

Fachartikel



ALL-IP

IP Access

WLAN

DECT

VoIP

All-IP fest im Griff

Balance zwischen Funktionsvielfalt und Kosten

Bernd Büttner

Der Zeitrahmen ist eng gesteckt. Bis Ende 2018 sollen alle ISDN-Anlagen im Netz der Deutschen Telekom auf All-IP umgestellt sein. Zwar wurden schon viele Umstellungen vorgenommen, doch bleibt noch genügend Arbeit übrig. Jede Umstellung hat ihre eigenen Herausforderungen. Und dabei wollen sowohl das umstellende Unternehmen als auch der Service Provider ihre Kosten im Griff behalten – bei Beibehaltung einer möglichst großen Vielfalt an Funktionen.

Die Umstellung von ISDN hin zu All-IP hat bereits die Phase erreicht, in der die Anzahl der IP-basierten Telefoniezugänge im Hinblick auf die Gesamtzahl vorhandener Zugänge zu festnetzbasierter Telefonie in Deutschland überwiegt. Im Gegensatz zu anderen VoIP/SIP-Anbietern (VoIP – Voice over IP, SIP – Session Initiation Protocol) konnte die Deutsche Telekom im vergangenen Jahr allerdings noch keinen SIP-Trunk-Anschluss anbieten, so dass der bei vielen Geschäftskunden vorhandene ISDN-Anlagenanschluss noch nicht in Richtung All-IP umgestellt werden konnte. Auch das Angebot cloudbasierter IKT-Lösungen ist ausgebaut worden, so dass eine Umstellung auf All-IP auch außerhalb der Geschäftsräume realisiert werden kann.

Leistungsmerkmale transformieren

Trotz allen Fortschritts bei der Umstellung und weiter stetig steigenden All-IP-Anschlusszahlen gibt es noch eine Reihe von Themen zu bewältigen. Viel Aufmerksamkeit wird der Transformation von Leistungsmerkmalen aus ISDN hin zu den IP-basierten Zugängen gegeben. Wie man bestehende ISDN-TK-Anlagen in die neue Welt migriert oder welche konsequent IP-basierten Lösungen möglich sind, bilden hierbei mit die Topthemen rund um All-IP. Daran, wie viele oder auch oftmals wie symmetrisch sich „neu“ gegenüber „alt“ verhält, wird die Qualität bemessen und bewertet. Dabei ist es mindestens so interessant wie wichtig, auch einen Blick auf und vor allem in die Systeme zu werfen, die am Übergang vom Unternehmensnetz hin zum öffentlichen Netz ihren Dienst tun sollen. Diejenigen Systeme, die einen Berg unterschiedlicher Aufgaben bewältigen müssen und sich dabei möglichst einfach in ihrer Handhabung präsentieren sollen.

Speziell sind im Segment kleinerer und mittlerer Geschäftskunden oftmals Systeme zu finden, die eine sehr hohe Anzahl an Leistungsmerkmalen verdichten. Das heißt, neben dem Breitbandzugang per integrierter xDSL-Komponenten kommen eine Reihe weiterer Funktionen und Techniken hinzu. Beispielsweise Onboard Wifi einschließlich der Möglichkeit, zusätzlich Wifi-Zugangspunkte als Gesamtwolke zu verwalten. Die Absicherung des primären Internetzugangs durch zusätzliche, drahtgebundene Breitbandzugänge oder mobilfunkbasiertes Backup etabliert sich mehr und mehr.

Darüber hinaus werden in der jeweiligen Systemsoftware immer mehr Funktionen wie VPN (Virtual Private Network) zur Standortvernetzung oder umfangreiche Telefonieeigenschaften angeboten. Quality of Service (QoS) bildet eine zentrale Funktionalität, die mit dem richtigen Regelwerk aus all den konkurrierenden Datenströmen die richtigen Entscheidungen zur Priorisierung der jeweiligen Datenpakete treffen muss. Alles in allem steigt damit die Komplexität der Systeme. Und die Anforderung, immer mehr Aufgaben parallel zu bewältigen, nimmt ebenfalls zu.

Business Case muss sich rechnen

Auf der anderen Seite sind eine Reihe von Anbietern bestrebt, ihre Serviceaufwendungen im Zuge der Umstellung auf All-IP und den damit verbundenen Installations- und Integrationsaufwendungen so gering wie möglich zu halten, damit sich der Business Case noch rechnet. Aus diesem Grund soll in vielen Fällen der Kunde oder Benutzer die Ersteinrichtung selbst durchführen, um zumindest ein Basispaket an Grundfunktionen in Gang zu bringen.

Bernd Büttner ist Director Strategic Marketing bei der Bintec Elmeg GmbH in Nürnberg

Einer Herausforderung, der sich die Hersteller damit nun gegenüber sehen, ist, Systeme zu schaffen, die auf der einen Seite den Ansprüchen für Geschäftskunden in Funktion und Betrieb gerecht werden, und andererseits deren Einrichtung möglichst so

miert werden kann, oder man möchte einen dedizierten separaten Internetzugang als Ausgang nutzen. Von solchen Überlegungen ist es nicht weit zu Themen wie VLAN (Virtual LAN), Firewall, Wifi-Management usw., die ebenfalls zur Konfiguration anstehen.

genschaften und Empfindlichkeiten nutzen IP. Somit ist im Fall von Störungen oder unerwartetem Systemverhalten die Notwendigkeit gegeben, qualifizierte Analysedaten zu generieren. Optimalerweise direkt aus dem System heraus, in einem allgemein

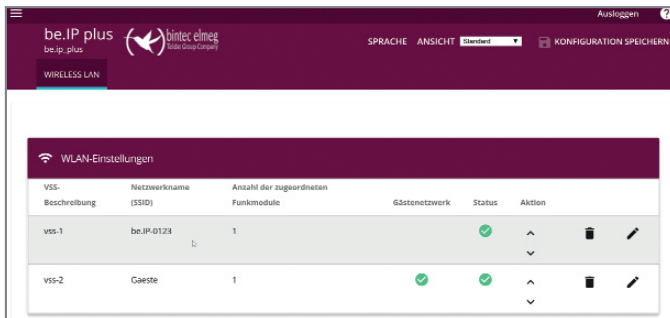


Bild 1: WLAN-Einstellungen im Programmmanager

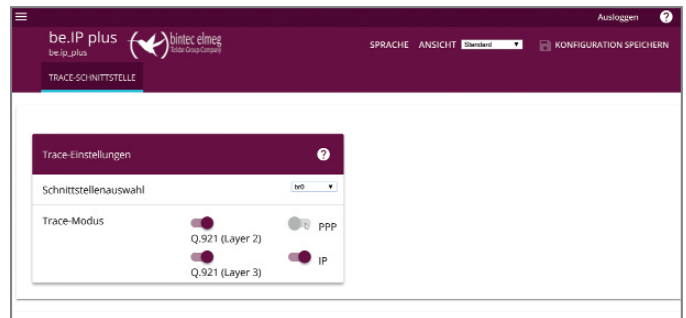


Bild 2: Trace-Einstellungen im Programmmanager

zu vereinfachen, dass kein externer Service zu Rate gezogen werden muss. Dabei werden teilweise auch vollautomatische Provisionierungsmechanismen eingesetzt, bei denen der Benutzer das System nur richtig verkabeln muss. In vielen Fällen ist jedoch ein „in Gang bringen“ eines vom Carrier bereitgestellten Automatismus notwendig. Dabei soll aber immer das Thema IT- bzw. Systemsicherheit nicht zu kurz kommen, damit die Infrastruktur auch die notwendige Robustheit aufweist.

Ein Beispiel

Nehmen wir an, es handelt sich um ein System, das vom Carrier automatisch provisioniert wird, um Grundfunktionen wie Internetzugang, Registrierung von SIP/VoIP-Konten und ein Setup für Basistelefonie bereitzustellen. Als nächstes soll ein drahtloser Zugangspunkt für Gäste und Geschäftspartner eingerichtet werden. Der Zugangsschlüssel wird im Bedarfsfall an die Besucher ausgegeben, so dass diese sich mit ihren Geräten einbuchten können. Man möchte ein solches Netz logisch von den internen Netzen trennen und höchstwahrscheinlich ein spezielles Sicherheitsregelwerk auf dieses Gästenetz applizieren. Weiterhin möchte man sicherstellen, dass die zur Verfügung stehende Bandbreite nicht vollständig konsu-

Also keine triviale Aufgabe, die es zu lösen gilt. Alle notwendigen Funktionen sind in einer Benutzeroberfläche oder anderen Konfigurations-Tools typischerweise zugänglich. Im Zuge der Einrichtung eines solchen Szenarios muss man dennoch einige konzeptionelle Überlegungen anstellen, damit sichergestellt wird, dass man sich keine überraschenden Seiteneffekte, z.B. über eine fehlerhafte Firewall-Konfiguration, einhandelt.

Es geht also darum, alle notwendigen Funktionen zur Einrichtung verschiedener Szenarien in einer Art und Weise zugänglich zu machen, damit auch weniger versierte Benutzer die Möglichkeit haben, sie zu realisieren. Das führt zu einer Aggregation, Abstraktion und Serialisierung von Konfigurationsschritten hin zu einer geführten Konfiguration (Bilder 1 und 2). Wichtig ist dabei, dass diese Art der Konfiguration „reentrant“ ist, d.h., in jedem beliebigen Schritt der Konfiguration ist es möglich, Veränderungen vorzunehmen, ohne dass der Gesamtkontext unbrauchbar oder zerstört wird und in jedem Falle eine lauffähige Konfiguration entsteht.

Im Weiteren zeigt sich auch die Stärke und Professionalität eines Systems in der Art und Weise, wie neben der Einrichtung von Funktionen auch die Erzeugung von Diagnoseinformationen vonstatten geht. All-IP heißt schließlich „Alles mit IP“, also alle Applikationen mit ihren unterschiedlichen Ei-

verarbeitbaren Format. Wenn möglich bereits vorgefiltert, das heißt z.B., nicht den gesamten Netzverkehr aufzuzeichnen, sondern nur den einer bestimmten Schnittstelle, an der das Problem lokalisiert wurde.

Die Reduktion von Komplexität in der Konfiguration hat ihre Grenzen. Diese ergeben sich auch dadurch, dass die Balance zwischen Einfachheit der Konfiguration und Erhaltung des Kontextes nicht verloren gehen darf. Oder anders gesagt: Eine vereinfachte Konfiguration, die eine Firewall nur ein- oder ausschaltet und damit ein kaum nachvollziehbares Regelwerk aktiviert oder deaktiviert, ist fraglich – Sicherheit gibt es nicht auf Knopfdruck. Ein anderes Extrem ist eine schier endlose Kette von Konfigurationsschritten, die alle möglichen und vor allem unmöglichen und de facto kaum relevanten Anwendungsfälle versucht abzudecken und dabei möglichst viele Fallunterscheidungen berücksichtigen möchte.

Es gilt aber in jedem Fall – für spezielle Erweiterungen, Anpassungen oder noch komplexere Szenarien, sind zusätzliche Beratungen und Services unerlässlich. Netzinfrastrukturen, die kabelgebundene und drahtlose Techniken einsetzen und sich der Dynamik ihrer Nutzung und deren Benutzer stellen müssen, brauchen eine sorgfältige Betreuung und hohe Kompetenz in der Konzeptions- und Designphase. (bk)