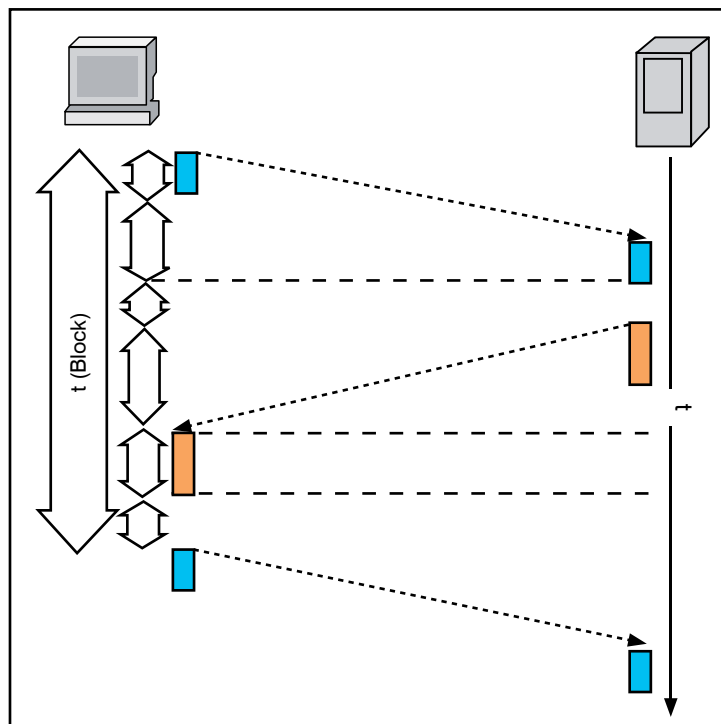


Wie viel Delay ist tolerierbar?

von Dr. Behrooz Moayeri



Seit einigen Monaten macht im Zusammenhang mit der Bewertung von LAN-Komponenten ein neuer Ausdruck die Runden: Ultra-Low Latency (ULL). Switch-Hersteller stufen ihre neuen Produkte gerne als ULL-Komponenten ein. Von Sub-Microsecond Latency ist die Rede. Nicht nur der einzelne Switch, sondern auch das Netzdesign soll auf ULL ausgerichtet werden.

Daher werben die Hersteller für vermaschte Konstrukte als Ablösung der klassischen Hierarchien im RZ. Auf der anderen Seite gibt es Veröffentlichungen zum Locator/ID Separation Protocol, das u. a. helfen soll, die Latenz beim Zugriff auf Ressourcen in einer auf verschiedene Data-Center-Lokationen verteilten Cloud zu minimieren¹. Wie sind diese neuen Verfahren und Konzepte einzustufen? Wie viel Delay ist tolerierbar? Der vorliegende

Beitrag geht diesen Fragen nach. Zunächst wird auf die Delay-Minimierung innerhalb der Rechenzentren eingegangen. Im zweiten Teil folgt die Betrachtung der Delay-Minimierung außerhalb der Rechenzentren, d. h. beim Zugriff der Clients auf Server.

weiter auf nächster Seite

Schwerpunkthema

Wie viel Delay ist tolerierbar?

Fortsetzung von Seite 1



Dr. Behrooz Moayeri ist bei der ComConsult Beratung und Planung GmbH als Mitglied der Geschäftsleitung tätig. Er hat in den letzten Jahren unter anderem viele Unternehmen zu Themen der RZ-Vernetzung beraten.

Was ist ULL?

Ultra-Low Latency ist ein Begriff, der ursprünglich aus dem Bereich Optical Networking kommt. In diesem Zusammenhang geht es darum, dass optische Komponenten wie Wellenlängenmultiplexer möglichst wenig Delay in den Signalpfad einfügen. In letzter Zeit wurde der Begriff von der Ethernet-Industrie übernommen. Dabei ist von „Sub-Microsecond Latency“ die Rede, das heißt die Switches sollen weniger als eine Mikrosekunde Delay bei der Übertragung jedes Paketes verursachen.

Unklar ist, welche Latency-Definition dabei gilt. Es gibt nämlich vier denkbare, die in der Abbildung 1 dargestellt sind. Je nach Wahl des Messverfahrens ergeben sich unterschiedliche Werte, die miteinander nicht vergleichbar sind. Für die Anwendungen ist die LILO-Latenz entscheidend, denn damit wird gemessen, um welche Zeit das letzte Bit des Paketes (das letztlich für den vollständigen Empfang des Paketes entscheidend ist) durch den Switch verzögert wird. Die LILO-Latenz ist nur gleich der FIFO-Latenz, wenn die Bitraten von Input und Output gleich

sind. Für den Vergleich zwischen zwei Switches, die im Modus Store & Forward arbeiten, sollte der LIFO-Wert herangezogen werden. Nicht sinnvoll ist die Betrachtung der FILO-Latenz.

Was können Switch-Hersteller tun, um Delays zu minimieren? Sie können Switch-Architekturen entwerfen, in denen die Pakete im Switch minimal verzögert werden. Wo entstehen im Switch die längsten Latenzzeiten? Sie entstehen nicht hauptsächlich auf den wenige Zentimeter oder Dezimeter langen Pfaden im Switch, sondern vor allem in den Zwischenspeichern (Puffern). Das Ziel sollte also sein, dass die Pakete nur minimale Zeit in den Puffern verweilen, auch wenn der Puffer groß dimensioniert sein sollte.

Aber es gibt noch eine Einflussgröße, und das ist der Switching-Modus.

Déjà-vu-Erlebnis

Diejenigen, die länger als 15 Jahre mit Lokalen Netzen zu tun haben, bekommen beim Verfolgen der ULL-Diskussion ein Déjà-vu-Erlebnis. In der ersten Hälfte des 1990er Jahrzehnts, also den An-

fängen der LAN-Switch-Technik, war eine Diskussion um das schnellste Switching-Verfahren ausgebrochen. Kalpana, einer der ersten LAN-Switch-Hersteller, der später von Cisco Systems übernommen wurde, brachte Switches auf den Markt, die eine Weiterleitung im Cut-Through-Modus unterstützten. Bei diesem Modus beginnt der Switch mit der Übertragung am Ausgangsport, ohne auf das letzte am Eingangsport empfangene Bit eines Frames zu warten. Im Gegensatz dazu wartet ein im Modus Store & Forward arbeitender Switch immer auf das letzte am Eingangsport empfangene Bit eines Paketes, bevor er das Paket am Ausgangsport weiter leitet. Der Geschwindigkeitsvorteil des Cut-Through-Modus ist einleuchtend (siehe Abbildung 2). Damals arbeiteten die Switches an allen Ports mit 10 Mbit/s. Bei einem Paket der Länge von ca. 1.500 Bytes lag der Geschwindigkeitsvorteil des Cut-Through-Modus in der Größenordnung einer Millisekunde. Eine Millisekunde entsprach und entspricht ungefähr einer zusätzlichen Kabellänge von 200 km. Bei fünf kaskadierten Switches (in einer typischen Hierarchie Access, Distribution, Core, Distribution, Access) käme dann der Gegenwert eines Kabelwegs von 1000 km zusammen, für die meisten Anwendungen auch auf der Ebene der Benutzerwahrnehmung relevant.

Der Cut-Through-Modus erledigte sich aber relativ schnell, nachdem 1995 der Fast-Ethernet-Standard vom Institute of Electrical and Electronic Engineers (IEEE) verabschiedet worden war und die ersten Switches mit Uplinks auf den Markt kamen, die 100 Mbit/s unterstützten. Wenn nämlich ein Frame an einem Port mit 10 Mbit/s empfangen wird, kann an einem mit 100 Mbit/s arbeitenden Zielport nicht mit der Weiterleitung begonnen werden, solange das letzte Bit des Pakets nicht vom Switch empfangen worden ist, denn

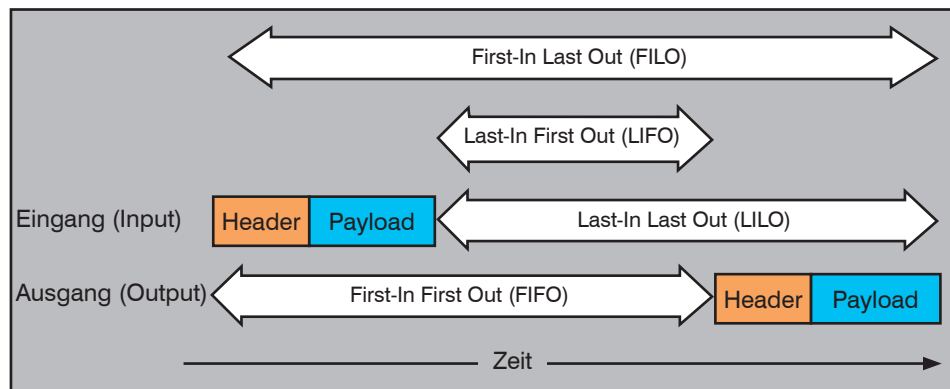


Abbildung 1: Verschiedene Verfahren der Latenzmessung

¹Beispiel: ComConsult Study.tv, LISP-Seminar, <http://www.comconsult-study.tv/de/LISP::1553:1314.html>

Wie viel Delay ist tolerierbar?

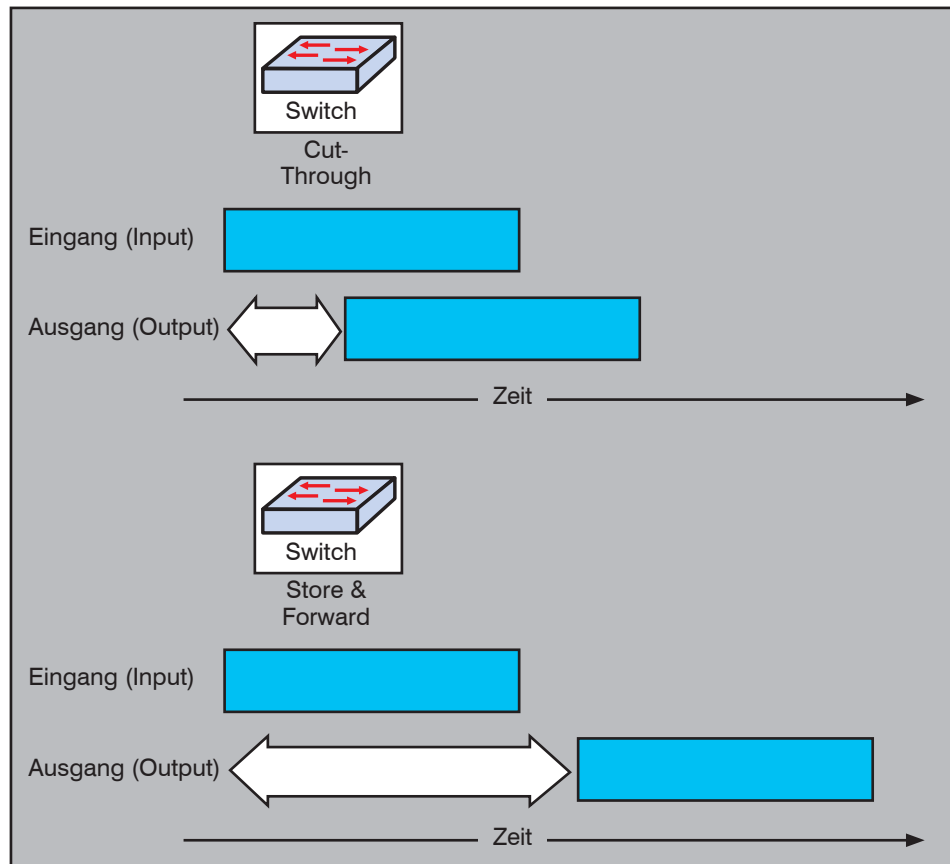


Abbildung 2: Cut-Through- versus Store&Forward-Modus

gen in Adresstabellen und anderen Verarbeitungsschritten im Switch erforderlich ist, lassen sich die theoretischen Minima der Switch-FIFO-Latenzen bei Switches, die durchgängig mit 10Gigabit Ethernet Ports ausgestattet sind, gemäß der Tabelle 1 ausrechnen (die FIFO-Latenz wäre aufgrund der einheitlichen Bitraten der Ports auch gleich der LIFO-Latenz). Das sind auch die für die Applikationen wirksamen Latenzen.

Pro Switch sind je nach Frame-Länge bis über 6 Mikrosekunden (genauer: 7,373 μ s minus 1,0 μ s, also 6,373 μ s, ungefähr 6,4 μ s) Unterschied zwischen den beiden Modi Cut-Through und Store & Forward anzunehmen. Eine Mikrosekunde entspricht einem Kabelweg von 200 m. Bei fünf kaskadierten Switches berechnet sich daher der maximale latenzbezogene Nachteil von Store & Forward wie folgt:

$$\text{Maximum_Delta (Cut-Through; Store \& Forward)} = 5 \times 6,4 \mu\text{s} = 32 \mu\text{s} \triangleq 6.400 \text{ m}$$

Der Latenzunterschied, der 6.400 m Kabelweg entspricht, ist ungefähr mit dem Unterschied vergleichbar, der sich ergäbe, wenn man die Systeme eines Data Centers auf zwei Lokationen an den beiden Endes eines großen Campus verteilte.

bekanntlich kostet aufgrund der unterschiedlichen Bitraten der beiden Ports das Senden des Paketes nur 10 % der Zeit, die für den Empfang erforderlich ist. Da das Paket am Stück gesendet werden muss, ist das Ende des empfangenen Pakets abzuwarten. Der Geschwindigkeitsvorteil des Cut-Through-Modus fällt dann nicht mehr so deutlich aus. (siehe Abbildung 3)

Die Lokalen Netze wurden von 1995 an in der Regel nach einem hierarchischen Konzept aufgebaut, bei dem die Uplinks normalerweise mit einer höheren Bitrate arbeiten als die Downlinks.

So kam es, dass der Cut-Through-Modus nach 1995 langsam in die Vergessenheit geriet, bis der Begriff in letzter Zeit wieder aufgetaucht ist.

ULL: wer braucht das?

Der neue Zusammenhang, in dem wieder vom Cut-Through-Modus die Rede ist, heißt Ultra-Low Latency (ULL). Der Anspruch ist, die Latenz von Switches in den Bereich von „Sub-Microsecond“ zu drücken. Geht man von einem Switch mit einer Mindestverarbeitungszeit von einer Mikrosekunde für die Weiterleitung eines Frames aus, die allein für das Nachschla-

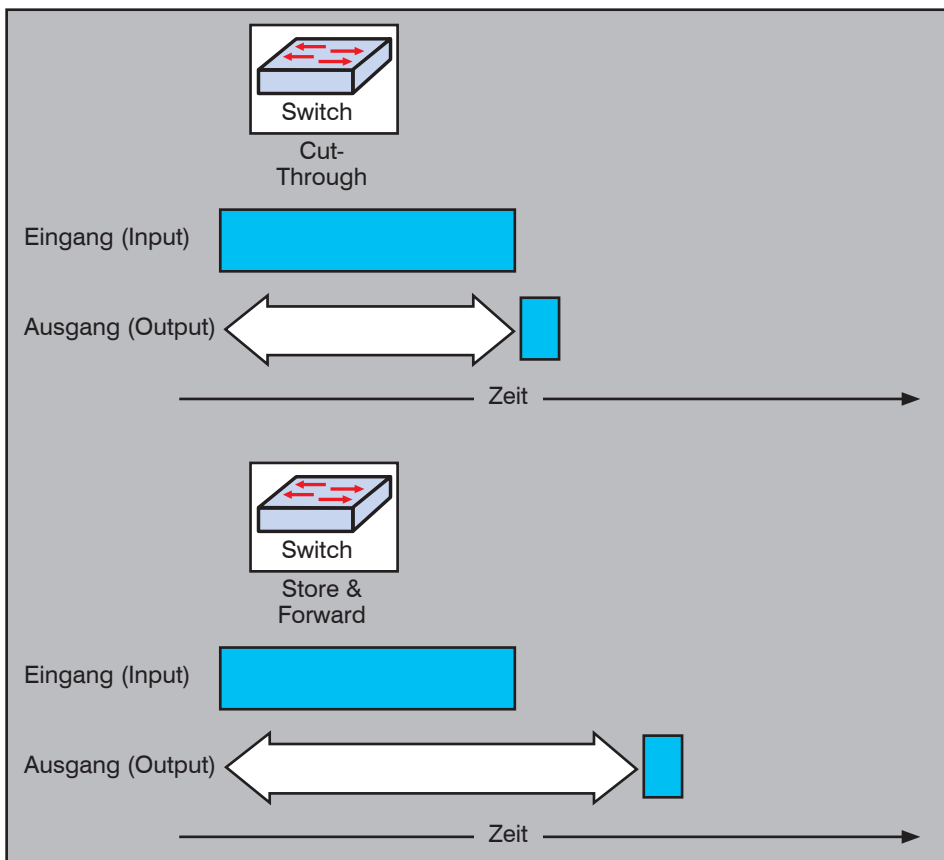


Abbildung 3: Cut-Through- versus Store&Forward-Modus bei unterschiedlichen Bitraten der Ports

Wie viel Delay ist tolerierbar?

Länge in Bytes	Länge in Bits	Mindest-FIFO/LILO-Latenz in Nanosekunden	
		Cut-Through	Store & Forward
72	576	1.000	1.000
144	1152	1.000	1.000
288	2304	1.000	1.000
576	4608	1.000	1.000
1152	9216	1.000	1.000
2304	18432	1.000	1.843
4608	36864	1.000	3.686
9216	73728	1.000	7.373

Tabelle 1: Vergleich der Mindestlatenzwerte bei Cut-Through und Store & Forward

Ist das überhaupt relevant? Müssen nicht alle rechenzentrumsinternen Datenströme Entfernungen tolerieren, die sogar weit über die Campusausdehnungen hinausgehen? Hinsichtlich Disaster Recovery würden zwei Data Center auf einem Campus nicht alle Szenarien abdecken, wenn man an solche Ereignisse wie Erdbeben, Tsunami, lang anhaltenden Stromausfall, Flugzeugabsturz, Hochwasser oder terroristische Anschläge denkt. Viele Unternehmen und Organisationen erheben den Anspruch, solche Ereignisse zu überleben und innerhalb sehr kurzer Zeit danach wieder arbeitsfähig zu sein. Die RZ-Betreiber sind in solchen Fällen gut beraten, zentrale IT-Ressourcen auf Lokationen zu verteilen, die auch bei größten anzunehmenden Unfällen (so etwa bei einem solchen Ereignis wie der März-Katastrophe in Japan) nicht gleichzeitig betroffen wären.

Nun kann man natürlich zwischen Disaster Recovery und dem normalen RZ-Betrieb unterscheiden. Im ersten Fall kann zum Beispiel der Anspruch „Business Continuity“ dahin gehend präzisiert werden, dass man nach der Katastrophe schnell wieder arbeitsfähig wird, aber nicht ganz ohne Datenverlust. In einem solchen Fall könnte es zum Beispiel reichen, dass eine Organisation mit Daten weiter arbeitet, die wenige Stunden vor dem Schadensfall gesichert worden sind, zum Beispiel mittels Snapshots von einem RZ auf eine andere Data-Center-Lokation ein paar hundert Kilometer weiter.

Dieselbe Organisation kann jedoch eine RZ-Infrastruktur konzipieren, die im Normalfall auf einen Campus oder sogar ein Gebäude konzentriert ist. In diesem Fall gäbe es natürlich einen signifikanten Latenzunterschied zwischen einem Netz auf der Basis von Cut-Through-Switches und einem Netz, das aus Store&Forward-Switches besteht. Die Größenordnung des Unterschieds liegt schlimmstenfalls im zweistelligen Mikrosekundenbereich.

Eine andere Frage ist, ob sich selbst solche großen Latenzunterschiede auf der Ebene der Anwendungen spürbar auswirken.

Wann wirken sich Mikrosekunden aus?

Das Zeitdiagramm einer typischen Client-Server-Applikation ist in der Abbildung 4 dargestellt.

Wenn man eine Transaktion auf der Anwendungsebene (zum Beispiel eine Datenbanktransaktion) als Folge von n Request-Response-Paaren modelliert, ergibt sich für die Dauer der Transaktion die Formel 1.

Dabei bedeuten:

- t (Transaktion): Dauer der Transaktion insgesamt, bestehend aus n Request-Response-Paaren
- t (Request_i): Dauer der Übertragung des Request-Blocks i auf dem langsamsten Übertragungssegment des Ende-zu-Ende-Pfades
- t (Latency1_i): Netz-Latency des Request-Blocks i
- t (Server_i): Server-Latency nach dem Request-Block i
- t (Latency2_i): Netz-Latency des Response-Blocks i

$$t(\text{Transaktion}) = \sum_{i=1}^{i=n} t(\text{Request}_i) + \sum_{i=1}^{i=n} t(\text{Latency1}_i) + \sum_{i=1}^{i=n} t(\text{Server}_i) + \sum_{i=1}^{i=n} t(\text{Latency2}_i) + \sum_{i=1}^{i=n} t(\text{Response}_i) + \sum_{i=1}^{i=n} t(\text{Client}_i)$$

Formel 1: Dauer der Transaktion

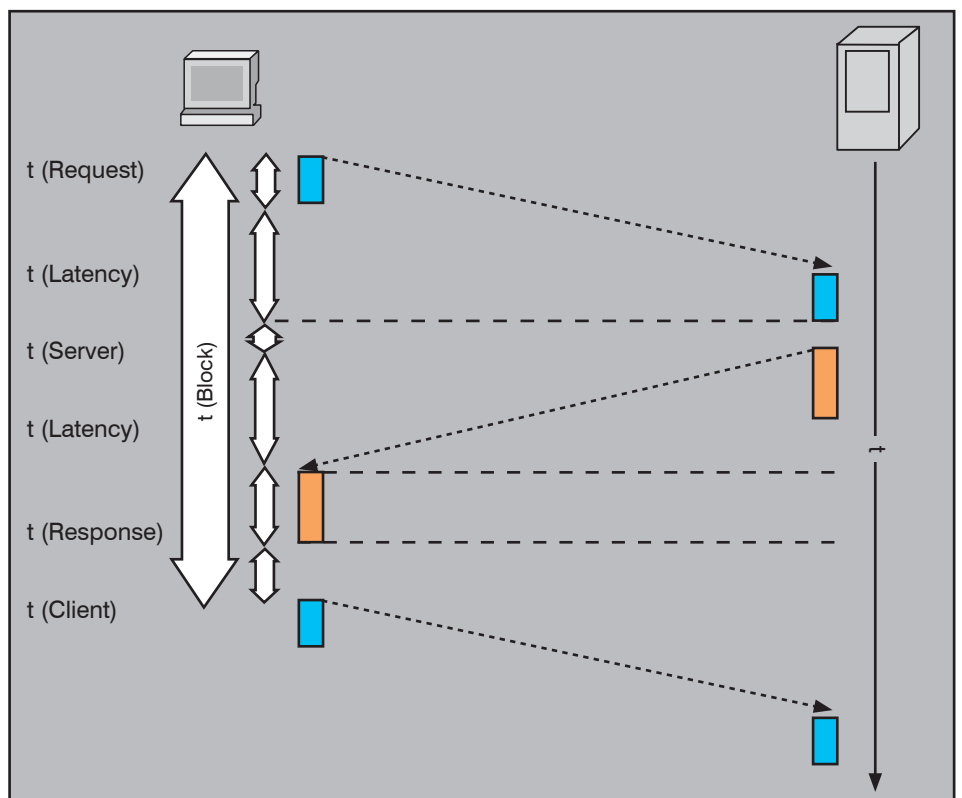


Abbildung 4: Zeit-Diagramm einer Client-Server-Applikation

Wie viel Delay ist tolerierbar?

- t (Response_i): Dauer der Übertragung des Response-Blocks i
- t (Client_i): Client-Latency nach vor dem Request-Block ($i+1$)

Mit entscheidend ist dabei die Blockgröße. Dies ist die Länge der Sequenz, die pro Richtung übertragen werden kann, ohne dass auf eine Bestätigung in entgegengesetzter Richtung gewartet werden muss.

Für die weitere Berechnung treffen wir folgende Vereinfachungen:

- Alle Request-Response-Paare einer Transaktion weisen gleiche Latenzwerte aller Komponenten auf.
- Die Netzlatenz ist in beiden Richtungen gleich.
- Die Blockgröße ist so klein, dass ein Block an einem Stück übertragen werden kann, ohne auf eine Bestätigung warten zu müssen (das entspricht der obigen Definition von „Block“).

Somit bekommen wir die einfachere Formel, in der RTT für Round Trip Time steht:

$$[t \text{ (Transaktion)} = n \times (t \text{ (Request)} + \text{RTT} + t \text{ (Response)} + t \text{ (Server)} + t \text{ (Client)})]$$

t (Request) und t (Response) sind wie folgt zu berechnen:

$$t \text{ (Request)} = \text{Länge des Request-Blocks} / \text{Bitrate}$$

$$t \text{ (Response)} = \text{Länge des Response-Blocks} / \text{Bitrate}$$

Wenn man für die Summe aus t (Request) und t (Response) einfach die ausgetauschte Datenmenge einsetzt, vereinfacht sich die o. g. Formel noch weiter:

$$t \text{ (Transaktion)} = n \times (\text{RTT} + t \text{ (Server)} + t \text{ (Client)}) + \text{Datenmenge} / \text{Bitrate}$$

Somit wirkt sich die Round Trip Time im Netz in drei Fällen nicht signifikant auf die Transaktion aus:

- Wenn $\text{RTT} \ll t \text{ (Server)}$
- Wenn $\text{RTT} \ll t \text{ (Client)}$
- Wenn $n \times \text{RTT} \ll \text{Datenmenge} / \text{Bitrate}$, d. h. wenn $n \times \text{RTT} \times \text{Bitrate} \ll \text{Datenmenge}$

Die Frage ist also, für welche Anwendungen der oben berechnete Latenzunterschied von $32 \mu\text{s}$, d. h. der RTT-Unterschied von $2 \times 32 \mu\text{s} = 64 \mu\text{s}$ zwischen Cut-Through und Store&Forward relevant ist. Nicht relevant ist dieser Unterschied in

folgenden Fällen:

- wenn die Entfernung zwischen Client und Server wesentlich größer als 6,4 km sein kann, d. h. für alle Anwendungen, die für das WAN und mobile Clients tauglich sein müssen,
- wenn Server und Clients im Durchschnitt wesentlich mehr als 64 Mikrosekunden Verarbeitungszeit für die Bearbeitung eines Request-Response-Paares benötigen, oder
- wenn das Produkt aus n , RTT und Bitrate wesentlich kleiner als die gesamte Datenmenge ist, die pro Transaktion übertragen werden muss.

Der letztgenannte Fall lässt sich für die Bitrate 10 Gbit/s und $\text{RTT} = 64 \mu\text{s}$ berechnen:

$$\text{Datenmenge} \gg n \times 64 \mu\text{s} \times 10 \text{ Gbit/s} = n \times 640.000 \text{ Bits} = n \times 80.000 \text{ Bytes}$$

Bei Datenbanktransaktionen sind mittlere sechsstellige Byte-Zahlen pro Transaktion keine Seltenheit; die letztgenannte Bedingung trifft daher nicht zu. Auch ist es nicht üblich, Client und Server eines typischen Datenbankprotokolls wie Net8 von Oracle weiter entfernt als wenige km aufzustellen.

Bleibt noch die Frage, wie schnell Server und Clients auf Requests bzw. Responses reagieren und ob deren Latenz wesentlich über 64 Mikrosekunden liegt. Diese Latenz ist natürlich nicht nur von den Prozessoren der betreffenden Maschinen abhängig, sondern auch von

der I/O-Leistung, die den Maschinen zur Verfügung steht. Letzteres würde bei der Nutzung eines zentralen Speichers der einem Server durchschnittlich zur Verfügung stehenden I/O-Leistung entsprechen. Geht man vom Wert 100.000 IOPS bei einem High-End-Speichersystem aus, welches 100 physikalische Server bedient, stehen einem Server durchschnittlich 1000 IOPS zur Verfügung. Selbst eine einzige I/O-Aktion würde also durchschnittlich einer Millisekunde entsprechen. ULL lohnt sich also nur dann, wenn pro Transaktion nur wenige I/O-Aktionen anfallen. Auf keinen Fall darf dann pro Request eine I/O-Operation erforderlich sein, denn eine Millisekunde I/O-Zeit ist ja bekanntlich wesentlich mehr als $64 \mu\text{s}$.

Anders stellt sich die Situation dar, wenn alle mit der Transaktion zusammenhängenden I/O-Operationen ohne Inanspruchnahme von Festplattenleistung vonstatten gehen, also wenn zum Beispiel statt Festplatten Solid State Devices (SSD) eingesetzt werden. Diese führen I/O-Operationen wesentlich schneller aus.

Hersteller wie Cisco geben bei der Werbung für ULL-Switches an, diese seien besonders geeignet für Börsenanwendungen in einer sogenannten Co-location, in der die Trading-Rechner zusammengeschaltet sind². Es geht darum, dass Transaktionen binnen Millisekunden über die Bühne gehen. Das sind dann keine von Menschen gesteuerten Transaktionen, sondern zum Beispiel Trading-Aufträge, die automatisch und ohne Zutun von menschlichen Händlern über die Bühne gehen. Bestimmte Ereignisse lösen den Kauf oder Verkauf bestimmter

Jetzt Leser werden

Der Netzwerk Insider

Der Netzwerk Insider erscheint 12 Mal im Jahr im PDF-Format und informiert Sie per eMail über die Hintergründe aktueller Netzwerk-Technologien. Jeden Monat werden zwei Themen gewählt, über die in ausführlicher Form topaktuelle Insider-Informationen gegeben werden. Der Netzwerk-Insider vertritt die Sichtweise von Technologie-Anwendern und bewertet Produkte und Technologien im Sinne der wirtschaftlichen und erfolgreichen Umsetzbarkeit in der täglichen Praxis. Durch seine strenge wirtschaftliche Unabhängigkeit (keine Hersteller-Anzeigen) kann er es sich leisten, Schwachstellen und Nachteile offen anzusprechen. Der Netzwerk-Insider ist bekannt für seine kritische, herstellerneutrale und fundierte Technologie-Bewertung.



Hier können Sie sich zum Netzwerk Insider kostenlos und ohne jede Verpflichtung registrieren lassen:
<http://www.comconsult-akademie.de/de/Registrierung.php>

²<http://www.cisco.com/en/US/products/ps11541/index.html>

Wie viel Delay ist tolerierbar?

Werte aus. Hier könnten theoretisch Millisekunden über Millionen Gewinn oder Verlust entscheiden.

Kritisch ist hier anzumerken:

- Ereignisse, welche die Börse betreffen, sind globale Ereignisse. Kursschwankungen in Japan machen sich in Europa frühestens nach hunderten Millisekunden bemerkbar. Dann sind Mikrosekunden Switch Latency bzw. wenige Millisekunden Transaktionszeit nicht mehr so relevant.
- Spätestens nach den vielen teuren Pannen, die durch automatisiertes Trading ohne Kontrollen durch Menschen passiert sind, ist die Frage nach der Sinnfälligkeit und den Risiken solchen Tradings berechtigt. Letztendlich ist High Frequency Trading nichts anderes als ein Automat, der auf externe Ereignisse mit Aktionen reagiert. Dazu ist eine Software erforderlich, die mit Heuristiken, Wahrscheinlichkeiten etc. arbeitet. Wenn diese Software nicht optimiert ist und Fehlentscheidungen trifft, nutzt ein schnelles System auch nichts. Werden jedoch Menschen für die Kontrolle von Trading und letzte Checks eingesetzt (damit Automaten keine milliarden schweren Schäden anrichten), brauchen die Aufträge keine Ultra-Low Latency.

Wie in den 1990er Jahren wird sich mit der Einführung von 40/100Gigabit Ethernet in den meisten Netzen ohnehin wieder eine hierarchische Anordnung von Links im Netz einstellen, die mit unterschiedlichen Bitraten arbeiten. Dann wird der Cut-Through-Modus wie vor 15 Jahren in Vergessenheit geraten. Was bleibt dann von ULL? Switches, die Weiterleitungsentscheidungen auch beim Ansatz Store & Forward schnell genug fällen, um allen Applikationen gerecht zu werden.

Full Mesh versus Tree

Was ist aber mit dem Netzdesign? Stimmt das, was zum Beispiel Juniper Networks über die Vorteile einer Full-Mesh-Topologie gegenüber einem hierarchischen, baumförmigen Design sagt?³

Die Quintessenz solcher Aussagen ist diese: Der „Tree“, also die baumförmige hierarchische Anordnung der Switches, ist mit zu viel Latenz verbunden. Sie muss durch Full Mesh ersetzt werden. Es geht darum, dass die Paketübertragung zwischen zwei beliebigen Punkten im RZ-Netz über möglichst wenige Switches geht, damit nicht zu viel Latenz auf dem Übertragungspfad anfällt.

Die Nachrichtentechnik und speziell die Netztechnik blickt auf jahrzehntelange Erfahrung zurück. Die hierarchischen Netzstrukturen sind nicht ohne Grund entstanden oder nur weil bestimmte Hersteller dazu passende Komponenten verkaufen wollten. Die Latenzproblematik stellt sich in anderen Größenordnungen auch in der weltweiten Telekommunikation. Auch da geht es um Latenzminimierung. Es wäre sicherlich vom Vorteil, wenn alle Provider-Switches dieser Welt über direkte Kabel miteinander vollvermascht wären. Dies ist aber aus Gründen der Skalierbarkeit der Switches und des hohen Verkabelungsaufwands nicht möglich. So entwickelte sich im Laufe der Jahrzehnte ein hierarchisches Netz.

Die Entstehungsgeschichte hierarchischer RZ-Netze war ähnlich. In der 1990er Jahren haben viele Unternehmen ihre wenigen Server direkt an große zentrale Switches angeschlossen. Bus- und ringförmige Lokale Netze wurden durch sogenannte Collapsed Backbones abgelöst. Auch vor 20 Jahren wusste man, dass damit Latenzen minimiert werden können.

Der Collapsed Backbone funktionierte aber nur bis zu einer niedrigen Anzahl zentraler Switches. Irgendwann waren mehr Ports für die Vollvermaschung der zentralen Switches erforderlich, als diese den Clients und Servern zur Verfügung

stellen konnten. Also behalf man sich der guten alten Graphentheorie, die schon immer ein verlässlicher Freund und Helfer der Nachrichtentechniker gewesen ist.

Was ist die optimale Netztopologie?

Stellen wir uns einem grundlegenden Problem der Netztechniker: Was ist die optimale Topologie für ein Netz, das aus Access Switches mit jeweils m Ports besteht und e Endgeräte miteinander verbinden muss?

Je nach Optimierungskriterien fällt die Antwort anders aus. Wenn zum Beispiel die Minimierung der Anzahl der Switches im Vordergrund steht, sollte m so groß wie möglich sein, damit die Anzahl n der Switches möglichst klein ist:

$$n = e \text{ mod } m$$

Was ist aber dann, wenn die Minimierung der Anzahl der Switches (am besten auf den Wert $n = 1$, aus ULL-Gesichtspunkten der beste Wert) nicht das einzige Kriterium ist, das ein Planer eines Rechenzentrums berücksichtigen muss?

Dann sind wir nämlich in der Realität des Netzdesigns angekommen. Eine Vielzahl von Kriterien ist zu berücksichtigen, darunter:

- Managebarkeit
- Hardware-Kosten

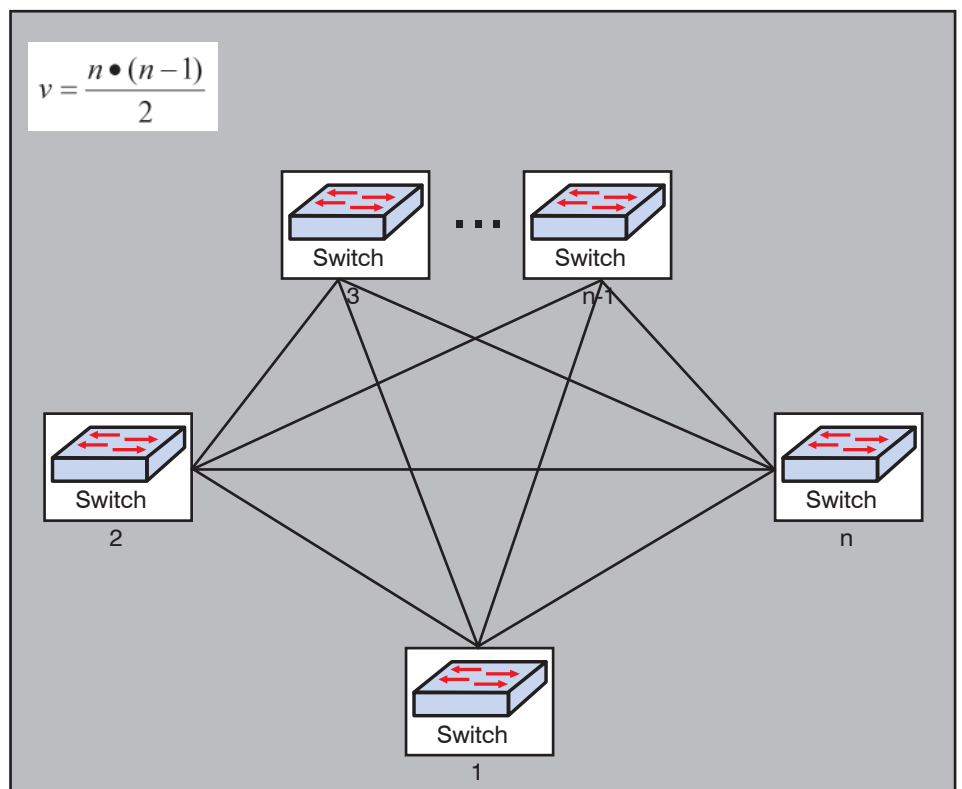


Abbildung 5: Vollvermaschung von n Switches

³http://junipernetworks.com/us/en/company/press-center/press-releases/2011/pr_2011_02_23-13_04.html

Wie viel Delay ist tolerierbar?

- Verfügbarkeit
- Gesamtleistung im Sinne von Durchsatz
- Latenzminimierung

Einige dieser Kriterien sind mathematisch zu fassen, andere nicht. Welche Netztopologie ist in einem RZ-Netz am besten managebar? Wie wichtig ist der Aspekt Managebarkeit insgesamt? Sicher ist die Antwort der RZ-Betreiber auf diese Fragen unterschiedlich. Die Antwort ist davon abhängig, wie groß das RZ ist, wie viele Server-Ports zu bedienen sind, wie das Wartungskonzept im RZ aussieht etc. Der Autor arbeitet zum Zeitpunkt der Ausarbeitung dieses Beitrags sowohl in einem Projekt, in dem der Betreiber die Konzentration hunderter Gigabit nebst ein paar Dutzend 10Gigabit Ethernet Ports auf zwei Switches bevorzugt, als auch in anderen Projekten, in denen die RZ-Betreiber auf Top of the Rack Switches bestehen. Wer hat Recht? Keinem dieser RZ-Betreiber darf man Unwissenheit oder Festhalten an überholten Konzepten vorwerfen. Die RZ-Randbedingungen und Präferenzen der unterschiedlichen Betreiber sind unterschiedlich.

Bei einer Vielzahl von RZ-Betreibern scheint sich die Präferenz für Top of the Rack Switches durchgesetzt haben. Betrachten wir diese Gruppe etwas genauer.

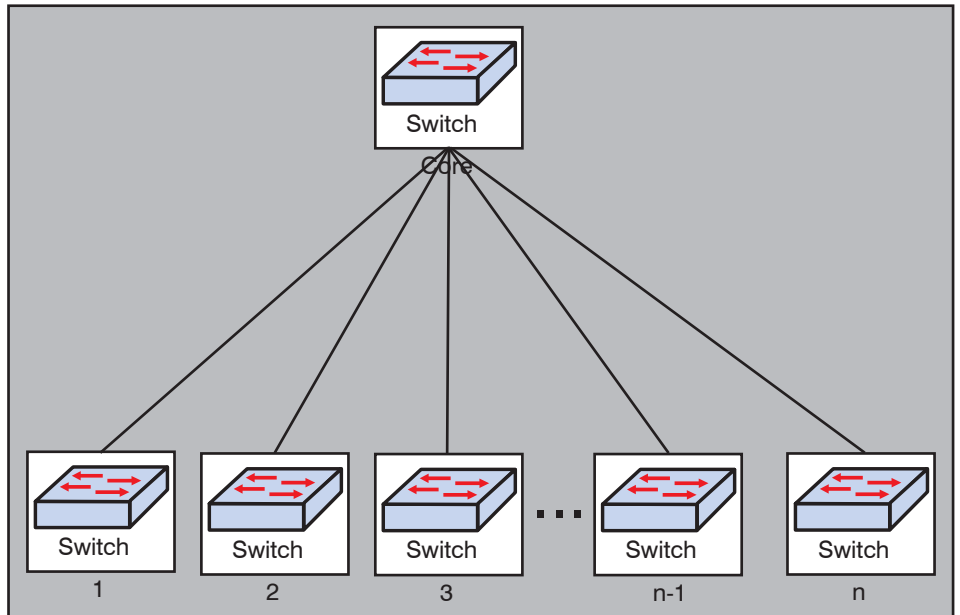


Abbildung 6: Core und Access Switches

Wir gehen davon aus, dass n solche Switches erforderlich sind, unabhängig davon, wie groß die Zahl e der zu realisierenden Server Ports ist.

Eine Vollvermaschung der ToR-Switches gemäß Abbildung 5 ist zwar aus Latenzsicht optimal, skaliert aber nur begrenzt,

denn bekanntlich brauchen wir dafür eine hohe Anzahl von Inter-Switch-Verbindungen v.

Außerdem können bei einem solchen Design, wenn es auf Up- und Downlinkseite der Switches mit derselben Bitrate arbe-

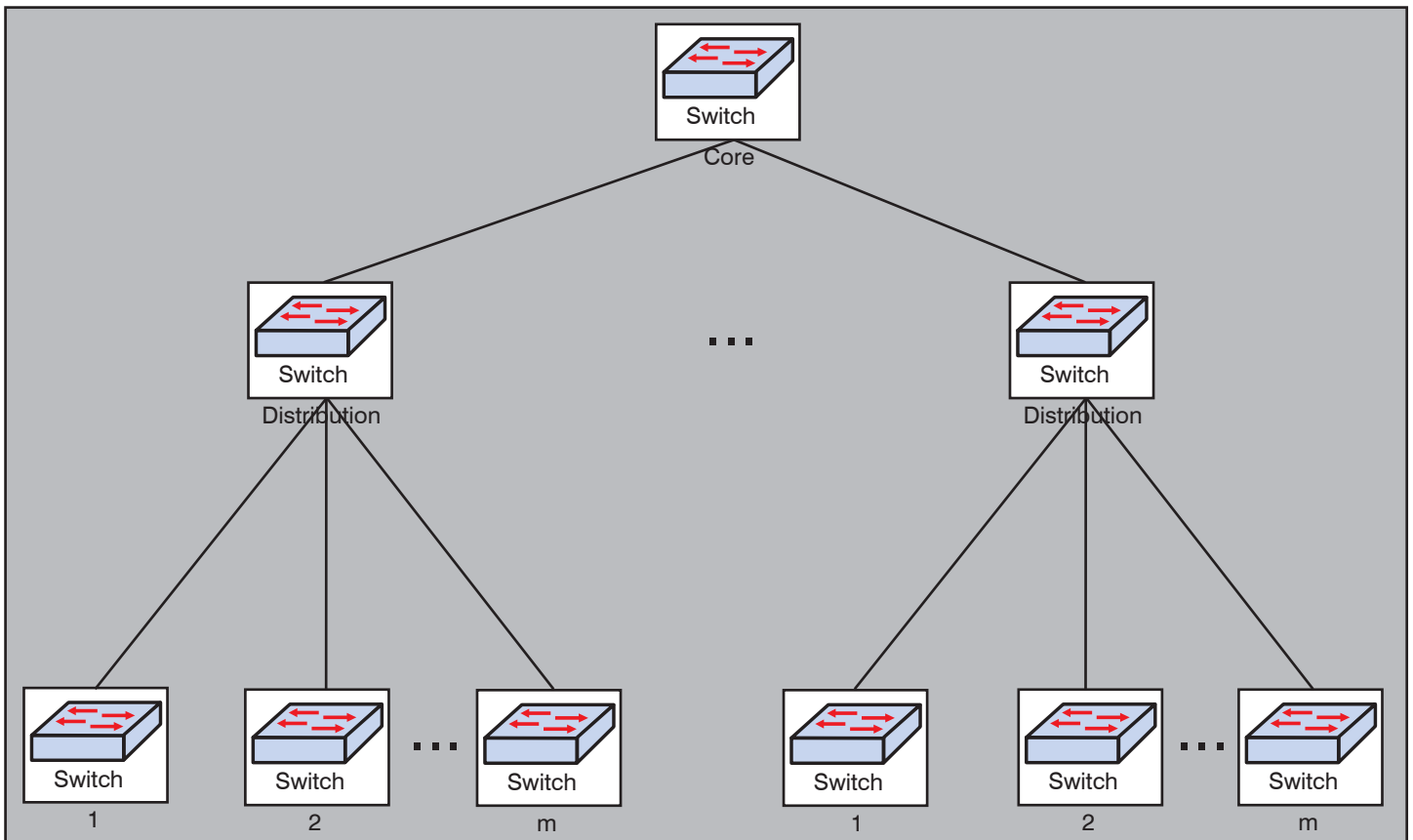


Abbildung 7: Dreistufige Netzhierarchie

Wie viel Delay ist tolerierbar?

tet, punktuelle Überlastsituationen dadurch entstehen, dass temporär oder permanent asymmetrische Lasten zu übertragen wären. Wenn also an den Switch x zum Beispiel ein Datensicherungsserver angeschlossen ist, kann die Verbindung zum Switch y, eine einzige Verbindung, die als „Shortest Path“ gilt, genau im Moment der Datensicherung überlastet sein.

Und hier sind wir an einer wesentlichen Ursache hierarchischer Netzstrukturen angelangt: dem Kommunikationsprofil. Wir haben es in den RZ-Netzen häufig nicht mit dem Profil „jeder mit jedem“ zu tun, sondern mit der Situation „viele mit wenigen“. Ein Datensicherungsserver, ein zentrales Speichersystem etc. gehören zu den „wenigen“, „normale“ Server zu den „vielen“.

Die Vollvermaschung ist nur bedingt skalierbar, und es gibt wenige Maschinen, welche die Last vieler anderer Maschinen aufnehmen müssen. Der Anforderung nach Skalierbarkeit und Asymmetrie wird man in der Regel durch eine hierarchische Struktur gerecht, auch wenn sie nur aus zwei Ebenen besteht: Access Switches und Core Switches, wie in der Abbildung 6 dargestellt.

Damit wird der Hop Count im Vergleich zur Vollvermaschung von zwei auf drei erhöht, was mit einer Erhöhung der Latenz im Netz verbunden ist. Solange die Uplinks mit der gleichen Bitrate wie die Downlinks arbeiten, beträgt der Latenznachteil 50 % (von 2 auf 3 erhöht). Hat man aber Switches zur Verfügung, deren Uplinks (auch aus Lastgründen) ohnehin mit einer wesentlich höheren Bitrate als die Downlinks arbeiten, relativiert sich der Latenzunterschied wieder, denn mit erhöhter Bitrate sinkt die Zeit, die ein Frame braucht, um einen Hop zurück zu legen.

Die meisten RZ-Netzbetreiber werden mit einer zweistufigen Hierarchie auskommen. In den größten RZ-Netzen reicht aber diese Struktur nicht aus; man denke etwa an Rechenzentren mit hunderten Schränken und damit hunderten Server Access Switches, womöglich verteilt auf verschiedene Lokationen. In solchen Umgebungen muss eine dritte Hierarchiestufe dazu kommen, wie in der Abbildung 7 dargestellt.

Auch hier gilt: die Verschlechterung der maximalen Hop Counts von 3 (im Falle der zweistufigen Hierarchie) auf 5 (im Falle der dreistufigen Hierarchie) wird dadurch kompensiert, dass Uplinks eine höhere Bitrate als die Downlinks unterstützen.

Die Anzahl der Hierarchiestufen und damit Hop Counts im Netz ist damit immer von der Größe des Netzes abhängig. Daran, dass größere Netze tendenziell mehr

Hierarchiestufen brauchen als kleinere, hat sich in den letzten Jahrzehnten nichts geändert.

Zwischenfazit zu ULL

Als Zwischenfazit zu Ultra-Low Latency ist festzuhalten:

- ULL ist bei Kommunikationsströmen irrelevant, welche wesentlich längere Entfernungen als wenige Kilometer zurücklegen müssen. Solche langen Entfernungen sind für Disaster Recovery geboten.
- Wenn überhaupt wirkt sich ULL nur bei sehr leistungsfähigen sonstigen Komponenten aus: Prozessoren auf beiden Seiten, Storage-Systeme.
- Mit der Einführung von 40/100Gigabit Ethernet wird der Cut-Through-Modus als wesentliche ULL-Eigenschaft in den meisten Netzen irrelevant.
- Transaktionen, die Menschen mit Reaktionszeiten im Sekundenbereich involvieren, brauchen ULL nicht, sondern nur Transaktionen mit Kommunikation zwischen Maschinen.
- ULL ändert nichts daran, dass die Anzahl der benötigten Hierarchiestufen mit der Größe eines RZ-Netzes steigt.

Switch- und Chip-Hersteller können weder mathematische Gesetze der Graphentheorie noch physikalische Gesetze aufheben. Signale sind maximal mit Lichtgeschwindigkeit zu übertragen. Dabei bleibt es.

Wenn jedoch mit ULL gemeint ist, dass neue Switches durch den Einsatz schneller Chips für die Minimierung der Latenzen im Switch sorgen, dann ist das eine Selbstverständlichkeit. Mit fortschreitender Chip-Technologie steigt die Geschwindigkeit von Switches, und die Latenz in den Switches sinkt. Allein schon die steigenden Bitraten erfordern immer schnellere Chips.

Delay im WAN

LAN Switch Delays sind je nach Anwendung vielleicht innerhalb eines Campus relevant, nicht jedoch im Wide Area Network (WAN). Wenn die Übertragungswege wenige Kilometer überschreiten, dann werden die Latenzunterschiede zwischen verschiedenen Switch-Produkten irrelevant. Im WAN entstehen lästige Latenzen vor allem durch andere Effekte:

- Ungünstige Wege (zum Beispiel von Deutschland nach Indien über Nordamerika, den Pazifik und den Indischen Ozean)
- Überlast an bestimmten Punkten und auf bestimmten Segmenten des Übertragungsweges

Hier muss man zwischen unvermeidbaren und vermeidbaren Latenzeffekten unterscheiden. Da man bekanntlich die Gesetze der Physik nicht überlisten kann, dauert die Signalübertragung von Deutschland nach Indien eine bestimmte Zeit. Man kann die Strecke berechnen⁴:

- Frankfurt am Main bis Mumbai auf dem kürzesten Luftweg: 6.574,536 km

Jetzt Leser werden

Der Netzwerk Insider

Der Netzwerk Insider erscheint 12 Mal im Jahr im PDF-Format und informiert Sie per eMail über die Hintergründe aktueller Netzwerk-Technologien. Jeden Monat werden zwei Themen gewählt, über die in ausführlicher Form topaktuelle Insider-Informationen gegeben werden. Der Netzwerk-Insider vertritt die Sichtweise von Technologie-Anwendern und bewertet Produkte und Technologien im Sinne der wirtschaftlichen und erfolgreichen Umsetzbarkeit in der täglichen Praxis. Durch seine strenge wirtschaftliche Unabhängigkeit (keine Hersteller-Anzeigen) kann er es sich leisten, Schwachstellen und Nachteile offen anzusprechen. Der Netzwerk-Insider ist bekannt für seine kritische, herstellerneutrale und fundierte Technologie-Bewertung.



Hier können Sie sich zum Netzwerk Insider kostenlos und ohne jede Verpflichtung registrieren lassen:

<http://www.comconsult-akademie.de/de/Registrierung.php>

⁴Siehe Luftlinie.org

Wie viel Delay ist tolerierbar?

- Dieselbe Strecke auf dem kürzesten befahrbaren Landweg: 9.306 km

$$t = \frac{10.000km}{200.000km/s} = 0,05s = 50ms$$

Wenn wir also von einem Kabelweg von 10.000 km ausgehen, lässt sich die Zeit für die optische Signalübertragung von Frankfurt am Main nach Mumbai wie folgt berechnen:

Ein kürzerer RTT-Wert als 100 ms ist also über optische Kabel nicht zu erreichen. Wenn also in High Frequency Trading Rechner an zwei Börsen in Frankfurt und Mumbai involviert sind, erfährt der eine Rechner frühestens nach 50 ms von einem Vorgang auf dem anderen Rechner (in Wirklichkeit frühestens nach ein paar Sekunden, denn zu einer solchen Meldung gehört mehr als nur eine unquitierte Übertragung). Diese Verzögerung ist unvermeidbar, auch wenn Milliarden Euro oder Dollar in neue Kabelwege durch neun Länder investiert werden.

Optimieren kann man also die WAN-Latenz durch die Vermeidung von Überlast (und den damit verbundenen Paketverlusten) bzw. durch die Wahl der direktesten möglichen Route. Ersteres kann man in Gestalt garantierten Netzdurchsatzes kaufen (es kostet nur eine Kleinigkeit). Wie der Provider den Durchsatz sicherstellt, muss ihm überlassen werden. Finanzielles überlassen wir einem geschickten Einkauf.

Letzteres, also die Wahl der optimalen Route, ist kniffliger. Denn dafür ist nicht nur der Provider zuständig, sondern auch der Kunde, wie wir sehen werden.

Ungünstige Wege

Für ungünstige Wege im WAN tragen nicht nur die Provider die Verantwortung. Man stelle sich eine Börse vor, die u. a. RZ-Standorte in Frankfurt am Main und New York unterhält. Von diesem Börsenverbund aus soll eine Verbindung zu einer indischen Börse mit einem RZ in Mumbai geschaffen werden. Da externe Verbindungen in der Regel über Komponenten der Perimetersicherheit geleitet werden, wird die Verbindung nicht direkt, sondern über Firewalls geführt. Weiterhin stelle man sich vor, dass die betroffenen Firewalls nicht in Frankfurt, sondern in New York aufgestellt sind.

Dann nämlich geht der Weg von Frankfurt zunächst nach New York, und erst von dort aus nach Mumbai, wie in der Abbildung 8 dargestellt. Der Weg wird mindestens verdoppelt und damit der RTT-Wert

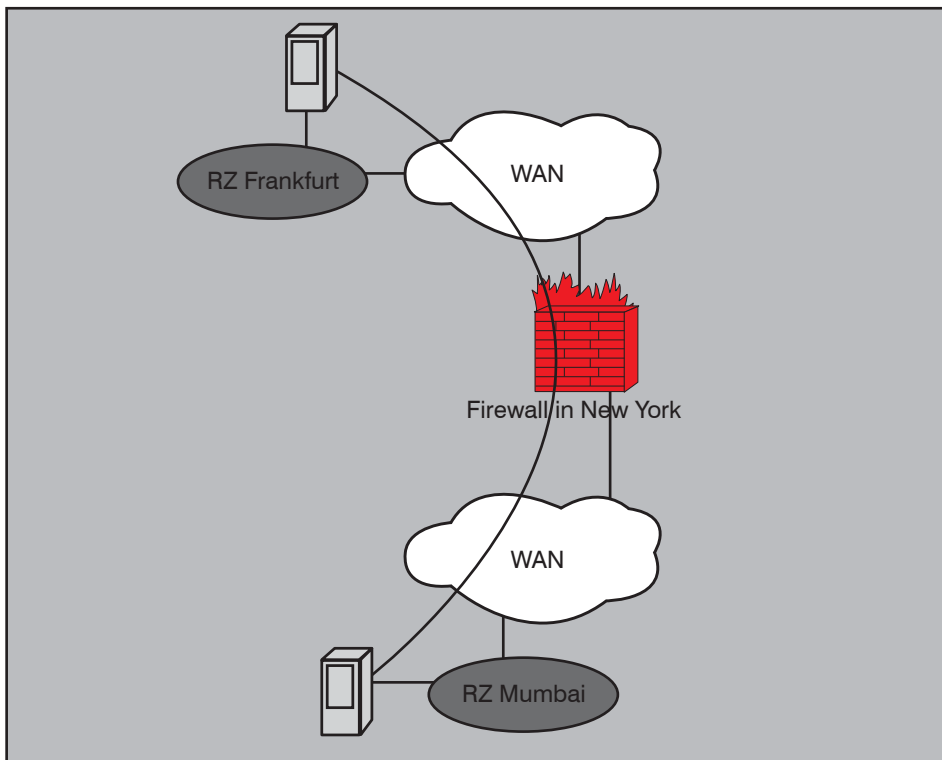


Abbildung 8: Ungünstiger Übertragungsweg

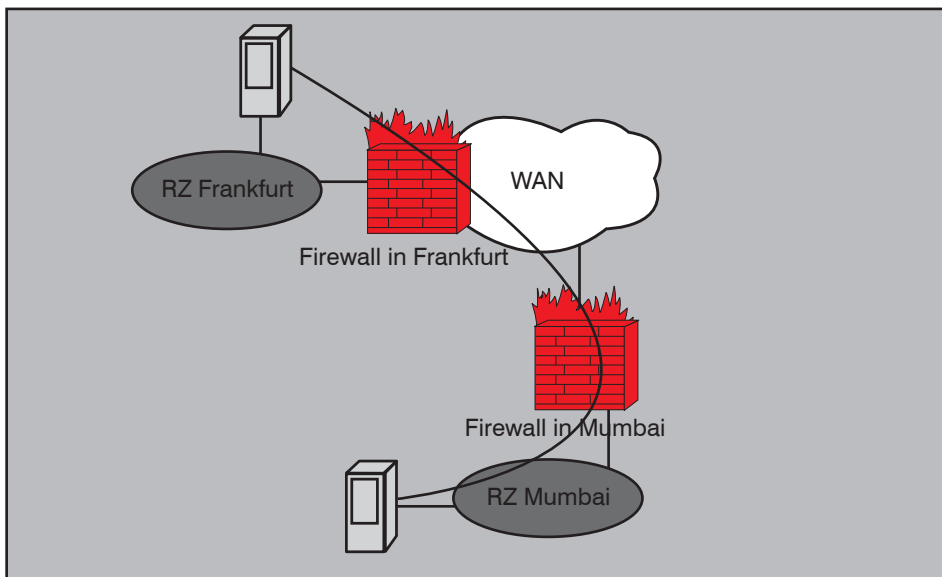


Abbildung 9: Günstiger WAN-Weg

von 100 auf 200 Millisekunden erhöht, auch wenn man Milliarden für einen neuen Kabelweg von New York über die Arktis, Skandinavien, Russland, Kasachstan, Usbekistan, Turkmenistan, Afghanistan und Pakistan ausgibt (je weiter wir auf dieser Strecke kommen, umso höher sind die Kosten, nicht nur für die Kabelverlegung, sondern für deren militärische Absicherung). Die absolute Steigerung der Responsezeiten fällt noch stärker als 100 Millisekunden aus, weil die Transaktion sicherlich ein paar Durchläufe zwischen

Frankfurt und Mumbai erfordern wird.

Um solche ungünstigen Wege zu vermeiden, müssen die RZ- und Netzbetreiber am besten für direkte Verbindungen sorgen. In unserem Fall heißt das: es muss auch Firewalls in Frankfurt und/oder in Mumbai geben, damit im WAN der Übertragungsweg optimiert werden kann, am besten so, dass der kürzeste Weg zwischen Frankfurt und Mumbai genommen wird. (siehe Abbildung 9)

Wie viel Delay ist tolerierbar?

Im oben genannten Beispiel verursacht die aus Gründen der IT-Sicherheit vorge-sehene Firewall-Inspektion den ungün-stigen Weg. Es gibt aber auch andere denkbare Ursachen, zum Beispiel:

- Wo ist der Übergabepunkt zwischen den Netzen der jeweiligen WAN Provider in Deutschland und Indien?
- Sind Overlay-Strukturen wie MPLS reali-siert, die ein Shortest Path Routing ver-hindern?
- Können Shortest-Path-Routing-Mecha-nismen anhand der IP-Adressen den wirklich kürzesten Weg berechnen?

Die Antworten auf diese Fragen sind nicht einfach. Wir werden anhand der dritten der oben gestellten Fragen sehen, dass neue RZ-Strukturen hier ein paar Unwäg-barkeiten schaffen.

Auswirkungen der Virtualisierung

Man stelle sich vor, ein Client greife über das WAN auf eine virtualisierte Serverfarm zu, wie in der Abbildung 10 dargestellt. Der Weg geht über den Router am Client-Standort, das WAN, den Router am Standort eines Load-Balancers, den Load Balancer selbst und die Layer-2-Verbindung zwischen zwei RZ-Standorten bis zum aktiven Knoten in der virtualisierten Serverfarm. Je nach Latenz auf der Layer-2-Verbindung zwischen den beiden Rechenzentren ist der Weg signifikant ungünstiger als ein denkbarer direkter Weg vom Client durch das WAN zum Server.

Nun sind Layer-2-Verbindungen zwischen RZ-Standorten, die tausende Kilometer entfernt sind, eher ungewöhnlich, weil andere Restriktionen den Aufbau von Server-Clustern über so lange Wege erschweren. Aber bei einer mehrstufigen Schleuse, zum Beispiel externes Netz - äußere DMZ - innere DMZ - RZ-Netz, in jeder Stufe mit Load Balancing, Firewalling etc. versehen, können aus wenigen Millisekunden auf der Layer-2-Verbindung schnell maximale Latenzen entstehen, die eine Größenordnung höher liegen.

Die Hauptursache hierfür: Die verschiedenen Netz- und Virtualisierungsebenen „wissen“ nichts voneinander und können ihre Wegewahlentscheidungen nicht so treffen, dass sie unter dem Strich, also für die Strecke von einem Ende zum anderen (von Client zum physikalischen Server) mit der kürzesten Latenz verbunden sind.

Dieses „Manko“ wurde mit dem Aufbau der Protokollhierarchie auf den verschie-

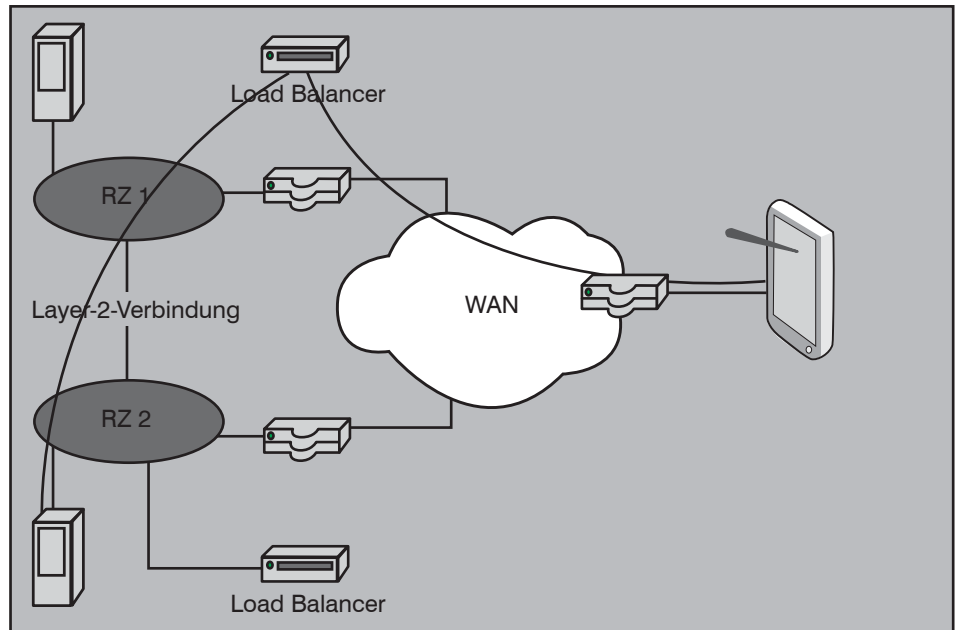


Abbildung 10: Ungünstiger Weg durch Virtualisierung

denen Ebenen des in Netzen üblichen Schichtenmodells bewusst in Kauf genommen. Die Wegewahl soll eben im Layer-2-Netz anhand der MAC-Adresse, im Layer-3-Netz anhand der IP-Adresse und auf höheren Schichten anhand von Session- und Applikations-bezogenen Merkmalen erfolgen, und Änderungen in einer Protokollschicht sollen möglichst keine Auswirkung auf andere Protokollschichten haben. Das ist seit vierzig Jahren das Erfolgsgeheimnis offener Netze. Somit haben wir es mit einem Segen zu tun, der zugleich ein Fluch sein kann, nämlich dann, wenn der Weg von einem Ende durch die Protokollschichten zum anderen Ende zu einem Schlingerkurs wird.

Gibt es Abhilfe dagegen?

Overlay-Strukturen

Overlay-Strukturen können helfen, den Weg durch ein WAN zu optimieren. Eine solche Overlay-Struktur ist in der Abbildung 11 dargestellt.

Der Client greift nicht direkt, sondern über ein Overlay-Netz mit Relays auf den Server zu. Die Relays sind möglichst engmaschig auf das WAN verteilt. In der Nähe des Clients sowie in der Nähe jedes der beiden RZ-Standorte ist jeweils ein Relay aufgestellt. Dann gibt es zwischen Client und Server im Overlay-Netz

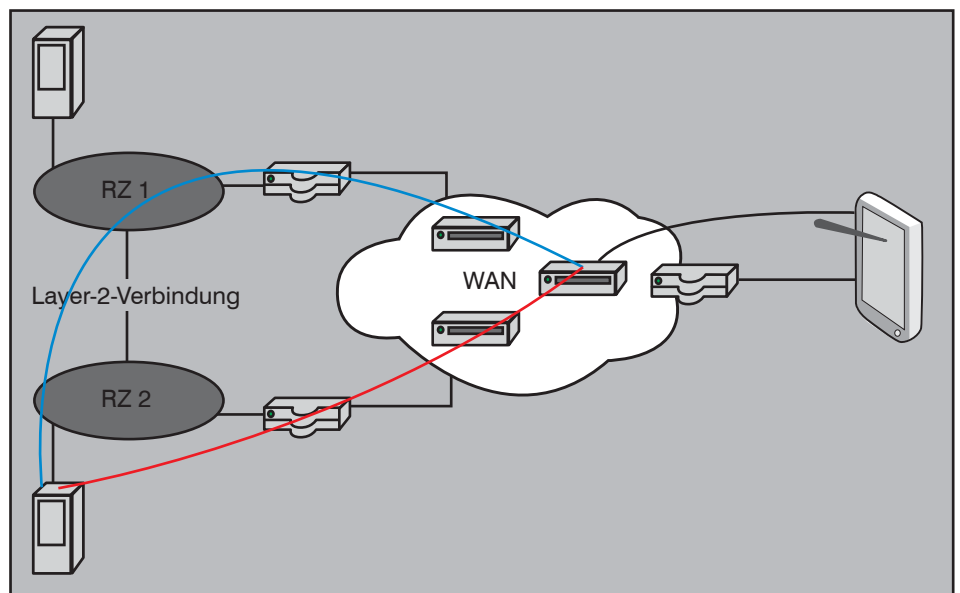


Abbildung 11: Overlay-Struktur

Wie viel Delay ist tolerierbar?

verschiedene Wege. Man könnte alle Pakete im Overlay-Netz über mehrere Wege übertragen. Die schnellste Kopie, die am Endziel ankommt, bestimmt den günstigsten Weg. Die anderen, langsameren Kopien werden verworfen. Man könnte das für alle Pakete tun oder nur auf den Verbindungsaufbau beschränken. Ersteres, wenn man auch eine Abhilfe gegen Paketverluste haben will, und Letzteres, wenn man befürchtet, dass überschüssige Kopien desselben Pakets Probleme verursachen könnten.

Genau eine solche Struktur nutzt die Firma Akamai, um den eigenen Kunden mit weltweiten Kommunikationsbeziehungen die Optimierung von Routen durch das globale Netz zu ermöglichen. Die Overlay-Struktur von Akamai ist im Internet erreichbar. In der Regel können die Akamai-Kunden durch ein „Umleiten“ von DNS-Einträgen auf die Akamai-Overlay-Struktur diese nutzen. Dann kann es sogar sein, dass ein Weg durch das Internet und die Akamai-Overlay-Struktur bessere Antwortzeiten aufweist als der Weg durch ein Virtual Private Network auf der Basis einer MPLS-Plattform.

Im Prinzip arbeiten globale Internet-Unternehmen wie Google nicht anders. Sie unterhalten ein engmaschiges Netz an Rechenzentren, die auf verschiedene Weltregionen verteilt sind. Die Inhalte werden zwischen diesen Rechenzentren repliziert (wie, das ist manchmal ein Geschäftsgeheimnis und grenzt an Zauberei). Der europäische Benutzer wird sicherlich nicht vom Fernen Osten aus bedient. Probieren Sie es aus: seit Kurzem liefert die Suchmaschine von Google sogar Zwischenergebnisse, noch während Sie die Stichworte eintippen! Das könnte man „Cut-Through Searching“ nennen.

LISP

Die Firma Cisco schlägt zur Optimierung von Übertragungswegen einen weiteren Weg vor: Locator/ID Separation Protocol (LISP). Wie der Name schon sagt, besteht die Grundidee darin, zwischen den Informationen über die Lokation eines Knotens im Netz und den Informationen über die Identität des Knotens zu unterscheiden. Das bisherige IP Routing macht diese Unterscheidung nicht. Für das IP Routing ist die IP-Adresse Identifikationsmerkmal und Lokationsinformation in einem. LISP arbeitet mit zwei verschiedenen Datenbasen für die Wegewahl:

- Routing Locators (RLOCs) für die Wegewahl im globalen Netz

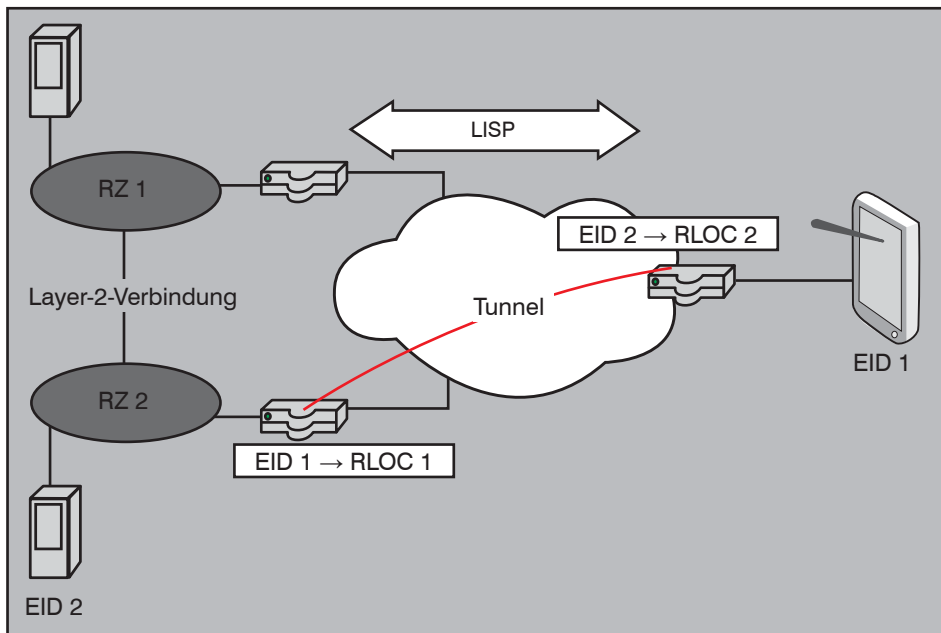


Abbildung 12: LISP

- End Point Identifiers (EIDs) für die Erkennung von Sessions zwischen Endgeräten

Jeder LISP-fähige Router ist in der Lage, EIDs auf RLOCs abzubilden. Die Abbildung erfolgt mithilfe von Informationen, die mittels LISP zwischen den Routern ausgetauscht werden. Diese bauen Tunnel zu anderen LISP-Routern auf. Beim Empfang eines Paketes an eine bestimmte EID ordnet ein LISP Router einen RLOC zur Ziel-EID zu, versieht das Paket mit der RLOC-Information und sendet das Paket durch den Tunnel zum Ziel-RLOC, d. h. zum LISP-Router in der Nähe der

Ziel-EID. Dieser entfernt die RLOC-Information und leitet das Paket zur Ziel-EID weiter. Sowohl EID als auch RLOC entsprechen in ihrem Format herkömmlichen IP-Adressen. Das Schema ist in der Abbildung 12 dargestellt.

Wenn die Abbildung der EIDs auf die RLOCs unter Berücksichtigung der „Nähe“ eines LISP-Routers zum Ziel erfolgt, kann der Weg vom Client zum Server optimiert werden. Ohne LISP wären in der Abbildung 12 die Pfade über den oberen und den unteren linken Router aus der Sicht von IP Routing gleich berechtigt, sodass es durchaus dazu kom-

Jetzt Leser werden

Der Netzwerk Insider



Der Netzwerk Insider erscheint 12 Mal im Jahr im PDF-Format und informiert Sie per eMail über die Hintergründe aktueller Netzwerk-Technologien. Jeden Monat werden zwei Themen gewählt, über die in ausführlicher Form topaktuelle Insider-Informationen gegeben werden. Der Netzwerk-Insider vertritt die Sichtweise von Technologie-Anwendern und bewertet Produkte und Technologien im Sinne der wirtschaftlichen und erfolgreichen Umsetzbarkeit in der täglichen Praxis. Durch seine strenge wirtschaftliche Unabhängigkeit (keine Hersteller-Anzeigen) kann er es sich leisten, Schwachstellen und Nachteile offen anzusprechen. Der Netzwerk-Insider ist bekannt für seine kritische, herstellerneutrale und fundierte Technologie-Bewertung.

Hier können Sie sich zum Netzwerk Insider kostenlos und ohne jede Verpflichtung registrieren lassen:
<http://www.comconsult-akademie.de/de/Registrierung.php>

⁵<http://tools.ietf.org/wg/lisp/>

Wie viel Delay ist tolerierbar?

men kann, dass der ungünstige Weg über den oberen linken Router genommen wird. Mit LISP kann dafür gesorgt werden, dass der günstigere Weg beschritten wird. Dazu ist erforderlich, dass nicht nur WAN-Router, sondern auch Switches in den beiden Rechenzentren LISP unterstützen und LISP-Tunnel aufbauen können. Diese Switches können weiterhin reines Layer 2 Switching ausführen, jedoch mit der zusätzlichen Intelligenz versehen werden, LISP-Routen zu optimieren und LISP-Tunnel mit minimaler Latenz aufzubauen.

Bewertung von LISP

Die Latenzminimierung ist nur ein Seiteneffekt von LISP. LISP ist in erster Linie mit anderen Zielen entwickelt worden, zum Beispiel der Reduzierung der Größe von Routing-Tabellen, der Erleichterung eines Providerwechsels durch die providerunabhängige EID-Adressierung und einer sanften Migration von IPv4 zu IPv6.

Die Internet Engineering Task Force hat eine sehr aktive LISP-Gruppe⁵. Was allerdings auffällt, ist die überwältigende Präsenz von Cisco bei den Autoren der

Drafts. Offensichtlich ziehen Cisco-Mitbewerber wie Juniper - wenn überhaupt - ein bisschen widerwillig mit.

Vor diesem Hintergrund ist noch nicht absehbar, ob sich LISP überhaupt durchsetzen wird und, wenn ja, wo die ersten Implementierungen stattfinden werden. In den letzten Jahren und Monaten hat die ehemals dominierende Marktmacht von Cisco nachgelassen, weshalb Cisco diesen neuen Ansatz nicht allein und nicht gegen massive Widerstände und Bedenken durchsetzen kann.

Es ist durchaus möglich, dass LISP zunächst innerhalb von Unternehmensnetzen Anwendung findet, denn LISP-Router sind zu herkömmlichen IP-Routern abwärtskompatibel. Ein LISP-Tunnel wird nur aufgebaut, wenn sich ein LISP-Partner finden lässt. Somit ist eine Mischung aus LISP- und herkömmlichen Routern, d. h. auch eine sanfte Migration möglich. Das ist ein wesentlicher Vorteil. LISP-Experimente können auch klein anfangen. Wenn sie die mit LISP verbundenen Versprechen einhalten, wird es die Nutznießer - das können Benutzer und IT-Verantwortliche in den Unternehmen sein - kaum

interessieren, wie lange es bis zur abschließenden Standardisierung von LISP dauert. Erfolgreiche Technologien sind daran zu erkennen, dass sie sich schneller verbreiten als Standardisierungskomitees arbeiten.

Zusammenfassung

Dieser Beitrag behandelt aktuelle Entwicklungen mit dem Ziel der Minimierung von Latenzen in Netzen. Aus der Sicht des Autors sind Marketing Hypes und Substantielles in der aktuellen Latenzdiskussion vermischt. Der Beitrag ist ein Versuch, auf zwei verschiedenen Ebenen - auf der RZ-internen und auf der WAN-Ebene - die Sachverhalte und Konzepte einzuordnen und zu bewerten. Während bei LAN Switches nach der Prognose des Autors die Diskussion um Ultra-Low Latency bald abebben wird, kann sich im Internet und WAN mit neuen Verfahren wie LISP einiges ändern. Hier ist auch der Handlungsbedarf zu sehen, wenn Cloud Computing, also der Zugriff auf Ressourcen „im Netz“ mit akzeptablen Antwortzeiten funktionieren soll.

Jetzt Leser werden



Der Netzwerk Insider

Der Netzwerk Insider erscheint 12 Mal im Jahr im PDF-Format und informiert Sie per eMail über die Hintergründe aktueller Netzwerk-Technologien. Jeden Monat werden zwei Themen gewählt, über die in ausführlicher Form topaktuelle Insider-Informationen gegeben werden. Der Netzwerk-Insider vertritt die Sichtweise von Technologie-Anwendern und bewertet Produkte und Technologien im Sinne der wirtschaftlichen und erfolgreichen Umsetzbarkeit in der täglichen Praxis. Durch seine strenge wirtschaftliche Unabhängigkeit (keine Hersteller-Anzeigen) kann er es sich leisten, Schwachstellen und Nachteile offen anzusprechen. Der Netzwerk-Insider ist bekannt für seine kritische, herstellernerneutrale und fundierte Technologie-Bewertung.

Bezug des Netzwerk Insiders

Die Verteilung des Netzwerk Insiders erfolgt als persönliche Zustellung via eMail im PDF-Format. Der Bezug dieser Zeitschrift ist eine kostenfreie Dienstleistung für die Kunden von ComConsult. Um in den Verteiler aufgenommen zu werden, müssen Sie sich in den eMail-VIP-Service eintragen lassen.

Technologie Information für ihre Aus-/und Weiterbildung

Primär werden die Insider-Informationen zur Unterstützung unserer Zertifizierungen erarbeitet. Die Ausbildungen erfordern eine intensive Nachbearbeitung der Ausbildungsthemen auch über die Seminare hinaus. Das dafür benötigte Arbeitsmaterial wird von uns bereitgestellt. Mit diesem Konzept schaffen wir die Basis für die professionelle Ausbildung für den beruflichen Erfolg des Teilnehmers.

Hier können Sie sich zum Netzwerk Insider kostenlos und ohne jede Verpflichtung registrieren lassen:
<http://www.comconsult-akademie.de/de/Registrierung.php>