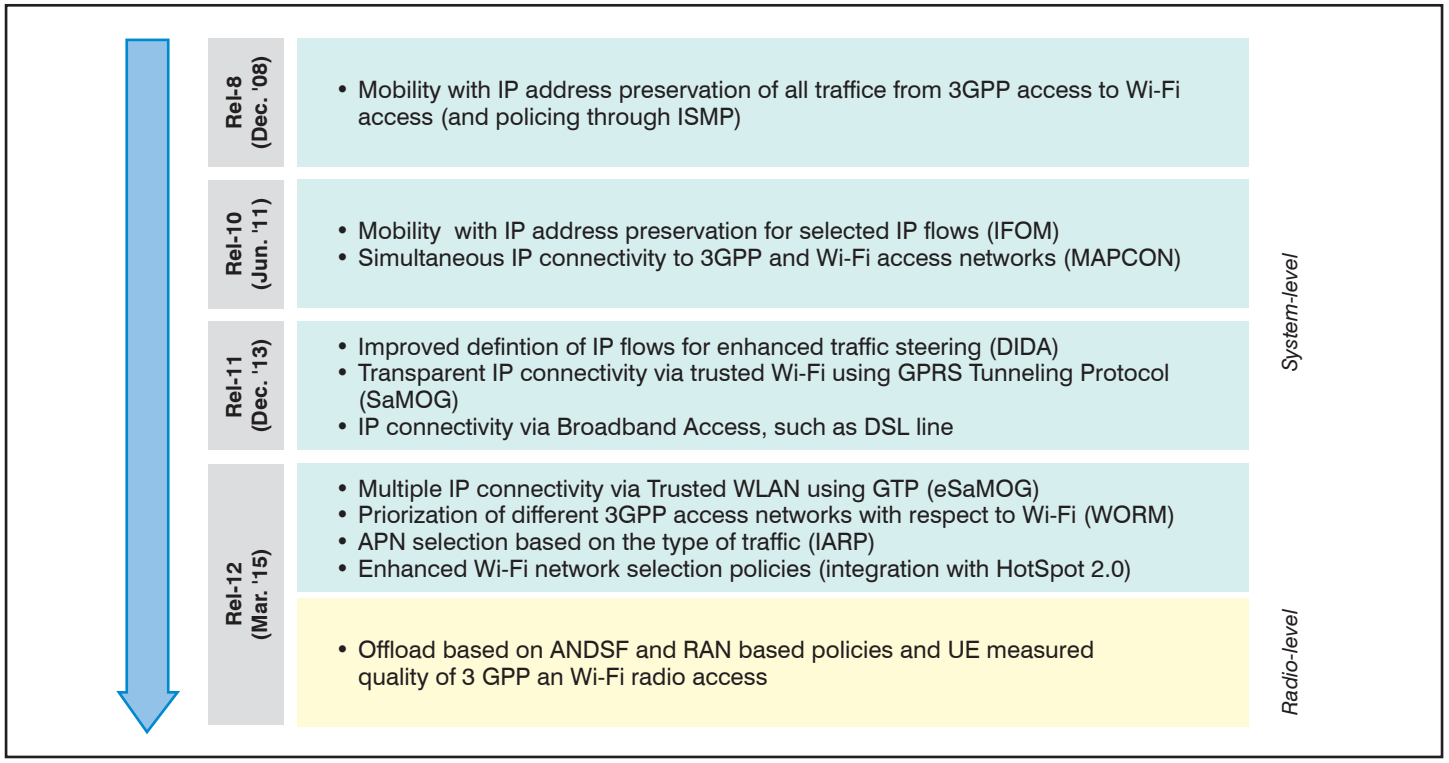


Abbildung 18: Kurze Historie des LTE/WiFi-Networkings Quelle: ATIS 5G Symposium, Juni 2015

Der wesentliche Punkt ist, dass LTE-U ohne die zurückhaltenden Steuerungsmechanismen arbeitet, die in LAA zu finden sind. Ganz grob kann man sagen, dass der Unterschied zwischen LTE-U und LAA in etwa so ist wie zwischen 802.11a und h. 11h wurde ja entworfen, um den Randbedingungen in der EU zu genügen. Deshalb können wir die Betrachtung von LTE-U hier direkt abkürzen, weil es in der EU keinen Einsatz finden wird. Außerdem ist es rein für den Downlink gedacht.

Wie sieht nun die Betriebsweise von LAA aus und wie ist die Fairness zu beurteilen? Die Basis von LAA ist die Aggregation einer primären Zelle, die in einem lizensierten Frequenzbereich arbeitet und hier sensible Informationen und Durchsetzung von Quality of Service behandelt, mit einer sekundären Zelle, die in einem lizenzfreien Bereich arbeitet und zur opportunistischen Leistungssteigerung genutzt wird. Die sekundäre Zelle kann so geschaltet werden, dass sie nur Downloads empfängt, aber auch so, dass sie Downloads und Uploads beherrscht. Das ist genau die Konfiguration, die man z.B. benötigt, um die Leistung von LTE auf relativ einfache Weise für den Download von Videos zu steigern. Ziel ist eine faire Koexistenz: LAA sollte die Qualität benachbarter WiFi-Dienste (Video, Daten und Sprache...) in den wesentlichen Parametern (Durchsatz, Latenz, Jitter...) nicht mehr behindern als ein anderes WiFi-Netzwerk auf dem gleichen Träger-Bereich. Die Funktionalitäten zu diesem Zweck sind:

- *Listen Before Talk* (LBT)
- Diskontinuierliche Übertragung mit begrenzter maximaler Übertragungsdauer auf einem Träger
- *Dynamic Frequency Selection* (DFS) zur Vermeidung von Interferenzen mit Radar in verschiedenen Regionen
- Carrier Selection
- *Transmit Power Control* (TPC)

Die diskontinuierliche Übertragung soll dazu dienen, dass LAA einen Kanal nicht völlig monopolisiert, alleine wird das aber nicht reichen, sondern es muss mit den entsprechenden protokollarischen Elementen von WiFi abgestimmt werden. Die Funktionen von LAA sollen aller Voraussicht nach für eine faire Koexistenz von WiFi und LAA sorgen. Allerdings gab es mittlerweile gemeinsame Sitzungen mit IEEE 802.11 und die sehen das naturgemäß völlig anders. Zu einen gibt es schon eine Reihe von Funktionen in der Standardisierung, die die friedliche und halbwegs faire Koexistenz unterschiedlicher WLAN-Systeme (unterschiedliche Generationen und Ausbaugrade) in den lizenzfreien Bändern sichern sollen. Auch

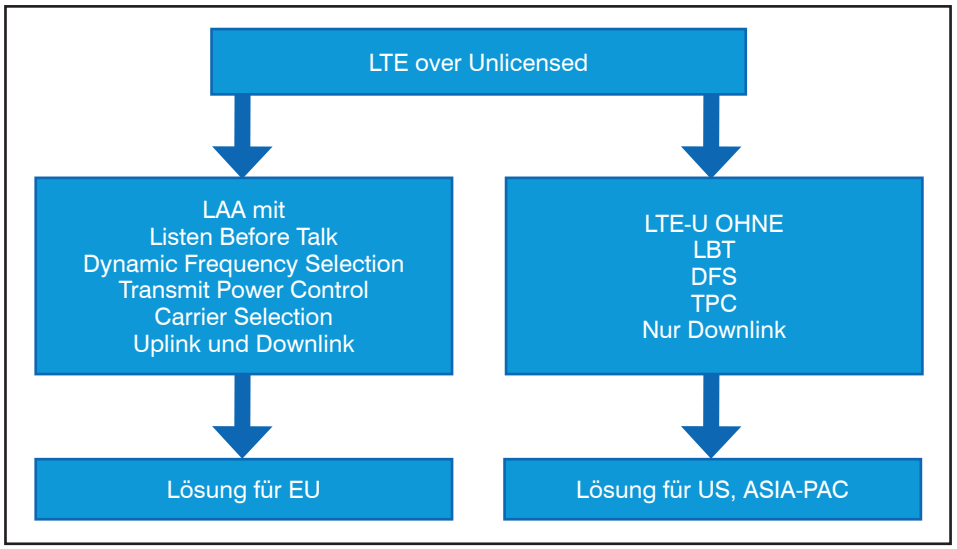


Abbildung 19: LTE over Unlicensed, LAA oder LTE-U?

wenn wir uns in der Vergangenheit wenig darum gekümmert haben, ist dies doch ein recht umfangreiches Werk. Mancher wird sich sicherlich noch an die frühen Versionen IEEE 802.11b und g erinnern und auch an die Empfehlung, bloß keinen Mischbetrieb zu machen. Messungen haben gezeigt, dass der Mischbetrieb nicht wie man eigentlich erwartet hätte, eine Zellenleistung „zwischen" der jeweiligen Nominal-Leistung von b und g ergibt, sondern meist deutlich schlechter als b alleine ist.

Heute wäre es unrealistisch, einen Mischbetrieb zu untersagen. Es sind nicht nur Endgeräte mit Transceivern nach unterschiedlichen Standard-Versionen (z.B. n und ac) unterwegs, sondern auch noch mit unterschiedlichen Qualitätsstufen hinsichtlich der Signalqualität, siehe dazu die Diskussion um Filter und Verstärker. Natürlich hat ein aktuelles iPhone6 eine deutlich bessere Signalverarbeitung als ein sagen wir vier Jahre altes Notebook in der gleichen Zelle.

Das Meiste lässt sich aber in dem Zusammenhang dadurch regeln, dass die Systeme nach IEEE 802.11 grundsätzlich das gleiche Steuerungsverfahren für den Medienzugriff verwenden, eben das von CSMA/CA abgeleitete DCF. Das ist zwar ziemlich schlecht, aber immerhin in allen Varianten prinzipiell gleich, eben stochastischer nicht-deterministischer wechselseitig ausgeschlossener Medienzugriff. Auch diese Kompatibilität hat für das Überleben von DCF gesorgt, obwohl es immer wieder bessere Verfahren in der Diskussion um eine neue Variante gegeben hat.

Möchte man aber LTE und WiFi in den gleichen lizenzfreien Bereichen verwenden, ergibt sich ein echter Kulturschock! LTE ist wie beschrieben ein völlig geordnetes System mit deterministischem Mehrfachzugriff durch prinzipiellen Zeitmultiplex mit ggf. überlagertem Raum-Multiplex. Zur Erläuterung nur ein kleines Beispiel: zwischen zwei aufeinanderfolgenden Paketen im WiFi-Netz unter DCF entstehen sehr unterschiedliche „Pausen", deren Länge davon abhängt, wie gut das nachfolgende Paket durch den Verkehr gekommen ist, um es einfach auszudrücken. Und das hängt wiederum von vielen Parametern wie der Gesamtlast, der Anzahl der Stationen, der mittleren Paketlänge und vielen anderen fast bis hin zum Cola-Preis in Papua-Neuguinea ab. MAC und Puffer sorgen dafür, dass die WiFi-Kommunikation dennoch funktioniert (einigermaßen). Das hört sich nachteilig an, ist es aber nicht immer. Bei wenigen Teilnehmern und anderen günstigen Bedingungen kann ein solches Verfahren eine hohe Leistung erzielen. Außerdem kommt DCF prinzipiell ohne zentrale Steuerung aus.

LTE-Pakete hingegen unterliegen einer genau definierten deterministischen Abfolge. Es gibt einen sehr genauen Zeitrahmen, in dem sie abgearbeitet werden. Das kommt daher, dass LTE natürlich trotz aller Weiterentwicklungen grundsätzlich der Telefontechnik entstammt, bei der Varianzen zwischen den Paketen, die ja Teile der Sprachinformation enthalten, zu als unangenehm empfundenen Störungen der Sprachqualität führen. Jetzt soll LAA plötzlich Listen before Talk beinhalten. Das ist dem LTE Datenfluss völlig fremd und eigentlich ziemlicher Sand im Getriebe. Wie soll LTE damit umgehen? Wahrscheinlich ist, dass aufgrund der Profile der Anwendungen entschieden wird, was

über welches Medium laufen soll. LAA stellt ja immer eine Kopplung zwischen einer Zelle im lizensierten Spektrum und einer Zelle im unlizensierten Spektrum dar. Nur im letzten Fall kann es zu Problemen kommen. Also könnte man den ziemlich unempfindlichen Video-Offload in die unlizensierte Zelle verlegen, die Sprachkommunikation aber im üblichen Bereich belassen.

Es gab schon eine Sitzung mit Teilnehmern von IEEE 802.11 und 3GPP. Blickt man die Unterlagen durch, gibt es oberflächlich freundlich geschleimte Absichtserklärungen, hinter denen bei IEEE das blanke Entsetzen versteckt ist. Denn *Simulationen und Berechnungen haben bereits gezeigt, dass der gleichzeitige Betrieb eines nicht-deterministischen freilaufenden Systems wie WiFi und eines deterministisch mit Zeit- und ggf. Raum-Multiplex gesteuerten Systems wie LTE zu grauenhaften Performance-Ergebnissen für beide führen.*

Ich kann das hier beim besten Willen nicht weiter ausführen, wer das aber spannend findet, sollte sich die IEEE Dokumentation IEEE 802.19-14/0080r2 von Herrn Nikolich ansehen, wo unter dem Titel „Coexistence Lessons Learned“ auch um Koexistenzfragen geht, die IEEE bislang schon lösen konnte.

Bei LTE-U sei noch erwähnt, dass die FCC Mitte 2015 Hersteller und Betreiber nach ihrer Position zu diesem Punkt gefragt hat, einfach weil eine erhebliche Unsicherheit besteht. Die Antworten:

- AT&T: grundsätzlich positiv, es ist aber mehr Normung nötig
- Google: eher negativ, mögliche WiFi-Degradation
- Ruckus: drückt starke Bedenken aus, deutliche WiFi-Degradation
- Cablevision: „die Befürworter von LAA/LTE-U zerstören die historische gesunde Dynamik der unlizensierten Bänder“ verlangt Schutz von Verbrauchern und Wettbewerbern
- Verizon: „das ist eine wichtige Technologie um den raketenartig nach oben schießenden Bedarf der Nutzer befriedigen zu können“

Weniger Einigkeit geht kaum. Alle diese Unternehmen beschäftigen jeweils ein Heer teurer Spezialisten. Diese haben offensichtlich noch keinen wissenschaftlich abgesicherten Standpunkt.

Die Arbeit von 3GPP ist mit der Diskussion um lizenzfreie Bereiche aber längst nicht abgeschlossen. Hier noch einige interessante Arbeitsbereiche in Stichworten.

Hinsichtlich der Funkübertragungstechnik gibt es Erweiterungen des Signalisierungs-Frameworks für die LTE Carrier Aggregation (CA). Das erlaubt jetzt bis zu 32 Einzel-Träger, was einer erheblichen Erweiterung der Möglichkeiten vor allem im Hinblick auf hohe Datenraten darstellt und auch nützlich für den LAA-Betrieb in unlizensierten Bereichen mit breiteren Blöcken freier Frequenzen ist. Projekte eruieren die Machbarkeit und mögliche Wirkung von sog. volldimensionalem MIMO und Beamforming mit zweidimensionalen Antennen-Arrays mit bis zu 64 MIMO-Kanälen. Schließlich arbeitet man an Downlink Multi-User-Transmission mit Superpositions-Codierung (ganz grob eine theoretisch fundierte Erweiterung von MU-MIMO).

Ein weiterer, wichtiger Arbeitsbereich von 3GPP ist die Unterstützung der Kommunikation im IoT. Aufbauend auf den Grundlagen in LTE R12 gibt es zusätzliche LTE-Erweiterungen für maschinen-basierte Kommunikation. Eine neue User Equipment Category (0) unterstützt eine 1,4 MHz Schmalband-Betriebsweise. Sie ist durchaus für das Multiplexing mit anderen Strömen in breiteren Kanälen geeignet. Insgesamt sind die LTE-Verfahren in ihrer vollen technologischen Breite viel zu komplex für bestimmte Kommunikationsanwendungen im IoT. Deshalb gibt es die Entwicklung eines völlig neuen Radioteils für Low-End IoT- Anwendungen mit nur begrenzter Mobilitätsunterstützung, rund 100 bps auf 200 kHz-Bändern sowie höherer Reichweite (20 dB besseres Link-Budget verglichen mit GPRS), sehr geringen Kosten und minimalem Leistungsbedarf.

Weitere Arbeitsbereiche sind:

- Indoor Positionierung. Die FCC hat gefordert, die Genauigkeit der Indoor-Positionierung zu verbessern, z.B. um bei Notrufen besser reagieren zu können.
- Single Cell Point-to-Multipoint. Evaluierung möglicher Vorteile der Nutzung des gemultiplexten LTE-Downlink-Kanals für SC-PtM.
- Low Latency LTE. Untersuchung der Möglichkeiten der Straffung von Protokoll-Elementen und Optimierung der Verarbeitung zur Realisierung kürzerer Latenz-Zeiten für die Realisierung einer besseren Benutzer-Erfahrung. Erste Ergebnisse werden allerdings erst für R14 erwartet.

Ewig wird die Standardisierung von 4G nicht „halten“, denn schon Ende 2015 beginnen die Arbeiten am Mobilfunk der 5. Generation, der ab 2020 kommen wird. (siehe Abbildung 20)

2.3 MuLTEfire: LTE-ähnliche Leistung mit WiFi Betriebsaufwand

Abschließend wollen wir noch auf eine andere Entwicklung eingehen, die aktu-

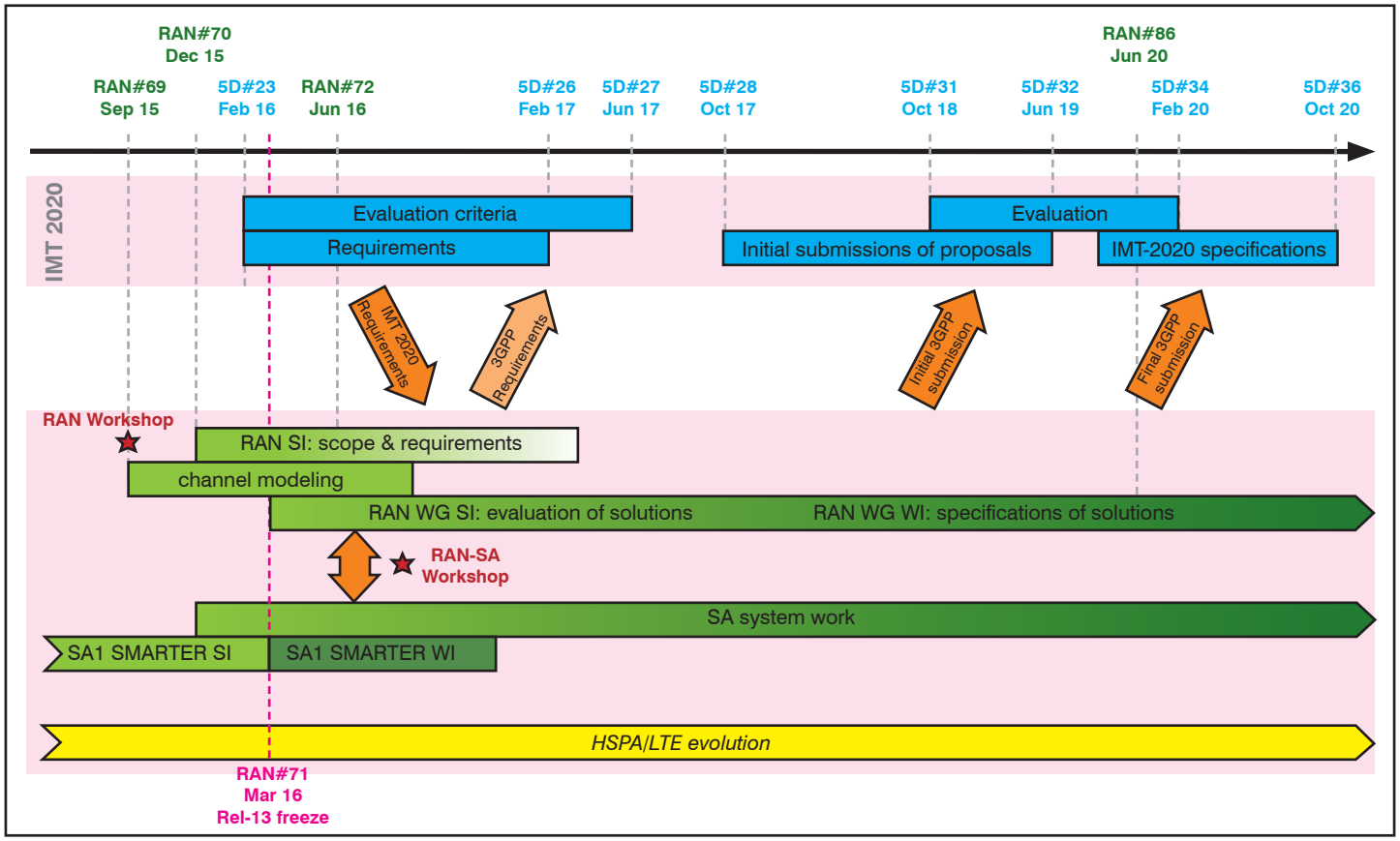


Abbildung 20: 5G Timeline

ell noch sehr frisch ist, aber durchaus das Potential hat, unser gesamtes Verständnis privat betriebener drahtloser Infrastrukturen auf den Kopf zu stellen: MuLTEfire !

Kurz gesagt ist MuLTEfire die mögliche Antwort privater Betreiber darauf, dass LTE-Provider in die unlizensierten Bereiche vordringen. Es handelt sich dabei um eine LTE-basierte Technologie, die ausschließlich in unlizensierten Bereichen arbeitet, ohne einen „Anker“ in einem lizensierten Bereich haben zu müssen. Mögliche Nutzer wären Internet Service Provider und vor allem Betreiber privater Netze (Unternehmen, Behörden). Wir haben die Kombination der technischen Vorzüge von LTE (Kapazität, Reichweite, Mobilität, Qualität, Stabilität) mit der Einfachheit der Installation von WiFi-Netzen.

Signalisierung und Kanalbildung sind wie bei LTE verbunden mit der Nutzung der Möglichkeiten zur Selbstorganisation in neuen LTE Varianten für hochdichte Installationen. Angestrebt ist auch eine„Gute Nachbarschaft“ zu bestehenden WiFi- und neuen LTE-U und LAA. Tatsache ist aber, dass MuLTEfire genau das Problem aus dem Weg räumen könnte, was vorhin angesprochen wurde: die fürchterlichen Folgen der Koexistenz eines Systems mit einer nicht-deterministischen freilaufenden Steuerung wie DCF und eines Zeit- und Raum-Multiplex-Systems mit höchst deterministischer Steuerung wie LTE in einem Funkbereich. Die friedliche Koexistenz eines Provider-LTE-Systems mit einem MuLTEfire-System in einem lizenzfreien Bereich wäre vergleichsweise leicht herzustellen. Aber auch in reinen Indoor-Bereichen ohne jede Interferenz mit einem öffentlichen Mobilfunkangebot wäre MuLTEfire eine den üblichen WLANs in jeder Hinsicht deutlich überlegene Technologie. Mögliche Nutzungen z.B. in Unternehmen wäre die Ausdehnung bestehender Systeme hinsichtlich zusätzlicher physikalischer Lokationen oder neuer Teilnehmer, die hochqualitative Versorgung nomadischer Teilnehmer ohne Abo oder SIM-Karte und natürlich die Möglichkeit der einfachen Zusammenarbeit mit mobilen Netzen zur Verbesserung des Data Offloads (mit SIM). Die gesamte Entwicklung liegt beim Chip-Hersteller Qualcomm, ein Standard ist aktuell nicht in Sicht. Wir müssen hier einfach abwarten, was Komponenten-Hersteller wie Cisco, HP oder Innovatoren wie Ruckus zu dieser neuen Alternative sagen. Rein technisch ist sie von Beginn an den 802.11-WLANs deutlich überlegen. Die Erfahrung der letzten Jahrzehnte hat aber leider gezeigt, dass das nicht immer nützt.

3. Konsequenzen für privat betriebene drahtlose Netze

Ob nun der „wireless Leistungshunger“ in einer Kombination aus Steigerung der Anzahl der mobilen Geräte und der individuell von ihnen verlangten Leistung in flächendeckenden Infrastrukturen in den nächsten Jahren tatsächlich den Faktor 1000 erreicht, wie es nicht nur der Hersteller Qualcomm verkündet, sei dahingestellt. Die ersten Planungen für 5G gehen aber ebenfalls von dieser Dimension aus. Innerhalb privater Netze herrschen jedoch etwas andere Bedingungen, so wird sicher kein Unternehmen Video-Streaming im gleichen Umfang unterstützen müssen wie Provider mit überwiegend privaten Endanwendern. Vielmehr ist zu erwarten, dass Lösungen nach wie vor primär die durch die im Unternehmen vorhandenen „wertschöpfenden“ Prozesse angemessen unterstützen müssen, wobei neue kooperative Anwendungen, wie sie z.B. IBM und Apple entwickeln sowie ein geändertes Verständnis von Unified Communications wesentliche Impulse setzen werden. Aber, da sich aktuell keine am Bedarf professioneller Anwender orientierte Video-Plattform durchsetzen konnte, kann man YouTube wohl vielfach in Zukunft in Unternehmen und Organsationen nicht so einfach sperren wie Netflix.

Wireless Trends: LTE-Entwicklungen und Konsequenzen für die Betreiber privater Wireless Infrastrukturen

Um es kurz zu machen: der Bedarf wird massiv wachsen, wie stark genau, hängt vom Einzelfall ab.

Wie können wir die beschriebenen Technologien in diesem Zusammenhang bewerten?

IEEE 802.11ac erreicht mit **Wave2** endlich professionelles Niveau. Es ist sicherlich die für die meisten privaten Betreiber die erste Wahl. Investitionen in Wave1 oder gar 11n lohnen sich nicht mehr, wenn Wave2 kommt. Alle wichtigen Hersteller unterstützen diesen Standard. Man wird mehr Zellen benötigen als bei 11n, wenn man eine wirkliche Leistungssteigerung sehen möchte. Die bisher erfahrenen Planer werden auch das bravourös bewältigen. Durch die neuen Ethernet-Standards mit 2,5 und 5 Gbps bekommen wir auch rechtzeitig die Geräte für den preiswerten Aufbau einer Infrastruktur für die Vernetzung der vielen APs. Auch hier wird es bald eine hinreichende Auswahl geben. Welchem Hersteller man letztlich den Vorzug gibt, hängt nicht von den genannten Übertragungstechnologien ab, sondern von Qualität und Funktionsumfang der betrieblichen Lösung sowie der Sicherheitsmaßnahmen. Nur hier können sich die Hersteller ja wirklich unterschieden und jeder private Betreiber sollte sich natürlich hier wirklich genau überlegen, was er einsetzen möchte.

Die persönliche Meinung des Autors ist, dass solchen Konzepten, wie sie von Meraki (gehört jetzt Cisco) entworfen wurden, die Zukunft gehört: Steuerung der wireless Infrastruktur aus einer nicht nur hinsichtlich der Anzahl zu versorgender Endgeräte sondern auch der Funktionen in Automation, Orchestrierung und Sicherheit massiv skalierbaren Cloud.

IEEE 802.11ad. Dieser seit einigen Jahren verabschiedete Standard für die Bildung höchst leistungsfähiger WLANs im Millimeterwellen-Bereich (60 GHz) schien schon fast vergessen. Auf der Consumer Electronic Show CES Anfang Januar wurde nicht nur von ACER das erste 11ad Notebook vorgestellt, sondern auch ein 11ad-Router von TP-Link. Der Talon AD7200 schafft nach Angaben des Herstellers einen Durchsatz von bis zu 7,2 Gbit/s. in Kombination von 60 GHz mit 5 und 2,4 GHz-Bändern. Das ist realistisch. 11ad arbeitet nur auf recht kurzen Distanzen, für multiple 4K-UHD-Versorgung im Wohnzimmer sollte es aber reichen.

LTE-U und LAA. Sollte tatsächlich LTE in unlizensierten Bereichen kommen, müssen sich viele private Betreiber sehr warm anziehen. Aus einer 50-jährigen Erfahrung mit Funkübertragungssystemen neigt der Autor der Fraktion zu, die eine erhebliche Degradation der WiFi-Services befürchtet. Populär: treffen sich LTE und WiFi in einem Frequenzbereich, wird WiFi platt wie Flunder. Das liegt einfach daran, dass WiFi durch und durch eine Billig-Technologie ist und es ein Wunder wie bei „My Fair Lady“ (oder „Pretty Woman“) bei WiFi nicht gibt. Man könnte auch sagen: man bekommt WiFi aus der Gosse, aber die Gosse nie aus WiFi! So oder so sollten private Betreiber aber immer die funktechnisch möglichst beste Produktstufe installieren, und das wäre aktuell 802.11ac Wave2.

MuLTEfire. Natürlich wäre es schön, wenn private Betreiber endlich eine sinnvolle Alternative zu WiFi bekommen könnten, die wenigstens zu einem guten Teil dem aktuellen Stand der seriösen Funktechnik entspricht. Leider müssen wir es abwarten.

Neue Anforderungen: neue Technologien Neue Lösungsmöglichkeiten: neue Diskussionen! Bleiben Sie dabei.

Standpunkt

Wenn Sicherheitskomponenten unsicher sind

Der Standpunkt von Dr. Simon Hoff 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.

Firewalls bilden einen wesentlichen Eckpfeiler unserer technischen Infrastruktur der Informationssicherheit und haben sich als Standardwerkzeug zur sicherheitstechnischen Segmentierung von Netzen seit Jahren etabliert:

- Firewalls kontrollieren und steuern Kommunikationsverkehr zwischen Netzen, blockieren und protokollieren nicht erlaubte Kommunikationsversuche.
- Firewalls enthalten oft eine VPN-Gateway-Funktion, d.h. sie bilden Verschlüsselungsendpunkte für SSL VPN oder IPsec VPN.
- Moderne Firewalls enthalten zusätzlich ein Intrusion Prevention System (IPS) zur Erkennung und Blockierung von Anomalien (inklusive Angriffsmustern). Zusätzlich erlauben Next Generation Firewalls eine anwendungs- und identitätsbasierte Filterung der Kommunikation, inklusive SSL-Inspection zur Analyse verschlüsselter Kommunikation.
- Proxies und Gateways (z.B. für Web-Verkehr) und weitere Funktionen wie z.B. Data Loss Prevention (DLP) können auch in Firewalls implementiert werden.

An die Sicherheit einer Firewall werden selbstverständlich hohe Anforderungen gestellt, um Netze mit unterschiedlichem Sicherheitsniveau (z.B. Internet und interne Netze) zu verbinden. Jedoch ist eine Firewall eigentlich nichts anderes als ein normaler Computer, der für einen speziellen Einsatzbereich gebaut und optimiert ist. Mit anderen Worten: In Firewalls wird mit dem ganz normalen Wasser der IT gekocht. In Folge finden sich grundsätzlich alle Bereiche mit potentiellen Schwachstellen von Computern (Anwendungen, Betriebssystem, Protokoll-Stacks und Schnittstellen, Administration) natürlich auch in Firewalls. Es sind also beispielsweise auch Viren, Trojaner und andere Schadsoftware in Firewalls theoretisch denkbar.

Daher wird vom Hersteller eines solchen Systems nicht nur erwartet, dass eine sehr hohe Softwarequalität vorliegt (denn Fehler in Software lassen sich immer wieder für Angriffe ausnutzen). Außerdem muss der Hersteller systematisch für die Vermeidung von Schwachstellen und die Systemhärtung Sorge tragen, d.h. Informationssicherheit muss integraler Bestandteil der gesamten Systementwicklung sein, d.h. in Entwurf, Programmierung, Integration und Maintenance angemessen berücksichtigt werden.

Nicht umsonst fordert man schon seit geraumer Zeit gerne in Ausschreibungen von Firewalls und allgemein von Sicherheitskomponenten einen entsprechenden Nachweis über eine Zertifizierung nach Common Criteria [1] und dies oft mit dem schon recht hohen Evaluation Assurance Level (EAL) 4+.

Umso erschreckender sind auf den ersten Blick die Nachrichten gewesen, die wenige Tage vor Weihnachten im letzten Jahr die Runde gemacht haben: Bei einem internen Code Review ist dem Hersteller Juniper Networks im Firewall-Betriebssystem ScreenOS nicht autorisierter Code (sprich: Schadcode) aufgefallen, über den von einem Angreifer VPN-Verbindungen per SSH-Hintertür [2] belauscht werden können. Ein Trojaner im vom Hersteller ausgelieferten Code einer Sicherheitskomponente (insbesondere, wenn die Sicherheitskomponente Verschlüsselungsendpunkte enthält) gehört zu den schlimmsten denkbaren Schwachstellen einer Sicherheitskomponente, die, sobald sie aktiv durch einen Angreifer ausgenutzt wird, sehr schnell zu einem unter Umständen katastrophalen Sicherheitsvorfall führen kann. Es kam dummerweise noch schlimmer: Ein paar Tage vor Weihnachten ist herausgekommen, dass für die Nutzung der SSH-Hintertür ein bereits bekanntes Master-Passwort ausreicht [3].

Beim Firewall-Hersteller Fortinet ist kürzlich ebenfalls eine sehr unangenehme Schwachstelle aufgefallen. Es gibt für ältere Versionen (betroffen sind Versionen von Ende 2012 bis Mitte 2014) des Betriebssystems FortiOS einen (bis dato unbekannten) SSH-Zugang mit statischem Passwort über den die volle administrative Kontrolle des Systems von außen möglich ist [4]. Seit Juli 2014 gibt es zwar einen entsprechenden Patch, interessant ist jedoch die Frage, wie viele produktive Systeme noch mit einer alten Software ohne Patch laufen, zudem inzwischen auch ein entsprechender Exploit öffentlich verfügbar ist [5].

Hätten solche Dinge nicht schon viel früher auffallen müssen (insbesondere im Rahmen einer Common-Criteria-Zertifizierung, der sich ja die meisten Firewall-Hersteller für ihre Produkte unterziehen)? Die Komplexität der Systeme scheint so groß geworden zu sein, dass regelmäßige Code Reviews nicht mehr die notwendige Tiefe erreichen bzw. tiefgehende Reviews nur noch auf Stichprobenbasis durchgeführt können. Außerdem sind Common-Criteria-Zertifizierungen aufwendig und kosten Zeit.

Die beschriebenen Probleme sind nicht auf Firewalls beschränkt, wie z.B. jüngst aufgefallene Schwachstellen im Passwort-Manager von Trend Micro gezeigt haben [6].

Was können wir als Nutzer von Sicherheitskomponenten angesichts solcher unangenehmen Sicherheitsprobleme tun?

1. Zunächst schadet ein gesundes Misstrauen den Herstellern gegenüber nicht.
2. Trotz aller Nachteile, eine Zertifizierung nach Common Criteria bleibt ein wichtiges Instrument, das bei Ausschreibungen berücksichtigt werden sollte. Allerdings muss man sich der Grenzen eines solchen Zertifikats bewusst sein.
3. Aufnahme weitergehender Sicherheitsanforderungen in Ausschreibungen, z.B. die Bestätigung, dass keine SSH-Hintertüren implementiert werden bzw. zum Ausschreibungszeitpunkt bekannt sind,

der Hersteller in seinen Prozessen systematisch solche Schwachstellen vermeidet bzw. danach sucht und entsprechende Feststellungen zeitnah veröffentlicht.

4. Verstärkte Überwachung von Sicherheitskomponenten wie Firewalls

5. Zusätzliche, eigene Härtung der Sicherheitskomponenten (z.B. konsequente Anwendung der entsprechenden Bausteine der BSI IT-Grundschutz-Kataloge und weiterer Empfehlungen des BSI)

6. Strenges Schwachstellenmanagement / Vulnerability Management für Sicherheitskomponenten und Optimierung der Prozessdurchlaufzeiten von Meldung einer Schwachstelle bis zur Behandlung bzw. bis zum Patch des Systems

7. Optimierung des Prozesses zur Behandlung von Sicherheitsvorfällen (z.B. besondere Priorisierung für Sicherheitskomponenten und strengere Zeitvorgaben für die Bearbeitung des Vorfalls)

Trotzdem, richtig zufriedenstellend ist das nicht. Eigentlich wäre es wünschenswert, eine viel strengere Prüfung als bei einer typischen Common-Criteria-Zertifizierung zu haben. Sicherheitskomponenten müssten eigentlich auf Herz und Nieren unter vollständiger Offenlegung der gesamten Spezifikationen, Quelltexte und aller Entwicklungs- und sonstiger produktbezogener Prozesse (z.B. Wartung, Lieferung) geprüft werden. Dies müsste strenggenommen dann zumindest in einem gewissen Umfang auch für jeden Patch erfolgen. Natürlich müsste der Hersteller dann auch nachweisen, wie er die Integrität des gelieferten Produkts sicherstellt (dann wäre das oben beschriebene Problem der Schadsoftware in einer Firewall erst gar nicht aufgetreten bzw. zumindest nicht erst nach Jahren aufgefallen).

Nur, wer könnte das bezahlen?

Die Kosten würden natürlich auf die Nutzer umgelegt. Außerdem würde es für den Hersteller bedeuten, der jeweiligen Zertifizierungsstelle praktisch das gesamte Produkt-Know-How offenzulegen. So etwas mag für Sicherheitskomponenten, über die Verschlusssachen z.B. im militärischen Bereich kommuniziert werden, vielleicht noch möglich sein, für den Bereich der normalen IT jedoch eher nicht. Es wird also auf einen Kompromiss hinauslaufen. Natürlich wäre es trotzdem wünschenswert, wenn wir künftig ein Prüfsiegel „geprüfte Informationssicherheit“ hätten, das über Common Criteria hinaus geht und trotzdem bezahlbar bleibt.

Bis dahin hilft es nichts: Wir müssen uns der Tatsache stärker bewusst werden, dass wir alle in der IT (inklusive der Hersteller von Sicherheitskomponenten) mit demselben Wasser kochen. Wäre es dazu nicht eine Idee als gute Vorsätze für das neue IT-Jahr die Verbesserung des eigenen Managements von Schwachstellen und Sicherheitsvorfällen ins Auge zu fassen (und dies auch konsequent umzusetzen)? Hierzu sei abschließend darauf hingewiesen, dass die Allianz für Cyber-Sicherheit für das erste Quartal 2016 als besonders wichtiges Thema den Bereich der Behandlung von Sicherheitsvorfällen (inklusive Cyber-Angriffe) auf die eigene Agenda gesetzt hat [7].

Verweise

[1] **Siehe http://www.commoncriteriaportal.org/**

[2] **Siehe http://forums.juniper.net/t5/Security-Incident-Response/Important-Announcement-about-ScreenOS/ba-p/285554**

[3] **Siehe http://www.heise.de/security/meldung/Exploits-fuer-SSH-Backdoor-in-Junipers-Netzgeraeten-3054308.html**

[4] **Siehe https://www.fortiguard.com/advisory/fortios-ssh-undocumented-interactive-login-vulnerability**

[5] **Siehe http://seclists.org/fulldisclosure/2016/Jan/26**

[6] **Siehe http://www.heise.de/security/meldung/Schwere-Sicherheitsluecken-im-Passwort-Manager-von-Trend-Micro-3069140.html**

[7] **Siehe https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/infos/20160106_quartalsthema.html**

Aktuelle Sonderveranstaltung

Das PSTN stirbt: Die neue Kommunikation mit SIP/IP 08.03.16 in Bonn

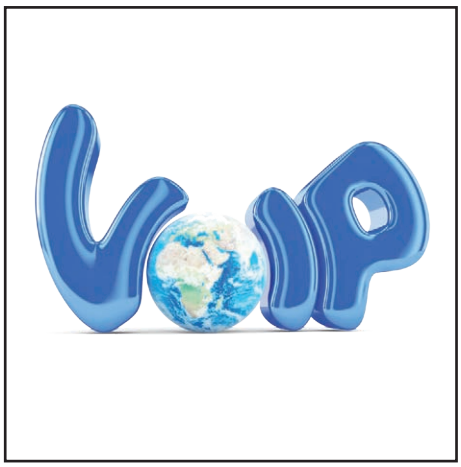
Die ComConsult Akademie veranstaltet am 08.03.16 ihre Sonderveranstaltung "Das PSTN stirbt: Die neue Kommunikation mit SIP/IP" in Bonn.

Die Deutsche Telekom hat angekündigt, bis 2018 das klassische PSTN-Netz, respektive analoge und ISDN-Anschlüsse abzuschalten. Dies betrifft alle Unternehmen, die weltweit kommunizieren wollen und müssen.

Abgesehen von den rein technischen Unterschieden: Leitungsvermittlung vs. Paketvermittlung, E.164 Telefonnummer vs. URI gibt es erhebliche funktionale Unterschiede, denn das Dienstspektrum bei All-IP wird erheblich umfangreicher sein als es im PSTN jemals der Fall war.

Soll sich eine globale SIP / All-IP Kommunikation auf breiter Ebene etablieren, muss dies auf der Basis von genormten oder de facto Standards erfolgen. Hierfür gibt es sowohl bei ECMA als auch dem SIP Forum Ansätze. Welcher hat das größte Marktpotenzial? Gibt es Zertifizierungsmöglichkeiten? Wie sieht die aktuelle Praxis aus?

Die Perimeter-Anschaltung des SIP/All-IP Trunks zwischen Enterprise und Provider wird heute typischerweise mit einem SBC realisiert. Wir analysieren, wie



die Anschaltung aussieht, welche Funktionalität von einer solchen Komponente erwartet werden sollte und wie sich der SBC-Markt präsentiert.

Im Rahmen der Veranstaltung analysieren wir, wie der Wechsel von PSTN auf All-IP im Unternehmen verläuft. Wir zeigen auf, welche Funktionalität heute erreicht werden kann und mit welchem Aufwand für Anpassung und Fehlersuche zu rechnen ist. Wie gut ist die Unterstützung durch den Enterprise-Hersteller und Provider? Wie ändert sich Betriebs- und Kostenaufwand?

Nicht nur klassische PSTN-Provider werden diesen Markt unter sich aufteilen, sondern auch Kabelnetzbetreiber, Mobilfunkanbieter und ISPs werden ihr Dienstspektrum auf den All-IP Kommunikationsmarkt ausdehnen. Wir analysieren, wie das aktuelle Angebotsspektrum aussieht und welche Roadmap erkennbar ist.

Für die Provider ist All-IP kein Neuland, aber dennoch ein Technologiewechsel mit großen Herausforderungen. Wir diskutieren, welche Anforderungen ein Provider an den Enterprise-Kunden stellt, wie SLAs gestaltet werden können, wie ein typischer Projektablauf aussieht und mit welchen Problemen zu rechnen ist.

Der Ersatz von E.164 durch All-IP muss zu einer neuen globalen Kommunikations-Architektur führen. Stand heute gibt es kein einheitliches, standardisiertes SIP-Interconnect zum Provider-Peering oder als Meta-Ebene. Wir zeigen die aktuellen Standardisierungs-Vorschläge, Möglichkeiten und Trends auf, über die die Provider diskutieren.

Diese Sonderveranstaltung analysiert, wie der Wechsel von PSTN auf All-IP im Unternehmen verläuft. Sie zeigt auf, welche Funktionalität heute erreicht werden kann und mit welchem Aufwand für Anpassung und Fehlersuche zu rechnen ist.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

Das PSTN stirbt:
Die neue Kommunikation mit SIP/IP

Ich buche das Seminar
Das PSTN stirbt:
Die neue Kommunikation mit SIP/IP

☐ 08.03.2016 in Bonn
zum Preis von € 1.090,-- 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

Zweitthema

Session Border Controller:

Die Perimeter-Komponente für All-IP

Fortsetzung von Seite 1

Dipl.-Inform. Petra Borowka-Gatzweiler leitet das Planungsbüro UBN und gehört zu den führenden deutschen Beratern für Kommunikationstechnik. Sie verfügt über langjährige erfolgreiche Praxiserfahrung bei der Planung und Realisierung von Netzwerk-Lösungen und ist seit vielen Jahren Referentin der ComConsult Akademie. Ihre Kenntnisse, internationale Veröffentlichungen, Arbeiten und Praxisorientierung sowie herstellerunabhängige Position sind international anerkannt.

Grundsätzliche Redundanz-Szenarien für HA oder UHA Session Border Controller wurden bereits in Teil 1 dargestellt. Aber welche Redundanzfunktionen werden hierbei für den SBC erwartet? Die schlichte Dopplung des SBC reicht klarerweise nicht aus, es bedarf eines Cluster- oder Redundanz-Protokolls mit Heartbeat zur automatischen Fehlerumschaltung bei Ausfall des aktiven SBC sowie eines Zustandsabgleichs für die jeweils laufenen Sessions: Die Umschaltung muss state-aware sein, der Backup SBC muss alle Zustandsinformationen über laufende Sessions vom aktiven SBC gespiegelt haben. Falls eine aktiv/aktiv Redundanz gefahren wird, müssen beide aktive SBCs einen Zustandsabgleich mit dem jeweils anderen SBC handhaben. Das genutzte Synchronisierungsprotokoll kann herstellerspezifisch oder standardisiert sein wie z.B. VRRP. Bei VRRP oder einem Layer-2 Hartbeat müssen beide SBCs im selben IP Subnetz angebunden sein, es bedarf also der Konfiguration desselben SBC-Subnetzes in beiden SBC-Standorten.

Fällt ein WAN-Uplink oder der Provider-Peer SIP Server beziehungsweise Provider SBC aus, muss der SBC für Fehlertoleranz über entsprechende Rerouting-Verfahren und Rerouting-Konfigurationen verfügen und bei Bedarf dynamisch mittels SIP Server DNS-Abfrage einen neuen Provider Peer finden können. Fällt ein komplettes Provider-Netz aus, hilft nur noch die Fehlerumschaltung in ein zweites Providernetz (sofern es Verträge mit zwei Providern gibt). Solange das PSTN noch vorhanden ist, ist natürlich auch die Umschaltung auf vorkonfigurierte PSTN-Zugänge als Backup möglich. Schwierig wird dies, wenn der SIP Provider (ITSP) ein anderer als der zuvor genutzte Telko Provider ist. In diesem Fall dürfte ein dynamisches automatisches Umlenken des weltweiten Call Routing Tabellen in das PSTN-Netz nur mit langen Umschaltzeiten möglich sein.

Eine aktiv / aktiv Redundanz erhöht die Verfügbarkeit durch schellere Schaltzeiten als die aktiv/passiv Redundanz, da das Failover System bereits aktiv in die Bearbeitung der laufenden Verkehrslasten eingebunden ist und nur für etwa die Hälfte des Sessions tatsächlich eine Umschaltung stattfindet. Durch die niedrigere Auslastung der Einzelverbindungen bei Load Balancing ist das Delay niedriger als bei einer aktiv / standby Konfiguration. Hierin liegt aber auch eine Backup-Falle: Steigt die Verkehrslast auf mehr als die Leistung eines einzelnen SBC, so würde die Verbindung im Fehlerfall degradieren. Hier ist also eine Überwachung des Loadbalancing auf Lastschwellen erforderlich.

Überschreitet die Summe der genutzten Leitungen 100% der bei worst-case Ausfall eines SBC noch verfügbaren Leitungskapazität, so muss hochgerüstet werden.

Quality of Service

Ihr PSTN-Gateway hat eine sehr klare Verhaltensstruktur: solange es noch freie Kanäle gibt, werden Verbindungen zugelassen, sind alle Kanäle belegt, erhält der nächste Nutzer, der nach draußen wählt, ein Besetztzeichen. Mit SIP Trunking enden jedoch die Zeiten von jeweils 30 PSTN-Kanälen je PMX - Ihr SIP Trunk verhält sich hier ganz anders: IP-Verbindungen arbeiten nicht kanal-orientiert und haben die Eigenart, keine native Qualitätskontrolle durchzuführen. Sie versuchen, die komplette Verkehrslast, die ihnen angeboten wird, über die Leitung loszuwerden. Auch wenn eine Überlast respektive Überbuchung anliegt, versucht IP diese soweit möglich auf die Leitung aufzubringen – die restlichen Pakete werden ohne weitergehende Fehlermeldung verworfen.

Ohne zusätzliche Call Admission Control (CAC) Funktionalität ist der SIP Trunk somit nicht in der Lage, eine angemessene Audio- und Video-Qualität bereitzustellen.

Und hier kommt wieder der Session Border Controller ins Spiel: er hat die Aufgabe, die PSTN-Gateway-Funktionalität der Kanalbelegung weitestmöglich auf SIP Trunking abzubilden. Das bedeutet, er muss die Anzahl parallel laufender Audio-/Video-Sessions überwachen, insbesondere da im Regelfall im Rahmen der Service Level Vereinbarungen mit dem SIP Trunking Provider eine maximale Session-Anzahl vereinbart wurde. Sofern die unterliegende vereinbarte Bandbreite ausgelastet ist, zum Beispiel aufgrund bandbreitenhungriger Video-Sessions, darf der SBC ebenfalls keine weitere Session auf dem SIP Trunk zulassen, selbst wenn die vereinbarte maximale Anzahl Sessions noch nicht erreicht ist. Der SBC muss somit für jede Session die benötigte Bandbreite berechnen und vom verfügbaren Gesamtbandbreitenbudget abziehen. Entsprechende CAC Regeln müssen entweder

vom Call Control Server zum SBC übertragen werden oder auf dem SBC selbst konfiguriert werden.

Bei unterschiedlichen respektive unterschiedlich wichtigen Verkehrslasten sollte der SBC zusätzlich sowohl eingehend als auch ausgehend Klassifizierung, Priorisierung (durch Lesen und Setzen der IP DSCP und MAC CoS Bits), Raten-Limitierung und Traffic Shaping durchführen können, wobei insbesondere Traffic Shaping dazu beiträgt, das Ende-Ende Delay zu reduzieren. Zu den QoS-Funktionen des SBC zählen insbesondere

- QoS-Kontrolle des Transport-Netzwerks
- Mappen von und Markieren mit QoS Werten
- Call Admission Control auf Basis der Verkehrslast (Signaling Element Load), verfügbarer Bandbreite und tatsächlich festgestelltem QoS
- Policy-based Call Routing
- QoS Reporting

Sofern dies die übergeordneten Management-Tools des TK-/UC-Ausrüsters nicht leisten, muss der Session Border Controller die Session-Qualität nicht nur überwachen und im Bedarfsfall entsprechende Fehlermeldungen senden, sondern auch Reports zur der aktuellen Session-Qualität und Einhaltung der Leistungs-Spezifikationen zwischen Enterprise und SIP Provider erstellen können.

In IMS-Netzen auf der Provider-Seite muss der SBC die Policy- und Accounting-Funktionen PCRF und Standard CAC- und -Zugangsfunktionen RACS unterstützen.

4.4 Regulatorische Compliance

Seit vielen Jahrzehnten unterliegt die öffentliche Telekommunikation den so genannten Regulierungs-Behörden der jeweiligen Länder. Diese erlassen Vorschriften hinsichtlich

- Notruf der öffentlichen Notfall-Nummern (110, 112)
- Nummernportierung
- Notfall- und Krisentelefonie für Regierung und Behörden in Krisen und Katastrophenfällen (GETS)
- Abhören von Gesprächen durch die Exekutive (CALEA in USA)

Hinsichtlich der Notfall-Nummern ist bei IP-Telefonie besonders wichtig, dass die konkrete Lokation des Notrufs festgestellt wird, da das Login ja über einen beliebigen Internet-Zugang erfolgt sein kann. Hierfür müssen durch den Provider oder am Zugangs-Edge die korrekten Lokations-Informationen eigetragen und an die zuständige Leitstelle weitergeleitet werden. Leider hat die Bundesnetzagentur hier bislang lediglich einen informellen Anhang zu Inhalt und Format der einzutragenden Informationen spezifiziert, so dass es derzeit keine verabschiedete technische Grundlage gibt. Hier muss vor Abschaltung der PSTN-Netze in jedem Fall seitens der Regulierung eine verpflichtende Vorgabe erfolgen, ansonsten hängt der Notruf in der Luft.

In jedem Fall ist jedoch der Session Border Controller am Enterprise Edge die Instanz, die Lokationsinformationen für einen Notruf einzutragen, der aus einem Unternehmensstandort kommt und den Notruf mit dem entsprechenden Call Routing zur Notruf-Leitstelle zu versehen.

Auch für die Abhörfunktion ist der Session Border Controller gut geeignet: läuft doch sämtlicher Verkehr von und zum Unternehmen durch ihn hindurch und wird bei Nutzung von Verschlüsselung entschlüsselt.

Für Nummern-Portierung und GETS-Funktionen sind die Provider zuständig.

4.5 Management

Oft werden Session Border Controller heute mit einer eigenen Management-Umgebung ausgeliefert. Ist der SBC nicht vom TK-Ausrüster, hat er in jedem Fall ein eigenes Management. Hier sind dann die entsprechenden Tools und OSS Schnittstellen für Konfiguration, Administration und IMAC (Installation, Moves, Adds and Changes) einzufordern.

Hierzu zählen insbesondere
- Reporterstellung
- Alarme
- Fehleranalyse und Troubleshooting

Der SBC muss nicht nur bei speziellen Quality of Service Anforderungen, Service Level Verletzungen oder Fehlersituationen Reports generieren, sondern auch Reports für die allgemeine Nutzungs- und Abrechungsstatistik erstellen, wie dies früher das PSTN-Gateway Management respektive TK-Management geleistet hat. (siehe Abbildung 4.7)

Werden die Reports nicht im SBC generiert, so muss er zumindest die Gesprächs- und Sessiondatenerfassung (CDR) für alle ein- und ausgehenden externen Verbindungen erstellen und an das entsprechende Management-Tool (gegebenenfalls im TK-Management oder einem allgemeinen Accounting Tool implementiert) weiterleiten.

Hierzu zählen mindestens
- Echtzeit-Erfassung der Auslastung / Nutzung für Rechnungstellung
- historische Erfassung der Auslastung / Nutzung via CDR für Rechnungsstellung
- Session-Leistungsdaten für Alarme
- Sicherheits-Events für Alarme

Abbildung 4.6: Der SBC muss das Abhören durch die Exekutive ermöglichen

Da der Session Border Controller den Perimeterschutz und für alle externen Verbindungen CAC und QoS-Überwachung leisten muss, ist den Echtzeit-Alarm-Management Funktionen natürlich erhebliche Aufmerksamkeit zu widmen. Solche Alarme muss der SBC nicht nur bei Sicherheits-Vorfällen generieren, sondern auch wenn QoS- und verfügbarkeitsrelevante Netzwerk-Ereignisse, Ressourcen-Mangel, Überbuchung oder andere Ereignisse auftreten, die den Quality of Service einzelner, mehrerer oder aller Sessions beeinträchtigen. Hierfür sollte der SBC Ereignisse in verschiedene Funktionsgruppen und Klassen einteilen können: mindestens kritisch, wichtig, unkritisch.

Da der SBC als Demarkationspunkt zwischen internen und externen Netzen der zentrale Konzentrationspunkt für ein- und ausgehende Verbindungen ist, ist er zusätzlich die geeignete Komponente, um Fehlerkontrolle, Fehleranalyse und Fehlerbehebung durchzuführen. Hierzu zählen das Durchführen von Testroutinen für Call Routing, Alive-Tests zum Provider-Peer, Neuaufbau der Verbindung zum Provider, Fehler-Isolierung für Signalisierung und / oder Media Streams und soweit möglich Fehlerbehebung für Signalisierung und / oder Media Streams. Verschlüsselungs- und Signatur-Fehler sollten und werden im Regelfall zum Verwerfen des entsprechenden Signalisierung- oder Media-Streams führen.

4.6 Architektur, Leistung, Skalierbarkeit

Die Architektur eines Session Border Controllers entscheidet, wie flexibel und weit-

Abbildung 4.7: SBC-Tools für Echtzeit- und historisches Monitoring

reichend ein SBC hinsichtlich Funktionalität und Skalierung einsetzbar ist. Zunächst ist zu unterscheiden, ob der Session Border Controller als virtualisierte Lösung oder als Hardware Appliance oder beides ausgeliefert wird. Vorab lässt sich an dieser Stelle schon anmerken:

Die virtualisierten Lösungen leisten im Vergleich mit den Appliances typischerweise nur einen Bruchteil der maximalen Anzahl parallel möglicher Sessions.

Zudem gibt es bei einigen Produkten herstellerseitige Einschränkungen der Funktionalität bei bestimmten Funktionen. Ein ganz einfaches Beispiel sind hier physische Schnittstellen wie ein Backup PSTN-Zugang. Teilweise sind auch Media-Ressourcen in der virtualisierten Variante nur beschränkt nutzbar. In jedem Fall ist zu erfragen, wie viele parallele Audio- und Video-Sessions die virtualisierte Lösung und die Appliance unterstützen. Auch die maximalen Sessionzahlen für verschüsselten Verkehr unterscheiden sich erheblich von der Anzahl unverschlüsselter Sessions und sind bei der Planung von Einsatz-Szenarien und der Produkt-Evaluierung zu berücksichtigen. Hierzu gehört ebenfalls die Information, wie sich verschlüsselte und unverschlüsselte Audio- und Video-Sessions auf die CPU-Last auswirken. Sofern diese sich nämlich gegen 100% bewegt, wird der Betreiber an der verfügbaren Leistung auch nicht mehr besonders viel Freude haben.

Zu den Leistungsdaten, die für die virtualisierte Lösung und die Appliance in Erfahrung gebracht werden sollten, gehören

- maximale Anzahl registrierter Benutzer (soweit Registrierung erforderlich ist)
- maximale Registrierungs-Rate
- maximale Anzahl paralleler unverschlüsselter Voice Sessions
- maximale Anzahl paralleler unverschlüsselter Video Sessions
- maximale Anzahl paralleler verschlüsselter Voice Sessions
- maximale Anzahl paralleler verschlüsselter Video Sessions
- maximale Anzahl paralleler Remote Nutzer Sessions

Soll eine virtualisierte Lösung eingesetzt werden, stellt sich die Frage nach der Unterstützung von VMware, Hyper-V, XEN oder anderen gewünschten Host Betriebssystemen. Soll eine VMware Lösung installiert werden, ist die SBC-Auslieferung als OVA gegebenenfalls wünschenswert. Darüber hinaus ist die Frage der Speicherversorgung für große SBCs zu klären: Muss ein externer SAN-Zugriff implementiert sein? Wie wird in diesem Fall Georedundanz ermöglicht?

Sowohl für die virtualisierte als auch die Appliance Lösung ist zu prüfen, welche Hardware unterstützt wird (Dell, HP, IBM, Cisco, andere?). Lässt sich weiterhin der Hardware-Hersteller einsetzen, den das Unternehmen bislang als präferierten Serverhersteller nutzt?

Auch die Anbindungsmöglichkeiten ins Produktivnetz und für den Management-Zugriff sind ein Thema. Kann der SBC mit redundanten 10 Gbit Schnittstellen an das Produktivnetz angeschaltet werden? Kann der Betreiber für die virtualisierte Lösung redundante 10 Gbit vNICs an zwei verschiedene vSwitches könfigurieren? Lässt sich der Management-Zugang redundant auslegen? Lässt sich für den Management Zugang ein separates IP Netz / VLAN konfigurieren, das mit den Produktiv-VLANs nicht durch Routing gekoppelt ist?

Welche Backup Funktionalität unterstützt der Session Border Controller? Nur Cold standby? 1+1 Redundanz oder N+1 Redundanz? Hot standby mit aktiv / aktiv oder aktiv / passiv Modus? Wie gut und gleichverteilt funktioniert eine Lastverteilung über mehrere SBCs in der Praxis? Wie schnell erfolgt im Fehlerfall eine Umschaltung? Erfolgt die Fehlerumschaltung transparent für die Clients oder müssen sich diese neu registrieren? Welche Kopplung erfordern beziehungsweise ermöglichen redundante SBCs – Layer-2 oder Layer-3? Wie sieht der Alive Mechanismus

oder Heartbeat zwischen den SBCs aus? Standard, zum Beispiel VRRP oder herstellerspezifisch?

Wie kann der SIP Trunk redundant ausgelegt werden? Über mehrere physische Schnittstellen? Wie findet der SBC einen neuen Provider-Peer – dynamisch mittels DNS-Abfrage gemäß RFC 3263 oder müssen die Alternativen statisch eingetragen sein? Verläuft ein Trunk Failover stateful oder mit Session-Verlust und –Neuaufbau?

Unterstützt der Session Border Controller Lastverteilung zum internen Netz und über redundante Trunkverbindungen? Wenn ja, bis zu wie vielen parallel lastverteilten Wegen im internen LAN?

5. Markt und Hersteller

Sowohl der SIP Trunking Markt im Allgemeinen als auch der Session Border Markt im besonderen zeigen aktuell und in den nächsten Jahren einen deutlich erkennbaren Boom: Allein der Session Border Controller Markt soll laut Infonetics Research bis 2018 mit einem CAGR von 7 Prozent auf 1,6 Milliarden USD wachsen.

Der globale SIP Trunking Service Markt ist schon in 2014 um 35% auf 4,4 Mrd. USD gewachsen (Infoneteics Research, Oktober 2014), und das Wachstum hält die nächsten 5 Jahre an: bis 2018 erwartet Infonetics ein weltweites Umsatzwachstum für SIP Trunking bis auf 8 Mrd. USD. Frost & Sullivan kommen zu ganz ähnlichen Ergebnissen: Sie sehen den Dienstleistungsmarkt für VoIP und SIP Trunking bis 2019 auf satte 9,35 Milliarden USD ansteigen (Frost & Sullivan, Okt. 2014). Hierbei stellt Nordamerika den stärksten Markt für SIP Trunking Service Angebote: schon mehr als 20% der Voice Trunks in USA laufen über SIP Trunking und bis 2016 planen drei Viertel aller US-Unternehmen den Einsatz von SIP Trunking. Aber neue geografische Märkte öffnen sich schrittweise und verstärken das Wachstum. Dies wird in Europa natürlich durch die Ankündigung der Telko-Provider beschleunigt, das PSTN mittelfristig abzuschalten.

Somit ist klar: Immer mehr Unternehmen wechseln freiwillig oder aufgrund der angekündigten PSTN-Abschaltung auf SIP Trunking. Aber besonders größere Unternehmen tun das typischerweise nicht mit einem 100% Schritt von Beginn an, sondern meistens erfolgt an einem oder an einigen Standorten ein vorsichtiger Einstieg in die SIP Trunking Technologie, bei dem es im Fehlerfall für jeden Schritt ein Fallback-Möglichkeit auf die Ursprungs-Lösung gibt. In solchen Migrations-Szenarien bleibt der PSTN-Zugang sowohl als Haupt-Standbein als auch als Backup-Möglichkeit für die SIP Trunks bestehen.

Hinsichtlich der Marktanteile einzelner Hersteller gibt es eine interessante SIP Umfrage über SIP Trunking und Session Border Controller von November 2015 (The SIP School), die die in Abbildung 5.1 gezeigten Marktanteile für Session Border Controller, die am Enterprise Edge zum Einsatz kommen, zum Ergebnis hatte. In dieser Umfrage waren 52,2 Prozent Teilnehmer aus den USA, 10,5 Prozent aus UK und Deutschland, 7 Prozent aus Indien, 6,6 Prozent aus Kanada und 23,5 Prozent aus anderen Ländern.

Auf den ersten Blick ist festzustellen, dass es noch keinen dominanten Platzhirsch gibt, der mehr als 30 Prozent Marktanteil beherrscht. Avaya ist in dieser Umfrage mit ihrer Sipera-Weiterentwicklung (ASBCE Avaya Session Border Controller Enterprise) der Marktführer, Platz zwei geht an Oracle (Acme), die ja vor einigen Jahren Acme eingekauft haben. An dritter und vierter Stelle kommen die Teilnehmer, die noch keinen SBC einsetzen oder sich aus Sicherheitsgründen zu ihrem SBC nicht äußern wollten. Im Mittelfeld stehen Mitel, Cisco und Audiocodes mit neun, acht und sechs Prozent Marktanteil. Da der Marktanteil von Cisco TK-Lösungen sehr viel höher ist als 8 Prozent, lässt sich messerscharf schließen, dass viele Unternehmen, die eine Cisco TK-Lösung einsetzen, entweder gar keinen oder aber keinen Cisco CUBE SBC nutzen.

Der niedrige Marktanteil von Provider-SBCs im Unternehmensumfeld ist darin begründet, dass diese Session Border Controller weniger Enterprise-spezifische Funktionalität besitzen und im Regelfall für große bis sehr große Einsatzszenarien entwickelt wurden, die die Anforderungen vieler Unternehmen übersteigen. Das Preisgefüge von „Provider"-SBCs ist entsprechend hoch angesiedelt – ein triftiger Grund für Unternehmen, sich für ein anderes Produkt zu entscheiden.

Zusätzlich zum Session Border Controller sollten die Teilnehmer der Umfrage beantworten, in welcher Beziehung sie zu dem Hersteller ihres SBC stehen. Hierbei hatten 26 Prozent ihren SBC vom TK-Her-

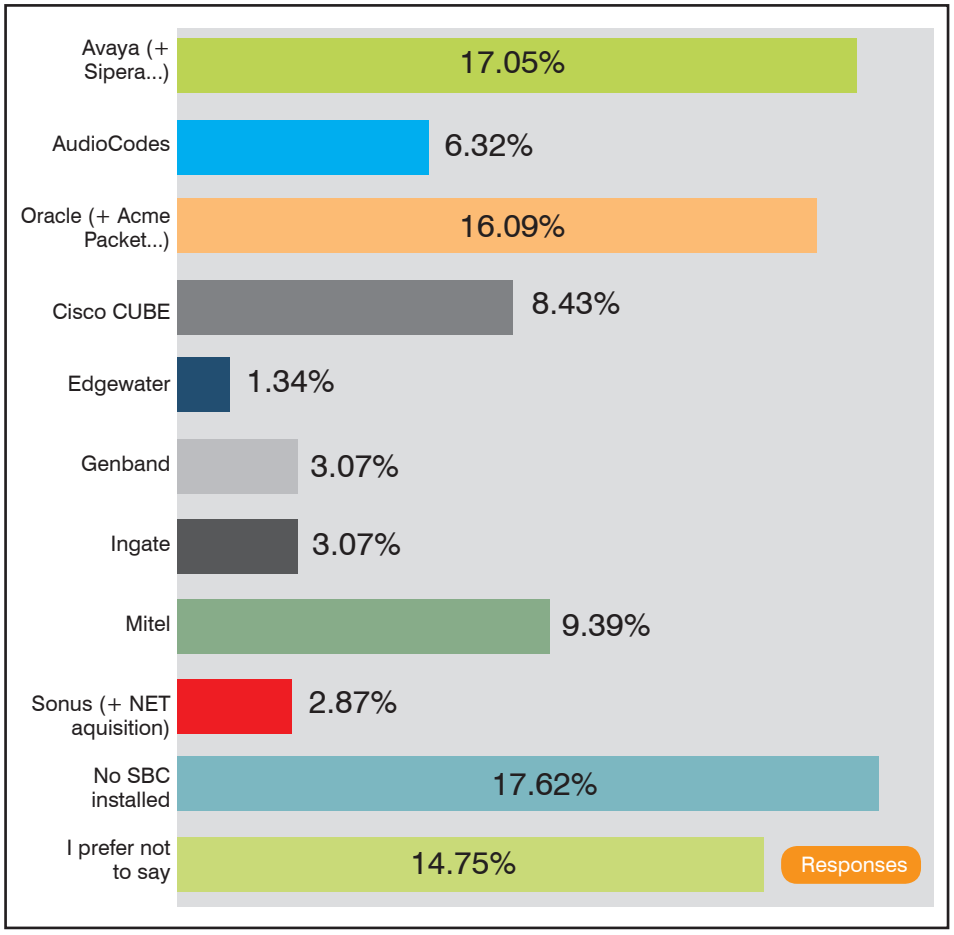


Abbildung 5.1: Marktanteile etablierter Hersteller am Session Border Controller Markt

steller gekauft, 25 Prozent ein völlig unabhängiges Produkt und nur 6 Prozent hatten den SBC vom SIP Provider erworben. Hierin ist ein starker Trend zu sehen: In den letzten drei Jahren hat jeder etablierte TK-/UC-Hersteller einen eigenen SBC entwickelt, eingekauft oder als OEM vermarktet. Somit kann der TK-/UC-Ausrüster dem Kunden ein immer besser integriertes Rundum-Sorglos-Paket inklusive SBC aus eigener Hand anbieten. Und dies wird massiv vermarktet, besonders was die Interworking Funktionen mit der herstellereigenen TK- und Videolösung betrifft! Auch die Videokonferenz-Hersteller haben ja seit Jahren ihren eigenen SBC im Portfolio (manchmal hat der einen anderen Namen als SBC). Durch diese Entwicklung hat der freie SBC-Markt, der durch Hersteller wie AudioCodes vertreten wird, klar an Bedeutung verloren.

In diesem Zusammenhang erklärt sich auch der starke Verlust an Marktanteilen, die der Oracle SBC erlitten hat. Nicht nur nimmt man es Oracle nicht so ganz ab, dass sie einen „neutralen“ SBC konsequent weiterentwickeln, sondern das Produkt ist auch für eine ganze Reihe „Enterprise-Einsatzszenarien“ schlichtweg überdimensioniert – sowohl preislich als auch architekturmäßig. Für die nächsten Jahre sehen wir aus den beschriebenen Gründen einen weiter abnehmenden Marktanteil des Herstellers Oracle/Acme am Enterprise Session Border Controller Markt.

Im nächsten Teil lesen Sie:

- Exemplarische SBC Produktbeispiele etablierter Hersteller
- Produkt-Evaluierung für Architektur, SIP Trunking und Sicherheits-Funktionen

Abkürzungen

ASBCE	Avaya Session Border Controller Enterprise
CAC	Call Admission Control
CAGR	Compound Annual Growth Rate
CALEA	Communications Assistance for Law Enforcement Act
CDR	Call Detail Records
CoS	Class of Service
CPU	Central Processing Unit
CUBE	Cisco Unified Border Element
DNS	Domain Name Service
DPI	Deep Packet Inspection
DSCP	Differentiated Services Code Point
GETS	The Government Emergency Telecommunications Service
HA	High Available
IMAC	Installation, Moves, Adds and Changes
IP	Internet Protocol
ISSU	In Service Software Upgrade
ITSP	Internet Telephony Service Provider
LAN	Local Area Network
MAC	Media Access Control
NIC	Network Interface Card
OSS	Operational Support System
OVA	Open Virtual Appliance
PCRF	Policy Charging and Rules Function
PMX	Primär-Multiplex
PSTN	Public Switched Telephony Network
OEM	Original Equipment Manufacturer
QoS	Quality of Service
RACS	Resource and Administration Control Subsystem
RFC	Request For Command
SAN	Storage Area Network
SBC	Session Border Controller
SIP	Session Initiation Protocol
SLA	Service Level Agreement
TE	Traffic Engineering
TK	Telekommunikation
UC	Unified Communication
UHA	Ultra High Available
VLAN	Virtual LAN
vNIC	virtual Network Interface Card
VRRP	Virtual Router Redundancy Protocol

Links

www.ietf.org
www.sipforum.org
www.sonus.net

Literatur

- Pat Hurley: Session Border Controller for Dummies; Wiley & Sons, 2nd Edition 2013
- Session Boder Controllers: A Primer; Oracle White Paper 2013
- Market Guide for Enterprise SBC; Gartner, Juni 2014
- John Hardwick: Session Border Controllers, Enabling The VoIP Revolution; Data Connection Whitepaper, 2005

ComConsult Veranstaltungskalender

Lokale Netze für Einsteiger, 15.02.-19.02.16 in Aachen

Dieses Seminar vermittelt kompakt und intensiv innerhalb von 5 Tagen die Grundprinzipien des Aufbaus und der Arbeitsweise Lokaler Netzwerke. Dabei werden sowohl die notwendigen theoretischen Hintergrundkenntnisse vermittelt als auch der praktische Aufbau und der Betrieb eines LANs erläutert. Ausgehend von einer Darstellung von Themen der Verkabelung und der grundlegenden Übertragungsprotokolle werden die wichtigen Zusammenhänge zwischen der Arbeitsweise von Switch-Systemen, den darauf aufsetzenden Verfahren und der Anbindung von PCs und Servern systematisch erklärt.

Preis: € 2.490,-- netto

IP-Wissen für TK-Mitarbeiter, 22.02.-23.02.16 in Bonn

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

Preis: € 1.590,-- netto

Das PSTN stirbt: Die neue Kommunikation mit SIP/IP, 08.03.16 in Bonn

Die Sonderveranstaltung zum Thema PSTN-Migration hin zu All-IP bietet top-aktuelle Informationen und Analysen mit ausgewählten Experten. Eine ausgewogene Mischung aus Analysen, Hintergrundwissen und Projekterfahrungen in Kombination mit Produktbewertungen und Diskussionen liefert das ideale Umfeld für alle Planer, Betreiber und Verantwortliche solcher Lösungen.

Preis: € 1.090,-- netto

Netzzugangskontrolle: Technik, Planung und Betrieb, 14.03.-16.03.16 in Berlin

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

Preis: € 1.890,-- netto

TCP/IP-Netze erfolgreich betreiben, 14.03.-16.03.16 in Berlin

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

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen, 14.03.-16.03.16 in Köln

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

Preis: € 1.890,-- netto

Interne Absicherung der IT-Infrastruktur, 14.03.-15.03.16 in Köln

In diesem Seminar lernen Sie wie man die Sicherheit von LAN, WAN, Endgeräten, RZ-Bereichen, Servern und SAN erreicht. Konkrete Beispiele aus der Praxis zeigen den Weg zu einer erfolgreichen IT-Sicherheits-Lösung.

Preis: € 1.590,-- netto

Internetworking: optimales Netzwerk-Design mit Switching und Routing, 04.04.-08.04.16 in Aachen

Dieses Seminar vermittelt alles Wichtige, was Sie zum Thema LAN wissen müssen. Es werden unterschiedlichen Einsatzszenarien für Routing und Switching beleuchtet und das notwendige Wissen zur erfolgreichen Planung und dem Betrieb von Netzwerk Infrastrukturen vermittelt. Die Abdeckung der Themen erstreckt sich über Layer 2 Redundanzverfahren, Routing und Tunneltechnologien, sowie Netzwerkmanagement Fragen. Einen weiteren Schwerpunkt bildet das Kapitel Office Network. Hier werden der Aufbau und die Integration von WLAN Strukturen detailliert beleuchtet. Abgerundet werden diese Informationen durch verschiedene praktische Übungen und einen Blick auf die aktuelle Markt- und Produktsituation der führenden Hersteller von Netzwerk-Komponenten.

Preis: € 2.490,-- netto

RZ-RZ-Kopplung - alles nur eine Frage der Bandbreite?, 11.04.16 in Stuttgart

Rechenzentren in entfernten Standorten zu betreiben erfordert sich mit IT-Sicherheit, Desaster Recovery, Service Level Agreements und Hochverfügbarkeit auseinander zu setzen. Dabei sind zum Teil Vorgaben bspw. vom BSI zu beachten. In dieser Schulung werden die aktuellen Techniken erläutert und für die richtige strategische Entscheidung zu einem Gesamtkonzept zusammengeführt.

Preis: € 1.090,-- netto

Crashkurs IT-Recht für Nichtjuristen, 11.04.-12.04.16 in Stuttgart

Diese Veranstaltung wendet sich an IT-Leiter, Compliance-Beauftragte und Geschäftsführer, die sich kompakte und praktische Grundkenntnisse zu den rechtlichen Eckpunkten des IT-Projektes verschaffen wollen. Die Inhalte sind insbesondere an Nichtjuristen gerichtet, die sich nicht alltäglich mit rechtlichen Fragestellungen befassen und eine Grundorientierung suchen. In dem Seminar werden auch Praxisfälle erörtert.

Preis: € 1.590,-- netto

Zertifizierungen

ComConsult Certified Network Engineer

Lokale Netze
15.02. - 19.02.16 in Aachen
09.05. - 13.05.16 in Aachen
19.09. - 23.09.16 in Aachen

TCP/IP-Netze erfolgreich betreiben
14.03. - 16.03.16 in Berlin
20.06. - 22.06.16 in Bonn
24.10. - 26.10.16 in Bonn

Internetworking
04.04. - 08.04.16 in Aachen
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
10.05. - 13.05.16 in Aachen
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
14.03. - 16.03.16 in Köln
11.05. - 13.05.16 in Bonn
24.10. - 26.10.16 in Frankfurt

Session Initiation Protocol Basis-Technologie der IP-Telefonie
11.04. - 13.04.16 in Stuttgart
20.06. - 22.06.16 in Bonn
09.11. - 11.11.16 in Berlin

Umfassende Absicherung von Voice over IP und Unified Communications
25.04. - 27.04.16 in Bonn
04.07. - 06.07.16 in Stuttgart
28.11. - 30.11.16 in Bonn

Optionales Einsteiger-Seminar: IP-Wissen für TK-Mitarbeiter
22.02. - 23.02.16 in Bonn
25.04. - 26.04.16 in Düsseldorf
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