ComConsult Research

Der Netzwerk Insider

Dezember 2007

Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

WLAN-Controller-Test von ComConsult Research

von Dr. Simon Hoff

Das Controller-basierte WLAN-Design verdrängt immer stärker den traditionellen WLAN-Aufbau mit autonomen Access Points („Fat Access Points"). Die entsprechenden Herstellerlösungen sind teilweise bereits seit mehreren Jahren auf dem Markt. Abgesehen von einem immer noch fehlenden verabschiedeten Standard, sollte man also annehmen, dass WLAN Controller inzwischen stabile und erprobte Geräte sind, über die in professionellen Enterprise WLAN auch Dienste mit hohen Anforderungen an Verfügbarkeit und Leistung des Netzes angeboten werden.

Besonders interessant ist die steigende Nachfrage nach sprachtauglichen WLAN-Lösungen. Je kritischer die über ein WLAN angebotenen Dienste sind, desto wichtiger ist das Monitoring des WLAN, insbesondere der besonders empfindlichen Luftschnittstelle.

weiter auf Seite 17

Zweitthema

Das preiswerte WAN - Utopie oder machbar?

Teil 2: Kostensparende Technik - Ansätze und Grenzen

von Dipl.-Inform. Andreas Meder

Mehr Kapazitäten im Weitverkehrsumfeld schaffen, und dies zu maximal gleich hohen - nach Möglichkeit gar niedrigeren - Kosten; dies ist häufig die Aufgabe, vor der die jeweils verantwortlichen IT-Kräfte in Unternehmen oder Behörden heute stehen.

Dabei können die Gründe hierfür durchaus unterschiedlicher Art sein: Grundlegende Änderungen an den Datenströmen im Weitverkehrsnetz - etwa in Folge einer Neuausrichtung der strategischen Positionierung von Dienste- bzw. Anwendungsservern im Sinne einer Serverkonsolidierung - können einen derartigen Bedarf ebenso auslösen wie der Einsatz neuer Applikationen, die häufig - anders als früher - die technologischen Grenzen zwischen Lokalen Netzinfrastrukturen und solchen im Weitverkehrsbereich schlichtweg ignorieren und damit mindestens einen kräftigen Zuwachs an Bandbreite motivieren wenn nicht gar unumgänglich machen.

weiter auf Seite 6

Kongress

Netzwerk-Redesign Forum 2008

ab Seite 4

Geleit

Sprachqualität und QoS: IP-Telefonie lässt traditionelle TK im Bereich Qualität hinter sich

ab Seite 2

Neues Seminar

Office Communications Server 2007

ab Seite 3

Zum Geleit

Sprachqualität und QoS: IP-Telefonie lässt traditionelle TK im Bereich Qualität hinter sich

Das ComConsult Voice-over-IP Forum 2007 war begleitet von intensiven Diskussionen und zum Teil auch direkten Auseinandersetzungen zwischen den Herstellern. Im Kern der Auseinandersetzungen stand wie zu erwarten Microsoft mit seinem neuen OCS-Produkt. ComConsult-Research stellte seine erste Analyse des Produkts vor und offenbarte überraschende Details zu nicht veröffentlichten Eigenschaften.

Auf jeden Fall schaffte es Microsoft, zu polarisieren. Zwei der andiskutierten Themen zogen sich dabei durch das ganze Forum:

- die Verbesserung der Sprachqualität durch die Nutzung eines Wideband Codecs
- Sinn oder Unsinn von Quality of Service

Microsoft hat seinen OCS mit einem neuen Codec ausgestattet, dem so genannten RTAudio. Dies ist ein adaptiver Wideband-Codec, der sich der Netzwerk-Qualität anpasst und auch bei schlechter Netzwerk-Situation zu akzeptablen Ergebnissen führen soll. ComConsult Research hatte dazu einen kleinen Laboraufbau auf dem Forum beigesteuert, der einen direkten Vergleich der Microsoft-Lösung mit Siemens Open Stage, Cisco 7960, Snom 360 und Polycom Soundpoint IP 650 erlaubte. Der direkte Vergleich machte zudem klar, dass der Microsoft-Ansatz nicht neu ist. Wideband-Codecs gibt es schon seit 20 Jahren, sie sind aber aufgrund der Beschränkungen des Festnetzes kaum zum Einsatz gekommen (ISDN lässt keinen Wideband-Einsatz zu). Neu an dem Microsoft-Ansatz ist die Art der Adaption an belastete und gestörte Netzwerke. Die ersten Analysen von ComConsult Research lassen vermuten, dass der Codec auf die Nutzung im Internet optimiert ist. Einwände von Cisco gingen in die Richtung, dass der Codec auf Leitungen mit stark limitierter Kapazität seinen Delay überproportional erhöht. Wir werden diese Aspekte in den nächsten Monaten weiter untersuchen.

Die zentrale Frage ist nun, wen das überhaupt interessiert. Sprachqualität war bisher im Markt kaum ein Thema. Und hier

zeigte das Forum, dass dies eine Fehleinschätzung sein könnte. Viele Teilnehmer waren angesichts von Sprachübertragung in CD-Qualität doch sehr angetan. Einige anwesende Firmen berichteten von produktiven Nutzungen von G.722 Wideband-Codecs. Die Endanwender reagierten offenbar sehr positiv darauf. Kernpunkt der Kritik: der Übergang ins Festnetz mit G.711 führt im direkten Vergleich zu einem derartig hohen Qualitätsverlust, dass massive Beschwerden an dieser Stelle aufkamen. Aber gerade dieses Beispiel zeigt, dass hier ein Markt ist.

So merkwürdig es auf den ersten Blick klingen mag: Internet-Telefonie ist der Weg in die höhere Sprachqualität! Dies ist für eine Reihe von Anwendungen durchaus entscheidend. Die Qualität einer Video- oder Webkonferenz und die Akzeptanz durch die Benutzer hängen im Wesentlichen davon ab, dass der Eindruck „wir können kommunizieren als wären wir in einem gemeinsamen Besprechungsraum“ gegeben ist. Aus diesem Grund sind Wideband-Codecs bei professionellen Videokonferenzen schon länger Standard. Polycom als einer der führenden Hersteller aus diesem Bereich hat auch erheblich zur Weiterentwicklung dieser Technologie beigetragen.

In der Praxis wird die hohe Sprachqualität zur Zeit auf die Nutzung innerhalb eines Unternehmens allerdings auch über Standortgrenzen hinaus beschränkt. Die Nutzung in der Kommunikation zu Externen ist nur über SIP-Trunks realisierbar. Dies würde aus heutiger Sicht erfordern, dass beide Kommunikationspartner über den SIP-Trunk eines Providers verbunden sind. Auch dies ist Theorie, da zur Zeit keiner der von ComConsult Research befragten Provider Wideband an der Trunk-Schnittstelle unterstützt.

Trotzdem gehen wir davon aus, dass dieses Thema ein Renner wird. Erheblicher Druck wird dabei aus dem Konsumer-Markt kommen. Neue SIP-Telefone wie das Siemens Gigaset S675IP werben mit der HD-Qualität, benötigen aber einen Provider, der dies unterstützt (zum Beispiel Sipgate). Und natürlich kann die HD-Qualität nur genutzt werden, wenn beide Teilnehmer am selben Provider hängen und ein G.722-Telefon benutzen. Trotz dieser Einschränkungen wird klar, dass hier ein Trend geboren ist.

So überraschend es also ist, Microsoft hat mit seiner Quality of Experience Initiative ins Schwarze getroffen. Sprachqualität wird zum Thema. Was dabei allerdings nicht übersehen werden darf, ist, dass das eingesetzte Telefon/Headset erheblichen Einfluss auf die Qualität auch unabhängig vom Codec hat. So kann das Microsoft-Telefon bisher nicht wirklich überzeugen (das Siemens OpenStage ist deutlich besser), allerdings ist das alternativ angebotene USB-Set ein absoluter Renner.

Der zweite Themenbereich, der durch Microsoft wieder zum Leben erweckt wurde, ist der Bereich Quality of Service. Mit der Behauptung, dass QoS unnötig ist und durch die Netzwerk-Hersteller nur gefördert wird, um Netzkomponenten zu verkaufen, hatte Microsoft einen sensiblen Nerv getroffen. Jedenfalls ging hier die Diskussion im Rahmen der Podiumsdiskussion rund, ohne Frage ein Highlight der Veranstaltung. Nun ist dieses Thema komplex, dies zeigt eine Auflistung der Argumente beider Seiten:

- Ohne QoS können Realzeitdienste bei Überlast nicht sauber funktionieren
- Messungen von ComConsult Beratung und Planung GmbH zeigen aber, dass dieses Problem in der Regel gar nicht besteht

Sprachqualität und QoS: IP-Telefonie lässt traditionelle TK im Bereich Qualität hinter sich

- Wer ein Netz hat, das überlastet werden kann, sollte am Netzwerkdesign und nicht an der QoS arbeiten
- Es wird immer Netzwerke wie das WAN geben, in denen zu wenig Kapazität gegeben ist und ohne QoS das Desaster droht
- Messungen von ComConsult Beratung und Planung GmbH zeigen aber, dass selbst in überlasteten Wireless-Zellen mit MOS-Werten von über 4 telefoniert werden kann
- QoS-Design macht Netzwerke komplex, erhöht die Betriebskosten und gefährdet den stabilen Betrieb

Diese Liste gegenseitiger Argumente könnte nun fast beliebig fortgeführt werden und zeigt die Emotionalität dieses Themas. Fast alle Teilnehmer der Podiumsdiskussion standen geschlossen hinter QoS, dagegen standen ComConsult und Microsoft, wenn auch mit sehr unterschiedlichen Sichtweisen.

Wie immer man den Eintritt von Microsoft in den Markt sieht, auf jeden Fall hat er zu einer deutlichen Belebung geführt. Die damit verbundene Diskussion ist wichtig und notwendig, bringt sie uns doch deutlich weiter. Microsoft wird die OCS-Lizenzen bei den großen Kunden sicher großzügig verteilen (vieler dieser Kunden haben aufgrund bestehender CAL-Lizenzen ohnehin das Nutzungsrecht). Die TK-Fraktionen kommen damit in Erklärungsnot mindestens beim Thema Sprachqualität, es ist gut, sich darauf entsprechend vorzubereiten.

In Erwartung eines spannenden Jahres 2008

Ihr
Dr. Jürgen Suppan

Office Communications Server 2007

Die ComConsult Akademie veranstaltet vom 18. - 19. Februar 2008 erstmalig ihr Seminar „Office Communications Server 2007“ in Bonn.

Der Office Communications Server 2007 von Microsoft besitzt ein Potenzial, dessen Sprengkraft nicht zu unterschätzen ist. Das Produkt soll Office-Anwendungen und umfangreiche Kommunikationslösungen integrieren und mittelfristig eine TK-Anlage ersetzen können. Da über 80 Prozent aller Clients Windows und MS-Office nutzen und viele bestehende Lizenzverträge die notwendigen Client-Lizenzen abdecken, wird schnell klar, dass die Hürde der Einführung niedrig ist. Im Moment positioniert Microsoft das Produkt als Ergänzung bestehender TK-Lösungen. Dies senkt die Hürde zum Einstieg weiter, sollte aber nicht darüber hinweg täuschen, dass bereits mittelfristig die Ablösung der bestehenden TK-Welt nach der Microsoft-Roadmap möglich ist.

Im Gegensatz zu seinem Vorgänger, dem „Live Communications Server 2005“, bietet der OCS neben Sprachübertragung nicht mehr nur Instant Messaging (IM) und die Anzeige von Präsenz-Informationen. Zu den wesentlichen Produktmerkmalen des Office Communications Server gehört vor allem eine SIP-Routing-Lösung, die den OCS zum Kern von Micorosofts Unified Communications Strategie macht. Darüber hinaus wurden Features wie Präsenzserver, VoIP Call Management, Audio-, Video-, Webconferencing und Instant Messaging implementiert. Zusammen mit Exchange 2007, Sharepoint und Groove bietet Microsoft somit ein umfangreiches Kollaborations-Portfolio, das in dieser Form mit Einschränkungen ansonsten nur bei IBM zu finden ist.

Die Kooperation mit Nortel erschließt Microsoft die Welt der komplexeren TK-Lösungen (zum Beispiel ACD). Es stellt sich also eigentlich nur noch die Frage, wie schnell Microsoft in der Lage sein wird, zuverlässige Lösungen zu entwickeln und beispielsweise den Softswitch von Nortel mit den Office-Applikationen zu verschmelzen.

In diesem Seminar werden sowohl die technischen als auch die strategischen Aspekte des Office Communications Servers analysiert. Unsere herstellerunabhängigen und neutralen Experten haben sich sehr ausführlich mit den technischen Details befasst und verfügen über langjährige Erfahrung bei der Implementierung von Microsoft-Lösungen, bei der Konzeption von TK-Lösungen sowie bei der Bewertung von Kommunikationstechnologien.

In diesem Seminar soll daher auf folgende Punkte eingegangen werden:

- Microsoft Unified Communications - Ein Überblick
- Komponenten, was steckt dahinter?
- Planung
- Clients und Endgeräte
- Sprachqualität
- Integration mit unterschiedlichen TK-Lösungen
- Integration mit sonstiger Software und Applikationen
- Vor- und Nachteile
- Ausblick

Die Referenten dieses Seminars sind Markus Holländer, Hans-Willi Kremer und Jindrich Slavik

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

☐ Ich buche das Seminar
„Office Communications Server 2007“
18.02. - 19.02.07 in Bonn
zum Preis von € 1.390,- zzgl. MwSt.

☐ Bitte reservieren Sie für mich
ein Hotelzimmer
vom_____bis_____08

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

_____ Vorname

_____ Nachname

_____ Firma

_____ Telefon/Fax

_____ Straße

_____ PLZ,Ort

_____ eMail

_____ Unterschrift

Aktueller Kongress

Netzwerk-Redesign Forum 2008

Die ComConsult Akademie veranstaltet vom 14. - 17. April 2008 das „Netzwerk-Redesign Forum 2008“ in Königswinter.

Netzwerke werden immer stärker integraler Teil von Applikations-Architekturen. Zum Teil sind sie auf Infrastruktur-Aufgaben reduzierbar, aber immer mehr werden sie selber Teil der Lösung.

In 2008 werden folgende Trends die Anforderungen an Netzwerke bestimmen:

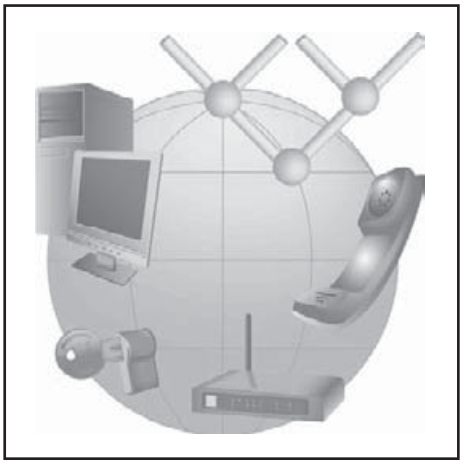
- SOA-basierte Architekuren werden sich weiter ausbreiten. Performance wird dabei eines der Kernprobleme sein. Netzwerke müssen ihren Teil dazu beitragen, dass SOA auch umgesetzt werden kann

- Kollaboration ist der Megahype, der von allen führenden Herstellern in den Markt getragen wird. Allerdings lässt der Begriff viele Freiheiten in seiner Ausprägung. Aus Sicht von ComConsult-Research ist Kollaboration die Kommunikation und Bereitstellung von Information entlang der gesamten Wertschöpfungskette eines Unternehmens. Dies beginnt in der Entwicklung, geht über Produktion und Vertrieb und endet beim Post-Sales-Service. Wir stehen am Beginn einer mehrjährigen Entwicklung, die unser Verständnis von Kommunikation deutlich verändern wird

- Realzeitkommunikation als Teil von Kollaboration wird sich ändern. Zum einen wird Mehrwert innerhalb der Unternehmen geschaffen, aber vor allem wird ein weitergehender Funktionsumfang zwischen verschiedenen Unternehmen geschaffen

- IP-Telefonie als Basis von Realzeit-Kommunikation wird 2008 einen Umbruch erleben. Proprietäre Lösungen sind tot, sie blockieren die Wertschöpfungskette, der Trend wird schnell und massiv zu SIP-basierten Lösungen gehen. SIP verlagert Intelligenz weg von einer zentralen Anlagenkomponente in Endgeräte und somit ins Netzwerk. Das Verständnis von Verfügbarkeit und Qualität von Netzwerken ändert sich wieder einmal

- Der Trend zu Ethernet in der Produktion, der seit Jahren stetig voran schreitet, wird auch 2008 weiter gehen. Damit entstehen immer mehr Teile von Netzwerken, die zwar auf LAN-Technologie basieren, in denen aber eigene Gesetze und Anforderungen gelten



- Die Konvergenz von Netzwerken im Sinne der Integration vom immer mehr Anwendungen in einer einzigen zentralen Infrastruktur wird begleitet davon, dass sich einige der neuen Anwendungen schützen. Es kommen immer mehr Dienste in Netzwerke, die Engpässe und Qualitätseinbrüche erkennen und darauf reagieren. Leider zu Lasten anderer Anwendungen. Dies führt zwingend zu der Frage, wie viel Intelligenz ein konvergentes Netzwerk benötigt

- Mobile Teilnehmer sind weiter auf dem Vormarsch. Immer mehr Bandbreite in Kombination mit immer besseren mobilen Endgeräten führt zur weiteren Ausdehnung der mobil genutzten Anwendungen

- Sicherheit ist weiter die Achillesferse aller Netzwerk-basierten Anwendungen. Mit immer mehr mobilen Teilnehmern und einem immer schwerer zu kontrollierenden Umfeld steigen die Anforderungen an ein gleichzeitig leistungsstarkes wie beherrschbares Sicherheitskonzept

Diese Entwicklungen erfordern ein solides Netzwerk-Fundament. Teile dieses Fundaments sind:

- Ausreichend Bandbreite sowohl im LAN als auch im WAN

- Das Beherrschen von Engpasssituationen, angefangen von der Vermeidung über die Erkennung bis zur Reaktion auf Engpässe

- Eine integrierte LAN/WAN-Architektur

- Netzwerk-basierte Dienste als Teil einer Unternehmens-übergreifenden Lösung

- Leistungsstarke und gleichzeitig einfach zu beherrschende Netzwerk-Produkte

- Applikations-Bewusstsein. Die Idee einer Applikations-neutralen Netzwerk-Infrastruktur, die alles leistet ohne die Applikationen zu kennen, ist gerade auch in Kombination mit der LAN/WAN-Integration nicht haltbar. Auch ist der Begriff Netzwerk nicht auf die reine Bitebene reduzierbar, mehr und mehr werden wichtige Dienste wie Directories oder auch SIP als Teil des Netzwerks und nicht der Applikation gesehen. Spätestens bei der Definition von Service-Level-Agreements und den darauf aufsetzenden Betriebs-Prozeduren wird klar, dass Netzwerke und Applikations-Bewusstsein zusammen gehören. Netzwerke müssen die zu unterstützenden Applikationen kennen und der Betrieb muss diese integrieren

- Eine Netzwerk-Architektur für mobile Teilnehmer. Die Integration in alle notwendigen Geschäftsprozesse an allen denkbaren Orten

- Die Sicherheits-Architektur. Aufbau einer einheitlichen Sicherheits-Lösung für Netzwerke und Applikationen. Die Diskussion um Voice-Sicherheit und der dortige Bedarf nach einer PKI-Infrastruktur zeigt auf, dass eine zentrale Lösung benötigt wird. Aber diese muss auch für kleinere Unternehmen noch beherrschbar sein

Das ComConsult-Netzwerk-Redesign-Forum 2008 wird folgende Fragen analysieren:

- Was müssen Netzwerke leisten, damit SOA umgesetzt werden kann?

- Wie entsteht eine integrierte LAN/WAN-Architektur, was passiert dabei zurzeit und in den nächsten Jahren auf der WAN-Seite?

- Wie können Engpässe beherrscht werden? Wo steht Quality of Service in einem Gesamtbild, wo ist es erforderlich, wo ist es schädlich?

Netzwerk-Redesign Forum 2008

- Welche Netzwerk-basierten Dienste werden an Bedeutung gewinnen, wo sind sie unverzichtbar, um den Gedanken einer Kollaboration entlang der Wertschöpfungs-Kette umzusetzen?
- Applikations-Bewusstsein, was bedeutet das?
- Wie sieht der Bandbreitenbedarf der nächsten Jahre aus? Wo stehen wichtige Anwendungen, die nur über Bandbreite umgesetzt werden können?
- Wo stehen die Hersteller, dreht sich der Markt immer mehr um die Cisco-Achse oder nimmt die Bedeutung anderer Hersteller eher zu? Wo stehen speziell Hewlett Packard und Enterasys?
- Cisco versucht, immer mehr Dienste in die Netzwerk-Ebene zu ziehen, aber ist das wirklich sinnvoll? Welche Dienste sollten im Switch, welche darüber in Servern erbracht werden?
- Mobile Teilnehmer: wie und wo integrieren?
- Beherrschbare und bezahlbare Sicherheit, wie geht das?

Diese Liste ist noch nicht vollständig. Aber sie zeigt bereits, wie spannend die Themen des Netzwerk-Redesign-Forums 2008 sind.

Das Netzwerk-Redesign-Forum 2008 ist für jeden Planer und Betreiber von Netzwerken ein Muss. Zögern Sie nicht, sich rechtzeitig einen Platz zu sichern.
Bis Jahresende können Sie vom vergünstigten Frühbucherrabatt profitieren.

10% Frühbucherrabatt bis zum 31.12.2007

Für Besucher unserer bisherigen Kongresse bzw. für die Teilnehmer am VIP-Verteiler bieten wir auch in diesem Jahr exklusiv eine Vorbuchungsphase für das Netzwerk-Redesign Forum 2008 bis zum 31.12.2007 für eine rabattierte Teilnahmegebühr an.

Die Buchung innerhalb der Frühbucherphase ist verbindlich, kann aber jederzeit auf einen anderen Mitarbeiter Ihres Unternehmens übertragen werden.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung Netzwerk-Redesign Forum 2008

Ich buche den Kongress
Netzwerk-Redesign Forum 2008
14.04. - 17.04.08 in Königswinter

☐ mit Intensiv-Training am letzten Tag
zum Preis von € 1.990,-* zzgl. MwSt.
* gültig bis 31.12.2007 -
dann regulär € 2.190,- zzgl. MwSt.

☐ ohne Intensiv-Training am letzten Tag
zum Preis von € 1.590,-* zzgl. MwSt.
* gültig bis 31.12.2007 -
dann regulär € 1.790,- zzgl. MwSt.

☐ Bitte reservieren Sie für mich
ein Hotelzimmer
vom_____bis_____08

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

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

Zweitthema

Das preiswerte WAN - Utopie oder machbar?

Teil 2: Kostensparende Technik - Ansätze und Grenzen

Fortsetzung von Seite 1

Dipl.-Inform. Andreas Meder ist im Team der ComConsult Beratung und Planung GmbH als Senior Consultant beschäftigt. Er verfügt aufgrund seiner langjährigen beruflichen Praxis über umfangreiche Kenntnisse und Erfahrungen aus den Bereichen Konzipierung und Betrieb von Netzwerken. Sein Themenschwerpunkt als Berater und Planer liegt in den Bereichen Internetworking und IT-Security. Zu diesen Themengebieten ist er als Referent bei der ComConsult Akademie tätig.

Dies erfordert in aller Regel neben einem technologischen Umdenken auch einen sinnvoll geeigneten strategischen Gesamtansatz, um die notwendigen grundsätzlichen Rahmenbedingungen zu schaffen, damit dieses Vorhaben überhaupt gelingen kann. Letzteres wurde bereits in Teil 1 (Anmerkung der Redaktion: Juni-Ausgabe des Netzwerk Insiders, die auf Anfrage zugeschickt werden kann) dieses zweiteiligen Artikels diskutiert; hier soll nunmehr die technologische Seite stärker im Vordergrund stehen.

Aufgabe verstanden - und nun?

Ist das Ziel soweit klar, macht zunächst eine Sichtung der vorhandenen Möglichkeiten Sinn.

Hinsichtlich des grundlegenden technologischen Ansatzes stellt in den allermeisten Fällen aktuell MPLS (Multiprotocol Label Switching) die Methode der Wahl dar. Nahezu immer lässt sich in umfangreichen Netzszenarien schon allein durch eine Ablösung althergebrachter Technologien wie z.B. Frame Relay oder ATM eine deutliche Reduzierung der Kosten erzielen. Oft ist dies sogar dann der Fall, wenn die Umstellung mit punktuellen Verbesserungen hinsichtlich der Anbindungskapazitäten einhergeht. Bleibt es in dieser Hinsicht mehr oder weniger beim Status Quo, kann pauschal ein Kostensenkungspotenzial in einer Größenordung von ca. 50% unterstellt werden.

Freilich soll nicht verschwiegen werden, dass der im Grunde durch seinen „Shared Use“-Ansatz erzielbare und in Form von günstigeren Preisen an den Kunden weitergegebene Synergieeffekt von MPLS (und in ähnlicher Weise aller plattformbasierenden Technologien einschließlich Internet-VPNs (s.u.)) nicht zwangsläufig zum Tragen kommen muss. In manchen Szenarien kann er sich gar ins Gegenteil verkehren. Dies liegt am grundlegenden Konzept: Standorte werden nicht (direkt) miteinander, sondern lediglich mit der Plattform verbunden, über die dann sehr wohl jeder mit jedem kommunizieren kann. Der Kommunikationspfad besteht aber de facto aus drei Teilen: den beiden Anbindungen an die Plattform in Form geeigneter physikalischer Netzverbindungen mit entsprechenden Zugangsknoten (Point of Presence, PoP), meist als „Local Tail“ oder „Local Loop“ bezeichnet, und einer Verbindung dieser PoPs innerhalb des Plattformnetzes. Hieraus resultieren mehrere potenziell problematische Aspekte:

- Die Local Tails werden stets zum nächstgelegenen PoP eingerichtet. Dieser kann sich aber durchaus in einer gewissen räumlichen Entfernung zum Standort befinden. Zwei oder mehr Standorte innerhalb z.B. einer Stadt müssten dann über vergleichsweise teure Local Tails versorgt werden, wenn der PoP entsprechend weit entfernt ist. Dieses Problem kann sich noch verschärfen, wenn besonders hochwertige Redundanzmaßnahmen zur Sicherstellung hinreichender Verfügbarkeiten notwendig sind: wird hier eine Anbindung an zwei verschiedene PoPs gefordert, so werden die zu überbrückenden Distanzen in aller Regel nochmals größer. Andererseits tritt das Problem nur bei Local Tail-Techniken auf, die zumindest anteilig nach Entfernung tarifiert werden (wie bei Festverbindungen, sogenannten „Leased Lines“ in der Regel üblich). Spielt die Entfernung hingegen keine Rolle wie bei DSL-basierten Local Tails, stellt eine solche Konstellation keinen kostenrelevanten Nachteil dar.
- Neben den Kosten ist auch die Kommunikationsqualität zu berücksichtigen: aufgrund der bei Plattformlösungen längeren Gesamtpfade steigt insbesondere die Paketverzögerung im Netz (Network Transit Delay, NTD) gegenüber „direkten“ Verbindungen in den allermeisten Fällen stark an. Dies ist insbesondere zu beachten, wenn derartige Kommunikationsnetze von Anwendungen genutzt werden, die laufzeitsensitiv

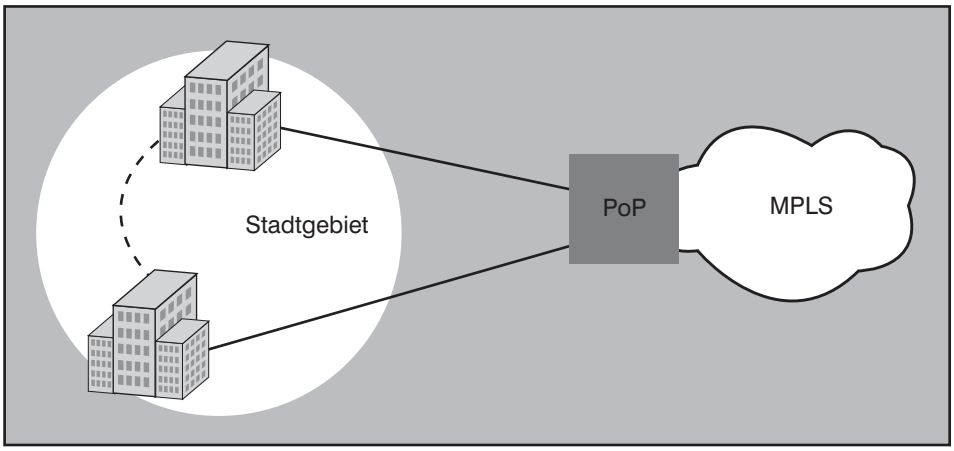


Abbildung 1: Ungünstige MPLS-Konstellation

Das preiswerte WAN - Utopie oder machbar? Teil 2: Kostensparende Technik - Ansätze und Grenzen

sind, d.h. auf höhere Verzögerungswerte im Netz mit deutlich schlechterem Antwortzeitverhalten reagieren oder anderweitig nicht mehr optimal einsetzbar sind. Zu nennen sind hier vor allem dialogorientierte Datenbankanwendungen; aber auch Standard-Mechanismen in Microsoft-dominierten Netzen weisen hier ein ungünstiges Protokollverhalten auf.

- Bei sehr kleinen Netzen (im Extremfall einem, das nur aus zwei Standorten besteht) ist die Gesamtzahl notwendiger Netzverbindungen (Local Tails) höher als bei Netzen auf Basis von Punkt-zu-Punkt-Verbindungen. Auch hieraus - womöglich in Kombination mit dem zuerst genannten Aspekt - resultieren nicht selten erhöhte Kosten gegenüber einer „klassischen" Netztechnologie.

Nichtsdestotrotz wird es heute in vielen Fällen auf MPLS hinauslaufen; ggf. sind einzelne Teile des Gesamtnetzes auf Basis anderer Ansätze zu realisieren. An anderer Stelle in diesem Artikel findet sich ein konkretes Projektbeispiel, bei dem genau von dieser Strategie Gebrauch gemacht wurde.

Nennenswerte Konkurrenz zu MPLS-basierten Installationen stellt lediglich ein Virtuelles Privates Netz (VPN) auf Basis verschlüsselter Kommunikationstunnel durch das Internet dar. Ein solches, typischerweise mittels IPSec (Internet Protocol Security) realisiertes Internet-VPN (auch PI-VPN für „Public Internet"-VPN genannt) bietet üblicherweise die niedrigsten Kosten; im Gegenzug existiert allerdings auch keine oder bestenfalls lediglich rudimentäre Quality of Service (QoS). Wer diesbezüglich - etwa infolge des Einsatzes nicht ausreichend robuster Anwendungen - Mindestanforderungen hat, die über das hinausgehen, was ein PI-VPN leisten kann (typischerweise eine Priorisierung auf dem jeweiligen Local Tail, um den diesbezüglich kritischen Anwendungen zumindest lokal optimale Kommunikationsbedingungen zur Verfügung zu stellen), sollte besser auf MPLS ausweichen.

Wenn es also MPLS sein soll, so stellt sich als nächstes die Frage nach dem Local Tail. Dieser macht üblicherweise einen großen Teil der Gesamtkosten für einen MPLS-Anschluss aus, so dass sich die Wahl einer kostengünstigen Lösung insgesamt sehr positiv auf das verfügbare Budget auswirkt - allerdings sind mit dieser Wahl potenziell Einschränkungen sowohl technischer Natur als auch hinsichtlich der möglichen Service Level Agreements (SLA) verbunden. Prinzipiell steht dabei eine Vielzahl technischer Anbindungsvarianten zur Verfügung; zu den am häufigsten eingesetzten gehören:

- Leased Lines
- DSL
- PI-VPN

Leased Lines stellen die mit Abstand teuerste aber auch qualitativ hochwertigste Variante dar. Dabei spielt es kaum eine Rolle, um welche technische Ausprägung es sich konkret handelt; diese kann je nach Anbieter und Verfügbarkeit vor Ort variieren. Basis ist jedoch in aller Regel SDH (Synchrone Digitale Hierarchie), ein Verfahren, das dem Kunden auf der Basis eines TDM-Mechanismus (Time Division Multiplex) einen festen exklusiv nutzbaren Anteil an der in der Netzinfrastruktur verfügbaren Übertragungskapazität zur Verfügung stellt. Anders als bei z.B. MPLS findet dabei prinzipbedingt keinerlei „Überbuchung" statt; temporär nicht abgerufene Kapazitäten können daher nicht von anderen Kunden genutzt werden. Aus diesem Grund ist SDH-Bandbreite teurer als MPLS-Bandbreite. In letzter Zeit beginnen sich insbesondere Leased Lines auf Ethernet-Basis auf breiter Front durchzusetzen. Hauptgrund hierfür sind neben der Option, über eine weitestgehend transparente Ethernet-Schnittstelle alle wesentlichen Protokollmerkmale übertragen und somit insbesondere auch VLANs über Standortgrenzen hinweg bilden zu können, auch die gegenüber den klassischen Leased Line-Varianten E1 (2 Mbps), E3 (34 Mbps) oder STM1 (155 Mbps) deutlich geringeren Kosten. Letztere wiederum resultieren vor allem aus dem Einsatz erheblich preiswerterer und dabei infolge weniger komplexer Technik robusterer Hardware-Baugruppen. In Deutschland bietet beispielsweise die Deutsche Telekom mit „EthernetConnect" (siehe Kasten) eine derartige Lösung an; von den Mitbewerbern sind meist vergleichbare Produkte erhältlich.

Leased Lines werden üblicherweise nach 2 Kriterien tarifiert (wenn man einmal von der Option auf diverse Redundanzmechanismen, die naturgemäß ebenfalls kostenrelevant sind, absieht): Entfernung und Kapazität, d.h. nutzbare Übertragungsbandbreite. Ersteres ist in der Regel mehr oder weniger fix, d.h. konzeptionell kaum beeinflussbar. Unterschiede ergeben sich hier bei MPLS-Angeboten verschiedener Carrier vor allem deshalb, weil die PoPs naturgemäß unterschiedlich platziert sind: ist der Abstand zum nächsten PoP bei einem Anbieter geringer als beim Mitbewerber, so dürften die Kosten tendenziell auch entsprechend geringer ausfallen.

Hinsichtlich der Kapazität hingegen kann man konzeptionell sehr wohl Einfluss nehmen. Zwar ergibt sich die nutzbare Gesamtbandbreite logischerweise unmittelbar aus dem konkreten Bedarf - oder sollte dies zumindest tun - es gibt aber u.U. verschiedene Möglichkeiten, diese nutzbare Bandbreite technisch zu realisieren. Dies wiederum hängt mit der aus Nutzersicht eher ungünstig ausgefalle-

Das preiswerte WAN - Utopie oder machbar? Teil 2: Kostensparende Technik - Ansätze und Grenzen

nen Staffelung der verfügbaren Local Tail-Bandbreiten zusammen. Die klassischen, direkt auf SDH aufsetzenden Festverbindungen stehen (s.o.) in den Bandbreitenstufen E1 (2 Mbps), E3 (34 Mbps), STM1 (155 Mbps) und - falls es etwas mehr sein darf - auch als STM4 (622 Mbps) und STM16 (2,4 Gbps) zur Verfügung; dort wo anstelle von SDH SONET (Synchronous Optical Network) eingesetzt wird (z.B. in den USA) sehen die Bandbreiten im unteren Bereich übrigens etwas anders aus: anstelle von E1 steht dort T1 (1,5 Mbps) und anstelle von E3 entsprechend T3 (45 Mbps) zur Verfügung.

Diese Abstufungen sind recht grob; es stellt sich schnell die Frage, was zu tun ist, wenn der konkrete Bedarf beispielsweise 4 Mbps beträgt. Die elegante und technisch sauberste Lösung lautet: man nehme die nächst höhere Bandbreitenstufe (in unserem Beispiel also E3/34 Mbps) und beschränke die in der MPLS-Plattform tatsächlich nutzbare Kapazität auf 4 Mbps (diese real nutzbare Bandbreite wird auch häufig als Committed Access Rate / CAR oder Port Speed bezeichnet). Dieser Ansatz funktioniert stets einwandfrei und ohne Einschränkungen. Nachteil: die Kosten - aufgrund des großen Anteils des Local Tails an den Gesamtkosten für einen MPLS-Anschluss wiegt die teure E3-Anbindung schwer!

Kostengünstiger lässt sich eine solche „Zwischenbandbreite“ mittels Link Aggregation abbilden. Hierbei werden mehrere (in unserem Beispiel zwei) schmalbandigere Leased Lines zu einer zusammengefasst, die dann die gewünschte Bandbreite bietet. Je nach Tarif des Anbieters rechnet sich diese Vorgehensweise stets, solange man nicht zu viele Leitungen aggregiert. Im häufigen Fall der Aggregation von E1-Links ist ein E3-Link meist erst ab der (notwendigen) Zusammenfassung von mehr als 6 - 8 E1-Links kostengünstiger. Ein angenehmer Nebeneffekt dieses Ansatzes ist, dass er sich meist gut mit Redundanzmechanismen kombinieren lässt: Existieren zum Zwecke der Link-Aggregierung ohnehin mehrere physikalische Anbindungen, so lässt sich eine redundante Anbindung ohne nennenswerten Mehraufwand hinsichtlich der Netzkapazitäten realisieren.

Dringt man allerdings in Regionen höherer Bandbreiten vor, so rechnet sich der Trick nicht mehr: beispielsweise sind die Kosten für zwei E3-Leitungen und die für eine STM1-Leitung nahezu identisch - letztere bietet aber fast die doppelte nutzbare Kapazität. Lediglich in Verbindung mit ohnehin notwendigen Redundanzmaßnahmen macht hier die Aggregation noch Sinn, wenn also die zusätzliche Anbindung unabhängig von der angestrebten Kapazitätserhöhung ohnehin erforderlich ist.

An dieser Stelle ist ein Hinweis für jene angebracht, die ihr Netz im Wege einer Ausschreibung realisieren lassen, sei es gezwungenermaßen (etwa als öffentlicher Auftraggeber) oder gezielt, um einen möglichst optimalen Preis am Markt zu erzielen: werden Kniffe der beschriebenen Art erwogen, so sollte in den Ausschreibungsunterlagen ausdrücklich auf eine solche Option hingewiesen werden. Da es nur bedingt im Interesse der Anbieter liegt, den Kunden auf Einsparpotenziale hinzuweisen, werden meist die teureren Varianten (s.o.) für das Design gewählt. Fairerweise muss darauf hingewiesen werden, dass die Link-Aggregation auch ihre Tücken hat, aber dazu später mehr…

DSL bietet die Option, Standorte extrem preiswert - zumindest verglichen mit den recht teuren Leased Lines - an den MPLS-Backbone anzubinden. Dabei stehen grundsätzlich beide Varianten, die asymmetrische wie auch die symmetrische, zur Verfügung. Voraussetzung ist natürlich, dass die Technologie am jeweiligen zu versorgenden Standort verfügbar ist und auch die benötigte Kapazität geschaffen werden kann. Da DSL ein Consumer-Produkt ist - nicht zuletzt deshalb ist diese Anbindungsvariante so kostengünstig - kann die lokale Verfügbarkeit stark schwanken, je nach momentaner Anzahl auf die DSLAMs (DSL Access Multiplexer) der Vermittlungsstelle aufgeschalteter Kunden.

Beim Schlagwort DSL ist zu unterscheiden zwischen dem Signalisierungsverfahren (letzteres wird auch bei Anbindungstechniken eingesetzt, wo man es aufgrund der mit dem Begriff verbundenen Assoziationen nicht unbedingt vermuten würde, z.B. EthernetConnect) und einer darauf basierenden Anbindungstechnik. Letztere ist hier gemeint und funktioniert grob gesagt wie folgt:

Die Verbindung zwischen Kundenstandort und Vermittlungsstelle erfolgt über Kupfer-Doppeladern und nutzt DSL als Signalisierung. In der Vermittlungsstelle werden die so übertragenen Daten über meist ATM-basierte Infrastrukturen zunächst zu einem BBRAS (Breitband Remote Access Server) übertragen, dabei handelt es sich um PPP-basierte Zugangssysteme des Anbieters (im Falle eines DSL-basierten Internetzugangs wäre dies typischerweise ein System in einem Internet-PoP dieses Anbieters). Diese Zugangssysteme übertragen die Daten dann zu einem Übertrittspunkt zur MPLS-Plattform. In der Regel erfolgt dies über einen Tunnel durch die Infrastruktur der Telekom unter Einsatz von L2TP (Layer 2 Tunneling Protocol). Dieses

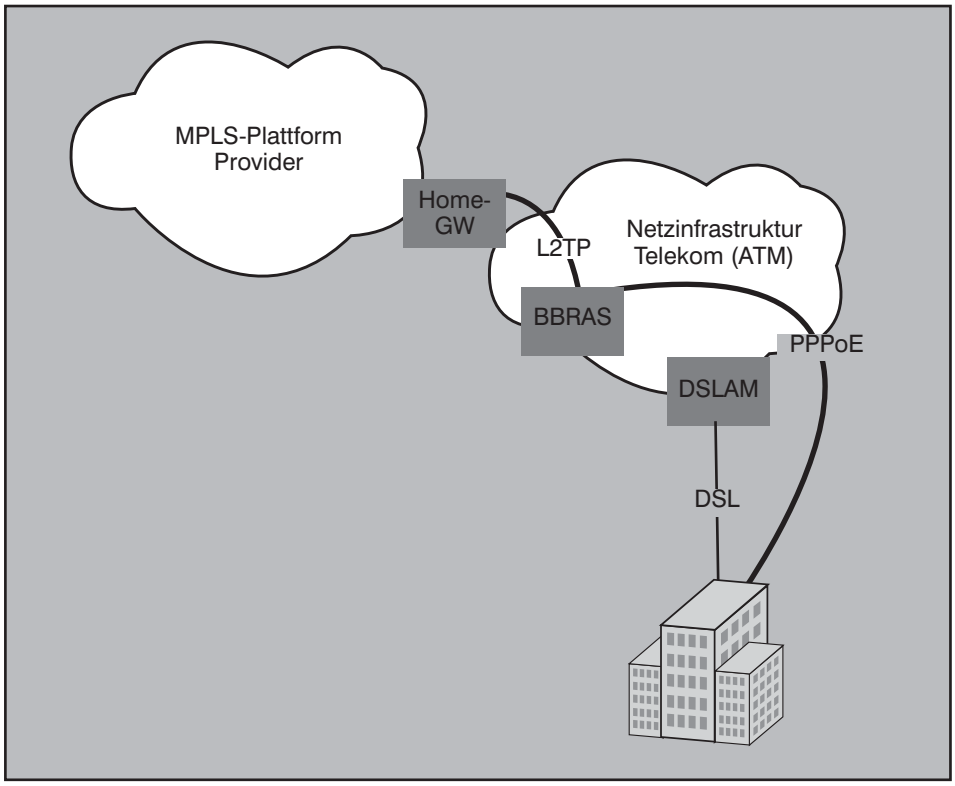


Abbildung 2: DSL-basierter Local Tail (via T-DSL)

Das preiswerte WAN - Utopie oder machbar? Teil 2: Kostensparende Technik - Ansätze und Grenzen

Konstrukt kommt praktisch immer dann zur Anwendung, wenn die Versorgung des Kundenstandorts über T-DSL erfolgt (siehe Abbildung 2). Man erkennt unschwer, dass der Gesamtpfad, dem der Local Tail folgt, nicht unbedingt optimiert erscheint. Schon die Zahl der zu durchlaufenden Einzelbausteine erschwert dies; hinzu kommt noch, dass die Home-Gateways üblicherweise an wenigen (oft nur einer oder zwei) Punkten zentral implementiert sind, wodurch Umwege im Transport der Datenpakete nahezu unausweichlich sind.

Unter günstigen Umständen, z.B. wenn der gewählte MPLS-Anbieter die fragliche Vermittlungsstelle vor Ort mit eigener Netzinfrastruktur versorgt, kann auch eine direkte ATM-basierte Anbindung an die MPLS-Plattform erfolgen, wodurch sich ein deutlich günstigerer Kommunikationspfad ergibt. In diesem Fall lassen sich sogar Service Level bezüglich CoS (Class of Service) vereinbaren, was bei der ansonsten üblichen Methode, wie sie oben dargestellt wurde, nicht möglich ist.

Steht DSL nicht zur Verfügung (aus welchem Grund auch immer), und kommen Leased Lines aus Kostengründen nicht in Betracht, so kann der Local Tail auch auf Basis von **PI-VPN**-Verbindungen realisiert werden.

Bei diesem Ansatz, der insbesondere im internationalen Umfeld zur Anbindung kleiner Außenstellen recht populär ist, wenn die wirtschaftliche Seite des Netzdesigns im Fokus steht, sind die Kommunikationspfade noch weniger optimiert, ja nicht einmal vorhersagbar, so dass im Zweifel mit eher ungünstigen Konstellationen zu rechnen sein wird.

Grenzen der Sparsamkeit

Mittels der dargestellten Ansätze - Einsatz von MPLS, kostengünstige Local Tail-Konstrukte - lässt sich das Budget für die Weitverkehrskommunikation spürbar entlasten, aber wie steht es mit möglichen funktionalen Einschränkungen der resultieren Architekturen? Je nach Art der Einschränkung und der Reaktion der Applikationen und /oder Anwender darauf lassen sich bestimmte theoretische Sparpotenziale möglicherweise nicht verwirklichen - zumindest dann nicht, wenn der geschuldete Service nicht leiden soll. Und einige nicht unwesentliche Nachteile technischer Art weisen die beschriebenen Technologien in der Tat auf; auf diese wollen wir im Folgenden etwas näher eingehen…

Hauptsächlicher Nachteil von **MPLS** ist der im Vergleich zu direkten Punkt-zu-Punkt-Verbindungen erhöhte Transit Delay. „Garantierte" Werte, d.h. SLA-relevante Zusagen der Provider/Carrier liegen hier für nationale Implementierungen typischerweise bei 30 bis 40 Millisekunden; dabei gilt dieser Wert häufig nur für die höherwertigen, d.h. gegenüber nachrangigen entsprechend bevorzugten, Service-Klassen. Für sehr viele Anwendungen reicht ein solcher Wert problemlos aus; insbesondere Web-basierte Applikationen sind hier absolut unempfindlich. Es gibt aber auch sehr kritische Anwendungen, für die ein solcher Wert bereits inakzeptabel schlecht sein kann. An dieser Stelle sind insbesondere Datenbank-Anwendungen mit Fat-Clients zu nennen. Aufgrund ihres Online-Charakters sind solche Applikationen ohnehin potenziell anfälliger; kommen dann noch ein ungünstiges Protokollverhalten und Überstrapazierung des Online-Zugriffs hinzu, werden solche Anwendungen schnell unbenutzbar. Untersuchungen bei festgestellter „schlechter" Performance in Projekten haben gezeigt, dass mitunter mehrere Hundert Request-Reply-Pärchen erforderlich sind, um eine Transaktion abzuschließen - es ist klar, dass sich unter solchen Rahmenbedingungen auch Delays von wenigen Millisekunden schnell zu inakzeptablen Wartezeiten für den Anwender summieren.

Als Beispiel mag der Fall eines Wasserversorgers in Norddeutschland dienen: dort kam in der Vorbereitung einer WAN-Ausschreibung die Frage auf, ob eine MPLS-basierte Lösung auch alle notwendigen Funktionalitäten unterstützen würde. Zur Beantwortung wurde die zukünftig hauptsächlich zu verwendende Applikation einem Test unter Emulation von realistischen WAN-Bedingungen unterzogen. Dabei zeigte sich, dass diese Applikation, ein speziell entwickeltes datenbankbasiertes Warenwirtschaftssystem, extrem empfindlich auf erhöhte Delay-Werte reagiert - dies war bis dato nicht aufgefallen, da die Anwendung ursprünglich nur am Zentralstandort, d.h. unter LAN-Bedingungen zum Einsatz gekommen war. Konkret zeigte sich eine annähernd lineare Abhängigkeit der Transaktionsdauer vom Delay: je Millisekunde One-Way-Delay ergab sich eine Wartezeit für den Anwender von rund einer Sekunde - bei MPLS, das auch in regionalen Szenarien aufgrund der oben beschriebenen prinzipbedingten potenziellen Nachteile kaum unter 10 Millisekunden One-Way-Delay realisiert, hätte dies zu jeweils 10 Sekunden Wartezeit geführt. Und dies, wohlgemerkt, bei jedem auszufüllenden Eingabefeld einer Bildschirmmaske mit rund 10 bis 12 solcher Felder; für eine vollständige Eingabemaske wären also rund 2 Minuten reine Wartezeit zu veranschlagen gewesen - ein aus Sicht der Anwender nicht mehr hinnehmbarer Wert. Aufgrund der (s.o.) ungünstigen Kommunikationspfade wäre die Bilanz bei Verwendung von DSL-basierten Local Tails gar noch verheerender ausgefallen.

Man muss übrigens gar nicht unbedingt „exotische" Spezialapplikationen bemühen, um in die Delay-Falle zu tappen. Hier reichen bereits ganz und gar normale Mechanismen in Windows-basierten Netzwerken. Begibt man sich in einer solchen, ganz gewiss nicht exotischen Umgebung z.B. - unter Zuhilfenahme der so genannten „Netzwerkumgebung" - in einem dreistufigen Verzeichnisbaum auf die Suche nach einer bestimmten Datei, so können die insgesamt angesammelten Wartezeiten, bis die Datei gefunden ist, sich ebenfalls zu erstaunlichen Größenordnungen aufsummieren (siehe Abbildung 3). Dies liegt an der erstaunlichen Zahl von rund 1300 Protokoll-Paketen je Verzeichnisebene, die zwischen Client- und Server ausgetauscht werden, um den jeweiligen Inhalt des Verzeichnisses anzuzeigen.

Man erkennt, dass in einem solchen Szenario in der Tat primär der Delay und erst in zweiter Linie die Bandbreite der limitierende Faktor ist - natürlich macht sich eine geringere Bandbreite spätestens dann bemerkbar, wenn die gefundene Datei übertragen wird…

Interessanterweise tritt der Effekt bei Verwendung verbundener Netzlaufwerke anstelle der Netzwerkumgebung nicht auf: hier sieht der Protokollmechanismus völlig anders aus und benötigt nur rund 15 Pakete je Verzeichnisebene…

Freilich muss auch gesagt werden, dass sich der dargestellte Effekt des in MPLS-Netzen höheren Delaypotenzials primär bei regionalen oder bestenfalls nationalen Szenarien bemerkbar macht. In internationalen Weitverkehrsnetzen sind die Delay-Werte ohnehin aufgrund der Entfernungen so hoch, dass sich der prinzipbedingte Nachteil von MPLS kaum noch bemerkbar macht.

Die Verwendung von **DSL** als Local Tail Technik verschärft in den meisten Fällen die dargestellte grundsätzliche Problematik noch weiter. Aufgrund des in aller Regel spürbar längeren Weges, den die Datenpakete durch die verschiedenen Netzinfrastrukturen zurückzulegen haben, steigt der Delay weiter an. Typische Werte liegen im Bereich um die 60 bis 70 Millisekunden (RTT), einzelne Anbieter geben gar nur SLA-Zusagen für Werte von 100 Millisekunden oder mehr - falls es überhaupt einforderbare Zusagen gibt.

Das preiswerte WAN - Utopie oder machbar? Teil 2: Kostensparende Technik - Ansätze und Grenzen

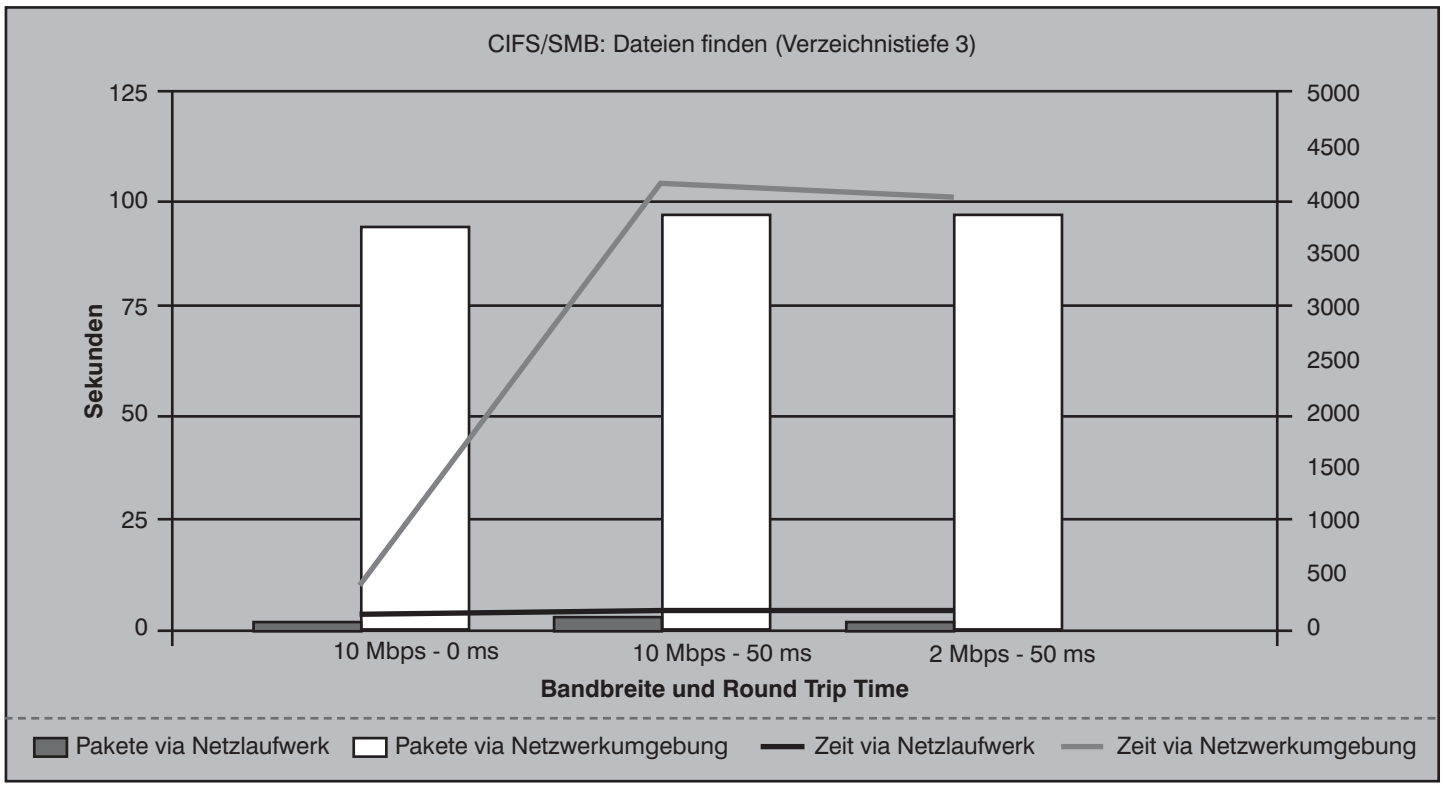


Abbildung 3: Zeitbedarf und Protokollpakete beim Suchen unter CIFS/SMB

Letzteres stellt einen weiteren Nachteil der DSL-Lösungen dar: SLAs sind für die meisten Implementierungen eher rudimentärer Natur; zugesagte Werte sind bestenfalls ungünstig (s.o.), falls es überhaupt Zusagen gibt. In den meisten Fällen ist eine DSL-basierte Lösung als Best Effort Ansatz zu sehen, d.h. das Potenzial ist da, aber Einschränkungen sind jederzeit möglich…

Eine gesonderte Betrachtung verdienen die mit DSL realisierbaren Übertragungskapazitäten. Diese sind zunächst durch die Kupfer-Doppelader zwischen Kundenstandort und Vermittlungsstelle (Teilnehmer-Anschlussleitung, TAL) limitiert: bei großen Kabellängen oder geringem Kabelquerschnitt sinken die erzielbaren Bandbreiten aufgrund der damit einhergehenden erhöhten Dämpfung schnell auf uninteressante Werte oder schließen eine DSL-Nutzung gar vollkommen aus. Es existieren zwar durchaus Techniken, mit denen sich die Nutzbarkeitsgrenze deutlich hinausschieben lässt, z.B. Reach-DSL oder Repeater (s.o.), diese werden aber aufgrund der damit verbundenen Zusatzaufwände nur in Ausnahmefällen eingesetzt.

Wird nun aufgrund der physikalischen Gegebenheiten der TAL ein DSL-Anschluss mit Bandbreite X realisiert, so bezieht sich dieses X zunächst nur auf eben die TAL, genauer: die Verbindung zwischen DSL-Modem und DSLAM. Inwieweit diese Übertragungsgeschwindigkeit auch für die Gesamtstrecke Kundenrouter <--> MPLS-PoP gilt, hängt von der Netzkapazität der Vermittlungsstelle ab. Da DSL-Anschlüsse erheblich überbucht sind (d.h. es wird in der Regel in Summe viel mehr Kapazität an die DSL-Kunden verkauft, als der jeweiligen Vermittlungsstelle auf deren Anbindung an die Backbone-Infrastruktur zur Verfügung steht), kann die je Anschluss nutzbare effektive Bandbreite stark schwanken; meist steht zwar in etwa die zugesagte Kapazität auch zur Verfügung, aber eine Garantie gibt es hierfür nicht.

Zu unterscheiden sind weiterhin die beiden grundsätzlich möglichen DSL-Varianten ADSL (Asymmetrical Digital Subscriber Line) und SDSL. Beim eher auf den Consumerbereich und dessen Nutzungsverhalten zugeschnittenen ADSL beträgt die Upstream-Kapazität typischerweise rund 1/10 der Downstream-Kapazität, während die Geschwindigkeiten bei SDSL für beide Übertragungsrichtungen gleich sind. Somit bietet SDSL insgesamt mehr Potenzial für den Einsatz im Business-/Enterprise-Umfeld, allerdings ist die Technik insgesamt aufwendiger (z.B. wird eine dedizierte TAL benötigt; eine gemeinsame Nutzung für Telefonie und Datenkommunikation ist nicht möglich), was die Realisierbarkeit erschwert (sind TALs frei?) und die Kosten erhöht (SDSL-basierte MPLS-Zugänge können um die dreimal so teuer sein wie ADSL-basierte).

Aus Gründen der Kosteneffizienz wird daher in Anwendungsszenarien, wo die Wirtschaftlichkeit oberste Priorität hat, meist ADSL der Vorzug gegeben. Die stark unterschiedliche Kapazität der beiden Übertragungsrichtungen hat allerdings ihre Tücken: Upload-Vorgänge (beispielsweise das Ablegen einer Datei auf einem zentralen Server oder das Versenden einer E-Mail) dauern nicht nur vergleichsweise lange, sondern sie blockieren gleichzeitig den Donwstream. Anders gesagt: wird der Upstream voll ausgelastet, sinkt die Übertragungsrate auf dem Downstream stark ab; im Extremfall bis auf nahezu Null. Dies erscheint seltsam, wird aber erklärlich, wenn man sich klarmacht, dass die weitaus meisten Anwendungen mit Quittungen arbeiten, d.h. erfolgreich empfangene Daten werden bestätigt. Dabei wird meist TCP (Transmission Control Protocol) eingesetzt; dieses bringt einen solchen Quittungsmechanismus bereits mit, so dass die Applikation kein eigenes Verfahren benötigt. Da sich TCP außerdem den Netzbedingungen (Last, Delay) dynamisch anpasst, passiert nun folgendes: findet in beiden Richtungen rege Kommunikation statt, so brauchen die Bestätigungen des Downstream-Datenverkehrs infolge der geringeren freien Kapazitäten des Upstreams länger als die des Upstream-Verkehrs.

Das preiswerte WAN - Utopie oder machbar? Teil 2: Kostensparende Technik - Ansätze und Grenzen

Deshalb steigt die TCP-Übertragungsrate auf dem Upstream schneller an, wodurch letzterer rasch seine Sättigung erreicht. Ist der Upstream gesättigt, kommt es zu Paketverlusten, insbesondere auch für die Bestätigungen des Downstreams. Hierdurch wird dieser immer weiter gebremst, bis dass ggf. gar keine Übertragung mehr stattfindet, bis der Upstream wieder genügend Kapzitäten für zügigen Bestätigungstransport aufweist.

Dieses Szenario (voller Upstream mit der Konsequenz eines nahezu leeren Downstreams) tritt dabei tendenziell umso eher auf, je mehr Nutzer parallel mit unterschiedlichen Anwendungen arbeiten. Für größere Standorte oder solche, an denen häufiger größere Datenmengen in Richtung Netzplattform zu übertragen sind, sollte daher eher eine SDSL-basierte Anbindung ins Auge gefasst werden…

Für **IP-VPN**-basierte Local Tails gilt sinngemäß das Gleiche wie oben für DSL beschrieben: es kommt potenziell zu erhöhtem Delay und reduzierten bzw. nicht sinnvoll einsetzbaren SLAs.

Bei **Leased Lines** bedarf primär der Ansatz der Link-Aggregation einer genaueren Betrachtung: auch hier können - je nach konkreter Implementierung - Einschränkungen unterschiedlicher Art auftreten.

Es gibt grundsätzlich zwei Arten, wie die Link-Aggregation technisch realisiert werden kann: entweder die einzelnen Links sind voneinander unabhängig und zu übertragende Datenpakete werden über einen Routing-Mechanismus auf diese Links verteilt, um sie mehr oder weniger gleichmäßig auszulasten, oder die Links werden zu einem virtuellen Link zusammengefasst. Letzteres kann z.B. mittes IMA (Inverse Multiplexing Access) oder PPP Multilink (Point-to-Point-Protocol Multilink) erfolgen; in beiden Fällen sorgt der jeweilige Mechanismus dafür, dass die zusammengefassten einzelnen Leitungen sich tatsächlich wie eine einzige Leitung mit entsprechend höherer Kapazität verhalten. Nachteilig sind bei letzterem Ansatz vor allem zwei Aspekte: der Overhead des eingesetzten Protokolls (dieser kann bis zu rund 15% der Brutto-Bandbreite kosten: so stehen etwa bei zwei mittels IMA aggregierten E1-Leitungen in Summe nicht 4 Mbps, sondern lediglich rund 3,4 Mbps zur Verfügung) und der durch das Framing und die damit einhergehende Zwischenpufferung erhöhte Delay. Je nach Verfügbarkeitsanforderungen ist auch noch die Tatsache als Nachteil zu sehen, dass zwar „automatisch" eine Redundanz für die Leitung gegeben ist (ausgefallene Leitungen werden in den Aggregierungsmechanismus nicht mehr einbezogen, Kommunikation bleibt aber möglich, solange mindestens eine Leitung arbeitet), eine Hardware-Redundanz für die Abschlusskomponenten aber nicht möglich ist.

Verzichtet man auf den „Virtual Link", arbeitet also mit einzelnen Leitungen, so muss ein Routing-Mechanismus für die sinnvolle Nutzung aller zur Verfügung stehenden Links sorgen. Dabei kommen mehrere Ansätze in Betracht. Bewährt hat sich in letzter Zeit vor allem die Verwendung des CEF (Cisco Express Forwarding); hierbei werden Datenpakete möglichst gleichmäßig auf alle Links verteilt. Dabei arbeitet der Mechanismus Flow-orientiert, d.h. Datenpakete, die zum selben Datenstrom gehören (erkennbar an den verwendeten IP-Adressen und TCP/UDP-Ports) nutzen stets denselben Link. CEF kommt ohne Overhead aus, beschleunigt den Routingprozess und erhält wie die zuvor dargestellten „Virtual Link"-Mechanismen die Konsistenz der einzelnen Datenströme; dafür wird allerdings die realisierbare Gesamtkapazität je Datenstrom auf die Kapazität eines einzelnen Links beschränkt. Der Ansatz funktioniert also gut, wenn die erhöhte Kapazität einer großen Anzahl von Kommunikationsbeziehungen geschuldet ist (beispielsweise, weil es sich um einen Standort mit vielen Anwendern handelt), aber gar nicht, wenn einzelne Datenströme Bedarf an mehr Bandbreite haben (beispielsweise für nächtliche Datensicherungen).

Soll also im Zweifel die gesamte aggregierte Kapazität nicht nur rechnerisch vorhanden sein, sondern auch einzelnen Kommunikationsbeziehungen/Datenströmen zur Verfügung stehen, muss auf CEF verzichtet werden; stattdessen werden die Datenpakete nach dem Round-Robin-Prinzip reihum auf die zur Verfügung stehenden Links verteilt, und zwar nicht auf Datenstrom-, sondern auf Paketbasis. Dieses Feature ist als ECMP (Equal Cost Multiple Path) in Routern üblicherweise implementiert.

Der ECMP-basierte Ansatz ermöglicht theoretisch die volle Ausnutzung der rechnerischen Gesamtbandbreite; in der Praxis wird diese jedoch so gut wie nie ganz erreicht, da der Round-Robin-Mechanismus keine Rücksicht auf die Paketgröße und die jeweilige Leitungsauslastung nimmt. Wenn deshalb die Paketgrößen ungleichmäßig auf die Links verteilt werden, bleiben auf einzelnen Links Kapazitäten ungenutzt. Dennoch hält sich der Verlust an Kapazität im Mittel durchaus in Grenzen. Viel problematischer ist ein anderer Aspekt der beschriebenen Verteilstrategie für Datenpakete: Da die Laufzeiten auf den einzelnen Links nicht exakt gleich sind (das ist schon wegen Unterschieden in der Leitungsführung zu erwarten - dies gilt insbesondere, wenn zur Erzielung besonders hoher Verfügbarkeiten bewusst getrennte Trassenführung und teilweise sogar verschiedene Zulieferer gewählt werden), kann sich die Reihenfolge der Pakete am empfangenden Router ändern. Dies klingt harmlos und ist es aus Sicht von IP auch; Auswirkungen zeigen sich nur bei TCP-basierten Anwen-

Das preiswerte WAN - Utopie oder machbar? Teil 2: Kostensparende Technik - Ansätze und Grenzen

dungen - letztere stellen aber derzeit die Mehrheit der relevanten Applikationen - in Form eines verminderten effektiven Durchsatzes, d.h. die Anwendung (bzw. das von der Anwendung genutzte Transportprotokoll TCP) nutzt die vorhandene Bandbreite nur zum Teil aus.

Die Erklärung für dieses Phänomen ist vergleichsweise einfach (wenn auch die exakten Details nicht trivial sind): durch die regelmäßige Änderung der Paketreihenfolge bei Empfänger kommt es häufig zu Retransmissions, d.h. erneuten Übertragungen scheinbar verloren gegangener Pakete; dies senkt nicht nur die nutzbare Datenrate aus Sicht der Applikation, sondern führt außerdem dazu, dass TCP eine Überlastsituation im Netz unterstellt und von daher tendenziell weniger Daten übertragt, als eigentlich möglich. Das Problem tritt u.a. deshalb so massiv auf, weil ja nicht nur die übertragenen Daten, sondern auch deren Bestätigungen dieser Änderung der Reihenfolge unterworfen sind.

Versuche im Rahmen eines WAN-Ausschreibungsprojekts (s.u.) ergaben u.a., dass unter den dort gegebenen Rahmenbedingungen einzelne Anwendungssitzungen (hier FTP-basierter Filetransfer, eine Anwendung, die üblicherweise nicht im Verdacht steht, verfügbare Kapazitäten ungenutzt zu lassen…) kaum über 25% der rechnerischen Gesamtkapazität hinauskamen.

Ein Projektbeispiel …

Zur Veranschaulichung der Problematik, ein Weitverkehrsnetz kostengünstig realisieren zu wollen aber trotzdem Mindestanforderungen an die Leistungsfähigkeit erfüllen zu müssen, wollen wir einen Blick auf ein reales Projekt aus der jüngeren Vergangenheit werfen. (Projektzeitraum war hier November 2005 bis September 2006).

Zu realisieren war ein Weitverkehrsnetz, das knapp 100 kleine Standorte mit nur wenigen Mitarbeitern sowie drei größere Standorte mit einem Zentralstandort verbinden sollte. Die bis dato eingesetzten Standard-Festverbindungen geringer Kapazität von 64 kbps (für kleine Standorte) bis 2 Mbps (für größere Standorte) sollten aus Kosten- wie auch Kapazitätsgründen durch eine neue Lösung ersetzt werden. Dabei war ein Gesamtbudget von deutlich unter einer halben Million Euro für eine Vertragslaufzeit von 3 Jahren einzuhalten.

Aus Kostengründen kam für die Masse der kleinen Standorte nur eine MPLS-Lösung mit Local Tails auf ADSL-Basis in Betracht - alternative, höherwertige Ansätze wurden im Wege der Ausschreibung als Option angefragt, erwiesen sich jedoch als deutlich zu teuer.

Für die drei größeren Lokationen musste eine andere Lösung eingesetzt werden, da MPLS infolge der Delay-Sensitivität der Haupt-Anwendung an diesen Standorten nicht in Frage kam: hier war eine maximale Round-Trip-Time von 10 Millisekunden einzuhalten und unter den gegebenen Umständen war mit rund 20 Millisekunden für MPLS-basierte Anschlüsse zu rechnen. Demzufolge wurden hier Leased Lines zur direkten Punkt-zu-Punkt-Anbindung dieser Standorte an den Zentralstandort vorgesehen, die aus Kostengründen die benötigten Kapazitäten von bis zu 8 Mbps für den größten der Standorte mittels Link-Aggregation bereitstellten. Um auch einzelnen Sessions eine nicht auf die Link-Bandbreite beschränkte Kapazität zugestehen zu können, sollte nicht CEF, sondern ECMP zur Anwendung kommen; der Einsatz von Virtual Links (etwa mittels PPP Multilink) scheiterte an der Delay-Anforderung.

Alle Anbindungen der Zentrale, d.h. die Anbindung an die MPLS-Plattform sowie die Leased Lines zu den größeren Standorten, waren beidseitig redundant auszulegen.

Als Besonderheit war außerdem die Anforderung nach Schutz der Kommunikationswege durch Verschlüsselung zu berücksichtigen. Hierzu wurde der Einsatz einer IPSec-basierten Verschlüsselungslösung vorgesehen, die analog zu den WAN-Anbindungen ebenfalls mit Redundanzmaßnahmen hinreichend ausfallsicher auszulegen war.

Im Zuge der Realisierung und mehr noch der Abnahme der WAN-Installationen zeigte sich, dass in der Tat die oben beschriebenen Effekte auftraten - und noch einige weitere, für die die Verschlüsselung verantwortlich war:

- Bei der Vorbereitung der Abnahme stellte sich heraus, dass FTP-Dateitransfers nur rund 25% der rechnerischen Gesamtkapazität ausschöpften. Die Ursache lag, wie oben dargelegt, in der Unverträglichkeit der TCP-Mechanismen mit der zwangsläufig anfallenden Änderung der Paketreihenfolge aufgrund des Einsatzes von ECMP. Vergleichende Lastmessungen auf UDP-Basis ergaben hier Durchsätze von annähernd 100%.

- Während der Abnahme, die statt mittels FTP-Dateitransfers mit einem speziellen Lastgenerator durchgeführt wurde, der mehrere parallele Anwendersitzungen simulieren kann, wurden dann höhere Werte um 50% erreicht. Das erneute deutliche Verfehlen der Zielmarke 100% resultierte vermutlich aus dem Verhalten der IPSec-VPN-Systeme: diese verwerfen aufgrund ihrer sehr restriktiven Konfiguration Pakete bei fehlerhafter Reihenfolge, wodurch bei steigender Last die Zahl der dadurch veranlassten Retransmissions nochmals zunahm; Konsequenz war die beschriebene Durchsatzlimitierung. Hier hätte durch entsprechende Änderung der Konfiguration der VPN-Systeme möglicherweise eine Besserung der Situation erreicht werden können; dies wurde jedoch aus Sicherheitsgründen nicht in Erwägung gezogen.

- Die VPN-Systeme sorgten für eine Erhöhung des Delay-Wertes um ein bis zwei Millisekunden, wodurch an einem Standort die 10 Millisekunden-Vorgabe nicht ganz eingehalten werden konnte.

- Bei den per ADSL versorgten kleinen Standorten war bei anliegender Last auf dem Upstream (d.h. Paketfluss vom Standort zur Zentrale) praktisch kein Datenverkehr auf dem Downstream mehr möglich. Dies war aus Kostengründen hinzunehmen, zumal infolge der geringen Personalstärke an diesen Standorten die gleichzeitige Nutzung der Datenverbindung in beiden Kommunikationsrichtungen eher die Ausnahme als die Regel darstellte.

- Das Umschalten zwischen den redundanten Pfaden dauerte insgesamt deutlich länger als zuvor erwartet; dies lag an dem notwendigen Zusammenwirken der Router und der VPN-Gateways, um wieder zu einem stabilen Routing auf Basis einer konsistenten Wegeinformation zu gelangen. Letzteres betraf allerdings vor allem das Rückschalten nach Wiederherstellung des Normalzustands; hier wurden vorübergehende Instabilitäten festgestellt, die u.a. zu vereinzelten Kommunikationsaussetzern (Paketverluste) führten. Allerdings war nach spätestens zwei bis drei Minuten wieder ein vollkommen stabiler Zustand erreicht.

Zur Illustration sind in Tabelle 1 exemplarisch einige der während der Abnahme am Zentralstandort ermittelten Messwerte wiedergegeben.

Fazit

Grundsätzlich sind die beschriebenen kostengünstigen WAN-Techniken geeig-

Das preiswerte WAN - Utopie oder machbar? Teil 2: Kostensparende Technik - Ansätze und Grenzen

Lfd. Nr.:	Test	Vorgehensweise	Standort A RTT: 6 ms				Standort B RTT: 8 ms			
			Durchsatz in Mbps		Unterbrechungs-dauer in Sec.		Durchsatz in Mbps		Unterbrechungs-dauer in Sec.	
			Up	Down	hin	zurück	Up	Down	hin	zurück
0	Bandbreite nominal		8,0	8,0			4,0	4,0		
1	Regelbetrieb		5,1	4,9			2,4	2,5		
2	WAN Router RZ aktiv	Abschalten Router	2,7	2,6	10	55	1,7	1,7	10	25
3	WAN Router RZ passiv	Abschalten Router	2,8	2,5	15	30	1,7	1,7	15	60
4	WAN-Switch RZ aktiv	Abschalten Router	5,0	2,5	10	75	2,5	1,7	150	75

Tabelle 1: Abnahme-Messwerte im Beispiel-Projekt (Auszug)

net, um funktionsfähige Netze zu realisieren. Es ist allerdings stets genau zu prüfen, ob die jeweiligen Rahmenbedingungen den Einsatz bestimmter Technologien zulassen, oder nicht; dabei muss, wie das Projektbeispiel zeigt, nicht zwangsläufig eine homogene technische Lösung angestrebt werden. Punktuell höherwertige Verfahren einzusetzen, um trotz eines insgesamt von der Wirtschaftlichkeit diktierten Designansatzes die jeweiligen Qualitätsansprüche zu befriedigen, kann eine sinnvolle Vorgehensweise sein.

Auch extrem preiswerte Anbindungen auf DSL- oder PI-VPN-Basis erfüllen ihren Zweck und können somit verwendet werden; bei DSL sollte allerdings besonders sorgfältig geprüft werden, ob nicht einer symmetrischen Anbindung bei umfassender Abwägung von Kosten und Nutzen gegenüber der deutlich kostengünstigeren asymmetrischen Variante der Vorzug zu geben ist.

Die je nach Anbindungsdesign resultierenden Eigenheiten sind dabei auch bei der Spezifikation von Abnahmekriterien zu berücksichtigen, damit nicht fälschlicherweise Abnahmemessungen zu negativen Ergebnissen führen, obwohl nur die gewählte Messmethode für den zu messenden Parameter ungeeignet war. Soll beispielsweise das Vorhandensein einer nutzbaren IP-Bandbreite von X Mbps nachgewiesen werden, so kann (bei Link-Aggregation mit den beschriebenen Effekten) eine anwendungsbasierte Messung (FTP-Download) falsche Resultate liefern; in diesem Fall muss eine andere Messmethode angewendet werden. Umgekehrt macht eine Messung mit reiner IP-Last keinen Sinn, wenn die Anforderung lautet, für bestimmte Anwendungen einen bestimmten Durchsatz zu erzielen. Letztlich ist, wenn man eine Abnahmemessung auch als Grundlage zur Spezifikation von Referenzwerten im Sinne eines Baselining versteht, aber meist der Applikations-orientierten Methode der Vorzug zu geben, da dieser Wert derjenige ist, den die Anwender bei der Applikationsnutzung „erleben“; die möglichen Abweichungen vom rechnerischen Sollwert sind dabei aber geeignet zu berücksichtigen.

Dort, wo die generellen, flächendeckenden Anforderungen an die Lösung mit den kostengünstigen Ansätzen aufgrund der damit verbundenen Einschränkungen nicht erfüllt werden können, muss jedoch allen grundsätzlichen Optionen zum Trotz zwangsläufig weiterhin eher kostspielig gebaut werden. Doch Vorsicht: auch bei Einsatz der prinzipiell „besten“ Technik ist man vor Effekten wie den beschriebenen nicht vollständig gefeit. Als abschließendes Beispiel mag hier eine Messung in einem emulierten WAN mit einer Kapazität von 34 Mbps (entsprechend einer E3-Verbindung) dienen: mit steigendem Delay (der bei zunehmender Entfernung unausweichlich ist) sinkt auch hier der Durchsatz für die einzelne Kommunikationssitzung merklich.

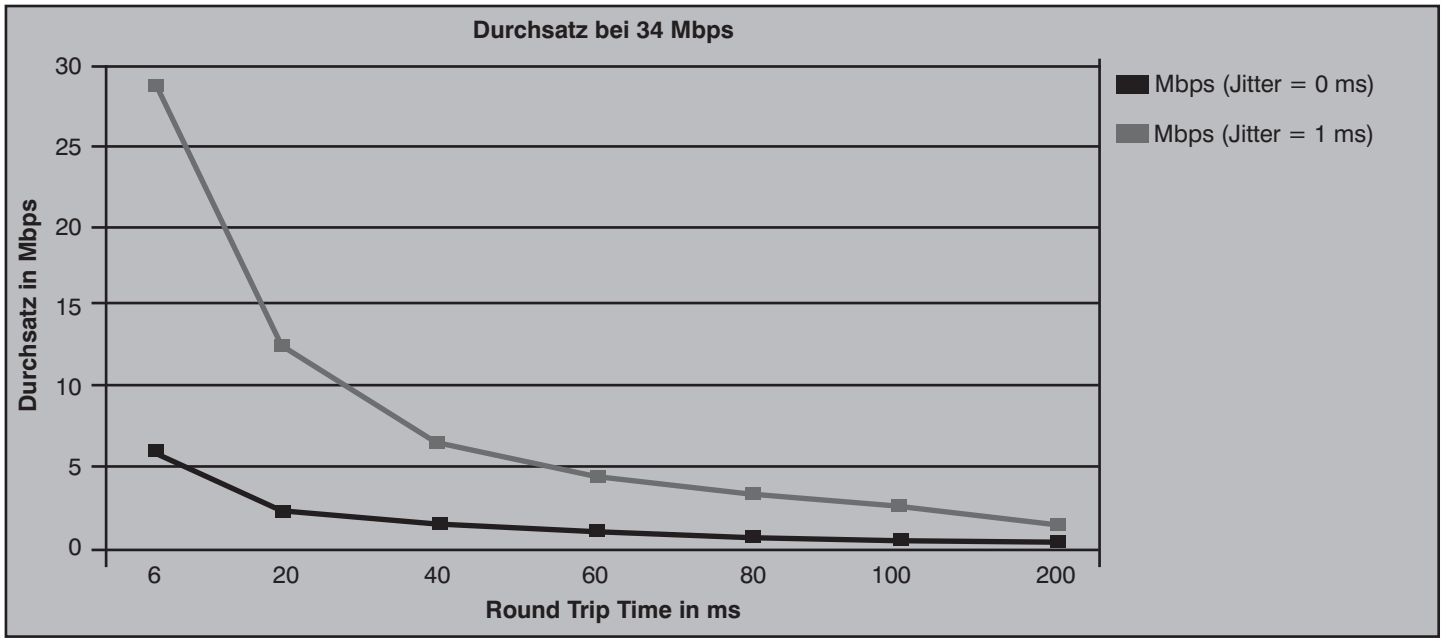


Abbildung 4: Emulierte Durchsatzwerte bei E3 (gemessen mit QCheck)

Das preiswerte WAN - Utopie oder machbar? Teil 2: Kostensparende Technik - Ansätze und Grenzen

Dies liegt daran, dass die Standard-Pufferkapazität von TCP für die heutigen schnellen Netze nicht mehr ausreicht: bei hohem Delay ist die für das Senden der pufferbaren Datenmenge notwendige Zeit kürzer als der Delay, so dass es zu Idle-Zeiten kommt.

Kommt nun noch eine Änderung der Paketreihenfolge infolge vergleichsweise geringfügiger Laufzeitdifferenzen auf unterschiedlichen Pfaden hinzu, so sind die zu verzeichnenden Performance-Einbrüche dramatisch (siehe Abbildung 4).

Konsequenz: Mit steigender Geschwindigkeit Techniken, die eine Änderung der Paketreihenfolge verursachen oder begünstigen können, mit Bedacht und nur nach sorgfältiger Vorplanung einsetzen …

EthernetConnect

EthernetConnect bezeichnet ein relativ neues Produkt der Deutschen Telekom im Weitverkehrsmarkt; die neutrale Bezeichnung des technischen Verfahrens lautet „Ethernet over SDH“. Die Idee hinter diesem Produkt, das bei den Mitbewerbern in der Regel ebenfalls erhältlich ist, wenn auch mit einem anderen Produktnamen, ist es, Business-Kunden mit entsprechendem Bedarf die Möglichkeit zu bieten, die aus den Lokalen Netzwerkinstallationen vertraute Ethernet-Technik auch WAN-seitig einzusetzen und insbesondere die Protokoll-internen Mechanismen, die bei Verwendung klassischer WAN-Technologien wie ATM, Frame Relay oder auch „nacktes“ SDH beim Übergang vom LAN zum WAN verloren gehen, auch über Standortgrenzen hinweg nutzen zu können. „Prominentes“ Beispiel ist hier die Bildung Virtueller Lokaler Netze (Virtual Local Area Networks, VLAN) auf der Basis von 802.1q.

Einige statistische Daten (Quelle: T-Systems 2007) belegen sofort das Potenzial einer solchen Technologie:

- Ca. 95% aller lokalen Netzwerke basieren auf Ethernet-Technologie.
- Allein in Deutschland existieren mehrere 100.000 Lokale Netze auf Ethernet-Basis.
- Die absoluten Installationszahlen für Ethernet-Technologie weisen nach wie vor ein starkes Wachstum auf.

Darüber hinaus scheint der Markt nach einer Lösung zu verlangen, die nach dem Motto „das WAN wird zum LAN“ die Kopplung der immer leistungsfähiger werdenden lokalen Ethernets ohne Einbußen an Leistungsfähigkeit und Qualität ermöglicht. Das Ganze soll natürlich zu vertretbaren Kosten möglich sein. Immerhin sind ultraschnelle LAN-Ports heute für extrem kleines Geld erhältlich; da sollte diese Technologie doch auch im Weitverkehrsumfeld erschwinglich sein…

Teilweise stimmt das auch, obwohl natürlich LAN-ähnliche Rahmenbedingungen (rein passive Infrastruktur zwischen den aktiven Ethernet-Ports) im WAN allenfalls im Metropolitan Area Network (MAN) Bereich gegeben sind. Dort kann über rein passive Glasfaserverbindungen („Dark Fibre“) Ethernet zu niedrigen Kosten geliefert werden, die insbesondere unabhängig von der gelieferten Bandbreite sind. Aufgrund der beschränkten Längen und der zunehmenden Schwierigkeit, bei größer werdenden Entfernungen direkte Glasfaserstrecken zwischen den zu versorgenden Anschlussorten vorzufinden (selber bauen ginge natürlich, würde aber die Kosten explodieren lassen) kommt dieser „echte“ Ethernet-Ansatz in den meisten WAN-Szenarien nicht in Betracht. Stattdessen nutzt man die vorhandenen SDH-Infrastrukturen und bildet das Ethernet-Protokoll darauf ab. Damit beschränkt sich das Kostensenkungspotenzial aber auf die preiswertere Netzabschlusstechnik; immerhin reicht dies im Zusammenwirken mit der höheren Robustheit der Technik (und damit niedrigeren Betriebs- und Unterhaltungsaufwendungen) aus, um EthernetConnect tatsächlich preiswerter anbieten zu können als klassische Verbindungsvarianten.

Ein immenser auch kostenrelevanter Vorteil für den Kunden ist übrigens, dass EthernetConnect in vergleichsweise granularen Bandbreitenabstufungen angeboten wird (s.u.); hierdurch lassen sich leichter maßgeschneiderte Kapazitäten realisieren und damit unnötige Kosten durch nicht genutzte Reserven vermeiden.

Die wesentlichen Eigenschaften des Produkts sind - kurz zusammengefasst:

- EthernetConnect realisiert - analog zu klassischen SDH-basierten Produkten - eine direkte Punkt-zu-Punkt-Verbindung.
- Diese Verbindung ist permanent und fest geschaltet; die jeweiligen Kapazitäten stehen exklusiv zur Verfügung.
- Der Transport der Daten erfolgt - im Backbone - über die SDH-Hochgeschwindigkeitsplattform der Telekom (aktuelle Bezeichnung: SDH2000+).
- Die Bandbreiten sind im Bereich von 2,5 Mbps bis 1 Gbps skalierbar.
- Internationale Verbindungen sind (in der Regel) möglich (in den Bandbreitenvarianten 10 Mbps und 100 Mbps).

Im Wesentlichen erhält der Kunde also vergleichbare Eigenschaften wie bei der unmittelbaren Nutzung von SDH; allerdings mit anderen Bandbreitenabstufungen und einer wesentlich einfacher zu bedienenden Schnittstelle.

Das Produkt steht dabei in drei unterschiedlichen Varianten mit jeweils diversen Bandbreitenstufen zur Verfügung:

- **EC 10M** (auf Basis Kupfer- oder Glasfasertechnologie) mit den Bandbreiten 2,5 Mbps, 5 Mbps und 10 Mbps
- **EC 100M** (auf Basis Glasfasertechnologie) mit den Bandbreiten 10 Mbps, 50 Mbps und 100 Mbps
- **EC 1G** (auf Basis Glasfasertechnologie) mit den Bandbreiten 150 Mbps, 300 Mbps, 600 Mbps, 900 Mbps und 1 Gbps

Die Varianten unterscheiden sich dabei nicht nur in den realisierbaren Kapazitäten:

EC 10M wird üblicherweise - je nach Bandbreite - über eine bis vier Kupfer-Doppeladern realisiert. Dabei wird zwischen dem Kundenanschlussgerät (NT 10 ETH mit Übergabeschnittstelle 10Base-T oder 100Base-T via RJ45-Buchse) und dem nächstgelegenen Telekom-Netzknoten SDSL (Symmetrical Digital Subscsriber Line) zur Signalisierung verwendet. Alternativ ist auch eine glasfaserbasierte Anschlussrealisierung möglich. Aufgrund der Verwendung von SDSL beträgt die Reichweite lediglich um die 3 km; wie die meisten aus dem privaten DSL-Umfeld wissen, kann diese Angabe je nach konkreter Qualität der Leitung (insbesondere Kabelquerschnitt) schwanken. Nach Telekom-Aussage ist eine einmalige Reichweitenverlängerung durch Einsatz von Repeatertechnik möglich - vorausgesetzt, ein Repeatereinsatz scheitert nicht an den Rahmenbedingungen (fehlende Infrastruktur, z.B. Spannungsversorgung).

Das Management der SDH- und der SDSL-Funktionen erfolgt bei dieser Anschaltevariante über den SDSL-Protokolloverhead.

EC 100M wird über Glasfaser realisiert und nutzt SDH bis zum Kundenstandort. Als Kundenanschlussgerät kommt demzufolge ein Add-Drop-Multiplexer (ADM) mit Übergabeschnittstelle 10Base-T oder 100Base-T via RJ45-Buchse zum Einsatz.

Das Management erfolgt Ende-zu-Ende SDH-basiert.

EC 1G wird ebenfalls über Glasfaser realisiert und nutzt SDH bis zum Kunden-

Das preiswerte WAN - Utopie oder machbar? Teil 2: Kostensparende Technik - Ansätze und Grenzen

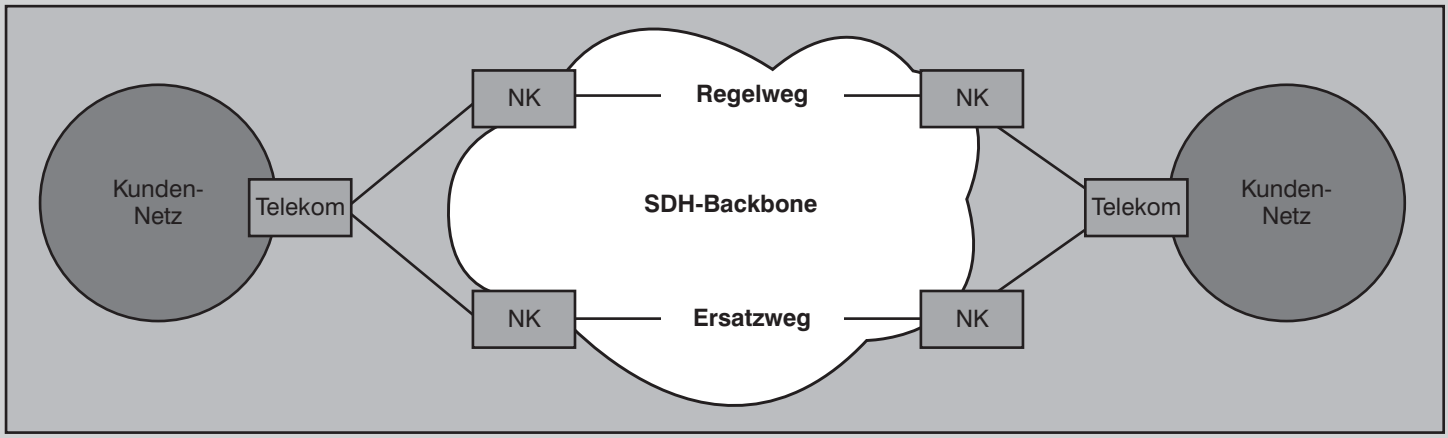


Abbildung 5: Prinzip HPS1

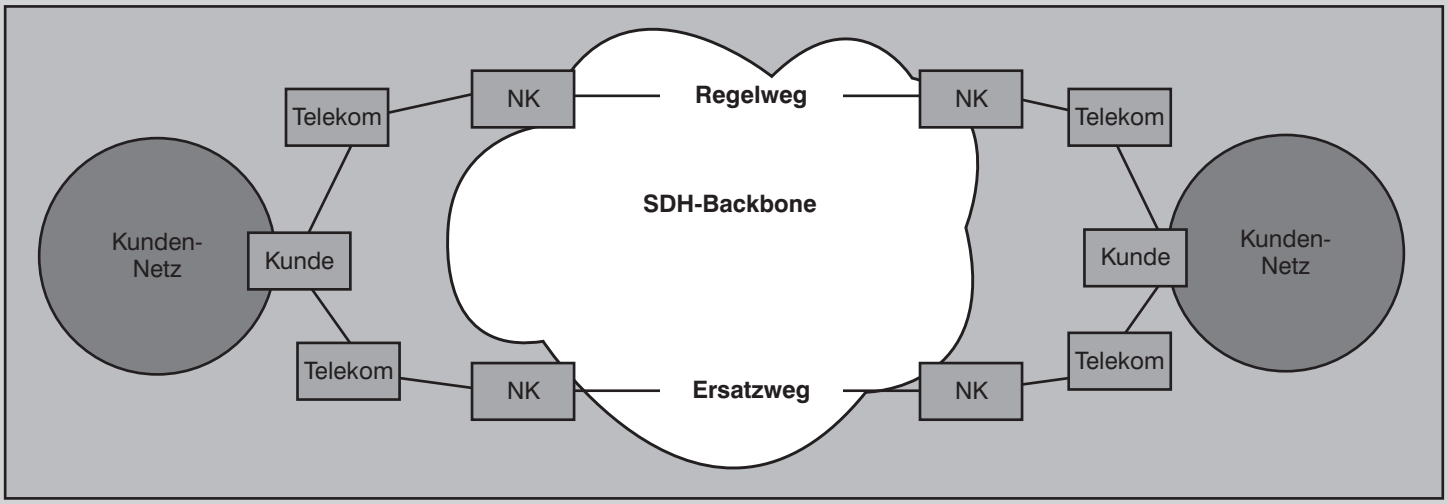


Abbildung 6: Prinzip HPS2

standort. Als Kundenanschlussgerät kommen ADVA FSP-Systeme (Fiber Service Platform) oder entsprechende Add-Drop-Multiplexer (ADM) mit Übergabeschnittstelle 1000Base-SX zum Einsatz.

Das Management erfolgt in der Plattform SDH-basiert; die Kundenendgeräte werden per DCN-Router (Data Communication Network) mit ISDN-Anschluss administriert.

Hinsichtlich der zugesicherten Verfügbarkeiten derart realisierter Verbindungen stehen verschiedene Optionen zur Verfügung, die Standard-Verlässlichkeit von 99,2% zu variieren.

Wirtschaftlich besonders interessant ist die Option, zwei separate Wege innerhalb der Plattform per Loadsharing zu einer entsprechenden Gesamtbandbreite zusammenzufassen. Der dabei in den Kundenanschlussgeräten eingesetzte Mechanismus LCAS (Link Capacity Adjustment Scheme) sorgt für die Synchronität der der beiden Pfade. Allerdings gilt die Verfügbarkeitszusage von 99,2% nur für die halbe Gesamtbandbreite; dies liegt daran, dass der „Backup“-Pfad, der standardmäßig als Ersatz für den Regelweg bei einer vorliegenden Störung dient, ja aktiv genutzt wird. Fällt nun einer der beiden Pfade aus, fällt der von diesem Pfad bediente Bandbreitenanteil ersatzlos weg. Diese Option steht für die Bandbreiten 5 Mbps (= 2x 2,5 Mbps), 10 Mbps, 300 Mbps und 600 Mbps zur Verfügung; 900 Mbps lassen sich sogar ausschließlich nur auf diese Weise realisieren.

Da bei dieser Option der stets geschaltete Backup-Pfad aktiv genutzt wird, also keine zusätzlichen Kapazitäten freigehalten werden müssen, entsteht der Telekom ein gewisser Kostenvorteil, den sie an den Kunden weitergibt; hieraus resultieren niedrigere Kosten (Ausnahme: wenn die Backbone-Struktur überhaupt nicht in Anspruch genommen wird, entsteht kein Preisvorteil; dies ist bei Verbindungen innerhalb der Ortszone 1 der Fall). Allerdings sind gewisse Einschränkungen bei der Verfügbarkeitszusage in Kauf zu nehmen. Soll über geschickte Mechanismen anstelle einer Kostenreduzierung eine erhöhte Verlässlichkeit erreicht werden, muss anders vorgegangen werden - auch hier existieren entsprechende Angebote, allerdings nur für die Varianten 100M und 1G:

Diese von der Telekom mit High Performance Solution (HPS) bezeichnete Option existiert in drei Varianten und erhöht die zugesicherte Verfügbarkeit auf bis zu 99,99% (im Jahresmittel). Die Varianten HPS1 und HPS2 setzen das Vorhandensein einer knoten- und kantendisjunkten Anbindung der Kundenstandorte voraus und unterscheiden sich in der Nutzbarkeit des Ersatzwegs: dessen Bandbreite kann (jenseits von Störungsfällen) nur bei HPS2 genutzt werden, allerdings liegt dann die Umschaltung im Fehlerfall in der Verantwortung des Kunden (siehe Abbildung 6) - bei HPS1 wird diese durch das Kundenanschlussgerät geleistet (siehe Abbildung 5). Die Variante HPS3 ist nicht mit einer Standardspezifikation hinterlegt, sondern bezeichnet eine individuelle Konzipierung der Anbindung in Abstimmung mit dem Kunden.

Das preiswerte WAN - Utopie oder machbar? Teil 2: Kostensparende Technik - Ansätze und Grenzen

Über die bisher dargestellten (Standard-) Dienstmerkmale hinaus können folgende Leistungsmerkmale (gegen zusätzliche Berechnung) hinzugebucht werden:

- VLAN-Tagging - zur Erweiterung virtueller LANs über Standortgrenzen hinweg
- Port-basierte Verkehrssteuerung - zur Bevorzugung von Voice-Datenverkehr; für letzteren wird standardmäßig ein Anteil von 20% der Gesamtkapazität vorgesehen
- VLAN-basierte Verkehrssteuerung - wie Port-basierte Verkehrssteuerung, allerdings ohne Notwendigkeit eines separaten Voice-Netzes; die Erkennung erfolgt wahlweise über eine entsprechend gesetzte User Priority oder eine eigene VLAN-ID für den Voice-Datenverkehr
- Point-to-Multipoint - zur sternförmigen Anbindung mehrerer (Außen-) Standorte an eine Zentrale (Hub-and-Spoke)

Zu beachten sind - vor allem bei Vorhandensein entsprechend sensitiver Applikationen - die Paketverzögerungswerte (NTD) auf den realisierten Verbindungen. Diese fallen zwar günstiger aus als bei MPLS; sie erreichen jedoch nicht die guten Werte direkt SDH-basierter Verbindungen. Dies liegt vor allem am notwendigen Ethernet-Framing: die hierzu notwendige Pufferung verzögert den Ende-zu-Ende-Pakettransport. Aktuell stellt die Telekom hier die in Tabelle 2 dargestellten Maximalwerte in Aussicht - dabei ist zu beachten, dass es sich um One-Way-Delays handelt; zum Vergleich mit den ansonsten (insbesondere aus Anwendungssicht) verwendeten Round Trip Werten, wie sie z.B. auch durch ein Ping ermittelt werden können, sind die angegebenen Zahlen daher zu verdoppeln:

EthernetConnect	10M		100M		1G
Geschwindigkeitsvariante	2,5 M	10 M	10 M	100 M	alle
Metro-Bereich	5 - 11	4 - 7	2 - 4	2	2
Regio-Bereich (bis 200 km)	7 - 13	6 - 9	4 - 6	4	4
National	12 - 18	11 - 14	9 - 10	9	9

Tabelle 2: Network Transit Delay für EthernetConnect (One-Way-Delay)

Schwerpunktthema

WLAN-Controller-Test von ComConsult Research

Fortsetzung von Seite 1

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.

In diesem Artikel wird eine Auswahl von marktgängigen Controller-basierten WLAN-Lösungen hinsichtlich dieser Anforderungen betrachtet. Das Ziel ist dabei nicht die Feststellung, welche Lösung die beste ist. Es geht in diesem Artikel darum, zu untersuchen, ob es Stand heute noch allgemeine Schwachstellen gibt, die in Planung, Ausschreibung und Betrieb besonderes berücksichtigt werden sollten.

1. Controller-basiertes WLAN-Design im Überblick

In einem Controller-basierten WLAN-Design werden WLAN-Funktionen durch zentral positionierte WLAN Controller realisiert und die Aufgaben der Access Points auf die reine Funkübertragung reduziert. Daher werden Access Points in einem Controller-basierten Design oft auch als Thin Access Points bezeichnet. Es sind auch andere Bezeichnungen gebräuchlich, wie Lightweight Access Points. In der IETF erarbeitet die Gruppe CAPWAP (Control and Provisioning of Wireless Access Points) einen Standard für einen Controller-basierten WLAN-Aufbau.

Die Kommunikation zwischen WLAN Controller und Thin Access Point erfolgt typischerweise über einen IP-Tunnel (siehe Abbildung 1). Über diesen Tunnel wird die gesamte Kommunikation von und zu den WLAN-Clients sowie alle Daten für das Management der Thin Access Points transportiert. Die WLAN Controller operieren dabei auf Layer 2, d.h. die Layer-2-Pakete der WLAN Clients werden über den Tunnel zwischen Access Point und WLAN Controller übertragen.

Der wesentliche Vorteil, der sich aus dem Tunnelmechanismus zwischen Thin Access Points und WLAN Controller ergibt, ist der Aufbau des WLAN als Overlay-Netz und der damit verbundenen Abstraktion von der Struktur des zu Grunde liegenden Transportnetzes.

Das Controller-basierte Design bietet weiterhin die folgenden Vorteile:

- vollständige zentrale Kontrolle der Konfiguration (Parameter und Firmware) der Thin Access Points
- Access-Point-übergreifendes Monitoring der Luftschnittstelle
- Load-Balancing zwischen Thin Access Points
- Optimierung von zeitkritischen Operationen, wie Handover und Authentisierung durch zentrale Realisierung im WLAN Controller

Für den Aufbau eines WLAN kann bei einer Controller-basierten Lösung die vorhandene LAN-Infrastruktur genutzt werden. Durch die Verwendung von IP-Tunneln besteht analog zu einem VPN eine logische Trennung des WLAN-Verkehrs von der sonstigen Kommunikation im LAN. Bei entsprechenden Sicherheitsanforderungen kann im Ausnahmefall eine weitergehende Trennung durch VLAN oder sogar eine separate physikalische Infrastruktur für das WLAN, d.h. eigene aktive Komponenten, erfolgen.

Die Thin Access Points werden also typischerweise unmittelbar am vorhandenen Access Layer an einen Access Switch angeschlossen. Da der Daten-Verkehr der WLAN-Clients zwischen Thin Access Points und WLAN Controller getunnelt wird, ist das LAN dabei für die WLAN-Endgeräte vollständig transparent.

Der Vorteil, der sich durch den Tunnelmechanismus ergibt, hat auch seine Tücken, denn jeglicher Verkehr muss durch den Controller. Stellt man sich ein Filial-Szenario vor, bei dem WLAN-Controller in der Zentrale aufgestellt sind und Thin Access Points in den Filialen über eine WAN-Strecke angebunden werden, kann sich folgende Situation ergeben: Wenn in einer Filiale von einem WLAN-Client eine Datei zu einem lokalen Drucker geschickt wird, müsste der gesamte Verkehr erst in die Zentrale zum WLAN Controller und dann wieder zurück zur Filiale. Die kostbare WAN-Strecke würde also nicht nur unnötig, sondern sogar gleich doppelt passiert. Zur Lösung dieses Problems bieten die meisten Hersteller die Möglichkeit den Verkehr lokal am Thin Access Point auszukoppeln. Damit gehen natürlich die Eigenschaften des Overlay-Netzes verloren, und es würde sich wieder die Situation des Anschlusses traditioneller Fat Access Points an ein Distribution System ergeben. Dies wäre damit verbunden, dass Distribution System und Access Points ein flaches Layer-2-Netz bilden müssten, wenn ein Handover unter Beibehaltung der Ende-zu-Ende-Kommunikation ermöglicht werden soll (was insbesondere für die Übertragung von VoIP über WLAN der Fall wäre).

Manche Hersteller empfehlen das Auskoppeln auch für den Campus-Bereich für Verkehr mit hohen Bandbreitenanforderungen und für delay-sensitiven Verkehr. Wie gesagt, der Preis sind massive Einschränkungen in Mobilität bzw. die Rückkehr zum Layer 2 Distribution System. Die Frage, ob bei einer Sprachübertragung der Tunnel zum WLAN Controller spürbar ist oder nicht, lässt sich nicht generell beantworten. Sofern hier im LAN kommuniziert wird und nicht stark verzögerungsbehaftete WAN-Strecken passiert werden, sollte der Effekt sich eigentlich in Grenzen halten. Ein weiterer Einfluss kann sich durch die Leistungsfähigkeit des WLAN Controllers ergeben. Die Betrachtung die-

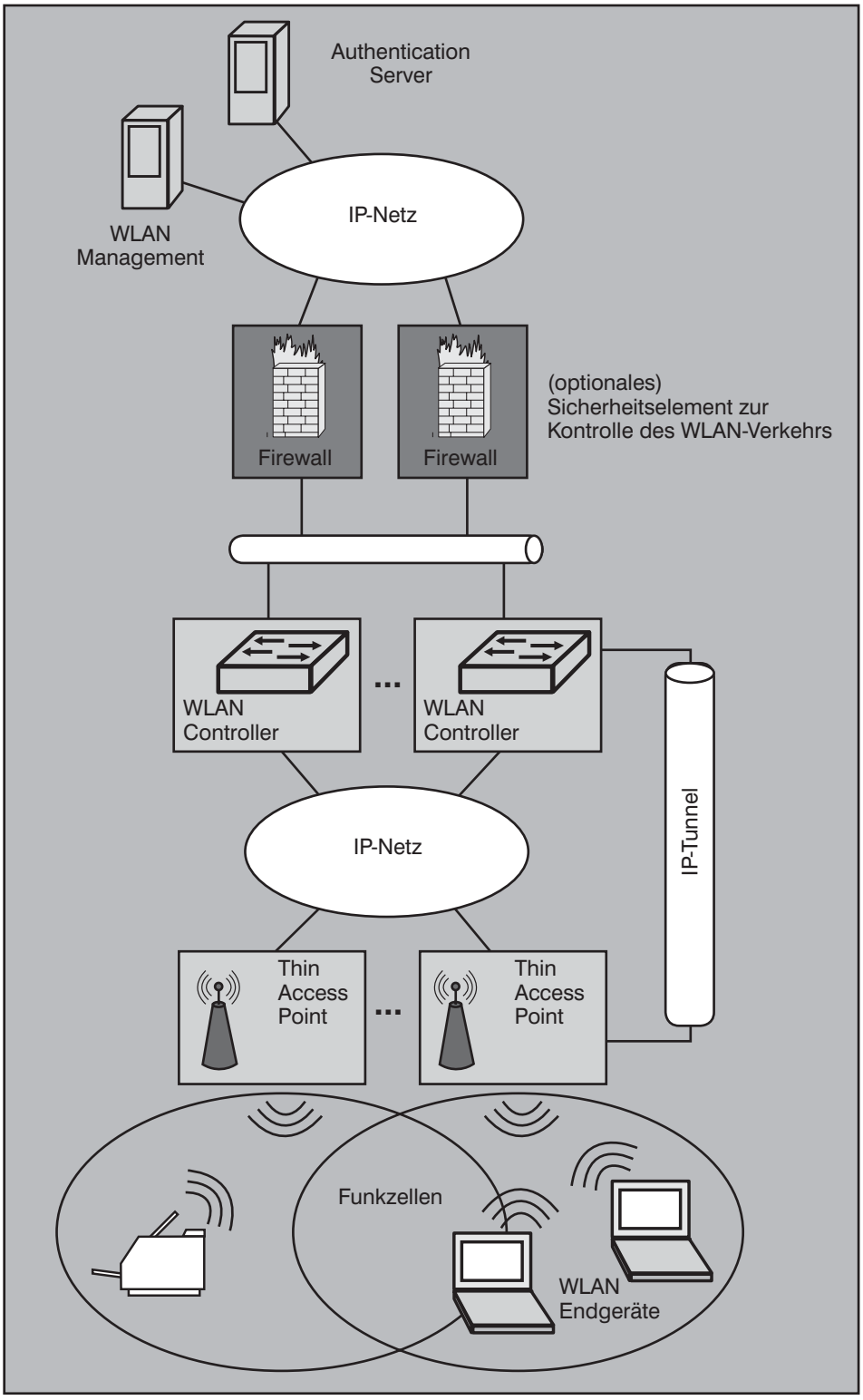


Abbildung 1: Conroller-basiertes WLAN-Design

ser Aspekte ist auch Inhalt der im Folgenden beschriebenen Tests.

Für den Tunnelmechanismus und die über den Tunnel ausgetauschten Daten liegt zwar seit geraumer Zeit die CAPWAP Protocol Specification als IETF Draft vor, bis auf die Controller-Lösung von LANCOM sind Stand Anfang Dezember 2007 ausschließlich Lösungen am Markt verfügbar, die herstellerspezifische Mechanismen implementieren. Manche Hersteller setzen mit Kontroll- und Datenkanal auf UDP auf (z.B. Cisco, LANCOM, Siemens), Trapeze verwendet IP Encapsulation within IP (RFC2003) und Aruba verwendet Generic Routing Encapsulation (GRE) und UDP.

Allerdings arbeiten alle Hersteller an einer CAPWAP-kompatiblen Lösung. Von einer Interoperabilität, die es gestattet, WLAN Controller und Thin Access Points von verschiedenen Herstellern zu kombinieren, ist man aber noch ausgesprochen weit entfernt. Mit der Auswahl eines Controllers ist die Palette an Access Points auch in der näheren Zukunft automatisch festgelegt.

Die Lösungen der Hersteller von WLAN-Controllern unterscheiden sich auch in der Rolle als Netzelement in Richtung der Übertragung der Client-Nutzdaten in das kabelbasierte LAN (und umgekehrt). Während beispielsweise die Lösungen von Cisco und Trapeze auf Layer 2 als Half-Bridge (siehe Abbildung 2), die Controller-Lösung von LANCOM als Router operiert, gestatten die Lösungen von Siemens und Aruba die Auswahl beider Möglichkeiten.

Tabelle 1 zeigt die Merkmale Tunnelmechanismus und Netzelementtyp im Vergleich für verschiedene Controller-Lösungen.

Weitere wichtige Elemente sind die Möglichkeiten der Absicherung der Kommunikation zwischen Thin Access Point und WLAN Controller. Die Kommunikation zwischen Thin Access Points und Clients (d.h. auf der Luftschnittstelle) kann adäquat mit IEEE 802.11i bzw. Wi-Fi Protected Access (WPA) oder WPA2 abgesichert werden. Die Kommunikation auf der Ethernet-Schnittstelle des Access Point ist davon nicht betroffen und muss daher bei Bedarf zusätzlich abgesichert werden. Dies ist beispielsweise sinnvoll, wenn Access Points in Bereichen montiert werden, in denen ein unberechtigter Zugriff auf den Access Point nicht ausgeschlossen werden kann. Während die CAPWAP Protocol Specification die Verschlüsselung des Kontrollkanals zwingend fordert und die des Datenkanals wenigstens optional hinzugeschaltet werden kann, bieten aktuell die Hersteller hinsichtlich der Verschlüsselung des Datenkanals keine Möglichkeiten an. Die Firma LANCOM hat die Verschlüsselung des CAPWAP Datenkanals immerhin auf ihrer Roadmap. Eine Ausnahme ist hier die Lösung von Aruba Networks. Die Verschlüsselung gemäß IEEE 802.11i kann bei Aruba auf dem WLAN Controller erfolgen. Die verschlüsselte Strecke wird dabei vom Client bis hin zum WLAN Controller verlängert.

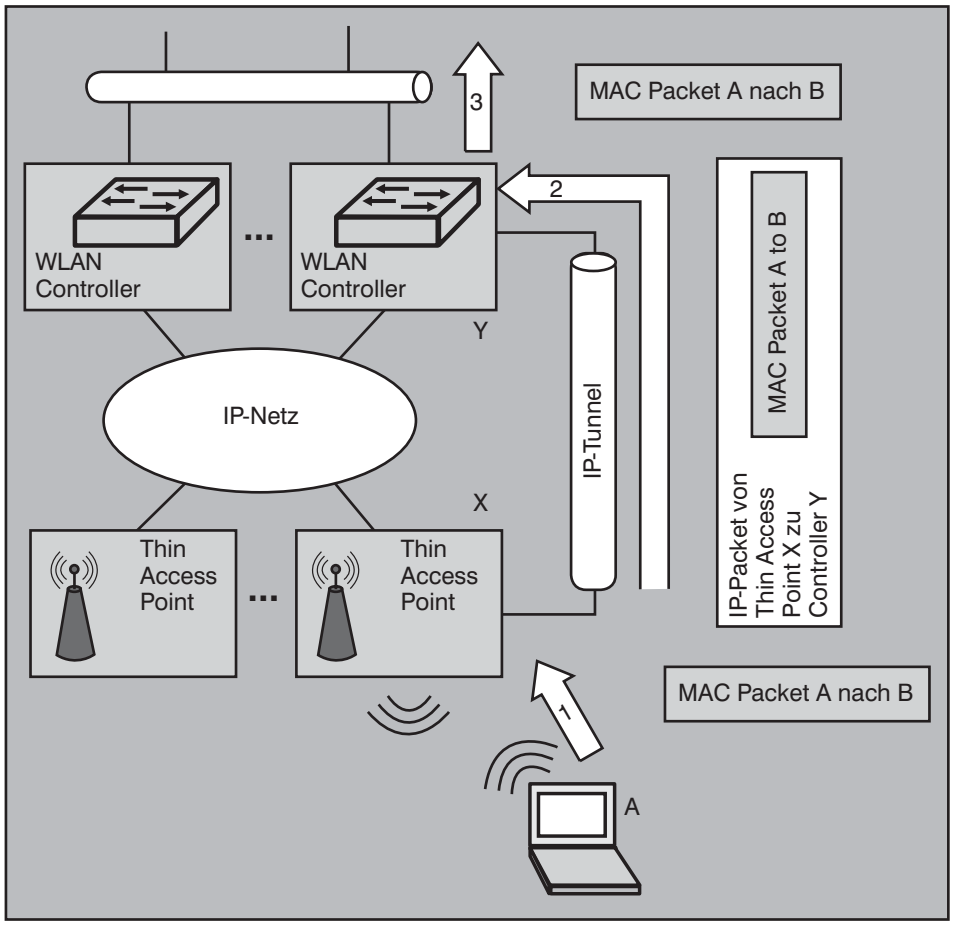


Abbildung 2: Beispiel einer Übertragung eines WLAN-Pakets über den Tunnel zwischen Thin Access Point und WLAN Controller

Egal wie man die Kommunikation absichert, WLAN Controller müssen erreichbar sein und sind daher unmittelbar potentielle Ziele für Angriffe vom Typ Denial of Service (DoS). Ziel eines solchen Angriffs kann beispielsweise ein UDP-Port sein, über den der Controller den Kontroll- oder der Datenkanal etabliert.

Abhängig von der für ein WLAN geforderten Verfügbarkeit muss eine redundante Ausgestaltung der Netzkomponenten möglich sein, die ansonsten einen Single-Point-of-Failure darstellen. Der einem Controller-basierten Design zugrundeliegende Redundanzmechanismus basiert auf dem zwischen Thin Access Point und

Hersteller	Tunnel-Mechanismus	Typ Netzelement
Aruba	Secure Light Access Point Protocol (SLAPP)	Router / Half-Bridge
	Generic Routing Encapsulation (GRE) für Kontrollkanal, UDP für Datenkanal	
Cisco	Light Weight Access Point Protocol (LWAPP)	Half-Bridge
	UDP-basiert; alternativ auch als L2-Tunnel konfigurierbar	
LANCOM	Erste Implementierung des CAPWAP-Protokolls	Router
	UDP-basiert	
Siemens	CAPWAP Tunneling Protocol (CTP) (*)	Router / Half-Bridge
	UDP-basiert	
Trapeze	Trapeze Access Point Access (TAPA)	Half-Bridge
	IP Encapsulation within IP (RFC2003)	

(*) Dies ist nicht das CAPWAP-Protokoll

Tabelle 1: Merkmale verschiedener Controller-Lösungen

WLAN Controller spezifizierten Discovery Process. Dieser Discovery Process wird im Fehlerfall eines WLAN Controller erneut initiiert; die betroffenen Thin Access Points führen im Prinzip einen Reboot durch, starten den Discovery Process erneut und wechseln gegebenenfalls auf einen anderen WLAN Controller.

Eine Redundanz wird also durch Hinzufügen eines oder mehrerer weiterer WLAN Controller zum Netz erreicht. Wenn ein WLAN Controller ausfällt, übernehmen andere WLAN Controller dessen Aufgaben. In vielen Fällen ist eine N+1-Redundanz der WLAN Controller ausreichend, um den Ausfall eines einzelnen WLAN Controller zu kompensieren.

Thin Access Points werden im Regelfall nicht redundant an Access Switches angebunden, und ein Access Switch versorgt mehrere Access Points. Die erforderliche Verfügbarkeit der Endgeräte-Anbindung wird durch überlappende Funkzellen, die auf diese Weise eine redundante Luftschnittstelle bilden, erreicht. Der Grad der Überlappung bestimmt dabei den Grad der Redundanz. Ist eine hohe Redundanz erforderlich, bedeutet dies meist, dass an jedem Punkt des WLAN sichergestellt werden muss, dass bei Ausfall eines Access Points mindestens ein anderer Access Point mit guter Qualität empfangen werden muss. Bei einem solchen Grad an Zellüberlappung sind Interferenzen in einem flächendeckenden WLAN bei 2,4 GHz praktisch unvermeidbar. Wie sich solche Störungen auswirken, wird noch in diesem Artikel betrachtet.

In Bereichen mit besonders hohen Anforderungen an die Verfügbarkeit kann eine redundante Anbindung eines Thin Access Points an zwei Access Switches erwogen werden, sodass der Ausfall eines Access Switches nicht mehr einen Ausfall der angebundenen Thin Access Points und zugehörigen WLAN-Clients bedingt. Als Einschränkung ist zu bemerken, dass ein solcher redundanter Anschluss der Thin Access Points derzeit nur von wenigen Herstellern, z.B. von Trapeze, unterstützt wird.

2. Betrachtete Hersteller und Geräte

Für den Test wurden Geräte der Hersteller Aruba, Cisco, Siemens und Trapeze betrachtet. Die in Tabelle 2 bis Tabelle 5 beschriebenen Geräte standen für die Tests zur Verfügung.

3. Testserien

Fokus der Tests ist die Bewertung der Voice-Tauglichkeit von Controller-basier-

WLAN Controller	
MC-800 Mobility Controller	
LAN-Schnittstellen	8 x 10/100 Base T + 1 x 1000 BaseX (GBIC)
Maximal unterstützte User-Anzahl	256
Maximalanzahl der administrierten Thin Access Points	16
Firewall-Durchsatz	1 Gbit/s
Durchsatz Verschlüsselung (3 DES, AES-CCM)	200 MBit/s
Access Points	
AP-65	

Tabelle 2: Getestete Geräte von Aruba

WLAN Controller	
Cisco 2106	
LAN-Schnittstellen	8 x 10/100 Base T
Max. Anzahl Lightweight APs	6
Access Points	
Aironet 1242G (als Lightweight-Version)	
Aironet 1232AG (als Fat-AP für Referenzmessungen)	

Tabelle 3: Getestete Geräte von Cisco

ten WLAN-Lösungen. Die Festlegung auf VoIP als Test-Applikation hat den Hintergrund, dass Sprache besonders empfindlich auf solche Schwachstellen in Access Point und WLAN Controller reagiert, die zu einem Leistungsengpass führen. Weiterhin wird in vielen Planungen Voice als eine der zu berücksichtigenden Anwendungen betrachtet, und generell hat die tatsächliche Häufigkeit der Nutzung Voice over WLAN (VoWLAN) signifikant zugenommen.

Ein Ranking der verschiedenen Produkte der Hersteller steht bei den Tests nicht im Vordergrund. Primär sollen Bereiche identifiziert werden, die Schwachstellen darstellen können und die daher bei Planung und Betrieb von Controller-basierten WLAN-Lösungen besonders berücksichtigt werden sollten.

Hierzu wurden die im Folgenden beschriebenen vier Testserien durchgeführt:

- Serie 1: Messung mit simulierten VoWLAN Clients
- Serie 2: Messung mit verschiedenen WLAN Handsets
- Serie 3: DoS auf WLAN Controller
- Serie 4: Monitoring auf der Luftschnittstelle

Auf Wunsch von Aruba Networks zeigen wir die Ergebnisse, die mit dem Aruba-System erzielt wurden, nicht. Nach Aussage von Aruba Networks hätten die Tests sicherheitskritische Defizite aufgezeigt, die Aruba Networks nicht veröffentlicht sehen möchte, um schnellstmöglich die Probleme analysieren und beseitigen zu können. Wir bedauern dies, werden aber die Gelegenheit für erneute Tests erhalten und darüber berichten.

WLAN Controller	
HiPath Wireless Controller C10	
LAN-Schnittstellen	4 x 10/100 Base T
Maximal unterstützte User-Anzahl	512
Maximalanzahl der administrierten Thin Access Points	30
Access Points	
HiPath Wireless Access Point AP2610	

Tabelle 4: Getestete Geräte von Siemens

WLAN Controller	
Mobility Exchange MX-216R	
LAN-Schnittstellen	2 x 10/100/1000 Base GBICs; 16 x 10/100 BaseT
Maximalanzahl der administrierten Thin Access Points	128
Access Points	
Mobility Point MP-422	

Tabelle 5: Getestete Geräte von Trapeze

4. Serie 1: Messung mit simulierten VoWLAN Clients

Bei dem hier betrachteten Szenario wird die auf das WLAN einwirkende Verkehrslast mit einem speziellen Werkzeug (Ix-Chariot, siehe unten) simuliert. Schwerpunkt ist dabei die Betrachtung des Einflusses einer höheren Kommunikationslast und von Gleichkanal-Interferenzen auf die Leistung der Sprachübertragung.

4.1 Testkonfiguration

Zwei Access Points wurden in 10 m Abstand aufgestellt und an jedem Access Point je zwei WLAN-Clients assoziiert. Der Abstand der Clients zu den Access Points wurde so gewählt, dass ein sehr guter Empfang besteht.

Auf zwei WLAN-Clients, die jeweils in verschiedenen Zellen angemeldet waren, wurde eine VoIP-Kommunikation simuliert. Dabei haben sich die beiden Clients gegenseitig angerufen und sobald ein Gespräch beendet worden ist, wurde ein erneutes Gespräch begonnen. Die Güte der VoIP-Kommunikation im Sinne von MOS-Wert (MOS = Mean Opinion Score), Jitter und Delay wurde als Testresultat aufgezeichnet. Die Sprachpakete laufen dabei vom Client über die Luftschnittstelle über den Access Point zum WLAN Controller und von dort zum anderen Access Point und dann zum zweiten VoWLAN-Client.

Als Codec wurde G.711 verwendet. Nun mag man hier die Bemerkung machen, dass ein adaptiver Codec besser geeignet sei, um mit den Verhältnissen einer drahtlosen Kommunikation zurecht zu kommen. Diese Vorhaltung ist grundsätzlich korrekt, jedoch ist der Codec nicht Inhalt der Tests und jedes zusätzliche dynamische Verhalten kann Testergebnisse verwischen.

Für die beiden Clients, die eine Voice-Übertragung simulieren, wurde jeweils ein WLAN-Adapter vom Typ Cisco CB21ag verwendet. Damit vergleichbare Resultate erzielt werden können, wurden keine CCX-Funktionen verwendet. Die Clients verwenden IEEE 802.11g. Um die Basis für eine akzeptable und vergleichbare Sprachqualität im WLAN zu schaffen, wird in der verwendeten Default-Konfiguration einheitlich Wi-Fi Multimedia (WMM) konfiguriert.

Die anderen beiden WLAN-Clients produzieren eine kontinuierliche UDP-Hintergrundlast und versuchen sich gegenseitig so viele Daten wie möglich über das WLAN zuzuschicken. Hier wurde der in den genutzten Notebooks verbaute Intel Pro Wireless 3945 abg verwendet.

Abbildung 3 zeigt den Testaufbau im Überblick.

Die Sendeleistung der Access Points wurde bei den verschiedenen getesteten Geräten so eingestellt, dass ungefähr jeweils 50 mW EIRP erreicht wurden. Sofern nicht explizit anders angegeben, sind die Access Points auf unterschiedlichen Kanälen (Kanal 1 und Kanal 13 bei 2,4 GHz) konfiguriert.

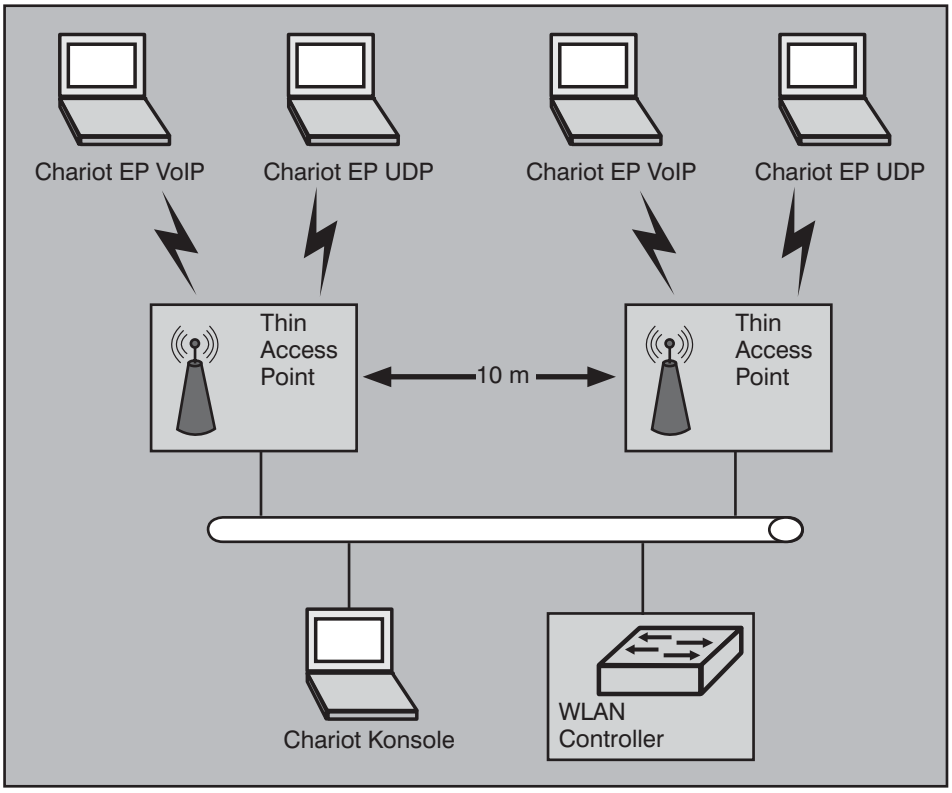


Abbildung 3: Testkonfiguration für Messung mit simulierten VoWLAN Clients

Als Verschlüsselungsverfahren wurde auf der Luftschnittstelle einheitlich WPA-Personal (d.h. Nutzung eines Pre-Shared Key, PSK) konfiguriert.

Als Simulationswerkzeug wurde der Lastgenerator IXChariot von der Firma IXIA verwendet. IxChariot erlaubt eine parametrierbare und programmierbare Simulation des Verhaltens von unterschiedlichsten Anwendungstypen. Dabei kann flexibel ein Verkehrsmix erzeugt werden. In dem hier betrachteten Fall besteht der Mix aus VoIP mit einer UDP-Hintergrundlast.

IxChariot erzeugt keinen echten Anwendungsverkehr, sondern einen „Dummy-Verkehr“, der sich aber von der Charakteristik (d.h. der verwendeten Ports, der Verteilung der Paketgrößen und der Verteilung der Zwischenankunftszeiten von Paketen) genauso wie die reale Applikation verhält. Ein Netzelement, das auf Layer 1 bis Layer 4 den Kommunikationsverkehr weiterleitet, z.B. Bridges, Router, (dynamische) Paketfilter oder eben Access Points und WLAN Controller, bemerken den Unterschied nicht, da sie nicht den anwendungsspezifischen Part analysieren.

Der Verkehr wird bei IxChariot von Agenten (sogenannten End Points, EPs) erzeugt, die auf konventionellen Endgeräten (PCs, Workstations, Server) laufen. Koordiniert werden die End Points von einer Konsole. Über die Konsole werden Test Scripts und Parameter auf die Endpoints heruntergeladen und der Test synchron gestartet. Die Endpoints melden die Testergebnisse zur Konsole. Abbildung 4 zeigt exemplarisch den Verlauf einer Durchsatzmessung und einen Ausschnitt aus dem zugehörigen Test Script.

4.2 Testfälle

Folgende Testfälle wurden mit den Geräten der betrachteten Hersteller durchgeführt:

- Szenario a: Als Referenz wurde lediglich ein VoIP-Verkehr zwischen zwei Clients bei IEEE 802.11g erzeugt und die VoIP-Qualitätsindikatoren gemessen und aufgezeichnet.
- Szenario b: Ergänzend zu Szenario a wird wie oben beschrieben eine UDP-basierte Hintergrundlast durch zwei weitere Clients, die im WLAN mit IEEE 802.11g übertragen, erzeugt.
- Szenario c: Ergänzend zu Szenario a wird wie oben beschrieben eine UDP-basierte Hintergrundlast durch zwei weitere Clients, die im WLAN mit IEEE 802.11b übertragen, erzeugt. Da bei IEEE 802.11b im Vergleich nur eine deutlich niedrigere Datenrate möglich ist, belegen die Übertragungen das Medium für einen längeren Zeitraum. Damit steht das Medium für die Sprachübertragung seltener zur Verfügung es entsteht eine höhere Belastung der Funkstrecke.
- Szenario d: Ergänzend zu Szenario b werden die Access Points auf einen gemeinsamen Funkkanal (Kanal 1 bei 2,4 GHz) konfiguriert. Auf die WLAN-Stationen, die VoIP übertragen, wirken jetzt

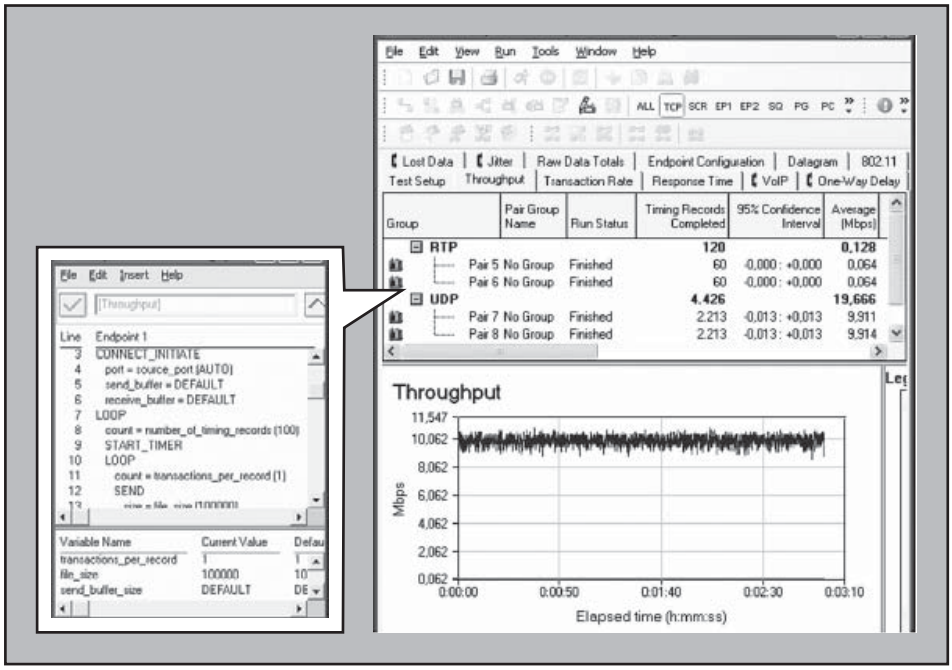


Abbildung 4: Bildschirmdarstellung des verwendeten Simulationswerkzeugs IxChariot

Szenarien	a	b	c	d	e
2 Clients (802.11g) telefonieren	X	X	X	X	X
802.11g-Hintergrundlast durch 2 Clients		X		X	
802.11b-Hintergrundlast durch 2 Clients			X		X
Interferenz: beide Zellen auf einem Kanal				X	X

Tabelle 6: Betrachtete Testfälle für die Messung mit simulierten VoWLAN Clients

neben der erhöhten Last auch Leistungseinbußen durch Gleichkanalstörungen ein.

- Szenario e: Ergänzend zu Szenario c werden die Access Points auf einen gemeinsamen Funkkanal (Kanal 1 bei 2,4 GHz) konfiguriert.

Die Betrachtung von Gleichkanalstörungen ist nicht nur wegen einer stärkeren Zellüberlappung aus Redundanzgründen wichtig. Bei einem WLAN-Design zur Unterstützung von Voice müssen sich die Funkzellen ebenfalls stärker überlappen, damit während eines Telefongesprächs ein reibungsloser Zellwechsel (Handover) ohne hörbare Beeinflussung der Ende-zu-Ende-Kommunikation möglich ist. Da bei 2,4 GHz lediglich drei überlappungsfreie Kanäle zur Verfügung stehen (Kanäle 1-7-13 bzw. 1-6-11), bedeutet eine stärkere Zellüberlappung automatisch ein Ansteigen von Gleichkanalstörungen, da der Abstand zwischen zwei Access Points, die auf dem selben Kanal konfiguriert sind, zwangsläufig abnimmt.

Tabelle 6 zeigt die verschiedenen Szenarien im Überblick.

4.3 Testergebnisse

Abbildung 5 zeigt für die betrachteten Szenarien den mittleren MOS-Wert. Zu beachten ist dabei, dass der MOS-Wert bei dem Werkzeug IxChariot basierend aus Paketverzögerungen und Paketverlusten berechnet wird. Der bei den Messungen erzielte mittlere MOS-Wert liegt stets über 3,84 und meist sogar über 4. Bei der üblichen Einstufung des MOS-Werts hat man damit eine ordentliche bis gute Qualität. Ein MOS-Wert von 2 gilt als mäßige Qualität (d.h. man muss sich sehr anstrengen, um überhaupt noch etwas zu verstehen) und bei einem Wert von 1 wird die Qualität als mangelhaft angenommen.

Betrachtet man dagegen in Abbildung 6 den mittleren Jitter (d.h. die Delay-Schwankung), zeigt sich, dass steigende Last und insbesondere erhöhte Interferenz einen sichtbaren Einfluss auf den Jitter haben. Trotzdem sind die Werte in einem Bereich, der keinen Einfluss auf die Güte der Sprachverbindung hat. Auch die Betrachtung der maximalen Jitter-Werte zeigt, dass in keiner Messung ein Wert von 18 ms überschritten worden ist.

Bei diesen Ergebnissen hat der Priorisierungsmechanismus in WMM einen deutlichen Einfluss, wie der Vergleich mit der in Abbildung 7 dargestellten Messung zeigt, bei der WMM jeweils deaktiviert war. Für das Szenario e zeigt Abbildung 8 die jeweiligen Einzelmessungen einmal ohne

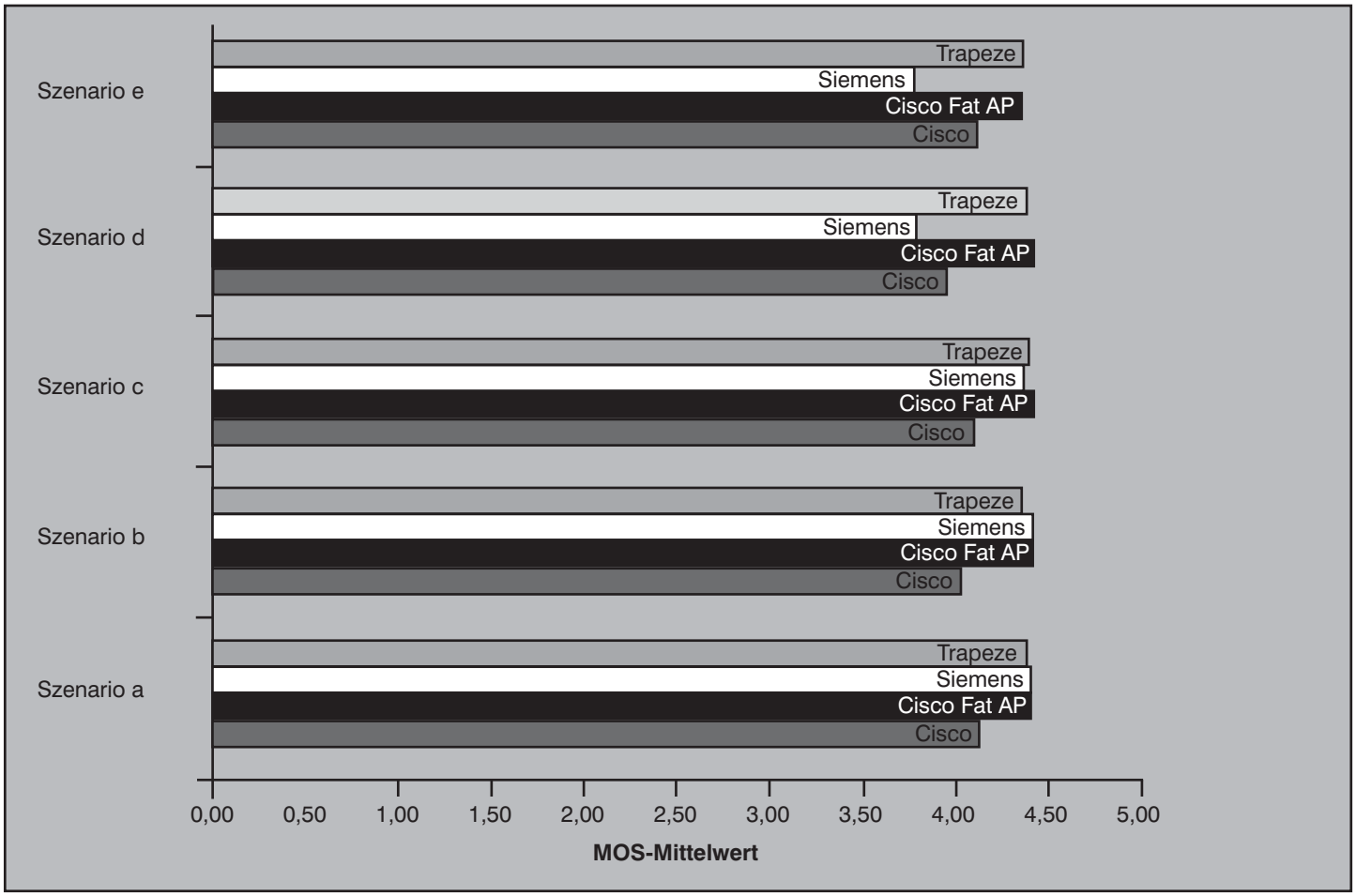


Abbildung 5: Mittlerer MOS-Wert im Vergleich

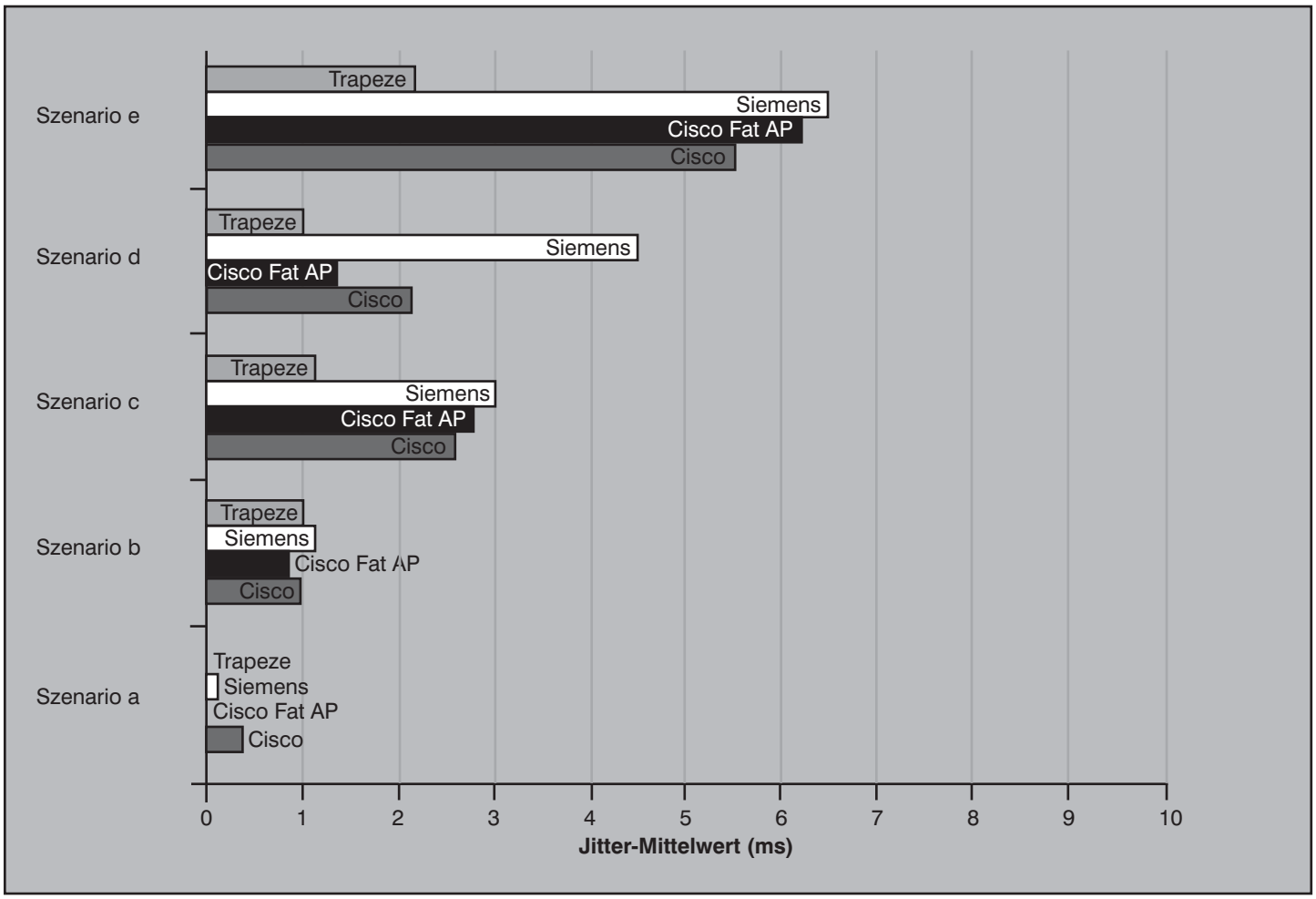


Abbildung 6: Mittlerer Jitter im Vergleich

QoS durch WMM und einmal mit. Hierbei wird auch deutlich, dass der Kanalzugriff bei WMM zufallsgesteuert bleibt, die Voice-Pakete aber im Mittel priorisiert werden.

Die gezeigten Ergebnisse machen zunächst deutlich, dass die betrachteten Produkte von Cisco, Siemens und Trapeze sowohl robust auf Gleichkanalstörungen reagieren als auch bei einer höheren Last in einer Zelle eine sehr gute Sprachübertragung ermöglichen.

An den in den Tests beobachteten Effekten sind allerdings die WLAN Controller weniger beteiligt, es waren primär die Access Points gefordert (insbesondere beim Umgang mit Gleichkanalstörungen). In der Praxis zeigt sich aber leider immer wieder, dass die Qualität der Access Points vernachlässigt wird.

In einer Ausschreibung sind solche Punkte nicht leicht zu berücksichtigen, da hier keine funktionalen Anforderungen abgefragt werden. Zumindest können aber Aussagen der Hersteller gefordert wer-

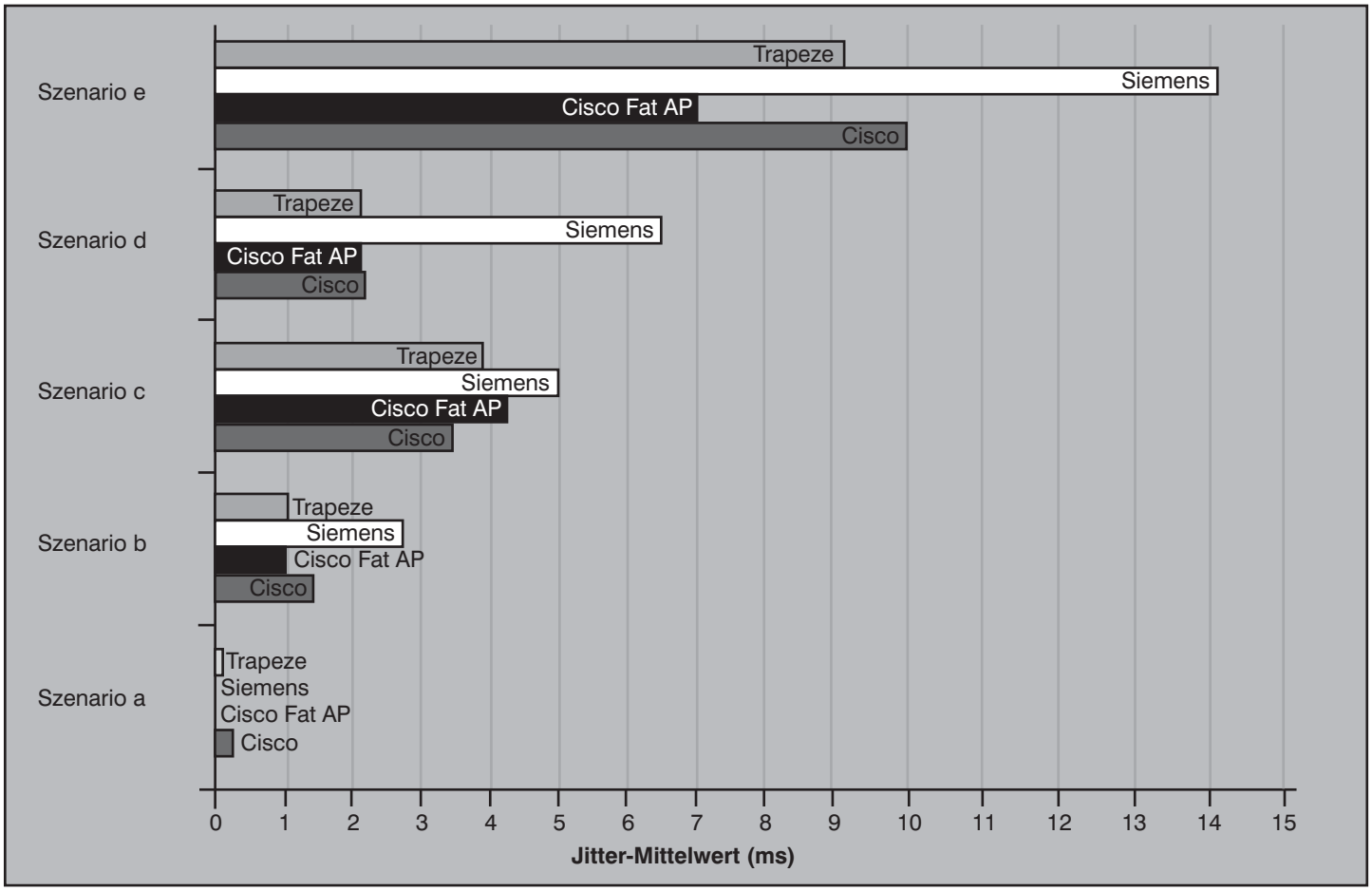


Abbildung 7: Mittlerer Jitter im Vergleich bei Deaktivierung von WMM

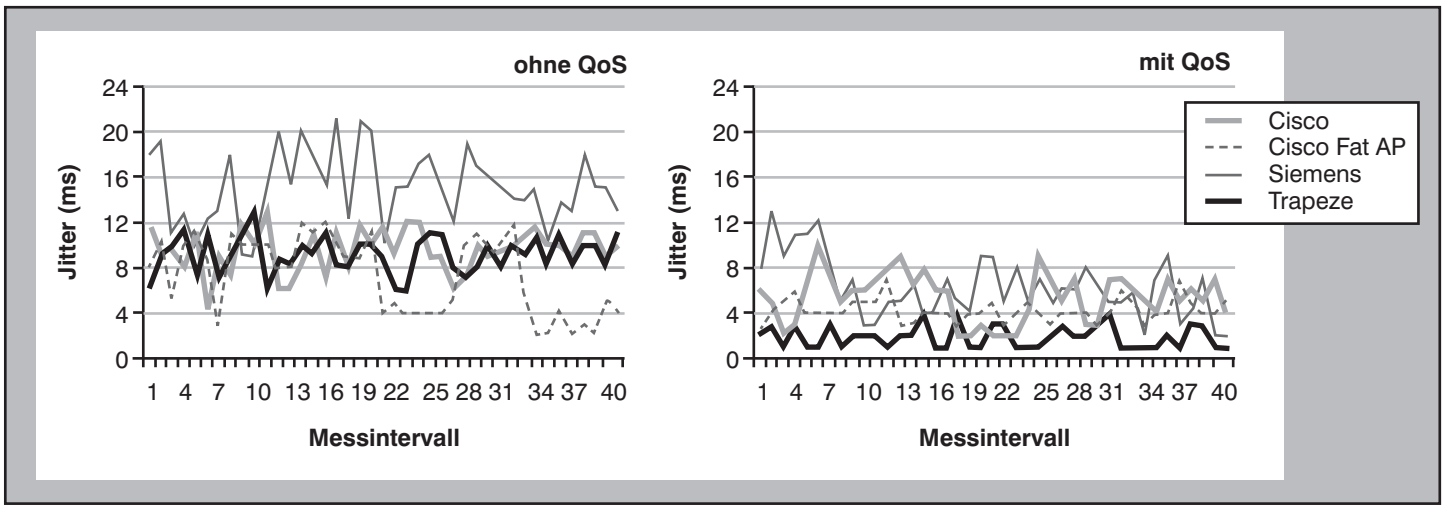


Abbildung 8: Darstellung des Einflusses von QoS anhand von Einzelmessungen für Szenario e

den, die beschreiben, wie ihr Produkt beispielsweise bei Gleichkanalstörungen und anderen Interferenzen reagiert und welche Maßnahmen der Hersteller empfiehlt.

4.4 Einfluss des Client-Adapters

Um den Einfluss von Client-Adaptern zu bewerten, haben wir die Messungen für die Szenarien a und c für die Voice-Clients jeweils auch mit einem Adapter vom Typ Intel Pro Wireless 3945 abg durchgeführt. Die in Abbildung 9 links dargestellten MOS-Mittelwerte zeigen keine Auffälligkeiten, die Messungen mit dem Intel-Adapter liegen jeweils geringfügig unter den Ergebnissen mit dem Cisco-Adapter. Überraschend ist dagegen der Vergleich der Minimalwerte für den MOS, wie in Abbildung 9 rechts gezeigt.

Eine Betrachtung der Einzelmessungen verschafft hier Klarheit, wie in Abbildung 10 für Szenario a gezeigt. Der Intel-Adapter führt in regelmäßigen Abständen

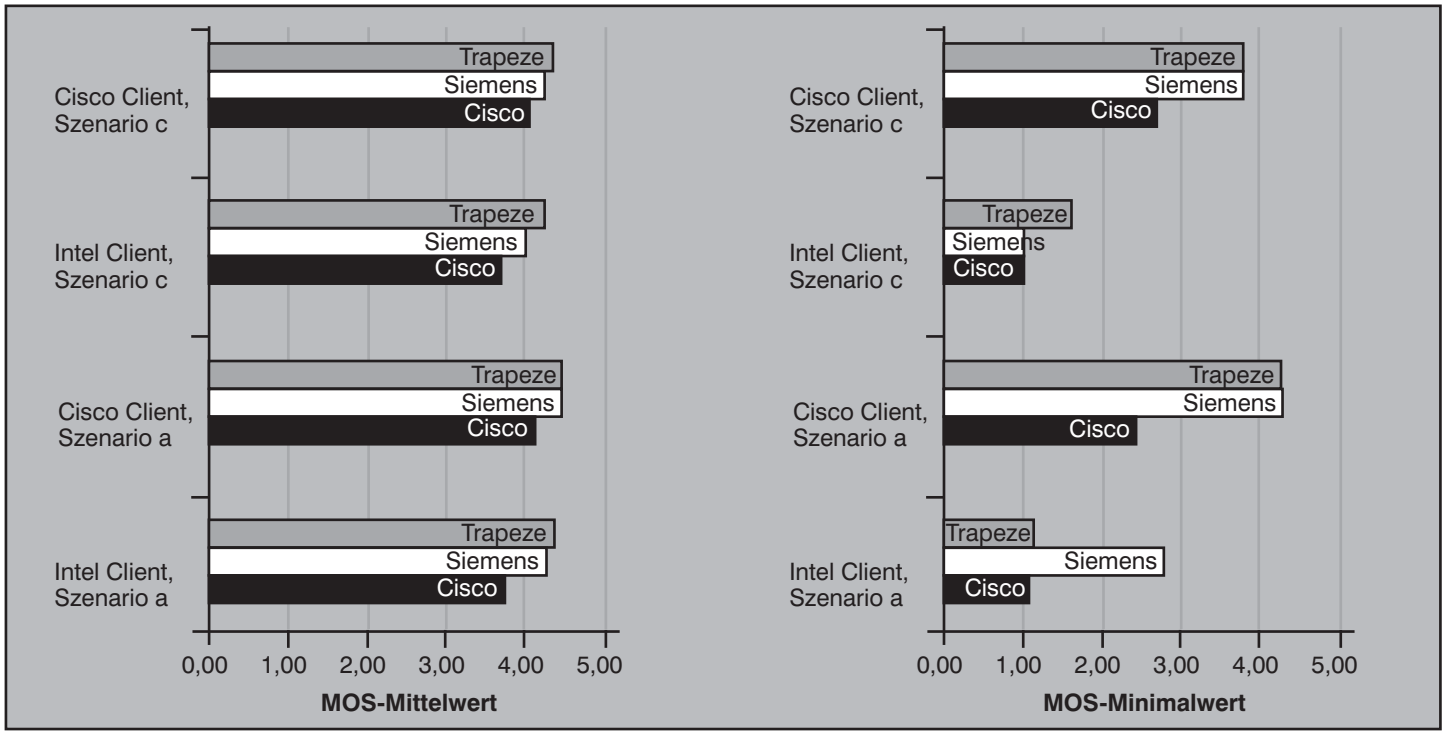


Abbildung 9: MOS-Mittelwert (links) und MOS-Minimalwert (rechts) im Vergleich zwischen Intel und Cisco WLAN-Adaptern

ein Scanning der Funkkanäle durch. Diese Phase ist offensichtlich so implementiert, dass der Adapter keine anderen Aktivitäten außer dem Scanning durchführen kann. Der Effekt ist unabhängig von Parametereinstellungen des Adapters hinsichtlich Roaming. Es wurde die aktuelle Version 11.1.1.11 des Intel-Treibers verwendet. Der beschriebene Effekt tritt auch in früheren Versionen auf.

Generell gilt, dass für einen PC-Einsatz die Firmware für einen WLAN-Adapter und die WLAN-Treiber meist durchsatzoptimiert implementiert sind und sich Scanning und Parameter für den Handover oft nicht adäquat an eine VoIP-Übertragung anpassen lassen. Hier ist man also gefordert, im Einzelfall die verwendeten Adapter und Treiber auf ihre Voice-Tauglichkeit zu prüfen bzw. zu akzeptieren, dass bei Nutzung von Softphones die Sprachqualität für einen kurzen Zeitraum ggf. etwas schlechter werden kann.

5. Serie 2: Messung mit verschiedenen WLAN Handsets

In dieser Testserie sollen Messungen mit verschiedenen am Markt gängigen WLAN Handsets bzw. Smartphones durchgeführt werden. Für die Hintergrundlast sorgt wieder IxChariot. Für diese Testserie wurde bewusst auch mit mehreren Clients in einer Zelle eine Hintergrundlast erzeugt. Ziel der Tests ist einerseits die Plausibilitätsprüfung der in Serie 1 mit simulierten IP-Telefonen erzielten Ergebnisse und andererseits die Betrachtung der Leistung beim Handover.

5.1 Testkonfiguration

Zunächst wurde ein Test mit nur einer Funkzelle aber mehreren WLAN Clients

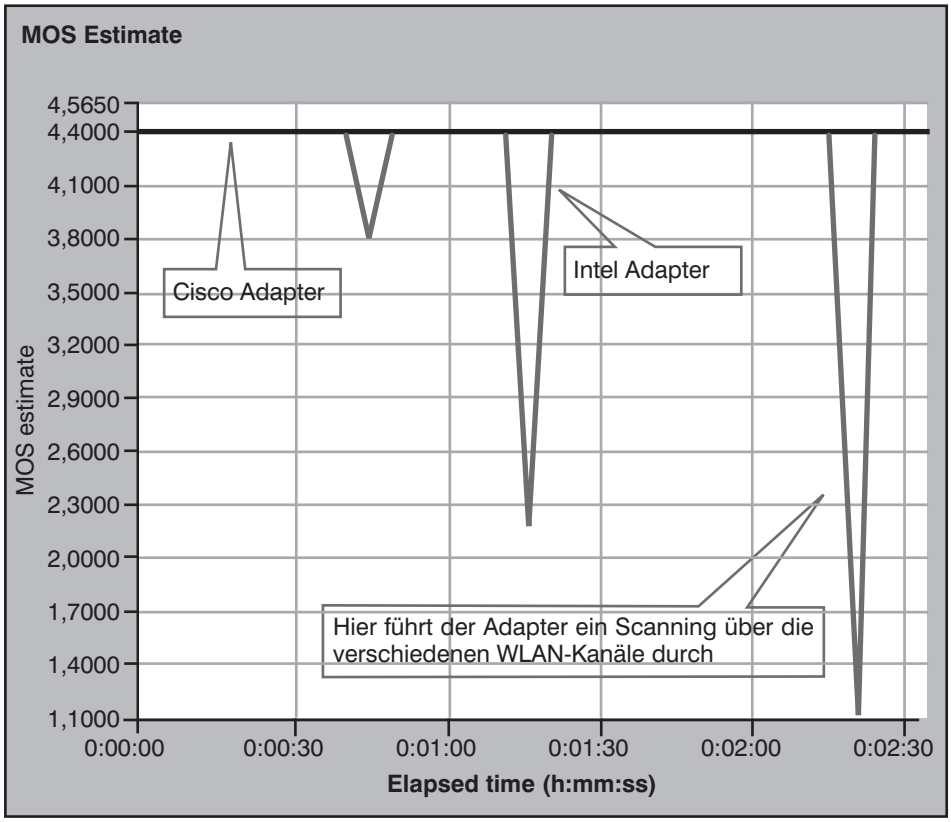


Abbildung 10: Vergleich für Szenario a bei Verwendung einer WLAN-Infrastruktur von Trapeze (Bildschirmdarstellung von IxChariot)

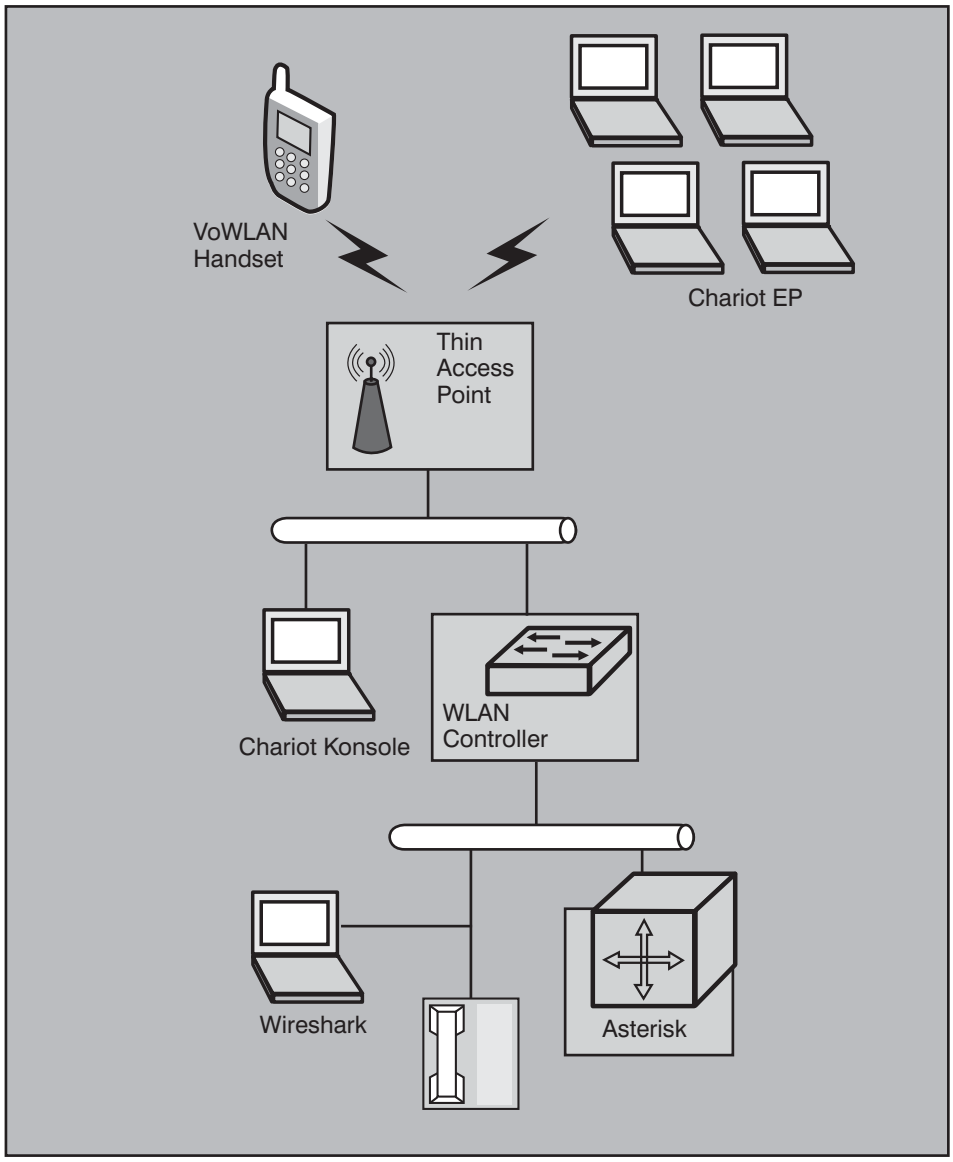


Abbildung 11: Testkonfiguration zur Messung mit verschiedenen WLAN Handsets

durchgeführt, wie in Abbildung 11 gezeigt. Die Sprachverbindung besteht zwischen WLAN Handset und einem Desktop IP-Telefon. Die Übertragung auf der Luftschnittstelle erfolgt mit IEEE 802.11g. Als Telefonie-Server wurde ein Asterisk-System und als Signalisierungsprotokoll wurde je nach WLAN-Handset das Session Initiation Protocol (SIP) oder das Skinny Client Control Protocol (SCCP) verwendet. Die Tests wurden am Desktop IP Phone mit Wireshark aufgezeichnet und die VoIP-Ströme herausgefiltert. Die Berechnung des Jitter erfolgte für die Strecke vom WLAN-Client zum Desktop IP-Telefon.

Als WLAN-Lösung wurde das System von Cisco verwendet. Die in Abbildung 12 gezeigten WLAN-Telefone wurden für die Tests eingesetzt.

Für Tests der Leistung beim Handover wurde der Testaufbau mit zwei Access Points gemäß Abbildung 13 verwendet.

5.2 Testfälle

Folgende Testfälle wurden durchgeführt:

- Messung A: Über WLAN-Telefon und Desktop IP-Telefon wird ein Gespräch geführt.
- Messung B: Zusätzlich zu Szenario A wird analog zu Testserie 1 (siehe Kapitel 4.1) eine durch vier weitere Clients mit IxChariot über IEEE 802.11g eine kontinuierliche UDP-Hintergrundlast erzeugt.
- Messung C: Dieses Szenario ist analog zu Szenario B, nur wird eine Hintergrund-Last durch vier Voice-Clients erzeugt.

Tabelle 7 zeigt die Testfälle im Überblick

Für die Bewertung der Mobilitätseigenschaften muss beachtet werden, dass der Zellwechsel zurzeit ausschließlich vom Client gesteuert und durchgeführt wird (es sei denn, es werden herstellerspezifische Verfahren eingesetzt). Erst mit den Standards IEEE 802.11r und IEEE 802.11k werden der Access Point bzw. der WLAN Controller in die Auswahl einer Funkzelle und in die Durchführung eines Handover involviert. Daher ist die Leistung beim Handover primär vom WLAN Client abhängig.

Aus diesem Grund ist für das Zellwechselverhalten nur ein Handset als Referenz (Siemens WL-2) ausgewählt worden und die betrachteten Controller-Lösungen sind mit diesem Handset getestet worden.

5.3 Testergebnisse

Abbildung 14 zeigt die Ergebnisse für die verschiedenen Handsets. Man erkennt zwar ein leichtes Abnehmen der Leistung bei höherer Last (Messungen B und

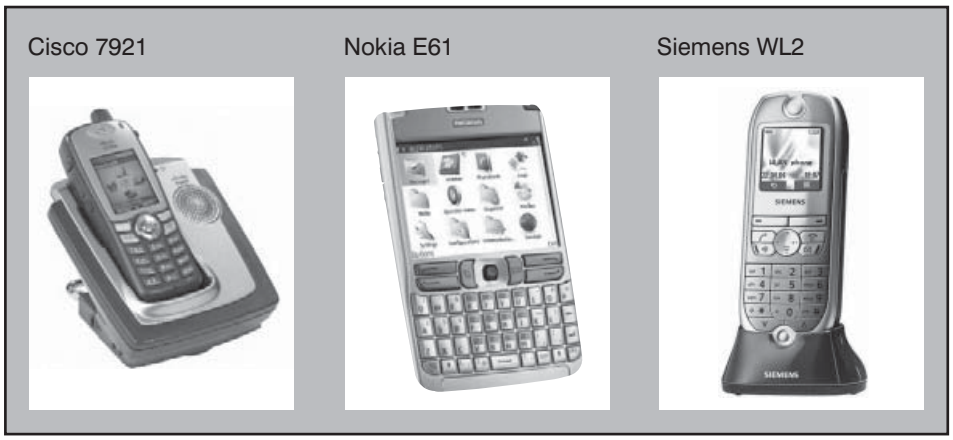


Abbildung 12: Verwendete WLAN-Telefone

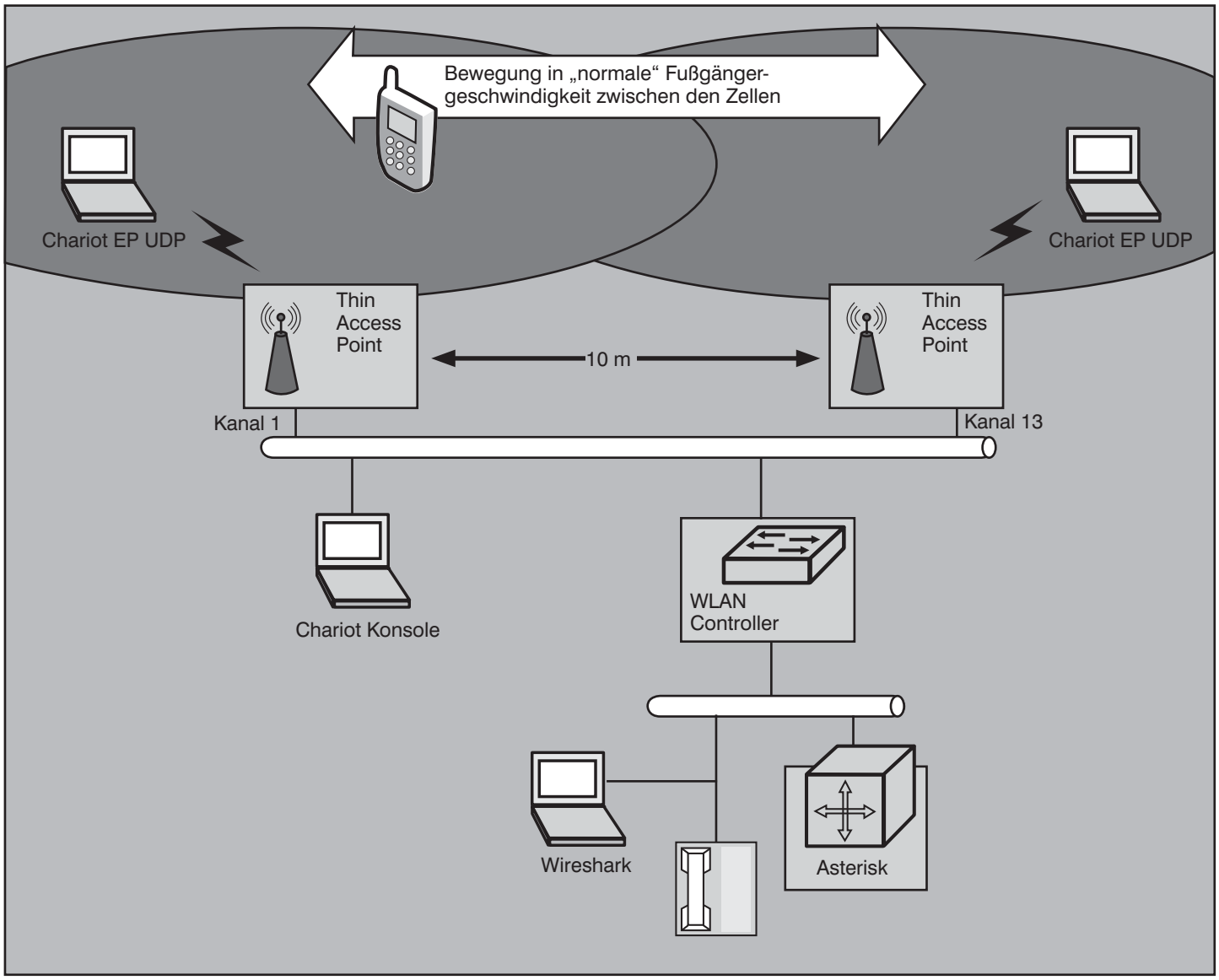


Abbildung 13: Testkonfiguration zur Messung der Leistung bei einem Handover

C), allgemein ist die Leistung aber erfreulich gut. Der maximal aufgetretene Jitter (siehe Abbildung 15) liegt auch bei höherer Last deutlich unter 20 ms. Insgesamt wird damit die These der Voice-Tauglichkeit von WLAN-Controller-Lösungen weiter gestützt.

Die Ergebnisse der Mobilitätsmessung sind in Abbildung 16 zusammengefasst. Der durchschnittliche Jitter ist wie in den anderen Messungen nicht der Rede wert. Jedoch ist die Zunahme des maximalen Jitter deutlich. Dies wird durch den Handover verursacht, bei dem gewisse Totzeiten unvermeidbar sind. Dabei kommt es zunächst zu einem Anstieg an Paketverlusten, die zwar zunächst noch durch Wiederholungen auf der MAC-Ebene ausgeglichen werden können, aber während des Handover nicht mehr vermieden werden können.

Dies zeigt sich auch unmittelbar im Delay aufeinanderfolgender RTP-Pakete, die ja bei G.711 alle 20 ms übertragen werden. Abbildung 17 zeigt hierzu exemplarisch den Verlauf des zeitlichen Abstands zwischen RTP-Paketen für die betrachtete Controller-Lösung von Siemens. Hier kann man sehr gut erkennen, wie beim Handover dieser Abstand für einen kurzen Zeitraum stark (bis zum sechsfachen des normalen Werts) zunimmt. Die Leistungseinbußen waren aber kaum hörbar.

Messung	A	B	C
2 WLAN Handsets (802.11g) telefonieren	X	X	X
802.11g-Hintergrundlast durch 4 Clients (UDP)		X	
802.11g-Hintergrundlast durch 4 Clients (Voice)			X

Tabelle 7: Betrachtete Testfälle für die Messung mit verschiedenen WLAN Handsets

6. Serie 3: DoS auf WLAN Controller

Mit der notwendigen Erreichbarkeit eines WLAN Controllers besteht automatisch die Gefahr eines DoS-Angriffs. Dies gilt unabhängig von einer Authentifizierung und Verschlüsselung nach IEEE 802.11i auf der Luftschnittstelle. Der Angriff kann an der Ethernet-Verbindung des Access Point zum LAN erfolgen oder ein Angreifer assoziiert sich an einer SSID, über die keine

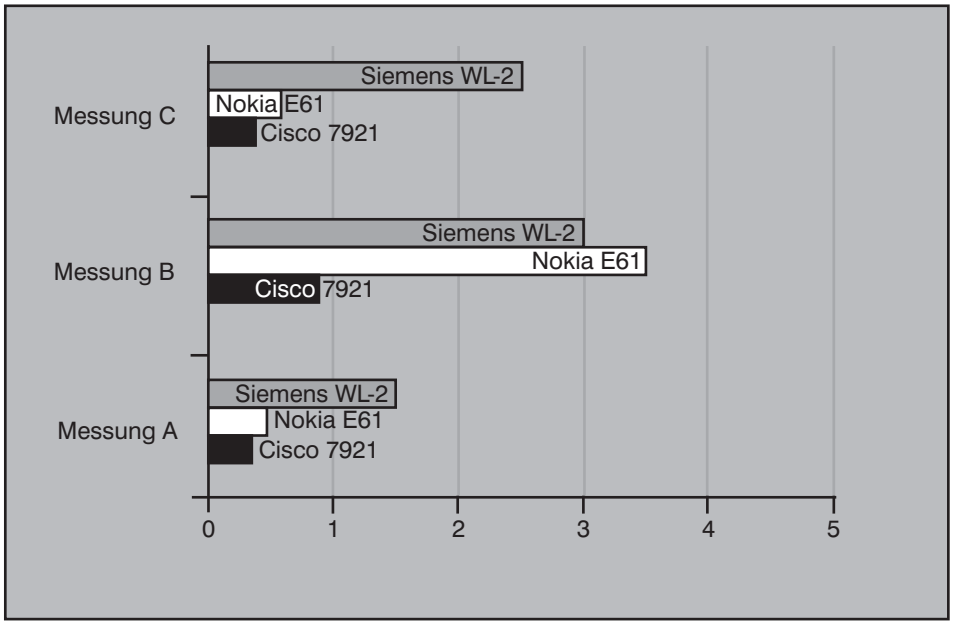


Abbildung 14: Mittlerer Jitter im Vergleich

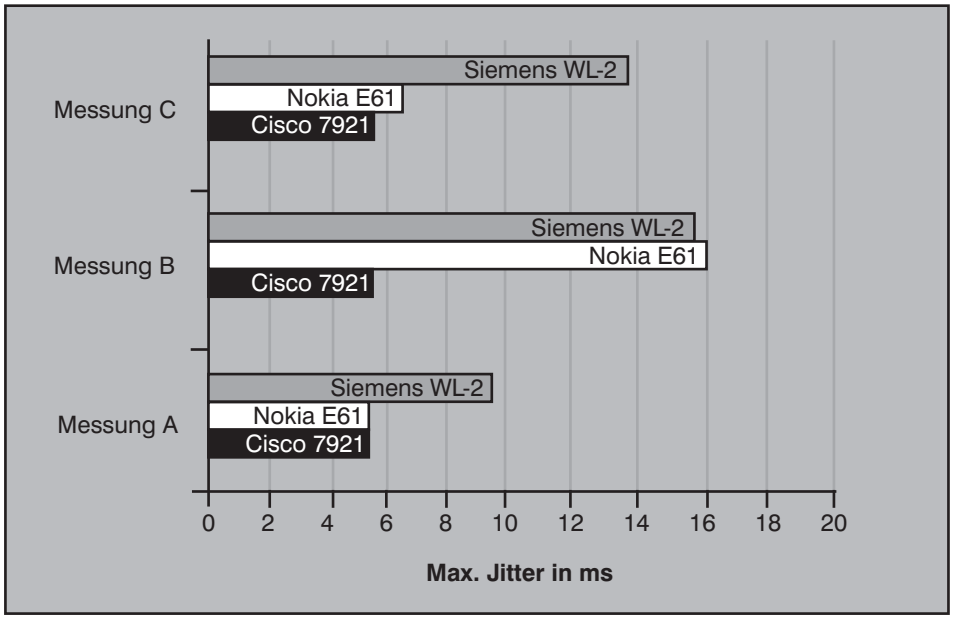


Abbildung 15: Maximalwert des Jitter im Vergleich

oder nur eine schwache Verschlüsselung (WEP) notwendig ist. Auch wenn ein solcher Zugang meist durch Firewall-Techniken geschützt ist, zum WLAN Controller selbst kommt der Angreifer immer. Also ist die Frage durchaus rechtfertigt, inwieweit die Controller-Lösungen gehärtet sind.

6.1 Testkonfiguration

Grundidee ist die Belastung eines WLAN Controllers durch das Senden von (sinnlosen) Paketen auf offenen Ports. Dabei muss die Anwendung auf dem Controller das Paket untersuchen, als unsinnig erkennen und verwerfen. Bei einem genügend großen Aufkommen solcher Pakete besteht prinzipiell die Gefahr, dass bei einer nicht geeigneten (oder nicht vorhandenen) Überlastabwehr der WLAN Controller seine Aufgaben nicht mehr verrichten kann und im schlimmsten Fall kollabiert.

Als Indikator für die Lebendigkeit des WLAN Controllers läuft während des Tests eine VoIP-Verbindung mit IxChariot über den WLAN Controller. Als Werkzeuge für die Belastung des Controllers wurden Jperf (siehe http://dast.nlanr.net/projects/jperf/) und der HP Internet Advisor eingesetzt.

Abbildung 18 zeigt die Testkonfiguration im Überblick.

6.2 Testfälle

In einem ersten Schritt wurde ein Test mit dem Port Scanner Nessus durchgeführt. Der Scan zeigte für die betrachteten Lösungen keine signifikanten Auffälligkeiten. Generell sind Ports für die Tunnel zu den Access Points und die benötigten Management Ports offen und daher konzentrierten sich die Tests auf diese Bereiche.

- Szenario 1: Sofern der Tunnelmechanismus UDP verwendet, werden mit Jperf Dummy-Pakete auf den Port für den Datenkanal geschickt (12222 bei Cisco, siehe Abbildung 19, 13910 bei Siemens).

- Szenario 2: Auf das Managementinterface wird mit dem HP Internet Advisor mit steigender Rate ein SNMP-Request geschickt (siehe Abbildung 20). Dabei wird bewusst ein falscher Community String verwendet. Die Management-Applikation kann das Paket daher schneller verwerfen.

In beiden Fällen handelt es sich um keine schwerwiegenden Angriffe, die eigentlich auch bei hoher Last zu keinen spürbaren Effekten führen sollten.

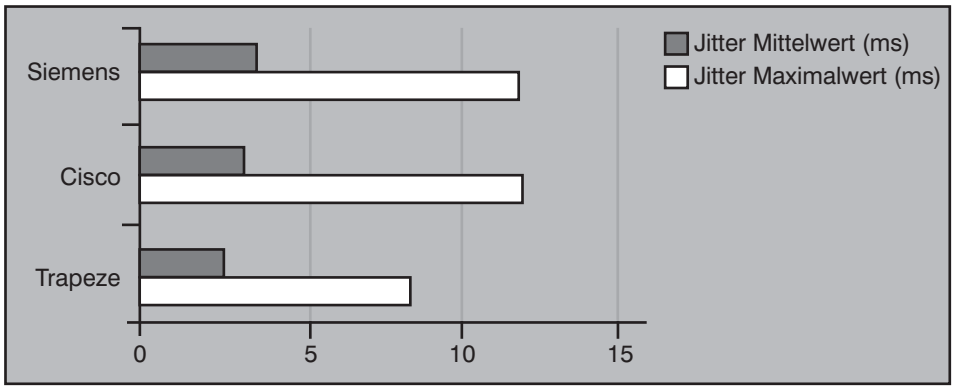


Abbildung 16: Jitter bei dem Szenario mit Handover

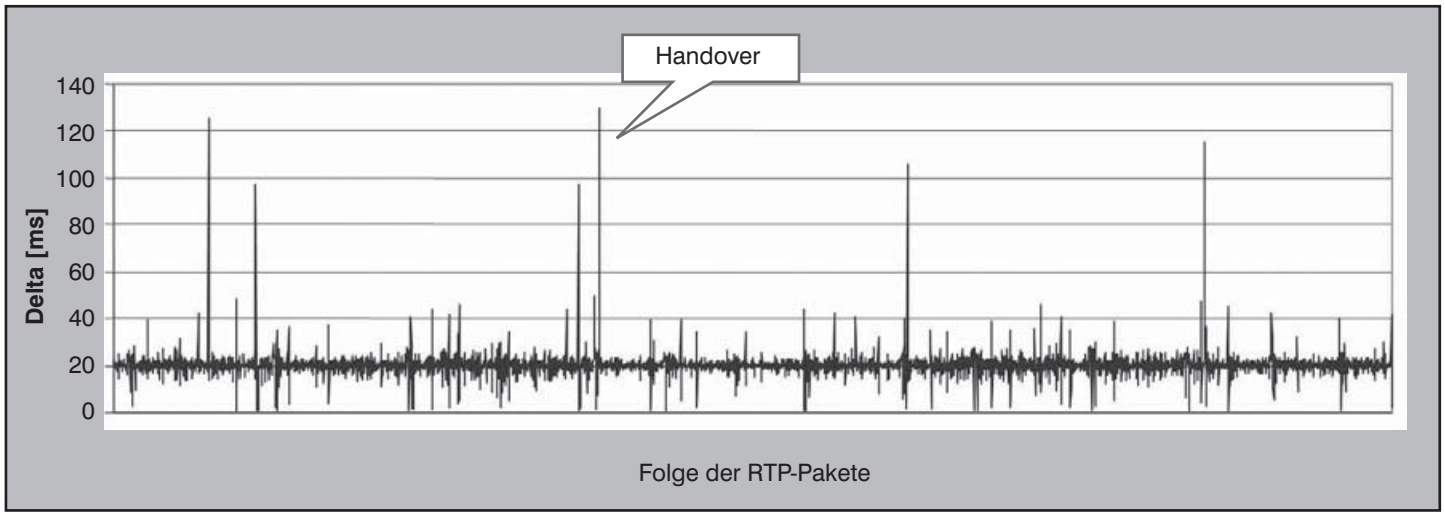


Abbildung 17: Anstieg des zeitlichen Abstands zwischen RTP-Paketen beim Handover am Beispiel der betrachteten Controller-Lösung von Siemens

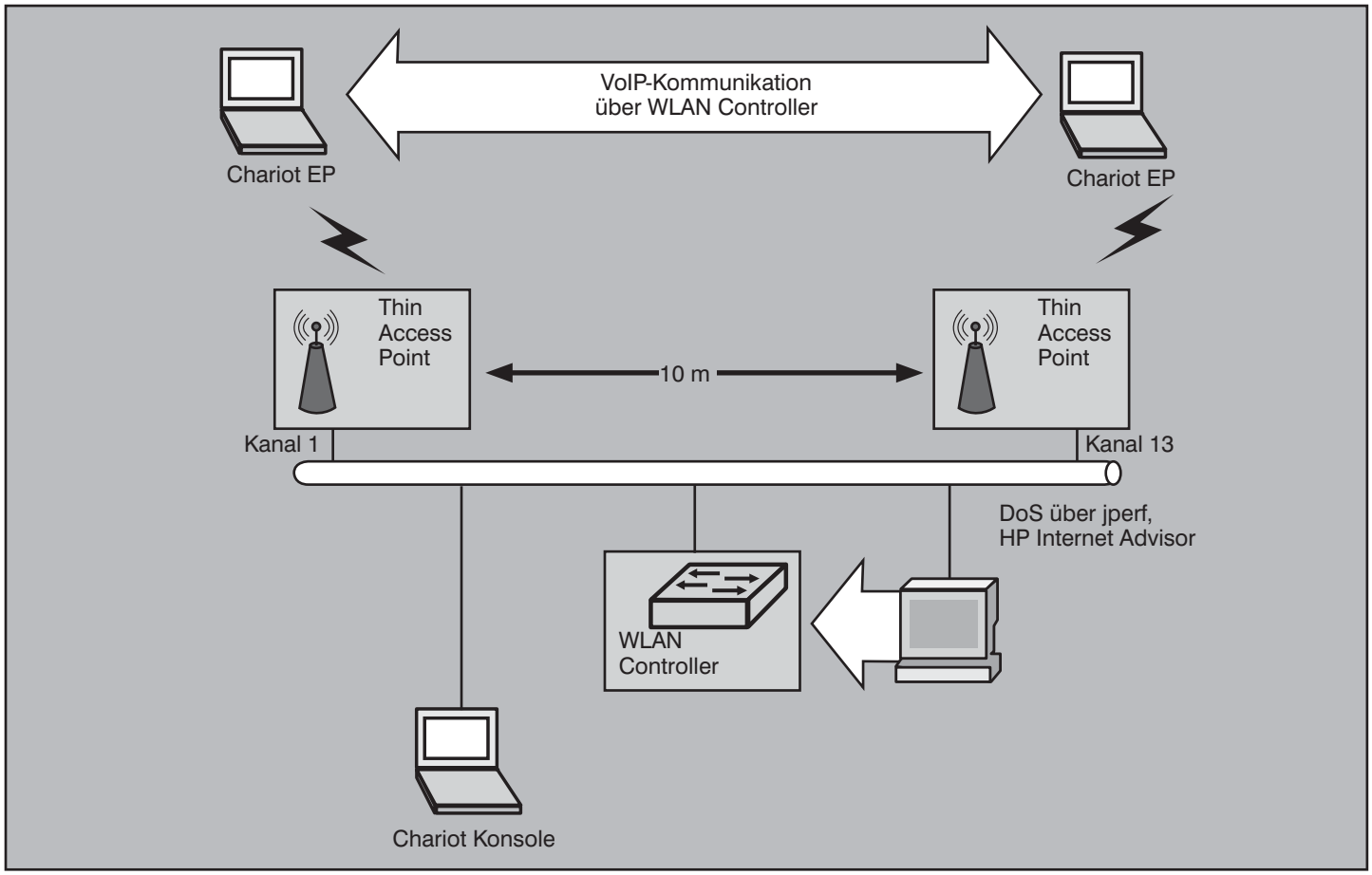


Abbildung 18: Testkonfiguration für DoS-Angriffe auf den WLAN Controller

6.3 Testergebnisse

Die Cisco-Lösung ist die von der Dimensionierung her kleinste Lösung im Test. Trotzdem ist es überraschend, dass bereits bei 24 MBit/s UDP-Last gemäß Szenario 1 der Controller kollabiert und praktisch keine WLAN-Kommunikation mehr möglich ist, wie in Abbildung 21 gezeigt.

Der Siemens-Controller zeigte sich robust. Im MOS-Wert konnte bis zum Maximum der Kapazität des Controllers keine sichtbare Leistungseinbuße verzeichnet werden.

Dass sich im Detail doch ein erheblicher Unterschied zwischen einer Belastung mit 50 MBit/s und mit 100 MBit/e ergibt, zeigt die Darstellung des maximalen Jitter in Abbildung 22.

Für das systematische Einspielen von SNMP-Verkehr gemäß Szenario 2 ergibt sich ein ähnliches Bild (siehe Abbildung 23). Der Cisco Controller hat bereits bei

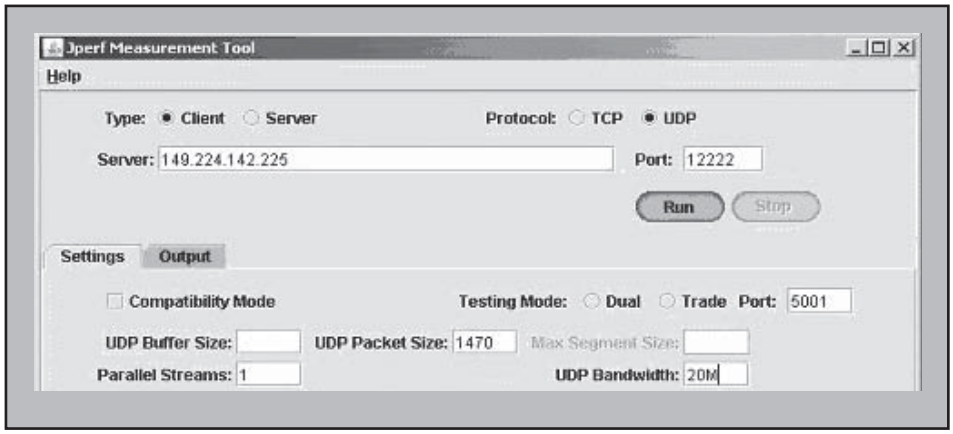


Abbildung 19: Ausschnitt aus der Jperf-Konfiguration

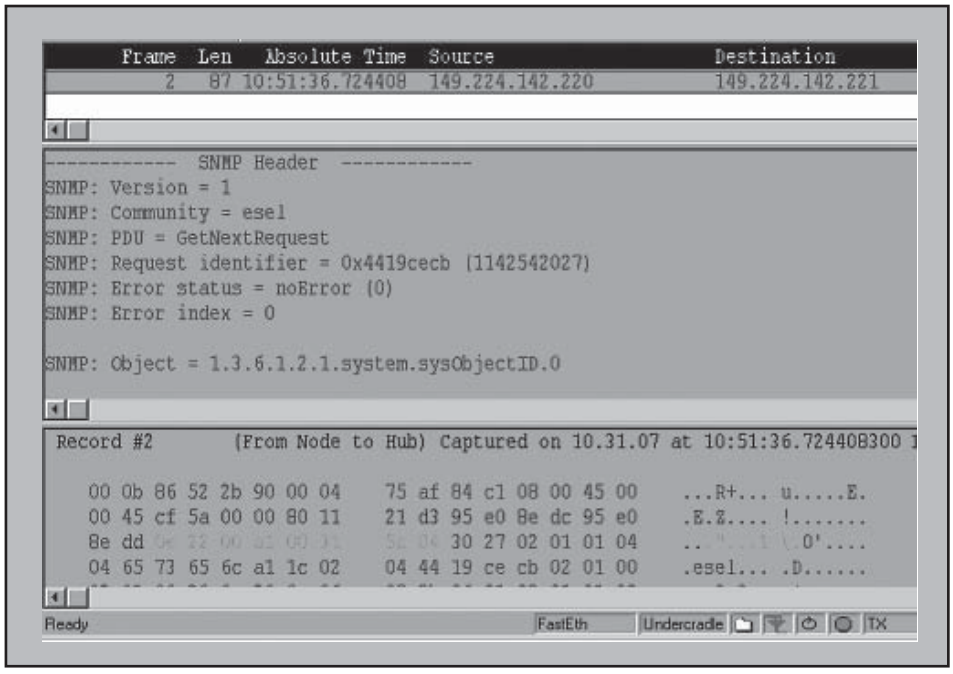


Abbildung 20: SNMP-Request an das Management-Interface der WLAN Controller

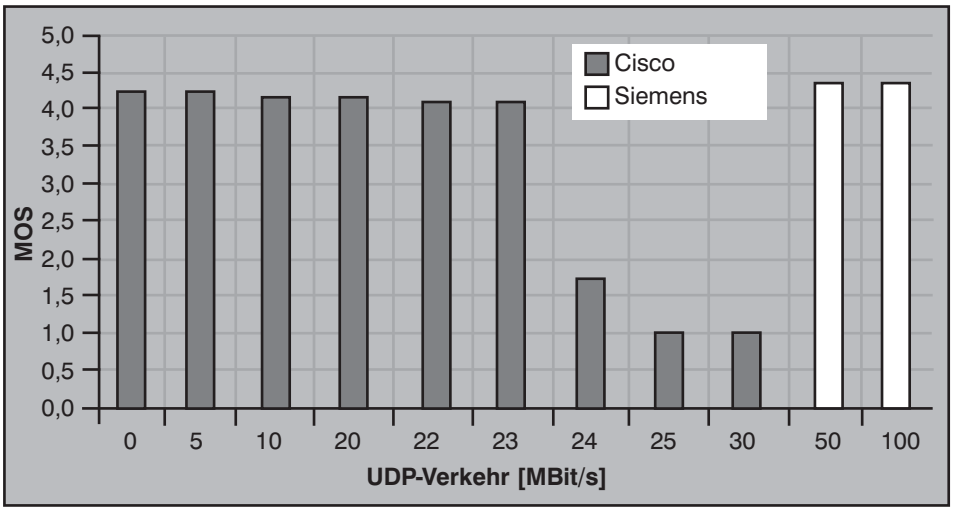


Abbildung 21: Sprachqualität bei unterschiedlicer Belastung des Controllers

20 MBit/s Last massive Probleme und bricht bei 22 MBit/s zusammen. Die Geräte von Siemens und Trapeze kommen fast ohne weitere Probleme zurecht. Bei Trapeze überrascht dies nicht, da im Vergleich die Ausbaustufe des Trapeze-Controllers die am größtem dimensionierte war.

Bei Betrachtung der Ergebnisse könnte man zu dem Fehlschluss verleitet werden, dass bei den betrachteten Geräten ja nur das am kleinsten dimensionierte Gerät Schwächen gezeigt hat, und DoS-Angriffe daher kein Problem darstellen würden, wenn man nur genügend groß dimensionierte Geräte verwenden würde. Die Praxis zeigt allerdings, dass es durchaus vorkommen kann, dass WLAN Controller ausgesprochen empfindlich gegenüber DoS (auch bei vergleichsweise geringer Angriffsintensität) reagieren können.

Für die Ausschreibung einer Controller-basierten WLAN-Lösung wird allgemein empfohlen, nicht nur den Funktionsumfang abzuprüfen, sondern auch Qualitäts- und Leistungs-orientierte Anforderungen zu stellen und entsprechende Nachweise zu verlangen.

7. Serie 4: Monitoring auf der Luftschnittstelle

Das Monitoring eines WLAN kann auf der Luftschnittstelle durch dedizierte Access Points, die ausschließlich eine Überwachungsaufgabe haben, erfolgen. Diese Access Points scannen kontinuierlich die Kanäle bei 2,4 GHz und ggf. bei 5 GHz und beobachten die Funkaktivität. Über eine zentrale Management-Anwendung kann dann die Qualität, mit der andere produktive Access Points empfangen werden, erfasst und in einer Karte des Versorgungsgebiets grafisch dargestellt werden. WLAN-Stationen (insbesondere fremde Access Points) können identifiziert und sogar lokalisiert werden. Abweichungen in der Konfiguration von Access Points und Endgeräten können erkannt und so Sicherheitsvorfällen vorgebeugt werden. Oft können diese Systeme auch Angriffsmuster im WLAN erkennen (z.B. DoS-Attacken zur Deauthentifizierung oder gegen EAP) und bei Bedarf einen Alarm auslösen (siehe Abbildung 24).

Auf dem Markt existieren hierzu dedizierte Systeme (z.B. Lösungen von AirMagnet und AirDefense). Controller-basierte Lösungen bieten meist auch die Möglichkeit Access Points dediziert als WLAN Probes zu nutzen. Die zusätzlichen Ac-

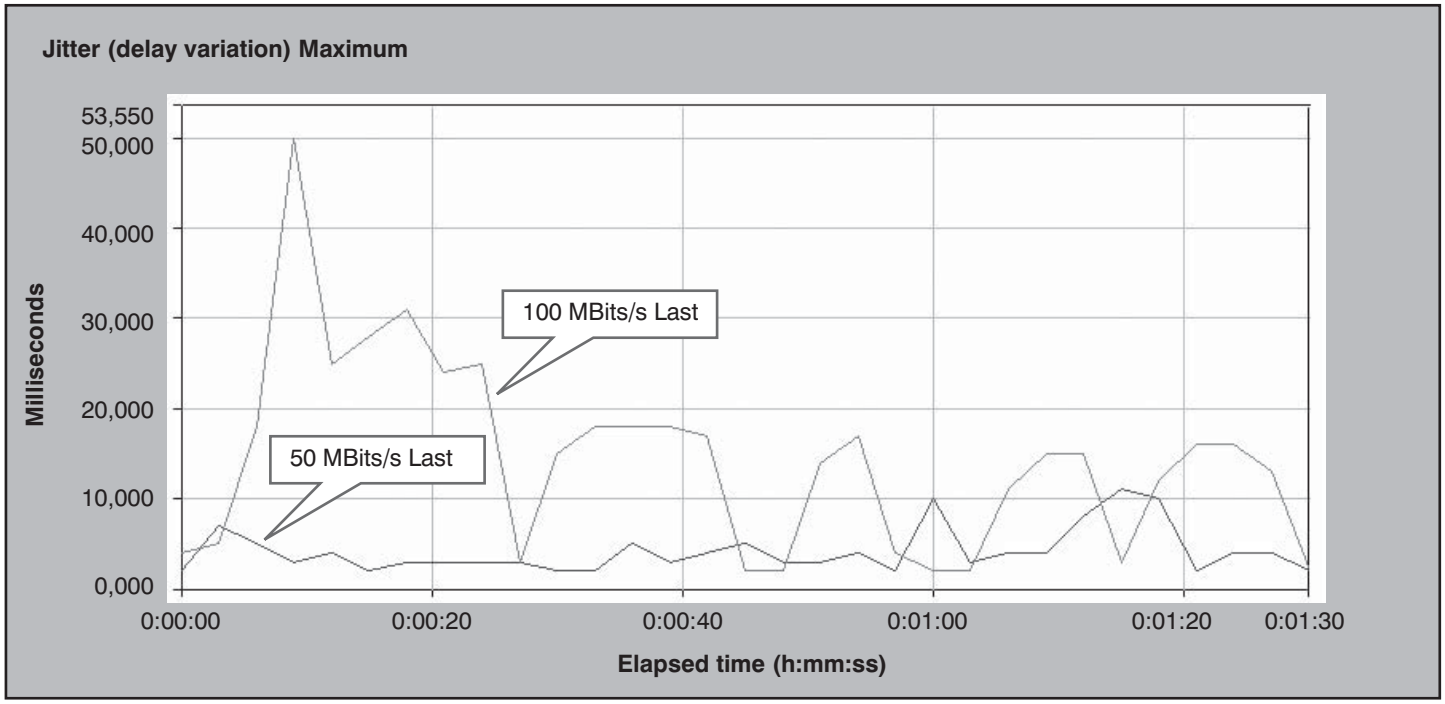


Abbildung 22: Zeitlicher Verlauf des Jitter Maximalwertes (Bildschirmdarstellung von IXCahriot)

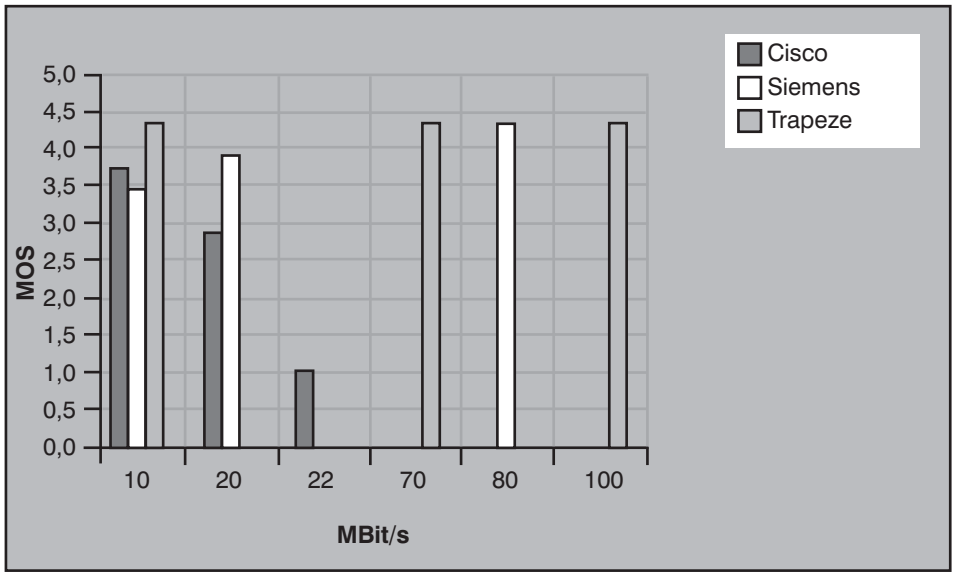


Abbildung 23: Sprachqualität bei unterschiedlicer Belastung des Controllers durch SNMP-Anfragen

cess Points verursachen natürlich Kosten und letztendlich entsteht ein Monitoring WLAN, welches das eigentliche produktive WLAN überwacht.

Natürlich ist es dann auch naheliegend, die produktiven Access Points als Messinstrument für das WLAN Monitoring zu verwenden. Die produktiven Access Points wechseln dabei zwischen dem Normalbetrieb und einem Messbetrieb und beobachten im Messbetrieb die verschiedenen Funkkanäle. Für die Dauer, die ein Access Point im Messbetrieb ist, kann dann der Access Point natürlich nicht mehr genutzt werden, um Pakete zu transportieren. Ein Leistungsverlust in Form von sinkendem Durchsatz und erhöhter Antwortzeit ist die Folge. Inwieweit dieser Effekt sichtbar und für eine Sprachübertragung spürbar ist, soll dieser Test bewerten.

Das wesentliche Element für die Nutzung eines Access Point zu Messungen ist die Möglichkeit zur Konfiguration der Zeiten zwischen zwei Messungen und der Dauer einer Messung. Abbildung 25 zeigt die entsprechenden Konfigurationsmöglichkeiten der Siemens WLAN-Controller-Lösung.

Beim Hersteller Trapeze werden die Parameter für das Monitoring über die Management-Applikation RingMaster gesetzt. Die Funktion zur regelmäßigen Messung des Funkkanals wird dann einfach durch Aktivierung der Option Enable Active Scan gestartet, wie in Abbildung 26 gezeigt.

Der Testaufbau zur Bewertung dieser Funktion entspricht dem Aufbau für Szenario a in Kapitel 4, in dem zwei IxChariot Endpoints ein VoIP-Gespräch führen (siehe Abbildung 3). Den Vergleich zwischen der aktivierten Scan-Funktion (Wechsel zwischen Normal- und Messbetrieb) und der deaktivierten Scan-Funktion (nur Normalbetrieb) zeigt Abbildung 27 für die Trapeze-Lösung. Durch den regelmäßigen Messbetrieb kommt es an den entsprechenden Zeitpunkten zu deutlichen Einbrüchen in der Sprachqualität.

Dieser Effekt ist auch bei anderen Herstellern ähnlich beobachtbar.

Generell gilt, dass bei Nutzung von VoWLAN möglichst auf eine solche Scan-Funktion in den produktiven Access Points verzichtet werden sollte und dedizierte Access Points (WLAN Probes) für das WLAN Monitoring eingesetzt werden sollten.

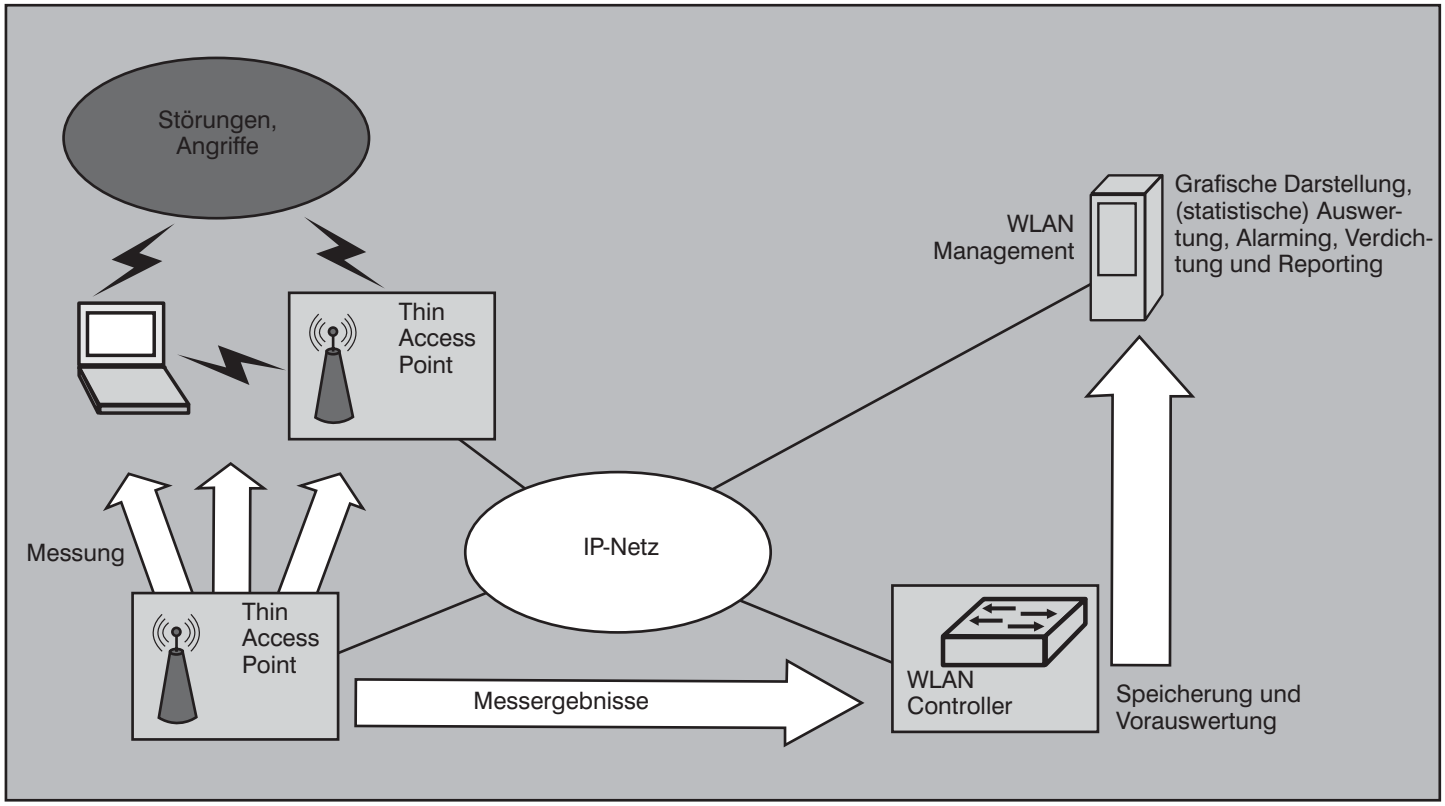


Abbildung 24: WLAN-Überwachung durch (produktive) Access Points

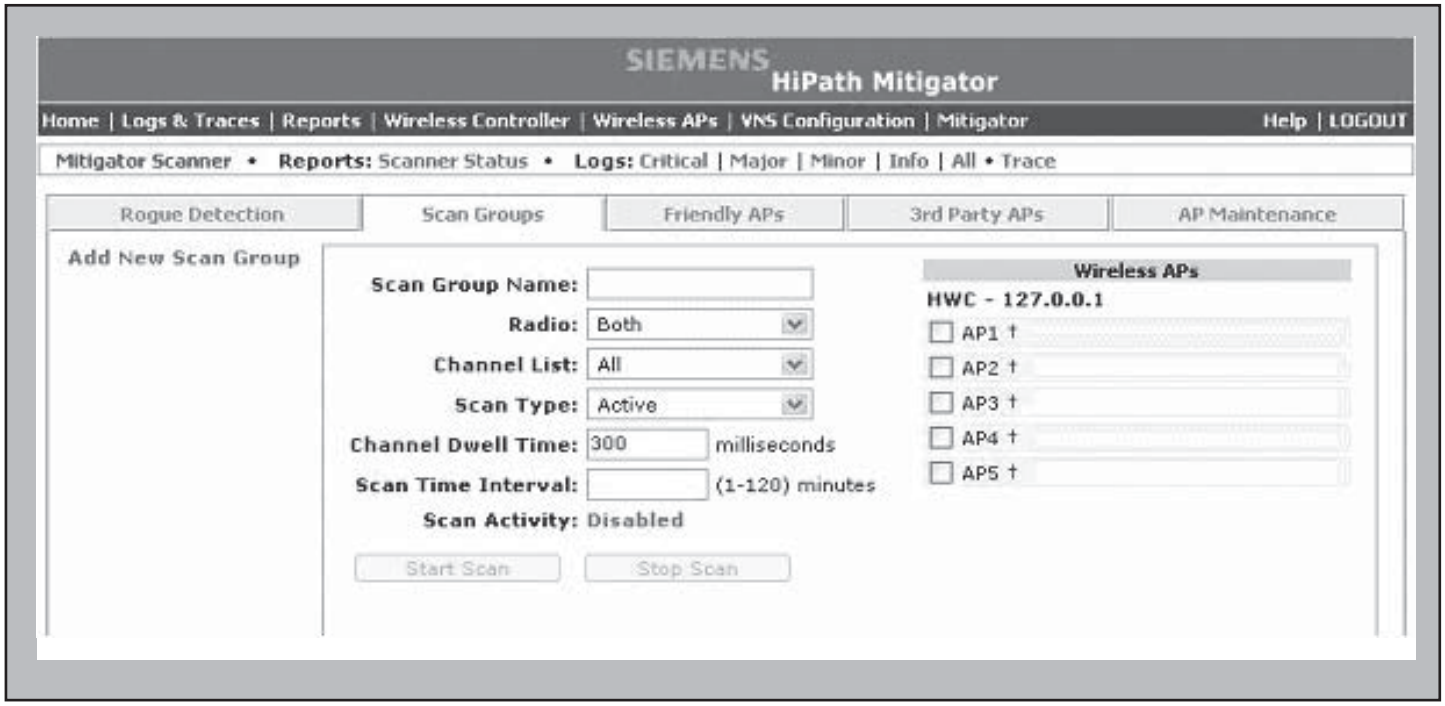


Abbildung 25: Konfiguration der Scan-Funktion bei der Siemens-Lösung

Zumindest sollte in Bereichen, in denen VoWLAN unterstützt werden soll, die Parameter zur Dauer der Messpause so eingestellt werden, dass der Einfluss auf die Sprachqualität nur noch kaum sichtbar ist. Grundsätzlich kann aber auch ein Mischbetrieb angedacht werden. Dabei würde man in kritischen Bereichen mit dedizierten WLAN Probes arbeiten und in weniger kritischen Bereichen das Risiko einer schlechteren Sprachqualität eingehen und mit einer Scan-Funktion in den produktiven Access Points arbeiten. Letztendlich bleibt es eine wirtschaftliche Entscheidung und eine Frage der Priorität des Sprachdienstes im WLAN.

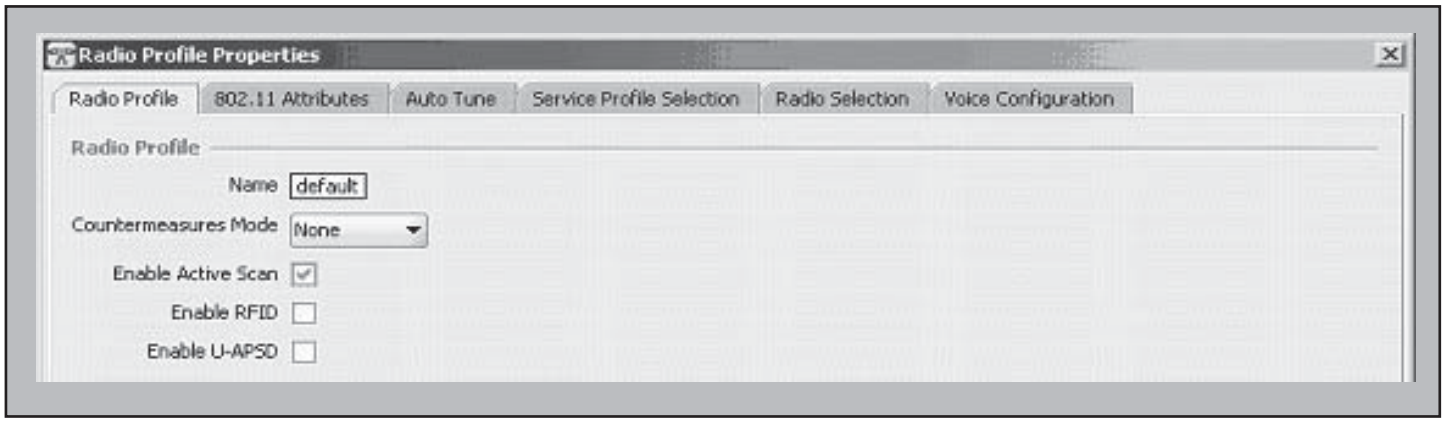


Abbildung 26: Aktivierung der Scan-Funktion bei der Trapeze-Lösung

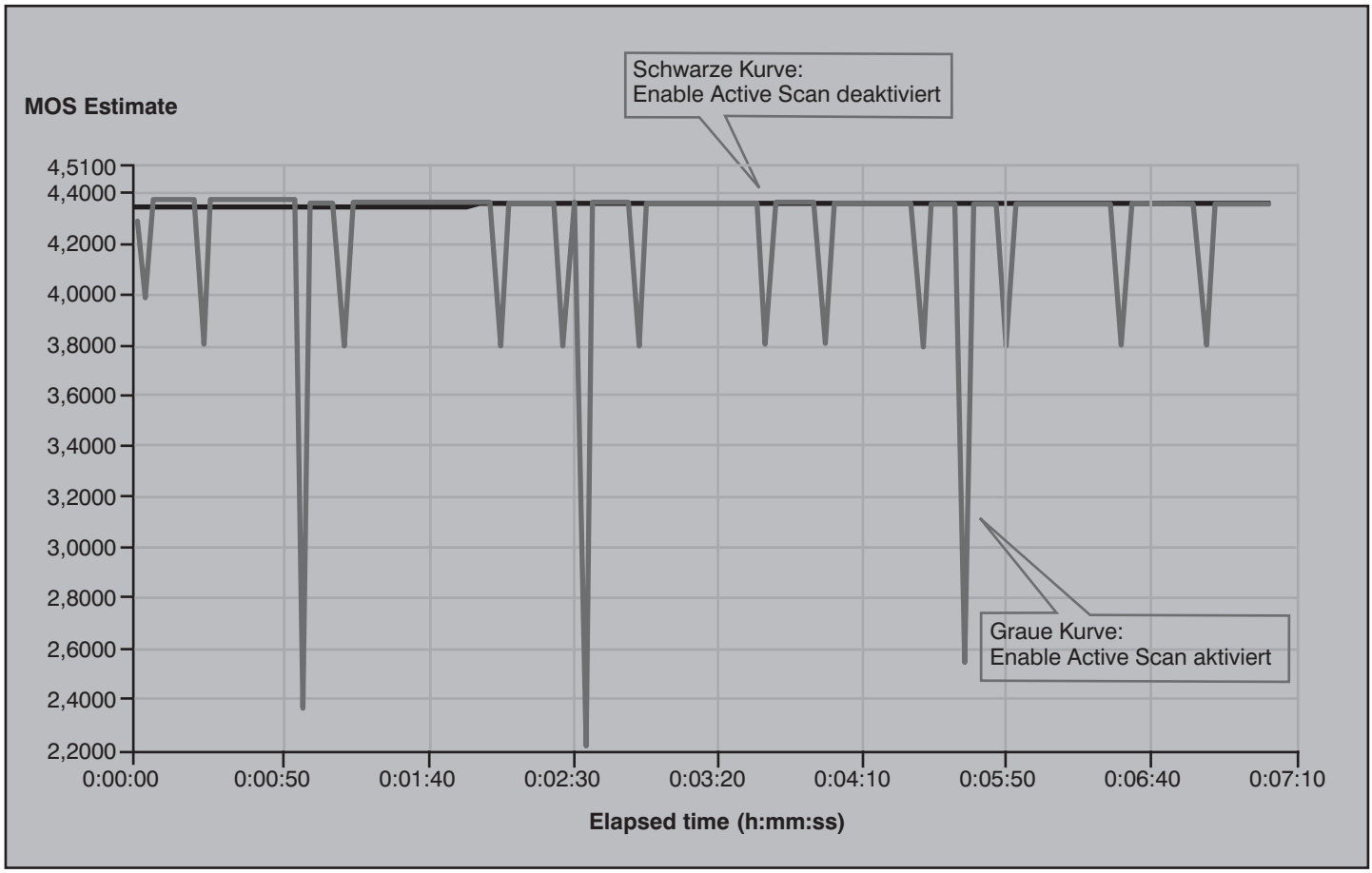


Abbildung 27: Einfluss der Scan-Funktion auf die Sprachqualität am Beispiel der Trapeze-Lösung (Bildschirmdarstellung von IXCahriot)

8. Fazit

Die Robustheit und Stabilität mancher Controller-Lösungen ist verbesserungswürdig. Dies betrifft nicht nur DoS-Angriffe. Auch ein Normalverkehr kann bei manchen Lösungen bereits sichtbare Einflüsse auf die Leistung kritischer Dienste haben. Gleichkanalstörungen sind bei 2,4 GHz praktisch unvermeidbar. Die Robustheit gegenüber diesen Störungen ist herstellerabhängig, wobei primär die Qualität der Access Points zählt. Die Überwachung der Luftschnittstelle über die produktiven Access Points bedingt einen sichtbaren Leistungsverlust. Weiterhin muss der Einfluss von WLAN Clients (speziell bzgl. der Funktionen Scanning und Handover) auf die Dienstgüte berücksichtigt werden.

Insgesamt ist zu empfehlen, bei der Beschaffung einer WLAN-Controller-Lösung nicht nur den Funktionsumfang abzuprüfen, sondern auch Qualitäts- und Leistungs-orientierte Anforderungen zu stellen und entsprechende Nachweise zu verlangen. Als Konsequenz sollte bei Abnahmetests - über die Prüfung der Güte einer Ausleuchtung hinausgehend - für kritische Dienste auch die Dienstgüte sowie Leistung, Stabilität und Verfügbarkeit unter Lastbedingungen getestet werden.

ComConsult Veranstaltungskalender

Aktuelle Veranstaltungen

IP-Telefonie evaluieren, planen, betreiben, 11.02. - 13.02.08 in Berlin

Dieses 3-tägige Seminar evaluiert Technologien und Produkte gegenüber den in der Praxis bestehenden Anforderungen. Es vermittelt die technischen Grundlagen, beschreibt die Arbeitsweise wichtiger Produkte, analysiert typische Nutzungsformen und gibt eine Prognose für die Marktsituation und weitere Entwicklung. Die Situation etablierter Hersteller wie Alcatel, Avaya/Tenovis, Cisco, Nortel und Siemens inklusive des Leistungsumfangs ihrer Produkte wird bewertet. Preis: € 1.690,- zzgl. MwSt.

Sicherheit im LAN mit IEEE 802.1X, 11.02. - 12.02.08 in Berlin

Dieses 2-tägige Seminar vermittelt den optimalen Umgang mit IEEE 802.1X, erläutert die Einsatzvarianten, beschreibt die gegebenen Fallstricke und liefert die ideale Basis zur Vorbereitung eines Einsatzes. Preis: € 1.390,- zzgl. MwSt.

WAN-Planung für zentrale Dienste, 11.02. - 13.02.08 in Berlin

Wide Area Networks (WAN) müssen kostengünstig, leistungsfähig, skalierbar, hochverfügbar, sicher und managebar sein. Während bis vor wenigen Jahren langfristige WAN-Verträge von drei bis fünf Jahren abgeschlossen wurden, legt die dynamische Entwicklung nahe, die Vertragsbindung zu verkürzen, was mit einem ständigen Planungsprozess einhergeht. Dieser Umstand und die fortlaufenden Veränderungen im Markt zwingen zu einem permanenten Lern- und Informationsprozess, dem auch dieses 3-tägige Seminar dienen soll. Preis: € 1.690,- zzgl. MwSt.

Sicherheit 1: Grundlagen und Kernbausteine zur erfolgreichen IT-Sicherheit, 18.02. - 22.02.08 in Aachen

Bedrohungen der IT-Sicherheit bestehen für praktisch alle Elemente einer vernetzten IT-Infrastruktur. Die Quelle der Bedrohung kann sowohl von außen auf das Netz wirken als auch von innen stammen. Sicherheit entsteht erst, wenn alle signifikanten Gefahrenbereiche systematisch verriegelt werden. Dieses Seminar identifiziert die wesentlichen Gefahrenbereiche und zeigt effiziente und wirtschaftliche Maßnahmen zur Umsetzung einer erfolgreichen Lösung auf. Dabei wird jeder einzelne Baustein detailliert erklärt und anhand typischer Einsatzszenarien wird der Weg zu einer erfolgreichen Sicherheits-Lösung aufgezeigt. Preis: € 2.290,- zzgl. MwSt.

Office Communications Server 2007, 18.02. - 19.02.08 in Bonn

In diesem Seminar werden sowohl die technischen als auch die strategischen Aspekte des Office Communications Servers analysiert. Unsere herstellerunabhängigen und neutralen Experten haben sich sehr ausführlich mit den technischen Details befasst und verfügen über langjährige Erfahrung bei der Implementierung von Microsoft-Lösungen, bei der Konzeption von TK-Lösungen sowie bei der Bewertung von Kommunikationstechnologien Preis: € 1.390,- zzgl. MwSt.

IP-Wissen für TK-Mitarbeiter, 18.02. - 19.02.08 in Hamburg

Dieses Seminar vermittelt kompakt und effizient das IP-Wissen, das TK-Mitarbeiter ohne Vorkenntnisse zur Planung und zum Betrieb von IP-basierten Telefonie-Lösungen benötigen. Preis: € 1.390,- zzgl. MwSt.

Projektmanagement I: Projekte erfolgreich leiten, organisieren und optimieren, 18.02. - 22.02.08 in Hamburg

In diesem 5-tägigen Intensiv-Kurs lernen Sie, ein Projekt erfolgreich zu leiten und organisieren. Es werden bewährte Wege aufgezeigt, wie Sie die Projektabwicklung im Alltag in Ihrem Unternehmen konkret optimieren. Preis: € 2.290,- zzgl. MwSt.

SIP (Session Initiation Protocol)- Basis-Technologie der IP-Telefonie, 25.02. - 27.02.08 in Stuttgart

Dieses 3-tägige Seminar vermittelt Planern und Betreibern Anforderungen und Technologien für den Einsatz von Telefonie und Mehrwertdiensten auf Basis des neuen Standards SIP. Chancen und Risiken werden anhand von Einsatzszenarien bewertet und kontrovers diskutiert.. Preis: € 1.690,- zzgl. MwSt.

Sicherheitsmechanismen für Voice over IP, 25.02. - 26.02.08 in Stuttgart

Angesichts der Offenheit und geringeren Verfügbarkeit von Datennetzen ist das Thema Sicherheit das zentrale Projektthema bei der Umsetzung von Voice over IP. VoIP benötigt Sicherheitsmechanismen, die mindestens ein den konventionellen Telekommunikationsnetzen entsprechendes Niveau an Vertraulichkeit, Verlässlichkeit, Verfügbarkeit und Integrität sicherstellen. Darüber hinaus bietet die Umstellung die Chance, die Sicherheit der Sprachkommunikation über das bisherige Niveau hinaus zu verbessern.

Preis: € 1.390,- zzgl. MwSt.

Wireless LAN: Planung, Produktauswahl, Installation, Trouble Shooting, 25.02. - 27.02.08 in Stuttgart

Dieses 3-tägige Seminar erklärt die Arbeitsweise von WLANs und beschreibt typische Einsatzszenarien von der Ergänzung bestehender LANs bis hin zur kompletten WLAN-Infrastruktur. Die letzten beiden Tage sind optinonal buchbar und liefern vertiefte Kenntnisse zur Planung, Konfiguration und Betrieb von flächendeckenden sicheren WLAN und Hotspots, ergänzt durch praktische Beispiele und Demonstrationen. Preis: € 1.690,- zzgl. MwSt.

TCP/IP und SNMP, 25.02. - 29.02.08 in Stuttgart

Dieses 5-tägige Seminar vermittelt systematisch die Grundlagen TCP/IP, beleuchtet Vor- und Nachteile und gibt wichtige Empfehlungen für den erfolgreichen Einsatz. Dies betrifft speziell auch die wichtigen IP-Infrastrukturdienste von der Adressierung über ARP bis zu DHCP, DNS, DDNS und NAT und die Management-Funktionalität SNMP. Preis: € 2.290,- zzgl. MwSt.

Zertifizierungen

ComConsult Certified Network Engineer

Lokale Netze
11.02. - 15.02.08 in Aachen
09.06. - 13.06.08 in Aachen
15.09. - 19.09.08 in Aachen
24.11. - 28.11.08 in Aachen

TCP/IP und SNMP
25.02. - 29.02.08 in Stuttgart
26.05. - 30.05.08 in Aachen
20.10. - 24.10.08 in Berlin

Internetworking
10.03. - 14.03.08 in Aachen
02.06. - 06.06.08 in Aachen
13.10. - 17.10.08 in Aachen

Paketpreis für alle drei Seminare € 6.183,-- zzgl. MwSt. (Einzelpreise: je € 2.290.--)

ComConsult Certified Trouble Shooter

Trouble Shooting in Lokalen Netzwerken - Grundlagen
03.03. - 07.03.08 in Aachen
16.06. - 20.06.08 in Aachen
01.09. - 05.09.08 in Aachen

Trouble Shooting in konvergenten Netzwerken
31.03. - 04.04.08 in Aachen
23.06. - 27.06.08 in Aachen
08.09. - 12.09.08 in Aachen

Trouble Shooting für TCP/IP- und Windows-Umgebungen
02.06. - 06.06.08 in Aachen
13.10. - 17.10.08 in Aachen

Paketpreis für alle drei Seminare, eine digitale Stromzange, die Prüfung und den Report „Fehlersuche in konvergenten Netzen“ € 6.990.-- zzgl. MwSt. (Einzelpreise: je € 2.490.--)

ComConsult Certified Security Expert

Sicherheit 1: Grundlagen und Kernbausteine zur erfolgreichen IT-Sicherheit
18.02. - 22.02.08 in Aachen
05.05. - 09.05.08 in Bonn
22.09. - 26.09.08 in Bonn

Sicherheit 2: Erarbeitung und Umsetzung von Sicherheitskonzepten
10.03. - 14.03.08 in Frankfurt
23.06. - 27.06.08 in Bonn
03.11. - 07.11.08 in Bonn

Sicherheit 3: Praxis-Intensiv-Seminar zur erfolgreichen Konfiguration von Firewalls, VPNs, Windows Clients und WLANs
07.04. - 11.04.08 in Aachen
25.08. - 29.08.08 in Aachen
01.12. - 05.12.08 in Aachen

Paketpreis für alle drei Seminare und die beiden Reports „VPN-Technologien: Alternativen und Bausteine einer erfolgreichen Lösung“ und „Sicherheit in Wireless LANs“. € 6.183.-- zzgl. MwSt. (Einzelpreise: je € 2.290.--)

ComConsult Certified Voice Engineer

Basis-Seminar: Session Initiation Protocol-Basis-Technologie der IP-Telefonie
25.02. - 27.02.08 in Stuttgart
05.05. - 07.05.08 in Bonn
15.09. - 17.09.08 in Frankfurt
17.11. - 19.11.08 in Frankfurt

Basis-Seminar: Sicherheitsmechanismen für Voice over IP
25.02. - 26.02.08 in Stuttgart
05.05. - 06.05.08 in Bonn
03.11. - 04.11.08 in Bonn

Alternative 1: IP-Telefonie evaluieren, planen, betreiben
11.02. - 13.02.08 in Berlin
21.04. - 23.04.08 in Bonn
01.09. - 03.09.08 in Stuttgart
27.10. - 29.10.08 in Bonn

Alternative 2: IP-Telefonie: Vorbereitung, Migration, Management
10.03. - 12.03.08 in Frankfurt
02.06. - 04.06.08 in Stuttgart
13.10. - 15.10.08 in Bonn

Optionales Einsteiger-Seminar: IP-Wissen für TK-Mitarbeiter
18.02. - 19.02.08 in Hamburg
10.06. - 11.06.08 in Bonn
08.09. - 09.09.08 in Bonn
17.11. - 18.11.08 in Frankfurt

Basis-Paket Alternative 1: Beinhaltet die zwei Basis-Seminare und Seminar „Alternative 1“ Grundpreis: € 4.250,-- zzgl. MwSt. statt € 4.770,-- zzgl. MwSt.

Basis-Paket Alternative 2: Beinhaltet die zwei Basis-Seminare und Seminar „Alternative 2“ Grundpreis: € 4.250,-- zzgl. MwSt. statt € 4.770,-- zzgl. MwSt.

Optionales Einsteigerseminar: Aufpreis € 990,-- zzgl. MwSt. statt € 1.390,-- zzgl. MwSt.

Impressum

Verlag:
ComConsult Technology Information Ltd.
121 Paton Rd. - RD1 - Richmond
New Zealand
GST Number 84-302-181
Registration number 1260709
Phone: 0064 3 3234415
German Hotline of ComConsult-Research:
02408-955300

E-Mail: insider@comconsult-akademie.de
http://www.comconsult-research.de

Herausgeber und verantwortlich im Sinne des Presserechts:
Dr. Jürgen Suppan
Chefredakteur: Dr. Jürgen Suppan
Erscheinungweise: Monatlich,
12 Ausgaben im Jahr

Bezug: Kostenlos als PDF-Datei über den eMail-VIP-Service der ComConsult Akademie