Datenpakete mit **Label**

von Rick Werner

Aktuelle Trends bei Netzwerk-Technologien: MPLS-basierte virtuelle Netze sorgen für eine hohe Sicherheit der Datenübertragung und geringe Investitionskosten. Application Performance Management führt zu einer Reduzierung der Datenlast auf den Leitungen.

Virtuelle Netzwerke (Virtual Private Network – VPN), in denen mit Hilfe von Chiffrier- und Authentifizierungstechniken vertrauliche Daten über ein öffentliches Netz abhör- und manipulationssicher zwischen zwei Kommunikationspartnern ausgetauscht werden können, finden heute bereits vielfach Anwendung in der öffentlichen Verwaltung. In den vergangenen Jahren haben dabei VPN auf Basis des Internet Protocol (IPsec beziehungsweise SSL) als sichere Lösung für komplexe Wide Area Networks (WAN) deutlich an Bedeutung gewonnen.

Ein Trend, der sich hier immer mehr durchsetzt, ist der Einsatz der MPLS-Technologie (Multi Protocol Label Switching). Dabei werden die Datenpakete nicht – wie sonst im Internet üblich – anhand der IP-Adresse weitergeleitet, sondern mit Hilfe von speziellen Labels. Diese vergibt ein Eingangsrouter (Label Edge Router) und fügt sie dem Datenpaket hinzu. Sie sind nur auf der Verbindung zum nächsten Router (Label Switch Router) gültig, der dann aus der Routing-Tabelle die diesem Label zugeordnete Verbindung ermittelt und das ursprüngliche Label durch ein neues ersetzt. Die Weiterleitung des Pakets erfolgt dann nur noch durch das vorher zugewiesene Label über einen sogenannten Tunnel, der Weg wird also durchgeschaltet. Durch die Definition des gleichen Weges für alle Pakete eines Datenstroms liegt bei MPLS, ähnlich wie beim Asynchronous Transfer Mode (ATM), eine verbindungsorientierte Übertragung vor. Dies ist die Grundvoraussetzung für ein Verkehrsmanagement und eine definierte Quality of Service (QoS) sowie die Möglichkeit, Bandbreiten zu reservieren.

Durch die Verwendung der Labels, die ja außerhalb eines MPLS-Netzes keinen Sinn ergeben, wird eine VPN-Funktionalität auf der Netzebene erreicht. Auch eine Trennung der Daten aus verschiedenen VPN ist gewährleistet, selbst wenn dieselben Wege zum Transport durch das Netz verwendet werden. Eine Vortäuschung oder Fälschung der Labels durch einen anderen Teilnehmer ist nicht möglich, da diese Kennungen nur innerhalb des MPLS-Netzes existieren und die Schnittstelle nach außen weiterhin auf Internet Protocol basiert. Neben diesem hohen Maß an Sicherheit ergeben sich weitere wesentliche Vorteile von MPLS-basierten IP-VPN durch geringere Investitionskosten und höhere Flexibilität gegenüber teuren Festverbindungen oder anderen Lösungen.

Ein Beispiel: Bei der Neugestaltung des niedersächsischen Landesdatennetzes (iznNet 2000) wurden die zuvor organisatorisch getrennten Infrastrukturen von allgemeiner Verwaltung, Finanzbehörden und Polizei physisch in einem einheitlichen Netz zusammengefasst. Um der Anforderung nach geschlossenen Benutzergruppen für einzelne Anwenderkreise wie zum Beispiel Polizei, Finanzbehörden und Justizverwaltung Rechnung zu tragen, wurden mehrere Virtual Private Networks eingerichtet. Denn angesichts der sensiblen Daten, die über das iznNet transportiert werden, sollten die einzelnen Bereiche hermetisch voneinander abgeschottet sein.

In sehr großen Netzwerken nimmt die Zeit, die insbesondere die zentralen Router benötigen, um einen bestimmten Subnetzeintrag zu finden oder ihre Einträge zu aktualisieren, sehr stark zu. Für das iznNet wirkte sich zusätzlich die IP-Adress-Struktur negativ aus. Denn sie ist nicht

Web-Service

News und technische Informationen zum Thema Multi Protocol Label Switching bietet das englischsprachige MPLS Resource Center:

- **www.mplsrc.com**

Diesen Link finden Sie auch unter www.kommune21.de.

Wer erzeugt den meisten Traffic im Netz?

geografisch, sondern behördlich ausgerichtet. VPNs lassen sich in einem solchen Netz zwar auch mit Hilfe von Access-Listen, Tunnel-Techniken oder Firewalls realisieren – die Verwaltung der einzelnen virtuellen Netze gestaltet sich jedoch mit zunehmender Teilnehmerzahl sehr aufwändig und ist fehleranfällig. Deshalb hat sich das izn für ein Netzkonzept auf MPLS-Basis entschieden.

Mit Hilfe von MPLS lassen sich erstmals auch in großen Infrastrukturen wie dem niedersächsischen Behördennetzwerk Mechanismen zur Verkehrskontrolle und Sicherung von Dienstqualitäten installieren. Durch diese wichtige Fähigkeit, QoS zu definieren und unterschiedliche Güteklassen für die Sprach-, Daten- oder Videokommunikation anbieten zu können, verbinden MPLS-basierte IP-VPN das Beste beider Technologien: Flexibilität und Geschwindigkeit von IP mit höchster Sicherheit zu transparenten Kosten. In Niedersachsen konnte so mit dem iznNet 2000 eine gute Basis für die Realisierung von vielfältigen E-Government-Anwendungen gelegt werden.

Doch angesichts des rasant steigenden Datenverkehrs stößt auch die beste Netzinfrastruktur an ihre Grenzen. Um den Zeitpunkt für eine Neugestaltung angesichts knapper Kassen in den öffentlichen Verwaltungen möglichst lange hinauszuzögern, hat sich das Application Performance Management (APM) bewährt. Hierbei handelt es sich um einen weiteren wichtigen Trend in der Netzwerk-Technologie, der sich in der letzten Zeit rasant entwickelt hat. Am Anfang eines APM-Projekts steht immer eine umfangreiche Analyse. Dort wird zum Beispiel untersucht, welche Applikationen von wie vielen Usern gleichzeitig genutzt werden. Dabei spielt auch eine wichtige Rolle, ob es sich um geschäftskritische Anwendungen handelt und wer den meisten Traffic im Netz erzeugt. Auch welche Applikationen unter einem besonders hohen Verkehrsaufkommen leiden und wie zum Beispiel das Antwortzeitverhalten in den Außenstellen aussieht, ist entscheidend.

Wenn klar ist, welche Anwendungen wie viel Bandbreite – sowohl im Durchschnitt als auch zu bestimmten Spitzen – benötigen, ist die Frage zu beantworten, ob die Übertragungskapazitäten ausgebaut werden müssen oder andere Wege zur Performance-Steigerung ausreichen. Dabei gilt es zu berücksichtigen, dass viele Anwendungen ursprünglich nur für den Einsatz in lokalen Netzwerken entwickelt wurden und beim Betrieb auf WAN-Strecken mitunter erhebliche Probleme mit sich bringen – etwa in Form von häufigem Session-Aufbau oder einem Datenaustausch mit kleinsten Paketgrößen. Die praktische Folge: Die Anwendungen laufen extrem langsam und die Nutzer beklagen sich über zu lange Antwortzeiten.

Das Application Performance Management führt dabei zu einer erheblichen Reduzierung der Datenlast auf den Leitungen, die im Mittel zwischen 50 und 85 Prozent betragen kann. Dadurch findet in der Regel eine spürbare Applikationsbeschleunigung statt, die sich beispielsweise in kürzeren Antwortzeiten von Anwendungen und schnelleren Backups bemerkbar macht. Oft ist auch eine Kostenreduzierung im Wide Area Network damit verbunden, weil vorhandene Leitungen reduziert werden können oder bei wachsendem Kapazitätsbedarf keine Bandbreitenerhöhung erforderlich ist.

Rick Werner ist Leiter Sales des Unternehmens NK Networks & Services, Hannover und Berlin.