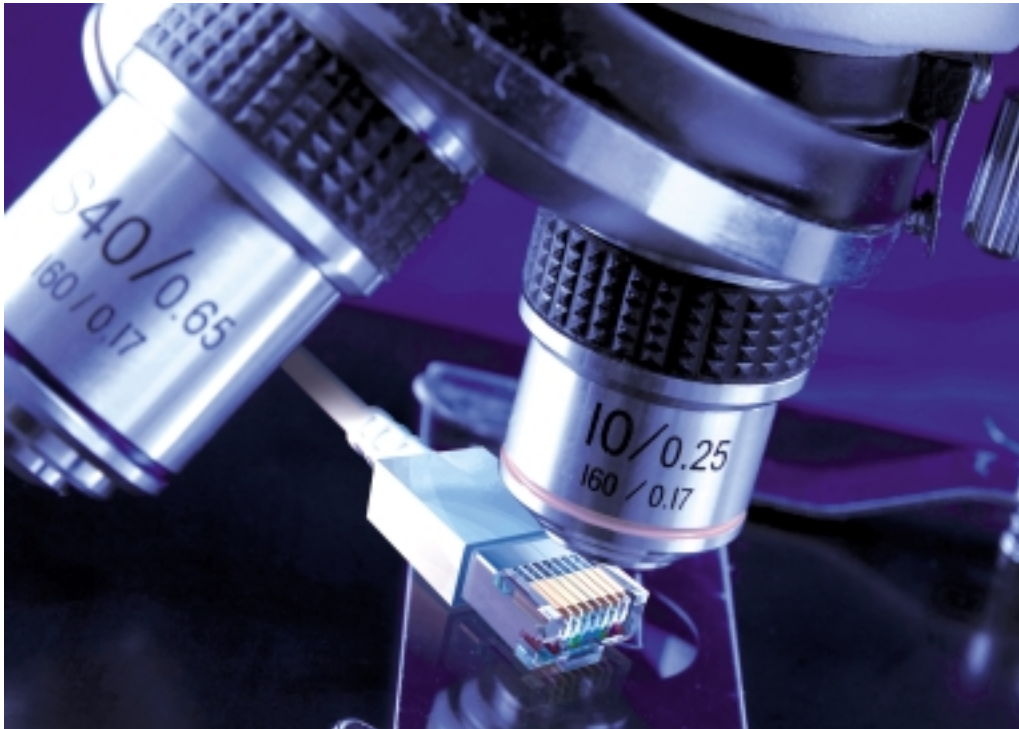


Tiefe Einblicke

Von Ales Mahler und David Eser

Bild: funkschau



Analyse-Werkzeuge sorgen unter anderem dafür, dass das Verständnis für innere Netzwerkläufe geschaffen wird. Dadurch erfahren die Administratoren, wie das Netzwerk im Normalzustand zu arbeiten hat, und können im Fehlerfall schneller und effizienter Probleme eingrenzen und lösen. Durch die regelmäßige Netzwerkanalyse entwickelt sich der Admin im Lauf der Zeit zum Netzwerkspezialisten. Leider wird häufig ein anderer Ansatz gewählt, und portable oder frei erhältliche Tools werden erst im Fehlerfall eingesetzt. Das führt dazu, dass Probleme nicht im ersten Schritt gelöst werden können, da die mangelnde Erfahrung mit diesen Tools und mit der Netzwerkanalyse oftmals nicht zum gewünschten Erfolg führt. Dies resultiert häufig in einer ungerichteten Abstufung der Netzwerkanalyse als komplex und schwer einsetzbar.

Ales Mahler arbeitet als Regional Sales Manager für Zentral- und Osteuropa bei Network Instruments.

David Eser ist als Sales Manager bei Psiber Data tätig, dem Distributor von Network Instruments.

Monitoring- und Analysesysteme verwenden verschiedene Netzwerkdienste. Darunter zählen Technologien wie SNMP, RMON, Netflow und die vom Analysesystem selbst erfassten Datenströme. Idealerweise sollten diese Technologien parallel verwendet werden, da sie sich gegenseitig ergänzen. Aktive Hardware, also zum Beispiel Router oder Switches, geben über das SNMP-Protokoll wichtige Netzwerkparameter wie Fehler auf OSI-Ebene 2, defekte oder zu lange/kurze Pakete, Kollisionen, Auslastung und Broadcast an das Analysesystem weiter. Eine zentrale SNMP-Managementkonsole sammelt über Fernabfragen entsprechende Netzwerkstatistiken und liefert eine Übersicht der Netzwerkengpässe, Broadcasttraffic, defekte Netzwerkkarten oder Hinweise auf Auto-Negotiation-Probleme. Neuere Technologien wie Netflow und Sflow dienen dazu, Applikationen genauer zu analysieren. Falls Netzwerkengpässe auftreten, verarbeitet Netflow/Sflow Informationen der Switches/Router und zeigt dadurch weitere Details des Problems an: Welches Protokoll beziehungsweise welche Applikation wur-

Probleme mit dem Durchsatz, Beschwerden der Anwender und Ausfallzeiten im Netzwerk können durch richtig angewendete Netzwerkanalyse und Überwachung vermieden werden und tragen damit zu Kostenreduktion und erhöhter Produktivität bei.

den verwendet und wer ist der Verursacher? Ist die Infrastruktur des Netzwerks nicht in der Lage entsprechende Parameter zu liefern, hilft ein direkter Anschluss des Messgeräts an den Switch mit entsprechender Portspiegelung. Aus Kostengründen ist es in der Regel nicht möglich, jeden Switch mit entsprechender Messtechnik auszustatten. Dies bedeutet für den Administrator aber auch, dass nur durch ein gut überlegtes Analysekonzept mit entsprechend geplanten Messpunkten eine kosteneffiziente und ganzheitliche Lösung möglich ist.

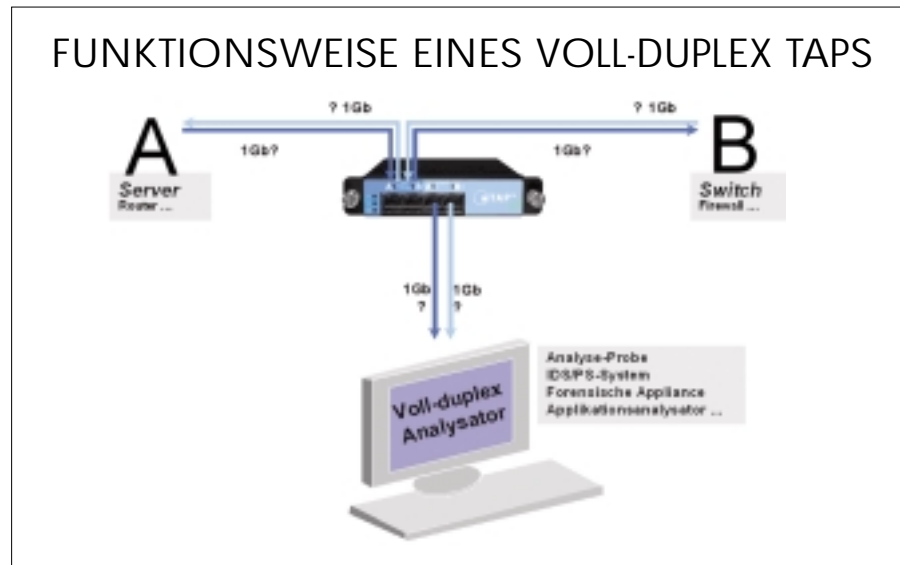
Proaktives oder reaktives Analysekonzept

Da heutige Netzwerke zunehmend stärker zentralisiert sind und die Netzwerkanwender auf Applikationen zugreifen, die sich in zentralen Serverfarmen befinden, ist ein proaktiver Analyse- und Monitoring-Ansatz sinnvoll. So sollten Analyse-Tools permanent an wichtigen Core-Verbindungen, die zu den Server-Farmen oder zu den Routern führen, installiert werden. Es können damit alle Anfragen zu Applikationsservern beziehungsweise der Datenverkehr ins WAN und von verteilten Netzen beobachtet werden. Neben den Informationen zu den größten Verursachern von Netzwerkauslastung können auch Verbindungs- und Performance-Probleme beobachtet werden.

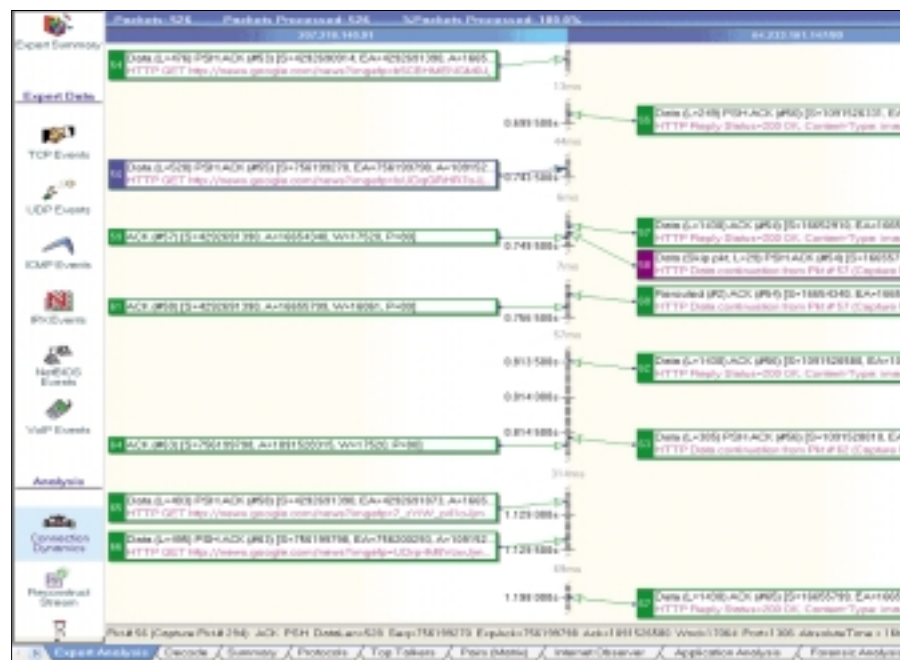
Sich verschlechternde Antwortzeiten können dabei bereits im Vorfeld erkannt werden, lange bevor es die Anwender merken. Ursachen dieser Probleme lassen sich dann im Detail untersuchen, und in den meisten Fällen ist es nachweisbar, dass diese gar nicht immer durch das Netzwerk hervorgerufen werden. Eine Echtzeit-Expertenanalyse ermöglicht das genaue Verhalten vom Server zu Client und Client-Gruppen, wie auch zwischen den Clients zum Server oder allen übrigen Servern zu messen. Außerdem kann es den Paketverlauf jeder einzelnen Übertragung übersichtlich anzeigen, wodurch man genau ersehen kann, wo die Ursache der schlechten Antwortzeiten liegt. Dabei kann es sich wie in vielen Fällen lediglich um einen langsamen Client handeln, denen heute immer mehr abverlangt wird, so dass diese kurzfristig zum Stillstand kommen und Probleme wie TCP-Retransmissions oder Zero-Windows verursachen. In anderen Fällen, was gravierender ist, entdeckt man einen langsamen Server, der aufgrund seiner Aufgaben oder Anzahl und Art der Anfragen überlastet ist und notfalls ein Upgrade benötigt.

Applikations-Antwortzeit und Netzwerk-Laufzeit

Bei der Betrachtung der Antwortzeiten ist es wichtig darauf zu achten, ob auf OSI Ebene 4 (TCP-Ebene) oder auf Ebene 7 (Applikationsebene) analysiert wird. Bei Antwortzeiten auf der TCP-Ebene werden die Zeiten eines Handshakes (wie lange es dauert, bis Pakete quittiert werden), von der Analysesoftware ausgewertet. Wird die Antwortzeit dagegen auf der Applikationsebene gemessen, so wird dort die Applikationsanfrage und -antwort betrachtet. Diese wiederum enthalten etliche Acknowledgements und zudem viele untergeordnete Abfragen (Application Turns). So kann der Aufruf einer Webseite zwar für den Client als eine Anfrage zu verstehen sein, im Hintergrund können jedoch etliche Webseiten-Elemente und Bilder mit einzelnen Unterabfragen vom Client angefordert werden, ohne dass es der Anwender bemerkt. Bei der hohen Anzahl von standardmäßigen wie auch nicht standardmäßigen Applikationen in Unternehmen, auf die entweder ‚remote‘ oder über das lokale Netzwerk zugegriffen wird, sind diese Details für das Netzwerk- und Applikationsdesign durchaus entscheidend. Durch jeden zusätzlichen ‚Application-Turn‘ wird die Netzwerk-Laufzeit um den gleichen Wert ansteigen, obwohl sie einzeln betrachtet akzeptabel er-



Moderne TAPs (voll-duplex) unterstützen den vollen Netzwerkverkehr. Das bedeutet, sie können bis zu 1 GBit/s in jede Richtung analysieren



Dieses Beispiel zeigt die Darstellung einer Anfrage zu einer Webseite mit mehreren Unterabfragen (Application Turns) mit Observer von Network Instruments

scheint. Die lokale Server-Client-Kommunikation mag sich dabei ganz unauffällig verhalten, aber für den Netzwerkanwender, der remote über ein WAN zugreift, ist der Frustrationsgrad bei zwanzig oder mehr Applikation-Turns entsprechend hoch.

Leider ist in letzter Zeit der Trend zu beobachten, dass die Zahl der Application Turns vieler Anwendungen wie etwa Web-basierender Anwendungen und Datenbank-Clients ansteigt und auch populäre Applikationen wie Microsofts Exchange über WAN recht ineffizient arbeiten. Eine

Untersuchung mit entsprechenden Analysetools enthüllen diese Ineffizienz.

Sieht man Probleme, die sich nicht auf einzelne Clients und Server beziehen, ist eine Analyse der allgemeinen Netzwerklaufzeit sinnvoll. Laufzeiten im lokalen Netzwerk von weniger als 10 ms gelten in der Regel als normal. Falls Netzwerkanwender über das WAN zugreifen, müssen natürlich andere Anforderungen an die Laufzeiten gelten. In der Praxis spielen nicht die absolute Laufzeit selbst, sondern eher hohe Laufzeitschwankungen und Pa-

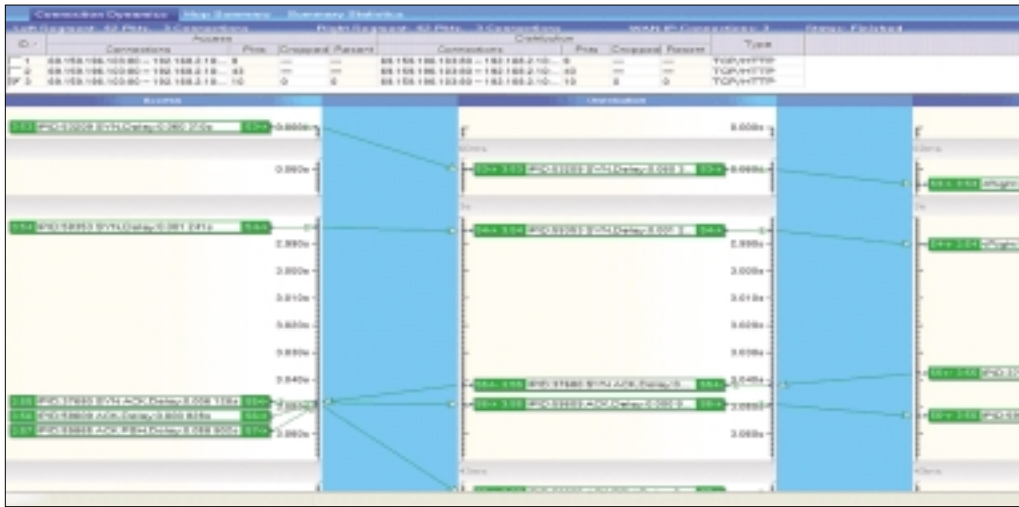


Bild: Network Instruments

Eine synchronisierte Messung über vier Messpunkte mit Observer von Network Instruments

ketverluste, vor allem bei Echtzeit-Applikationen wie VoIP, eine wesentlichere Rolle. Beim Paketverlust kommt es im Falle von TCP-Daten zu Retransmissions, bei UDP zu erneuter Übertragung auf höheren OSI-Schichten. Bei VoIP kommt es nicht zu einer erneuten Übertragung der UDP-basierenden RTP-Pakete (Real Time Protocol), aber das RTCP-Kontrollprotokoll sendet eine Statusmeldung, dass Paketverlust und Laufzeitschwankung (Jitter) ansteigt. Da man meist nicht direkt auf der WAN-Strecke Parameter wie Paketverlust messen kann (da es sich um Bereiche des Providers handelt, auf die man keinen Zugriff hat), hilft dazu eine Synchronisation der Messungen vor und nach dem jeweiligen Router, wie etwa bei der Multihop-Analyse. Dadurch ermittelt der Administrator die tatsächliche Laufzeit und Laufzeitschwankungen zwischen Messpunkten und kann somit auch Paketverluste nachweisen.

Retrospektive Analyse

In der Praxis werden die meisten Probleme von den Netzanwendern erst später gemeldet. Da viele dieser Probleme nicht permanent oder reproduzierbar auftreten, ist es sehr schwierig, diese zu erfassen und einzugrenzen. Sehr oft wird eine ausführliche Analyse unterlassen und verschiedene Performance-Probleme bleiben oftmals ungelöst. Ähnlich ist es mit den unterschiedlichen Alarmen, die das Monitoring-System liefert. Der Alltag eines Netzwerkadministrators erlaubt es in der Regel nicht, sofort auf wichtige Warnungen zu reagieren. Wenn er später mit der Fehlersuche beginnt, steht meist der historische Datenverkehr im Detail nicht mehr zur Verfügung. Der Administrator kann daher nur warten

und hoffen, dass sich diese Fehler irgendwann reproduzieren lassen. Für diesen Zweck wurden neue Lösungen entwickelt, die es ermöglichen, Netzwerkdaten wichtiger Core-Verbindungen für Stunden, Tage oder sogar für Wochen mitzuschneiden und bei Bedarf zu analysieren. Damit lassen sich Probleme viel schneller und effizienter lösen, ohne diese zeitaufwendig und nervenaufreibend reproduzieren zu müssen. Mittels entsprechender Geräte können wichtige Statistiken und Parameter zeitlich angezeigt werden, ohne entsprechende Erfassungsdateien suchen oder laden zu müssen. Auf einer Core-Verbindung werden schnell einige Terrabytes an Daten in Hunderten von Dateien erfasst. Da auch die Angaben des Anwenders, wann genau ein Problem aufgetreten ist und wie es sich geäußert hat, meist recht ungenau sind, ist die Suche ohne ‚zeitnavigierendes Dataming-System‘ mit der Suche nach der Nadel im Heuhaufen gleichzusetzen.

Anschluss eines Analysators

Im kabelgebundenen Teil eines Netzwerkes sind die Arbeitsstationen im Zugangsbereich meist an Switches mit 10/100-MBit-Ports angeschlossen. Ein Analysator oder eine so genannte Probe lässt sich entweder über eine Portspiegelung (Span-Port) oder über ein in die Verbindung eingebundenes TAP (Test Access Port) anschließen. Falls es sich jedoch um voll-duplex Verbindungen handelt und diese noch zeitweise über 50 Prozent ausgelastet sind, gehen bei der Analyse wichtige Daten verloren, wodurch wiederum die Analyse an Wertigkeit verliert.

Nicht viel anders ist es im Backbone des Netzwerkes, wobei es sich meistens um Gigabit-Verbindungen handelt, manchmal

sogar um Gigabit-Trunks, wo mehrere Gigabit-Verbindungen gebündelt werden, um mehr Durchsatz zu erhalten. Diese Verbindungen sind voll-duplex; das bedeutet, es werden gleichzeitig jeweils bis zu 1.000 MBit/s in jede Richtung übertragen. Zusammengenommen sind dies bis zu 2.000 MBit/s an Daten. Bei geringen Auslastungen kann man weiterhin mit einer Portspiegelung arbeiten oder mit Aggregierung-TAPs. Diese kopieren den aus beiden Richtungen kommenden voll-duplex Datenstrom zu einem halb-duplex Datenstrom zum Analysator hin. Dies funktioniert natürlich nur, wenn diese zwei Datenströme zusammengenommen die 1.000-MBit/s-Grenze nicht überschreiten. Im Falle, dass zwei Pakete zeitgleich oder überlagert ankommen, werden diese vom Switch zwischengepuffert und erst dann weitergeleitet. Dadurch werden allerdings die Zeitstempel der Pakete verändert, und jede zeitliche Analyse ist somit wertlos. Dies ist bei Applikations-Performance-Analyse und vor allem bei der VoIP-Analyse ein K.o.-Kriterium für die Portspiegelung.

Aus diesen Gründen ist man bei der Analyse auf einen voll-duplex-fähigen TAP und Analysator angewiesen, der mit einer Dual-Receive-Erfassungskarte ausgestattet ist. Bei Kupfer-Datennetzen handelt es sich dabei um Kupfer-Taps und Analysatoren, die mit jeweils zwei Ports ausgestattet sind. Die Glasfaser-Taps haben in der Regel nur einen Port, der jedoch auf beiden Glasfasern den Datenstrom in eine Richtung zum Analysator weiterleitet. TAPs bieten außerdem noch weitere Vorteile: Da sie permanent an allen kritischen Verbindungen installiert werden, stellen sie wichtige Messpunkte im Netzwerk dar, an die man Analysatoren wie auch ‚Intrusion Detection‘-Systeme anschließen kann, ohne die kritischen Verbindung zu unterbrechen, oder das Netzwerk zusätzlich zu belasten.

Fazit

Durch Echtzeitapplikationen wie Voice over IP nimmt die Netzwerkanalyse einen neuen Stellenwert innerhalb einer modernen IT-Infrastruktur ein. War es in der Vergangenheit ausreichend, Analysen über eine Portspiegelung durchzuführen, ist zum Beispiel zur Analyse des Antwortzeitverhaltens einer Applikation eine Echtzeitmessung direkt im Link unabdingbar. Ein modernes System sollte neben vertretbaren Kosten einen maximalen Einblick in die wichtigsten Stellen im Netzwerk bieten und für die Zukunft skalierbar sein. (CK)