



**University of
Zurich**^{UZH}

**Zurich Open Repository and
Archive**

University of Zurich
University Library
Strickhofstrasse 39
CH-8057 Zurich
www.zora.uzh.ch

Year: 2009

TuneInNet könnte den Datentransfer im Internet vereinfachen

Stiller, B

Posted at the Zurich Open Repository and Archive, University of Zurich

ZORA URL: <https://doi.org/10.5167/uzh-19499>

Journal Article

Originally published at:

Stiller, B (2009). TuneInNet könnte den Datentransfer im Internet vereinfachen. Bulletin SEV/VSE, (0905):13-16.

TunelnNet könnte den Datentransfer im Internet vereinfachen

Gesendet werden die Daten an alle, der Empfänger selektiert

Die verschiedenen Dienste im Internet auf der Basis von IP (Internetprotokoll) erreichen heute eine Vielfalt, die den Aufwand für den Datentransfer stark anwachsen lässt. TunelnNet ist eine Idee, diesen Aufwand im Netzwerk drastisch zu vereinfachen. Sie basiert auf der Annahme, dass die verfügbaren Bandbreiten im Backbone deutlich stärker wachsen als der hypothetisch aggregierte Bedarf an allen Endpunkten eines Netzes zusammen.

Das ursprüngliche Internet auf der Basis von IP der 70er-Jahre war als wissenschaftliches Netzwerk von Universitäten geplant und gebaut worden. Erst die Kommerzialisierung zu Beginn der 90er-Jahre – unter anderem getrieben durch das World Wide Web (WWW) im Jahr 1990 – hat das Internet zu einem allumfassenden Medium für den Datentransport gemacht. Dieses muss im neuen Jahrtausend dann auch sehr verschiedenen Anforderungen diverser multi-

Burkhard Stiller

medialer Applikationen und anderer Geschäftsanwendungen standhalten. Als technische Grundlage dieses Datenaustauschs ist es essenziell, dass die im Internet als Datengramme bezeichneten Daten – im Folgenden der Einfachheit halber «Pakete» genannt – den Weg vom Sender zum Empfänger finden. Wobei Sender wie auch Empfänger je ein Endpunkt im Netz darstellen. Da das Internet als robustes und ausfallsicheres Netzwerk konzipiert wurde, sind die einzelnen Router im Netz autonom darum besorgt, die den Paketen inhärenten Ziel- und Absenderadressen zu

analysieren und anhand dieser Angaben den Weg vom Sender zum Empfänger zu finden. Dies geschieht heute typischerweise nur auf der Grundlage möglicher Wege, aber keiner weiterer Parameter, wie zum Beispiel der verfügbaren Bandbreite oder gar der erreichbaren Verzögerungszeiten. Damit sind die Aufgaben der Router im Kern des wissenschaftlichen Problems auf die Wegewahl (Routing) und die Weiterleitung (Forwarding) beschränkt – natürlich neben den im produktiven Betrieb notwendigen Überwachungs- und Kontrollaufgaben.

Die Idee: TunelnNet
An dieser Stelle setzt TunelnNet an und schlägt einen einfacheren Mechanismus zum Datenaustausch in einem zukünftigen Internet vor: Die Pakete werden nicht mehr anhand der Wegewahlfunktion der Router dezidiert durch das Netz geleitet, sondern im Netzwerk breit verteilt (Bild 1). Dies macht die direkte Wegewahl überflüssig. Der Ansatz ähnelt dem «Wasserfluss auf offenem Gelände» oder dem «Directed Diffusion»-Ansatz. In gewisser Weise kann diese Verteilung (eben die Weiterleitung) der Pakete als ein Fluten angesehen werden, da jeder Knoten im Netz die Pakete erhält. Diese Pakete beinhalten nur wenige, verschlüsselte Zusatzinformationen (Etikette), die nur vom Empfänger korrekt interpretiert werden können – und nicht von anderen Knoten. Ferner werden Weiterleitungsentscheidungen in Netzknoten im Zusammenspiel mit Regeln (Policies) angewendet, um den Verkehr klein bzw. domänenspezifisch lokalisiert zu halten. Jedes Paket kann somit vom Empfänger an einem beliebigen Ort aus dem Netz herausgezogen werden, was ferner den Vorteil hat, dass der Mobilität der Benutzer keine Grenzen gesetzt sind und keine besonderen Protokolle für mobile Dienste notwendig sind. Um dies zu erreichen, können Pakete in Caches zwischengespeichert werden, wofür eine implizite Adressierung zwischen zwei vertrauenswürdigen Kommunikationspartnern notwendig ist. Daher verhindert dieser Ansatz auch traditionelle Denial-of-Service-(DoS)-Angriffe, da der Empfänger aktiv auf ein

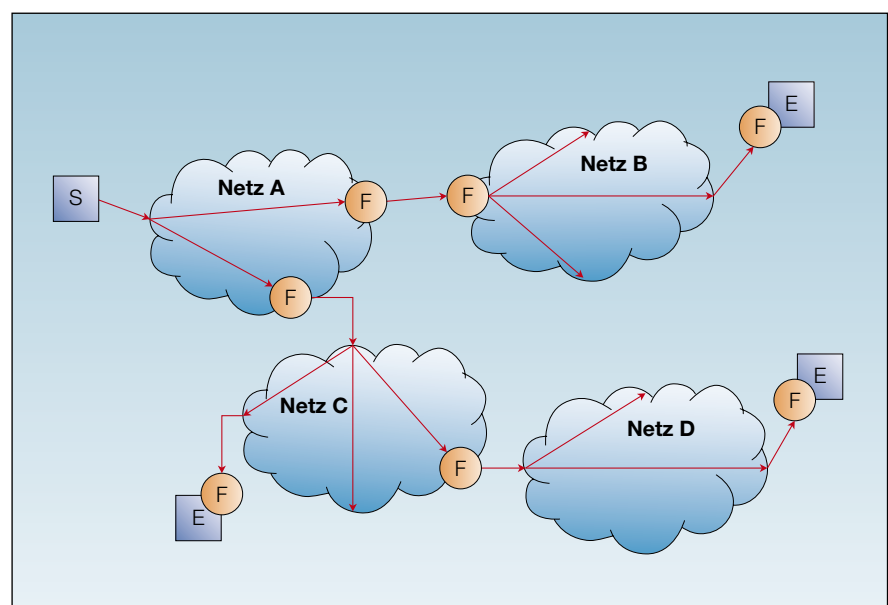


Bild 1 Funktionsweise des senderbasierten Flutens von Daten in Kommunikationsnetzen mit der Möglichkeit einer hierarchischen Filterung, basierend auf Download Clearing Codes (DCCs).

Paket zugreifen muss. Weitere Sicherheitsanforderungen, beispielsweise die Vertraulichkeit, können integral in TunnelNet erreicht werden, wenn die gesamten Paketinhalte – neben der obligatorischen Zusatzinformation – verschlüsselt werden. Dieses hat nur einen Zusatzaufwand zur Berechnung der Verschlüsselung in den beteiligten Endpunkten zur Folge.

Um grundsätzlich sicherzustellen, dass tatsächlich kein falscher Empfänger die Daten empfängt, müssen die Pakete in TunnelNet etikettiert werden. Diese Etiketten sind die verschlüsselten Zusatzinformationen (Download Clearing Code), die im Allgemeinen bei Kommunikationsprotokollen als Kontrollinformation bezeichnet werden und den Ziel- und Quelladressen zugeordnet sind. Als Grundlage dieser Verschlüsselungen und der sie ausführenden Algorithmen wird eine Schlüsselverwaltungsinfrastruktur (PKI, Public Key Infrastructure) [6] verwendet.

Natürlich ist bei TunnelNet und den soeben skizzierten Vorzügen auch ein Nachteil zu finden, der je nach Situation einmal stärker und einmal schwächer gewichtet werden kann. Die Datenvolumina werden im Netz steigen – speziell in einer aggregierten Form über das gesamte Netz und die Endpunkte hinweg betrachtet. Dieser Nachteil stellt jedoch in Zukunft kein unlösbares Problem dar, da (a) eine begründete Annahme der ständig wachsenden Backbone-Kapazität zukünftiger Netzwerke im Internet besteht [5] und (b) TunnelNet Massnahmen vorsieht, die Pakete in einem Netzknoten zwischen gekoppelten Netzwerken zu filtern. Die Konfiguration dieser Filter erlaubt es, ein unnötiges Weiterleiten zwischen zwei Netzdomänen zu vermeiden, oder schränkt dieses explizit ein. In einem solchen Fall können beide Netzwerkanbieter angepasste Filterregeln lokal aus ihrer Sicht heraus etablieren, was dem möglicherweise fehlenden Vertrauen zwischen den Providern untereinander Rechnung trägt.

Architektur

TunnelNet verändert somit auch die zugrundeliegende Architektur der Netzwerke positiv – sei es das Department-of-Defence-Model des Internets oder das ISO/OSI-Basisreferenzmodell (Bild 2). Diese Veränderung ist als Vereinfachung erkennbar, da einige der bis anhin bekannten Schichten aufgelöst und fast ersatzlos gestrichen werden können. Während im heutigen Netzwerk ebenso wie in einem TunnelNet die Schicht 1 für die Übertragung über das physikalische Medium verantwortlich (drahtgebunden oder drahtlos) und die Schicht 2a für den Netzwerkzu-

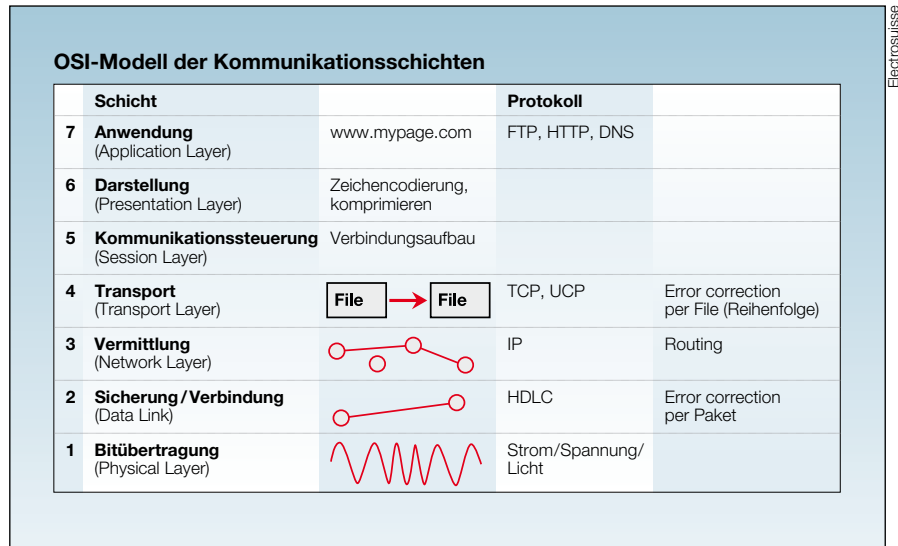


Bild 2 OSI-Schichtenmodell.

gang und deren Verteilung zuständig ist, braucht es für TunnelNet keine Schichten 2b bis 3 mehr. Die Netzwerktopologie besteht einzig aus Endpunkten und Netzknoten, wobei Letztere als Non-Forwarding Engines (NFE) bezeichnet werden, die die oben erwähnte Filterfunktion zwischen den traditionellen Subnetzen oder zwischen administrativen Domänen übernehmen.

Diese NFEs ersetzen die heutigen Router vollständig und fungieren damit als «brückenartige» Firewall, da neben dem Filtervorgang – basierend auf den Zusatzinformationen sowie den Adressen – nur noch bei Auswertung der vorliegenden Filterregeln eine einfache Paketweiterleitung oder eben keine Weiterleitung ermittelt wird. Diese Auswertungen erleichtern damit in der Folge die Aufgaben des Netzwerkmanagements [2], da einfachere Informationsmodelle, keine Routingtabellen und -protokolle sowie eine reduzierte Anzahl von Schichten erreicht werden.

Weiterleitungs- und Filtermechanismus

Alle Endpunkte sind innerhalb einer Domäne angesiedelt, die selber über mindestens einen NFE an das weltweite Netz angeschlossen sind. Die Endpunkte generieren dann beispielsweise einen Paketstrom wie bis anhin auch. Zu jedem dieser Pakete wird die Empfängerindividualisierung mindestens in Form des Download Clearing Codes hinzugegestellt, und dann wird beides in konkatenierter Form in das Netz versandt.¹⁾ Der erste NFE empfängt dieses Paket und entscheidet, ob das Paket an alle oder nur einige weitere interkonnek-

tierte NFEs weitergeleitet wird, jeweils auf der Basis der vorab definierten Filterregeln (Policies) des Anbieters. Diese Entscheidungen werden an jedem weiteren NFE für jedes Paket in gleicher Form wiederholt, jeweils aufgrund der lokal vorliegenden Regeln.

Der Look-up-Mechanismus des Endpunktes erlaubt dann einem beliebigen Empfänger, die Pakete, die für ihn vorgesehen sind (anhand des im Paket enthaltenen Download Clearing Codes eindeutig erkennbar), aufzunehmen – entweder im laufenden Verkehr oder aber aus einem Cache, falls der Empfänger gerade beim Vorbeiziehen des Pakets nicht aktiv gewesen sein sollte. Dieser Look-up-Mechanismus ist somit als eine am Empfänger angewendete Filterregel anzusehen.

Nach dem gleichen Prinzip können NFEs diverse weitere Filterregeln anwenden, um das vollständige Fluten von Domänen oder von deren Teilbereichen einzuschränken bzw. gänzlich zu unterbinden. Dieses wird technologisch auf Basis von heute bekannten Policy-basierten Netzwerk-Management-Methoden und -Systemen geschehen. Hierbei können ferner die Filterregeln für alle NFEs einer Domäne identisch, topologiespezifisch oder gemäss vorliegender Interkonnektionsvereinbarungen und benötigter Anbietervorgaben individuell konfiguriert werden.

In Bezug auf eine Anwendung von TunnelNet und seinen Mechanismen ist anzuführen, dass es in einer Migration eingesetzt werden kann, da es Teilomänen geben wird, die voneinander unabhängig, aber parallel laufend traditionell oder TunnelNet-basiert arbeiten können. NFE-zu-Router-Gateways sorgen dann für ein ein-

faches Ab- oder Überstreifen der Etiketten, welches im Kern einem MPLS-Border-Router (Multi-Protocol Label Switching) ähnelt, der MPLS-Label für den Transport von IP-Daten hinzufügt bzw. abstreift.

Annahmen

TunelnNet ist aufgrund der obigen Beschreibung algorithmisch und protokoll-technisch realisierbar, da die notwendige Architektur, die angepassten Protokolle und die Paketformate bekannt sind. Damit ist TunelnNet auch praktisch anwendbar, wenn vier Annahmen zutreffen, die im Folgenden diskutiert werden. Diese Diskussion zeigt im Besonderen auch, dass die Annahmen in einem überschaubaren Zeithorizont erreicht werden können.

Erste Annahme: Grosse Bandbreiten sind verfügbar, weiter wachsende Bandbreiten sind angekündigt und technologisch praktikabel. Die Bandbreiten in den Backbone-Netzen der Anbieter übersteigen um ein Vielfaches die aggregierten Kapazitäten der Endpunkte. Durch die optischen Übertragungsmedien auf Schicht 1 stehen Broadcaster und Repeater im Tbit/s-Bereich vor der Einführung. Generell unterliegen die Bandbreitenentwicklungen einer ungefähren Verdoppelung alle 9 Monate [5]. Basierend auf diesen Technologien sind ferner die Kosten für die Kanäle auf der Schicht 1 sehr günstig, während die Kosten von Routern auf Schicht 3 stetig aufgrund deren Komplexität steigen und zusätzliche, bei günstigeren Modellen potenzielle Flaschenhälse für die Paketweiterleitung darstellen können.

Zweite Annahme: In wenigen Zwischenknoten sind grosse Caches ebenso wie höhere Verarbeitungsleistungen möglich. Zwischenpuffer für Kontroll- und Steuerdaten sind im Bereich von mindestens einigen Gigabit pro Knoten verfügbar, noch wachsend und kostengünstig [4]. D.h., verbunden mit wenigen NFEs in einer Topologie gekoppelter Teilnetze, sind die Aufgaben dieser NFEs selber auch auf einfache Berechnungsaufgaben (Filter) reduziert. Weiterhin sind damit auch ausreichend hohe Verarbeitungsleistungen (CPU) – im Speziellen für die Verschlüsselungen, mindestens jedoch der Etikette – zu erreichen.

Dritte Annahme: Schlüsselverwaltungen auf der Basis einer PKI sind realisiert. Diese Art der Infrastruktur einer Sicherheitsunterstützung hat deutlich an Bedeutung und in der Anzahl existierender Installationen und deren Anwendung zugenommen [6]. Auch ist der Einsatz in anderen kommerziellen Bereichen stark, d.h., ein Synergieeffekt aus dem Einsatz mittels TunelnNet im Netzwerkbereich ist zu erwarten. Allerdings

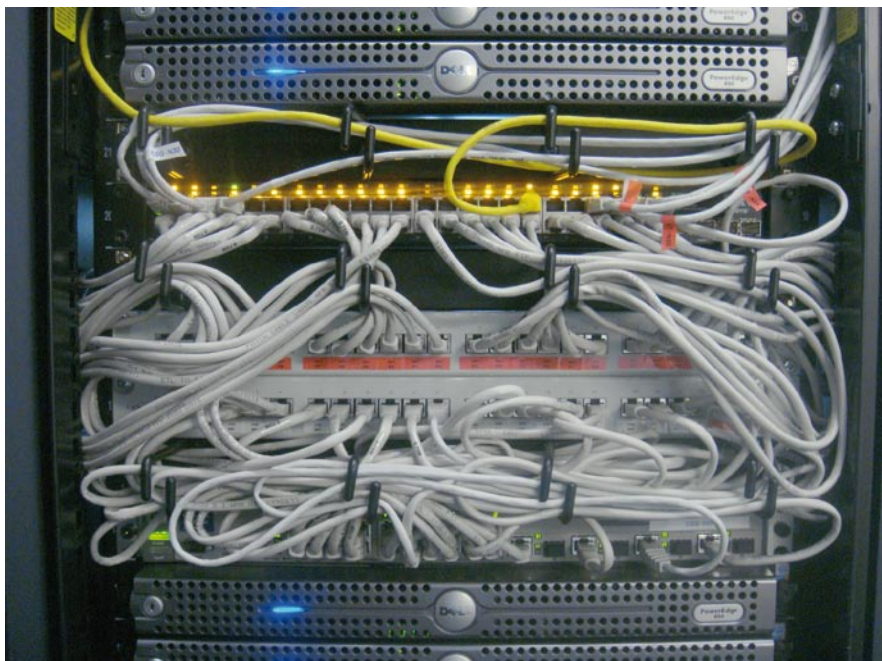


Bild 3 Ethernet-basierte Netzwerkinfrastruktur.

müssen in dieser Situation Gruppenschlüssel ebenso verwaltbar sein, und das Vorhandensein von Gruppenadressen muss sichergestellt werden können.

Vierte Annahme: Extensive Applikationsanzahlen und Overlay-Netzwerke sind für die nahe Zukunft sicher zu erwarten. Wenn davon ausgegangen wird, dass alle der weltweit ca. 10 000 TV-Stationen und ca. 100 000 Radiostationen kontinuierlich das Netzwerk mit ihren Datenströmen füllen, dann ist mit einem grossen Datenvolumen zu rechnen. Zusätzlich ist der Verkehr aus Overlay-Netzwerken signifikant und im Steigen begriffen [1]. Dieses steigende Volumen wird aber ungleich weniger dramatische Auswirkungen in einem TunelnNet haben, da die Empfänger sich einfach in die weitergeleiteten Paketflüsse einklinken können und Multicast-Eigenschaften vorhanden sein werden. Hier ergeben sich für Sender wie auch Empfänger sowie Netzwerkanbieter ökonomisch positive Anreize [7].

Simulation des Netzes

Auf der Basis dieser technischen Grundlagen für TunelnNet ist ein kleines Simulationsmodell untersucht worden, welches die Validierung der Konsequenzen dieses Ansatzes auf der Basis obiger Annahmen in einem Worst-Case-Szenario – also einer Abschätzung einer oberen Schranke für den Gesamtaufwand – erlaubt.

Die Verwendung eines Topologiegenerators scheint wegen der vielfältigen Netz-

werktopologien in heutigen Netzen angebracht, um keine «vorbelastete» Topologie zu verwenden. Ferner können die Anzahl der Transitdomänen, die den Backbone definieren, ebenso wie die mittlere Anzahl von Zugriffsnetzwerken und die mittlere Anzahl von Endpunkten in diesen parametrisiert werden. Die Verkehrsflussdaten wurden (a) in einem konventionellen Routing-Modus sowie (b) mittels eines einfachen Tune-in-Net-Modus behandelt. Schliesslich sind die Paketgrösse, die Ankunftsdaten auf der Basis einer Zipf-Verteilung und die Senderate pro Endpunkt in dieser Topologie parametrisierbar.

Für eine zufällig generierte Topologie mit 3 Transitdomänen, einer mittleren Anzahl von 3 Hops in jeder von dieser und einer mittleren Anzahl von 6 Zugriffsnetzwerken je Transitdomäne wurden im Mittel 7 Endpunkte je Zugriffsnetz generiert. Dieses resultierte in einem Gesamtnetz mit 645 Knoten. Auf diese Topologie wurden 150 Byte grosse Pakete in einer zufälligen Gleichverteilung pro Knoten und pro Sekunde aufgebracht.

Nach einer Simulationszeit von 60 s wurde das Resultat im Fall (a) des traditionellen Routings mit (b), dem Resultat des einfachsten TunelnNet-basierten Verfahrens (Fluten ohne Beschränkungen), verglichen. In beiden Fällen sind 38 634 Look-ups (also Lesevorgänge der Empfänger) durchgeführt worden, von welchen in (a) 37 901 Look-ups (98%) und in (b) 38 352 Look-ups (99%) erfolgreich waren. Diese Zahlen zeigen, dass beide Verfahren – Routing und NFE-

Paketweiterleitung – in Bezug auf die Zuverlässigkeit des Erreichens des Empfängers vergleichbar sind. Wie erwartet, sieht es hingegen in Bezug auf die ausgetauschten Daten anders aus. Während im Fall von (a) 301 404 Pakete verschickt wurden (oder $45 \cdot 10^6$ Byte), sind es im Falle von (b) 58 988 526 Pakete oder $8,8 \cdot 10^9$ Byte, jeweils in dem über das gesamte Netzwerk hinweg aggregierten Volumen.

Damit benötigt TunelnNet in diesem einfachen, aber den Worst Case beschreibenden Umfeld ca. den 100-fachen Bandbreitenbedarf, wobei in diesem Fall keinerlei NFEs mit Filtern eingesetzt worden sind, die das Datenvolumen deutlich reduzieren würden – natürlich abhängig von den expliziten Kommunikationsbeziehungen im Netz. Dennoch liegt dieses Resultat keinesfalls um Grössenordnungen neben den initial erwartbaren Ergebnissen! Eben aufgrund der oben erwähnten Annahme, dass sich die Bandbreite im Backbone alle 9 Monate verdoppelt, wird in gut 5 Jahren der Faktor von 100 erreicht sein. Ferner hat die Einführung von WDM (Wavelength Division Multiplexing) gezeigt, dass mit einem einzigen Technologieschritt auf einem Lichtwellenleiter die 100-fache Kapazität erzielt werden kann. Damit ist das Risiko in Bezug auf nicht bearbeitbar grosse Datenvolumina in Backbone-Netzen klein. Ferner sind von den heute gut 40 000 registrierten Autonomous Systems (AS) [3] nur wenige reine Transitdomänen, d.h., dass die Verwendung eines einfachen Time-to-Live-(TTL)-Feldes in den Zusatzinformationen der Pakete und deren Testen an Domänengrenzen durch die NFEs möglicherweise zirkulierende Pakete abfangen kann. Dieses führt zu einer Reduktion des aggregierten Verkehrs, was in den oben skizzierten Ergebnissen ebenfalls noch nicht einbezogen wurde.

Zusätzlich ist ein Vergleich der Routingkosten zwischen traditionellen Netzen und einem TunelnNet angebracht: Während heute ein Backbone-Router-Port zwischen 25 000 und 180 000 CHF kostet, werden je nach Grösse des Netzes davon Dutzende bis viele Hundert benötigt – zusätzlich zu den Betriebs- und Wartungskosten. Für TunelnNet fallen mindestens diese Portkosten vollständig weg.

Schliesslich ist es angebracht, auf die zu erwartenden Verzögerungszeiten im Ende-zu-Ende-Fall zu achten, die neben den Laufzeiten an sich unter anderem durch die Verschlüsselung auftreten können. Diese Zeiten sind in traditionellen Netzen natürlich vom Routingverfahren unabhängig, da die Routingtabellen vorab bzw. dynamisch erstellt werden (den Fehlerfall einmal ausser Acht lassend). Der Zeitbedarf für die reinen Weiterleitungen eines sehr guten Back-

bone-Routers liegen bei ca. 10 ns je Paket, die in einem NFE auf der Schicht 1 auch erreicht werden. Da die Schicht 3 nicht mehr im Protokollturm enthalten sein muss, bleibt zum Ver- und Entschlüsseln genügend Zeit. Damit stellt ein TunelnNet-Knoten keinen Engpass in dieser Situation dar.

Schlussfolgerungen

Die Bedeutung des Datentransfers im Internet hat in der Gesellschaft heute eine derart grosse Bedeutung erlangt, wie es das Wasser für Pflanzen hat: Ohne das Internet kann die Wirtschaft faktisch nicht mehr überleben. Dieses heisst im Umkehrschluss, dass die Robustheit, die Sicherheit, die Dienstgüte (QoS) und die Fehlertoleranz eines zukünftigen Netzes ebenso behutsam wie deutlich verbessert werden müssen, wie ein Anwender die Optimierung der reinen Nutzdatenübertragung erwartet. Wenn im gleichen Zug einer Evolution – oder einer Weiterentwicklung mit revolutionären Zügen – auch die Komplexität der netzwerkinhärenten Netzknoten verkleinert werden kann bzw. ganz wegfällt, wie im TunelnNet-Ansatz vorgeschlagen, dann gewinnen die Benutzer durch verbesserte Dienstleistungen (zumindest in Form einer kostengünstigeren Alternative) und die Netzwerkdienstanbieter durch reduzierte Betriebskosten sowie reduzierten Wartungsaufwand. Damit ist TunelnNet auch technologisch effizienter als heutige Wegehahlverfahren in und für IP, einfach anwendbar, migrierbar und ökonomisch effizienter durch eben diesen vereinfachenden Technologieeinsatz.

Natürlich ist es noch ein weiter Weg, bis ein Internet der Zukunft in dieser Form vom TunelnNet-Ansatz im Grossen realisiert werden wird, aber die ersten Simulationen des Worst Case und deren Untersuchungen zeigen plausibel, dass dem Ansatz technisch keine expliziten Hinderungsgründe im Wege stehen. Die zu erwartenden Einsparungen an Aufwand und Kosten bieten ein auszuschoöpfendes Potenzial für

Optimierungen, während gleichzeitig sowohl gewohnte Dienste unverändert angeboten als auch neue Dienste einfacher und mit besseren Kennzahlen in das Portfolio der Anbieter aufgenommen werden können.

Referenzen

- [1] Cisco Systems: Cisco Visual Networking Index – Forecast and Methodology, 2007–2012, June 2008.
- [2] Emanics (European Network of Excellence for the Management of Internet Technologies and Complex Services), EU Projekt Nr. FP6-2004-IST-026854; <http://www.emanics.org>, März 2009.
- [3] G. Huston: Exploring Autonomous System Numbers, The Internet Protocol Journal, Vol. 9, Nr. 1, März 2006.
- [4] G. E. Moore: Cramming More Components onto Integrated Circuits, Electronics, Vol. 38, Nr. 8, April 1965.
- [5] J. Nielsen: Nielsen's Law of Internet Bandwidth; <http://www.useit.com/alertbox/980405.html>, April 1998.
- [6] Schweizerische Akkreditierungsstelle (SAS): Public Key Infrastructure (PKI); <http://www.seco.admin.ch/sas/00229/00251/index.html?lang=de>, September 2008.
- [7] SmoothIT (Simple Economic Management Approaches of Overlay Traffic in Heterogeneous Internet Topologies), EU Projekt Nr. FP7-2008-ICT-216259; <http://www.smoothit.org>, März 2009.

Angaben zum Autor

Prof. Dr. **Burkhard Stiller** ist seit September 2004 an der Universität Zürich in der Lehre und Forschung über Kommunikationssysteme, ihre Technologien und ihre ökonomischen Eigenschaften sowie Perspektiven tätig. Sein wissenschaftlicher Hintergrund liegt in der Informatik und die früheren Orte seiner Tätigkeiten umfassten die Universität Karlsruhe, die University of Cambridge, U.K., die ETH Zürich und die Universität der Bundeswehr München. Der Ansatz TunelnNet entstand aus gemeinsamen Überlegungen und Arbeiten mit den Professoren Georg Carle, jetzt Technische Universität München, Jochen Schiller, Freie Universität Berlin, und Andreas Schrader, Universität Lübeck. Der Autor dankt auch den FP7-EU-Projekten Smooth-IT sowie Emanics für die Unterstützung.

Universität Zürich, Institut für Informatik,
8050 Zürich, stiller@ifi.uzh.ch

¹⁾ Konkateniert bedeutet hier, dass die Informationen an der richtigen Stelle an das Paket angehängt werden.

Résumé

TunelnNet pourrait simplifier le transfert de données sur internet

Les données sont envoyées à tous, le destinataire fait la sélection. Les différents services à base IP (internet protocol) sur internet ont maintenant atteint une telle variété que l'effort de transfert de données augmente considérablement. TunelnNet est une idée destinée à simplifier radicalement le travail nécessaire sur le réseau. L'idée est basée sur l'hypothèse que les bandes passantes disponibles augmentent beaucoup plus fortement sur le réseau de base que le besoin hypothétiquement accumulé aux points terminaux d'un réseau.