BURSTS ERKENNEN UND VERMEIDEN

Ein modernes Netzwerk ist ein wahrer Lastenesel. Trägt es doch die verantwortungsvolle Aufgabe, sich um die Produktivität des Unternehmens zu kümmern. Zudem schultert es eine Vielzahl an unterschiedlichen Geräten und Diensten. Doch so heterogen heutige Netzwerke auch sind, so reglementierend kann sich im Gegenzug das physische Netzwerkkabel auf das Netzwerk auswirken.

Autor: Klaus Degner **Redaktion: Axel Pomper**

➤ Das Netzwerkkabel kann exakt nur die Zahl an Bits übertragen, für die es ausgelegt ist. Der Switch oder Router hat dann beim LAN-Uplink den Job, den ankommenden Netzwerkverkehr zu verarbeiten und an die niedrigere Bandbreite anzupassen. Wenn dabei mehrere Datenpakete gleichzeitig ankommen, kann der Switch nicht über sich hinauswachsen, sondern nur ein Paket nach dem anderen weitergeben. Pakete gehen verloren.

Spitzen- vs. Durchschnittslast

Allein diese Diagnose reicht dem Systemadministrator allerdings nicht aus, um eine valide Problemlösung herbeizuführen. Denn Paketverluste können sporadisch vorkommen – was ganz normal ist – oder aber häufiger auftreten. Zudem macht es einen großen Unterschied, ob das Netzwerk die ganze Zeit auf Volllast fährt oder ob es lediglich vereinzelt zu einem ungewöhnlichen Konglomerat an Verkehrsvolumen kommt.

Bei einer maximalen Belastung im Netzwerk will der IT-Profi wissen, wann diese vorherrscht, wie lange und wie oft es zu einer solchen Volllast kommt und von welchen Netzteilnehmern sie verursacht wird. Erst diese Erkenntnisse erlauben es ihm, Vorkehrungen für einen reibungslosen Netzwerkverkehr zu treffen.

Auswirkungen von Bursts auf das Netzwerk

Wie solche Bursts näher untersucht werden können, soll zunächst hintangestellt werden. Denn zunächst gilt es die Frage zu klären, wie sich das Netzwerk bei Bursts verhält. Paketverluste und Retransmissions gehören zur Normalität. Besteht denn überhaupt Handlungsbedarf?

Ja und nein. Paketverluste gehören zum Netzwerk wie das Amen in der Kirche. Aber nehmen sie eine Größenordnung an, die sich negativ auf die Performance auswirkt. Am besten lassen sich die Auswirkungen auf das Netzwerk beleuchten, indem die Datenübertragungsprotokolle auf der einen und die Dienste mit Bedarf an einer gesicherten Bandbreite auf der anderen Seite betrachtet werden.

Bei den wichtigsten Protokollen wie etwa HTTP oder DNS wirkt sich eine Überlast zwar nicht verheerend aus, IT-Verantwortliche sollten sie auf Dauer aber dennoch beheben. Als Beispiel dient ein Webseitenaufruf, bei dem schnell mehrere Dutzend DNS-Abfragen gestellt werden. Gehen davon nur fünf Prozent verloren, die im Anschluss neu gesendet werden, verzögert sich der Aufruf um mehrere Sekunden. Zu lange für das heutige Userverhalten.

Kritischer wirkt sich eine Überlast auf Dienste aus, die auf eine garantierte Bandbreite angewiesen sind. Kommt es zu einer Überlast, fällt der jeweilige Dienst komplett aus. In enem Unternehmen, das die Mitarbeiter gerade per Online-Kurs einarbeitet, wäre das der GAU.

Bursts richtig einordnen

Oft genügt es nicht, wie zuvor angesprochen, bei solch einer Analyse allein die Durchschnittslast in dem betroffenen Zeitintervall zu kennen. Zeigt diese beispielsweise, dass es auf einer Ein-GBit/s-Leitung im Minutenmittel 100 MBit/s Verkehr gibt, lässt sich keine Aussage darüber treffen, ob der Link zu zehn Prozent der Zeit komplett ausgelastet oder ob gleichmäßiger Verkehr den Link kontinuierlich zu zehn Prozent füllt. Um bei schlechter Netzwerkperformance kluge Anpassungsvorschläge machen zu können, kommt es zusätzlich auf einen bestimmten Wert an: wie viel Prozent der Zeit der Link unter Volllast lief. Liegt der Wert bei null Prozent, lassen sich Probleme auf Basis von Bandbreitenüberlast ausschließen. Liegt der Wert höher, ist das Netz überlastet, sei es punktuell oder flächendeckend.

Was genau das Zuviel an Last verursacht, ist mit intelligenten Monitoring-Lösungen schnell erkannt. Typische Ursachen für einen LAN-Burst sind etwa Back-ups, ein großer Dateitransfer oder ein Windows-Update, das kurzfristig LAN oder WLAN ans Limit treibt.

Dabei handelt es sich um normale Vorgänge, die in vielen Fällen überhaupt kein Problem darstellen. Zum Problem werden sie nur dann, wenn plötzlich mehrere dieser Dienste parallel Bandbreite beanspruchen. Zum Beispiel am Montagmorgen, wenn die Smartphones der Mitarbeiter im WLAN automatisch ihre Updates fahren und hohe Traffic-Raten verursachen. Dann streiten sich die Dienste um

Bandbreite. Kommt eine weitere Anwendung wie ein Telefonat hinzu, kann dieses nicht mehr reibungslos funktionieren. Sobald jedoch klar ist, was für die Überlast verantwortlich ist, können geeignete Maßnahmen ergriffen werden.

Analyse im Millisekundenbereich

Eine entsprechende Burstanalyse ist in vielen Fällen die lösungsorientierteste Variante. Ein Beispiel: Ein Telekommunikationsanbieter, der seinem Kunden ein bestimmtes Bandbreitenpaket verkauft und entsprechend zur Verfügung stellt. Klagt der Kunde anschließend über Bandbreitenengpässe, hilft eine Burst-Analyse, genaue Angaben über das Traffic-Aufkommen zu treffen. In solch einem Bereich ist es wünschenswert, eine Detailtiefe dargestellt zu bekommen, die über das übliche Minuten- oder ein 30-Sekunden-Intervall hinausgeht.

Ein anderer Fall ist die Voice-Telefonie. Die Datenübertragung per SIP/RTP erfolgt mit einer Rate von einem Paket alle 20, 25 oder 30 Millisekunden. Um Abweichungen zwischen gesendeten und empfangenen Daten – der häufigsten Ursache für verschluckte Buchstaben – auf die Spur zu kommen, bedarf es einer Burst-Analyse im Millisekundenbereich. Erst diese zeigt, ob die Leitung tatsächlich für einige Millisekunden überlastet war. Liegen die Analyseergebnisse lediglich im Minutenbereich vor, würden die Fehler nicht erkannt und somit auch nicht behoben werden können.

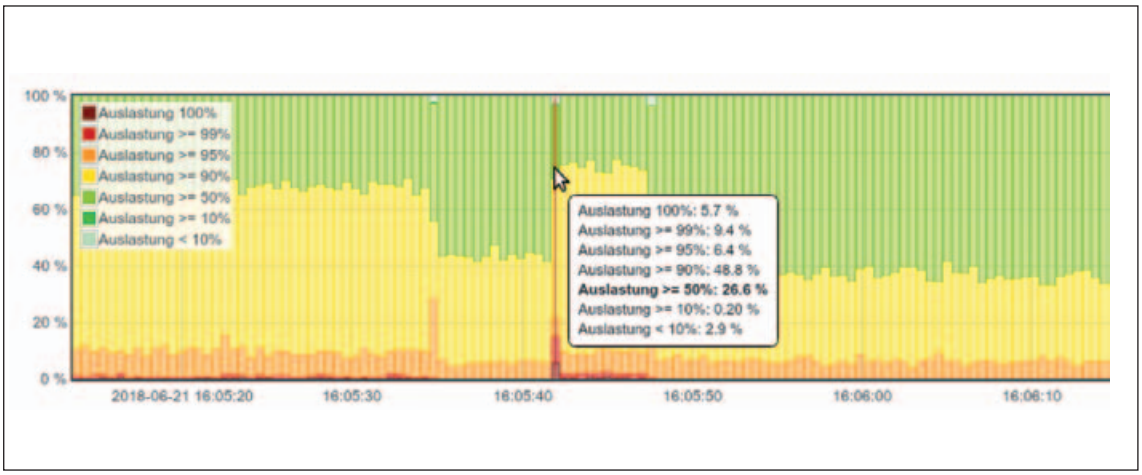
Ein weiterer Anwendungsfall, bei dem eine Qualitätsauswertung im Millisekundenbereich notwendig wird, sind kritische Dienste. Während manche Anwendungen nach dem Prinzip des Best-Effort funktionieren, also so schnell wie möglich, sind andere Dienste extrem zeitkritisch. Der Vergleich zwischen E-Mail und Voice-Telefonie verdeutlicht dies: Beim Versenden einer E-Mail ist es in den meisten Fällen kaum von Belang, ob sie dafür eine oder drei Sekunden benötigt. Beim VoIP-Telefonat ist es hingegen sehr kritisch. Hier sollten die Pakete möglichst alle im konstanten, kurzen Zeitintervall ankommen.

Gerade bei der Voice-Telefonie, aber auch bei allen anderen zeitkritischen Anwendungen, kommt es wesentlich darauf an, das Netzwerk millisekundengenau debuggen zu können. Inzwischen sind Monitoring-Tools auf dem Markt erhältlich, die dem Systemadministrator diese Qualitätsmerkmale liefern sollen.

Vorgehensweisen bei Lastspitzen

Hat eine Analyse der Netzwerkprobleme tatsächlich Bursts als Ursache ans Tageslicht gebracht, besteht für den Administrator Handlungsbedarf. Doch welche Strategie ist die richtige? Gilt es, einfach die Bandbreite des Links zu erhöhen und alle Probleme sind gelöst? Wie verhält sich beispielsweise ein System mit 10G-Netzwerkanschluss, wenn das dahinterliegende 1G-Netzwerk auf 10G erhöht wird?

Folgendes Beispiel soll den Fall erläutern: Ein Link ist mit zehn Gbit/s voll ausgelastet und zwei mit 10G angeschlossene Server sind so konfiguriert, dass die Back-ups neu starten, sobald die letzte Sicherung endet. Um die volle Auslastung des Links zu entschärfen, wird daraufhin der Link auf 40G aufgerüstet, was mit großem Aufwand und hohen Kosten verbunden ist. Als die Beteiligen das Projekt abschließen, zeigte sich, dass der Link jedoch ebenso ausgelastet ist wie zuvor. Eine neuerliche Analyse bringt anschließend ans Tageslicht, dass sich das Problem an den dahinter liegenden Clustern finden lässt. Diese sind mehrfach mit 10G angeschlossen. Der Link, der vorab mit zehn Gbit/s voll ausgelastet war, erzeugte nach dem Upgrade so viel Traffic, dass auch der 40G-Link keine Kapazitäten mehr hatte. Die Backups liefen in vierfacher Geschwindigkeit.



Grafik: Allegro Packets

Analyse der Netzwerkperformance

Das teure Upgrade wäre also nicht notwendig gewesen, eine dezidierte Burst-Analyse hätte dies im Vorfeld erkannt. Denn neben der Dauer der Peaks stellt sie unter anderem auch dar, welche Netzwerkteilnehmer die Bursts eigentlich verursachen. Sie erkennt, welche Dienste den Link sättigen. Statt eines Link-Upgrades hätte es genügt, deren Geschwindigkeiten zu drosseln.

Leidet eine Netzwerkarchitektur unter Bursts, ist ein Upgrade also nicht immer die richtige Verfahrensweise. Mitunter ist es ratsam, stattdessen das System auf das Prinzip Quality of Service umzustellen. So kann den einzelnen Diensten eine entsprechende Bandbreite zugeordnet werden. Eine weitere Alternative ist eine logische oder physische Trennung der Dienste. So können Verantwortliche beispielsweise dem Telefonnetz eine hohe Priorität oder eine gänzlich eigene Leitung zuordnen.

Wer also nach einer Universallösung sucht, wie ein Netzwerk bei voller Auslastung zu behandeln ist, wird leider enttäuscht. Sind die Ursachen der Bursts aber hinlänglich bekannt, ist die Entscheidung über den Lösungsweg wesentlich einfacher.

Klaus Degner ist Geschäftsführer von Allegro Packets