ComConsult Research

Der Netzwerk Insider

November 2008

Systematische Weiterbildung für Netzwerk- und IT-Professionals

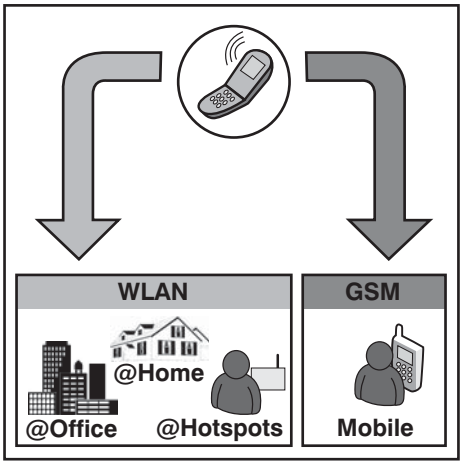
Schwerpunktthema

Fixed-Mobile-Convergence

Ist das Roaming zwischen WLAN und GSM schon reif für die Ablösung von DECT?

von Dr. Frank Imhoff, Dipl.-Inform. Nick Schirmer, Dr. Michael Wallbaum

Das Zusammenwachsen von Fest- und Mobilfunknetzen wird in der Regel als Fixed-Mobile-Convergence (FMC) bezeichnet. Dabei wird sowohl die Integration von GSM-Netzen und klassischen Telekommunikationsanlagen als auch die Nutzung von Wireless-LAN zur Übertragung von Sprache unter diesem Begriff zusammengefasst. Einige Hersteller verfügen schon länger über entsprechende FMC-Lösungen, dennoch ist bisher ein wirklicher Durchbruch ausgeblieben. Ohne eine solche Alternative ist aber vor allem die Ablösung von bestehenden DECT-Installationen kaum sinnvoll möglich. Und ohne die Ablösung von DECT ist die konsequente Einführung neuer, gänzlich IP-basierter Kommunikationslösungen nur bedingt möglich. Dabei wäre es für immer mehr Nutzer höchst wünschenswert, wenn sie statt DECT-Telefon, Festnetz-Apparat und Mobilfunk-Handy nur noch ein Gerät hätten, mit dem sie überall erreichbar wären. Für Unternehmen kommt neben der erheblich reduzierten Endgeräte-Vielfalt auch noch der Wegfall von DECT-Infrastrukturen hinzu. Damit verbunden sind natürlich nicht nur erhebliche Einsparpotenziale, sondern auch ein deutlicher Zuwachs an Komfort für die Nutzer.



weiter auf Seite 29

Zweitthema

Sicherheitszonen in LAN und Rechenzentrum

von Dipl.-Inform. Matthias Egerland, Dr. Simon Hoff, Dipl.-Inform. Daniel Meinhold

Mandantenfähigkeit von Netz und Rechenzentrum (RZ) sowie der Aufbau von Sicherheitszonen (Security Domains) sind immer häufiger gestellte Anforderungen an die IT-Infrastruktur. Das für Universitäten typische Szenario eines Campus, auf dem unterschiedlichen unabhängigen Parteien (d.h. den verschiedenen Instituten und Lehrstühlen), die ein berechtigtes Interesse der Trennung ihrer Daten voneinander haben, gemeinsam genutzte Netzinfrastruktur und RZ-Ressourcen zur Verfügung gestellt werden, findet sich in ähnlicher Form oft auch in anderen Bereichen.

In manchen Fällen sollen Entwicklungsabteilung, Personalabteilung oder Vorstand mit den von ihnen genutzten IT-Ressourcen von den anderen Nutzern abgetrennt werden, ohne dass die Vorteile einer gemeinsam genutzten Infrastruktur verloren gehen. In anderen Fällen geht es beispielsweise um den Schutz kritischer Kernsysteme im RZ oder in Bereichen der industriellen Fertigung.

weiter auf Seite 9

Top-Seminar

Sonderveranstaltung: Wireless Technologie

ab Seite 8

Geleit

Das Ende von 802.11g ist nah, Technologie-Wechsel im Wireless-Markt

ab Seite 2

Neuer Report

Green VoIP: Energieeffizienz und Wirtschaftlichkeit von VoIP-Lösungen

auf Seite 6

Zum Geleit

Das Ende von 802.11g ist nah, Technologie-Wechsel im Wireless-Markt

Atheros, einer der führenden Anbieter von Chips für Konsumer-Wireless-Lösungen, hat am 27. Okober seine neue Chip-Generation unter dem Namen Align-Technologies angekündigt (http://www.atheros.com/news/Align.html).

Diese neue Chip-Generation wird vollständig auf 802.11n basieren. Damit läutet Atheros den lange erwarteten endgültigen Übergang zu 802.11n-Produkten ein. Obwohl der Standard noch nicht verabschiedet ist, macht diese Entscheidung Sinn:

- 802.11n-Chips sind rückwärtskompatibel und beherrschen auf jeden Fall auch 11b und 11g. Wer also n nicht mag oder vorläufig nicht einsetzen will, kann ja im g-Modus arbeiten. Hinzu kommt, dass diese Art von Chips selbst im g-Modus leistungsfähiger ist als die reinen g-Chips

- 802.11n ist in jedem Fall deutlich besser als 802.11g oder gar b. Neueste Untersuchungen belegen eine mittlere Leistungssteigerung in der Größenordnung von Faktor 6 (mit dem generellen Hinweis auf die notwendige Vorsicht, wenn von Leistungsangaben zu Wireless-Produkten die Rede ist)

- Die Wi-Fi Alliance (www.wi-fi.org) hat ein Programm zur Sicherstellung der Interoperabilität aufgestellt. Wer hier immer noch auf die Verabschiedung des Standards wartet, der sei darauf hingewiesen, dass IEEE- und IETF-Standards in der Regel kein Garant für Interoperabilität sind. Sie gestatten in der Regel eine Reihe von Freiheitsgraden in der Implementierung. Es wird häufig ein zusätzliches Testprogramm erforderlich sein, das den Nachweis erbringt, dass Produkte verschiedener Hersteller unter Beibehaltung der vollständigen Leistung miteinander kombiniert werden können. An dem Umfang der bisher von der Wi-Fi-Alliance zertifizierten Produkte (mehr als 1000 Zertifizierungen seit September 2007) kann man erkennen, dass sich die Produkte und der 11n-Markt in einem guten Zustand befinden

Damit ist für den Markt der endgültige Umstieg in diese neue Klasse von Produkten gekommen. Tatsächlich ist für Unternehmens-Kunden der Wechsel nach 11n aber deutlich aufwendiger als für den Konsumenten. Die Gründe dafür sind:

- Die meisten der Hersteller haben mit der Einführung der 11n-Chips ihr gesamtes Produkt-Design ändern müssen. Mehr Durchsatz erfordert auch mehr CPU-Leistung, größere Puffer und vor allem Gigabit-Ethernet-Schnittstellen

- Mit 802.11n ist im Unternehmens-Markt auch der generelle Wechsel auf ein Controller-basiertes Design gekommen. Dieses realisiert u.a. einen schnelleren Zellwechsel bei mobilen Teilnehmern und vereinfacht das Aufsetzen und die Verwaltung von Wireless-Netzwerken erheblich

- In der Regel wird man überlegen, ob man generell mit Access Points mit mehreren Radioteilen arbeitet. So kann man für die Rückwärtskompatibilität zu 11g getrennte Radios einsetzen und für 11n den dringend anzuratenden Wechsel in das 5 GHz-Band machen

- Mit dem Einstieg in neue Standards muss auch die Nutzung von MESH-Netzwerken angedacht werden. Die Standardisierung ist hier recht weit, so dass für Umgebungen, wo MESH-Architekturen einen Zugewinn darstellen, zumindest die Option offen gehalten werden sollte. Neben Access Points, die darauf vorbereitet sind, sollte man die Eigenschaften von MESH-Netzwerken genau kennen, sonst droht vor allem ein Performance-Disaster. In keinem Fall sollte man MESH-Netzwerke mit normalen, nicht auf den MESH-Einsatz optimierten Access Points andenken.

Wer also bisher noch die „alten“ Produkte eingesetzt hat, der muss jetzt umdenken. 802.11n-Netzwerke erfordern eine angepasste Planung. Vor allem der Einsatz von Wireless-Controllern oder Switches erfordert genaue Produktkenntnisse, da sich die Leistungen der Hersteller in diesem Bereich deutlich unterscheiden.

Und gerade auch im Bereich der Wireless-Controller zeichnen sich verbesserte Lösungen am Horizont ab. Diese Art von Produkten wirft generell die Frage nach der Interoperabilität zwischen den Produkten verschiedener Hersteller auf. Da viele Hersteller für die Kontrolle der Access-Points von den Controllern aus hersteller-spezifische Protokolle einsetzen, ist die Entscheidung für den Kauf eines Controller-basierten Designs häufig eine Langfrist Entscheidung. Daher sollte sie genau überdacht werden.

Tatsächlich müssen sich die führenden Hersteller an dieser Stelle auch Kritik gefallen lassen. Mit CAPWAP existiert ein durchaus akzeptabler Standard in diesem Bereich. Neueinsteiger in den Controller-Markt wie Lancom haben diesen Standard auch erfolgreich genutzt. Es gibt also kaum ein technisches Argument gegen Offenheit auch an dieser Stelle. Nun hat auch Cisco die Unterstützung für diesen Standard bekannt gegeben. Damit ist die Messlatte für die Konkurrenz klar gelegt. CAPWAP sollte für alle Kunden zum KO-Kriterium werden. Auf die Offenheit von Netzwerken sollte auch im Wireless-Bereich nicht verzichtet werden.

Trotz aller großen Vorteile, die mit dem Umstieg auf IEEE 802.11n basierte Netzwerke verbunden sind, müssen die Details beachtet werden. Tatsächlich sind auch schon einige Projekte ins Straucheln gera-

Zweitthema

Dr. Simon Hoff ist technischer Direktor der ComConsult Beratung und Planung GmbH und blickt auf jahrelange Projekterfahrung in Forschung, Standardisierung, Entwicklung und Betrieb im Bereich lokaler Netze, mobiler Kommunikationssysteme und deren Anwendungen zurück.

Herr Matthias Egerland hat an der RWTH Aachen Informatik studiert und ist seit 2005 Mitarbeiter der ComConsult Beratung und Planung GmbH. Als Mitglied des Competence Center IT-Sicherheit beschäftigt er sich insbesondere mit der Sicherheit in LAN- und WAN-Umgebungen. In Projekten beteiligt sich Herr Egerland darüber hinaus an Konzeptionierungen und Ausschreibungen von IT-Infrastruktur-Lösungen in den Bereichen Virtual Private Networks (VPN), Metropolitan Area Networks (MAN) sowie konvergenten Netzen.

Dipl.-Inform. Daniel Meinhold hat an der FH Aachen Informatik mit dem Schwerpunkt Kommunikationssysteme studiert und ist heute Consultant bei der ComConsult Beratung und Planung GmbH. Im Competence Center Communications, Collaboration, Mobility ist er vor allem für die Konzeption von Telekommunikationslösungen sowie für die Durchführung von Tests und Messungen verantwortlich. Im Rahmen dieser Tätigkeit hat er sich auch mit dem Session Initiation Protocol (SIP) und der Open Source Telefonanlage Asterisk befasst.

Sicherheitszonen in LAN und Rechenzentrum

Fortsetzung von Seite 1

Dieser Artikel beschreibt die Techniken für den Aufbau von Sicherheitszonen in LAN und RZ und diskutiert anhand von Implementierungsbeispielen die Herausforderungen der Umsetzung dieser Konzepte.

1. Bausteine für den Aufbau von Sicherheitszonen

Die wesentlichen Bausteine für den Aufbau von Sicherheitszonen sind, wie in Abbildung 1 gezeigt:

- Trennung der Daten der Sicherheitszonen durch Virtualisierung im Netz und in Servern
- Kontrolle des in eine Sicherheitszone ein- und ausgehenden Verkehrs
- Kontrolle des Zugangs zur Sicherheitszone für Endgeräte

Die interne Kommunikation, d.h. der Verkehr zwischen Geräten, die einer Sicherheitszone zugeordnet werden, muss im Netzwerk von der anderen (d.h. externen) Kommunikation außerhalb der Sicherheitszone getrennt werden. Dies kann grundsätzlich durch ein physikalisch separates eigenes Netzwerk erfolgen. Bei kleineren Sicherheitszonen speziell zur Abtrennung von Servern im Rechenzentrum ist dies durchaus ein gangbarer Weg. Sobald mehrere (sich geographisch überlappende) Sicherheitszonen oder größere Sicherheitszonen aufzubauen sind, ist es oft eher sinnvoll, eine Sicherheitszone als virtuelles Netz auf einer gemeinsam genutzten Netzinfrastruktur zu realisieren. Die Trennung wird dabei auf Layer 2 durch einfache VLAN-Bildung erreicht und muss auf Layer 3 fortgesetzt werden. Auf Layer 3 ist hierfür nutzer-

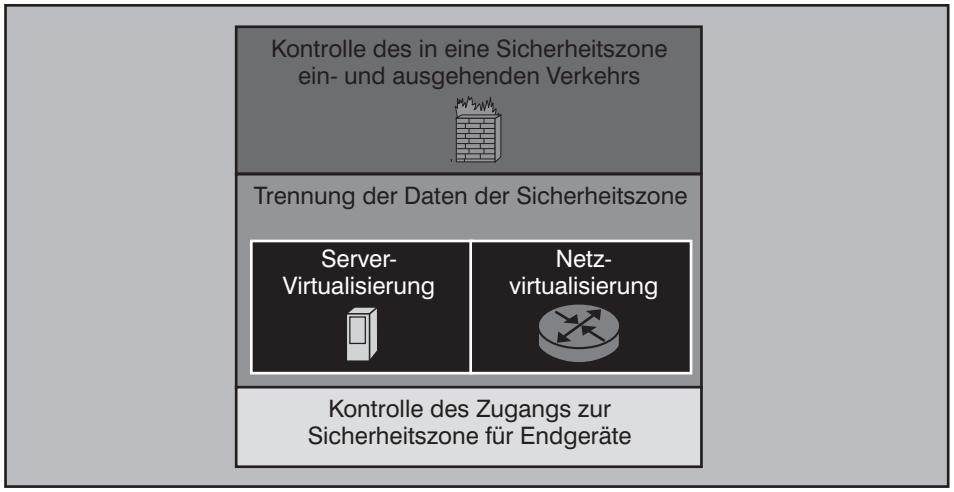


Abbildung 1: Elemente für den Aufbau von Sicherheitszonen

gruppenorientiertes Routing erforderlich. Hierzu werden die im Folgenden genauer beschriebenen Techniken wie beispielsweise virtuelle Routing-Instanzen mit Multi-VRF (Virtual Routing and Forwarding) oder mit Multi Protocol Label Switching (MPLS) eingesetzt. Neben der Frage, ob mit einer Netzvirtualisierung spezifische Sicherheitsrisiken verbunden sind, werden insbesondere die Komplexität von Aufbau und Betrieb und die Skalierbarkeit hinsichtlich Anzahl und Größe der Sicherheitszonen betrachtet.

Eine Sicherheitszone wird nur in den seltensten Fällen komplett isoliert werden können. Typischerweise ist eine Kommunikation über die Sicherheitszone hinaus erforderlich. Neben anwendungsspezifischem Verkehr können auch zentrale Netzdienste von einer Sicherheitszone mitgenutzt werden und die entsprechende Kommunikation muss über die Sicherheitszone hinaus erfolgen können. Ein anderes Beispiel ist das Management der Komponenten einer Sicherheitszone, das ggf. auch zentral erfolgen soll. Es ist also notwendig, eine Sicherheitszone durch ein Koppelelement mit Sicherheitsfunktion abzuschließen, das den ein- und ausgehenden Verkehr kontrollieren (und ggf. blockieren) kann. Die dabei verwendeten Techniken, beispielsweise eine Firewall und/oder ein Intrusion Prevention System (IPS), werden im Folgenden beschrieben. Ein besonders kritisches Element ist dabei neben der hohen erforderlichen Leistung der redundante Aufbau zur Sicherstellung einer hohen Verfügbarkeit.

Die Virtualisierung von Servern hat sich massiv etabliert und muss daher auch beim Aufbau von Sicherheitszonen berücksichtigt werden. Analog zur Betrachtung der Netzvirtualisierung kann man zunächst argumentieren, dass Server, die einer Sicherheitszone zugeordnet sind, physikalisch von anderen Servern zu trennen sind. Dem mag man bei einem erhöhten Schutzbedarf noch folgen, bei einem normalen Schutzbedarf wird man sich trotzdem oft damit beschäftigen müssen, dass virtuelle Server auf einer Hardware unterschiedlichen Sicherheitszonen bzw. Mandanten zugeordnet sind. Die dabei zu beachtenden Gefährdungen und entsprechende Sicherheitsmaßnahmen werden im Folgenden erörtert.

Die Ausdehnung und Positionierung von Sicherheitszonen kann erheblich variieren. Man kann grob die folgenden Kategorien unterscheiden:

- Flächendeckende Sicherheitszonen (siehe Abbildung 2)
- Punktuelle Sicherheitszonen: Sicherheitszonen im Rechenzentrum (siehe Abbildung 3), Sicherheitszonen mit Endgeräten (siehe Abbildung 4) und Kombinationen aus beidem

In vielen Fällen soll durch die Sicherheitszone vor unberechtigtem Zugriff aus dem gemeinsam genutzten Netz geschützt werden, d.h. in der Sicherheitszone wird ein höheres Sicherheitsniveau als im gemeinsam genutzten Netz erreicht. Die Si-

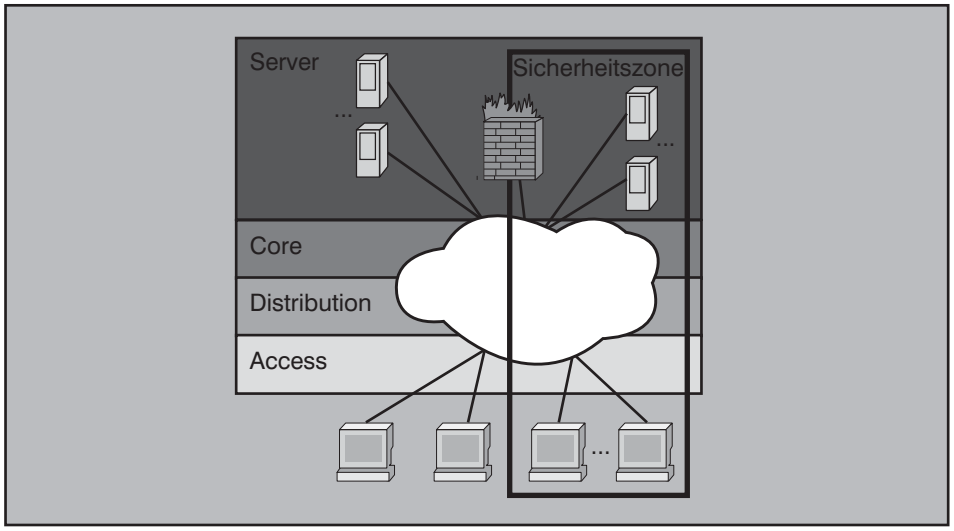


Abbildung 2: Flächendeckende Sicherheitszone

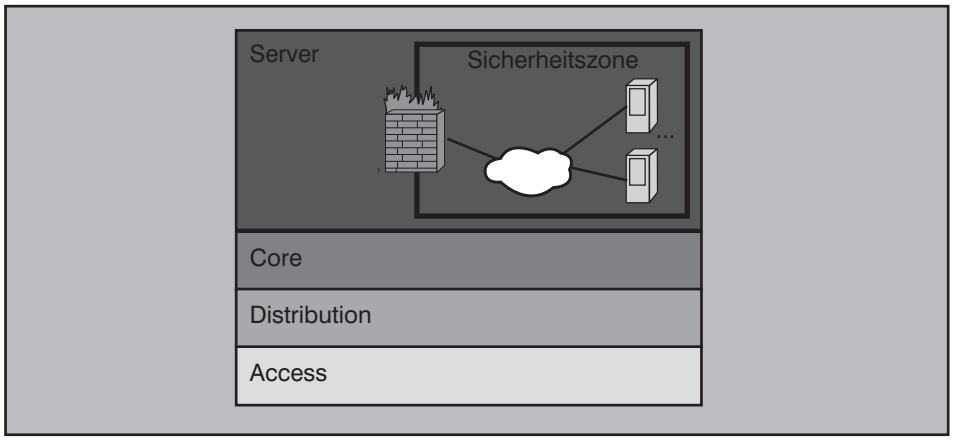


Abbildung 3: Sicherheitszonen im Rechenzentrum zum Schutz dedizierter Server

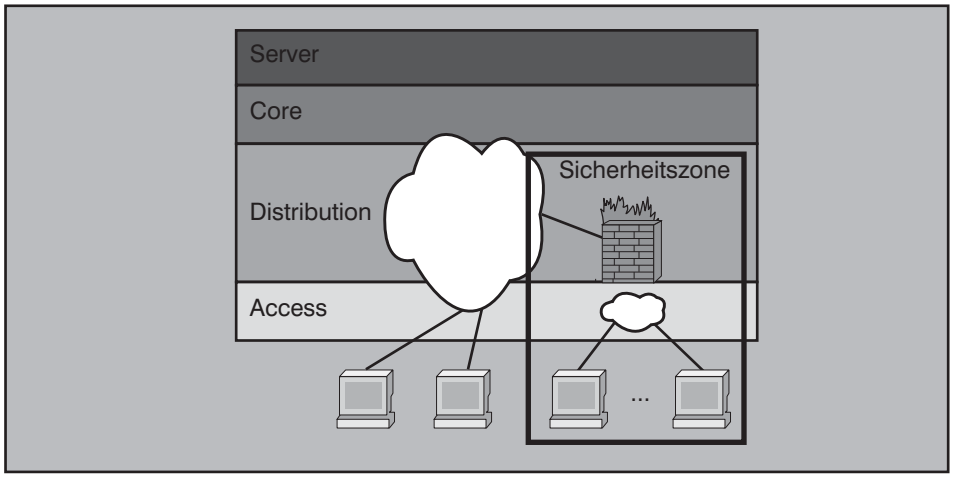


Abbildung 4: Sicherheitszone in einem Gebäude zum Schutz gewisser Endgeräte

Schwerpunktthema

Dr. Frank Imhoff ist technischer Direktor und Senior Consultant der ComConsult Beratung und Planung GmbH. Er blickt auf jahrelange Erfahrung in Forschung, Entwicklung und Betrieb von lokalen Netzen, Voice-over-IP, Wireless Local Area Networks sowie anderen Mobilfunk- und Telekommunikationssystemen zurück. Zu diesen Themenbereichen sind von ihm bereits zahlreiche Veröffentlichungen erschienen und Seminare betreut worden.

Dipl.-Inform. Nick Schirmer ist bei der ComConsult Beratung und Planung GmbH auf Unified-Communications- und Fixed-Mobile-Convergence-Lösungen spezialisiert. Darüber hinaus konnte er in zahlreichen Projekten Erfahrungen bei der Planung und Implementierung von komplexen Kommunikationslösungen sammeln. Weitere Schwerpunkte seiner Arbeit liegen in der Konzeption von Test-Umgebungen sowie in der Durchführung von umfangreichen Produkttests im ComConsult-eigenen Test-Center.

Dr. Michael Wallbaum ist Senior Consultant der ComConsult Beratung und Planung GmbH. Er blickt auf jahrelange Projekterfahrung in Forschung, Entwicklung und Betrieb im Bereich mobiler Kommunikationssysteme, Voice-over-IP und Groupware zurück. Zu diesen Themenbereichen sind von ihm zahlreiche Veröffentlichungen und Buchbeiträge erschienen.

Fixed-Mobile-Convergence: Ist das Roaming zwischen WLAN und GSM schon reif für die Ablösung von DECT?

Fortsetzung von Seite 1

Es stellt sich also einerseits die Frage, welche Anforderungen an eine moderne FMC-Lösung zu stellen sind, um große DECT-Lösungen wirtschaftlich und technisch sinnvoll abzulösen. Andererseits müssen die unterschiedlichen Ansätze der Hersteller kritisch auf ihre unterschiedlichen Möglichkeiten und Leistungsmerkmale hin betrachtet werden, um sicherzustellen, dass eine ähnlich hohe Akzeptanz der Nutzer zu erzielen ist wie bei DECT. Hauptaugenmerk muss dabei sicherlich auf die Sprachqualität gelegt werden, weil hier eine Gewöhnung an die vergleichsweise gute DECT-Qualität stattgefunden hat. Ein weiterer wichtiger Aspekt ist aber auch die Nutzung und der Übergang von eigenen Infrastrukturen wie Wireless-LAN und öffentlichen GSM-Netzen. Dieser Artikel widmet sich vor allem der letzteren Frage. Und wieder einmal ergeben sich dabei überraschende Unterschiede zwischen den Herstellern und Lösungsansätzen.

Der Innovationsdruck unter den Herstellern von modernen Kommunikationslösungen und die weiter zunehmende Nutzung von Mobilkommunikationslösungen haben unter anderem dazu geführt, dass die bisherigen Grenzen zwischen Mobilfunk- und Festnetz-Telefonie, aber auch zwischen unterschiedlichen Funktechnologien, immer weiter verschwimmen. Zukunftsträchtige Kommunikationslösungen erlauben daher eine möglichst nahtlose - und damit benutzerfreundliche - Nutzung unterschiedlicher Technologien. Dadurch wird einerseits die Flexibilität und Erreichbarkeit der Nutzer erhöht, andererseits werden Mehrwertdienste und Kostenvorteile der unterschiedlichen Kommunikationsmöglichkeiten vereint. Ein Hauptaugenmerk der Hersteller liegt dabei auch auf der Nutzung von Wireless Local Area Networks (WLAN) als Medium für die Sprachübertragung. Kommunikationssysteme, die sowohl WLAN als auch Mobilfunk mit den Eigenschaften von modernen Kommunikationslösungen verbinden, werden häufig unter der Bezeichnung „Fixed Mobile Convergence“ (FMC) zusammengefasst.

Die zentrale Herausforderung für eine transparente Integration von zumeist firmeneigenen WLAN und öffentlichen Mobilfunknetzen ist die möglichst störungs- und unterbrechungsfreie Übergabe (Roaming) laufender Telefongespräche zwischen den beiden Funktechnologien. Erste Ansätze führten diesen Wechsel nicht automatisch durch, sondern machten den Eingriff des Nutzers erforderlich. Der Nutzer musste den Roaming-Vorgang am Mobilgerät selbst einleiten und bestätigen, so dass der Wechsel im laufenden Gespräch kaum sinnvoll möglich war. Neuere Systeme übernehmen diesen Roaming-Vorgang automatisch. Der Nutzer einer solchen Lösung kann, je nach Hersteller, lediglich bestimmte Schwellwerte einstellen und den Vorgang so an seine Bedürfnisse anpassen.

Fixed-Mobile-Convergence: Ist das Roaming zwischen WLAN und GSM schon reif für die Ablösung von DECT?

Um ein möglichst störungsfreies Roaming zu gewährleisten, sind vor allem zwei Aspekte von zentraler Bedeutung: Die Minimierung der Verbindungsaufbauzeiten und die richtigen Schwellwerte für das Auslösen eines Roaming-Vorgangs. Grundvoraussetzung für einen störungsfreien Übergang sind darüber hinaus aber auch die richtige Zellplanung und die Auswahl eines möglichst effizienten Handover- und Roaming-Verfahrens.

Derzeit bieten erst wenige Hersteller Fixed-Mobile-Convergence-Lösungen für WLAN und Mobilfunk an. Dabei ist festzustellen, dass diese Lösungen sich sowohl in ihren Ansätzen, als auch in Umfang und Realisierung unterscheiden. Die objektive Analyse und Bewertung der jeweils für das Roaming verwendeten Verfahren war dabei Bestandteil der Tests und Analysen zu diesem Artikel.

Testumgebung

Die WLAN-Infrastruktur für die Testreihen bestand aus Siemens Access Points der 2600er Serie sowie einem Controller vom Typ HiPath Wireless Controller C10.

Im Zuge der Analyse sind dabei folgende Aspekte genauer untersucht worden:

- *Roam-In / Roam-Out:* Einfluss des Wechsels der Kommunikationstechnologie auf die Qualität und die Unterbrechungsfreiheit der übertragenen Sprache. Untersuchung der verwendeten Verfahren und deren Schwellwerte zur Beurteilung der einzelnen Lösungen.

- *WLAN-Handover:* Untersuchung der entstehenden Verzögerungszeit (Delay) und der möglichen Unterbrechungen, bezüglich der Übertragung der Sprache, beim Wechsel von einer WLAN-Zelle zur nächsten.

- *Sprachqualität:* Anhand des PESQ-Verfahrens (Perceptual Evaluation of Speech Quality) nach ITU-T P.862 wurde die Sprachqualität eines WLAN-Gesprächs mit dem MOS-Wert (Mean Opinion Score) bewertet. Anhand der ermittelten Werte wurde ein Vergleich der möglichen Qualitäten im WLAN und GSM erstellt.

- *WLAN-Planung:* Einfluss der Stärke des WLAN-Signals auf die Sprachqualität und die Sicherheit des Handovers zwischen zwei WLAN-Zellen. Beeinträchtigung des Roaming-Vorgangs zwischen WLAN und GSM, durch mögliche Störungen des WLAN-Signals. Unterschiede bei der Planung eines WLAN für reine Datenübertragung und der Planung eines WLAN für Sprachübertragungen in Echtzeit.

Da es sich beim WLAN sowohl um ein Shared Medium als auch um eine physikalisch bedingt, störanfällige Funkverbindung handelt, sind einige Gesichtspunkte bei der qualitativen Bewertung bei der Übertragung von Sprache von besonderer Bedeutung. Dazu gehören

- *Handover-Zeiten:* Die Handover-Zeiten zwischen benachbarten WLAN-Funkzellen müssen möglichst gering gehalten werden, damit diese die Übertragung der Sprache nicht beeinträchtigen.

- *Grenzwerte für Signalstärke:* Damit eine durchgängig gute Sprachqualität garantiert werden kann, müssen im gesamten Gebiet des WLAN festgelegte Grenzwerte für die Signalstärke eingehalten werden. Dazu müssen sich die einzelnen Funkzellen bis zu einem bestimmten Grad überlappen, um so auch das rechtzeitige Handover zu begünstigen.

- *Rechtzeitiges Handover:* Ein bekanntes Problem bei Wireless-LAN Geräten ist die rechtzeitige Einleitung des Handovers/Roamings. Es muss eine software-gesteuerte Schranke eingerichtet werden, ab der das System selbstständig den Handover- / Roaming-Vorgang einleitet.

- *Schnelle Authentifizierung:* Die Zugriffssteuerung sollte den Zeitbedarf des Handover- / Roaming-Vorgangs nicht negativ beeinflussen.

- *Sicherheit:* Es muss trotz Handover-Beschränkungen ein sicheres Verfahren zur Authentifizierung der mobilen Nutzer gewählt werden.

- *Kanalplanung:* Zur Kanalplanung stehen im 2,4 GHz-Band nur wenige interferenzfreie Kanäle zur Verfügung. Nutzt man statt dessen das 5 GHz-Band, (802.11a) so ist die Kanalplanung erheblich einfacher, allerdings wird dieses Frequenzband derzeit nicht von allen Fixed-Mobile-Convergence-Systemen unterstützt. Weitere Störquellen sind Bluetooth-Geräte, DECT bei 2,4 GHz, Videoübertragungssysteme, Amateurfunk, Mikrowellenherde etc.

In Bezug auf die Zellplanung eines WLAN sind ebenfalls einige Einschränkungen gegenüber reiner Datenübertragung zu berücksichtigen. Ein mit G.711 kodierter Anruf erzeugt beispielsweise Ethernet-Rahmen mit einer Rahmengröße von 228 Byte inklusive aller Header. Ein Gespräch erzeugt einen RTP-Verkehr von 50 Paketen pro Sekunde in jede Richtung, womit ein Gespräch rund 182 kbit/s beansprucht. Demnach könnten bei 802.11b in einer Funkzelle theoretisch rund 60 Gespräche parallel stattfinden. Diese naive Berechnung berücksichtigt jedoch weder Paketwiederholungen, Empfangsbestätigungen, Management Rahmen, konkurrierenden Datenverkehr noch die Einflüsse des Medienzugriffsverfahrens. Planerisch sinnvoll sind maximal acht Telefonate pro Zelle. Auch bei einer reinen VoIP-Nutzung sollte der Wert kaum über zehn gleichzeitige Telefonate hinausgehen, da man die abnehmende Datenübertragungsrate am Rand der Zelle einkalkulieren muss. Damit müssen WLANs, die auch für Sprache genutzt werden, in der Regel viel dichter und mit kleineren Zellradien geplant werden als reine Daten-WLANs, um eine qualitativ hochwertige und unterbrechungsfreie Sprachübertragung zu gewährleisten.

Neben diesen von der gewählten FMC-Lösung unabhängigen Faktoren sind jedoch noch eine ganze Reihe Hersteller-spezifischer Unterschiede zu beachten. Dazu zählen unter anderem die angebotenen Sprach-Codecs der Endgeräte und vor allem die eingestellten Schwellwerte für Handover- und Roaming-Vorgänge. Auf diese Unterschiede zwischen den Herstellern soll im Folgenden eingegangen werden.

Siemens HiPath Mobile Connect

Zu den Aufgaben des HiPath Mobile Connect Controller gehören unter anderem Handover-Vorgänge, Gesprächsaufbau und Gesprächs-Routing im Zusammenspiel mit der TK-Anlage. Der Mobile Connect Controller kann mit jeder SIP-fähigen Telefonanlage gekoppelt werden. Im vorliegenden Testaufbau war dies die HiPath 8000 von Siemens, die wiederum über eine HiPath 4000 an das öffentliche Netz angeschlossen wurde. Bei dieser Lösung übernimmt der Mobile Connect Controller – im Zusammenspiel mit der HiPath 8000 – auch das Roaming zwischen GSM und WLAN. Aus diesem Grund müssen sowohl die GSM-Telefonnummer, als auch die interne Telefonnummer des Mobiltelefons auf dem Mobile Connect Controller hinterlegt werden. (siehe Abbildung 1)

Der HiPath Mobile Connect Client (HPMC) wurde auf einem Nokia E60 installiert (Symbian S60 3rd Edition), das auch ohne Installation von spezieller Client-Software die Nutzung von SIP-Profilen zur VoIP-Telefonie bietet. HPMC basiert auf dem von fgMicrotec entwi-