ComConsult Research

Der Netzwerk Insider

November 15

Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

Session Border Controller: Die Perimeter-Komponente für All-IP - Teil 1

von Dipl.-Inform. Petra Borowka-Gatzweiler

All-IP respektive SIP Trunking ist das Schlagwort, das den Wechsel des öffentlichen Telekommunikations-Netzes hin zu IP und SIP bezeichnet. Dies betrifft nicht nur die Sprachübertragung (VoIP) sondern auch Video, Erreichbarkeitsanzeige, Chat, A/VWeb-Konferenzen und alle weiteren UCC-Dienste.

Der Übergang auf IP im öffentlichen Telekommunikationsnetz birgt ähnliche Risiken wie wir sie seit Jahr(zehnt)en für IT-Kommunikation über Internet kennen. Das bedeutet, der Netzwerk-Perimeter muss besonders geschützt werden.

Und hier kommt der Session Border Controller (SBC) ins Spiel.

weiter auf Seite 9

Zweitthema

Kühltechniken im Rechenzentrum, Alternativen zur klassischen Raumkühlung

von Dipl.-Ing. Hartmut Kell

Die herkömmliche Methode zur Kühlung von Serverräumen ist die Raumkühlung. Dabei wird dem Serverraum von mehreren parallel arbeitenden Klimaanlagen Kaltluft zugeführt, zumeist über einen Doppelboden, und warme Abluft im Deckenbereich entzogen. Im Falle von Bestandsrechenzentren wird man in der Regel diese Technologie nach Möglichkeit weiterverwenden, jedoch kommt sie bei hohen Leistungsdichten in den Serverracks an ihre Grenzen. Auch ein Verzicht auf Doppelböden bzw. auf ausreichend hohe Doppelböden, wie sie sich durchaus bei Umbau von vorhandenen Räumlichkeiten wegen der fehlenden Raumhöhe ergeben kann, macht andere Kühlkonzepte notwendig.

Der nachfolgende Artikel beschäftigt sich mit Kühlkonzepten, die eine rack- oder reihenbasierende Kühlung als Basis-Technologie verwenden und soll im Rahmen der ein oder anderen RZ-Planung den interessierten Leser dazu anregen, auch diese Alternativen in Betracht zu ziehen.

weiter auf Seite 21

Geleit

Bieten neue WLAN- und LTE-Varianten die richtigen Antworten auf die Anforderungen der mobilen Revolution oder entstehen sogar noch mehr Probleme?

auf Seite 2

Standpunkt

Vertrauenskrise bei Zertifikaten

auf Seite 19

Aktueller Kongress

ComConsult UC-Forum 2015

ab Seite 5

Aktuelles Seminar

Die neue EU-Datenschutzgrundverordnung

auf Seite 20

Aktuelles Intensiv-Seminar

Winterschule 2015

ab Seite 7

Zum Geleit

Bieten neue WLAN- und LTE-Varianten die richtigen Antworten auf die Anforderungen der mobilen Revolution oder entstehen sogar noch mehr Probleme?

Ernst zu nehmende Prognosen von Herstellern, Providern und Marktforschern gehen davon aus, dass sich in den nächsten Jahren die Anforderungen an Mobilfunknetze durch die Steigerung der Anzahl der Endgeräte multipliziert mit der von jedem mobilen Endgerät benötigten Leistung grob um einen Faktor 1000 erhöhen werden. Das hört sich dramatisch an, ist aber letztlich nichts anderes als eine plakative Projektion der bisherigen Entwicklung. Die Prognose betrifft natürlich nicht nur Provider, sondern auch Betreiber von privaten wireless Infrastrukturen, weil es ja auf Dauer nicht hinzunehmen wäre, wenn ein Mitarbeiter mit seinen mobilen Endgeräten eine erhebliche Service-Degradation erfahren würde, wenn er das Unternehmens-WLAN benutzt.

Ein großer Teil der zusätzlichen Last wird auf Video entfallen. Natürlich benötigt man in einem Unternehmen oder einer Organisation kein Netflix, aber welche Konsequenzen hat die Einführung neuer Dienste wie sie für eine „gesteigerte Benutzererfahrung“ im Rahmen von Kooperationen z.B. zwischen IBM und Apple oder Apple und Cisco oder einfach durch höhere Video-Anteile bei UC mittelfristig flächig eingeführt werden können?

Mit IEEE 802.11ac Wave2 steht ab Herbst 2015 eine neue Evolutionsstufe für WLANs zur Verfügung. Vereinzelt wurde auch schon Wave3 mit einer theoretischen Leistung von 10 Gbps angekündigt. Die wichtigen neuen Funktionen von Wave2 und 3 müssen auf den Prüfstand. Was können sie bewirken? Und: sind sie überhaupt erlaubt? Für die Nutzung von 160 MHz breiten Kanälen in flächendeckenden Infrastrukturen ist eine Erweiterung der bisher zulässigen Frequenzbereiche notwendig. Die ist auf dem Weg, aber erreicht sie uns rechtzeitig?

Aber auch LTE ist in einer permanenten Entwicklung und es entstehen Begehrlichkeiten der Provider hinsichtlich der lizenzfreien Bänder, die bislang den WLANs vorbehalten waren. Betreiber sollten akzeptieren, dass ein Bereich, auf den man normalerweise kaum schaut, erheblich an Wichtigkeit gewinnt:

die Filter- und Verstärkertechnik der Wireless-Transceiver. Durch die immer weiter voranschreitende Füllung der Bänder entsteht die Notwendigkeit, die bisher recht großzügig ausgelegten Lücken zwischen den Bändern zu verdichten, z.B. durch Modulationsverfahren mit höherem Wirkungsgrad. Ohne weitere technische Erläuterungen werden dabei ältere Systeme, die nicht mit der neuesten Transceivertechnik ausgestattet sind, den Kürzeren ziehen.

Das IoT stellt eine eher schleichende Gefährdung dar. Auch hier kann es zu deutlichen Überschneidungen mit unternehmensinternen WLAN-Versorgungsstrukturen kommen.

Schließlich: wie werden die neuen Systeme in die Gesamt-Architektur integriert?

Spätestens bei der Sicherheit könnte man zu dem Schluss kommen, dass durchschnittliche Unternehmen und Organisationen mit konventioneller Technik hier schnell an Grenzen stoßen.

Video als Triebkraft des Massengeschäfts

Das Thema Video führt zu einem Bereich heftiger Entwicklungstätigkeit, nämlich Mobilfunk mit LTE. Provider gehen davon aus, dass Nutzer massenhaft Videos auf ihre immer besser werdenden Endgeräte streamen möchten und sie als Kunden verloren gehen, wenn das nicht richtig klappt. Dazu kommt, dass man mit zunehmender Netzleistung den Kunden relativ einfach Mehrwertdienste anbieten kann, die sie an einen Anbieter binden.

Bislang war die Ausgangslage für private Betreiber eher ungünstig, aber jetzt kommen die „Wave2“-Produkte von 802.11ac. Praktisch alle wichtigen Hersteller haben sie noch für das dritte oder letzte Quartal 2015 angekündigt. Sie erreichen zwar immer noch nicht den gesamten Funktionsumfang, der in 11ac definiert wurde, sind

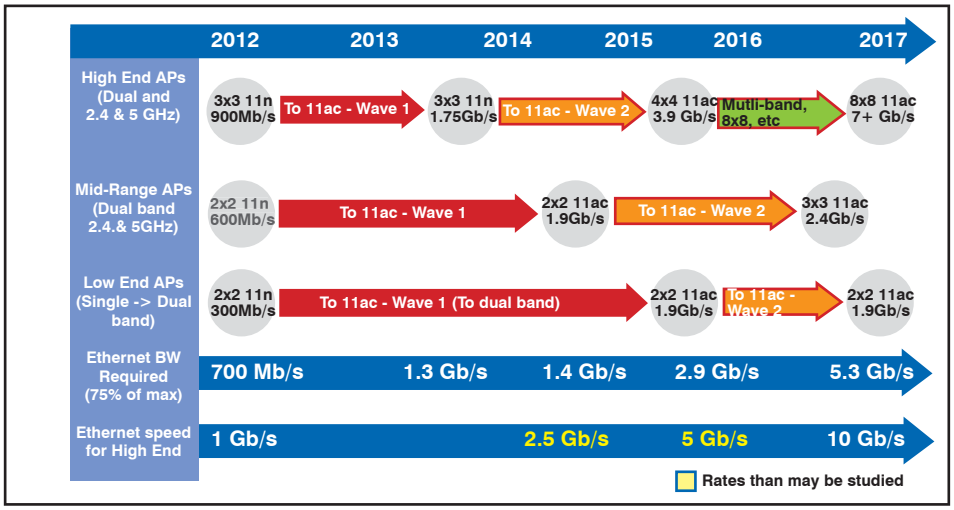

Abbildung 1: 802.11ac Enterprise AP Segmente und Trends

Schwerpunktthema

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

Teil 1

Fortsetzung von Seite 1

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

1. Wofür brauchen wir SBCs?

Da die durchschnittliche Vertrautheit der ICT-Welt mit Session Border Controllern bislang nur mittelmäßig ausgeprägt ist, rollt dieser Beitrag das Thema von der Basis her auf (siehe Abbildung 1.1, Quelle: 2015 UC, SIP and SBC Plans and Priorities; Webtorials 12/2014).

Früher - ja früher war nicht nur alles besser, sondern hatten wir statt IP-basierter Telefonie das ISDN/PSTN Netz. Die Endgeräte waren autorisierte völlig unkriminelle Telefone, das Telko-Netz war ein privates Netz des Telko Providers, die betriebene Anwendung war Voice-only: soll heißen simple Telefonie, auf der Basis vergleichsweise sicherer Leitungsvermittlung (siehe Abbildung 1.2).

Heute sind wir dabei, diese friedliche Umgebung mit einer wesentlich chaotischeren zu tauschen: genutzt werden beliebige Endgeräte, das Netzwerk besteht aus mehreren kaskadierten öffentlichen Netzwerken, die betriebenen Anwendungen sind Multimedia, auf der Basis eines vergleichsweise unsicheren paketvermittelten Netzwerks (wie Abbildung 1.3 zeigt).

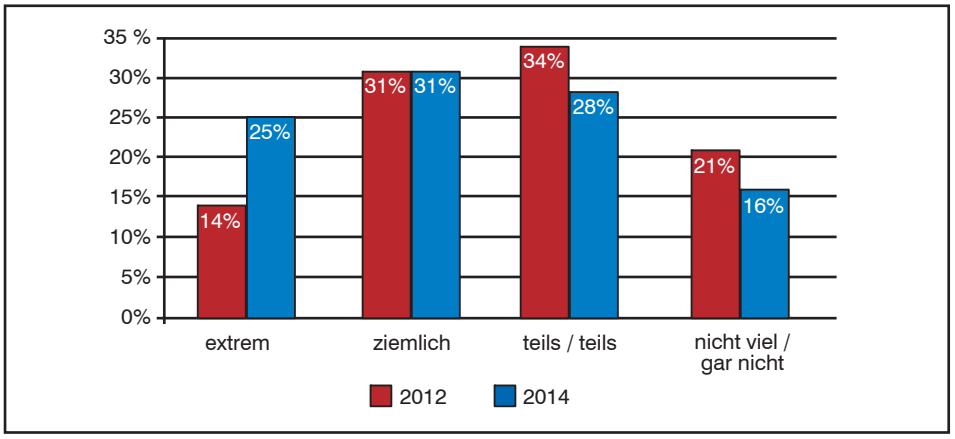

Abbildung 1.1: Vertrautheit mit Session Border Controllern
Quelle: 2015 UC, SIP and SBC Plans and Priorities; Webtorials 12/2014

Der Session Border Controller steht – nicht nur als Schutz- und Trutz-Komponente – an der Grenze zweier unterschiedlicher Netzwerkbereiche und kontrolliert diese, wie der Name "Border Controller" schon sagt. Somit gibt es mindestens eine Aufgabe, die er zuverlässig erledigen muss: den Perimeterschutz. Dies gilt sowohl für Enterprise-Provider-Übergänge als auch für Provider-Provider-Übergänge. Der direkte Übergang zwischen zwei Enterprise-Netzen würde auch unter diesen Schutzbedarf fallen, soweit er tatsächlich ohne zwischengeschaltetes öffentliches Netz vorhanden ist. Letzteres könnte beispielsweise bei der Verbindung zweier Mandanten innerhalb eines privaten Campus-Netzes der Fall sein.

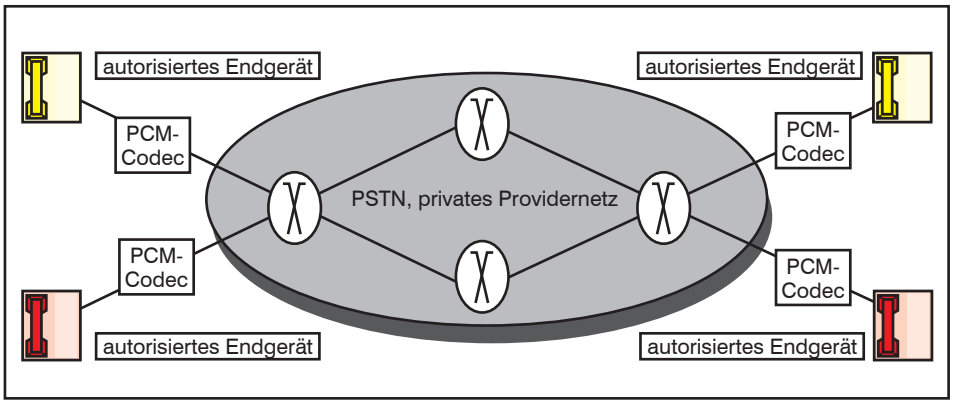

Abbildung 1.2: ISDN Telefonie auf Basis leitungsvermittelter Verbindungen

Der Session Border Controller übernimmt die Aufgabe eines Firewalls für Voice, Video und Multimedia Echtzeitkommunikation.

Das Wort "Session" im SBC bezieht sich auf SIP Sessions. Jetzt werden Sie vielleicht fragen: Warum macht das nicht mein "normaler" Perimeterschutz – der Firewall? Die Antwort ist ebenso leicht wie ärgerlich: Der kann es eben nicht ordentlich. Insbesondere die höchst dynamisch bei Sessionbeginn eines Mediastreams ausgehandelten und dann nur für die Dauer der Session gültigen beliebigen UDP Portnummern zwischen 1024 und 65535 sind der Feld-, Wald- und Wiesen-Firewall ein Greuel. Kurz gesagt:

Session Border Controller: Die Perimeter-Komponente für All-IP - Teil 1

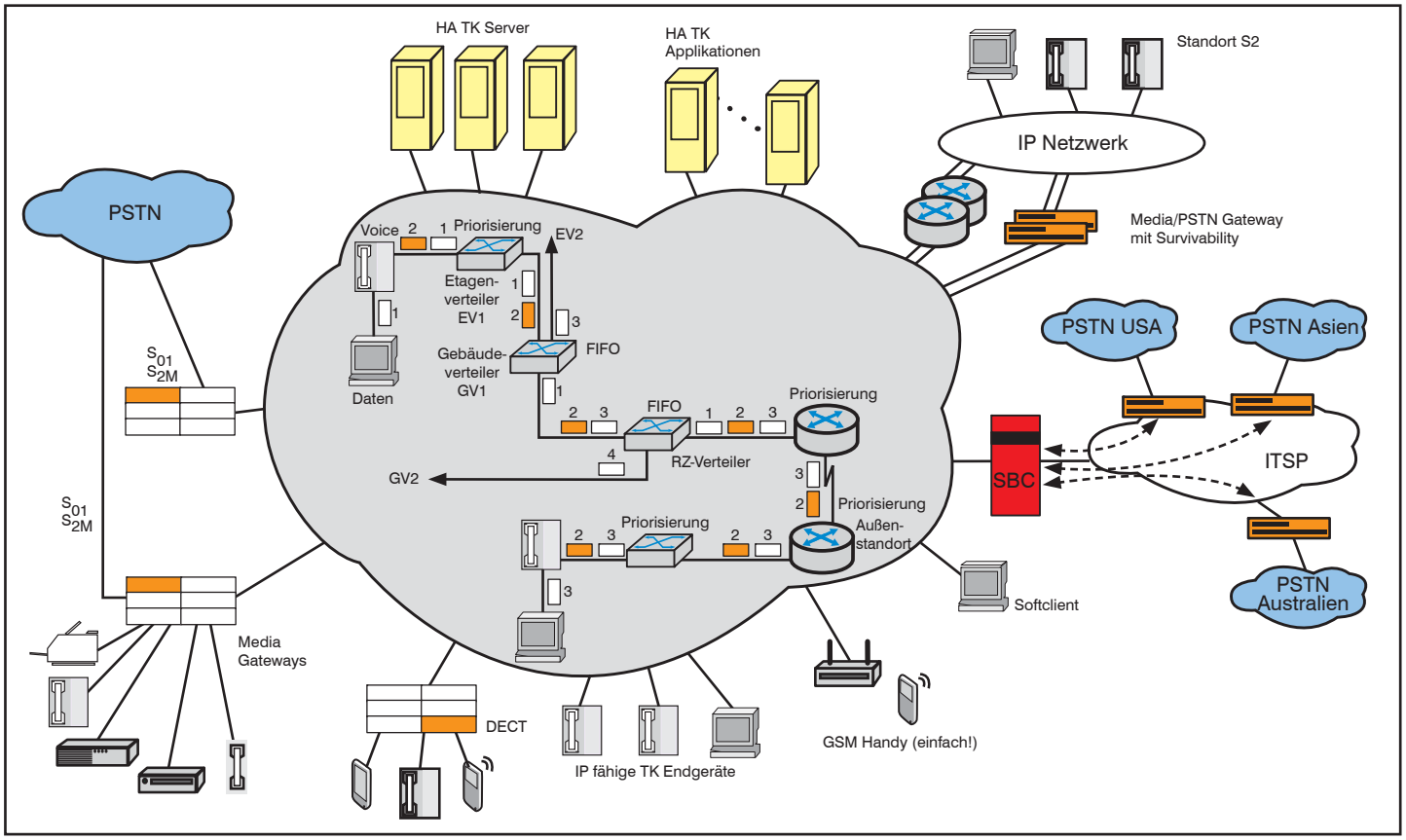

Abbildung 1.3: Multimedia VoIP / SIP Universum auf Basis paketvermittelter IP-Netze

Voice und Video war nie ein Kern-Markt der traditionellen Firewall-Hersteller.

Session Border Controller sind aktuell die einzigen Netzkomponenten, die für den Perimeterschutz und andere Border-Funktionen der Echtzeit-Kommunikation sowohl die Control Plane (SIP Signalisierung) als auch die Data Plane (RTP/RTCP Media Streams) vernünftig integrieren können. Weder Router noch Softswitches/TK-Server noch Firewalls leisten diese Integration. Somit hat sich in den letzten Jahren ein eigener Session Border Controller Markt entwickelt, der den Firewall-Herstellern inzwischen so weit voraus ist, dass sie diesen Vorsprung kaum noch aufholen könnten, wenn sie es denn wollten. De facto ist aber auch gar nicht erkennbar, dass sie es wollen. Vielleicht ist das auch gut so, denn der Session Border Controller als solches ist funktional gewiss ausreichend komplex und kann somit gut auf die spezifischen IT-Firewall-Funktionen verzichten.

Das führt wiederum sofort zu folgender Frage: Wird der Voice- und Video-Verkehr dann gar nicht über den normalen Firewall geführt? Diese Frage lässt sich mit einem klaren Jein beantworten: Typischerweise leistet der IT-Firewall einen Basis-Schutz für den SBC selbst und die Verkehrslasten, die zum SBC durchgelassen werden: Soll heißen, der SBC steht zwischen den IT-Firewalls und diese lassen nur Verkehr von und zu der IP-Adresse des SBC durch: Abbildung 1.4 zeigt die Positionierung eines SBC in der DMZ am Enterprise Perimeter.

Aktuell sind Session Border Controller noch ziemlich Voice-fokussiert, zunehmend erhalten sie jedoch mehr und mehr Multimedia Funktionen, das bedeutet zusätzlich zur Telefonie auch Video, Text-Nachrichten, Datei-Anhänge, Online-Kollaboration und ähnliche Streams zu handhaben. In dieser Rolle sind sie kritische zentrale Echtzeitkommunikations-Komponenten, die zusätzlich zum Perimeterschutz weitergehende Funktionen hinsichtlich Quality of Service und Ver-

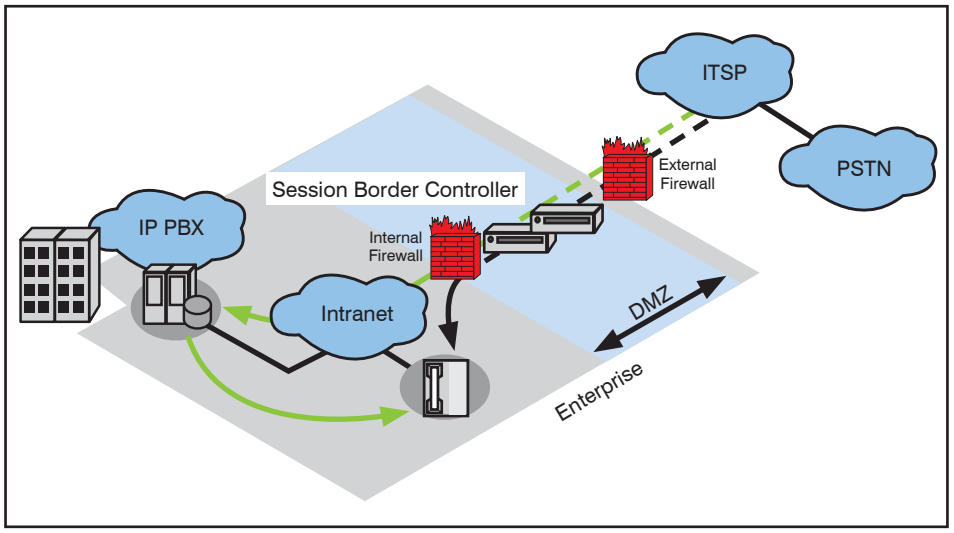

Abbildung 1.4: Positionierung des Session Border Controllers am Enterprise Perimeter

Zweitthema

Kühltechniken im Rechen-zentrum, Alternativen zur klassischen Raumkühlung

Fortsetzung von Seite 1

Dipl.-Ing. Hartmut Kell kann auf eine mehr als 20-jährige Berufserfahrung in dem Bereich der Datenkommunikation bei lokalen Netzen verweisen. Als Leiter des Competence Center IT-Infrastrukturen der ComConsult Beratung und Planung GmbH vermittelt er sein Fachwissen aus umfangreichen Praxiserfahrungen bei der Planung, Projektüberwachung, Qualitätssicherung und Einmessung von Netzwerken in Form von Publikationen und Seminaren.

Methoden der Server-Kühlung

Grob unterteilt erfolgt die Kühlung von Servern in den meisten Rechenzentren mit Hilfe der folgenden Techniken:

Bei der Methode 1 wird der gesamte Raum über einen Doppelboden mit kalter Luft versorgt und auf dem Doppelboden stehen die zu kühlenden Server-Racks relativ unsortiert bzw. verteilt. Die kalte Luft strömt über mehr oder weniger gut verteilte Lochplatten in den Raum oberhalb des Doppelbodens. Diese Methodik findet man eher in kleineren Server-Räumen, wie z.B. bei einer Stadtverwaltung einer kleineren Stadt.

Eine erste und noch einfache Optimierung besteht bei der 2. Methode darin, die zu kühlenden Schränke sinnvoll zu platzieren. Die Schränke werden in Gruppen so aufgestellt, dass die aus dem Schrank rausgeblasene warme Luft nicht durch benachbarte Schränke wieder angesaugt werden kann. Man bildet einen Kaltgang und/oder einen Warmgang. Dieser Gang entsteht zunächst nur durch die geschickte Platzierung der Schränke. Ein großes Problem besteht darin, dass man durch einfaches Platzieren der Schränke nur schwer verhindern kann, dass warme Luft doch auf unterschiedlichen Wegen in den Bereich der kalten Luft geblasen wird und damit natürlich die Effektivität sinkt. Das führt zu Methode 3.

Methode 3 unterscheidet sich zu Methode 2 darin, dass einer der beiden Gänge – der Warm- oder Kaltgang – mit baulichen Maßnahmen gekapselt wird, das nennt man Einhausung. Man verhindert „Luftkurzschlüsse“ und steigert die Effektivität. Diese Methode 3 stellt heute DIE Standardmethode dar zur Kühlung von Server-Schränken in den meisten Server-Räumen. Doch wie die Tabelle unten zeigt, stößt auch diese Methode bei Server-Schränken mit Hochleistungs-Servern irgendwann an ihre Grenzen.

Es ist nachvollziehbar, dass eine Kühlung umso besser funktioniert, je näher das kühlende Element an die zu kühlende Einheit gebracht wird. Darauf zielt die Methode 4 bzw. 5 hin. Bei Methode 4 spielt der Doppelboden als kaltluftzuführendes Element keine Rolle mehr, stattdessen wird kaltes Wasser (oder auch ein anderes Kühlmedium) zu der Server-Rack-Reihe (am besten natürlich mit Einhausung) über eine entsprechende Verrohrung geführt und dort in einen Wärmetauscher. Luft wird über diesen Wärmetauscher geblasen, kühlt sich ab und wird durch die Server geführt.

Methode 5 unterscheidet sich zu Methode 4 darin, dass pro Rack (oder auch pro 2 Racks) ein Kühlgerät bereitgestellt wird und die warme Luft nicht in den Raum geblasen wird, sondern im Schrank oder der Schrankreihe bleibt und durch das Kühlgerät heruntergekühlt wird.

Der wesentliche Unterschied zwischen den Methoden liegt also in der Luftverteilung, das Liefern der Gesamtkühlkapazität und der damit verbundene Energieaufwand bleibt gleich. Die Bitkom gibt für diese Methoden unterschiedliche maxi-

male Kühlleistungen an (siehe Tabelle 1). Deutlich wird, dass die zu wählende Methode im Wesentlichen von der zu erwartenden benötigten Kühlleistung abhängt, sie ist im Prinzip gleich der elektrischen Leistung der im Rack vorgesehenen Komponenten. Ab einer bestimmten geforderten Leistung hat man keine Wahl mehr und wird wassergekühlte Lösungen einsetzen müssen. Nicht alle Klimafachplaner setzen diesen Schwellwert wie in der Tabelle dargestellt erst bei 10 kW/Rack an, häufig wird bereits bei niedrigeren Werten auf Methode 4 oder 5 zugegriffen.

Beschreibung der Lösung	Maximal mögliche Kühllast
Klimatisierung über Doppelboden ohne Bildung von Kalt/Warm-Gang	max. 1 kw/qm bzw. 4 kW/Rack
Klimatisierung über Doppelboden mit Bildung von Kalt/Warm-Gang	max. 2 kw/qm bzw. 8 kW/Rack
Klimatisierung über Doppelboden und Einhausung der Kaltgänge	12-20 kW/Rack
Eigene Klimageräte werden in die Schrankreihen (1 Gerät versorgt mehrere Schränke) gestellt und Warmgang wir eingehaust	ca. 10-25 kW/Rack
Klimatisierung über wassergekühltem Rack (geschlossenes System)	ca. 20-45 kW/Rack

Tabelle 1: Leistungsfähigkeit der verschiedenen Kühlmethoden

Grundprinzip: Kalte Luft in den Server und warme Luft aus dem Server

Bei allen Methoden besteht die Grundforderung, eine kalte Lufttemperatur am Luftansaugbereich der Server- oder Switch-Einheiten bereitzustellen. In sehr vielen Planungskonzepten beruft man sich bei der Festlegung des Temperaturbereiches für die zugeführte kalte Luft auf die ASHRAE (American Society of Heating, Refrigerating and Air-Conditioning Engineers) einem Berufsverband aller in Heizungs-, Kühlungs-, Lüftungs- und Klimaanlagenbau Tätigen in den USA. Diese empfiehlt einen Bereich von 18 bis 27 Grad Celsius. Die Effizienz der Kühlungstechnik nimmt zu, wenn die Temperaturdifferenz zwischen der eintretenden und der austretenden Luft (oder anderen Kühlmitteln) am Kälte erzeugenden Gerät möglichst groß ist, deshalb ist man zunächst einmal bestrebt, möglichst kalte Luft am Klimagerät zu erzeugen und diese mit so wenig Aufwand wie möglich zum zu kühlenden Gerät zu bringen. Dies erfolgt immer mit Hilfe von Lüftereinheiten, welche am effektivsten eingesetzt werden, wenn sie nicht unter Vollast laufen. Das hat zur Folge, dass bei langen „Luftwegen“ entweder die eingeführte Lufttemperatur sehr niedrig sein muss (z.B. 13 Grad Celsius) oder aber die Luftgeschwindigkeit bzw. der Druck sehr hoch. Die zugeführte Luft darf nicht zu kalt sein, sonst wird man mit Kondensationsproblemen rechnen müssen.

Kühlung über den Doppelboden

Da die meisten Serverräume über einen Doppelboden verfügen und auch bei neuen Rechenzentren der Doppelboden in der Regel mitgeplant wird, stellen die Lösungen mit einer Kaltluftzuführung über den Doppelboden die gängigste Lösung dar; ältere Serverräume häufig noch mit Methode 1 und 2, neu geplante Rechenzentren eher mit Methode 3. Das bedeutet, dass ein Großteil der Serverracks in Gruppen angeordnet und eingehaust wird. Die Planung bzw. Dimensionierung einer solchen Kühlung muss sorgfältig durchgeführt werden, u.a. muss festgelegt werden,

- wie hoch der Doppelboden mindestens sein muss, um die Kaltluft zu allen Doppelbodenplatten mit Luftaustritt bringen zu können,
- wie stark die Klimaanlage insbesondere die Lüftereinheit(en) sein muss, um die Luft dorthin zu bringen,
- mit welcher Temperatur die kalte Luft in den Boden eingeblasen wird.

Die geplante raumspezifische Klimainfrastruktur schränkt gegebenenfalls auch die Planungsmöglichkeiten des eigentlichen Rechenzentrumsnutzers oder IT-Fachplaners ein. Beispielsweise die Grundrissplanung bzw. Positionierung der Serverracks kann nicht losgelöst von den vorausgegangenen Planungen der Raumklimatisierung stattfinden, dazu zwei Beispiele.

Das Vorhandensein einer funktionierenden Kühlung über einen Doppelboden bedeutet nicht automatisch, dass die geplante Klimatechnik an jedem Punkt eine ausreichende Kaltluft zur Verfügung stellt. Der Abstand zwischen dem Serverrack und dem Klimagerät, welches häufig auch als CRAC bezeichnet wird (= Computer Room Air Conditioner), kann nicht beliebig groß sein. Ein Irrtum ist die Annahme, dass man mit einer entsprechenden Steigerung der Luftmenge (das erfolgt z.B. über eine Erhöhung der Lüfterdrehzahl am CRAC) jede noch so weite Ecke im Raum erreichen kann. Wird die Luftgeschwindigkeit im Doppelboden zu stark erhöht, so kann dies im Extremfall dazu führen, dass die wärmere Luft oberhalb der Doppelbodenplatten mit Luftaustrittsöffnungen nach unten in den Doppelbodenhohlraum gezogen wird und damit „warme“ Luft in den Boden gelangt. Fachleute sprechen von der maximalen „Wurfweite“ einer CRAC, man empfiehlt als Anhaltspunkt diese auf 12 bis 15 m zu begrenzen.

Sehr häufig steht die Planung der Kabelführung im Doppelboden unmittelbar in Zusammenhang mit der Planung der Schrank- bzw. Reihenpositionen und es muss durch den IT-Planer berücksichtigt werden, dass etwaige Trassen nicht zu einer starken Beeinträchtigung des Luftstromes führen dürfen. Gerade in Räumen, bei denen der Doppelboden aus unterschiedlichen Richtungen mit Luft versorgt wird, erschwert dies die Lage bzw. Ausrichtung der Trassen. Die EN 50174 gibt hierzu beispielsweise eine Empfehlung,

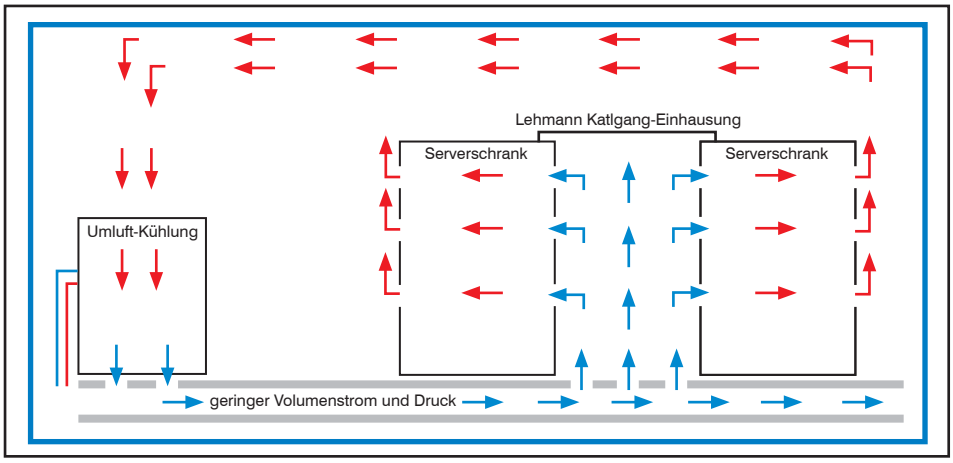

Abbildung 1: Prinzip der Kaltgangeinhausung