LANline

9,– €

Mai 2015
28. April

ITP VERLAG

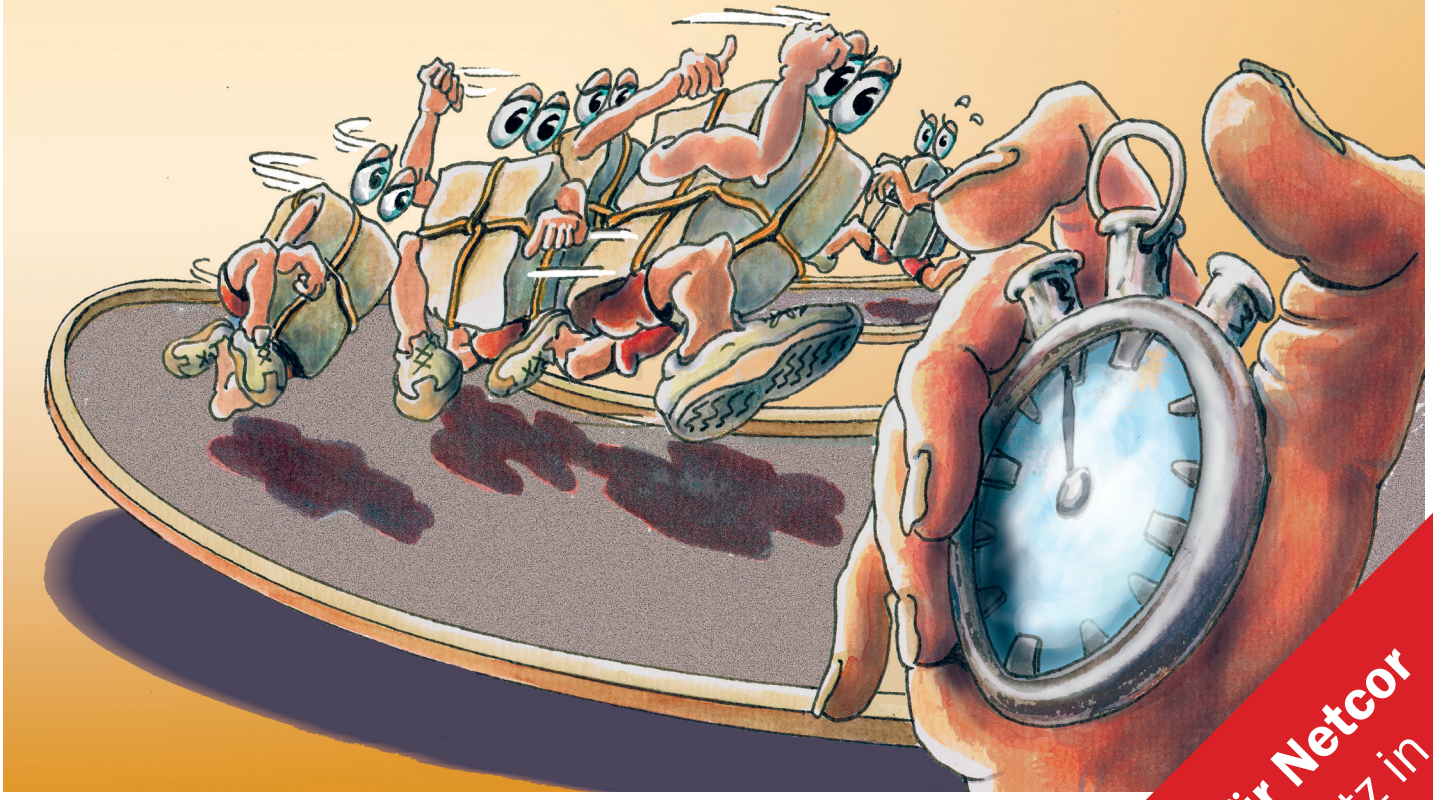
IT ■ Netze ■ Infrastruktur www.lanline.de

Netzwerk-Messtechnik und Monitoring

Paketerfassung in 10GbE-Netzen

Monitoring dynamischer Netze

Mit Marktübersicht Messtechnik für optische Datenübertragung



LANline-Serie SDN
Teil 1: Grundlagen
Software-Defined Networking im Überblick

Aagon ACMP 5.0 im Praxistest
Client-Management unter der Lupe

Stromv
Klim
M

Sonderdruck für Netcor
Wireshark-Einsatz in 10GbE-Netzen

Paketerfassung und -analyse

Wireshark-Einsatz in 10GbE-Netzen

Moderne 10-Gigabit-Ethernet-Netze stellen eine große Herausforderung für die zuverlässige Analyse des Datenverkehrs dar. Bislang von Administratoren geschätzte Tools sind für die hohen Leitungsgeschwindigkeiten zu langsam, und proprietäre Messhardware ist in vielen Fällen zu teuer. Doch es gibt praktikable Lösungen.

Viele Unternehmen rüsten heute von 1GbE- auf 10GbE-Netzwerkkomponenten um – und bringen damit ihre IT-Administratoren in Bedrängnis. Diese wollen ihre gewohnten Analyse-Tools wie beispielsweise Wireshark weiterhin effizient bei der Fehler- und Ereignisanalyse einsetzen. Doch die Performance von Notebooks und PCs reicht für das Packet Tracing in 10GbE-Netzwerken nicht mehr aus. Zwar gibt es leistungsfähige Messhardware namhafter Anbieter, die auch mit den hohen Leitungsgeschwindigkeiten klarkommt, diese ist aber für viele Unternehmen kaum bezahlbar.

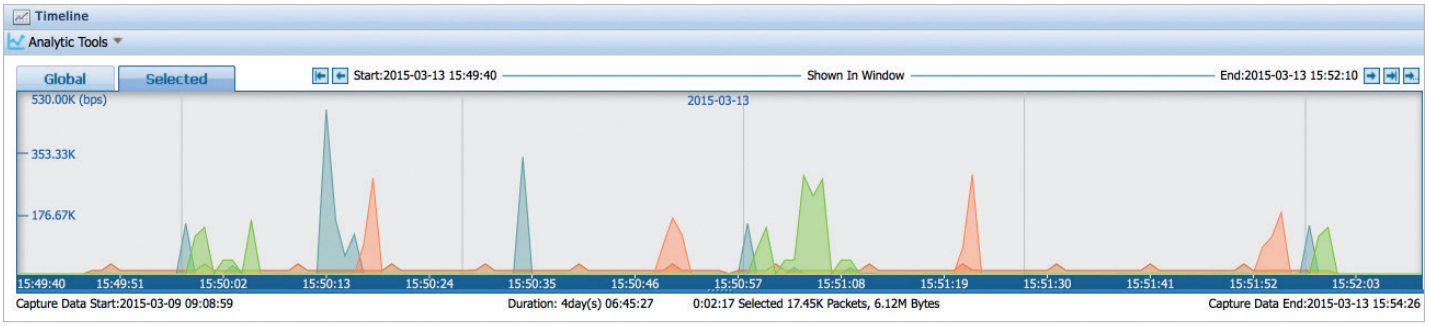
Bewährte Analysesoftware

Viele IT-Teams verfolgen für die Traffic-Analyse in ihren Netzwerken bislang einen bewährten Do-it-yourself-(DIY)-Ansatz: Aus einem schnellen Notebook, PC oder Server, einer Netzwerkkarte und geeigneter Open-Source-Software wie Tcpdump, Netsniff oder Wireshark bauen sie einen Analysator für das gezielte Packet Tracing im Netzwerk auf. Dieser ist verhältnismäßig günstig und liefert eine Performance, die für eine detaillierte Paketanalyse in 1GbE-Netzwerken ausreicht.

Wireshark hat sich in diesem Szenario als Quasistandard für die detaillierte Paketanalyse etabliert. Die Software ist für Windows, Unix und Mac OS X erhältlich. Das beliebte Freeware Tool analysiert den Datenverkehr im Netzwerk auf Protokollebene. Wireshark kennt 472 verschiedene Protokolle, von Virtual LAN über Fibre Channel bis hin zum klassischen IP und dem neueren IPv6. Ist die Winpcap-Bibliothek auf dem Analyserechner installiert, kann der Anwender den Netzwerk-Traffic aufzeichnen und auswerten. Der Sniffer geht bei Bedarf tief ins Detail und erlaubt zum Beispiel Einblicke in die Paket-Header und -inhalte.

Mit zunehmenden Leitungsgeschwindigkeiten gerät dieser DIY-Ansatz jedoch an seine Grenzen. Für 10GbE-Netzwerke sind Hardware-Performance und Skalierbarkeit unzureichend. Bei Vollauslastung überträgt eine 10GbE-Leitung zirka 1,25 GByte/s – bei einer Paketrate von 800.000 bis 14 Millionen Paketen pro Sekunde.

Ein PC ist mit dem Traffic in solch schnellen Infrastrukturen überfordert und kann



CONVERSATION(110) CONVERSATIONv6(20)

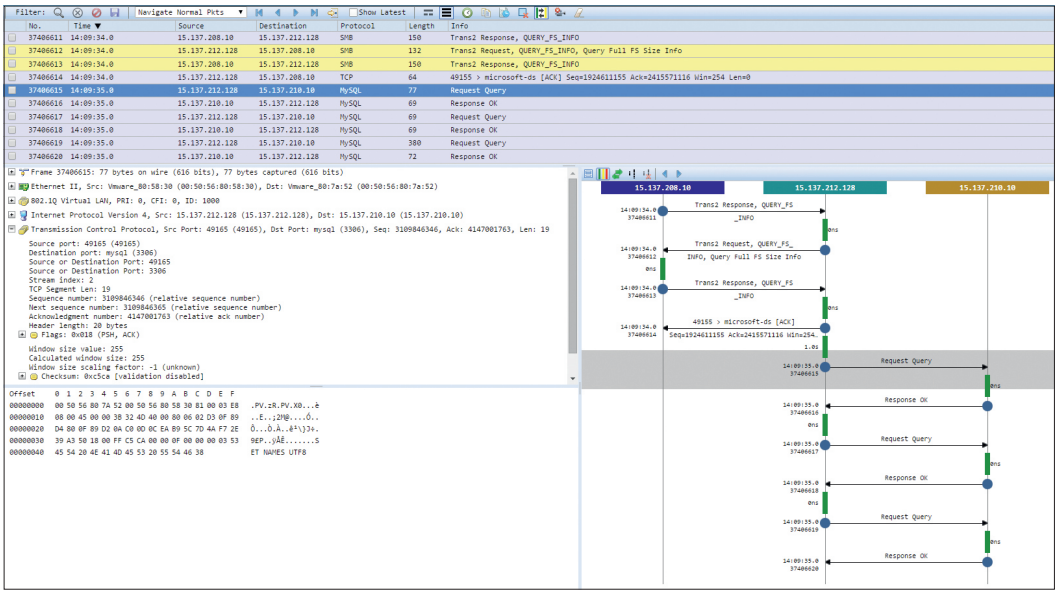
First | Previous 20 | Next 20 | Last | Filter Value: | Mask: 255.255.255.255 | Type: Source | Apply | Clear

SN	IP A	IP B	Packets A→B	Bytes A→B	Packet Rate A→B	Bit Rate A→B	Packets B→A	Bytes B→A	Packet Rate B→A	Bit Rate B→A	Nr. Of TCP Conn.	Nr. Of UDP Conn.	Nr. Of Other Conn.
1	15.137.208.111	15.137.208.14	1,370	1,597,350	10	93,275.92	586	200,399	4.28	11,702.16	undefined	undefined	undefined
2	15.137.208.111	15.137.210.87	1,090	430,701	7.96	25,150.4	846	345,489	6.18	20,174.56	undefined	undefined	undefined
3	15.137.210.10	15.137.212.128	1,660	343,957	12.12	20,085.12	1,602	120,928	11.69	7,061.52	undefined	undefined	undefined
4	15.137.208.111	15.137.210.110	156	155,286	1.14	9,067.76	96	50,082	0.7	2,924.48	undefined	undefined	undefined
5	15.137.208.111	15.137.210.23	478	105,714	3.49	6,173.12	356	128,402	2.6	7,497.92	undefined	undefined	undefined
6	15.137.208.10	15.137.212.128	766	95,724	5.59	5,589.76	634	95,380	4.63	5,569.6	undefined	undefined	undefined
7	15.137.210.10	15.137.209.8	356	59,356	2.6	3,466.08	536	120,720	3.91	7,049.36	undefined	undefined	undefined
8	15.137.208.111	15.137.208.17	129	45,020	0.94	2,628.88	203	110,532	1.48	6,454.4	undefined	undefined	undefined

Mit einer Visibility-Lösung wie Flowmagic lässt sich der zu analysierende Zeitraum mit der Maus auswählen. Zusätzlich kann der Anwender Filter für eine effizientere Analyse verwenden.

nicht alle Pakete erfassen. Schon Microbursts von wenigen 100 ms können ausreichen, den Softwareanalysator aus dem Tritt zu bringen. Die möglichen Folgen sind Paketverlust und letztlich mögliche Falscheinschätzungen aufgrund fehlender Daten in den Trace-Dateien.

Hinzu kommt, dass ein solches System massenhaft Rohdaten ohne Indexierung auf das Speichermedium schreibt. Sucht der Anwender bei der Analyse Pakete einer bestimmten Kommunikation, sind sämtliche Dateien zu durchsuchen. Dies ist sehr zeitaufwendig und somit für eine schnelle Fehleranalyse kontraproduktiv.



Analyse der Pakete ohne zusätzlich Software – direkt im Web-Browser: Die Darstellung entspricht der von Wireshark.

Ein weiterer Nachteil der beliebten DIY-Lösungen ist zudem, dass keine Funktionen für Remote-Management und Teamzusammenarbeit vorgesehen sind. Dabei ist es bei der aktuellen Vielfalt möglicher Fehler und auffälliger Ereignisse vorteilhaft, wenn zuständige Administratoren beispielsweise kurzfristig die Meinung externer Spezialisten einholen können.

Lösung: Starke Hardware, flexible Software

Was Administratoren für die Paketanalyse in modernen, verteilten Netzwerken benötigen, ist eine flexible, effizient und akkurat arbeitende Visibility-Lösung. Die Skalierbarkeit einer solchen Lösung steht und fällt mit der Architektur des Gesamtsystems. Wenn sämtliche für die Netzwerkanalyse nötigen Funktionen in Software abgebildet sind, hängt die Erweiterbarkeit des Gesamtsystems praktisch nur davon ab, wie weit sich die Hardware transparent erweitern lässt, sodass mehr Rechenkapazität für die gewünschten Funktionen zur Verfügung steht. Zu den Hardwarekomponenten zählen die Switching-Fabric, die Control Plane, die Speicheranbindung, Traffic-Analysemodule, Remote-Storage-Prozessoren sowie die Capture- und Processing-Module für den Datenverkehr.

Der Hersteller Infinicore beispielsweise hat zu diesem Zweck die „Elastic Network Visibility Architecture“ (EVA) für seine Lösung „Flowmagic“ entwickelt. Diese setzt sich aus vier Funktionsblöcken zusammen: Capture, Storage, Analysis und Collaboration. Spezielle Visibility-Aufgaben verarbeitet diese Lösung nicht mit einer jeweils dedizierten Hardwarekomponente, die schnell zum Flaschenhals werden kann. Vielmehr verteilt sie die Berechnungen flexibel auf erweiterbare Funktionsblöcke, die sich proportional mit der Zahl der Netzwerkanschlüsse skalieren lassen. So entsteht eine Unified-Visibility-Lösung, die auch in 10GbE-Netzen sämtliche Analyseaufgaben übernehmen kann: vom Erfassen und Ablegen aller Pakete über die direkte Paketdekodierung und -ansicht, den Export und das Prioritäts-Management bis hin zu Teamarbeitsfunktionen.

Eine Kernkomponente des Systems ist das leistungsfähige, skalierbare Speicherkonzept. Als Massenspeicher für das Stream-to-Disc-Modul eignen sich lokal installierte Festplatten oder schnelle SAN-/NAS-Anbindungen. Sämtliche Pakete versieht die Lösung sofort beim Eintreffen mit einem hoch genauen Zeitstempel und legt sie dann ab. Dank des Index ist es möglich, relevante Daten auch später jederzeit schnell aufzufinden.

Eine intuitive Web-basierende Benutzeroberfläche mit integriertem Dashboard vermittelt dem Anwender einen guten Überblick über den Zustand seiner IT. Mithilfe leistungsfähiger Filter- und Maskierungsfunktionen lassen sich auffällige Ereignisse schnell selektieren und detailliert in ihrem Kontext betrachten.

Fazit

Der DIY-Ansatz für die Analyse des Datenverkehrs hat in schnellen 10GbE-Netzwerken ausgedient. Trotzdem müssen Anwender nicht zwangsläufig in oft sehr teure proprietäre Messhardware investieren. Einen preislich attraktiven Ansatz bieten moderne Visibility-Lösungen, mit denen Administratoren die Möglichkeit erhalten, auch in 10GbE-Netzwerken den gesamten Datenverkehr aufzuzeichnen sowie detailliert und schnell zu analysieren.

Leistungsfähige Teamfunktionen und eine Web-basierende Benutzeroberfläche vereinfachen die Zusammenarbeit mit anderen Experten. Gewohnte und bewährte Analysesoftware wie Wireshark kann dabei weiterhin zum Einsatz kommen. Ein zusätzliches Merkmal einer solchen Lösung: Dank ihrer extrem flexiblen Architektur lässt sich ein Grundsystem anschaffen und bei Bedarf um zusätzliche Capture- und Processing-Module erweitern.

Jos Op ’t Root/pf

Jos Op ’t Root ist Geschäftsführer von Netcor, www.netcor.de.