

FÜR JEDES PROBLEM DAS GEEIGNETE TOOL

NETZWERK-ANALYZER IN ALLEN VARIATIONEN

Die Auswahl des geeigneten Werkzeugs zur Fehlerbehebung stellt die ersten Hürden für eine erfolgreiche Netzwerkanalyse und ein schnelles Troubleshooting auf. Im günstigsten Fall berücksichtigt der Netzwerkplaner von Anfang an geeignete Monitoring- und Analysewerkzeuge und bindet sie in das Netzwerkmanagement ein. Dabei sollte er sich nicht von teuren und komplexen Lösungen blenden lassen, die in der Praxis schwer zu bedienen sind.



Die Auswahl an Analyse- und Troubleshooting-Tools ist groß und reicht bis ins Netzwerkmanagement hinein. Doch kann das klassische Netzwerkmanagement (mit Vertretern wie HP Open View, Open Master oder Tivoli) das Monitoring und die Analyse niemals ersetzen, sondern ist das ideale Werkzeug zur Überwachung von Endgeräten – nicht mehr und nicht weniger. Denn diese Lösungen sind “blind” für Ereignisse,

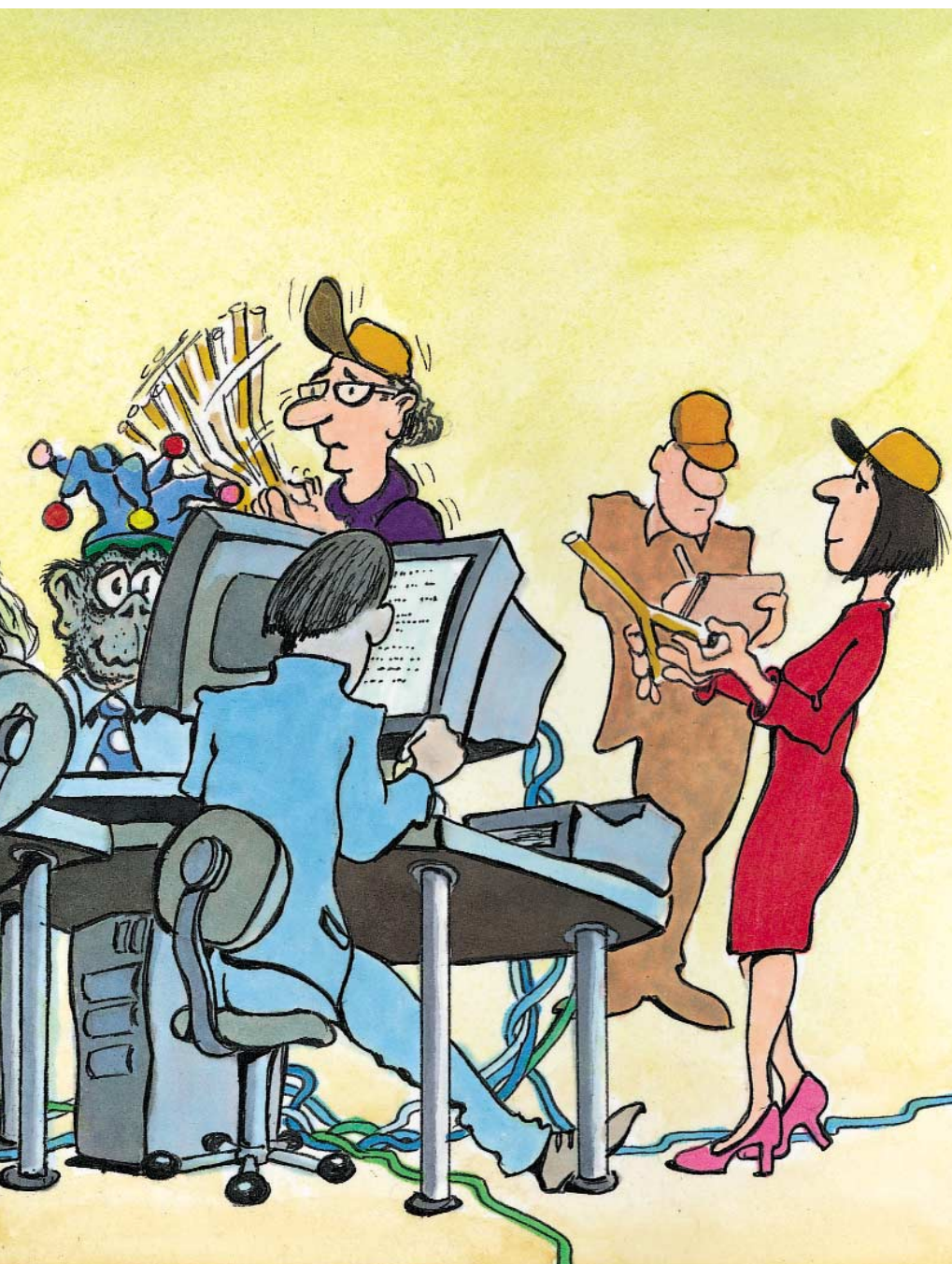
die sich außerhalb ihrer Agenten abspielen. In einem nicht mehr funktionsfähigen Netzwerk sind solche Lösungen schlicht und einfach hilflos. Netzwerkmanagement bedeutet auch immer, dass eine zentrale Konsole alle Daten ihrer Agenten sammelt. Im Fehlerfall muss ein Techniker in den meisten Fällen vor Ort das Problem analysieren, sodass an dieser Stelle wieder der klassische Analysator benötigt wird, zumindest aber

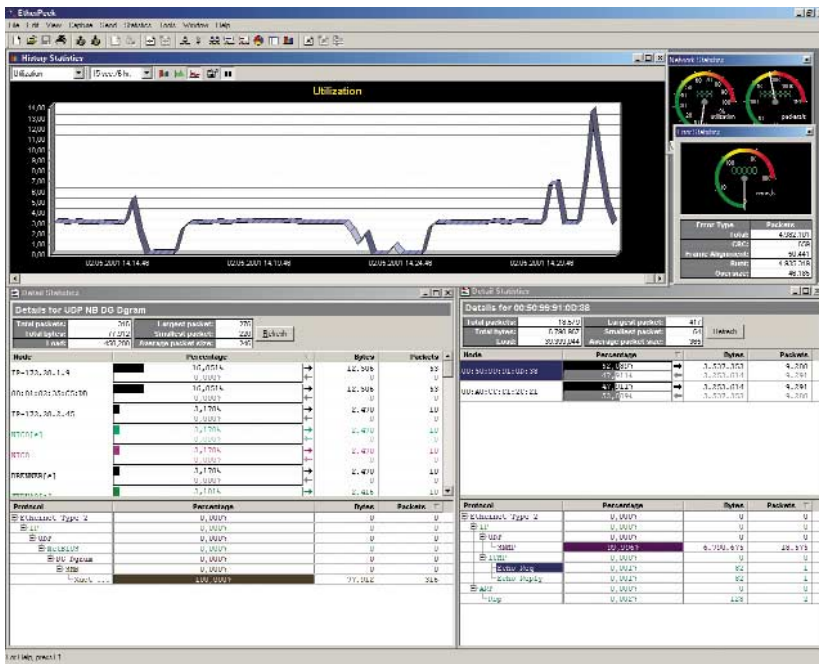
ein Analysator mit Soft- oder Hardware-Agenten, die in dem betroffenen Segment platziert werden können.

Nichtsdestotrotz enthalten Analysatoren mittlerweile neben der klassischen Analyse, also dem Sammeln von Daten und Dekodieren von Paketen, vermehrt Reporting- und Messaging-Funktionalitäten. So ist es mit wenigen Mausklicks möglich, einen einfachen Report über das Netzwerkgeschehen der letzten Tage, Wochen oder Monate zu erstellen. Alarmfunktionalitäten beschränken sich nicht nur auf die Anzeige eines überschrittenen Schwellwerts, sondern versenden auf Wunsch eine E-Mail oder eine SMS an den Administrator mit der entsprechenden Fehlermeldung.

STATUSABFRAGEN Um dem Fehlerfall vorzubeugen, verfügen alle Analysatoren über umfangreiche Statistikfunktionen und automatisch generierte Reports. Damit erkennen sie frühzeitig verhängnisvolle Trends. So lässt sich mit einem Ping ganz einfach überprüfen, ob Komponenten oder Netzwerksegmente verfügbar sind. Zusätzlich sollte der Administrator damit die Erreichbarkeit wichtiger Dienste (wie POP, SMTP, DNS oder http) abfragen sowie Alarmer und Benachrichtigungen konfigurieren können. Solche Statusabfragewerkzeuge sind hilfreich, um Netzausfälle und Geräteausfälle zu erkennen. Sie sind jedoch nur begrenzt im Analyse- und Troubleshooting-Bereich verwendbar. Vertreter für derartige Tools wie What's Up Gold von Ipswitch und Link Analyst 3.0 von Network Instruments sind dafür konzipiert und ähneln sich in ihren Grundfunktionen. Beide sind einfach zu bedienen, leicht verständlich und bieten für einen Preis von zirka 2000 Mark nützliche Dienste.

LOKALE ANALYSE Der klassische Netzwerkanalysator kommt immer dann zum Einsatz, wenn der Techniker direkt im betroffenen Segment messen muss, weil dort kein Agent verfügbar ist oder





Auslastung und Statistiken bei Etherpeek von Wild Packets

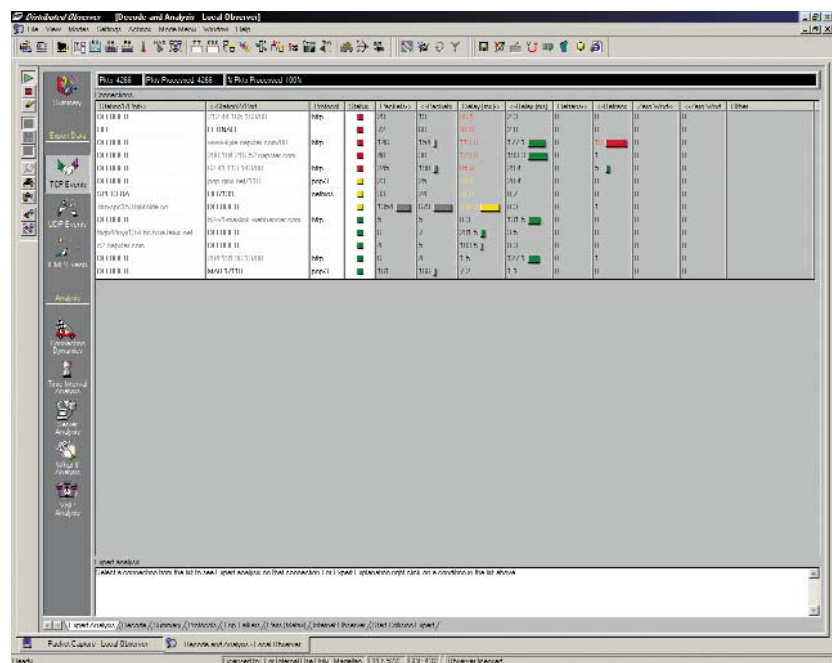
mit den Agenten nicht mehr kommuniziert werden kann. Grund dafür ist vielleicht ein defektes Router- oder Switch-Interface. Manchmal ist es aber auch nur eine defekte Netzwerkkarte, die ein ganzes Netzwerksegment zum Erliegen bringt. Gerade für Servicetechniker, die häufig in Kundennetzwerken Fehler suchen und beheben müssen, ist ein klassischer Analysator das Werkzeug der Wahl. Idealerweise wird er auf einem Laptop installiert, um ortsunabhängig direkt im betroffenen Segment messen zu können. Hier gibt es auf dem Markt eine Vielzahl von Lösungen. Zwei sehr leistungsfähige und dennoch nicht teure Produkte sind der Observer (in der aktuellen Version 7.1) von Network Instruments und Etherpeek (aktuelle Version: 4.1) von Wild Packets. Beide Analyser hat das LANline-Lab auch schon getestet. In LANline 10/2000 erschien ein Test von Observer 7.0 (ab Seite 94), in LANline 9/2000 einer zu Etherpeek 4.02 (ab Seite 82).

VERTEILTE ANALYSE In großen Netzwerken, die einer ständigen Pflege bedürfen, ist der Einsatz von Netzwerkanalysesystemen geboten, die kritische Segmente zeitgleich beobachten und

analysieren. So kamen Systeme auf den Markt, die mehrere Agenten gleichzeitig ansprechen und managen können. Die Kommunikation zu den Agenten erfolgt zumeist über eigene TCP/IP-Verbindungen. Die Einbindung von RMON1/2-Agenten (Remote Network Monitoring von IETF für das Simple Network Management Protocol SNMP)

ist sicherlich sinnvoll, die Übertragung von RMON-Daten erzeugt jedoch eine nicht unerhebliche Netzlast. Aus diesem Grund benutzen Analysensysteme für die Kommunikation mit ihren Agenten proprietäre Protokolle, die deutlich weniger Netzlast als klassische SNMP/RMON-Protokolle erzeugen und auch eine wesentlich schnellere Kommunikation ermöglichen. Zwei sehr umfangreiche und leistungsfähige Lösungen sind Tevista von Chevin und Surveyor THG von Shomiti.

NETZWERKKARTE Im Prinzip kann der Anwender für diese Analyser jede Netzwerkkarte verwenden, die den Promiscuous Mode unterstützt. Der ermöglicht es der Netzwerkkarte, alle Datenpakete mitzulesen, auch die Pakete, die nicht an sie selber adressiert sind. Herkömmliche Netzwerkkarten und NDIS-Treiber (Network Device Interface Specification) unterstützen das Erkennen von physikalischen Fehlern nämlich nur rudimentär. Deshalb empfehlen Network Instruments und Wild Packets Netzwerkkarten mit Intel/DEC-21xx4-Chipsatz, mit denen ein Maximum an Leistung erreichbar ist. Eigens für diese Chipsätze programmierte Treiber sind den Produkten beigelegt,



Expertenanalyse mit dem Observer von Network Instruments

weitere unterstützte Netzwerkkarten und Chipsätze sind auf den Web-Seiten der Hersteller zu finden.

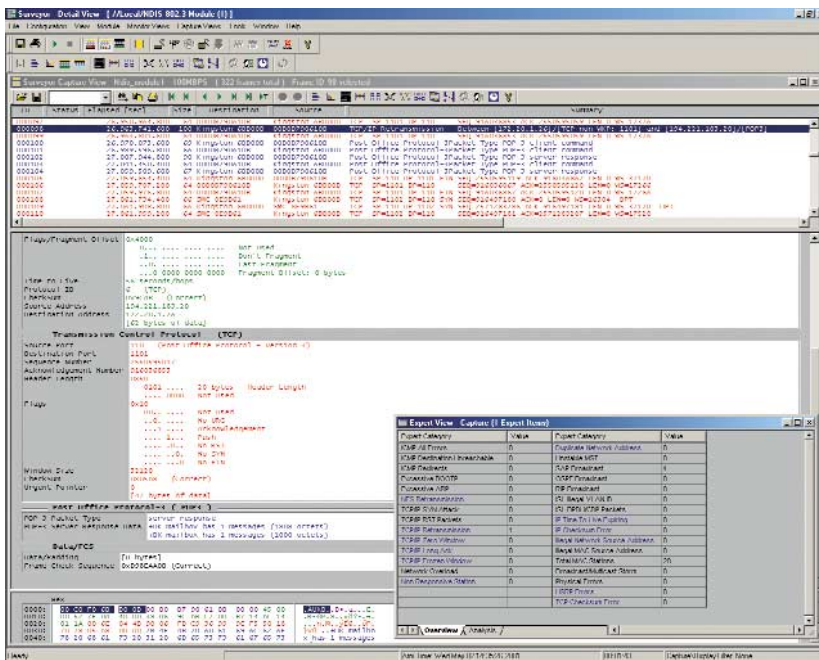
ETHERPEEK Der günstigste Analysator auf dem Markt wird von Wild Packets (früher AG Group) hergestellt. Etherpeek ist übersichtlich aufgebaut, die Installation verläuft ohne Probleme, und auch die mitgelieferten Treiber lassen sich einfach und schnell installieren. Zudem ist es als Macintosh-Variante erhältlich. Die Capture-, Transmit- und Statistikfunktionen sind leicht und intuitiv zu bedienen.

der Anwender zu jedem Wert mit einem einfachen Klick einen Graph oder eine Tortengrafik erzeugen lassen kann. Um die augenblickliche Situation festzuhalten und dann mehrere Intervalle miteinander vergleichen zu können, hat der Anwender jederzeit die Möglichkeit, einen Snapshot anzulegen. Die Alarmfunktion überwacht außerdem fast alle Statistikdaten. Die Benachrichtigung erfolgt über E-Mail oder SMS. Zudem kann der Anwender den Analysator auch so einstellen, dass er ihm erneut eine Nachricht sendet, wenn ein Wert

up Language), HTML (Hypertext Markup Language) oder Textdatei ab. Ein eigenes Reporting fehlt leider.

Etherpeek erlaubt das gleichzeitige Starten mehrerer Packetcaptures und dekodiert die Messdaten schon während des Mitlesens. Das Decoding erkennt und dekodiert alle wichtigen und unwichtigen LAN-Protokolle, zum Beispiel auch Cisco-Protokolle. Die einzelnen Parameter dekodiert das Tool ausführlich und stellt sie übersichtlich dar. Darüber hinaus hat der Anwender die Möglichkeit, mithilfe der vorkonfigurierten Filter seine Messdaten nach bestimmten Kriterien zu untersuchen. Wenn die nicht ausreichen, kann er intuitiv einen eigenen definieren, und über einen Advanced Mode sind selbst sehr komplexe Filter möglich.

Grundsätzlich eignet sich Etherpeek besonders gut für Protokollanalysen in kleinen Netzen. Durch sein ausführliches Decoding lassen sich auch ungewöhnliche Protokollfehler erkennen. Das Tool verfügt zwar über kein eigenes Expertensystem, erkennt jedoch einige TCP-Attacken (Transmission Control Protocol) und liefert eine Statistik der ICMP-Meldungen (Internet Control Message Protocol). Für eine Detailanalyse der Messdaten bietet Wild Packets mit Netsense zudem ein Expertensystem an.



Expertenanalyse mit dem Surveyor von Shomiti

Dabei hat der Hersteller die Statistiken in sechs Bereiche unterteilt: Node, Protocol, Conversations, Network, Error und Size.

Netzlast und Fehler zeigt der Analysator entweder tabellarisch oder mittels Tacho an. Unter dem Menüpunkt "Protocoldetails" listet er nicht nur die einzelnen Protokolle auf, sondern ordnet jedem Protokoll die Stationen mit Mengendetails zu. Umgekehrt ordnet die Funktion "Nodedetails" jeder Station die benutzten Protokolle mit Mengendetails zu. Die Summary-Funktion stellt alle Details tabellarisch dar, wobei sich

nach einer Störung wieder "im grünen Bereich" ist.

Schließt der Anwender einen Etherpeek an sein Netz, listet dieser in einer Namenstabelle alle gefundenen Stationen auf. Die Auflösung der Namen geschieht über DNS (Domain Name Service) und NetBIOS-Abfragen (Network Basic Input/Output System). Diese kann er dann in Gruppen zusammenfassen, was vor allem bei großen Netzen Sinn macht.

Statistikdaten speichert der Analysator automatisch als CSV (Comma-Separated Values), XML (eXtensible Mark-

OBSERVER Der Observer von Network Instruments ähnelt im Aufbau und der Funktionalität sehr stark dem Sniffer von Sniffer Technologies (NAI). Die Handhabung des Observers ist einfach, und das ausführliche Handbuch beantwortet alle offenen Fragen.

Der Schwerpunkt liegt bei diesem Tool eindeutig im Monitoring und Statistikbereich. Es zeigt Statistiken entweder tabellarisch oder in zwei verschiedenen grafischen Formaten an. Die Lösung besitzt mehr als die üblichen Statistikfunktionen für "Top Talker", Protokolle oder Nodes und ermittelt zum Beispiel auch die Auslastung eines Routers oder überwacht einen Web-Server. Der Kollisionstest überprüft Netzwerkkarten auf

deren Kollisionsverhalten, um Defekte frühzeitig zu erkennen. Benutzt der Anwender einen Observer mit eigener Netzwerkkarte, dann kann er physikalische Fehler der zugehörigen Sendestation zuordnen. Der "Burst Mode" testet die Belastbarkeit eines Netzwerks. Und die Funktion "Internet Observer" überwacht alle IP-Verbindungen mit den benutzten Protokollen und Datenmengen. IP-Adressen werden über DNS und Net-BIOS in Klartextnamen umgesetzt.

Das "Network Trending" sammelt im Hintergrund alle Netzwerkkdaten über frei konfigurierbare Intervalle. Darüber erstellt der Analysator nicht nur einfache Reports, sondern vergleicht auch beliebige Zeiträume miteinander. Über einen integrierten Web-Server kann der Anwender jederzeit via Browser auf die Statistikdaten zugreifen. Zudem lassen sich die Daten auf Stations- und Intervallebene herunterbrechen, um über einen längeren Zeitraum hinweg Trends und Entwicklungen sichtbar zu machen.

Im Gegensatz zum Etherpeek kann der Anwender allerdings immer nur ein Capture gleichzeitig starten. Über viele vordefinierte Filter (Protokoll-, Stations- und Offsetfilter) lässt sich die Messdatenerfassung genau steuern. Das Erstellen eigener Filter geht einfach und schnell. Tritt ein Fehler nur sporadisch auf, kann der Analyzer die Messdaten kontinuierlich abspeichern und so über einen längeren Zeitraum danach suchen. Das Decoding der Protokolle ist leider nur mäßig und beschränkt sich auf die wichtigsten Parameter. Gerade das wichtige SMB-Protokoll (Server Message Block) wird häufig nicht völlig dekodiert. Wie der Etherpeek dekodiert der Observer die mitgelesenen Datenpakete schon während der Messung.

Seit Version 7 enthält der Observer ein Online-Expertensystem, das TCP/IP-Verbindungen während des Mitlesens analysiert. Fehler und Unregelmäßigkeiten in den Verbindungen werden hervorgehoben und erklärt. TCP-Verbindungen stellt der Analysator auch grafisch dar, was die Analyse über einen bestimmten Zeitraum erleichtert. Die Stärken des Ob-

servers liegen somit eindeutig im Statistik- und Monitoring-Bereich. Sein Expertensystem macht es auch Einsteigern leicht, Störungen zu erkennen und zu beheben.

SURVEYOR THG Shomiti stellt mit seinem Surveyor THG eine Verbindung von Hardware- und Software-Analyser vor, der sowohl lokal als auch verteilt messen kann.

Der Surveyor ist ein klassischer Analyser mit grundlegenden Statistik- und Re-

Probe oder aber auf die Hardware-Probes von Shomiti.

Der Surveyor liefert die Statistiken auf Basis von Host-, Network- und Application-Tabellen und stellt sie tabellarisch oder grafisch dar. Die so gemessenen Daten können nur im CSV-Format exportiert werden, ein eigenes Reporting ist nicht vorhanden.

Als einziger Hersteller bietet Shomiti mit THG eine Hardware-Probe, die 10/100-Ethernet und Gigabit Ethernet gleichzeitig messen kann, sowohl bei

Alias Name	Packets	Octets	Errors	Collisions	Up Time	Last Pa.	Last Oc.	Last Er.	Last Col.	Last Period
RMON:10/100 VLAN 1	1128794	18504	0.01%	347012	86 days, 00:00	234	78558	0.00%	0	8.280 seconds
Uplink zum Backbone-Switch	153729	21228	0.00%	0	86 days, 00:00	18	1703	0.00%	0	7.295 seconds
RMON:10/100 Port 2 on Unit 1	122858	40428	0.00%	197	86 days, 00:00	21	2291	0.00%	0	7.181 seconds
RMON:10/100 Port 3 on Unit 1	209381	264996	0.00%	0	86 days, 00:00	0	0	0.00%	0	7.171 seconds
RMON:10/100 Port 4 on Unit 1	125748	38078	0.00%	0	86 days, 00:00	12	1635	0.00%	0	7.230 seconds
RMON:10/100 Port 5 on Unit 1	0	0	0.00%	0	86 days, 00:00	0	0	0.00%	0	0.000 seconds
RMON:10/100 Port 6 on Unit 1	44198	16538	0.00%	2835	86 days, 00:00	127	20918	0.00%	0	17.376 seconds
RMON:10/100 Port 7 on Unit 1	55528	18278	0.00%	0	86 days, 00:00	12	1635	0.00%	0	7.258 seconds
RMON:10/100 Port 8 on Unit 1	49898	15518	0.01%	0	86 days, 00:00	0	0	0.00%	0	8.848 seconds
RMON:10/100 Port 9 on Unit 1	0	0	0.00%	0	86 days, 00:00	0	0	0.00%	0	8.902 seconds
RMON:10/100 Port 10 on Unit 1	53488	14448	0.00%	1073	86 days, 00:00	18	2029	0.00%	0	6.875 seconds
RMON:10/100 Port 11 on Unit 1	138848	12018	0.01%	0	86 days, 00:00	0	0	0.00%	0	6.885 seconds
RMON:10/100 Port 12 on Unit 1	97088	107252	0.00%	0	86 days, 00:00	0	0	0.00%	0	6.887 seconds
RMON:10/100 Port 13 on Unit 1	1036708	18578	0.00%	0	86 days, 00:00	79	11273	0.00%	0	6.890 seconds
RMON:10/100 Port 14 on Unit 1	87278	35458	0.00%	803	86 days, 00:00	12	1635	0.00%	0	8.801 seconds
RMON:10/100 Port 15 on Unit 1	100198	97858	0.00%	0	86 days, 00:00	13	1703	0.00%	0	8.937 seconds
RMON:10/100 Port 16 on Unit 1	29728	11888	0.00%	0	86 days, 00:00	0	0	0.00%	0	6.885 seconds
RMON:10/100 Port 17 on Unit 1	0	0	0.00%	0	86 days, 00:00	0	0	0.00%	0	6.843 seconds
RMON:10/100 Port 18 on Unit 1	172118	17238	0.00%	0	86 days, 00:00	12	1635	0.00%	0	6.835 seconds
RMON:10/100 Port 19 on Unit 1	35278	16598	0.00%	0	86 days, 00:00	0	0	0.00%	0	6.808 seconds
RMON:10/100 Port 20 on Unit 1	72888	17098	0.00%	0	86 days, 00:00	11	1571	0.00%	0	6.845 seconds
RMON:10/100 Port 21 on Unit 1	0	0	0.00%	0	86 days, 00:00	0	0	0.00%	0	6.852 seconds
RMON:10/100 Port 22 on Unit 1	387488	12128	0.01%	254871	86 days, 00:00	158	55512	0.00%	0	8.844 seconds
RMON:10/100 Port 23 on Unit 1	84128	17388	0.00%	0	86 days, 00:00	0	0	0.00%	0	6.834 seconds
RMON:10/100 Port 24 on Unit 1	81628	10388	0.00%	0	86 days, 00:00	0	0	0.00%	0	6.740 seconds
RMON:10/100 Port 25 on Unit 1	0	0	0.00%	0	86 days, 00:00	0	0	0.00%	0	6.816 seconds

Tevista von Chevin hat einen SNMP/RMON-Reporter, der die einzelnen Ports eines Switches überwacht

porting-Fähigkeiten. Durch seine Skalierbarkeit kann er sowohl als Einzelplatzgerät als auch als Lösung für große Netzwerke verwendet werden. Zu der Basisvariante kommen verschiedene Plugins. Dazu zählen das Online-Expertensystem "Expert", "Packet Blaster" – ein Modul zu Generierung von künstlichem Verkehr sowie "Remote", mit dem der Anwender Probes und Agenten einbinden kann und schließlich das Plug-in "Multi QoS". Es analysiert und dekodiert Multimediaverbindungen. Ausgangspunkt des Surveyors ist der Ressourcen-Browser. Über ihn greift das System auf jede lokale Netzwerkkarte zu, auf jede beliebige im Netz vorhandene RMON-

Half- als auch bei Fullduplex-Verbindungen. Dadurch können selbst hundertprozentig ausgelastete Verbindungen annähernd verlustfrei gemessen werden. Das Filtermenü des Surveyors erfordert eine gewisse Einarbeitungszeit. Eine Vielzahl von vorkonfigurierten Filtern, selbst für das Cisco-ISL- und VLAN-Protokoll, sind vorhanden. Das Erstellen eigener Filter erfordert einige Übung und ist variabel gehalten. Mit dem Surveyor können bis zu 2500 Probes gleichzeitig verwaltet und gemessen werden.

Sein Protokoll-Decoding gehört zu den umfangreichsten auf dem Markt. Der Surveyor dekodiert über alle sieben OSI-Schichten mehr als 250 Protokolle inklu-

sive aller Details. Ein übersichtliches Expertensystem findet und erklärt alle wichtigen Standardfehler. Über die Response Time Analysis untersucht das Gerät das Antwortzeitverhalten von Applikationen. Zusätzlich werden mit dem Multi-QoS-Plug-in die verbreitetsten Multimedia-protokolle (H.323, Q.931, H.245, RTP, RTCP, SCCP, G.7x, H.261, H.263, etc.) vollständig dekodiert und analysiert. Diese Skalierbarkeit und umfassende Ethernet-Unterstützung macht den Surveyor zum idealen Werkzeug für große Netze.

TEVISTA Die Überwachung großer Netzwerke mit allen Außenstellen ist mit normalen Analyseplattformen nur schwer und äußerst kostenintensiv zu bewerkstelligen. Chevin stellt mit Tevista eine Lösung vor, die einfach zu bedienen ist und eben dieses ermöglicht. In der kleinsten Ausführung arbeitet Tevista schon mit 25 Agenten.

Im Gegensatz zum klassischen Analyzer startet Tevista mit dem "Enterprise Manager", über den der Netzwerkadministrator die einzelnen Segmente überwacht und analysiert. Tevista verwendet zur Kommunikation mit seinen Probes das HSRMON- (High-Speed-Remote-MONitoring-) Protokoll. Somit können selbst schmalbandige Leitungen (9.600er-Modem oder GSM-Verbindungen) zur Kommunikation verwendet werden.

Jede Probe bietet die gleichen umfangreichen Möglichkeiten wie der klassische Analyzer (beispielsweise Statistiken, Alarmer, Packet Capture mit Filter, Namenstabellen). Sie sammeln jeweils die in ihrem Segment anfallenden Statistikdaten, und Tevista erstellt daraus umfassende Reports mit einer Vielzahl von Grafiken. Der Anwender erreicht über die rechte Maustaste jederzeit die zugehörigen Detailstatistiken der verschiedenen Probes. Um die Verfügbarkeit wichtiger Komponenten (wie Server, Router, Switches) zu garantieren, können mit Tevista solche Stationen regelmäßig mit einem Ping abgefragt werden. Die Antwortzeiten speichert das System und verarbeitet sie automatisch zu einem Report.

Einzigartig an dieser Lösung ist die Möglichkeit, Daten mehrerer Switchports zu synchronisieren und zusammenzufassen. Beliebige Agenten auf einem Switch können zu einem Agenten zusammengefasst werden (Switch Aggregator). Im besten Falle wäre auf jedem Switchport ein Agent vorhanden. Somit könnte der gesamte Datenverkehr eines Switches in einem einzigen Packet Capture mitgelesen werden. Tevista entfernt dabei alle doppelten Pakete, sodass ein Broadcast zum Beispiel nur einmal mitgelesen wird und nicht auf jedem einzelnen Port.

Mit dem integrierten SNMP/RMON-Reporter können alle gängigen SNMP- und RMON-fähigen Switches und Router analysiert werden. Dazu liest die Lösung die SNMP- und RMON-Tabellen eines Switches/Routers Port-weise aus und zeigt die Auslastung aller Ports übersichtlich in einer Grafik an. In der Detailansicht werden pro Port nicht nur die Auslastung, sondern auch alle anderen Zähler (Packets, Bytes, Errors) ausgelesen. Für jeden Port können umfangreiche Alarmer konfiguriert werden.

Mit Tevista erhalten vor allem Administratoren von mittleren und großen Unternehmensnetzen einen umfassenden Blick über ihr Netzwerk.

(Oliver Thewes/db)

Der Autor ist Experte für Netzwerkanalyse bei Magellan Netzwerke in Köln.

Weitere Informationen:

Network Instruments:
Web: www.linkanalyst.de
www.observer-analyzer.com

Ipswitch:
Web: www.ipswitch.de

Wild Packets
Web: www.wildpackets.de

Chevin
Web: www.tevista.de

Shomiti
Web: www.shomiti.com
www.magellan-net.de/shomiti

Sniffer Technology
Web: www.sniffer.de