Eine Themenbeilage der Heise Zeitschriften Verlag GmbH & Co. KG

KOMMUNIKATION UND NETZE

I 2014

ITK – PRODUKTE UND LÖSUNGEN

Next Generation Network:

Wie Unternehmen von ISDN auf IP-Betrieb umstellen Seite 6

www.kommunikation-netze.de

powered by iX

BUSINESS CLASS WLAN

MADE IN GERMANY

bintec W-Serie

MIMO 802.11n by bintec

Wi Fi CERTIFIED

- Gleichzeitiger Betrieb auf dem 2,4-GHz und 5-GHz-Band
- Bruttoübertragungsraten bis zu 2x 450 Mbit/s (802.11n Mimo 3x3)
- Stand-Alone Betrieb oder Betrieb mit **bintec** WLAN Controller
- 2-Port Gigabit Ethernetanschluss mit PoE (Power over Ethernet)
- Elegantes, unauffälliges Gehäusedesign für Wand-und Deckenmontage
- Integrierte Mimo-Antennen für 2,4-und 5-GHz

NEU! Mit integrierter **kostenloser** WLAN-Controller Lizenz zur Steuerung von bis zu 6 Access Points

funkschau ITK-Produkte des Jahres WLAN im Unternehmen bintec elmeg bintec W2004n 2013

Erfahren Sie mehr über bintec WLAN-Produkte und Lösungen auf unserer Webseite:
www.bintec-elmeg.com/wlanpower

bintec elmeg Teldat Group Company

bintec elmeg GmbH
Südwestpark 94
D-90449 Nürnberg
Telefon: +49-911-96 73-0
www.bintec-elmeg.com/wlanpower

Diese Geister, die wir riefen

Zugegeben – als ich vor über 20 Jahren für eine der ersten Zeitschriftenbeilagen zum Thema Digitale Kommunikation begeistert schrieb, habe ich nicht geahnt, worauf wir uns tatsächlich einlassen. Das wurde mir auf dem ersten IT-Rechtstag bewusst, der vorige Woche in Berlin stattfand. Datenschützer und Juristen diskutierten unter anderem rechtliche Komplikationen, die uns Maschinen bereiten, die wir vernetzen, damit wir alle besser, schneller und effizienter miteinander (?) kommunizieren können als je zuvor. Als Moderator einer Podiumsdiskussion stellte ich am Ende eine einfache Frage, die und deren Antwort ich Ihnen am Ende dieses Beitrags verraten möchte.

Dass 2013 laut Incapsula bereits 61,5 Prozent des Internet-Datenverkehrs auf Robots zurückzuführen waren, dürfte kaum jemanden erstaunen. Das Web spricht in immer größerem Ausmaß mit sich selbst. Würde nicht in ebenso gesteigertem Maße Video durchs Netz gehen, fiele der humane Anteil wohl noch einmal deutlich geringer aus.

In der Tat ist der Mensch für den massenhaften Hochgeschwindigkeitsumgang mit digitalen Daten denkbar schlecht ausgelegt. Und welche Rolle er im heranbrausenden Internet of Everything spielen wird, bleibt, gelinde gesagt, spannend. In jedem Fall muss ein mobiles Netz, das Verkehrsmittel und bewegte Sensoren versorgt, künftig sehr viel leistungsstärker sein als das aktuelle 3G/4G-LTE. Von der Arbeit am 5G-Mobilfunk, der ab 2020 mit 10 GBit durch die Luft gehen will, berichtet Harald B. Karcher ab Seite 16. Das ist allerdings erst noch Zukunftsmusik.

In der Gegenwart geht es für viele Unternehmen oft praktisch darum, endlich den letzten analogen Telefonanschluss abzuklemmen. Weil die POTS-Dienste im Einzelfall aber extrem hartnäckig sind, muss man bei der Umstellung von ISDN-Anlagen auf IP-Kommunikation sehr behutsam vorgehen. Genau damit befasst sich unsere Titelgeschichte zu Heftbeginn. Johann Deutinger zeigt ab Seite 6, dass es bei der Telefonie-Migration ins Next Generation Network mitunter sinnvoll ist, die BPX auch für Altfälle offen zu halten. Und noch etwas gilt es in vielen Fällen nachzuholen: die Verschlüsselung von Voice over IP. Am Beispiel einer Asterisk-Snom-Kombination erklärt daher Dominik Mauritz im Anschluss, wie man SIPS und SRTP standardmäßig aktiviert.

Das dritte Mal beschäftigt sich dieses Heft mit dem Thema Sicherheit, wenn es um die Anbindung verstreuter Standorte geht. Tobias Frielingsdorf rät in solchen Fällen zur Netzbündelung per Multichannel VPN. Seine Argumente – geringere Ausfallwahrscheinlichkeit von der Fallback-Logik her und gesteigerte Transportsicherheit durch gestückelte (und verschlüsselte) Übertragung – legt er ab Seite 12 dar.

Der andere Heftschwerpunkt liegt auf dem Thema Wireless. Denn durch das rasante Mobile-Wachstum stoßen die bestehenden Funknetzinstallationen immer öfter an ihre Grenzen. Und wieder einmal soll es ein neuer Standard richten: IEEE 802.11ac soll bis zu 2,6 GBit/s schaffen und sich im 5-GHz-Frequenzband deutlich weniger von Interferenzen beirren lassen. Ab Seite 20 erklärt Christoph Becker, welche Vorteile ein AC-WLAN sonst noch ausspielen könnte.

Zugleich war Harald B. Karcher wieder im Wi-Fi-Feldtest unterwegs. Einmal spielte er den Xirrus Wi-Fi Inspector auf seinen Laptop, um zu untersuchen, was das kostenlose Tool kann und wie sich ältere und neueste Funknetzwerke damit noch verbessern lassen; seinen Testbericht finden Sie ab Seite 22. Ein andermal packte er die Koffer und begutachtete die komplexe Access-Point-Verteilung in einigen großen Hotels der Luxusklasse, vom Pionier in München, dem klassischen Vier Jahreszeiten, bis zum hochmodernen Emirates Palace Abu Dhabi, in dem das Herrscherhaus bereits nach AC-Standard funkversorgt wird.

Kommen wir zu der eingangs erwähnten „Berliner Frage“: Wer der anwesenden Experten glaubt noch daran, dass wir Menschen die juristischen Folgen – also eine funktionierende Gesetzgebung mit seriösen Geschäftsmöglichkeiten für Unternehmen bei gleichzeitig realistisch praktizierbarem Daten- und Verbraucherschutz – im Griff haben und behalten werden? Drei zögerliche Hände gingen nach oben. Gegenprobe: Wer von Ihnen denkt, dass wir die Kontrolle verloren haben und weiter verlieren werden? Bei dreißig Händen habe ich aufgehört zu zählen.

Thomas Jannot

BITKOM-PROGNOSE

2014 werden 30 Millionen Smartphones verkauft

Der Smartphone-Boom ist ungebrochen. Laut BITKOM sollen 2014 rund 30 Millionen Internet-fähige Handys verkauft werden – ein Plus von 12 % im Vergleich zum Vorjahr. Die starke Nachfrage lasse auch den Umsatz weiter steigen – auf voraussichtlich 9,3 Milliarden Euro. Das ist ein Wachstum um 10 % gegenüber 2013.

„Auch im achten Jahr des Smartphone-Booms ist die Begeisterung bei den Verbrauchern ungebrochen“, sagte dazu BITKOM-Präsidiumsmitglied Jens Schulte-Bockum. „Smartphones sind die Treiber des digitalen Wandels – nicht nur im Telekommunikationssektor. Auch in anderen Bereichen schieben sie ganz neue Geschäftsmodelle an.“ Smartphones seien heute schon Mittelpunkt des digitalen Lebens: „Wir zahlen, planen und buchen mit ihnen“, so Schulte-Bockum. „Künftig werden sie weitere Bereiche erobern, durch neue Anwendungen etwa im Automotive- oder Gesundheitsbereich. Rund um Smartphones entstehen so neue Ökosysteme, die enorme Chancen gerade auch für junge Unternehmen bieten.“

LTE IM PKW

Funkverbindung aus dem Zigarettenanzünder

Mit einem LTE-WiFi-Stick für Pkw will Vodafone auch ältere Wagen zum vernetzten Fahrzeug machen. Die Lösung wird derzeit mit ausgewählten Fahrern von Taxi Berlin getestet.

Der LTE-Stick baut ein WLAN im Fahrzeug auf. Beim Einloggen hält der Nutzer ein Gerät mit NFC-Technik an einen dafür vorgesehenen Chip oder er erfasst mit der integrierten Kamera einen passenden QR-Code. Bis zu zehn Geräte sollen so gleichzeitig mit schneller LTE-Anbindung surfen können. Seine Energie bezieht der Stick kabellos aus dem Zigarettenanzünder. Für den Einsatz an der heimischen Steckdose oder auf Reisen verfügt das Gerät über einen entsprechenden Adapter. Bei Neufahrzeugen im gehobenen Segment ist die integrierte Internet-Anbindung mittlerweile ein häufiges Zusatzangebot der Hersteller; für den Gebrauchtwagenmarkt fehlten aber durchdachte Lösungen.

AUFTRAGSDATENVERARBEITUNG

Mustervertrag für externe IT-Services

Immer mehr Unternehmen und andere Organisationen übertragen Teile ihrer Datenverarbeitung an externe IT-Dienstleister. Dabei müssen die Vertragspartner Regelungen zum Datenschutz treffen. Der Hightech-Verband BITKOM hat zu diesem Zweck nun seine „Mustervertragsanlage zur Auftragsdatenverarbeitung“ auf Version 4.0 aktualisiert. Damit sollen die Geschäftspartner sicherstellen, dass die Daten gesetzeskonform verarbeitet werden.

Die BITKOM-Vorlage berücksichtigt sowohl die Interessen von Auftraggebern als auch von Auftragnehmern. Die aktualisierte Version 4.0 enthält zudem englische Übersetzungshilfen für internationale Geschäftspartner. Für ein konkretes Projekt müssten die Vertragsparteien das Muster gegebenenfalls anpassen.

CONNECTED CARS

SAP und BMW forschen am Auto der Zukunft

SAP und BMW entwickeln gemeinsam eine Infrastruktur für Mobilitätsdienste in Fahrzeugen auf Basis der SAP HANA Cloud Platform. Dabei sollen Informationen aus Diensten, die von externen Partnern angeboten werden, orts- und routenbezogen aggregiert und Autofahrern direkt im Fahrzeug angezeigt werden. SAP Hana fungiert dabei als Mittler zwischen den Diensten der externen Partner und BMW. Ein virtueller Marktplatz bündelt die Informationen unterschiedlichster Anbieter und könnte es BMW künftig ermöglichen, seinen Kunden individuelle Angebote im Fahrzeug bereitzustellen.

Zwei Anwendungsfälle wurden als Prototypen bereits umgesetzt: Parken und Couponing. Der Prototyp für den Bereich Parken sucht nach Benutzerprofil und aktueller Verfügbarkeit passende Parkmöglichkeiten im Umfeld des Fahrziels. Zusätzlich werden Detailinformationen wie Tarif und möglicherweise die Eignung für bestimmte Fahrzeuge angezeigt. Die Lage eines durch den Fahrer ausgewählten Parkplatzes kann einfach in die Navigation übernommen werden.

Beim Couponing erhält der Fahrer auf Basis seiner aktuellen Position, der gewählten Route und seiner persönlichen Vorlieben passende Angebote, zu denen er Detailinformationen aufrufen kann. Auch hier lässt sich die Zieladresse übernehmen. Der entsprechende Coupon wird direkt an das Smartphone des Fahrers geschickt.

Für Dienstleister sollen sich daraus langfristig attraktive Chancen ergeben: Ein Informationskanal zum Fahrzeug eröffnet ihnen eine neue Möglichkeit, Kunden zu erreichen. Und über eine standardisierte Plattform könnten Automobilhersteller gleichzeitig den Zugang zu einer Vielzahl von Dienstleistern flexibel erhalten, ohne für jeden von diesen individuelle Schnittstellen einzurichten.

DEVICE-INDEPENDENT MULTI REALITY INTERFACES

Fabrikfernwartung geschieht per Live-Schaltung

Wenn es in einer Produktionsanlage zu Fehlern kommt und das Personal vor Ort sie nicht beheben kann, müssen Experten anreisen – normalerweise. Forscher des Intel Visual Computing Instituts (VCI), zu dem unter anderem auch die Universität des Saarlandes gehört, haben für solche Situationen nun eine Plattform entwickelt, die den Ingenieur in seinem Büro live mit dem Produktionsstandort zusammenbringen soll. Dem VCI zufolge werden Sensor- und Umgebungsdaten, Videosignale und Computergrafik in einer einzigen Anwendung verbunden.

„Eine Kamera filmt die zu untersuchende Maschine“, erklärt Projektleiter Michael Karl. „Das Video wird in Echtzeit auf den Rechner übertragen. Nutzer beider Standorte können das Modell interaktiv bedienen. Der Ingenieur kann so dem Personal vor Ort zum Beispiel zeigen, welches Teil der Maschine ausgetauscht werden muss.“ Die Plattform stellt außerdem verschiedene Messdaten von Sensoren zur Verfügung, die etwa Aufschluss über Temperatur oder Druck geben und so auch Hinweise zur Schadensursache liefern können. Über eine Videokonferenzschaltung seien alle Akteure außerdem miteinander verbunden. Weitere Informationen zu den Device-Independent Multi Reality Interfaces gibt es auf www.intel-vci.uni-saarland.de.

FNT

// Software für Infrastruktur- und Servicemanagement in IT und Telekommunikation

Auf Basis einer Plattform mit einem durchgängigen, integrierten Datenmodell entwickelt FNT für alle relevanten Aufgabenfelder ausgereifte Lösungen.

So bietet FNT Software leistungsfähige Spezialwerkzeuge, um IT-, telekommunikations- und rechenzentrumsspezifische Aufgaben und Prozesse in einer Software optimal zu unterstützen.

// when transparency matters.

weitere Informationen unter www.fntsoftware.com

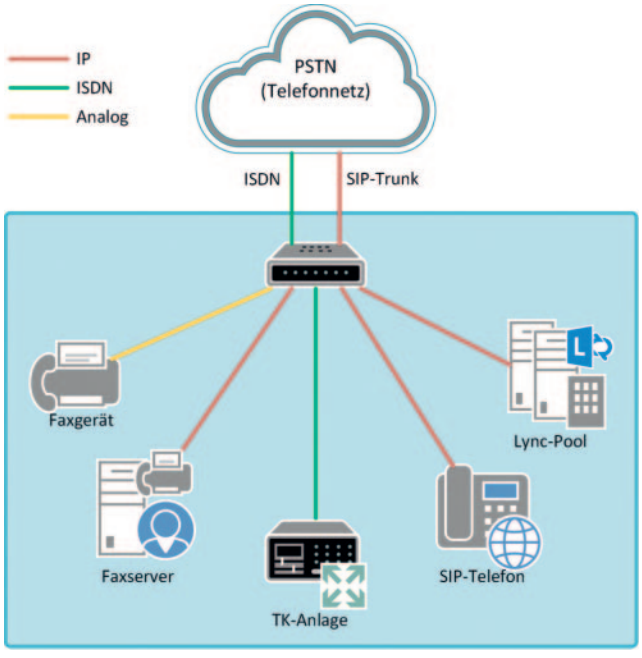
Vom Media Gateway zum Session Border Controller

Die Migration von ISDN auf reinen IP-Betrieb geschieht am besten schrittweise.

Media Gateways spielen eine etablierte Rolle als Bindeglied zwischen ISDN und lokalen Kommunikationsdiensten. Das Ende der ISDN-Ära ist jedoch abzusehen, auch wenn es bisher mehrmals verschoben wurde – aktuell ist das Jahr 2018 im Gespräch. Wie sieht die neue Welt der rein IP-basierten Kommunikation aus?

Die anstehende Umstellung stellt Unternehmen in der verknüpften Telekommunikationswelt vor eine ganze Reihe von Einzelfragen. Funktioniert Faxen weiterhin wie bisher? Welche Strategien führen zu einer erfolgreichen Migration? Welche Rolle spielen Session Border Controller (SBC) als Nachfolger der Media Gateways? Kann man sogar auf dedizierte Hardware verzichten und Schlüsselkomponenten wie Gateways bzw. SBCs virtualisieren?

Ein weiteres Thema ist die Kompatibilität zu Schnittstellen und Protokollen. Das im IP-Umfeld übliche SIP-Protokoll unterscheidet sich bei verschiedenen Implementationen oft im Detail, sodass genau abzustimmen ist, was auf Anhieb funktionieren muss und wo Anpassungen notwendig sind. Hersteller wie Microsoft, die in ihren UC-Lösungen (Unified Communications) auf SIP setzen, bemühen sich um Kompatibilität durch umfangreiche Spezifikationen und aufwendige Zertifizierungsverfahren. Am Beispiel von Microsoft Lync Server werden in diesem Beitrag einige typische Anforderungen beschrieben.



Quelle: Ferrari Electronic AG

Größtmögliche Flexibilität durch Platzierung des Gateways zwischen Amt und TK-Anlage (Drop and Insert) (Abb. 1).

ISDN als TK-Universalnetz

In der Einführungsphase wurde ISDN eher skeptisch betrachtet. Besonders im privaten Umfeld war nicht einzusehen, warum man für einen etwas anderen Telefonanschluss deutlich mehr ausgeben sollte als bisher. Scherzhafte Interpretationen der Abkürzung ISDN („Ist Sowas Denn Nötig?“) gaben das Meinungsbild treffend wieder.

Dabei hatte die neue Technologie im Vergleich zum analogen Amtszugang durchaus einiges an Mehrwert zu bieten, etwa zwei gleichzeitige Gespräche und zusätzliche Telefonnummern am Mehrgeräteanschluss; auch war es nun ohne großen technischen Aufwand möglich, eine durchwahlfähige Telefonanlage am Anlagenanschluss zu betreiben. Ebenso war die gleichbleibende Qualität der Verbindung von Vorteil.

Für Firmenkunden war die höhere Grundgebühr kein großes Hindernis im Verhältnis zu den Vorteilen. Die große Masse war jedoch nur zu erreichen, wenn auch ein Großteil der Privatkunden zum Umstieg bewegt werden konnte. Aber selbst nachdem die Phase der nationalen ISDN-Protokolle – in Deutschland ab 1989 nach 1TR6-Standard – durch das gemeinsame EURO-ISDN im Jahre 1994 überwunden war, bedurfte es massiver Fördermaßnahmen, um endlich eine nennenswerte Teilnehmerzahl zu erreichen: Der Umstieg auf einen ISDN-Anschluss wurde mit 300 DM belohnt bzw. mit 700 DM, wenn eine ISDN-Telefonanlage angeschafft wurde. Eine Reihe von Herstellern brachte kleine Anlagen in dieser Preisklasse heraus. Nach dem Ende der Förderung Mitte 1996 verschwanden einige davon schnell wieder von der Bühne.

Migrationskonzepte und Herausforderungen

Viele Gründe führen inzwischen zur Ablösung der leitungsvermittelnden ISDN-Technologie durch paketvermittelnde Next Generation Networks (NGN), allen voran die niedrigeren Kosten. Neben anderen Aspekten ist der Unterhalt der veralteten Hardware sowie die Bereitstellung einer Stromversorgung für Teilnehmerapparate wesentlich teurer als der Betrieb einer modernen IP-Infrastruktur. Letztere hat auch weitere Vorteile; die eine oder andere Einschränkung muss jedoch hingenommen werden, wie weiter unten noch ausgeführt wird.

Der Umstieg betrifft zwei Bereiche, die einigermaßen unabhängig voneinander zu betrachten sind: die Ersetzung herkömmlicher TK-Anlagen (Private Branch eXchange/PBX) durch IP-basierte UC-Lösungen und den Wechsel des Netzzugangs von ISDN zu einem SIP-Trunk.

Betrachten wir zunächst ein typisches Beispiel für den ersten Fall: Eine Firma nutzt eine TK-Anlage mit einem ISDN-Primärmultiplexanschluss als Amtszugang. Der Vertrag mit dem TK-Lieferanten läuft in einem Jahr aus. Bis dahin sollen alle Benutzer sukzessive auf Microsoft Lync 2013 migrieren, damit sie neben der Telefonie auch die neuen Kommunikationsarten wie Instant Messaging, Audio- und Videokonferenzen, Desktop Sharing usw. nutzen können. Ein Umstieg „über Nacht" wäre zu radikal – vielmehr sollen die Anwender sowie die Kommunikationseinrichtungen schrittweise auf die neue Lösung umgestellt werden.

Das Ganze beginnt meist mit einer Pilotphase, um festzustellen, ob das Ziel den Vorstellungen entspricht (Proof of Concept). Diese wird mit ausgewählten Benutzern durchgeführt, die in dieser Phase ausschließlich mit der neuen Technik arbeiten. Der Testbetrieb wird mit möglichst geringem Aufwand aufgesetzt. Typischerweise ist die Lösung an eine interne Schnittstelle der Telefonanlage angebunden und die bisherigen Durchwahlnummern der Benutzer werden von der Anlage dorthin umgeleitet.

Nach erfolgreichem Abschluss der Testphase beginnt die eigentliche Migration. Lync wird dabei über ein Media Gateway mit der TK-Anlage verbunden. Hier gibt es zwei Möglichkeiten: Wenn das Gateway hinter der TK-Anlage (downstream) hängt, muss für die Migrationsdauer ein separater Primärmultiplexanschluss für die Anlage beschafft werden, was in der Regel mit hohen Kosten verbunden ist. Außerdem wird ein zusätzlicher Nummernbereich im Wählplan benötigt, um TK- und Lync-Nutzer parallel zu versorgen. Eleganter (und deshalb gängige Praxis) ist die Platzierung des Gateways zwischen Amtsanschluss und TK-Anlage (upstream, auch „Drop and Insert" genannt). Einziger Nachteil dieser Lösung ist, dass am Gateway während der Migration sowohl ein externer als auch ein zusätzlicher interner ISDN-Port benötigt wird. Die Kosten hierfür liegen jedoch meist deutlich unter denen für eine Erweiterung der TK-Anlage. Vor allem

IP-PLATTFORMEN ERMÖGLICHEN VERNETZTES ARBEITEN

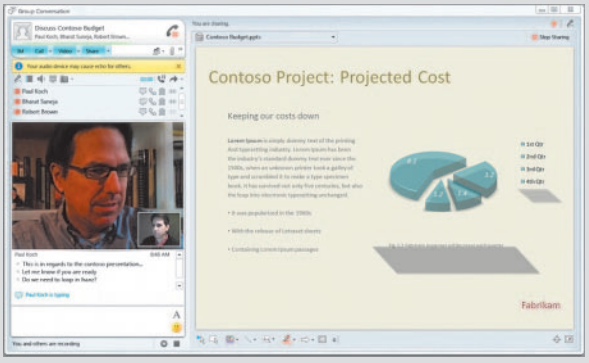
Sämtliche Kommunikationskanäle auf eine gemeinsame Basis zu stellen und über das Internet Protocol abzuwickeln, ist die Grundvoraussetzung für Unified Communications. Da die Telefonie durch Voice over IP ebenfalls auf IP-Basis funktioniert, steht der Einbindung der altbekannten Durchwahl in ein umfassendes UC-Konzept nichts mehr im Wege.

Allerdings setzt nur eine Minderheit die Technik auch ein, obwohl gerade mittelständische Kunden das Thema Unified Communications für sehr interessant halten. Als Grund werden zumeist eine mutmaßlich hohe Komplexität der Systeme und eine schwierige Administration genannt, hinzu kommen die weitverbreitete Unkenntnis des Nutzens und nicht zuletzt knapp bemessene IT-Budgets. Diese Zurückhaltung ist verständlich, wenn man bedenkt, dass jede UC-Lösung in der Tat erheblich mehr Installations- und Administrationsaufwand als eine herkömmliche Telefonanlage und ein alleinstehender E-Mail-Server erfordern.

Bei Erstinstallationen kommt insbesondere noch der Bedarf an externen Beratungs- und Integrationsleistungen hinzu. Axel Oppermann vom MSFTbriefing betont, dass der Bedarf an externen Wissensträgern deshalb relativ hoch sei, da man bei solchen Projekten nicht auf etablierte Strukturen und auf Erfahrungen der eigenen Mitarbeiter zurückgreifen kann. Daher werde für viele Microsoft-Lösungen der Bedarf an Beratungsleistungen in den kommenden Jahren steigen. Insbesondere Themen wie Social Business für Collaboration und Communication werden für die Produkte SharePoint, Lync (teilweise Exchange) und CRM die Beratungs- und Integrationsumsätze erhöhen.

Immerhin kann Microsoft bei seiner Kommunikationssoftware Lync den Vorteil der weiten Verbreitung seiner Serverprodukte und Office-Programme nutzen: Der Microsoft-Lync-Server, Nachfolger des Office-Communications-Servers, setzt auf die nahtlose Integration in die Windows-Welt. Lync verbindet einen Instant-Messaging- und Chat-Dienst mit Präsenzinformationen, Voice over IP, Konferenzschaltungen und der Möglichkeit zu Festnetztelefonaten.

Mit der zunehmenden Umstellung der Unternehmenskommunikation auf IP-basierte Lösungen werden die Vorteile, die UC-Systeme bieten, jedoch immer deutlicher. Die rasante Verbreitung von Smartphones, Tablets, ultraleichten Notebooks und anderen Mobilgeräten, die die Benutzer ständig übers Internet erreichbar machen und sogar Videokonferenzen ermöglichen, tut ein Übriges.



Quelle: Microsoft

Microsoft integriert in seine UC-Umgebung unter anderem eine Videokonferenzlösung (Abb. 2).

muss bei dieser Variante die Konfiguration der Anlage nicht geändert werden; der entsprechende ISDN-Port des Gateways verhält sich aus Sicht der Anlage exakt so wie der bisherige Amtsanschluss.

Bei der Auswahl des Media Gateways sollte man darauf achten, dass es in der Lage ist, statt des ISDN-Amtsanschlusses auch einen SIP-Trunk zu nutzen. Außerdem ist die Zertifizierung für Microsoft Lync wichtig (mehr dazu später).

Wie funktioniert dieser Mischbetrieb in der Migrationsphase? – Wenn das Gateway zwischen Amt und TK-Anlage hängt, übernimmt es eine zentrale Vermittlungsfunktion für alle Anrufe. Insgesamt müssen mindestens sechs mögliche Wege abgebildet werden. Für die Benutzerakzeptanz ist wichtig, dass alle Teilnehmer weiterhin ihre Ziele wie gewohnt wählen können und dass das komplette Routing vollautomatisch erfolgt. Dies geschieht wie folgt:

Vom Amt zu Lync-Benutzern: Das Gateway erkennt im Active Directory, dass der Benutzer bereits über eine Lync-Telefonnummer verfügt, und leitet den Anruf direkt an Lync weiter.

Vom Amt zu TK-Teilnehmern: Wenn die gewählte Nummer nicht im Active Directory als Lync-Nummer vorhanden ist, wird der Ruf an die TK-Anlage weitergeleitet.

Von Lync zu externen Zielen über den Amtsanschluss: Das Gateway erkennt, dass die Zielnummer nicht zum eigenen Nummernkreis gehört, und sendet den Ruf zur Amtsleitung.

Von Lync zu internen PBX-Teilnehmern: Da das Ziel im eigenen Nummernkreis liegt, wird direkt zur Telefonanlage geroutet.

Von TK-Benutzern zu Lync: Das Gateway erkennt, dass die Nummer im eigenen Bereich liegt, und leitet den Ruf an Lync weiter.

Von TK-Benutzern zu externen Zielen: Alle Nummern, die nicht zum eigenen Bereich gehören, gehen über die Amtsleitung ins Netz..

Weitere Verbindungswege führen – je nach der gewählten Nummer – zu Faxservern, Faxgeräten und anderen analogen Einrichtungen. Diese Ziele sind zwar zunächst weiterhin über die TK-Anlage erreichbar, sollten aber im Laufe der Migration so umgestellt werden, dass das Media Gateway die Verbindung herstellt.

Um Benutzer auf Lync zu migrieren, sind lediglich zwei Schritte erforderlich: die Konfiguration der Lync-Telefonnummer im Active Directory und die Einrichtung einer Rufumleitung in der Telefonanlage, um PBX-interne Anrufe an den Amtsanschluss zu leiten. Von dort verbindet das Gateway direkt mit dem Lync-Teilnehmer. Damit müssen Nutzer der bisherigen Telefone nicht wissen, ob der gewünschte Gesprächspartner bereits auf Lync migriert ist.

In einer idealen Welt würden alle Benutzer auf die beschriebene Weise nach und nach auf Lync umsteigen und spätestens nach einem Jahr könnte die alte TK-Anlage ihren verdienten Ruhestand antreten. Leider ist die Realität etwas anders, und es sind noch weitere Anforderungen abzudecken:

Faxgeräte können entweder direkt an analoge Ports des Media Gateways oder auch indirekt über externe SIP-Analogadapter (ATA) angeschlossen werden. Diese Adapter kommunizieren per SIP mit dem Media Gateway.

Faxserver arbeiten im Idealfall direkt mit dem Media Gateway zusammen, entweder über das T.38-Protokoll oder das Gateway übernimmt den kompletten Faxtransport und tauscht sich mit dem Faxserver auf Basis von Sende- bzw. Empfangsaufträgen aus.

Modems funktionieren bei schnellen Vollduplexverfahren aufgrund der systembedingten Verzögerungen (Latenz) bei der IP-Kommunikation nicht zuverlässig mit SIP-ATAs. Einige Gateway-Hersteller bieten Analogschnittstellen an, die ohne IP-Umsetzung direkt mit der Amtsschnittstelle kommunizieren. An diesen Ports funktionieren alle Arten von analogen Endgeräten.

Türsprechanlagen können über Media Gateways integriert werden. Mit Zusatzsoftware ist auch die Anzeige eines Videosignals von der Sprechstellenkamera möglich.

Die meisten DECT-Apparate werden nicht direkt von Lync unterstützt. Mit entsprechender Zusatzsoftware (zum Beispiel SIP2Lync) verhalten sich diese Telefone wie normale Lync-Apparate, sodass alle Funktionen wie Wählplan, Präsenzsteuerung etc. zur Verfügung stehen.

Erfolgt der Amtsanschluss ebenfalls über SIP, fungiert das Media Gateway als Enterprise Session Border Controller, der eine Vielzahl von Aufgaben übernehmen kann. Zu diesen Aufgaben gehören unter anderem der Übergang von öffentlichen zu privaten IP-Netzen mit Absicherung durch eine Firewall, die Registrierung/Authentifizierung an SIP-Trunks, die Anpassung zwischen verschiedenen Ausprägungen des SIP-Protokolls (als Back-to-Back User Agent/SIP-B2BUA), die Umsetzung zwischen UDP, TCP oder TLS sowie zwischen verschlüsselter und unverschlüsselter Sprachübertragung (SRTP/RTP), die Faxkommunikation (wahlweise über ein integriertes Softmodem mit T.30-Protokoll oder das IP-basierte T.38-Protokoll), die Ausfallsicherheit durch Failover an Mehrfachziele, die Lastverteilung durch Round-Robin-Verfahren sowie die Umsetzung von SIP auf ISDN zum Anschluss älterer TK-Anlagen an den SIP-Trunk.

Zu beachten ist, dass nicht alle SIP-Provider eine stabile Faxkommunikation unterstützen. Manche Anbieter können auch direkt mit Lync verbunden werden – in der Regel wird aber auch dann ein SBC verwendet, um Fax und weitere Analoggeräte zu integrieren. Außerdem unterstützt der SBC das sogenannte Media Bypass, also die Punkt-zu-Punkt-Sprachverbindung zum gerufenen Endgerät, und erspart damit den Betrieb von separaten Lync-Mediation-Servern.

Da SBCs nicht zwingend über Hardwareschnittstellen verfügen müssen, gibt es inzwischen bereits rein virtuelle Lösungen für die SIP-zu-SIP-Kommunikation. Vorteile sind hier unter anderem die einfache Testmöglichkeit durch Softwaredownload sowie die hohe Verfügbarkeit auf modernen Virtualisierungsplattformen.

SIP-Zertifizierung in zwei Klassen

Da Microsoft selbst keine Hardware für die Telefonieinfrastruktur anbietet, wird dieser Bedarf durch Drittanbieter gedeckt. Für das reibungslose Zusammenspiel sorgt ein Zertifizierungsprogramm (OIP/Open Interoperability Program), das umfangreiche Spezifikationen vorgibt und in dem autorisierte Testlabore nach strengen Regeln die Einhaltung der Spezifikationen prüfen.

Für Gateways gibt es zwei Zertifizierungsstufen: Basic Gateways müssen die wichtigsten Grundfunktionen erfüllen, während Enhanced Gateways den vollen Leistungsumfang abdecken. Zu diesen Erweiterungen gehören unter anderem die verschlüsselte Kommunikation über TLS und SRTP, DNS Load Balancing und die Unterstützung von Media Bypass; außerdem müssen sie strenge Vorgaben bezüglich der Sprachqualität erfüllen (niedrige Latenz, Echounterdrückung, Reparatur von Paketverlusten, Ausgleich von Jitter, Silence Suppression usw.). Für Session Border Controller gelten ähnliche Vorgaben. Zertifizierte Lösungen verzeichnet Microsoft im Internet unter http://technet.microsoft.com/en-us/lync/gg131938.aspx.

Insgesamt wird kein Unternehmen mit einem „sauberen Schnitt“ seine Telefonanlage auf IP umstellen, sondern über Pilot und Parallelbetrieb. Und oft genug erweist sich irgendwo doch ein einzelner Analoganschluss als notwendig. Dafür ist am anderen Ende der Innovationskette der Weg frei für Unified Communications (UC).

Johann Deutinger
Vorstand Ferrari electronic AG

Sicher in vier Zusatzzeilen zur sip.conf

Um VoIP-Gespräche zu verschlüsseln, muss die PBX mit SIPS und SRTP umgehen können.

Die Spionagepanik hat das Land erfasst und mit abhörsicheren Kanzlerhandys lässt sich prima Werbung treiben. Im Unternehmensalltag wären weniger spektakuläre Maßnahmen weitaus sinnvoller: Ordentliche VoIP-Telefonanlagen beherrschen von Haus aus Verschlüsselungstechniken. Man muss sie nur aktivieren.

In den meisten Unternehmensbereichen ist Verschlüsselung gang und gäbe. Wenn es jedoch um die VoIP-Telefonanlage geht, denken die wenigsten über eine wirksame Verschlüsselung nach. Obwohl es seit vielen Jahren Protokolle und Standards zur Verschlüsselung der Sprachdatenströme gibt, werden sie nur selten eingesetzt. Unverschlüsseltes Voice over IP bedeutet: Jeder, der Zugriff auf den Datenübertragungspfad zwischen VoIP-Telefon und VoIP-Server hat, kann ohne Aufwand das Gespräch mithören oder aufzeichnen.

Standards und Protokolle

Voice over IP bedeutet grundsätzlich nur, dass Sprache digital über das Internet-Protokoll übertragen wird. Dem All-over-IP-Ansatz folgend, wurden viele Techniken, die eigene Verfahren für die digitale Sprachübertragung nutzen, wie zum Beispiel ISDN in die einheitliche Übertragung per IP-Netz überführt. Neben Herstellern wie Cisco (SCCP), Mitel (MiNET), Nortel (UNIStim) oder Siemens (CorNet-IP), die eigene Protokolle für VoIP nutzen, gibt es auch offene Standards wie IAX2 oder das veraltete H.323. Aktuell gilt das Session Initiation Protocol (SIP) als Quasi-Standard. Es wurde 1999 von der Internet Engineering Task Force (IETF) als Spezifikation RFC 2543 entwickelt. Schon 2002 begann aber mit RFC 3261 eine lange Reihe von Erweiterungen, die das Protokoll unter anderem um Verschlüsselungsstandards erweitert hat.

SIP ist jedoch nur die Basis der VoIP-Kommunikation; es wird nur zum Aufbau, zur Steuerung und zum Abbau einer Sitzung verwendet. Ist die Sitzung einmal ausgehandelt, wird das Medium (zumeist eben: Sprache) als kontinuierlicher Strom aus UDP-Paketen mittels RTP-Protokoll übertragen.

Schlüsselaustausch und Zertifikate

Diese Aufgabenteilung hat viele Vorteile. Wenn man allerdings auf Verschlüsselung aus ist, erkennt man schnell, dass nur eine Absicherung beider Protokolle für Schutz sorgen kann. Sichert man nämlich nur den Medienstrom durch die Secure-Erweiterung SRTP ab, schützt man sich an dieser Stelle zwar grundsätzlich vor Manipulation und Abhören. Doch bei genauerer Betrachtung wird deutlich, dass die Funktionsweise von SRTP den SIP-Kanal mit einbezieht. Die symmetrischen Schlüssel, die für die Codierung des Medienstroms ausgehandelt werden, tauschen die Kommunikationspartner im Klartext per SIP miteinander aus. Ein Angreifer müsste also nur den Schlüssel aus den SIP-Nachrichten extrahieren und wäre dann in der Lage, den SRTP-Datenstrom zu entschlüsseln.

Glücklicherweise hat man auch das SIP-Protokoll um einen Secure-Zusatz erweitert: Das SIPS-Protokoll setzt wie HTTPS, POPS oder IMAPS auf das TLS-Protokoll. Um eine gesicherte Verbindung aufzubauen, müssen auch bei TLS die symmetrischen Schlüssel ausgetauscht werden. Mit einem cleveren Trick umgeht TLS aber die Gefahr des Abhörens, da es die asymmetrischen Schlüssel der SSL-Zertifikate nutzt, um diesen Schlüsselaustausch zu chiffrieren.

Kombiniert man also SIPS mit SRTP, erreicht man eine lückenlose Verschlüsselung, die nach heutigem Stand der Technik höchste Sicherheit bietet. Sowohl SRTP als auch das auf TLS basierende SIPS setzen auf AES, das ab einer Schlüssellänge von 128 Bit zurzeit als sicher gilt. Man erreicht daher mit SRTP in Kombination mit SIPS eine vollständige Verschlüsselung der Kommunikation.

Ein weiterer Vorteil der Verschlüsselungsmechanismen ist, dass sie die Identitäten der Kommunikationspartner sicherstellen. Man-in-the-Middle- und Denial-of-Service-Angriffe sind in einer SIPS/SRTP-Kommunikation um ein Vielfaches schwieriger umzusetzen als in Klartext-SIP/RTP-Umgebungen.

SIPS und SRTP aktivieren

Standards und Protokolle gibt es. Clients und Server können verschlüsseln. Es wäre also kein Problem, VoIP-Gespräche konsequent abzusichern. Wie einfach es ist, SIPS und SRTP zu aktivieren, soll am Beispiel der gängigen Kombination von Asterisk und Snom-Telefonen gezeigt werden.

Eine Asterisk-Anlage ab Version 1.8 als SIP-Server unterstützt sowohl TLS als auch SRTP. Mittels einer Änderung in der Konfigurationsdatei sip.conf ist die Arbeit hier fast schon getan. Bevor man TLS aktivieren kann, braucht man, wie bei einem Apache-Webserver, ein SSL-Zertifikat mit passendem SSL-Key. Zum Testen reichen auch die Snakeoil-Beispielzertifikate, die die meisten Linux-Distributionen mitbringen. Debian und Ubuntu zum Beispiel bringen die beiden Dateien /etc/ssl/certs/ssl-cert-snakeoil.pem (Zertifikat) und /etc/ssl/private/ssl-cert-snakeoil.key (Key) mit. Möchte man prinzipiell mit selbst signierten Zertifikaten arbeiten, kann man mit dem Paket ssl-cert auch eigene Zertifikate erstellen. Da Asterisk darauf besteht, den privaten

Schlüssel zusammen mit dem Zertifikat in einer .pem-Datei übergeben zu bekommen, erstellt man diese kurzerhand mit den folgenden zwei Aufrufen:

```
cat /etc/ssl/private/ssl-cert-snakeoil.key > /etc/asterisk/asterisk.pem
cat /etc/ssl/certs/ssl-cert-snakeoil.pem > /etc/asterisk/asterisk.pem
```

In der /etc/asterisk/sip.conf fügt man die folgenden vier Zeilen ein:

```
tlsenable=yes
tlsbindaddr=0.0.0.0:5061
tlscertfile=/etc/asterisk/asterisk.pem
encryption=yes
```

Dadurch erhält Asterisk die Anweisung, auch TLS-Verbindungen an allen Interfaces auf dem Standardport 5061 entgegenzunehmen. Das dafür nötige SSL-Zertifikat samt SSL-Key übergeben wir in der Datei asterisk.pem. Und die Anweisung encryption=yes veranlasst Asterisk, alle von ihm ausgehenden Einladungen (invites) mit SRTP-Anforderung zu verschicken. Damit sind nach einem Asterisk-Reload TLS und SRTP generell aktiviert.

Für jede Nebenstelle muss nun noch der transport auf tls gesetzt werden, um dies auch zu forcieren. Für ein Snom-Telefon sähe der Gerätekonfigurationsabschnitt in der sip.conf so aus:

```
[snom]
type=friend
callerid=snom
context=from-sip
defaultuser=snom
secret=password
host=dynamic
transport=tls
```

Am Snom-Telefon richtet man eine reguläre Identität ein und trägt zusätzlich den Asterisk-Server unter Outbound Proxy in diesem Format ein: asterisk.server.ip;transport=tls, wobei asterisk.server.ip mit dem Eintrag unter Registrar identisch sein muss. Im Reiter RTP der Identität reicht es „RTP Verschlüsselung: An“ zu setzen (was mittlerweile sogar der Default bei Snom-Telefonen ist) und die Einrichtung ist erledigt. Probiert man jetzt einen Echo-Testanruf auf der 600 (Asterisk-Default-extensions.conf), kann man im Snom-Telefondisplay ein kleines Vorhängeschloss entdecken. Dies ist das Zeichen dafür, dass die vollständige Verschlüsselung aktiv ist.

Probe aufs Exempel

Mittels Wireshark oder tcpdump kann man einfach nachweisen, auf welchem Port und mit welchem Protokoll die Kommunikation zwischen SIP-Client und SIP-Server stattfindet. Ruft man auf dem Asterisk-Server

```
tcpdump -nqt -s 0 -A port 5061
```

auf, sieht man nur kryptische Zeichenketten – also genau das, was wir wollen. Zum Vergleich kann man das Snom-Telefon ohne den Outbound Proxy und die Asterisk-sip.conf ohne transport=tls konfigurieren. Ruft man nun

```
tcpdump -nqt -s 0 -A port 5060
```

auf, kann man die SIP-Nachrichten in Klartext mitlesen. Das Gleiche gilt auch für den SRTP-Datenstrom – ruft man

```
tcpdump -nqt -s 0 -A dst portrange 10000-20000
```

auf, kann man mit und ohne Verschlüsselung zwar nur wilde Zeichenketten sehen. Bei eingeschaltetem SRTP sieht man jedoch noch nicht einmal die IP-Header, in denen die Quell- und Ziel-IP-Adressen stehen.

K.-o.-Kriterium für Firmenanlagen

Obwohl Standards, Techniken und Endgeräte ausgereifte und durchgehende VoIP-Verschlüsselung bieten, wird sie nur selten aktiv genutzt. Aus genau diesem Grund hat zum Beispiel vio:networks als Anbieter von Cloud-Telefonanlagen die vollständige Verschlüsselung zum Standard gemacht. Es liegt letztlich an den IT-Verantwortlichen, bei der Ausschreibung Sicherheitsstandards wie SIPS und SRTP zum Entscheidungskriterium einer VoIP-Anlage zu machen.

Dominik Mauritz
vio:networks GmbH

Abhörsichere ISP-Aggregate

Netzbündelung kann die Datenkommunikation auch bei Lastspitzen aufrechterhalten.

Modular angelegte Multichannel VPN Hubs fassen unterschiedliche Zugangstechnologien zu einem redundant ausfallsicheren Unternehmensnetz zusammen. Anwendern steht die Summe der gebündelten Bandbreite zur Verfügung, Angreifer können mit dem fragmentierten und verschlüsselten Datenverkehr nichts anfangen.

Seit der Erfindung des Internets ist der Anteil von sicherheitsrelevanten Verbindungen gewaltig gewachsen – beim Bezahlen mit Kredit- oder EC-Karte, beim Finanztransfer, auf dem Smartphone, bei Sensoren oder bei der alltäglichen Unternehmenskommunikation. Überall kommt es auf eine zuverlässige und sichere Anbindung an – nahezu jeder Ablauf auf IP-Basis ist heute abhängig von einer nahezu hundertprozentigen Verfügbarkeit und Abhörsicherheit der Informationen. Technisch ist dies in der Praxis durchaus möglich: durch die Nutzung mehrerer Zugangsmedien zur selben Zeit, also durch Bündelung von Internet-Verbindungen.

Die Bündelung bewirkt zunächst, dass beim Ausfall eines Mediums die Konnektivität nicht abbricht, sondern erhalten bleibt, weil der Datenstrom über andere, noch bestehende Verbindungen geht. Zwar vermindert sich dann die Bandbreite um den weggefallenen Kanal, aber der Datenstrom wird insgesamt nicht unterbrochen.

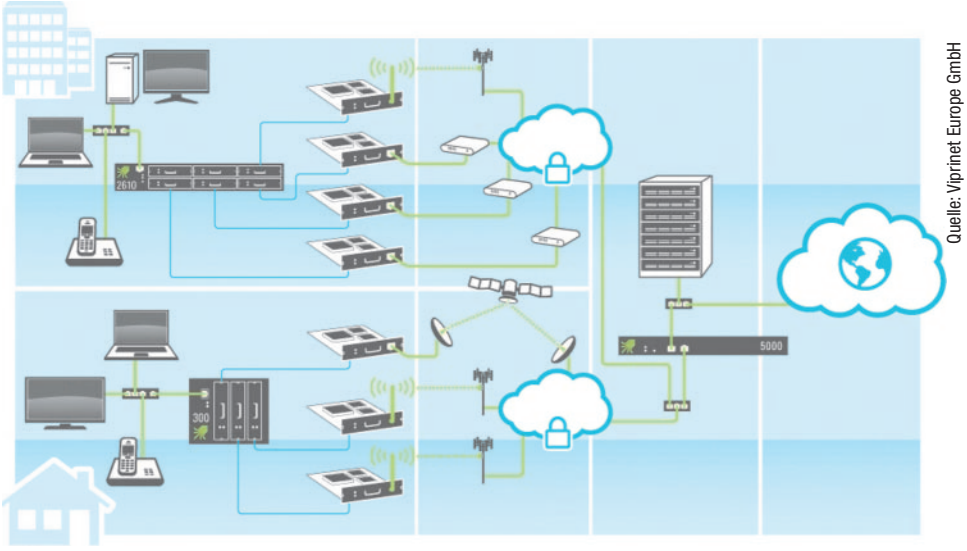
Ausfallsicherheit durch Risikoverteilung

So ist es möglich, alle verfügbaren Internet-Zugangswege eines Standorts in einem speziellen Router zu aggregieren. Dies können zum Beispiel ein DSL-Anschluss von Provider A, ein DSL-Anschluss von Provider B, ein Kabelanschluss, eine UMTS-Verbindung von Provider C, eine LTE-Verbindung von Provider D und eine Satellitenverbindung sein. Falls nun, aus welchen Gründen auch immer (Beschädigung des Kabels, Ausfall eines Rechenzentrums, Überlastung eines Provider-Netzes etc.), der DSL-Anschluss von Provider B wegfällt, würde der Datenverkehr einfach über die weiterhin bestehenden mobilen oder kabelgebundenen Verbindungen der anderen Provider abgewickelt. Anders als beim Load Balancing wird dabei der Datenstrom nicht unterbrochen, sondern aufrechterhalten und mit verringerter Bandbreite weiter übertragen. Dies geht theoretisch so lange, bis keine funktionierende Verbindung mehr verfügbar ist.

Technisch lassen sich hierbei alle aktuell bekannten Zugangsmöglichkeiten nutzen; hierzu wird ein geeigneter Router einfach mit den jeweiligen WAN-Modulen bestückt. Durch die modulare Nutzung sind solche Geräte gleichzeitig für zukünftige technische Entwicklungen gerüstet: Bei der Einführung neuer Übertragungsstandards muss nicht das gesamte Gerät erneuert werden, sondern es genügt, wenn ein Modul getauscht wird.

Echte Bündelung aller WAN-Links

Durch diese Bündelungstechnik ist es außerdem möglich, die Vorteile einzelner Verbindungen gezielt zu nutzen und die Nachteile anderer Verbindungen auszuschließen. So lassen sich in einem entsprechenden Router softwareseitig verschiedene Einstellungen zur Optimierung des Gesamtsystems vornehmen. Beispielsweise kann man die Grundlast des Datenaufkommens über kostengünstige und nicht volumenbeschränkte DSL-Verbindungen leiten; erst wenn Lastspitzen auftreten, schalten die teureren LTE-Verbindungen dazu. Das gleiche Prinzip



Quelle: Viprinet Europe GmbH

Das Hauptbüro bündelt mit einem Viprinet Multichannel VPN Router 2610 drei DSL-Anschlüsse und einen UMTS-Zugang. Der Router baut seinen VPN-Tunnel zu einem Multichannel VPN Hub im Rechenzentrum auf. Das Nebenbüro ist mit einem VPN Router 300 angebunden (Abb. 1).

Quelle: Viprinet Europe GmbH

Multichannel VPN Router 2610 mit sechs Slots für Module (Abb. 2)

Quelle: Viprinet Europe GmbH

Der zentrale Hub 5000 zum Einbau im Rechenzentrum (Abb. 3)

greift, wenn man zum Beispiel teure Satellitenverbindungen nur als Redundanz im Notfall nutzen will oder wenn für empfindliche Anwendungen wie Videokonferenzen Satellitenverbindungen mit hohen Latenzen außen vor bleiben sollen.

Spezielle Bündelungsrouter ermöglichen zusätzlich eine Traffic-Priorisierung. Das heißt, dass man im Unternehmen festlegen kann, welche Art von Datenverkehr bevorzugt behandelt werden soll. Ein weiterer positiver Effekt der Bündelung ist schließlich der, dass durch die Aggregation der Verbindungen auch in schlecht versorgten Gebieten eine vernünftige Bandbreite zur Verfügung steht – und das ohne die hohen Kosten einer Standleitung.

Verschlüsseltes VPN-Netzwerk

Die Funktionsweise der Bündelung lässt sich anhand einer Infrastruktur aus Multichannel-VPN-Routern und Hubs folgendermaßen darstellen: Jeder angeschlossene Router baut über jede der angeschlossenen Leitungen einen verschlüsselten VPN-Tunnelkanal zu einer zentralen Gegenstelle, dem Hub, auf (Abb. 1). Diese VPN-Tunnelkanäle werden zu einem Gesamttunnel gebündelt, durch den dann die eigentliche Datenübertragung erfolgt. Gesichert sind die Tunnel mit einem nach heutigem Stand der Technik nicht entschlüsselbaren AES-256-Bit-Verfahren. Der Austausch der Schlüssel erfolgt über das Diffie-Hellman-Verfahren, das Perfect Forward Secrecy gewährleistet.

Der Multichannel VPN Hub, der üblicherweise in einem hochausfallsicheren Rechenzentrum platziert ist, fungiert als Vermittlungsstelle: Daten mit Ziel in einer anderen Niederlassung werden über den zugehörigen VPN-Tunnel weiter versandt. Daten mit Ziel im öffentlichen Internet werden hingegen entschlüsselt und in Richtung des Ziels weitergeleitet. Der Hub sorgt für eine sichere und schnelle Kommunikation der Router untereinander, dient aber zugleich auch als zentraler Austauschpunkt zwischen dem verschlüsselten VPN und dem öffentlichen Internet oder dem Unternehmensnetzwerk.

Sichere Standortvernetzung

Dieses Prinzip der gebündelten Nutzung bringt einen deutlichen Sicherheitsgewinn. Denn alle Datenpakete werden zunächst zum Versand über mehrere Datenleitungen „zerhackt“ und dann für jede Leitung separat verschlüsselt. Es transportiert in dieser Architektur also kein einzelnes Provider-Netz jemals einen vollständigen Nutzdatenstrom. Das bedeutet: Selbst wenn ein Angreifer in der Lage wäre, die Verschlüsselung der Pakete auf ihrem Transportwege zu knacken, erhielte er nur Bruchteile der Daten. Um sinnvolle Informationen zu

stehlen, müsste er alle Pakete in den unterschiedlichen Betreibernetzen zugleich abfangen und zuordnen.

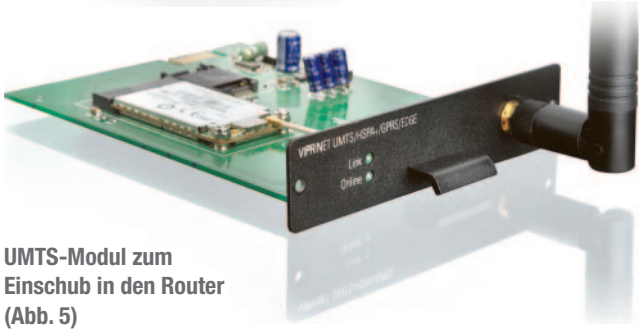
Vertrauen und Kontrolle

Mit einer derartigen Router-Hub-Infrastruktur können Unternehmen eine sichere Kommunikation selbst mit ihren Zulieferbetrieben einrichten: Diese müssen nur einen Router nutzen, der auf den gleichen Hub terminiert, über den auch die Unternehmenskommunikation abläuft. Wer innerhalb dieses „privaten Netzes“ auf welche Datenströme zugreifen kann, lässt sich feingranular konfigurieren. Dabei können die Zulieferer nach Bedarf dauerhaft oder zeitlich befristet eingebunden werden.

Voraussetzung dafür, dass die übertragenen Daten vertraulich und sicher bleiben, ist natürlich ein Produkt, das keine versteckten Hintertüren, von wem auch immer, verbirgt. Ein entscheidender Punkt bei der Auswahl der Hersteller sollte deshalb sein, dass der Anbieter garantieren kann, die komplette Fertigungskette unter Kontrolle zu haben. Nur so kann er ausschließen, dass die Lösung in irgendeiner Weise kompromittiert ist. Die Erfahrung hat gezeigt, dass dies eigentlich nur bei Produkten made in Germany möglich ist.

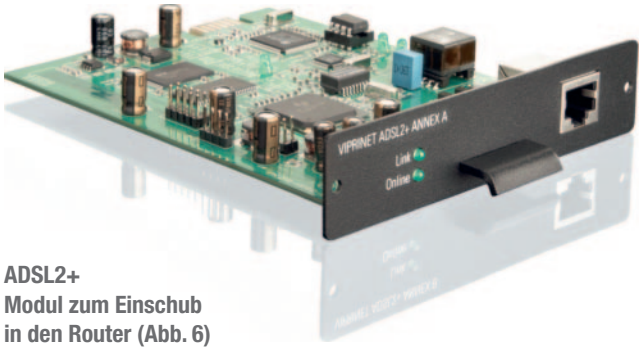
Quelle: Viprinet Europe GmbH

Fahrzeugrouter 500 mit vier integrierten UMTS-Modems (Abb. 4)



Quelle: Viprinet Europe GmbH

UMTS-Modul zum Einschub in den Router (Abb. 5)



Quelle: Viprinet Europe GmbH

ADSL2+ Modul zum Einschub in den Router (Abb. 6)

Mit mobilen Routern, die vorrangig die unterschiedlichen Mobilfunknetze und -standards nutzen, ist auch die Anbindung der Außendienstler gewährleistet. So haben die Mitarbeiter im Feld einen breitbandigen Zugriff auf das Unternehmensnetzwerk und senden Schadensmeldungen oder Bestandsaufnahmen direkt, zum Beispiel per Videostream, an die Zentrale. Bei komplizierten Aufgaben oder Schwierigkeiten vor Ort können sich auf diese Weise Experten in der Niederlassung live zuschalten. Dadurch können diese Fachkräfte wesentlich effektiver eingesetzt werden, da ihnen der Fahrweg erspart bleibt. Auch für die sichere Anbindung eines Heimarbeitsplatzes ist die Bündelung geeignet.

Einzelhandel und Telemedizin

Die Bündelungstechnologie lässt sich in einer Vielzahl von Szenarien einsetzen. Neben der hochsicheren Unternehmensvernetzung hat sich die Anbindung von Kassensystemen im Einzelhandel oder bei Tankstellenbetreibern als wichtiges Einsatzfeld etabliert. Zum einen wird so, gerade dort, wo der ländliche Raum mit Breitband schlecht versorgt ist, eine vernünftige Anbindung geschaffen, die auch für Warenwirtschafts- und PoS-Systeme, Alarmsysteme, VoIP oder Mitarbeiterschulungen via Videokonferenz tauglich ist. Viel wichtiger ist aber, dass sich damit eine ununterbrochene bargeldlose Bezahlung sicherstellen lässt. Die betreffenden Unternehmen vermeiden direkte Umsatzeinbußen durch Downtime und sind normalerweise in der Lage, die Anschaffungskosten der Gräte rasch zu refinanzieren.

Auch in der Telemedizin ist eine sichere und immer verfügbare Internet-Anbindung von großer Bedeutung. Netzbündelung macht es letztlich möglich, Patienten früher aus dem Krankenhaus zu entlassen und zu Hause weiter zu betreuen. Für den Patienten bedeutet dies, dass er sich im Kreis seiner Familie wesentlich besser erholen kann. Das Gesundheitssystem hingegen kann Einsparungen durch die Reduzierung von teuren stationären Klinikbetten erreichen.

Der mobile Einsatz per Videostream in Krankenwagen hinwieder gibt Notfallopfern eine signifikant höhere Überlebenschance. Durch die Zuschaltung von Fachärzten aus der Klinik bereits im Krankenwagen profitieren Patienten sofort von der bestmöglichen Erstversorgung. Gleichzeitig können in der Klinik schon alle nötigen Vorbereitungen für weitere medizinische Maßnahmen getroffen werden.

Kommunikation im Notfall

Auch bei anderen Blaulichtorganisationen wie Polizei oder Feuerwehr ist eine zuverlässige mobile Internet-Anbindung Voraussetzung der bestmöglichen Beurteilung der Lage im Katastrophenfall. Hierbei sind besonders Videoübertragungen in Echtzeit zur Einsatzleitstelle oder die Koordination der Einsatzkräfte zu nennen. Die Tragödie der Love-Parade 2010 hat gezeigt, was passieren kann, wenn bei Großveranstaltungen die Kommunikation der Einsatzkräfte nicht in einem ausreichenden Maß funktioniert.

Die Anbindung von Fahrzeugen erfordert eine hohe Flexibilität, wenn sich Fahrzeuge bewegen und die Verbindung von Funkzelle zu Funkzelle ständig neu aufgebaut werden muss. Dabei muss diese gleichzeitig den permanenten Wechsel zwischen unterschiedlichen Mobilfunkstandards (GPRS, UMTS, LTE) bewältigen. Speziell entwickelte Fahrzeugrouter sind hier die weitaus bessere Lösung als die verbreitete Praxis, einen UMTS-Stick zu nutzen. Neben der unterbrechungsfreien Verbindung ist so auch eine ausreichende Bandbreite für mehrere Passagiere möglich.

Tobias Frielingsdorf
Head of Press & PR, Viprinet Europe GmbH

Mobilität, Mensch, Maschine

Unternehmen und IT im Wandel

heise Events-Konferenz

Top-Referenten + praxisnah

Foto: © zentilia + tanatat – Fotolia.com

Der nächste Schritt zum mobilen Arbeitsplatz der Zukunft

Smartphones, Tablets und ultraportable Notebooks sind aus dem Alltag nicht mehr wegzudenken. Der rasante Wandel zwingt Unternehmen zur Neugestaltung von Arbeit und Arbeitsplätzen. Dabei greift der herkömmliche Ansatz, mobile Geräte noch immer wie stationäre Clients zu behandeln – restriktiv, zentral organisiert und abgesichert –, zu kurz.

Auf der heise Events-Konferenz erhalten Sie Denkanstöße & Best Practices für den nächsten Schritt zur Entwicklung des mobilen Arbeitsplatzes der Zukunft.

Unsere Experten erläutern Ihnen dabei anhand von Fallbeispielen einen ganzheitlichen Ansatz vom Device zum Workplace Management. Dieser eröffnet nicht nur neue Chancen, durch optimale Arbeitsbedingungen auch die Attraktivität des Unternehmens für die Mitarbeiter zu erhöhen, sondern fördert auch das Potenzial der Mitarbeiter und eine zukunftsfähige IT-Architektur zum strategischen Nutzen der Firma zu verbinden.

Zielgruppe: Entscheider Strategie- und Unternehmensentwicklung; Technische Entscheider, IT-Manager- und -Berater

Teilnahmegebühr: 475,- Euro

Programmschwerpunkte:

- **Arbeitstypen der Zukunft**
  Dipl.-Psych. Jürgen Wilke, Fraunhofer-Institut für Arbeitswirtschaft
- **Cyber Physical Systems – Mobil und wissensbasiert**
  Prof. Dr.-Ing. Thorsten Schöler, Fakultät für Informatik der Hochschule für angewandte Wissenschaften Augsburg
- **Die Firma auch nach Feierabend in der Hosentasche**
  Peter Meuser, iTlab Consulting

Ihre Benefits:

- Hochkarätige Referenten
- Praxisrelevanz der Vorträge
- Networking und Erfahrungsaustausch
- Begleitende Ausstellung mit Informationen über die neuesten IT-Lösungen & -Produkte

Goldsponsoren: CORTADO, F-Secure, magic OUTPERFORM THE FUTURE

Silbersponsoren: Check Point SOFTWARE TECHNOLOGIES LTD., Samsung KNOX

Organisiert von: heise Events

In Zusammenarbeit mit: brainworks

Weitere Informationen und Anmeldung unter: **www.heise-events.de/momema2014**
Krypto-Kampagne: **www.ct.de/pgp**

Internet of Everything mit 10 GBit/s

Die fünfte Mobilfunkgeneration 5G verspricht drahtloses Internet mit 10 GBit/s auf Smartphones, Tablets, Laptops und in Autos. Ab 2020 soll der kommerzielle 5G-Rollout starten.

Das aktuelle 4G-LTE schafft Peaks von 50 MBit auf dem Lande, 100 bis 150 MBit in vielen größeren Städten und bis zu 500 MBit in vereinzelten Feldtests. Der Nachfolger 5G verspricht Peaks bis 10 GBit ab 2020 auf jedes Handy. Das wäre tausendmal schneller als das zurzeit ausgerollte LTE-Cat3 mit 100 MBit.

Das bedeutet: Mit 5G dürfte der User ab 2020 einen kompletten Spielfilm binnen weniger Sekunden auf sein Handy, Tablet, Notebook oder ins Auto bekommen. Der 4G-Nachfolger ist zwar noch nicht ganz funktionsfähig, aber wo sich die Fachwelt trifft, wird er seit Anfang 2014 zunehmend diskutiert.

Optionshandel auf die Mobilzukunft

Auf dem Mobile World Congress 2014 in Barcelona war 5G das Modethema der EU-Politiker. Zwei Wochen später sagte der britische Premierminister David Cameron bei der CeBIT-Eröffnungsfeier mit Kanzlerin Dr. Angela Merkel, dass Deutschland und das Vereinigte Königreich bei der Entwicklung des 5G-Internets kooperieren wollen: Die Technische Universität Dresden, das King's College in London und die Universität von Surrey in Südostengland sollen gemeinsam an 5G forschen. Europa hat immerhin GSM, UMTS und LTE maßgeblich entworfen und will sich jetzt bei 5G nicht von den Asiaten abhängen lassen.

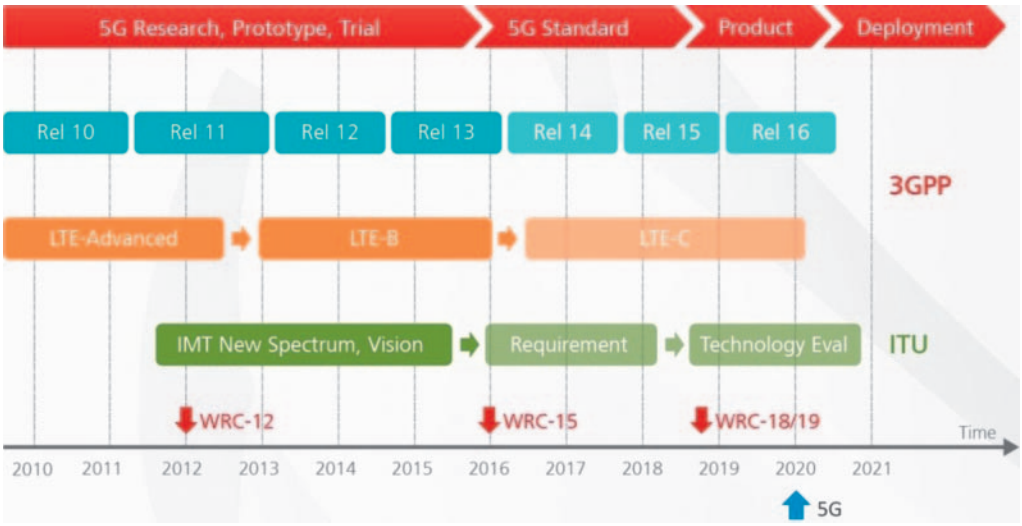
Strategische Zusammenarbeit

Doch wie kann 5G technisch einen solchen Sprung auf 10 GBit/s machen? Das erklärte der chinesische Vorzeigekonzern Huawei schon vor den beiden Megamessen auf dem 5G@Europe Summit 2014 im Sofitel Hotel München. Dazu hatte Huawei die klügsten Wireless-Köpfe aus Europa, Asien und Nordamerika geladen, etwa Forscher und Vorstände europäischer Netzbetreiber wie Vodafone, Telekom und Telefonica, namhafte EU-Politiker, führende Wireless-Professoren und innovative Automobilhersteller. Sogar Huawei-Konkurrenten wie Alcatel, Ericsson und NSN durften nach Bayern kommen. Denn je schneller sich Ausrüster, Telcos und Anwender gemeinsam auf die

Quelle: Huawei Technologies Co., Ltd.

5G soll 10 GBit/s auf jedes Endgerät bringen und 100 Milliarden Mobilfunk-Connections gleichzeitig ermöglichen. Dazu müssen die Telcos viel mehr Antennen als bei 4G aufstellen und ein gewaltiges Frequenzspektrum von 300 MHz bis zu 300 GHz nutzen dürfen (Abb. 1).

Zurzeit ist 5G noch im Stadium der Forschung und der frühen Prototypen. Ab 2016 will man die 5G-Standards definieren. Ab 2019 soll es kommerzielle 5G-Systeme und -Geräte für Pilotprojekte und Friendly User Trials bei den Telcos geben. Ab 2020 soll 5G in den Flächen-Rollout gehen (Abb. 2).



Quelle: Huawei Technologies Co., Ltd.

neuen 5G-Standards einigen, desto früher können sich neue Märkte rund um 5G entwickeln.

Bis die neuen 5G-Standards vollends definiert sind, arbeiten die Konkurrenten vorübergehend und partiell zusammen. Doch spätestens mit der kommerziellen 5G-Einführung sind sie dann wieder scharfe Konkurrenten. So ähnlich war das auch schon bei 2G, 3G, 4G. Neu ist jetzt nur, dass nicht mehr altverdiente GSM-UMTS-Pioniere wie Siemens, Nokia, Ericsson, Alcatel oder NSN ganz vorneweg marschieren, sondern zunehmend Asiaten wie Huawei, LG, Samsung oder ZTE den 5G-Fortschritt mit anschieben.

5G soll ab 2020 die tausendfache Wireless-Kapazität in die Mobilfunknetze bringen. Das ermöglicht dann 100 Milliarden Mobilfunkverbindungen für Menschen und Maschinen gleichzeitig. 10 GBit auf jedem Endgerät. Pings unterhalb von einer Millisekunde. 90 Prozent weniger Energieverbrauch pro Mobilfunkdienst. Tausendmal weniger Energieverbrauch pro übertragenem Bit in den Endgeräten, auch um deren Akkuverbrauch zu reduzieren. Und daraus resultierend: neue Anwendungen und Geschäftsmodelle rund um das drahtlose, superschnelle 5G-Cloud-Computing.

Mit tausendfacher Mobilfunkkapazität

Um 5G zu realisieren, braucht man neue Funkstationen und Endgeräte mit viel mehr MIMO-Antennen als heute, eine viel höhere geografische Dichte von Basisstationen mit viel kleineren Funkradien sowie viel breitere Frequenzspektren in der Luft als heute für LTE verfügbar sind, meint Dr. Wen Tong, der profilierteste 5G-Vordenker von Huawei, Inhaber von 180 US-Patenten und Chef von 700 Huawei-Forschern.

5G soll ein enormes Spektrum von 300 MHz bis 300 GHz flexibel nutzen können. Zum Vergleich: LTE nutzt in Deutschland gerade mal drei fixe Frequenzblöcke bei 800 MHz, 1800 MHz und 2600 MHz. Die restlichen 297 GHz sind für den terrestrischen Mobilfunk noch gar nicht aktiviert.

Ab wann weitere Frequenzen für das drahtlose Internet versteigert werden, ist nicht zuletzt eine Frage der Politik. Deshalb kamen auch mehrere EU-Politiker aus Brüssel zum 5G-Kongress nach München. Daneben wird auf der World Radiocommunication Conference 2015 (WRC-15) der ITU vom 2. bis 27. November 2015 in Genf eine größere Einigung über die Verwendung weiterer Frequenzbänder für das mobile Internet erwartet.

Der Endanwender soll mit 5G bis zu 10 GBit/s auf sein Endgerät bekommen. Das heißt: Glasfaserspeed beim Senden und Empfangen, nur eben per Mobilfunk. Mit so einem Durchsatz werden auch Videostreamings und Telekonferenzen in 4K-Ultra-HD-Qualität von Smartphone zu Smartphone möglich. Das gebogene Smartphone LG G Flex etwa hat schon heute eine Videokamera mit Ultra-HD-Aufzeichnung von 3840 × 2160 Pixeln. Will man den 4K-UHD-Stream aber mobil senden und empfangen, so braucht man dazu am besten drahtlose 5G-Netze.

Fortschritt macht Tempo

Zum Vergleich: UMTS kam anno 2004 mit 0,384 MBit/s auf den deutschen Markt. Die ersten Siemens-UMTS-Videohandys waren damals noch so dick wie eine Faust, hatten winzige und gering auflösende Videodisplays und wurden im Betrieb recht heiß. Doch danach ging es rasant weiter: HSDPA, HSUPA, HSPA, DC-HSPA und dann 4G-LTE.

LTE-Cat3-800-MHz wird seit Dezember 2010 mit bis zu 50 MBit/s auf dem Lande kommerziell ausgerollt. Dann brachte die Telekom LTE-Cat3-1800-MHz bis 100 MBit/s in über hundert deutsche Städte. Seit Herbst 2013 kommt auch LTE-Cat4 mit 150 MBit/s von Telekom und Vodafone auf den deutschen Markt. Auf dem Münchener Oktoberfestgelände 2013 zum Beispiel konnte der Autor schon 121 MBit/s Nettodownload messen, und zwar mit dem ersten lieferbaren LTE-Cat4-Smartphone überhaupt (Huawei Ascend P2) in einer LTE-Cat4-2600-MHz-Funkzelle von Vodafone.

Seit Ende 2013 wird auch LTE-Cat6 mit 225 MBit/s pilotiert: in München von O_2, in Dresden von Vodafone. Im November 2013 konnte der Autor netto 207 MBit/s mit einem LTE-Cat6-Prototypen von Huawei in zwei aggregierten Funkzellen von O_2 in München messen. Im weiteren Verlauf des Jahres 2014 wird man auch LTE bis 300 MBit im deutschen Felde sehen, allerdings nur an bestversorgten Standorten.

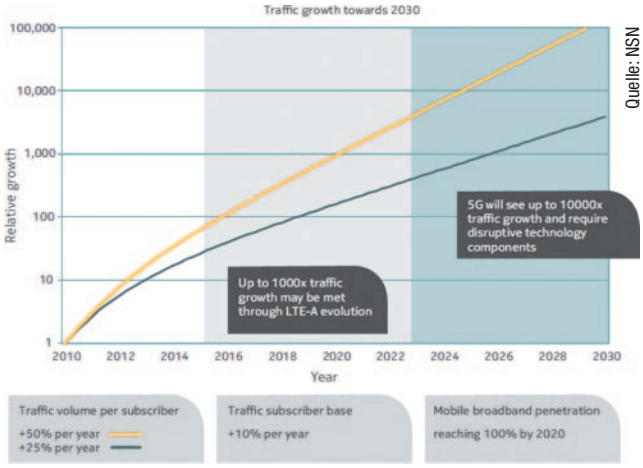
Natürlich sollen die neuen 5G-Techniken auch kreuz- und rückwärtskompatibel zu den heute verbreiteten Funksorten 3G, 4G und WiFi sein. Die meisten User wollen ja nicht ständig neue Endgeräte kaufen.

Pings unter einer Millisekunde

Die bisherige 5G-Forschung gibt Grund zur Annahme, dass man die Ping-Zeiten in Mobilfunknetzen auf unter eine Millisekunde drücken kann. Beim Surfen oder Business-Cloud-Computing würde sich das

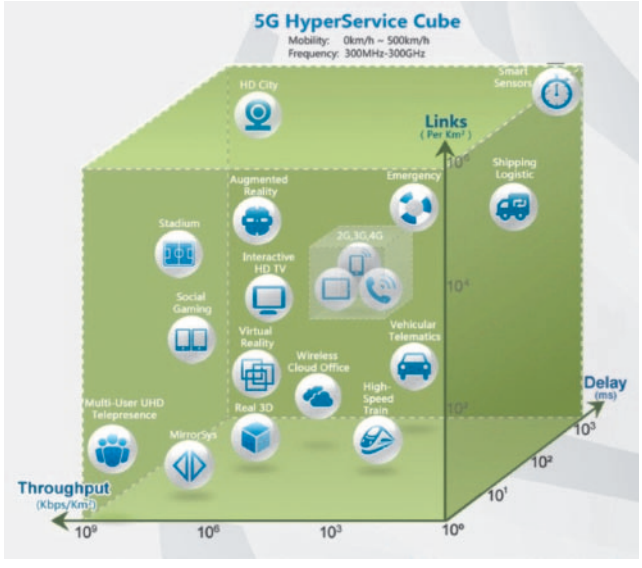
extrem zackig anfühlen und die Akzeptanz der Cloud vermutlich sehr verbessern. Bei der Wireless-Kommunikation zwischen schnell bewegten Fahrzeugen wären rasante Reaktionszeiten sogar noch wichtiger, um etwa Kollisionen zu vermeiden. Die heute in der Praxis üblichen LTE-Reaktionszeiten zwischen 30 und 80 Millisekunden fühlen sich beim Surfen zwar auch schon gut an, aber für schnelle Fahrzeuge mit automatischen Lenk- und Bremsauslösungen können die Reaktionszeiten gar nicht kurz genug sein.

5G-Reaktionszeiten unter einer Millisekunde gelten natürlich nur innerhalb des gleichen 5G-Funknetzes. Im mobilen Betrieb muss das Handy, die vernetzte Maschine oder das vernetzte Fahrzeug bis auf Weiteres auch noch zwischen (!) verschiedenen Funksorten wie 3G, 4G und WiFi hin- und herschalten. Solche Schaltvorgänge dauern heute manchmal mehrere Sekunden. Auch hier arbeiten Huawei und Konsorten auf ein „Zero-Second-Switching“ hin: Maximal 10 Millisekunden soll die Umschaltung zwischen 4G, 5G und WiFi in absehbarer Zukunft nur noch dauern, damit der User nichts mehr davon merkt. Das betrifft den gefühlten Gebrauch und ist nicht zu verwechseln mit den Ping-Zeiten innerhalb (!) der 5G-Netze, die wie gesagt unter eine Millisekunde kommen sollen.



Quelle: NSN

Der Datenverkehr im Internet wächst exponentiell. Ab 2020 wird LTE und LTE-Advanced an seine Kapazitätsgrenzen stoßen. Danach muss 5G das weitere Wachstum bedienen (Abb. 3).



Quelle: Huawei Technologies Co., Ltd., Februar 2014

Der 5G-HyperService-Würfel von Huawei zeigt, welche neuen Mobilfunkanwendungen welchen Durchsatz (Throughput) pro Quadratkilometer, welche Ping-Zeiten (Delay) in Millisekunden und wie viele Verbindungen (Links) pro Quadratkilometer benötigen. Der kleine Würfel innen zeigt die Leistungsgrenzen der heutigen 2G-3G-4G-Netze. Der große Würfel außen symbolisiert die Power von 5G (Abb. 4).

Mit Menschen, Dingen und Sensoren

Heute müssen die Mobilfunknetze weltweit etwa 5 Milliarden User always on verkraften. Die meisten nutzen Handys oder Smartphones. Dazu kommen mobilfunkbestückte Tablets, Laptops, Router, Surfsticks, Autos und Navigationssysteme, die aber nicht immer always on sind. In Zukunft sollen die Mobilfunknetze auch noch mehrere Milliarden Apps und mehrere Hundert Milliarden Sachen und Maschinen versorgen. Deshalb geht Huawei davon aus, dass die Menschheit bald eine tausendfache Mobilfunkkapazität benötigen wird, die nur noch mit 5G-Netzen abgefedert werden kann.

Das mobile Internet erlaubt im Prinzip Person-to-Person-, Person-to-Machine- und Machine-to-Machine-Kommunikation. In der ersten Stufe diente der digitale GSM-Mobilfunk seit 1992 überwiegend der Person-to-Person-Vernetzung von Mensch zu Mensch; anfangs geschah das auch nur via Sprache, aber seit dem Aufkommen von Facebook und Konsorten auch immer stärker mit Fotos und Videos, was den Mobilfunknetzen viel mehr Durchsatz abfordert.

Das Wachstum in der Handy-Sprachkommunikation scheint derweil zu stagnieren, aber der mobile Daten-Foto-Video-Hunger der Handy-Tablet-Laptop-Nutzer wird auch künftig weiter wachsen. Daher müssen die Netzbetreiber ihre Kapazitäten weiterhin drastisch hochfahren, um erstens aktuelle Engpässe zu beseitigen und zweitens das weitere Wachstum überhaupt noch bedienen zu können.

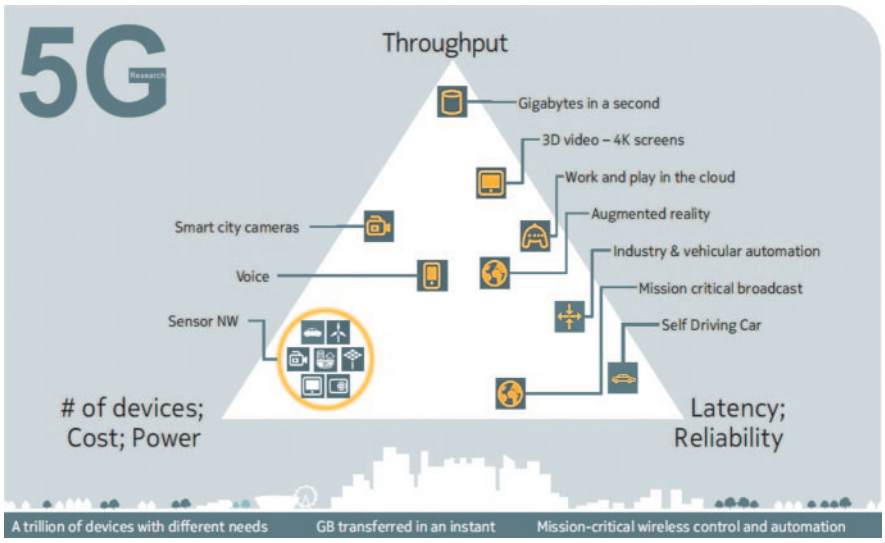
5G und IPv6 für das Internet of Things

Daneben dürften sich ganz neue Anwendungen bei der mobilen Vernetzung von Autos, Dingen, Sachen, Sensoren und Maschinen entwickeln. Die Branche spricht von Machine-to-Machine-Kommunikation (M2M), vom Internet of Things (IoT) oder wie Cisco gar vom Internet of Everything (IoE).

Huawei geht davon aus, dass bereits vor dem Rollout der 5G-Technik bis 2020 circa 50 bis 100 Milliarden Geräte vernetzt sein könnten. Damit steigt der Druck auf die 2G-3G-4G-Netze. 5G wird ab 2020 vielleicht gerade noch rechtzeitig kommen, um die älteren Netze zu entlasten.

Bei diesen neuen IoT-Milliardenmärkten bekommen nicht nur Telcos und deren Ausrüster, sondern auch klassische Netzwerker wie Cisco leuchtende Augen. Dank IPv6 könnten nämlich Hunderte Milliarden von Handys, Dingen und Maschinen eigene, sprich: unverwechselbare Internet-Adressen bekommen. Mit IPv4 dagegen herrscht schon heute IP-Adressenknappheit, die man mit Tricks und Kompromissen wie Network Address Translation umsegeln muss. IPv4 ist auf circa 4 Milliarden Adressen limitiert.

Prof. Dr. Hans D. Schotten vom Lehrstuhl für Funkkommunikation und Navigation an der TU Kaiserslautern zeigte das gigantische Potenzial der Vernetzung von Sachen, Fahrzeugen und Maschinen per



Quelle: NSN, April 2014

Die eierlegende 5G-Wollmilchsau aus Sicht von NSN soll enormen Datendurchsatz (oben), extrem kurze Reaktionszeiten (rechts) und eine gigantische Zahl an gleichzeitigen Mobilfunk-Connections ermöglichen (Abb. 5).

Mobilfunk: 8000 Frachtschiffe, 25 Millionen Container, 255 Millionen Autos, 345 Millionen Energiesensoren, 3,7 Millionen Verkaufsautomaten und last, but not least 110 Millionen Haustiere, die man ja ebenfalls mit winzigen Smartphones und GPS allzeit überwachen und betreuen könnte. Das heißt: Bald dürfte auch der Hund zu Weihnachten jedes Jahr ein neues Handy bekommen.

Vernetzung von selbstfahrenden Autos

Dr. Sebastian Zimmermann, Head of Automotive Connectivity and Security Solutions bei BMW, machte auf dem 5G@Europe Summit von Huawei klar, dass auch Autos in Zukunft so stark vernetzt sein werden, dass man die Kapazität der 5G-Netze brauchen wird. Wenn sich weitgehend automatisiertes Fahren, Augmented Reality im Head-up-Display auf der Windschutzscheibe, die automatische Erkennung von Fußgängern und Radlern im Interesse der Kollisionsvermeidung sowie Location-based Services im Auto durchsetzen sollen, wird man dazu enorme Wireless-Internet-Kapazitäten benötigen, die heutige Mobilfunknetze alleine gar nicht voll bedienen können.

Dr. David Soldani, Vice President Huawei European Research Centre und Head of Central Research Institute (CRI) im European Research Centre bei Huawei in München, erklärte am 5G-HyperService-Würfel, wie und warum 5G-Netze ganz neue Anwendungen möglich machen (siehe Abb. 4). Zum Beispiel wird man den hohen Speed, die hohe Verfügbarkeit, die enorme Kapazität und die rasanten Ping-Zeiten von 5G in unterschiedlichem Maße für Smart Cities, für intelligente und selbstfahrende Autos, für Hochgeschwindigkeitszüge, Augmented Reality, interaktives HDTV, Real 3D, Telemedizin und Rettungsdienste oder auch für Telepresence-Videokonferenzen in Ultra-HD-Auflösung benötigen.

5G-Know-how aus Shenzhen

Unterdessen ändert sich die ITK-Welt rasant: Amerikanische IT- und Netzwerkgiganten wie HP, IBM, Dell und Cisco kennt fast jeder. Europäische Mobilfunkausrüster wie Siemens, Nokia, Alcatel, Ericsson und NSN (vormals Nokia Siemens Networks) vermutlich ebenso. Chinesische Netzwerkkonzerne dagegen, vor allem Huawei, aber auch ZTE, sind in aller Stille als B2B-Lieferanten groß geworden. HP machte zuletzt einen Jahresumsatz von circa 112 Milliarden US-Dollar, IBM machte 99, Dell 56, Cisco 48, Huawei 39, NSN 14 und Alcatel-Lucent ebenfalls 14 Milliarden US-Dollar. Siemens wurde 1847 gegründet, Ericsson 1876, Alcatel 1898, IBM 1911, HP 1939, Dell und Cisco 1984, ZTE 1985 und Huawei 1988. Der jüngste Netzwerker wächst also mit am schnellsten.

Zurzeit unterstützt Huawei laut eigener Auskunft mehr als 500 Mobilfunknetzbetreiber und mehr als 2 Milliarden Mobilfunknutzer mit seiner 3G- und 4G-Technik. Auch in Deutschland ist Huawei seit Jahren still und effizient auf dem Vormarsch: Vodafone zum Beispiel investiert gerade zwei Milliarden Euro jährlich in die Netzmodernisierung. Dabei wird tonnenweise alte Siemens-Mobilfunktechnik aus dem Netz genommen und durch vielfach kleinere Huawei-Aggregate ersetzt. Auch andere Asiaten wie LG, NTT, Samsung oder ZTE haben enormes Know-how rund um den Mobilfunk aufgebaut. Die Chinesen nur als Copycats und Raubkopierer westlicher Technik zu sehen, wird der Realität schon länger nicht mehr ganz gerecht.

Zukunft und Gegenwart

Zunächst (2014) kommen jedenfalls erst einmal Netze und Geräte für LTE-Cat6 bis 300 MBit/s in den Rollout. Die entsprechenden Smartphones, Tablets, USB-Sticks und Router können sich mit zwei verschiedenen LTE-Funkzellen gleichzeitig verbinden. Mit dieser Dual-Carrier-Technik kann das LTE-Cat6-Gerät im besten Falle zweimal 150 MBit/s addieren (aggregieren), also $2 \times 150 = 300$ MBit/s downloaden. Daher spricht man auch von „Carrier Aggregation“ (CA).

300 MBit/s bekommt man aber nur, wenn beide LTE-Zellen jeweils die vollen 150 MBit/s leisten können, was hierzulande nur in den Frequenzbändern bei 1800 und bei 2600 MHz funktioniert. Koppelt man LTE 2600 dagegen mit LTE 800, so kommt man „nur“ auf $150 + 75 = 225$ MBit/s. Diese Kombination haben O_2 und Vodafone seit Ende 2013 kommuniziert, eben weil sie just über diese beiden Frequenzbereiche verfügen können.

Wenn ein Provider es darauf angelegt, kann er 2014 immerhin ein spezielles Firmengebäude mit LTE-Cat6 so gezielt bestrahlen, dass es die vollen 225 oder 300 MBit/s bekommt. Passende Router dürften in Kürze verfügbar werden. Auf dem Mobile World Congress 2014 in Barcelona wurde bereits ein Router für LTE Carrier Aggregation bis 300 MBit/s samt Gigabit-WLAN 11ac angekündigt: der E576. Von wem? Von Huawei.

Dr. Harald B. Karcher
freier Mobile-Communications-Tester

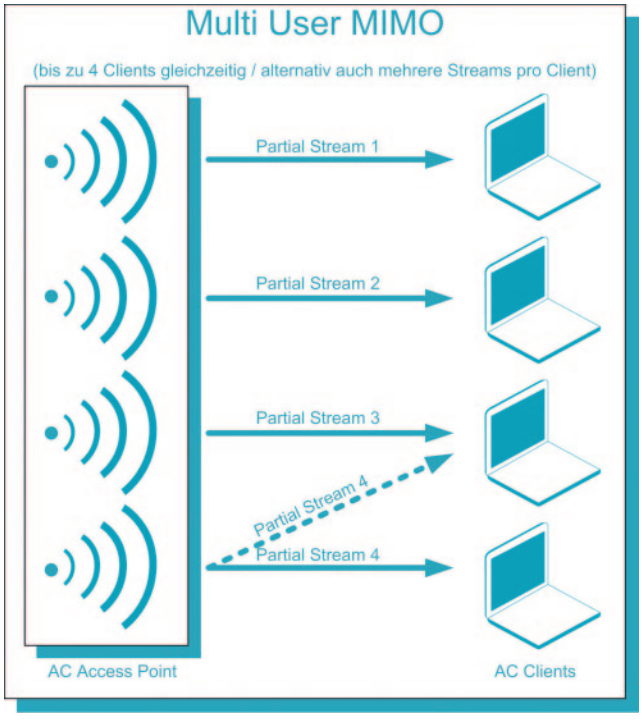
Stabiles Wireless auf 5 GHz

IEEE 802.11ac geht mit der Bandbreite flexibler um und stört sich nicht an konkurrierenden 2,4-GHz-Netzen.

Web- und Videoconferencing, Cloud Computing und Collaboration in Echtzeit bringen die bestehenden WLAN-Netzwerke in Bürogebäuden derzeit an ihre Grenzen. Dafür steht der Standard IEEE 802.11ac bereits in den Startlöchern: Er verheißt bessere Performance und weniger Interferenzen in komplexen Umgebungen.

Seit der Ratifizierung des 802.11-Standards (1997) mit zunächst 2 MBit/s haben sich WLAN-Netzwerkumgebungen stark weiterentwickelt. So stiegen die möglichen Bruttoübertragungsraten mit dem 802.11n-Standard auf bis zu 450 MBit/s. Mit der zunehmenden Anzahl von Clients wachsen allerdings auch die Anforderungen an die Bandbreite des oft bereits stark ausgelasteten Netzwerkes weiter.

Die Lösung bietet Wireless AC (IEEE 802.11ac), die mittlerweile fünfte Generation der WLAN-Netzwerkstandards, die eine deutlich schnellere und leistungsfähigere Funkverbindung möglich macht. Das IEEE (Institute of Electrical and Electronics Engineers) verabschiedete den neuen Standard im November 2013; mit der endgültigen Finalisierung ist in Kürze zu rechnen. Insbesondere für den privaten Einsatz sind bereits zahlreiche AC-fähige Geräte auf dem Markt, zunächst zwar meist in einer Draft-Version, doch lassen sich letzte Änderungen im finalen Standard problemlos per Firmware-Update aktualisieren. Nach und nach kommen auch Geräte für den Business-Einsatz hinzu.



Quelle: D-Link

Richtfunk für Access Points: MU-MIMO versorgt separate Geräte simultan mit unterschiedlichen Datenströmen.

Durchsatz bis 2,6 GBit/s

Eine der signifikantesten Neuerungen des Wireless-AC-Standards im Vergleich zur Vorgängerversion sind die bis zu vierfach schnelleren Datenübertragungsraten: Wo Wireless N auf maximal 450 MBit/s kommt, lassen sich mit AC bis zu 2,6 GBit/s erzielen. Dieser deutliche Sprung kommt in erster Linie durch die Ausweitung des Funkkanals zustande: Während die älteren Standards 802.11b und 802.11g lediglich 20 MHz nutzen, belegt der Nachfolger 802.11n bereits den 40-MHz-Block; mit 802.11ac verdoppelt sich der Funkkanal weiter auf 80 MHz oder sogar auf maximal 160 MHz.

Zum verbesserten Datendurchsatz trägt auch ein besseres Modulationsverfahren bei – die Quadraturamplitudenmodulation mit 256 Stufen (QAM256). QAM256 transportiert pro Übertragungsschritt 8 Bit, wohingegen die im Standard 11n maximal verwendete QAM64 lediglich 6 Bit erreicht.

Kaum Interferenzen

Im Gegensatz zu seinen Vorgängern arbeitet der Wireless-AC-Standard mit dem 5-GHz-Frequenzband. Dieses ist bei Wireless N bislang weitaus weniger verbreitet und daher auch weniger überlastet als das gängige 2,4-GHz-Band, auf dem die meisten Geräte funken. Auf dem 5-GHz-Band stehen theoretisch bis zu neun Kanäle bei 40 MHz Kanalbandbreite überlappungsfrei zur Verfügung, während im 2,4-GHz-Bereich höchstens drei Kanäle eingesetzt werden können. Für den praktischen Einsatz in stark ausgelasteten Büroumgebungen heißt das: deutlich weniger Interferenzen.

Optimierte Antennentechnik

Für die neue Höchstgeschwindigkeit sorgt außerdem eine neue Antennentechnik: MU-MIMO (Multi-User-Multiple-Input-Multiple-Output) bedeutet, dass die Technologie statt bislang vier nun bis zu acht gebündelte Datenströme an mehrere Empfänger gleichzeitig übertragen kann. Es ist genau diese gleichzeitige Übertragung, die wesentliche Vorteile gegenüber bisherigen WLAN-Infrastrukturen birgt, bei denen ein Access Point immer nur einen Client gleichzeitig bedienen konnte. Alle anderen Geräte im Funknetz mussten auf einen freien Übertragungsslot warten.

Standardmäßig kommt bei Wireless AC zudem die Beamforming-Technik zum Einsatz. Dabei werden über die Antennen exakt berechnete Funkwellen ausgesendet, die kontinuierlich wechselnden Bedingungen angepasst werden. So lassen sich auch Bereiche, die vorher

unter schlechter Erreichbarkeit litten, ganz gezielt mit schnellem drahtlosem Internet versorgen.

Überlappende Funkbereiche

Bei der Planung und Realisierung neuer Bereiche im Unternehmen ermöglicht der AC-Standard nicht nur eine bessere Performance, sondern durch neun überlappungsfreie Kanäle (bei einer Kanalbandbreite von 40 MHz) auch deutlich mehr Flexibilität. So profitieren Unternehmen ganz besonders von der AC-Technologie, wenn viele Clients im Netzwerk versorgt werden müssen, ohne dass dabei höchste Performance benötigt wird. Die Multi-User-MIMO-Funktion ermöglicht es, einzelnen Clients mehr Bandbreite zur Verfügung zu stellen. Einige AC Access Points bieten hierfür bereits spezielle Konfigurationsmöglichkeiten, die es bei den Wireless-N-Netzen noch nicht gab.

Netzwerk migrieren und anbinden

Bei WLAN-Infrastrukturen, die auf eine Wireless-AC-Lösung migriert werden sollen, spielen folgende Faktoren eine Rolle:

Vorhandene Clients: Der neue Wireless-AC-Standard ist abwärtskompatibel zu den älteren Standards 802.11a/b/g/n, was eine problemlose Integration der Clients in die neue Lösung ermöglicht. Da mit Wireless AC oft auch 5 GHz erstmals Einzug ins Unternehmensnetzwerk hält, können ältere Clients auf der 2,4-GHz-Frequenz verbleiben und neue AC-Clients das 5-GHz-Band nutzen.

LAN-Infrastruktur: Für eine performante Anbindung der Wireless AC Access Points muss das bestehende LAN über Gigabit-Anschlüsse verfügen; andernfalls bremsen vorhandene Fast-Ethernet-Anschlüsse unter Umständen den Datenverkehr aus. Vor diesem Hintergrund muss auch über eine entsprechend leistungsfähige Verbindung von Etagen zum Rechenzentrum nachgedacht werden. Hier kann Multilink-Aggregation mit mehreren Gigabit-Verbindungen eine Option sein.

Power over Ethernet: Ein weiterer Punkt, der in den LAN-Bereich fällt, ist die Stromversorgung der Access Points über PoE. Bislang war dies mit dem Standard 802.3af problemlos möglich, der maximal 15 Watt pro Port zur Verfügung stellt. Access Points nach 802.11ac benötigen zum Teil allerdings mehr Leistung (z.B. wegen leistungsstärkerer Prozessoren, mehr Funkmodulen und Ethernet-Ports), sodass 15 Watt nicht mehr ausreichen. Dann kommt der Standard 802.3at zum Einsatz, der pro Port bis zu 30 Watt bereithält und somit auch leistungshungrigere Access Points versorgen kann. Eventuell muss man bei einer Migration vorhandene PoE-Switches austauschen.

Stabil auf durchfunkten Etagen

Der neue AC-Standard wird derzeit hauptsächlich mit der höheren Bandbreite beworben. Dabei bietet er bei genauerem Hinsehen deutlich mehr: Es lässt sich mit Multi-User-MIMO eine größere Zahl an Clients gleichzeitig ansprechen; zudem kann man die höhere Bandbreite auf mehrere simultane Verbindungen aufteilen und so den einzelnen Clients mehr Performance zur Verfügung stellen. Und die Verwendung von 5 GHz ermöglicht einen verlässlicheren WLAN-Einsatz, auch in schwierigen Umgebungen mit vielen 2,4-GHz-Netzen. Nicht zuletzt bietet die Abwärtskompatibilität gute Migrationsmöglichkeiten für vorhandene Clients.

Christoph Becker
Senior Consultant Business Development & Product Marketing Management, D-Link (Deutschland) GmbH

Xirrus Wi-Fi Inspector im Test

In jedem Wireless-Netzwerk steckt noch etwas mehr drin. Aber wo genau?

Der Xirrus Wi-Fi Inspector ist ein kostenloses Werkzeug zur Überwachung, Verfeinerung und Optimierung von WLAN-Installationen. Im April 2014 lief er auf Windows 7, Vista und XP. Wir haben ihn unter realistischen Einsatzbedingungen mit Access-Points aus 13 Jahren getestet, von 802.11b (2001) bis 11ac (2014).

Um die Einsatzmöglichkeiten des Xirrus Wi-Fi Inspectors zu prüfen, nahmen wir mehrere WLAN-Basisstationen bzw. Access-Points (AP) aus den wichtigsten 802.11-Generationen der letzten 13 Jahre in Betrieb, und zwar einen 11b-AP von 3Com bis 11 MBit/s aus dem Jahr 2001, einen 11b/g-AP von 3Com bis 54 MBit/s (2003), einen 11a/b/g/n-Router AVM Fritzbox 7390 bis 300 MBit/s (2009), einen 11a/b/g/n/ac-Router Buffalo AirStation 1750 bis 1300 MBit/s (2012), einen 11a/b/g/n/ac-Router AVM Fritzbox 7490 bis 1300 MBit/s (2013) und einen aktuellen 11a/b/g/n/ac-Router Netgear R7000 AC1900 bis 1300 MBit/s (2014).

Daneben strahlten mehrere fremde WLAN-Router aus der Nachbarschaft in das Testbüro herein. So eine „Luftverschmutzung“ ist auch in anderen Büros meist unvermeidbar, besonders in dicht besiedelten Gebieten.

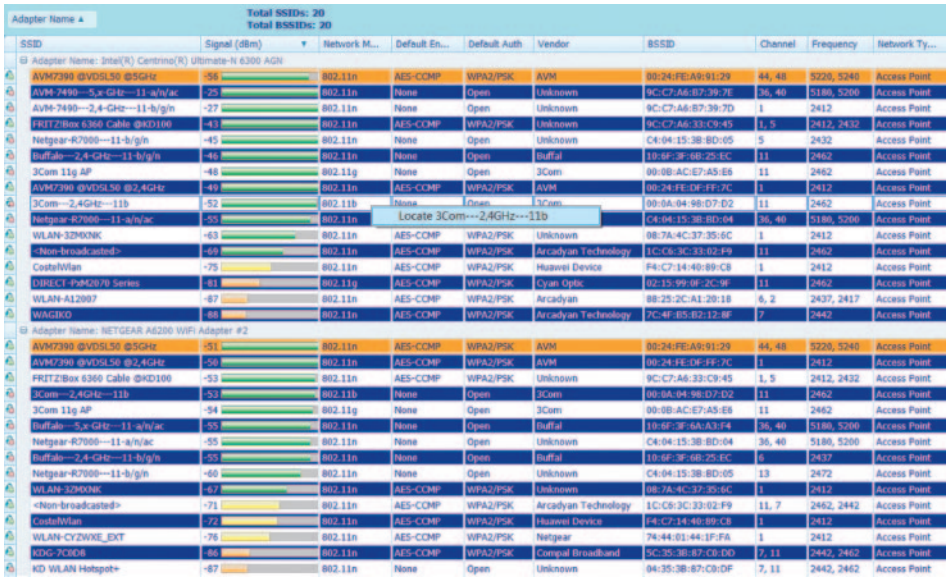
Der Xirrus Wi-Fi Inspector wurde auf einem Business-Laptop Dell Latitude E6520 mit Intel Core i7 und Windows 7 Ultimate 64 Bit installiert. Der Laptop hat ab Werk ein 3×3-MIMO-Funkmodul bis 450 MBit/s der Marke Intel Centrino Ultimate-N 6300 AGN verbaut; das taugt zur Kommunikation mit WLAN-a/b/g/n-Funkzellen, beherrscht aber noch kein Gigabit-WLAN-AC. Um den Laptop zusätzlich mit AC-Funk nachzurüsten, installierten wir einen Netgear AC1200 WiFi USB Adapter an der USB-2.0-Buchse. Dieser Netgear-Stick beherrscht bereits WLAN-11ac, aber nur mit 2×2-MIMO. Deshalb bringt er nicht die vollen 1300 MBit/s, sondern maximal zwei Drittel, sprich 867 MBit/s. Davon bleibt knapp die Hälfte als Netto-Speed übrig. Deshalb wirkt sich der USB-2.0-Port des Laptops mit maximal 480 MBit/s brutto nicht als Durchsatzbremse aus.

Wi-Fi-Funkmodule

Das Xirrus-Softwaretool verstand sich mit beiden WiFi-Adaptern, dem internen von Intel und dem externen von Netgear. Es konnte deren Funksignale sogar gleichzeitig im gleichen Fenster live anzeigen. Das ist erfreulich.

Network Modus

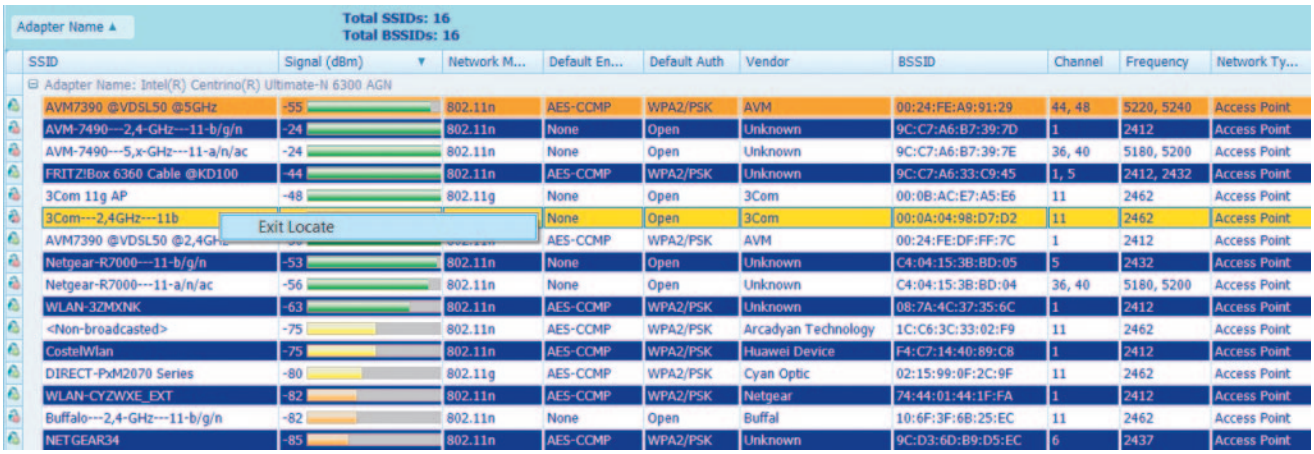
Beide Adapter erkannten im Prinzip alle Funkzellen. Allerdings attestierte das Xirrus-Tool maximal 11n; den schnellsten Netzwerk-Modus 11ac dagegen erkannte der Wi-Fi Inspector nicht. Beim integrierten 11n-Funkmodul von Intel überrascht das nicht, weil es noch gar kein 11ac versteht. Beim externen 11ac-Stick von Netgear dagegen schon. Wo liegt der Fehler? War die Xirrus-Software noch nicht in der Lage, 11ac zu erkennen? Versteht sie sich nicht optimal mit dem Netgear-AC-Stick? Oder schaltet der Netgear-AC-Adapter im Messmodus nicht auf 11ac hoch?



Quelle: Harald Karcher

Im oberen Teil der Grafik werden all jene WLAN-Zellen gelistet, die das im Dell Latitude E6520 verbaute 11a/b/g/n-Funkmodul von Intel erkannte. Im unteren Teil sind jene Wi-Fi-Zellen gelistet, die vom extern angesteckten Netgear AC1200 WiFi USB Adapter in den Laptop gemeldet wurden (Abb. 1).

Quelle: Harald Karcher



SSID	Signal (dBm)	Network M...	Default En...	Default Auth	Vendor	BSSID	Channel	Frequency	Network Ty...
Adapter Name: Intel(R) Centrino(R) Ultimate-N 6300 AGN									
AVM7390 @VDSL50 @5GHz	-55	802.11n	AES-CCMP	WPA2/PSK	AVM	00:24:FE:A9:91:29	44, 48	5220, 5240	Access Point
AVM-7490---2,4-GHz---11-b/g/n	-24	802.11n	None	Open	Unknown	9C:C7:A6:B7:39:7D	1	2412	Access Point
AVM-7490---5,x-GHz---11-a/n/ac	-24	802.11n	None	Open	Unknown	9C:C7:A6:B7:39:7E	36, 40	5180, 5200	Access Point
FRITZ!Box 6360 Cable @KD100	-44	802.11n	AES-CCMP	WPA2/PSK	Unknown	9C:C7:A6:33:C9:45	1, 5	2412, 2432	Access Point
3Com 11g AP	-48	802.11g	None	Open	3Com	00:0B:AC:E7:A5:E6	11	2462	Access Point
3Com---2,4GHz---11b			None	Open	3Com	00:0A:04:98:D7:D2	11	2462	Access Point
AVM7390 @VDSL50 @2,4GH			AES-CCMP	WPA2/PSK	AVM	00:24:FE:DF:FF:7C	1	2412	Access Point
Netgear-R7000---11-b/g/n	-53	802.11n	None	Open	Unknown	C4:04:15:3B:BD:05	5	2432	Access Point
Netgear-R7000---11-a/n/ac	-56	802.11n	None	Open	Unknown	C4:04:15:3B:BD:04	36, 40	5180, 5200	Access Point
WLAN-3ZMXNK	-63	802.11n	AES-CCMP	WPA2/PSK	Unknown	08:7A:4C:37:35:6C	1	2412	Access Point
<Non-broadcasted>	-75	802.11n	AES-CCMP	WPA2/PSK	Arcadyan Technology	1C:C6:3C:33:02:F9	11	2462	Access Point
CostelWlan	-75	802.11n	AES-CCMP	WPA2/PSK	Huawei Device	F4:C7:14:40:89:C8	1	2412	Access Point
DIRECT-PxM2070 Series	-80	802.11g	AES-CCMP	WPA2/PSK	Cyan Optic	02:15:99:0F:2C:9F	11	2462	Access Point
WLAN-CYZWXE_EXT	-82	802.11n	AES-CCMP	WPA2/PSK	Netgear	74:44:01:44:1F:FA	1	2412	Access Point
Buffalo---2,4-GHz---11-b/g/n	-82	802.11n	None	Open	Buffal	10:6F:3F:6B:25:EC	11	2462	Access Point
NETGEAR34	-85	802.11n	AES-CCMP	WPA2/PSK	Unknown	9C:D3:6D:B9:D5:EC	6	2437	Access Point

Ein Highlight des Xirrus Wi-Fi Inspectors ist die Locate-Funktion zum Aufspüren verdächtiger Access-Points. Markiert man den gesuchten AP per Mausrechtsklick, dann piepst der Laptop umso lauter, je näher man diesem AP kommt. Mit „Exit Locate“ wird die Piepserei wieder beendet und die gelbe Hinterlegung verschwindet (Abb. 2).

Wir vermuten Ersteres und hoffen auf ein Softwareupdate für 11ac von Xirrus. Also: Unsere Testkonfiguration eignet sich zum Monitoring von 11a/b/g/n-Infrastrukturen, konnte aber noch keine 11ac-Netzwerk-Modi erspähen.

Default Encryption und Authentication

Das Xirrus-Tool erkannte den Verschlüsselungsmodus der aufgebauten WLAN-APs korrekt. In der Xirrus-Tabelle war auch zu sehen, welche APs unverschlüsselt senden. Bei Bedarf kann der Funknetzadministrator reagieren und die Verschlüsselung an den unverschlüsselten APs einschalten.

Die Authentifizierungsmethode der Test-APs wurde ebenfalls aus der Luft erkannt. Die meisten hatten WPA2/PSK eingeschaltet. Ein fremder „KD WLAN Hotspot“ aus der Nachbarschaft meldete „Open“. Sollte so ein offenes Netz nicht im Sinne des Funknetzadministrators sein, dann könnte er das jetzt korrigieren.

Channel und Frequency

In der Spalte „Channel“ werden die WLAN-Kanäle angezeigt, unter „Frequency“ die Frequenzen, auf denen die WLAN-Geräte funken. Hier kann der Funknetzoptimierer prüfen, wie weit er vom Ideal einer überlappungsfreien WLAN-Installation entfernt ist. Eventuell schaltet er die automatische Kanalsuche in seinen APs ab und vergibt die Kanäle nach eigenem Ermessen, um die Interferenzen so gering wie möglich zu halten.

Lokalisierung per Piepston

Gefallen hat uns die Suchfunktion im Xirrus Wi-Fi Inspector. Ein Beispiel: Wir markieren den uralten 11b-AP von 3Com und schalten das Locate-Feature ein: Sogleich ertönt ein Piepston aus dem Laptop, der immer aufgeregter wird, je näher wir dem 3Com-AP mit dem Laptop kommen. So können wir den alten AP aufspüren, um ihn aus dem Netz zu nehmen, falls er stören sollte. Oder wir markieren den modernsten AP und nähern uns per Suchdetektor so lange, bis wir die beste Verbindungsqualität bekommen. Im ersten Szenario hilft das Tool dem Funknetzplaner, im zweiten eher dem Funknetznutzer.

Signal History

Diese Funktion protokolliert die Signalstärken aller erkannten WLAN-Zellen im Zeitverlauf. Hier sieht man, welche APs die höchsten und stabilsten Werte bringen. Ebenso erkennt man auf einen Blick die APs mit sehr geringen oder sehr schwankenden Signalstärken. Wandert man mit dem Signal-History-Tool durch mehrere Räume, dann sieht man, welche Funkzellen aus welchen APs in welchen Räumen besonders stark oder besonders schwach ankommen. Daraus kann man gute Schlüsse für die weitere Funknetzoptimierung ziehen.

Speed-Quality-Connection-Tests

Beim Klick auf den „Speed Test“ des Xirrus Wi-Fi Inspectors wird das extern eingebundene Werkzeug www.speedtest.net aufgerufen. Es misst den Internet-Durchsatz des WLAN-Routers, mit dem der Laptop gerade verbunden ist.

Beim Klick auf „Quality Test“ ruft der Inspector den ebenfalls bekannten und beliebten www.pingtest.net auf. Er misst Paketverluste, Ping-Zeit, Jitter und den MOS-Wert des verbundenen WLAN-Routers.

Beim Klick auf „Connection Test“ werden erstens die Ping-Zeiten zwischen Laptop und WLAN-Router und zweitens jene zwischen dem Laptop und der Internet-Seite http://173.194.69.147/ gemessen, besser bekannt als Startseite der Google-Suche www.google.com.

Dazu lässt sich schnell und bequem herausfinden, wie gut jeder AP oder WLAN-Router mit dem Internet verbunden ist.

Fazit: Noch ohne AC, dafür mit Spürsuche

Von allen sechs APs wurden wichtige Funktionen über die Luft ausgelesen und in Tabellen oder Kurven dargestellt. Der kombinierte Einsatz aller Tools des kostenlosen Xirrus Wi-Fi Inspectors lässt zwar keine perfekte, aber brauchbare Qualitätskontrolle von WLAN-Installationen zu. Die freie Software kann gute Anregungen zur Ausmerzung von Fehlern und zur weiteren Optimierung einer WLAN-Installation liefern. Gefallen hat besonders die Lokalisierungsfunktion, mit der sich über ein akustisches Feedback verdächtige APs aufspüren lassen.

Dr. Harald B. Karcher
freier Mobile-Communications-Tester

Flächendeckend Antennen verstecken

Viele Nutzer über mehrere Etagen hinweg – große Hotels sind Musterfälle anspruchsvoller WLAN-Installationen.

Theoretisch lassen sich die funkoptimalen Positionen und Mengen der benötigten Wi-Fi-Basisstationen per Software genau vorausberechnen. In der Praxis muss sich die Wireless-Planung weiteren Aspekten unterordnen, vor allem der Ästhetik. Am besten lässt sich das an WLAN-Hotelinstallationen zeigen.

Wi-Fi-Design-Tools geben wertvolle Tipps und liefern exakte Pläne für die ideale Positionierung und Optimierung von WLAN-Basisstationen: so etwa der AirMagnet Planner, Aruba Visual RF Plan, Ekahau Site Survey, Ekahau HeatMapper, Network Stumbler, InSSIDer oder der Xirrus Wi-Fi Inspector (siehe Seite 22).

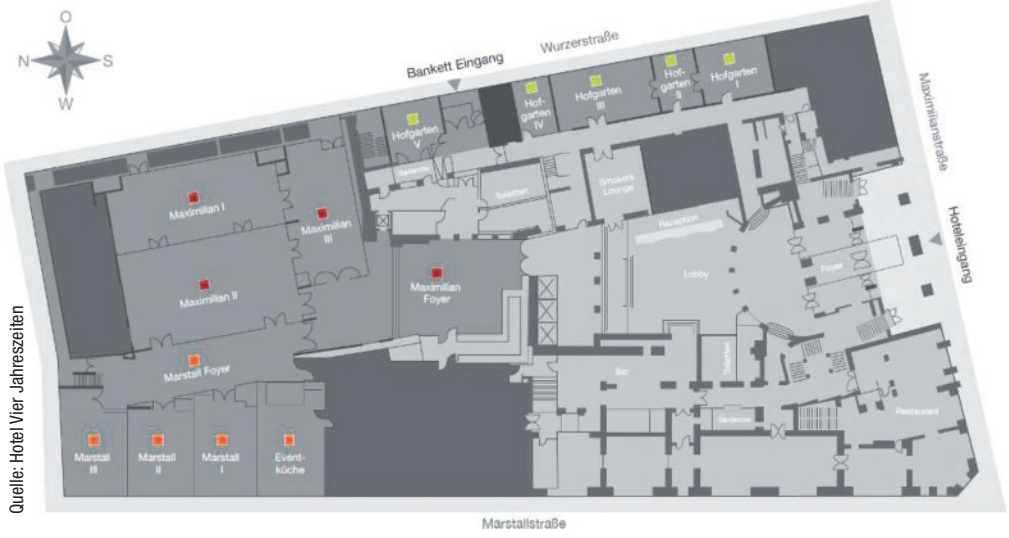
In der Praxis sitzen die WLAN-Access-Points und Antennen aber selten am funkoptimalen Punkt, sondern eher dort, wo der WLAN-Benutzer sie nicht gleich sieht, wo dicke Kabelstränge hinter abgehängten Doppeldecken verlaufen, wo zufällig schon ein Ethernet-Anschluss vorhanden war oder wo man ein neues Ethernet-Kabel mit verschmerzbaren Kosten hinlegen konnte. Daran hat sich vom ersten 11b-WLAN-Hotspot anno 2001 bis zu den jüngsten 11ac-Projekten 2014 nicht viel geändert. Eine Zeitreise.

Kempinski München 2001: 4 × 11b

Das Hotel Vier Jahreszeiten Kempinski München eröffnete im August 2001 den ersten öffentlichen WLAN-Hotspot Deutschlands. Die erste Funkbegehung machte der Autor damals mit einem Business-Laptop der Marke Toshiba Tecra 8200 samt eingebautem WLAN-11b. Dessen vorinstallierte WLAN-Client-Software fand im Erdgeschoss des Hotels gerade mal vier Access-Points von Symbol Technologies.

Der erste Access-Point saß, völlig unsichtbar, hinter einer Holzvertäfelung hinter der Rezeption und versorgte vor allem die Lobby und das Foyer. Der zweite AP saß, gleichfalls völlig unsichtbar, zwischen zwei Sandsteinmauern hinter einer Schiebewand aus schwerem, dunklem Edelholz in den Banketträumen Diana I und Diana II, westlich vom heutigen Maximilian Foyer. Der dritte AP saß, ebenso unsichtbar, hinter einer großen und gewölbten Deckenleuchte des Cherubin-Ballsaals, etwa dort, wo jetzt der Konferenzraum Maximilian II eingezeichnet ist. Der vierte AP hing in einer grauen Stahlkonstruktion zwischen Wand und Decke in einem kleinen Raum des Konferenzflügels Hofgarten. Im Gegensatz zu den drei anderen APs war er frei sichtbar.

Bei einer Outdoor Site Survey des Autors drang die WLAN-Strahlung übrigens kaum irgendwo durch die dicken Mauern des 1858 eröffneten Vier Jahreszeiten auf die Straßen hinaus. Lediglich auf der Wurzerstraße konnte man fast ebenso gut drahtlos surfen wie im In-



Quelle: Hotel Vier Jahreszeiten

Das Hotel Vier Jahreszeiten Kempinski München hatte 2001 den ersten Public-WLAN-Hotspot der Nation. Vier Access-Points reichten für die Erstversorgung mit WLAN 802.11b im Erdgeschoss: hinter der Rezeption, im Bankettraum Hofgarten I, im Ballsaal an der Decke Maximilian II sowie westlich vom Maximilian-Foyer. Im Restaurant Walterspiel an der Maximilianstraße kam allerdings kein mobiles Internet an (Abb. 1).

Quelle: Harald Karcher

Hier blicken wir vom zwölften Stock hinunter in die Lobby des Hilton Frankfurt. Wer dieses ungewöhnliche Gebäude mit WLAN ausrüsten darf, bekommt erst mal graue Haare, denn hier kreuzen sich die Signale in der offenen Halle (Abb. 2).

Quelle: Harald Karcher

Das Kempinski Emirates Palace Abu Dhabi gehört zu den ersten Hotels der Welt, die schon einen Gigabit-WLAN-Hotspot haben. Dafür kamen mehr als 1000 Access-Points der Speed-Gattung 802.11ac zum Einsatz (Abb. 3).

neren des Hotels – sofern man den Zugangscode hatte. Der Access-Point im Raum Hofgarten strahlte nämlich bestens durch die Fenster.

Hilton Frankfurt 2003: WLAN nach Fluchtplänen

Mit seiner extrem offenen Atrium-Architektur und seiner zwölf Etagen hohen Hotelhalle war das Hilton Frankfurt Hotel ein wahrer Intelligenztest für Funktechniker: Bei der Erstausstattung mussten über 70 Access-Points montiert werden.

Der Funknetzplaner Martin Palzer machte die Site Survey. Dazu hätte er am liebsten die exakten Originalbaupläne studiert, doch die waren nicht so einfach zu bekommen, denn Hilton war „nur“ der Mieter des Objektes. Ersatzweise kopierte Palzer die Fluchtpläne, die ja ebenfalls Etagengrundrisse enthalten.

Dann nahm Palzer einen batteriebetriebenen Access-Point und klebte ihn mit Klettband an diejenigen Stellen, Wände und Decken im Hotel, die er aus dem Bauch heraus für die besten Montagepunkte hielt; manche APs legte er in Revisionsklappen, andere befestigte er provisorisch an den Lüftungsschlitzen. Dann wanderte er mit seinem Wireless-Notebook samt Messprogramm um die Batterie-APs herum und zeichnete die Reichweiten und die Qualität der Verbindung in seine Grundrisse ein. Idealerweise entstehen auf diesen Grundrissen dann mehrere Funkzellen in Form von Kreisen, Waben oder ähnlichen Ausbreitungsmustern. Am Ende konnt Palzer gut abschätzen, wie viele Access-Points er für das ganze Gebäude brauchte und wo sie am besten montiert sein sollten.

Weniger Sendepower, kleinere Zellen

In der Regel strahlt so ein Access-Point durch die Betondecken hindurch, eine Etage nach unten und eine Etage nach oben. Das Vertrackte an diesem Hotel ist aber: Durch die extrem hohe Halle strahlt ein Access-Point auch völlig ungehindert zig Meter weit in die drei gegenüberliegenden Hotelflügel hinein. Irgendwann ist da der Punkt erreicht, wo sich die APs gegenseitig stören, weil das 2,4-GHz-Frequenzband für solche Überlappungssituationen eigentlich zu schmal ist. Also musste man die Sendeleistung der APs je nach Montagepunkt unterschiedlich stark reduzieren, damit die Zellen kleiner werden.

In der Regel kann man die Sendestärken kommerzieller APs leicht verändern. Durch die Power-Reduktion brauchte Palzer aber letztlich doppelt so viele Access-Points wie bei einer vergleichbaren Zimmerzahl in einem normalen Hotelbau nötig gewesen wären.

Funk aus der Revisionsklappe

Außerdem konnte Palzer in diesem Business-Hotel mit seinem hohen Anspruch an Design und Ambiente die Access-Points nicht genau dort montieren lassen, wo sie funktechnisch optimal hingehören. Er musste jede Menge Kompromisse eingehen. Letztendlich wurden die meisten APs in den Revisionsklappen in den Decken der Etagen versteckt. Dazu muss man allerdings auf Leitern klettern – ein Spektakel, das in einem gediegenen Hotel nicht gern gesehen wird. Die WLAN-Monteure mussten daher Zeiträume abwarten, in denen gerade kein voller Gästebetrieb herrschte.

Letztlich wurden im Hilton Frankfurt per August 2003 für die Erstausstattung 74 Access-Points montiert. Und für ein paar letzte Ecken und Winkel hätte Palzer lieber sogar noch ein paar mehr APs gesehen.

Doch die Access-Points sind nicht einmal das Teuerste an so einem Hotspot, erklärt der Funknetzplaner: Ein Access-Port von Symbol kostete damals laut Liste 200 Euro, die bloße Verlegung des Ethernet-Kabels kostete 300 bis 500 Euro (pro Kabel zum Access-Port). Auch 2014 kommt ein fertig montierter und angeschlossener Access-Point auf um die 600 Euro. Ein vergleichbares Projekt mit 74 Access-Points dürfte auch heute, grob gesagt, rund 45.000 Euro kosten.

Das Hilton Frankfurt hat 342 Zimmer, 14 Suiten, 16 Meeting-Räume und einen Ballsaal für knapp 600 Gäste. Unterstellen wir grob gesagt 500 Räume und 74 APs, dann hätte in der Erstausstattung ein AP im Schnitt 6,7 Räume versorgt.

Emirates Palace 2013: Upgrade auf AC

Das Kempinski Emirates Palace Abu Dhabi gehört zu den ersten Hotels der Welt, die schon einen nennenswerten Gigabit-WLAN-Hotspot in Betrieb haben. Laut ipt.net kamen für die Coral-, Pearl- und Diamond-Gäste mehr als 1000 Access-Points der Speed-Gattung 802.11ac

Aruba AP-225 und ein Mobility Controller der Serie 7220 zum Einsatz. Laut Datenblatt bedient der Aruba 7220 bis zu 24.576 User gleichzeitig und lässt bis zu 40 GBit durch die Firewall.

Das 2005 eröffnete Hotel stellt Gästen offiziell 302 Zimmer und 92 Suiten zur Verfügung. Dazu kommen allerdings noch die nichtöffentlichen Suiten der Regenten der Vereinigten Arabischen Emirate. Veranschlagen wir für den Standort Abu Dhabi grob gesagt 1000 größere Räume und 1000 APs, so würde ein AP im Schnitt einen Raum versorgen. Eine derart hohe Dichte ist bei 11ac auch naheliegend, weil der 11ac-Funk im 5-GHz-Band an dicken Wänden viel stärkere Verluste hat als die älteren Standards 11b und 11g bei 2,4 GHz.

Der Autor hatte 2006 Gelegenheit, die Erstausstattung auf 2,4 GHz anzutesten. Seinerzeit funkten weitaus weniger Access-Points von Cisco Systems im 11g-Speedlevel mit 54 MBit/s brutto auf den Kanälen 1 und 6 und 11. Das WLAN wirkte aber schon damals unterdimensioniert und passte nicht ganz zum Luxus des Hauses. Warum Cisco das Upgrade auf 11ac in einem solchen Referenzpalast nicht gewonnen hat, ist nicht bekannt. Vielleicht kam der große Catalyst-Produkte-Relaunch von Cisco 2013 doch etwas zu spät.

Die Gründe für das WLAN-Upgrade im Emirates Palace stellen sich kaum anders dar als in vielen weiteren Hotels der Welt: Gäste und Mitarbeiter haben eine immer größere Menge von Smartphones, Tablets und anderen Mobilgeräten im Dauereinsatz. Deshalb erwarten sie heute ein stabiles, schnelles und kostenloses Internet per WLAN in allen Zimmern, in Restaurants, Cafés, Lobbys, Büros und Konferenzbereichen.

In verdichtetem Parallelbetrieb

Schon beim ersten Public-WLAN-Hotspot der Nation, dem Hotel Vier Jahreszeiten in München, musste sich die schnöde WLAN-Technik der Ästhetik des Hauses unterordnen. Genauer gesagt: Man strebte einen guten Kompromiss zwischen den Gesetzen der Wellenausbreitung und den architektonischen Geboten der baulichen Gefälligkeit an. Auch wenn die Access-Points in vielen Hotels und Büros früher oder später auf das neue Gigabit-WLAN IEEE 802.11ac umgestellt werden, wird sich am Primat der Ästhetik kaum etwas ändern.

Ob sich die neuen 11ac-Wellen in komplexen Gebäuden besser durchsetzen können als die alten 11b-Wellen, wäre erst noch zu beweisen. Wireless AC funkt ja nur im 5-GHz-Band, das alte 11b/g nur im 2,4-GHz-Band. Die kurzen 5-GHz-Wellen verpuffen in dicken Mauern viel schneller als die längeren 2,4-GHz-Wellen. Das bedeutet: Im 5-GHz-Band muss man die APs dichter setzen als im 2,4-GHz-Band. Dazu braucht man mehr Access-Points – und das wird am Ende teurer.

Dafür ist das 5-GHz-Band noch nicht so überfüllt wie das 2,4-GHz-Band. Im Zweifelsfall installiert man somit künftig das Beste aus beiden Frequenzwelten, sprich: beide Bänder, also Dualband 11a/b/g/n/ac. Die alten AP-Montagepunkte kann man in vielen Fällen beibehalten. Meist wird man aber noch ein paar neue Funkpositionen dazu nehmen, um das Funknetz engmaschiger zu machen.

Dr. Harald B. Karcher
freier Mobile-Communications-Tester

Impressum
Themenbeilage Kommunikation und Netze

Redaktion just 4 business GmbH
Telefon: 080 61/348 111 00, Fax: 080 61/348 111 09,
E-Mail: tj@just4business.de

Verantwortliche Redakteure:
Thomas Jannot (v.i.S.d.P.), Florian Eichberger (Lektorat)

Autoren dieser Ausgabe:
Christoph Becker, Johann Deutinger, Tobias Frielingsdorf, Dr. Harald B. Karcher, Dominik Mauritz

DTP-Produktion:
Enrico Eisert, Kathleen Tiede, Matthias Timm, Hinstorff Verlag, Rostock

Korrektorat:
Silke Peters

Titelbild:
© agsandrew – shutterstock.com

Verlag
Heise Zeitschriften Verlag GmbH & Co. KG,
Postfach 61 04 07, 30604 Hannover; Karl-Wiechert-Allee 10, 30625 Hannover;
Telefon: 05 11/53 52-0, Telefax: 05 11/53 52-129

Geschäftsführer:
Ansgar Heise, Dr. Alfons Schräder

Mitglied der Geschäftsleitung:
Beate Gerold

Verlagsleiter:
Dr. Alfons Schräder

Anzeigenleitung (verantwortlich für den Anzeigenteil):
Michael Hanke (-167), E-Mail: michael.hanke@heise.de

Assistenz:
Stefanie Frank -205, E-Mail: stefanie.frank@heise.de

Anzeigendisposition und Betreuung Sonderprojekte:
Katharina Kraft -534, E-Mail: katharina.kraft@heise.de

Anzeigenverkauf:
PLZ-Gebiete 0 – 1, Ausland: Tarik El-Badaoui -395, E-Mail: tarik.el-badaoui@heise.de,
PLZ-Gebiete 2 – 3, 8 – 9: Ralf Räuber -218, E-Mail: ralf.raeuber@heise.de

Anzeigen-Inlandsvertretung:
PLZ-Gebiete 4 – 7: Karl-Heinz Kremer GmbH, Sonnenstraße 2,
D-66957 Hilst, Telefon: 063 35/92 17-0, Fax: 063 35/92 17-22,
E-Mail: karlheinz.kremer@heise.de

Leiter Vertrieb und Marketing:
André Lux

Druck:
Dierichs Druck + Media GmbH & Co. KG, Kassel