

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 Qua- lität hinter sich

ab Seite 2

Neues Seminar

### Office Communications Server 2007

ab Seite 3

## 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 Größenordnung 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 ver-

schärfen, 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 laufeitensensitiv

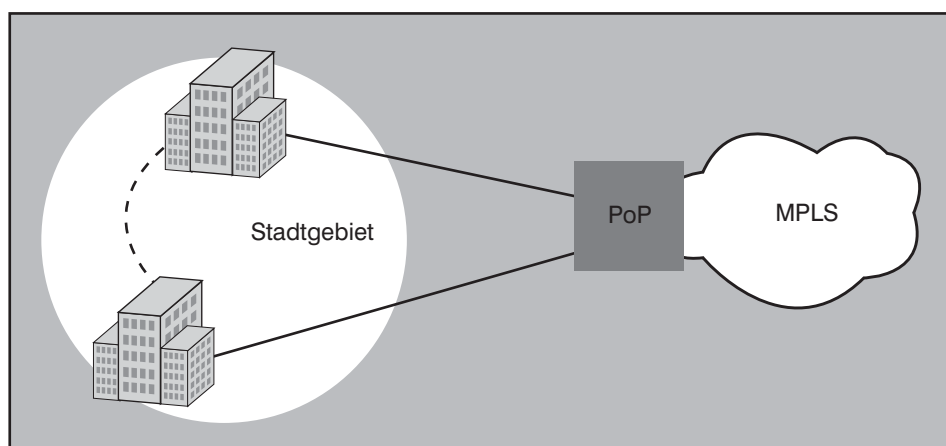


Abbildung 1: Ungünstige MPLS-Konstellation

## 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 ausgefallenen

## Seminar



### 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.

Referenten: Dipl.-Inform. Andreas Meder, Dr.-Ing. Behrooz Moayeri  
Preis: € 1.690,- zzgl. MwSt.



Buchen Sie über unsere Web-Seite [www.comconsult-akademie.de](http://www.comconsult-akademie.de)

## 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-Aggregation 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 An-

bindungsvariante so kostengünstig - kann die lokale Verfügbarkeit stark schwanken, je nach momentaner Anzahl auf die DSLAMs (DSL Access Multiplexer) der Vermittlungsstelle angeschalteter 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

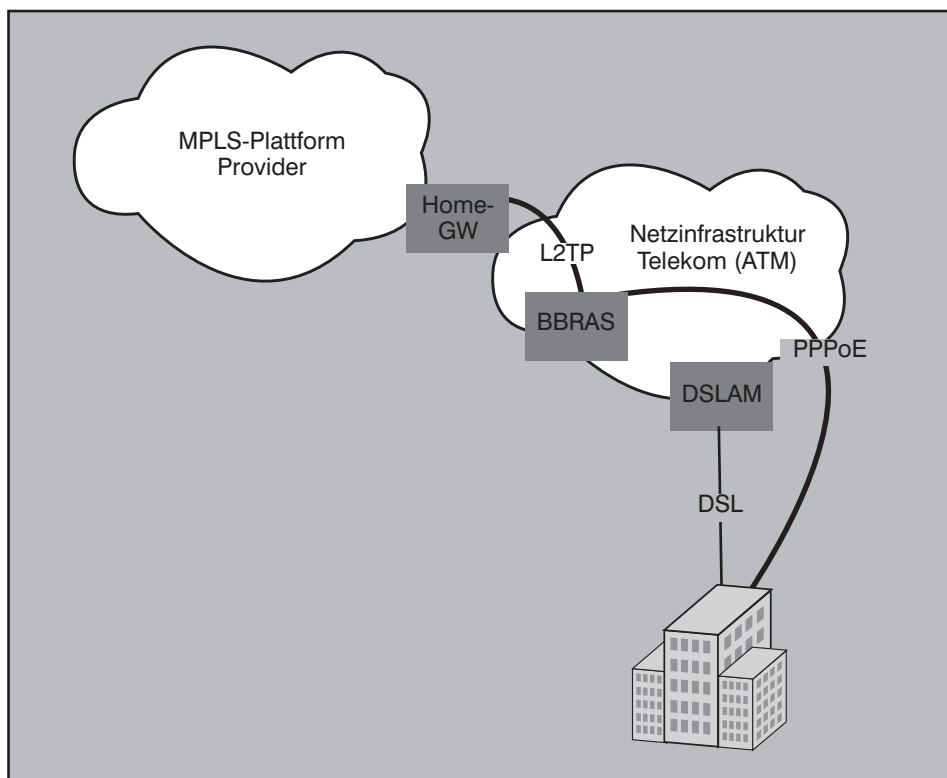


Abbildung 2: DSL-basierter Local Tail (via T-DSL)

---

 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 resultierenden 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, wohlgedenkt, 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

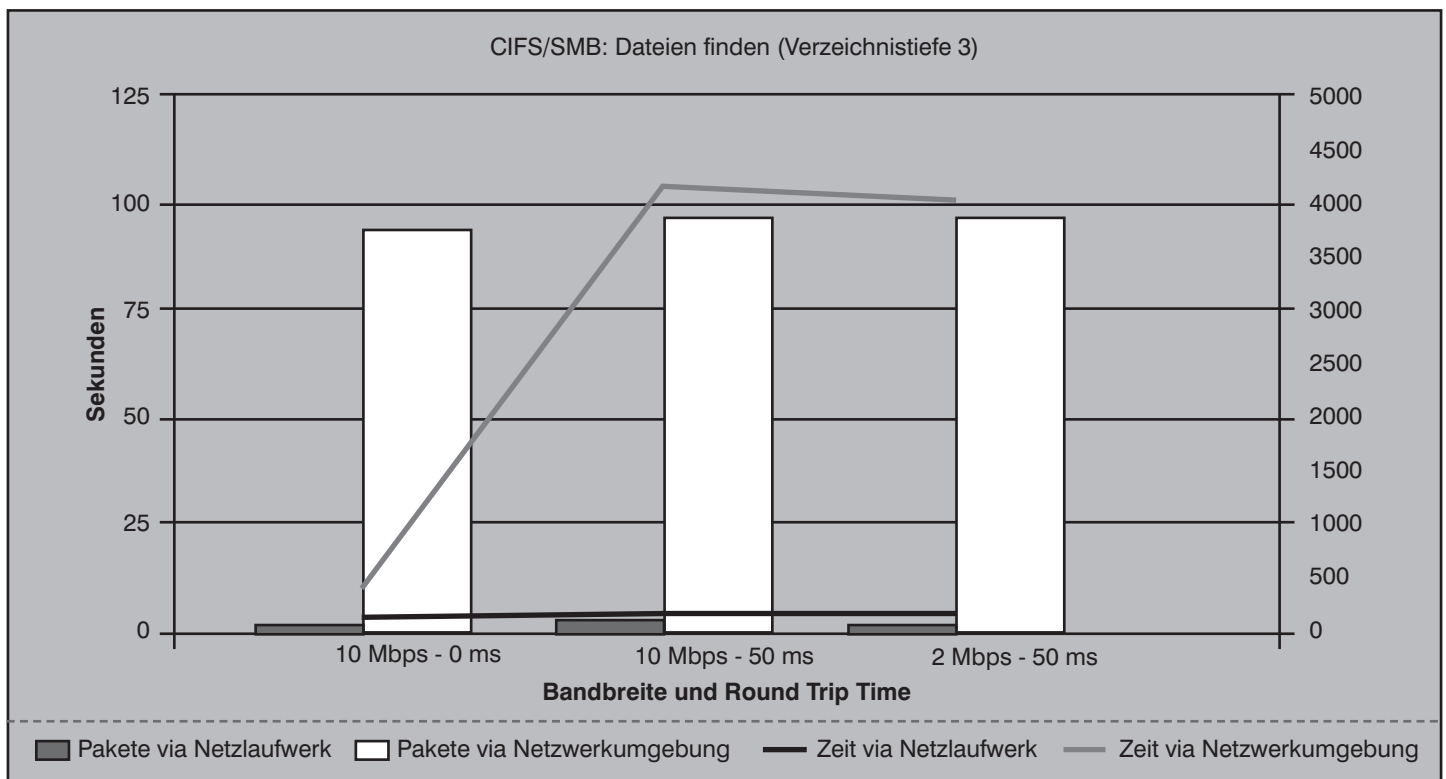


Abbildung 3: Zeitbedarf und Protokollpakete beim Suchen unter CIFS/SMB

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 Downstream. 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-Übertragungsrates 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 Kapazitäten für zügigen Bestätigungs-transport 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. mittels 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-

## Report



### Wide Area Networks Stand der Technik und Leitfaden für ein Redesign

Diese Studie behandelt das gesamte Spektrum von den technologischen Grundlagen über Projekt- und Designplanung und Ausschreibungsdetails bis zu Betriebskonzepten und Management von WANs. Die Autoren zeichnen sich durch jahrelange Erfahrung im Bereich der Konzipierung und Planung von WAN-Lösungen sowohl bei der Übertragung und Überprüfung von Kommunikationsdiensten an Provider als auch beim Aufbau eigener WAN-Infrastrukturen aus. Beide Autoren sind auch als Referenten auf Kongressen und Seminaren der ComConsult Akademie bekannt und erhalten dort regelmäßig hervorragende Beurteilungen.

Autoren: Dipl.-Inform. Andreas Meder, Dr.-Ing. Behrooz Moayeri  
Preis: € 398,- zzgl. MwSt. und Versand



Bestellen Sie über unsere Web-Seite [www.comconsult-research.de](http://www.comconsult-research.de)

## 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 überträgt, 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-Ausbauprojekts (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 Be-

tracht - 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 auszuliegen.

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 Anwendungssitzungen 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 vereinzelt 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		Unterbrechungsdauer in Sec.		Durchsatz in Mbps		Unterbrechungsdauer 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 anwendungsorientierte 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 Baselineing versteht, aber meist der Applikations-orientierten Methode der Vor-

zug 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 kostengünstigsten 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.

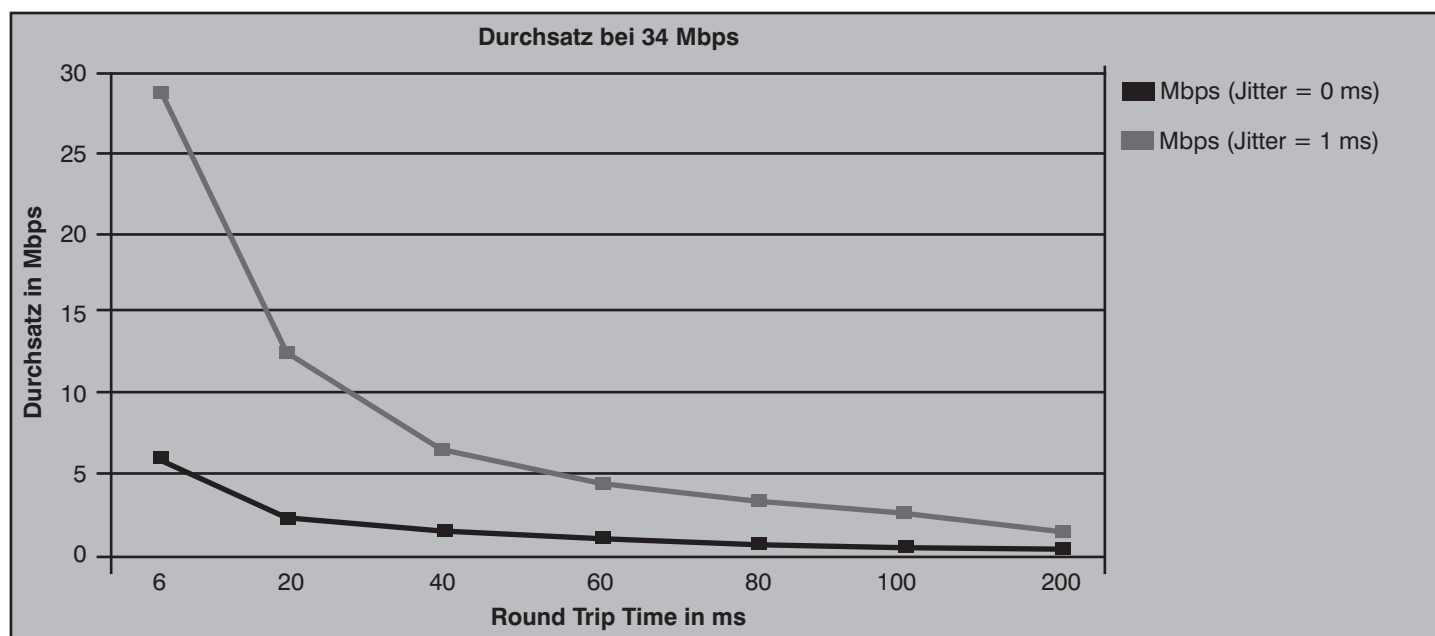


Abbildung 4: Emulierte Durchsatzwerte bei E3 (gemessen mit QCheck)

## 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 Netzwerkinstallation 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 Koppelung der immer leistungsfähiger werdenden lokalen Ethernets ohne Einbußen an Leistungsfähigkeit und Qualität ermög-

licht. 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 Netzabschlussstechnik; 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 granulareren 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-Netzknotten SDSL (Symmetrical Digital Subscriber 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-Protokoll-overhead.

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

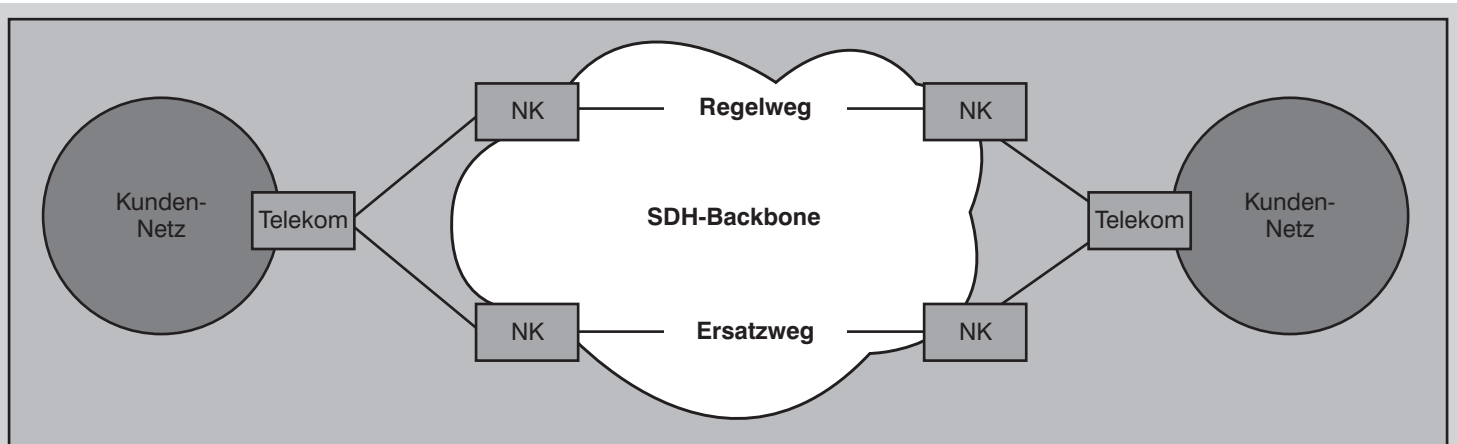


Abbildung 5: Prinzip HPS1

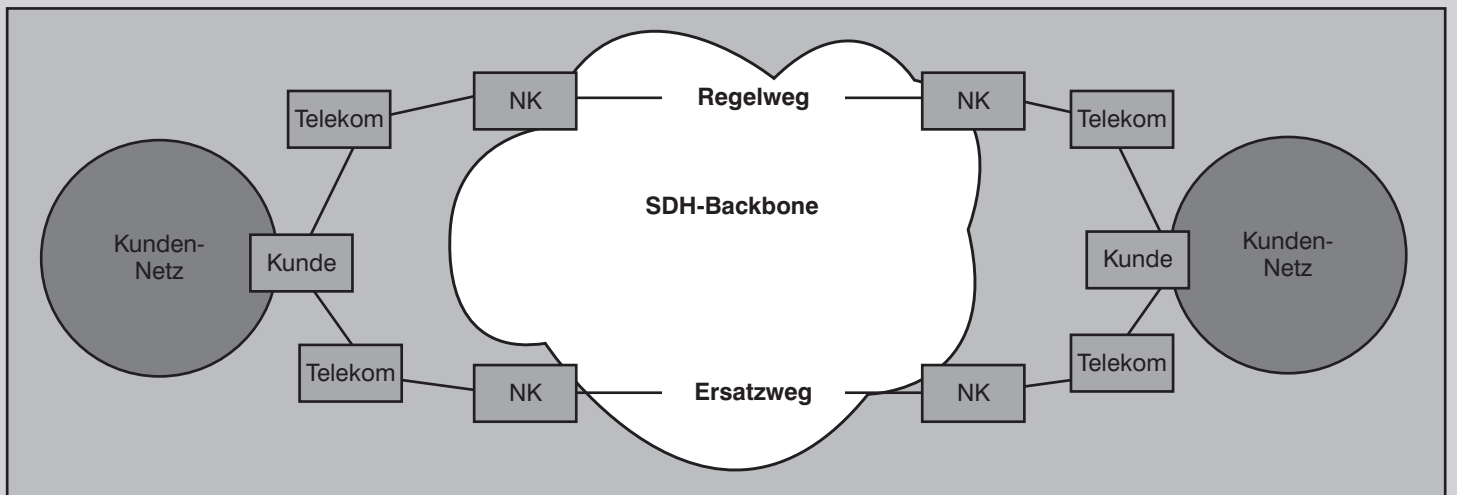


Abbildung 6: Prinzip HPS2

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 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 anstel-

le 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 sensibler 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
<b>Geschwindigkeitsvariante</b>	2,5 M	10 M	10 M	100 M	alle
<b>Metro-Bereich</b>	5 - 11	4 - 7	2 - 4	2	2
<b>Regio-Bereich (bis 200 km)</b>	7 - 13	6 - 9	4 - 6	4	4
<b>National</b>	12 - 18	11 - 14	9 - 10	9	9

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

## Kongress



### Kongress des Jahres 2008: Netzwerk-Redesign Forum

**14.04. - 17.04.08 in Königswinter**

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?
- 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 noch vom vergünstigten Frühbucherrabatt profitieren.

Moderation: Dr. Jürgen Suppan

Preis: inkl. Intensiv-Training € 1.990,-\* zzgl. MwSt. - ohne Intensiv-Training € 1.590,-\* zzgl. MwSt. (\*Preise gültig bis 31.12.2007)



Buchrn Sie über unsere Web-Seite [www.comconsult-akademie.de](http://www.comconsult-akademie.de)