LANline

10,– €

Oktober 2017
22. September

ITP VERLAG

IT ■ Network ■ Datacenter www.lanline.de

Security in der Cloud

Hype um KI und ML für die IT-Sicherheit

Handlungsdruck durch EU-DSGVO

Mit Marktübersicht Verschlüsselung für mobile Endgeräte

Veritas NetBackup 5240 Appliance im Test
Komplettpaket für die Datensicherung

Windows Server 2016 und DNS
Sicherheit per Richtlinie steuern

Schwe… Phy…
M…

Sonderdruck für Netcor
Die Last mit der Last

Blinde Flecken beim SNMP-Monitoring

Die Last mit der Last

Wenn wichtige Geschäftsanwendungen immer wieder haken, obwohl das SNMP-Monitoring grünes Licht zeigt, sind mit hoher Wahrscheinlichkeit TCP-Microbursts beteiligt. Doch die Ursachen dafür sind sicher und effizient zu erkennen.

Seit Wochen klingeln die Telefone am Helpdesk: Mitarbeiter beschweren sich über zäh reagierende Programme und langsame Datenübertragungen. Doch das SNMP-Monitoring des Applikations- und des Netzwerks-Performance-Teams zeigt keine Probleme an. Keine Ereignisse, die sich mit den gemeldeten Zeiträumen korrelieren lassen. Was ist da los?

SAP, Citrix, Exchange, Excel, Word etc. – nahezu alle geschäftswichtigen Anwendungen nutzen TCP, etwa um zwischen Unternehmenszentrale und Zweigstelle Daten auszutauschen. Die Auslastung des Rechenzentrums und der Übertragungsstrecke überwachen IT-Verantwortliche in der Regel mittels SNMP-Monitoring. Das Simple Network Management Protocol hat man entwickelt, um Netzwerkelemente zentral überwachen zu können.

Die Überlegung dahinter ist folgende: Wenn SNMP kein übermäßiges Ausnutzen der verfügbaren Bandbreite feststellt, kann das Netzwerk nicht Ursache für auftretende Performance-Probleme sein. Doch diese Rechnung geht nicht auf. Häufig erkennt SNMP keine Fehler, und trotzdem reagieren Business-Apps zäh wie Kaugummi. Wenn auch der Server keine übermäßige Auslastung meldet, ist guter Rat teuer. Besonders sporadisch auftretende Probleme treiben IT-Verantwortlichen den Schweiß auf die Stirn. Schnell taucht die Frage auf, ob die überwachten Parameter eigentlich relevant für die Applikations-Performance sind. Ist SNMP überhaupt in der Lage, Hilfestellung zu geben?

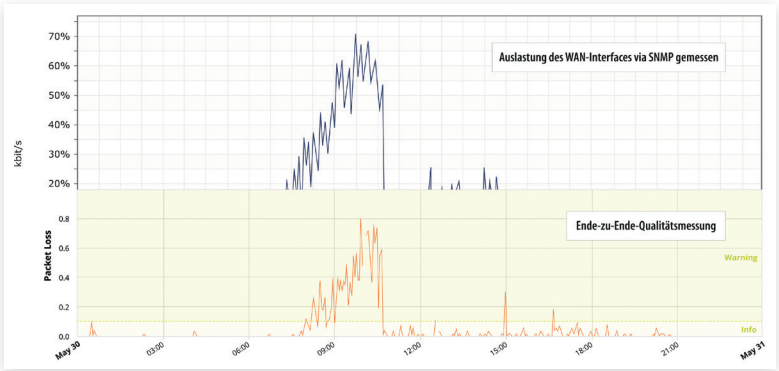
SNMP misst Quantität, nicht Qualität

Werfen wir einen Blick in eine typische IT-Zentrale: Mitarbeiter setzen Tools wie MRTG, PRTG oder Nagios ein, um per SNMP Kennzahlen der Komponenten auszulesen – typischerweise die Auslastung von Interface, CPU und Speicher. Mit Ping-Tests ermitteln sie die Erreichbarkeit von TCP-Ports und deren Antwortzeiten.

Anhand der Ergebnisse beurteilen sie die Qualität des Netzwerks oder besser: dessen Quantität und Verfügbarkeit. Lediglich die Ping-Werte sind echte Qualitätskriterien. Ähnlich wie Laufzeit, Jitter und Paketverlust – doch die erfasst SNMP nicht.

Besonders Paketverluste erweisen sich als Performance-Killer. Bereits bei Verlustraten von 0,5 Prozent spüren Anwender Beeinträchtigungen – zum Beispiel wenn Applikationen verzögert auf Klicks oder Tastatureingaben reagieren. Steigen die Paketverluste weiter, etwa auf zwei bis fünf Prozent, beschweren sich Nutzer nachdrücklich über schlechte Performance.

Wie kann es sein, dass sich eine auf den ersten Blick so geringe Fehlerrate stark auf die Leistung auswirkt? Um das zu verstehen, lohnt eine detaillierte Betrachtung der Übertragungsmechanismen von TCP.



GeNiEnd2End zeigt Paketverluste, die SNMP übersieht – und eine deutliche Korrelation mit der Auslastung. Bild: Netcor

Retransmission: TCP gibt kein Paket verloren

Die Performance der meisten Netzwerkanwendungen hängt zum großen Teil von TCP ab. Ein Grund dafür ist die Art und Weise, wie TCP mit Paketverlusten umgeht. Das Protokoll nutzt zwei Mechanismen, mit denen es fehlende Pakete nachordert: „Fast Retransmission“ und „Retransmission Time-out“ (RTO). Beim Aufbau einer TCP-Verbindung handeln beide zunächst die Größe des Empfangspuffers (Receive Window) aus. Im weiteren Verlauf und nach dem erfolgreichen TCP Slow Start schiebt der Sender Blöcke an Datenpaketen ins Netzwerk und wartet auf die Empfangsbestätigung in Form von ACK-Paketen. Anhand der Sequenznummern kann der Empfänger erkennen, ob alle Pakete eines Blocks eingetroffen sind. Fehlt ein Paket, bestätigt der Empfänger mit jedem weiteren empfangenen Paket das fehlende Paket (DUP-ACK). Schickt der Sender maximal 20 ms nach dem letzten empfangenen DUP-ACK das fehlende Paket, spricht man von einer Fast Retransmission. Diese hat keine nennenswerten Auswirkungen auf die TCP-Verbindung und die Performance des Netzwerks.

Problematisch wird es, wenn das letzte Paket eines Blocks verloren geht oder nur ein Paket gesendet wird. Da der Sender keine Bestätigung erhält, wartet er und schickt das Paket noch einmal. Diese Wartezeit heißt Retransmission Time-out. TCP berechnet sie dynamisch. Beim Initialisieren einer Verbindung liegt sie bei rund drei

Sekunden. Abhängig von der ermittelten Paketlaufzeit passt das Protokoll den RTO mit jedem ACK an.
TCP halbiert zudem das Congestion Window (Cwnd) und initialisiert die TCP-Anwendung neu per Slow-Start. Der RTO und die resultierenden Konsequenzen führen zu einem für Anwender spürbaren Einbruch der Performance.

Wie entstehen Paketverluste?

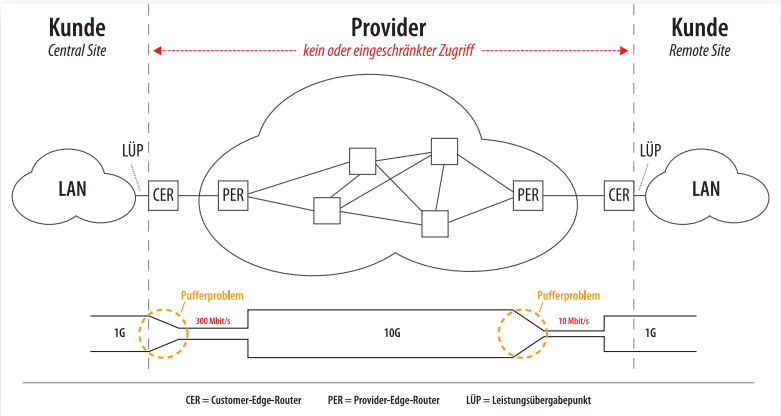
TCP arbeitet grundsätzlich „bursty“: Es schiebt große Datenmengen binnen Millisekunden ins Netzwerk. Diese Microbursts können kurzfristig die gesamte Bandbreite im Sender-LAN ausfüllen. Was in hochperformanten LAN-Umgebungen unproblematisch ist, führt an WAN-Übergabepunkten zum Teil zu massiven Paketverlusten. Der Grund: Die Gateways, meist Router, müssen den Traffic aus dem LAN in die WAN-Verbindung einfädeln. Diese hat jedoch weit weniger Bandbreite. Also muss das Gateway den blitzartig auftretenden Datenüberschuss im Interface zwischenspeichern.
Wenn mehrere Clients zeitgleich senden, was bei großen Abteilungen mit vielen Mitarbeitern häufig vorkommt, addieren sich ihre Bursts. Die Schnittstelle befindet sich in einer permanenten Überlastsituation. Ist ihr Puffer zu klein, gehen Pakete verloren. Oft erfolgt die Flusskontrolle dann auf Basis von RTO – der denkbar schlechtesten Option.
Dabei verfügt TCP mit „TCP Self-Clocking“ über eine effiziente Datenflusssteuerung, mit der sich Paketstaus entschärfen und Bandbreiten optimal nutzen lassen. Sie funktioniert so: An einem Übergang von hoher zu niedriger Bandbreite werden die ankommenden Paketblöcke bildlich in die Breite gequetscht, was einer längeren Übertragungszeit entspricht. Entsprechend folgen die ACKs in größerem zeitlichen Abstand aufeinander.
Gelangen diese Pakete wieder in eine Leitung mit höherer Bandbreite, übernimmt TCP die größeren Intervalle. Der Abstand zwischen den Paketblöcken ist im Empfänger-LAN also deutlich größer als im Sender-LAN. Anhand der ACKs erkennt der Sender die Diskrepanz und schickt die nächsten Pakete in größerem zeitlichem Abstand – er synchronisiert sich also mit dem Empfänger. Das führt zu einer gleichmäßigeren Auslastung am kritischen Interface. TCP Self-Clocking arbeitet dann effizient, wenn keine Pakete verloren gehen und somit kein RTO auftritt. Das setzt jedoch ausreichend große Pufferspeicher – auch Queues genannt – an den Schnittstellen voraus.

Die Wolke außerhalb des eigenen Hoheitsbereichs

Router bieten die Möglichkeit, die Queue-Länge einzustellen. Das Erhöhen wäre in vielen Fällen eine probate Lösung, um Paketverluste trotz TCP-Microbursts dort zu vermeiden, wo eine Verjüngung der Bandbreite stattfindet. Doch die eigene IT-Abteilung hat meist keinen Zugriff auf diese Router, da sie sich im Verantwortungsbereich des Providers befinden.
Ein Beispiel: Eine Zweigstelle ist per WAN mit dem Unternehmensnetzwerk der Zentrale verbunden. Bereits der Customer-Edge-Router (CER) am WAN-Übergabepunkt der Unternehmenszentrale befindet sich im Hoheitsbereich des Providers. Die Bandbreite verjüngt sich hier von 1 GBit/s auf beispielsweise 300 MBit/s. Mit dieser Geschwindigkeit führt die Übertragung über einen Provider-Edge-Router (PER) weiter in die „Wolke“ – einen Infrastrukturverbund des Providers. Die Übertragung in dieser Wolke erfolgt meist via MPLS mit Bandbreiten von 10 GBit/s oder mehr. Dieser Vorgang ist für Kunden völlig transparent. In Richtung Filiale verjüngt sich die Bandbreite im PER am Ausgang der Wolke nochmals auf etwa 10 MBit/s. Ein weiterer CER koppelt schließlich die Zweigstelle an.
Bei Traffic in Richtung Filiale erfolgt somit zweifaches Queueing: einmal am CER und einmal am PER. Bereits auf CER haben viele Kunden, wenn überhaupt, nur sehr begrenzten Zugriff, etwa um per SNMP-Interface Statistiken auszulesen. PERs bleiben für sie komplett unsichtbar. Kurzum: Der Kunde kann nicht per SNMP erfassen, ob an den kritischen CERs und PERs Queueing-Probleme und Paketverluste auftreten. Und ob der eigene Provider bereit ist, die Puffergröße anzupassen, hängt vom Vertrag ab.

SNMP-Messung vs. Realität

Schon geringe Paketverlustraten können die Applikations-Performance erheblich verschlechtern. SNMP bleiben sie verborgen: einerseits, weil diese Kennzahl (Outgoing Queue Drop) oft gar nicht abgefragt wird; andererseits, weil SNMP viel zu grob auflöst. In den meisten Fällen ist es bestenfalls auf ein Abfrageintervall von 60 Sekunden eingestellt.



An den Übergängen zwischen dem eigenen Netz und dem des Providers gibt es Bandbreiten-Flaschenhälse und dadurch Pufferprobleme.
Bild: Netcor

Ein Beispiel verdeutlicht den Zusammenhang. Ein TCP-Microbursts dauert oft nur rund 5 ms. In einer Sekunde können also bis zu 200 Microbursts auftreten, die die Bandbreite kurzfristig auslasten. Im betrachteten Zeitraum zeigt Wireshark bei einer Auflösung von 10 ms tatsächlich viele Peaks mit bis zu 1,2 MBit/s, die nur 10 bis 20 ms lang sind.
In einer Minute, der üblichen Minimalauflösung von SNMP, können bis zu 12.000 solcher Events auftreten. Doch SNMP

nimmt in diesem Zeitraum lediglich zwei Messwerte auf und bildet den Mittelwert daraus. Die Wahrscheinlichkeit, dass das Monitoring Microbursts übersieht, liegt damit praktisch bei 100 Prozent. SNMP zeigt also nicht die realen Verhältnisse der betrachteten IT-Umgebung.

Lösungswege: Sehen, was wirklich passiert

IT-Verantwortlichen bieten sich zwei – kombinierbare – Möglichkeiten an, um reale Paketverluste zu ermitteln und so Performance-Problemen auf die Spur zu kommen: Drop-Counter an den Routern auslesen und Ende-zu-Ende-Messungen der Übertragungsqualität durchführen.

Auch wenn viele die Funktion nicht nutzen – SNMP kann Drop-Counter auslesen. Router und andere Netzwerkkomponenten halten mit diesen Zählern fest, wie viele Pakete sie verworfen haben. Der Wert ermöglicht Rückschlüsse darauf, ob und wie oft beispielsweise die Queues des genutzten CERs oder PERs überlaufen. Dafür ist allerdings ein Zugriff auf diese Router nötig – vielen Unternehmen bleibt dieser Weg daher versperrt.

Eine effiziente Methode zum realistischen Erfassen der Qualität ist eine Ende-zu-Ende-Messung mithilfe eines spezialisierten Software-Tools wie GeNiEnd2End. Sie funktioniert unabhängig von der IT-Infrastruktur auch über LAN- und WAN-Übergänge hinweg. Mit GeNiEnd2End lässt sich mit geringem Aufwand die gesamte Übertragungsstrecke von der Unternehmenszentrale zur Filiale überprüfen.

Faktencheck statt Stochern im Nebel

Bei Problemen mit der Applikations-Performance ist die erste zu klärende Frage: Lässt sich das Netzwerk als Verursacher sicher ausschließen? Gängige SNMP-Monitoring-Werkzeuge müssen hier passen, da sie fast nur quantitative statt qualitative Kennzahlen liefern.

Nur eine Ende-zu-Ende-Messung auch über Geräte außerhalb des eigenen Hoheitsbereichs hinweg kann klar aufzeigen, ob zum Beispiel Paketverluste in definierten QoS-Klassen (Quality of Service) auftreten. Eine Messung mit einem Tool wie GeNiEnd2End lässt sich sofort einrichten und ermöglicht rund um die Uhr eine feingranulare Bestandsaufnahme der Netzwerkqualität.

Die Ergebnisse liefern IT-Verantwortlichen stichhaltige, belastbare Argumente gegenüber ihren Providern, wenn beispielsweise Paketverluste zeitlich mit schlechter Applikations-Performance korrelieren. Gemeinsam lässt sich dann eruieren, ob und wo es Potenzial für eine Optimierung gibt.

Henrik Wahsner/ts

Henrik Wahsner ist Senior Berater Netzwerkanalyse bei Netcor, www.netcor.de.