LAN-Diagnose mit dem Network Multimeter

Ob hängende Onlinemeetings oder träge Applikationen: Das Analysieren von Übertragungsfehlern im Netzwerk ist häufig komplex und zeitraubend. Das Network Multimeter vereinfacht die Fehlersuche.

Von Benjamin Pfister

Zum Alltag von Systemadministratoren gehören schon immer Beschwerden über lahme oder ausgefallene On-Premises- oder Cloud-Applikationen. In den letzten Jahren hat der Anteil der Videokonferenz- und anderer Echtzeitdienste zugenommen, die nicht nur sehr viel höhere Anforderungen ans Netz stellen als die Klassiker E-Mail und WWW, sondern deren Störung auch besonders unangenehm auffällt. Der erste Verdacht fällt dabei meist aufs Netzwerk, doch eine Ursachenanalyse kann recht aufwendig sein.

Je nach Komplexität und Durchsatz des Netzwerks stößt ein handelsübliches Notebook als Testausrüstung rasch an seine Grenzen. Als Alternative kommt ein spezialisiertes Gerät infrage. Das Network Multimeter (NMM) 1000 rev. 3 v3.4.1 von Allegro Packets enthält neben dem RJ45-Port für das IP-KVM des zugrunde liegenden Supermicro-Systems sechs RJ45-LAN-Ports, von denen einer fest zum Administrieren des Systems vorgesehen ist. Hinzu kommen drei 1GBASE-T- und zwei 10GBASE-T-Ports. Für eine Anbindung per Glasfaser stehen zwei SFP+-Slots zur Verfügung, für die der Hersteller Dual-Speed-1G-SX- und 10G-SR-SFP+-Module mitliefert. Hinzu kommen zwei USB-A-Anschlüsse, die beispielsweise einen WLAN-Adapter wie den ebenfalls mitgelieferten TP-Link TL-WN725N aufnehmen können (Abbildung 1). Das System verfügt über acht CPU-Kerne. Größere Captures mit bis zu 10 GBit/s speichert eine 2 TByte große NVMe-SSD (Seagate FireCuda 520).

Das Testgerät war im Unterschied zur Standardausstattung mit einer Speichererweiterung von 16 auf 64 GByte RAM ausgerüstet. Die Tragetasche hilft bei der mobilen Nutzung. Die getestete Appliance bietet kein redundantes externes Netzteil, was im Inline-Aufzeichnungsmodus – mit dem Gerät als Bridge im Datenstrom – heikel sein kann: Die integrierten Ports ermöglichen – anders als bei größeren Modellen – kein physisches Durchschalten bei Stromausfall.

Linux-Appliance als Netzwerktester

Das NMM basiert auf Debian Linux. Zur schnellen Paketverarbeitung greift die Appliance auf das Open-Source-Projekt Dataplane Development Kit (DPDK) zurück, das der Hersteller aktiv unterstützt. Es verwendet im Default zunächst nur In-Memory-Speicher und speichert Netzwerkinformationen nicht dauerhaft. Das bietet Vorteile in Bezug auf den Datenschutz. Die Daten stehen zunächst nur während der Analyse zur Verfügung. Eine In-Memory-Datenbank speichert die Metadaten der verarbeiteten Pakete – sie gehen also bei einem Neustart oder Herunterfahren verloren. Das gilt auch für einen unerwarteten Stromausfall, was gerade bei längeren Troubleshootings ärgerlich ist.

Zusätzlich bietet Allegros NMM jedoch auch einen Paketringpuffer. In diesem Fall landen die Pakete auf der NVMe SSD. Sie stehen also auch nach einem Neustart zur Verfügung. Eine interessante Möglichkeit ist die nachträgliche Analyse des Paketringpuffers: Man kann Ereignisse also unabhängig von Zeit und Ort nachvollziehen. Die Analyse unterbricht jedoch den Livemodus, also die Verarbeitung im In-Memory Speicher.

Bis zum Erreichen von 90 Prozent der maximalen Speicherkapazität beschreibt das NMM den Ringpuffer. Danach beginnt es die ältesten Daten zu überschreiben. Die maximale Länge der Aufzeichnung hängt vom Traffic und der Speicherkapazität ab und ist daher schwer planbar. Dies kann beim Troubleshooting kritisch sein, wenn relevante Daten überschrieben werden. Es empfiehlt sich also ein Test vor einer eventuellen Beschaffung, damit man genügend Puffer einplanen kann. Hilfreich sind E-Mail-Reports mit Schätzungen, wie lange es noch bis zum Erreichen von 90 Prozent Speicherauslastung dauert.

Neben der hier genutzten Appliance bietet der Hersteller mehrere Varianten vom kleinsten und mit 260 g leichtesten Allegro 200 mit zwei GE-Schnittstellen bis hin zu 19-Zoll-Appliances (Allegro

iX-TRACT

- Das Network Multimeter (NMM) der Leipziger Allegro Packets dient als Stand-alone-Appliance für die Problem- und Nutzungsanalyse in komplexen Netzen – auch bei Providern.
- Mit dem NMM lassen sich zahlreiche Fehlerquellen auf übersichtliche Weise einkreisen.
- Echtzeit-Medienstreaming als zeitkritische und damit besonders fehlersensible Anwendung findet beim NMM besondere Beachtung.

5500) mit vier Höheneinheiten und bis zu 150 GBit/s Durchsatz sowie 576 TByte integriertem Ringpuffer. Auch eine virtuelle Appliance steht bereit.

Integrationsmöglichkeiten

Damit das Gerät Statistikdaten produzieren und analysieren kann, muss es zunächst Traffic sammeln. Das kann auf unterschiedliche Weisen geschehen: Der Hersteller nennt diese Sink-, Bridge- und Endpoint-Modus (Abbildung 2).

Im Sink-Modus, also out of band, erhält das Gerät Traffic von einem Test-Access-Point (TAP) oder einem Spiegel-Port (SPAN, Switched Port Analyzer) am Switch. Beim SPAN-Modus muss man jedoch im Auge behalten, dass das SPAN-Ziel für eine bidirektionale Aufzeichnung mindestens die doppelte Link-Kapazität für die Übertragung von Sende- und Empfangsrichtung bereitstellen sollte.

Im Bridge-Modus arbeitet das Gerät inline, also als Teil des Kommunikationspfads. Physische und vertikal zueinandergehörende Schnittstellenpaare bilden immer eine transparente Bridge. Die Betriebsart lässt sich zwischen Sink und Bridge umschalten. Fällt das Analysegerät aus, bedeutet der Bridge-Modus eine Unterbrechung des Produktiv-Traffics.

Für den Fall, dass sich das Gerät nicht im selben LAN wie die Traffic-Quelle befindet, kann das NMM im Endpoint-Modus als ERSPAN-Senke (Encapsulated Remote SPAN) dienen, also den Traffic über einen Tunnel mitschneiden. Dies macht die Appliance flexibel einsetzbar und funktionierte im Labor gut.

Zudem bietet das NMM die Möglichkeit eines Internet Protocol Flow Information Export (IPFIX) an einen entsprechenden Collector zur zentralen Sammlung. Dies empfiehlt der Hersteller auch für Langzeitstatistiken.

Für korrekte Zeitstempel in den Statistiken steht sowohl NTP als auch PTP (Network Time Protocol / Precision Time Protocol) zur Verfügung. Das ist für eine korrekte Korrelation von Ereignissen im Troubleshooting unabdingbar.

Erste Schritte mit oder ohne Draht

Das System lässt sich out of band managen, sowohl per Kabel als auch drahtlos. Der dedizierte Management-Port arbeitet im DHCP-Client-Modus. Wenn kein DHCP-Server zur Verfügung steht, kann man über eine USB-Tastatur und Shift+S die IP-Adresse 192.168.0.1 zuweisen. Außerdem besteht die Möglichkeit, ein sekundäres Management-Interface per USB-Ethernet-Adapter zu ergänzen.

Allegros Network Multimeter bietet diverse LAN-Anschlüsse. WLAN-Konnektivität stellt ein USB-Adapter her, der sich im Lieferumfang befindet (Abb. 1).

Über ein WLAN-USB-Dongle steht zusätzlich eine 802.11b/g/n-Schnittstelle im Access-Point-Betriebsmodus und vorkonfigurierter SSID nach dem Muster allegro-mm-xxxx bereit. In diesem Fall dient der Allegro auch als DHCP-Server und hat selbst die IP-Adresse 192.168.4.1. Diese wird auch als DNS-Serveradresse per DHCP verteilt, wodurch sich das Web-GUI einfach über https://allegro oder https://192.168.4.1 ansteuern lässt. Die Analysefunktionen decken controllerbasierte WLANs ab. Mittels CAPWAP (Control And Provisioning of Wireless Access Points) sind Daten wie die zugewiesenen Übertragungsraten und Signalqualitäten auslesbar.

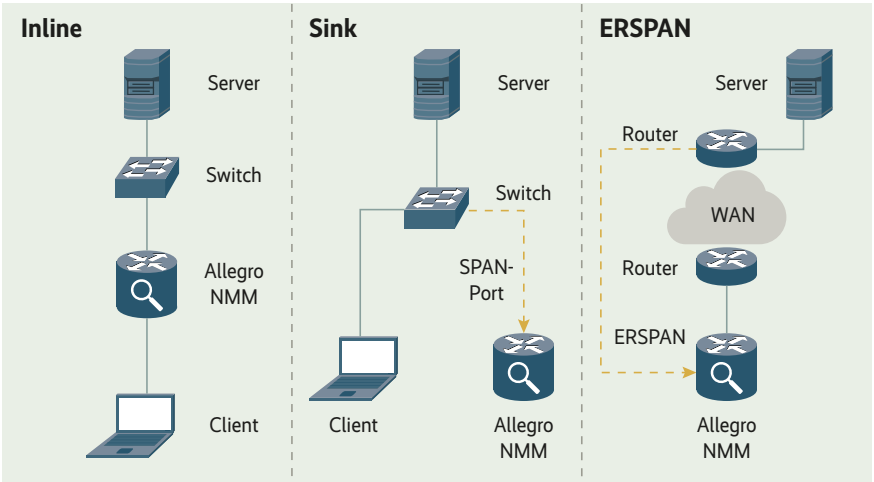
Ein HTTP-zu-HTTPS-Redirect für das Webinterface hat der Hersteller schon eingerichtet. Der Webserver verfügt zunächst über ein selbst signiertes Zertifikat, das sich im Test einfach durch ein eigenes im PEM-Format austauschen ließ. Die initialen Credentials finden sich in der Installationsanleitung.

Das Web-GUI lädt sehr zügig und ist klar strukturiert. Netzadmins werden sich schnell im Menübaum zurechtfinden, da der Aufbau dem OSI-Modell folgt (Abbildung 3). Auf allgemeine Menüpunkte folgen Layer 2 bis 4 und zu guter Letzt die Applikationsschicht (Layer 7).

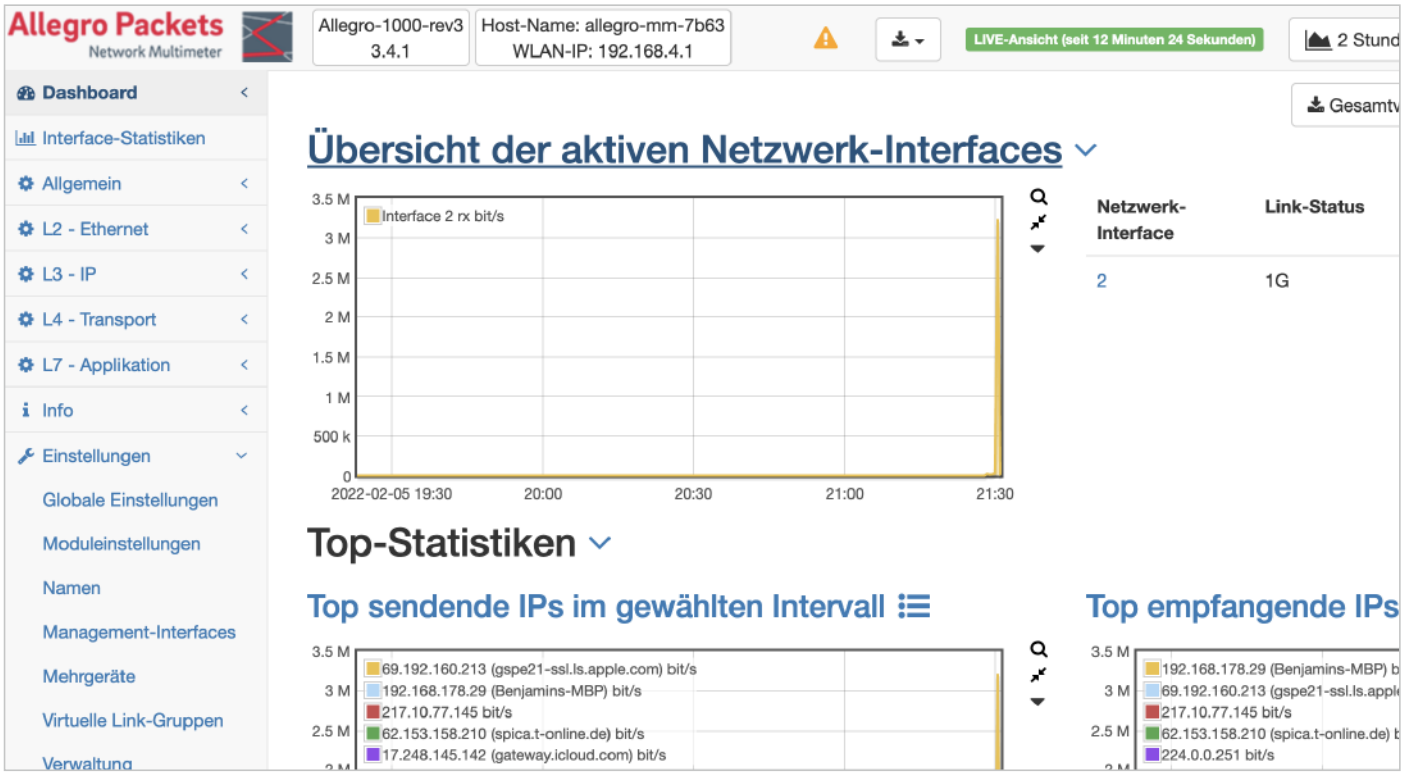
Das Dashboard startet mit Grafiken und Tabellen zum Status, dem Modus und der Auslastung der Schnittstellen. Auch die „Top Talker“ in Bezug auf sendende und empfangenden IP- und MAC-Adressen mitsamt Anzahl der übertragenen Pakete und Bytes sowie Top-Protokolle sind direkt einsehbar. Im oberen Bereich rechts lassen sich Refresh-Intervalle für die Graphen und Counter definieren und der Zeitbereich lässt sich durch einfaches Markieren mit der Maus einschränken, was beim Erforschen von Anomalien sehr hilfreich ist. Einen Zeitraum kann man sowohl absolut als auch relativ angeben (letzte Minute oder Stunde, gestern, heute et cetera).

Daneben gibt es die Möglichkeit, den Gesamtverkehr oder den Verkehr einer spezifischen Schnittstelle mitzuschneiden. Im Bridge-Modus ist jeweils nur die Empfangsrichtung des aufzuzeichnenden Interface sichtbar und nicht der von diesem Interface ausgehende Traffic. Andernfalls müsste man einen Mitschnitt aller Ports erstellen.

Das globale Dashboard enthält Traffic-Mengen pro NMM oder virtueller Linkgruppe in Form von Paketanzahl, Paketen pro Sekunde, übertragenen Bytes und Bits pro Sekunde.



Das Network Multimeter kann den Traffic auf dreierlei Weise mitschneiden: inline als Bridge, über den SPAN-Port am Switch als Sink und per ERSPAN-Tunnel von einem Router aus einem anderen Subnetz (Abb. 2).



Das Dashboard hält nach dem initialen Log-in bereits einige grundlegende Informationen bereit (Abb. 3).

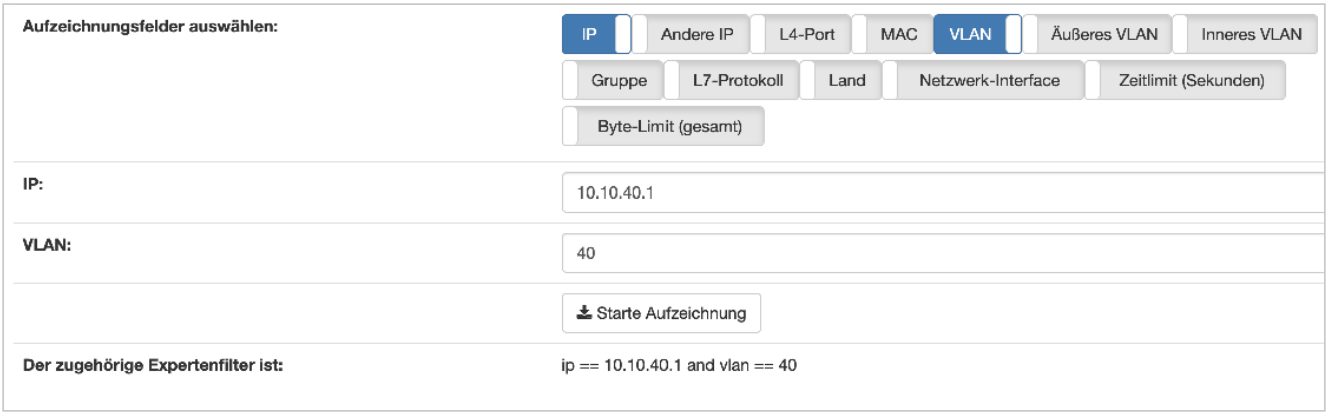
Neben dem globalen Dashboard zeigt das Qualitäts-Dashboard eine vereinfachte Analyse bekannter Fehlerbilder und Fehlerindikatoren an. So bietet es unter anderem die Darstellung von Bursts, anhand derer man temporäre Engpässe auch nachträglich erkennen kann. Auch TCP-Antwortzeiten eröffnen die Möglichkeit, ein träges Applikationsverhalten zu entlarven. TCP Retransmissions (wiederholte Übertragungsversuche) können auf fehlerhafte Transportwege hindeuten, etwa eine WAN-Anbindung mit Paketverlusten. Aber auch geblockte Kommunikationsbeziehungen auf Firewalls führen zwangsläufig zu Retransmissions der SYN-Pakete und fallen folglich hier auf. Das Erkennen von TCP Zero Windows erleichtert das Aufspüren überlasteter Zielsysteme.

Wem die fertigen Dashboards nicht ausreichen, der kann nach Bedarf auch eigene Dashboards mithilfe von Widgets zu den vier infrage kommenden OSI-Schichten erstellen.

Internettelefonie im Fokus

Eine Stärke des NMM ist die Analyse von VoIP, sprich des Signalisierungsprotokolls SIP und des Medientransportprotokolls RTP. Hierzu bietet das Dashboard unter „Triple Play“ einen Überblick über SIP-Antworttypen als Indikatoren für Fehler in der Signalisierung – etwa beim Anrufauf- und -abbau –, die RTP-Datenraten und die verwendeten Codecs. Bei Beeinträchtigungen der Sprach- oder Videoübertragung gibt es hier erste Anhaltspunkte. Etwas tiefer geht die Multi-SIP-Ansicht, die auch Gespräche mit den SIP-URIs anzeigt, die im öffentlichen Telefonnetz die Rufnummer im User-Anteil enthalten. Darin sind auch QoS-Markierungen und RTP-Paketverluste enthalten.

Der Menüpunkt Interface-Statistiken bietet einen grafischen Überblick über die physischen Schnittstellen, deren Modus (Sink oder Bridge), den Link-Status, die ausgehandelte Übertragungsrate, die



Parametrisierung einer einfachen Aufzeichnung. Hier wird nach der IP-Adresse 10.10.40.1 im VLAN 40 gefiltert. Die aktiven Filter sind oben hervorgehoben, unten sind die zugehörigen Expertenfilter sichtbar (Abb. 4).

Empfangsdatenrate und Fehler in Empfangsrichtung.

Der Bereich „Allgemein“ dient dem Aufzeichnen von Traffic. Hier kann man auch die angeschlossenen Speichermedien verwalten, im vorliegenden Fall die NVMe SSD. Massenspeicher lässt sich auch per USB und iSCSI anbinden. Die Einstellungen zum Paketringspeicher ermöglichen eine spätere Extraktion von Paketen auf interne oder externe Datenträger. Zudem besteht die Möglichkeit, Regeln für den Umfang der Aufzeichnungen zu erstellen.

Im Default sind vier parallele Aufzeichnungen möglich. Dabei lassen sich Dateien nach Zeit oder Größe aufteilen, um eine spätere Fehleranalyse zu vereinfachen, wenn der genaue Zeitpunkt eines Fehlers klar ist.

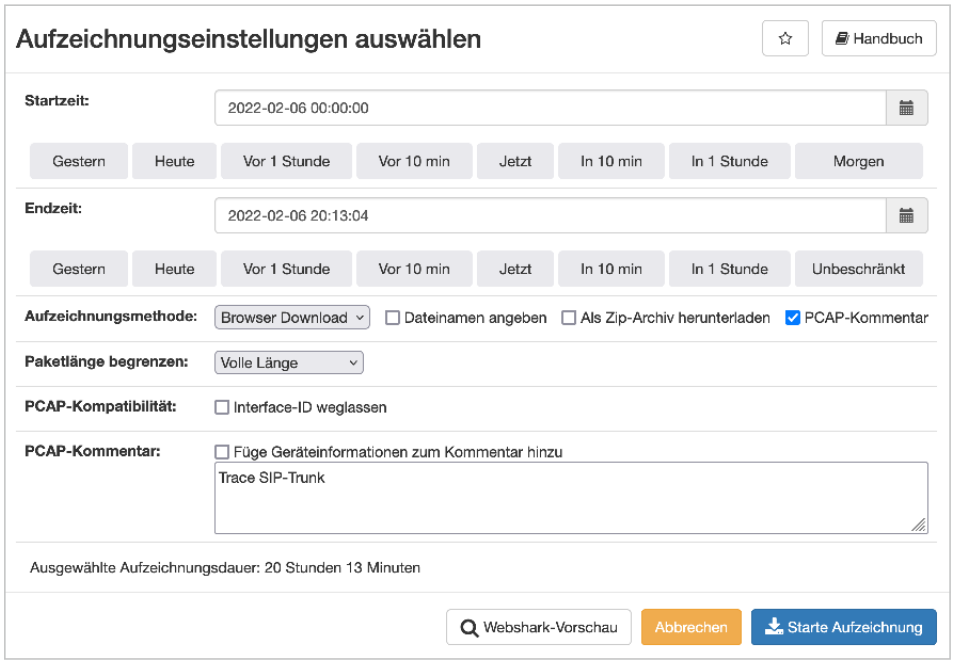
Um gezielt nur die benötigten Daten aufzuzeichnen, bietet das NMM Capture-Filter an, wie sie aus Tools wie tshark oder Wireshark bekannt sind. Allegro unterscheidet hier zwei Arten des Aufzeichnens: einfach und für Experten. Bei der einfachen Aufzeichnung lassen sich einzelne Filter wie IP-Adresse, MAC-Adresse, VLAN, Layer-7-Applikation oder das zugehörige Land über Schaltflächen aktivieren (Abbildung 4). Für Neugierige sind die zugehörigen Expertenfilter dargestellt.

Bei der Aufzeichnung im Expertenmodus können Geübte komplexe Filter erstellen, sei es mit Vergleichsoperatoren oder mit regulären Ausdrücken.

Unter dem Menüpunkt „Starte Aufzeichnung“ gelangt man – etwas überraschend – zu weiteren Einstellungen. Darin kann man einen Start- und Endzeitpunkt auswählen; in diesem Fall sogar retrospektiv und so weit der Paketringspeicher reicht. Als Ziel der Aufzeichnung stehen neben dem Browser-Download die lokale Ablage auf dem NMM, eine ERSPAN-Verbindung oder ein physisches Interface zur Verfügung.

Je nach organisatorischen Richtlinien und regionalen gesetzlichen Rahmenbedingungen kann es notwendig sein, die Paketlänge über sogenannte Capture Profiles zu begrenzen, um etwa im Falle von VoIP-Telefonaten nur die Header und nicht die Nutzdaten – also Sprache und Video – mitzuschneiden. Dies nutzen beispielsweise große Anwender wie der Provider Swisscom in der Schweiz. In den Headern sind das korrekte VoIP-Framing oder auch fehlende Sequenznummern erkennbar.

Für eine schnelle Analyse steht außerdem das Webshark-Feature zur Verfügung. Es bietet, wie der Name vermuten lässt, eine grafische Darstellung der aufgezeichneten PCAPs im Webbrowser. Im Default sind diese jedoch auf 1 MByte und im Maximum auf 500 MByte beschränkt. Das Feature erspart einem jedoch das Installieren von Software wie Wireshark und Co. Für den Fall wiederkehrender Fehlersymptome zu bestimmten Tageszeiten kann man Aufzeichnungen auch planen.



Ergänzende Einstellungen zu einer Aufzeichnung lenken den Fokus auf ein bestimmtes Zeitfenster (Abb. 5).

Passive Analyse von WAN-Strecken

Mit einem zweiten NMM eröffnet sich das Feature einer passiven WAN-Streckenmessung. Dabei findet im Unterschied zu Messungen gemäß RFC 2544, wie sie häufig bei Providern stattfinden, keine Injektion von Nutzdaten statt, sondern nur eine passive Prüfung auf Latenz und Paketverluste. Laut Allegro sind dabei etwa fünf Prozent Overhead für die Übertragung von Metadaten zwischen den beiden NMMs zu veranschlagen.

Bei Paketen, die nicht direkt über das NMM fließen, bietet sich ein Traffic-Export auf dem zu monitorenden Host an; Export-Agents stehen für Linux und Windows zur Verfügung. Dies sollte jedoch aufgrund der zusätzlichen Netzwerklast beim Export mit Vorsicht zur Anwendung kommen.

Auch eine statistische Analyse bereits aufgezeichneter Mitschnitte ist möglich. Dies bietet eine interessante Möglichkeit, von Kunden in Fehlersituationen produzierte PCAP-Dateien retrospektiv zu analysieren. Jedoch gehen bei einem Import im Default alle vorherigen Statistiken verloren und der Traffic wird nicht mehr weitergeleitet. Um dies zu verhindern, kann jedoch die Parallelanalyse zum Einsatz kommen.

Wer das Network Multimeter als Monitoring-Werkzeug einsetzen möchte, kann sich per E-Mail oder Syslog über Ereignisse benachrichtigen lassen, etwa über neue MAC- oder IP-Adressen (was natürlich nur in sehr statischen Netz-

Vordefinierte Rechte und Rollen beim Network Multimeter

Rechtename	Berechtigung
admin	unbeschränkter Zugriff
user	Lesezugriff, keine PCAP-Aufzeichnungen
replay-user	lesender Zugriff auf Replay-Analysen
capture	PCAP-Aufzeichnungen
restart-analysis	Neustart der aktuellen Ringpuffer-Analyse
api-pcap-4-eyes-authorization	PCAP-Aufzeichnungen muss ein anderer Nutzer mit dieser Rolle oder mit der Rolle admin freigeben.
api-voip-4-eyes-authorization	Zugriff auf SIP- und RTP-Statistiken muss ein anderer Nutzer mit dieser Rolle oder mit der Rolle admin freigeben.

werksegmenten sinnvoll ist), auffallend lange TCP-Handshakes, fehlende DNS-Antworten oder Änderungen von IP-Adressen (ARP-Spoofing-Erkennung).

Hinzu kommen Berichtsfunktionen zur grundlegenden Netzwerkstruktur, aber auch zu Abweichungen und Lastentwicklungen. Berichte sind stündlich, täglich, wöchentlich oder monatlich verfügbar. Sie zeigen unter anderem die meistgenutzten Protokolle und Kommunikationspartner, die meistgenutzten Verbindungen mitsamt Layer-7-Anwendungen sowie Start und Ende der Kommunikationsbeziehungen.

Analysen gemäß dem OSI-Schema

In Anlehnung an das OSI-Modell bietet das NMM vielfältige Statistikdaten. Diese sind klar strukturiert und man kann über verlinkte Referenzen auf andere Bereiche zugreifen, beispielsweise aus der Layer-2-Sicht auf zugehörige IP-Adressen oder Layer-7-Anwendungen. Ziel des Herstellers ist es, primär das Troubleshooting zu vereinfachen und sich dabei möglichst nicht an starre Konstrukte zu binden.

Zu den Layer-2-Statistiken, der Basis einer NMM-Analyse, gehören Aussagen über die MAC-Adressen wie die übertragenen Bytes und Paketanzahlen, die Anzahl der zugehörigen IP-Adressen, DHCP-Namen, Aktivitätsdauer sowie die genutzten Layer-7-Anwendungen. Hinzu kommen Informationen zur VLAN-Nutzung (inklusive Q-in-Q-Tunneling), zu Layer-2-QoS-Markierungen und zu ARP-Anfragen. Zudem stehen auch die per LLDP aufgezeichneten Inventarisierungsdaten sowie Informationen zum Spanning Tree Protocol (STP) zur Verfügung, anhand derer man beispielsweise Angriffe oder Fehlkonfigurationen erkennen kann. Ein Burst-Menüpunkt stellt die Empfangsauslastung nach einzelnen Schnittstellen dar, um diese besser erkennen zu können. Vor allem an Provider richten sich die Features zum Auflisten von PPPoE-Sessions mit Authentifizierungsstatus sowie Übertragungsmengen je Session und zu einzelnen MPLS-Labels.

Namensvergaben unter der Lupe

Umfassend stellt das NMM auch die Erkenntnisse auf Layer 3 dar: Hier findet man neben einzelnen IP-Adressen die zugehörigen Namen aus Quellen wie DHCP, DNS, NetBIOS oder LLDP. Selbst Länderinformationen auf Basis einer Geo-IP und des zugehörigen AS stehen zur Verfügung. Hinzu kommen Performanceindikatoren wie TCP-Handshakezeiten, übertragene Pakete und Bytes im gewählten Zeitintervall sowie der Durchsatz in Bit/s, aber auch DSCP-Markierungen. Zudem sind Fehlerindikatoren wie TCP-Retransmissions, DUP-ACKs, RSTs, Zero Windows und fragmentierte Pakete erkennbar.

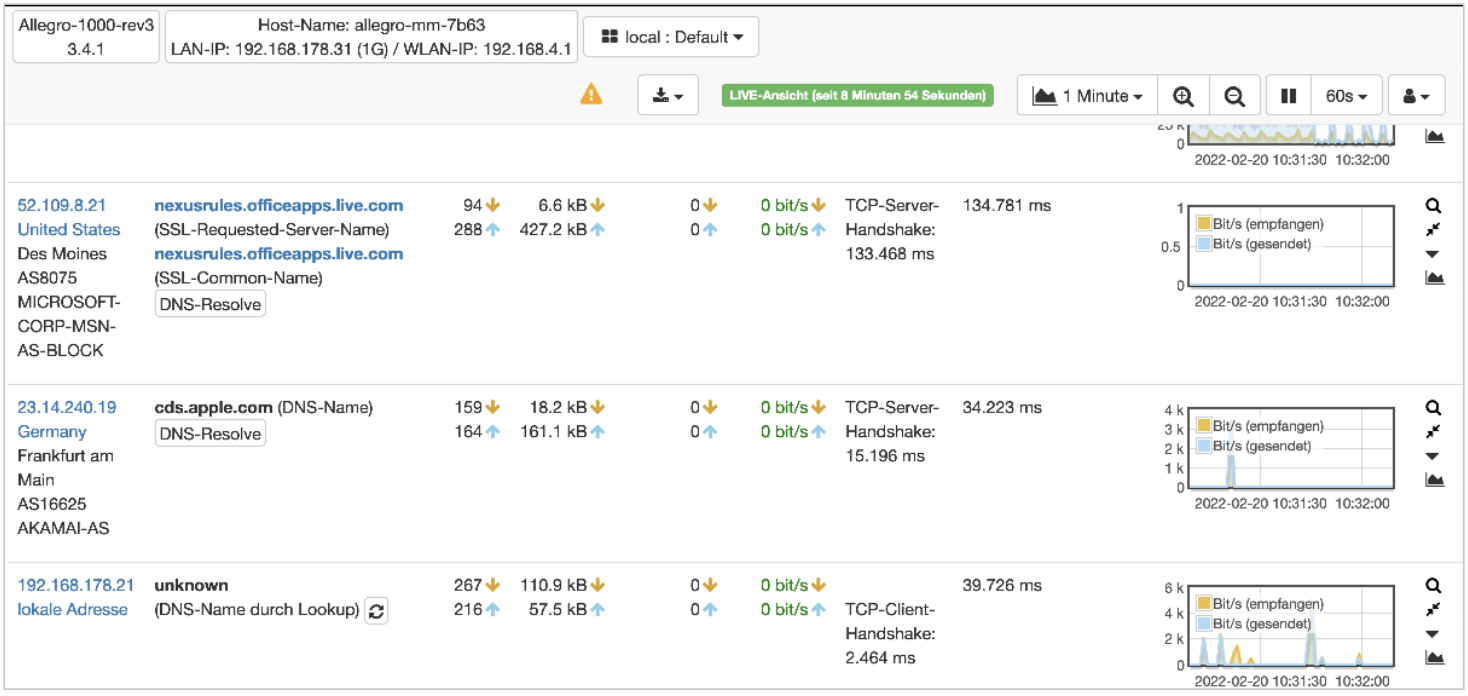
Wer bestimmte IP-Bereiche gruppiert auswerten möchte, kann flexibel Subnetze zusammenstellen. Zudem lassen sich Paare von Quell- und Ziel-IP-Adressen auswerten, um beispielsweise unerwünschte Kommunikationsbeziehungen in Incident-Response- oder Überlastungsszenarien erkennen zu können.

Auch wenn es vom OSI-Modell ausgehend nicht ganz passt, sind unter dem Menüpunkt Layer 3 auch DHCP- und DNS-Statistiken zu finden, etwa zu Record-Typen oder auch NX-Domain- und SERV-Fail-Antworten. Das NMM liefert auch Graphen zu unterschiedlichen ICMP-Typen wie Time Exceeded, Destination Unreachable, Echo Request/Reply sowie Latenzzeiten.

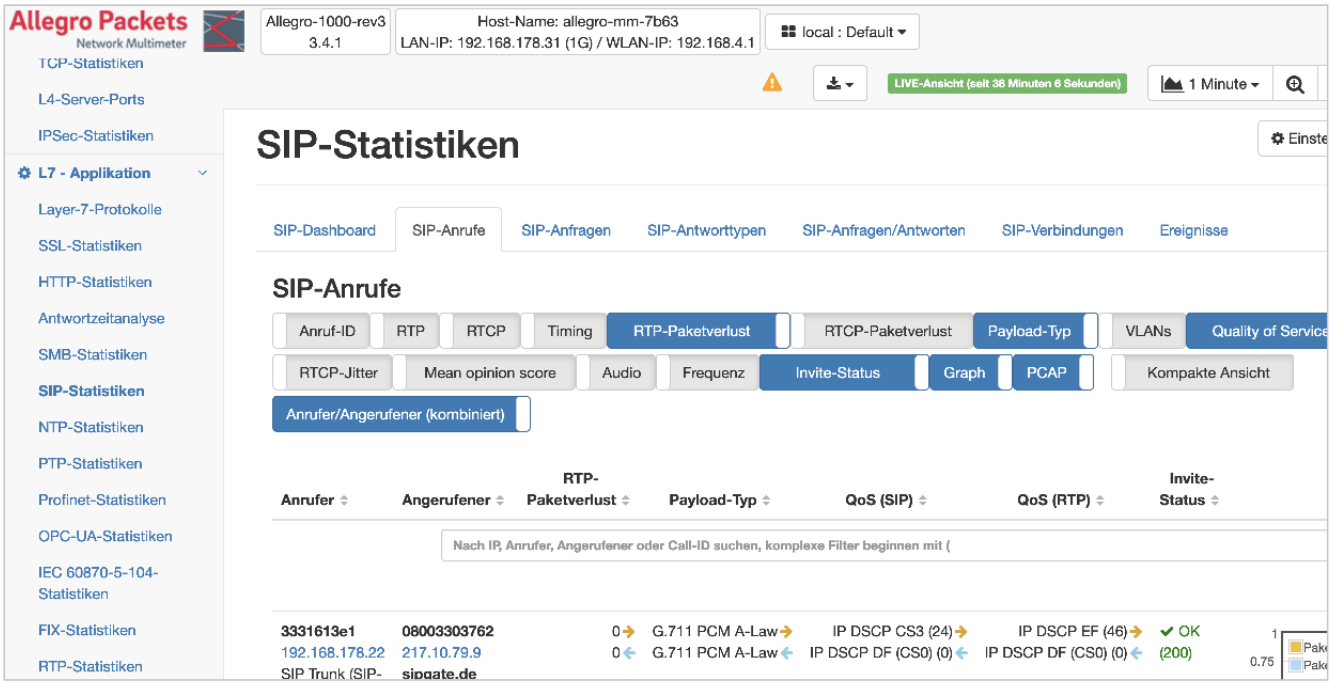
Die Statistiken der Transportschicht (Layer 4) liefern Informationen über die meistgenutzten Kommunikationsbeziehungen mit der erkannten Applikation sowie Antwortzeiten mitsamt Bewertungen von exzellent über normal bis problematisch. Auch DUP-ACKs, Retransmissions und One-Way/Two-Way-Latenzen finden in der Darstellung ihren Platz. Sogar Paketanzahlen und übertragene Bytes in bestimmten Intervallen und aufgelistet nach Zielports lassen sich angeben.

Layer 7 – endlich auf Anwendungsebene

Besonders spannend war im Test die Auswertung der Layer-7-Statistiken. Diese



Die IP-Statistiken zeigen die übertragenen Pakete, Datenmengen, Übertragungsraten und TCP-Handshake-Zeiten. Leider sind die Überschriften nicht fixiert und laufen somit beim Scrollen aus dem Bild (Abb. 6).



Das Network Multimeter liefert ausführliche Applikationsstatistiken zu VoIP. Aus diesem Fenster heraus wäre sogar ein PCAP-Export des Gesprächs möglich (Abb. 7).

bieten in Grafiken und Auflistungen einen guten Überblick der Top-Protokolle nach Paketen, Bytes und QoS. Sogar anwendungsspezifische PCAP-Exports lassen sich erstellen.

Für Sicherheitsaudits liefern die SSL-Statistiken Informationen etwa über die verwendeten Cipher Suites. Das NMM bietet aber auch Zertifikatsinformationen wie Gültigkeitszeiten, um korrespondierende Fehler beim TLS-Handshake erkennen zu können. Anhand der Bewertungen von TLS-Handshake-Zeiten sind Perfomanceengpässe rasch erkennbar.

HTTP-Statistiken bieten die Möglichkeit, die meistgenutzten Server, Antwortzeiten und Antwortcodes zu erkennen. Dies betrifft meist OCSP-Abfragen (Online Certificate Status Protocol) während des Aufbaus von TLS-Verbindungen. Die meisten anderen Verbindungen sind glücklicherweise bereits über TLS verschlüsselt.

Bei SMB-Problemen oder Audits von Fileshare-Zugriffen über dieses Protokoll ist das SMB-Statistikmodul hilfreich. Es bietet Ansichten der Anzahl von SMB-Shares mitsamt erfolgreichen und fehlerhaften Verbindungen zu Shares sowie die zugehörigen Clients und Server. Aber auch die Informationen zur eingesetzten SMB-Version und einer Information, ob SMB-Verschlüsselung zum Einsatz kommt, unterstützen Sicherheitsaudits.

Eine besondere Stärke des NMM sind, wie bereits angedeutet, die VoIP-Funktionen, konkret die SIP- und die RTP-Statistiken. So listet es Anrufe mit Rufnummern, den beteiligten SIP-Servern, dem Codec, Paketverlusten, QoS-Markierungen und INVITE-Status auf. Selbst eine Suche nach Gesprächen einer bestimmten Zielrufnummer ist möglich. Aber auch andere Qualitätsmerkmale wie Paketverluste und Jitter sind auswertbar.

Darüber hinaus lassen sich die verwendeten SIP-Methoden statistisch auswerten. Im SIP-Modul kann man Ereignisse anlegen, die eine Benachrichtigung auslösen, etwa über erhöhte Latenzzeiten oder die Überschreitung einer gewissen Anrufdauer, um die missbräuchliche Anwahl teurer Sonder- oder Auslandsrufnummern erkennen zu können.

Im Fehlerfall könnten sogar Gespräche retrospektiv als PCAP-Datei exportiert werden. So ließe sich – unter Beachtung gesetzlicher und betrieblicher Vorgaben – die Gesprächsqualität unabhängig von der subjektiven Anwendermeinung direkt prüfen.

Ohne Zeit kein Netz

Korrekte Zeitstempel sind essenziell fürs Funktionieren von Netzwerken. Ohne sie können beispielsweise TLS-Verbindungen fehlschlagen. Das NMM listet die NTP-Server mit letzter Aktivität, deren Versionsnummer, das Abfrageintervall, die Strata sowie die Anzahl der Clients auf. So fällt beispielsweise ein falsch konfigurierter NTP-Server auf. Für PTP gibt das NMM die PTP-Peers an, inklusive des Zeitpunkts der letzten Synchronisation.

Neben den Statistiken zu klassischen IT-Applikationen stehen solche zu den OT-Applikationen Profinet und OPC-UA zur Verfügung. So können Systemverantwortliche auch im industriellen Umfeld Ursachen von Lasten, Performanceengpässen und sonstigen Fehlerbildern erkennen. Profinet bietet beispielsweise eine Auflistung der Top Talker, die verwendete Bandbreite, den Jitter sowie Profinet-Fehler und -Alarme. Das OPC-UA-Modul erkennt unbeantwortete oder doppelte Anfragen sowie unangefragte Antworten und Dienstefehler des OPC-UA-Servers.

Ergänzend zu den Statistik- und Aufzeichnungsfeatures bringt das Network Multimeter auch einen iPerf3-Server für Performancemessungen mit. Ein Aufbrechen der TLS-Verschlüsselung bietet das Gerät nicht, da Allegro es mit Fokus auf das Troubleshooting und nicht als Securitywerkzeug entwickelt hat.

Zum NMM gehört natürlich auch ein Rechte- und Rollenmodell (siehe Tabelle). Als Authentifizierungsprotokolle bietet es LDAP und TACACS+. RADIUS befindet sich noch auf der Roadmap des Herstellers. Leider fehlt die Dokumentation für TACACS+. LDAP funktionierte im Test inklusive LDAP-Gruppenzuweisung zu einer Rechtegruppe problemlos.

Für lokale Anwender besteht auch die Möglichkeit einer Zwei-Faktor-Authentifizierung auf Basis von TOTP (Time-

based One-Time Password) – jedoch nicht für LDAP-User. Managementzugriffe lassen sich derzeit nicht auf bestimmte Quell-IP-Adressen einschränken. Dies wäre die Aufgabe einer vorgelagerten Firewall. Für kommende Versionen plant Allegro, das Rechte- und Rollenmodell um weitere Möglichkeiten zur Umsetzung des Vier-Augen-Prinzips zu erweitern.

Schnittstellen zu Drittsystemen

Für Zugriffe eigener Managementsysteme auf die Statistikdaten bietet das NMM eine REST-API an. Es liefert die Daten als JSON-Objekte. Die Dokumentation ist jedoch recht dürftig. Für kommende Releases sind laut Allegro auch Schnittstellen zu Monitoringsystemen wie Zabbix, aber auch zu Securitydiensten geplant, um Hinweise zu potenziellen Kommunikationsbeziehungen mit bekannten Spam- oder Malware-Quellen anzeigen zu können.

Erfreulicherweise gibt es keine Lizenzen für einzelne Funktionen, sondern nur eine Gesamtlizenz mit allen Features. Firmware-Updates erfordern einen aktiven Supportvertrag. Allegro legt dem Network Multimeter keine deutsche Dokumentation bei, sondern verweist auf eine Google-Übersetzung.

Für das reguläre Management im Unternehmens- oder Behördeneinsatz liefern regelmäßig versendete E-Mail Benachrichtigungen mit Crash-Berichten, Uptime, Temperatur der CPU, IP-Adressen, aber auch die voraussichtliche Zeit bis zum Erreichen der 90-prozentigen Ringspeicherauslastung. Die ist ein wichtiger Indikator, da ab dann das Löschen der ältesten Daten beginnt.

Mittels Syslog-Export ermöglicht das Network Multimeter das Sammeln von Meldungen an einem zentralen Punkt. Auch ein SNMPv3-Zugang ist möglich. Ein Backup der Konfiguration existiert in Gestalt von neun JSON-Dateien als ZIP-Archiv.

Willkommene Neuerungen in Release 3.5

Im nach dem Test erschienenen Release 3.5 hat Allegro eine TCP-Flussgraph-Analyse auf Paketebene ergänzt. Sie stellt eine Liste von Paketen dar, über die Referenzzeiten zu vorangegangenen Paketen erkennbar sind. Auf diese Weise lassen sich beispielsweise Handshake- und Applikations-Delta-Delays erkennen. Zusätzlich ist nun ein PCAP-Streaming an SFTP-Server möglich, um nicht auf lokale Ressourcen der Appliance oder des Administratorendgeräts beschränkt zu sein.

Zudem gab es Ergänzungen im Rechte- und Rollenmodell. Konfigurierbare Schablonen für bestimmte Gruppen und neue Rollen erhöhen die Flexibilität insbesondere in größeren Umgebungen. Außerdem sind nun mehrere Storage-Devices gleichzeitig aktivierbar. Damit läuft der Paketringspeicher parallel zur PCAP-Speicherung. Bei der Übertragung bestehender PCAP-Dateien auf ein Speichergerät muss die Festplatte nicht mehr deaktiviert und damit der Ringspeicher ausgeschaltet werden. Zudem kann das NMM nun LTE-USB-Adapter für die Fernverwaltung per Mobilfunk einbinden.

Auch die in der getesteten Version bereits recht weit gediehenen VoIP-Funktionen wurden nochmals erweitert, beispielsweise um weiter gehende RTP-Visualisierung und -Analyse. Zudem besteht nun die Möglichkeit, Datenverkehr zwischen IP-Adressgruppen auszuwerten, etwa aller Adressbereiche von Standort A zu all jenen von Standort B.

Für die kommende Version 3.6 will Allegro nach eigenen Angaben die Authentifizierung gemäß IEEE 802.1X auf der Managementschnittstelle sowie für Let's-Encrypt-Zertifikate implementieren. Zudem ist geplant, dass das Network Multimeter mehrere PCAP-Dateien importieren kann.

Fazit

Das Network Multimeter von Allegro Packets erleichtert die Auswertung von Netzwerkmitschnitten erheblich. Das aufgeräumte, dem OSI-Modell nachempfundene Menü und die schnelle Suche überzeugten im Test. Das Handling des Paketringspeichers erfordert jedoch einiges an Eingewöhnung. Die gute Performance durch den Einsatz der In-Memory-Datenbank unterstützt das Troubleshooting. Das ERSPAN-Feature macht die Appliance auch bei zentralisierten Installationen in komplexen Netzumgebungen flexibel einsetzbar. (un@ix.de)

Benjamin Pfister

ist Leiter des Sachgebiets Netze und Telekommunikation der Stadt Kassel sowie Inhaber der Pfister IT-Beratung.

WERTUNG

⊕ Web-GUI und Suchfunktionen sehr performant durch In-Memory-Datenbank
⊕ umfassende VoIP-Analyse sowohl für SIP als auch für RTP
⊕ Einsatz als Ziel eines ERSPAN-Tunnels
⊕ Entwicklung und Support komplett in Deutschland

⊖ Dokumentation lückenhaft und nur auf Englisch verfügbar
⊖ nur bedingt für Langzeitanalysen geeignet
⊖ keine passive Durchschaltung der integrierten Ports im Bridge-Modus bei fehlender Stromversorgung (nur über Zusatzbaugruppen)

DATEN UND PREISE

Hersteller	Allegro Packets GmbH
Modell	Network Multimeter 1000
aktuelle Version	3.5 (im Test 3.4.1)
Maße (B × H × T)	264 mm × 43 mm × 226 mm
Plattform	Super Micro Server, Debian Linux
Skalierung	Capture und Analyse bis 20 GBit/s, Historie bis zu 4 Mio. Verbindungen (16 GByte RAM)/128 Millionen Verbindungen (512 GByte RAM), bis zu 1 Million offene Verbindungen
Monitoring-Ports	3 × 1 GE, 2 × 10 GE (Kupfer), 2 × SFP+
Optionen	Bypass-Karte für LWL (2 × 10GBase-SR) oder Kupferanschlüsse (4 × 1000Base-T), 2 × 10GE mit nBase-T, SFP28, QSFP, QSFP28, GPS-Messkarte