LAN diagnostics with the Allegro Network Multimeter

Whether lags in online meetings or sluggish applications: Analyzing transmission errors in the network is often complex and time-consuming. The Allegro Network Multimeter simplifies troubleshooting.

By Benjamin Pfister

The everyday life of system administrators has always included complaints about slow or erroneous on-premises or cloud applications. In recent years, the proportion of video conferencing and other real-time services has increased, which is not only much more demanding on the network requirements than the classics email and WWW. Such disruption is also particularly unpleasant. The first suspect is usually the network, but a root cause analysis can be quite complex.

Depending on the complexity and throughput of the network, a standard notebook quickly reaches its limits as test equipment. The alternative is a specialized instrument. In addition to the RJ45 port for the IP KVM of the underlying Supermicro system, the Allegro Network Multimeter (ANM) 1000 rev. 3 v3.4.1 from Allegro Packets contains six RJ45 LAN ports, one of which is permanently designated for administering the system. In addition, there are three 1GBASE-T and two 10GBASE-T ports. Two SFP+ slots are available for a fiber optic connection, for which the manufacturer supplies dual-speed 1G-SX and 10G-SR SFP+ modules. In addition, there are two USB-A ports that can, for example, accommodate a WLAN adapter such as the TP-Link TL-WN725N, which is also included (Figure 1). The system has eight CPU cores. Larger captures with up to 10 GBit/s are stored by a 2 TByte NVMe SSD (Seagate FireCuda 520).

In contrast to the standard configuration, the test device was equipped with a memory expansion from 16 to 64 GB RAM. The carrying case helps with mobile use. The tested appliance does not offer a redundant external power supply. This can be tricky in inline recording mode, if the device is used as a bridge in the data stream: The integrated ports, unlike larger models, do not allow physical power-through in case of a power failure.

Linux appliance as a network tester

The ANM is based on Debian Linux. For fast packet processing, the appliance uses the open source project Dataplane Development Kit (DPDK), which the manufacturer actively supports. By default, it only uses in-memory storage and does not permanently store network information. This offers advantages in terms of data protection.

X-TRACT

- The Allegro Network Multimeter (ANM) from Leipzig-based Allegro Packets serves as a stand-alone appliance for problem and usage analysis in complex networks - even for providers.
- With the ANM, numerous sources of error can be isolated in a clear manner.
- The ANM pays special attention to real-time media streaming as a time-critical and thus particularly error-sensitive application.

Initially, the data is only available during the analysis. An in-memory database stores the metadata of the processed packets - so they are lost during a reboot or shutdown. This also applies to unexpected power failures, which are particularly annoying during longer troubleshooting sessions.

In addition, however, Allegro Packets' ANM also offers a packet ring buffer. In this case, the packets end up on the NVMe SSD. Thus, they are available even after a reboot. An interesting possibility is the subsequent analysis of the packet ring buffer: You can thus track events independent of time and place. However, the analysis interrupts the live mode, i.e. the processing in the in-memory storage.

Until 90 percent of the maximum memory capacity is reached, the ANM stores in the packet ring buffer. After that, it starts to overwrite the oldest data. The maximum length of the recording depends on the traffic and the memory capacity and is therefore difficult to plan. This can be problematic for the troubleshooting as relevant data might be overwritten. Therefore, it is advisable to test prior purchase so that you can plan for sufficient buffer. Email reports with estimates of how long it will take to reach 90 percent memory utilization are helpful.

In addition to the appliance used here, the manufacturer offers several options, from the smallest and lightest Allegro 200 (260 g) with two GE interfaces to 19-inch appliances (Allegro 5500) with four height units and up to 150 GBit/s throughput as well as

a 576 TByte integrated ring buffer. A virtual appliance is also available.

Integration options

In order for the device to produce and analyze statistical data, it must first collect traffic. This can be done in different ways: The manufacturer calls these sink, bridge and endpoint modes (Figure 2).

In sink mode, i.e. out of band, the device receives traffic from a test access point (TAP) or a mirror port (SPAN, switched port analyzer) on the switch. In SPAN mode, however, it is important to keep in mind that the SPAN destination should provide at least twice the link capacity for transmit and receive direction transmission for bidirectional capturing.

In bridge mode, the device operates inline, as part of the communication path. Physical and vertically related interface pairs always form a transparent bridge. The operating mode can be switched between sink and bridge. If the analyzer fails, bridge mode means an interruption in productive traffic.

In the event that the appliance is not on the same LAN as the traffic source, the ANM can serve as an ERSPAN (Encapsulated Remote SPAN) target in endpoint mode, i.e., it can record the traffic via a tunnel. This makes the appliance flexible to use and worked well in the lab.

In addition, the ANM offers the possibility of an Internet Protocol Flow Information Export (IPFIX) to a corresponding collector for central collection. The manufacturer also recommends this for long-term statistics.

Both NTP and PTP (Network Time Protocol / Precision Time Protocol) are available for correct time stamps in the statistics. This is essential for correct correlation of events in troubleshooting.

First steps with or without wire

The system can be managed out of band, both wired and wireless. The dedicated management port works in DHCP client mode. If a DHCP server is not available, a USB keyboard and Shift + S can be used to assign the IP address 192.168.0.1. It is also possible to add a secondary management interface via USB Ethernet adapter.

The Allegro Network Multimeter offers various LAN connections. WLAN connectivity is provided by a USB adapter, which is included with delivery (Fig. 1).

A WLAN USB dongle additionally provides an 802.11b/g/n interface in access point mode and a pre-configured SSID according to the pattern allegro-mm-xxxx. In this case, the Allegro Network Multimeter also serves as a DHCP server with the IP address 192.168.4.1. The latter is also distributed as a DNS server address via DHCP, making it easy to control the web GUI via https://allegro or https://192.168.4.1. The analysis functions cover controller-based WLANs. Using CAPWAP (Control And Provisioning of Wireless Access Points), data such as the assigned transmission rates and signal qualities can be read out.

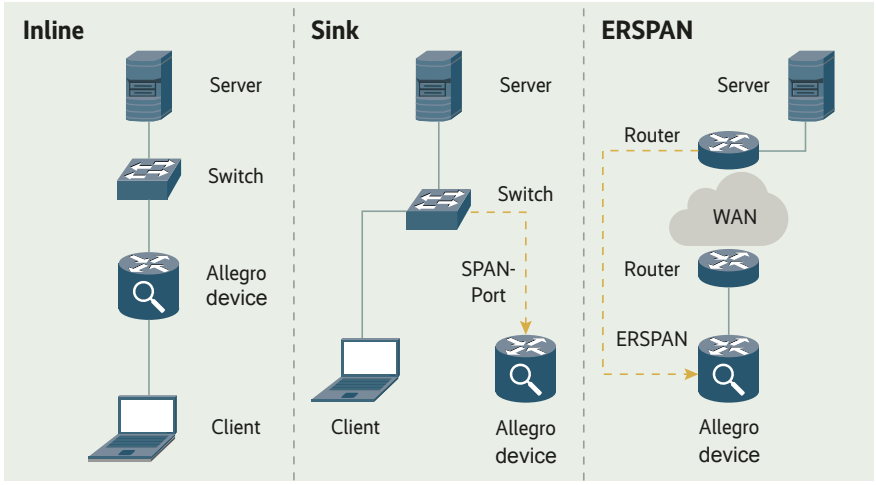
An HTTP-to-HTTPS redirect for the web interface has already been set up by the manufacturer. The web server initially has a self-signed certificate, which in the test could easily be replaced with one in PEM format. The initial credentials can be found in the installation manual.

The web GUI loads very quickly and is clearly structured. Network admins will quickly find their way around the menu tree, since the structure follows the OSI model (Fig. 3). General menu items are followed by Layers 2 to 4 and, last but not least, the application layer (Layer 7).

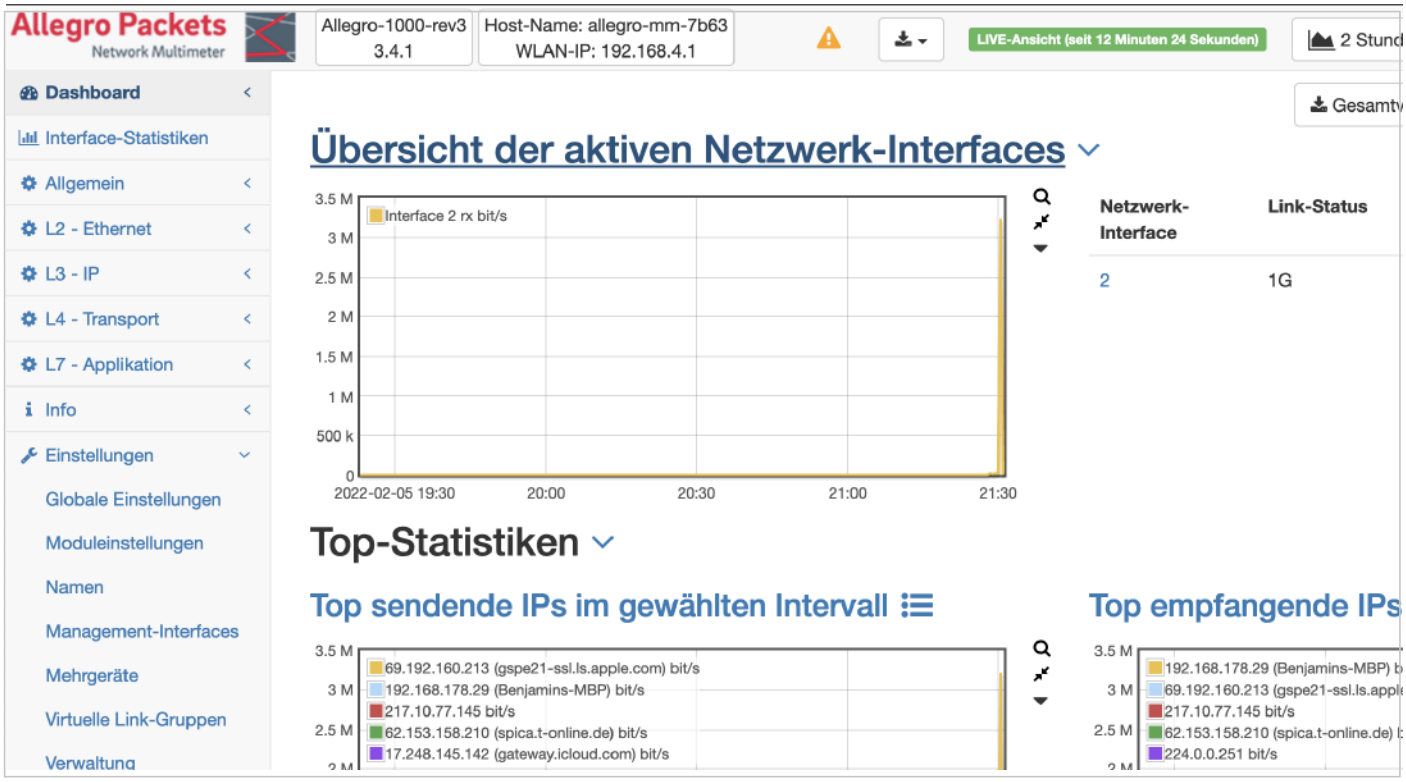
The dashboard starts with graphics and tables on the status, mode and utilization of the interfaces. The "top talkers" in terms of sending and receiving IP and MAC addresses, including the number of packets and bytes transmitted, as well as top protocols can also be viewed directly. In the upper area on the right, refresh intervals can be defined for the graphs and counters, and the time range can be restricted by simply marking it with the mouse, which is very helpful when exploring anomalies. A time period can be specified both absolutely and relatively (last minute or hour, yesterday, today et cetera).

Furthermore, there is the possibility to record the total traffic or the traffic of a specific interface. In bridge mode only the receive direction of the interface to be recorded is visible and not the traffic originating from this interface. Otherwise, you would have to create a recording of all ports.

The global dashboard contains traffic quantities per ANM or virtual link group in the form of packet count, packets per second, transmitted bytes and bits per second.



The Allegro Network Multimeter can record traffic in three ways: inline as a bridge, via the SPAN port on the switch as a sink, and via ERSPAN tunnel from a router from another subnet (Fig. 2).



After the initial login, the dashboard already displays some basic information (Fig. 3).

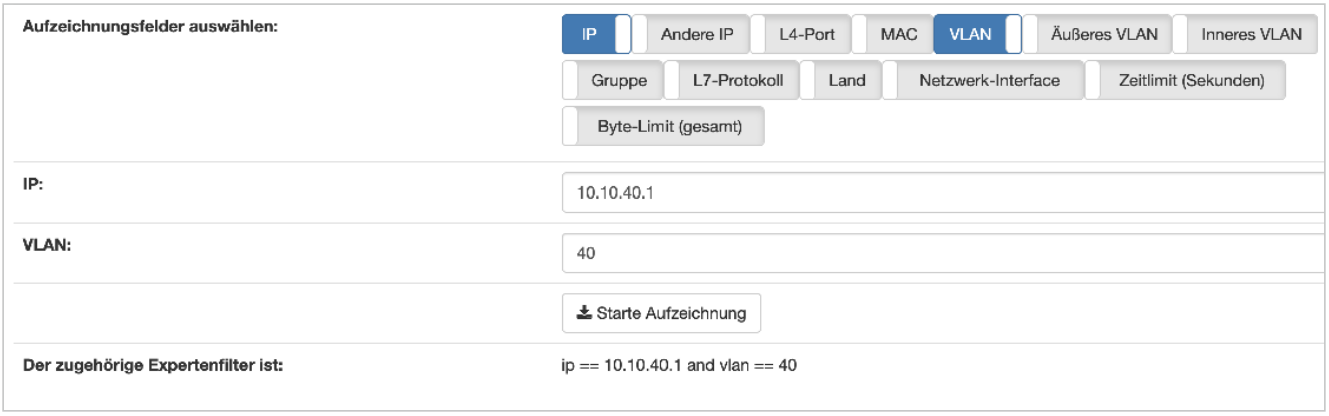
In addition to the global dashboard, the quality dashboard displays a simplified analysis of known error patterns and error indicators. Among other things, it offers the display of bursts, which can also be used to retrospectively identify temporary bottlenecks. TCP response times also open up the possibility of exposing sluggish application behavior. TCP retransmissions (repeated transmission attempts) can indicate faulty transport paths, such as a WAN connection with packet losses. But blocked communication relationships on firewalls also inevitably lead to retransmissions of SYN packets and are consequently conspicuous here. The detection of TCP Zero Windows facilitates the detection of overloaded target systems.

If the ready-made dashboards are not sufficient for you, you can also create your own dashboards using widgets for the four OSI Layers in question.

Internet telephony in focus

One of the strengths of the ANM is the analysis of VoIP, i.e. the signaling protocol SIP and the media transport protocol RTP. For this purpose, the dashboard provides an overview of SIP response types under "Triple Play" as indicators of errors in the signaling - for example, during call setup and teardown -, the RTP data rates and the codecs used. In the case of impairments in voice or video transmission, this provides the first clues. The multi-SIP view, which also displays calls with SIP URIs that contain the phone number in the user portion of the public telephone network, goes a bit deeper. This also includes QoS markers and RTP packet loss.

The Interface Statistics menu item provides a graphical overview of the physical interfaces, their mode (sink or bridge), link status, negotiated transmission rate, receive data rate and errors in receive direction.



Parameterisation of a simple capturing, where filtering is done according to the IP address 10.10.40.1 in VLAN 40. The active filters are highlighted at the top, the associated expert filters are visible at the bottom (Fig. 4).

The "General" area is used to record traffic. Here you can also manage the connected storage media, in this case the NVMe SSD. Mass storage can also be connected via USB and iSCSI. The settings for the packet ring buffer enable a later extraction of packets to internal or external storage media. In addition, it is possible to create rules for the scope of captures.

By default, four parallel captures are possible. Files can be divided according to time or size to simplify later error analysis when the exact time of an error is clear.

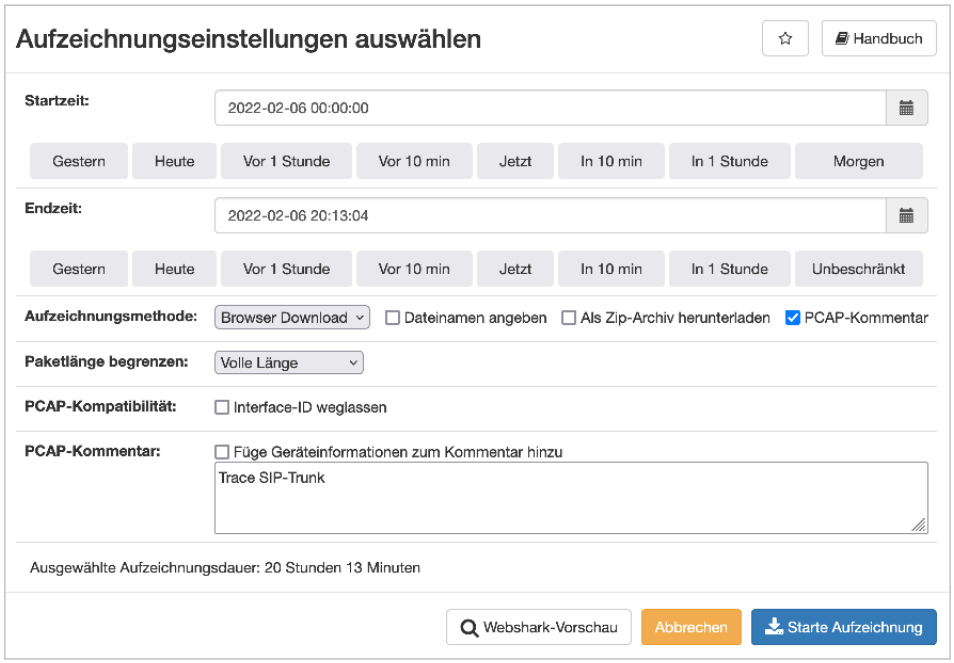
In order to selectively record only the required data, the ANM offers capture filters, as known from tools such as tshark or Wireshark. The Allegro Network Multimeter distinguishes here between two types of capturing: simple and for experts. In the simple recording mode, individual filters such as IP address, MAC address, VLAN, Layer 7 application, or the associated country can be activated via buttons (Figure 4). For the curious among us, the associated expert filters are shown.

When capturing in expert mode, experienced users can create complex filters, be it with comparison operators or with regular expressions.

The menu item 'Capture all traffic' leads - somewhat surprisingly - to further settings. Here you can select a start and end time; in this case even retrospectively and as far as the packet ring buffer recorded. In addition to the browser download, local storage on the ANM, an ERSPAN connection, or a physical interface is available as a destination for the capturing.

Depending on organizational guidelines and regional legal conditions, it may be necessary to limit the packet length via so-called capture profiles, for example, to capture only the headers and not the user data - i.e., voice and video - in the case of VoIP telephone calls. This is used, for example, by large users such as the provider Swisscom in Switzerland. The correct VoIP framing or even missing sequence numbers can be identified in the headers.

The Webshark feature is also available for a quick analysis. As the name suggests, it offers a graphical representation of the recorded PCAPs in the web browser. However, these are limited to 1 MByte by default and 500 MByte at the maximum. However, the feature saves you from installing software like Wireshark and such. You can also schedule captures in case of recurring error symptoms at certain times of the day.



Complementary settings for a capturing direct the focus to a particular specific time window (Fig. 5).

Passive analysis of WAN links

A second ANM opens up the feature of passive WAN link measurement. In contrast to measurements in accordance with RFC 2544, which often take place at providers, there is no injection of user data, but only a passive check for latency and packet loss. According to the Allegro Network Multimeter, this involves about five percent overhead for the transmission of metadata between the two ANMs.

For packets that do not go directly through the ANM, a traffic export on the host to be monitored is a good option; export agents are available for Linux and Windows. However, this should be used with caution due to the additional network load during export.

Statistical analysis of previously recorded captures is also possible. This offers an interesting possibility to retrospectively analyze PCAP files produced by customers in error situations. However, when importing in Default mode, all previous statistics are lost and the traffic is no longer forwarded. To prevent this, however, parallel analysis can be used.

Those who want to use the Allegro Network Multimeter as a monitoring tool can be notified via email or syslog about events, such as new MAC or IP addresses (which of course only makes sense in very static network segments), conspicuously long TCP handshakes, missing DNS responses or changes to IP addresses (ARP spoofing detection).

Predefined rights and roles in Allegro Network Multimeter

Right name	Authorization
admin	Unrestricted access
user	Reading access, no capturing
relay-user	Reading access to replay analysis
capture	PCAP capturing
restart-analysis	Restarting the current ring buffer analysis
apl-pcap-4-eyes-authorization	PCAP capturing must be shared by another user with this role or with the admin role
apl-voip-4-eyes-authorization	Access to SIP and RTP statistics must be shared by another user with this role or with the admin role

In addition, there are reporting functions on the basic network structure, but also on deviations and load developments. Reports are available hourly, daily, weekly, or monthly. Among other things, they show the most frequently used protocols and communication partners, the most frequently used connections including Layer 7 applications, and the start and end of communication relationships.

Analysis according to the OSI scheme

Based on the OSI model, the ANM offers a wide range of statistical data. These are clearly structured and one can access other areas via linked references, for example from the Layer 2 view to associated IP addresses or Layer 7 applications. The manufacturer's goal is primarily to simplify troubleshooting and, as far as possible, not to be bound to rigid constructs.

Layer 2 statistics, the basis of an ANM analysis, include statements about MAC addresses such as the bytes and packet numbers transmitted, the number of associated IP addresses, DHCP names, activity duration and the Layer 7 applications used. Added to this is information on VLAN usage (including Q-in-Q tunneling), Layer 2 QoS markings and ARP requests.

In addition, inventory data captured via LLDP and information on the Spanning Tree Protocol (STP) are also available, which can be used to detect attacks or misconfigurations, for example. A burst menu item displays the receive load according to individual interfaces in order to be able to recognize them better. The features for listing PPPoE sessions with authentication status and transmission quantities per session and for individual MPLS labels are aimed primarily at providers.

Name assignments under the microscope

The ANM also comprehensively presents the findings on Layer 3: Here, in addition to individual IP addresses, the associated names from sources such as DHCP, DNS, NetBIOS or LLDP can be found. Even country information based on a geo-IP and the associated AS is available. In addition, there are performance indicators such as TCP handshake times, transmitted packets and bytes in the selected time interval, and throughput in bit/s, as well as DSCP markers. In addition, error indicators such as TCP retransmissions, DUP-ACKs, RSTs, Zero Windows and fragmented packets can be identified.

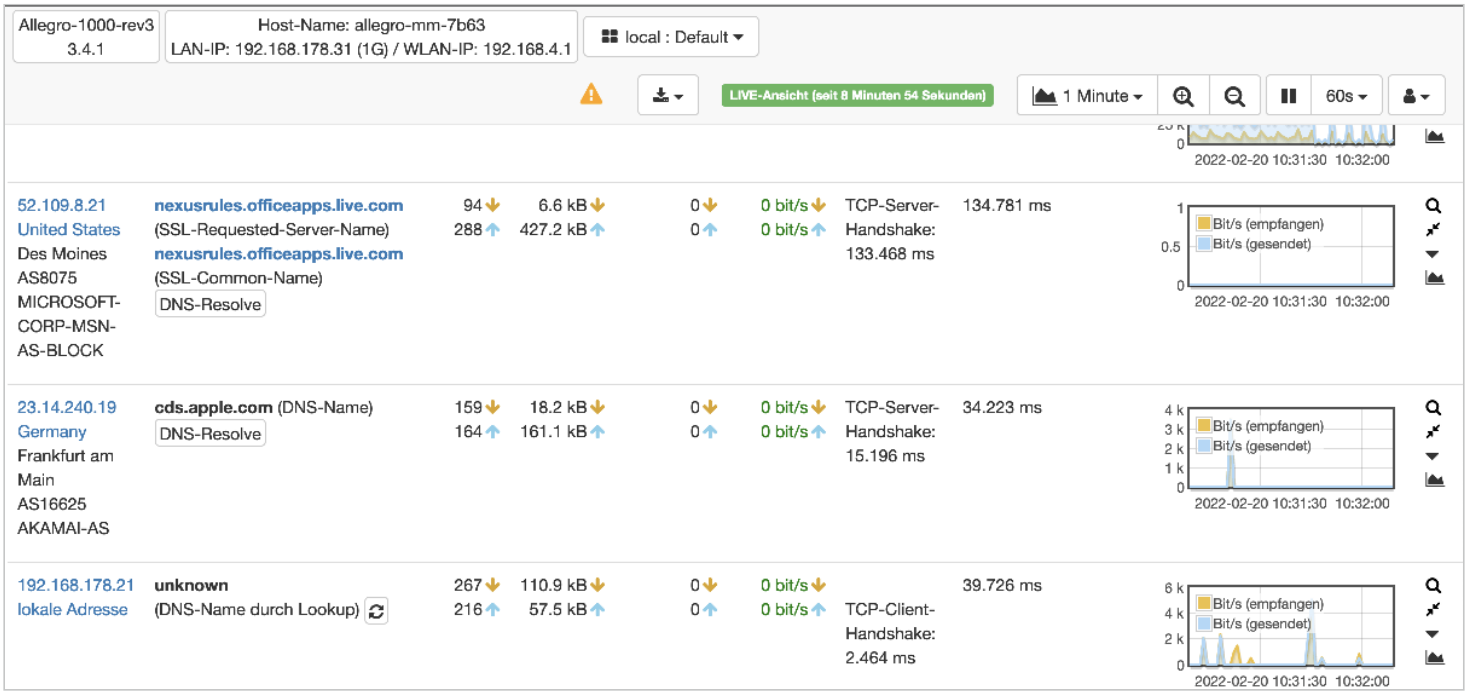
If you want to evaluate specific IP ranges in groups, you can flexibly compile subnets. In addition, pairs of source and destination IP addresses can be evaluated in order to be able to detect undesired communication relationships in incident response or overload scenarios, for example.

Even if it does not quite fit the OSI model, DHCP and DNS statistics can also be found under the Layer 3 menu item, for example on record types or NX domain and SERVFail responses. The ANM also provides graphs for different ICMP types such as Time Exceeded, Destination Unreachable, Echo Request/Reply and Latency.

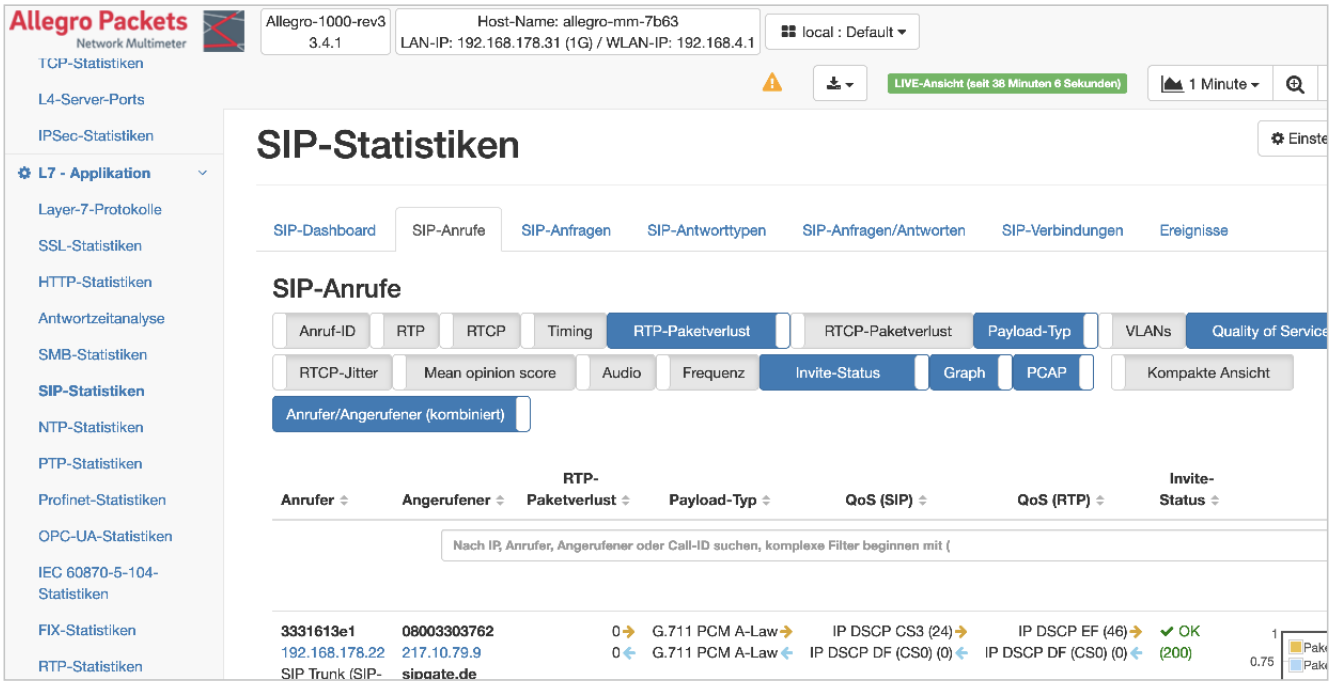
The transport layer (Layer 4) statistics provide information about the most used communication relationships with the detected application as well as response times including ratings from excellent to normal to problematic. DUP-ACKs, retransmissions and one-way/two-way latencies also find their place in the display. Even packet counts and bytes transferred at certain intervals and listed according to target ports can be specified.

Layer 7 - finally at application stage

The evaluation of the Layer 7 statistics was particularly exciting in this test.



The IP statistics show the transmitted packets, data volumes, transfer rates and TCP handshake times. Unfortunately, the headers are not fixed and thus run out of the picture when scrolling (Fig. 6).



The Allegro Network Multimeter provides detailed application statistics for VoIP. From this window, even a PCAP export of the call would be possible (Fig. 7).

These provide a good overview of the top protocols according to packets, bytes, and QoS in graphics and listings. Even application-specific PCAP exports can be created.

For security audits, the SSL statistics may provide information about the cipher suites used. The ANM also provides certificate information such as validity times to detect corresponding errors during the TLS handshake. Performance bottlenecks can be quickly identified by evaluating TLS handshake times.

HTTP statistics offer the possibility to identify the most used servers, response times and response codes. This mostly concerns OCSP (Online Certificate Status Protocol) queries during the establishment of TLS connections. Fortunately, most other connections are already encrypted via TLS.

In case of SMB problems or audits of file share accesses via this protocol, the SMB statistics module is helpful. t provides views of the number of SMB shares, including successful and failed connections to shares, as well as the associated clients and servers. But also the information about the used SMB version and information whether SMB encryption is used support security audits.

As already mentioned, a particular strength of the ANM, is the VoIP functionality, specifically the SIP and RTP statistics. It lists calls with phone numbers, the SIP servers involved, the codec, packet losses, QoS markings and INVITE status. Even a search for calls to a specific destination number is possible. Other quality features such as packet loss and jitter can also be evaluated.

In addition, the SIP methods used can be evaluated statistically. In the SIP module, it is possible to create events that trigger a notification, such as increased latency or exceeding a certain call duration, in order to be able to detect the misuse of expensive special or international numbers.

In case of an error, calls could even be exported retrospectively as PCAP files. In this way, the call quality could be directly checked - in compliance with legal and operational requirements - independently of the subjective user opinion.

No network without time

Correct time stamps are essential for networks to function. Without them, TLS connections can fail, for example. The ANM lists the NTP servers with the last activity, their version number, the polling interval, the strata and the number of clients. For example, a misconfigured NTP server will be noticed. For PTP, the ANM gives the PTP peers, including the time of the last synchronization.

In addition to the statistics for classic IT applications, statistics for the OT applications Profinet and OPC-UA are also available. Those enable system managers to identify the causes of loads, performance bottlenecks and other error patterns in the industrial environment as well. Profinet, for example, offers a listing of the top talkers, the bandwidth used, the jitter, and Profinet errors and alarms. The OPC UA module detects unanswered or duplicate requests as well as unsolicited responses and service errors of the OPC UA server.

Complementing the statistics and logging features, the Allegro Network Multimeter also comes with an iPerf3 server for performance measurements. The device does not offer TLS encryption breaking, as Allegro Packets developed it with a focus on troubleshooting and not as a security tool.

ZOf course, the ANM also includes a rights and role model (see table). It offers LDAP and TACACS+ as authentication protocols. RADIUS is still on the manufacturer's roadmap. Unfortunately, the documentation for TACACS+ is missing. LDAP worked without problems in the test, including LDAP group assignment to a rights group.

For local users, there is also the option of two-factor authentication based on TOTP (Time-based One-Time Password) -

but not for LDAP users. Management access cannot currently be restricted to specific source IP addresses. This would be the task of an upstream firewall. For upcoming versions, Allegro Packets plans to extend the rights and roles model with further options for implementing the dual control principle.

Interfaces to third-party systems

For accesses of own management systems to the statistics data the ANM offers a REST-API. It delivers the data as JSON objects. However, the documentation is rather poor. According to Allegro Packets, interfaces to monitoring systems such as Zabbix, but also to security services, are also planned for upcoming releases in order to be able to display indications of potential communication relationships with known spam or malware sources.

Fortunately, there are no licenses for individual functions, but only an overall license with all features. Firmware updates require an active support contract. Allegro Packets does not include German documentation with the Allegro Network Multimeter, but refers to a Google translation.

For regular management in corporate or government use, regular email notifications provide crash reports, uptime, temperature of the CPU, IP addresses, but also the expected time until the 90 percent packet ring buffer utilization is reached. This is an important indicator, because from that point on the deletion process of the oldest data is started.

By means of syslog export, the Allegro Network Multimeter allows messages to be collected at a central point. SNMPv3 access is also possible. A backup of the configuration exists in the form of nine JSON files as a ZIP archive.

Welcome new features in Release 3.5

In the post-test release 3.5, Allegro Packets has added a TCP flow graph analysis at the packet level. It presents a list of packets over which reference times to previous packets can be identified. In this way, handshake and application delta delays can be detected, for example. In addition, PCAP streaming to SFTP servers is now possible so as not to be limited to local resources of the appliance or the administrator's terminal.

There were also additions to the rights and roles model. Configurable templates for specific groups and new roles increase flexibility, especially in larger environments. In addition, multiple storage devices can now be activated simultaneously. This means that packet ring buffer runs in parallel with PCAP storage. When transferring existing PCAP files to a storage device, the hard disk no longer has to be deactivated and thus the packet ring buffer switched off. In addition, the ANM can now incorporate LTE USB adapters for remote management via cellular.

The VoIP functions, which were already quite advanced in the tested version, have also been expanded again, for example with more extensive RTP visualization and analysis. In addition, it is now possible to evaluate data traffic between IP address groups, for example all address ranges from location A to all those from location B.

For the upcoming version 3.6, Allegro Packets says it plans to implement IEEE 802.1X authentication on the management interface and for Let's Encrypt certificates. In addition, it is planned that the Allegro Network Multimeter will be able to import multiple PCAP files.

Conclusion

The Allegro Network Multimeter from Allegro Packets makes the evaluation of network captures much easier. The tidy menu, which is based on the OSI model, and the fast search were convincing in the test. However, the handling of the packet ring buffer requires some getting used to. The good performance due to the use of the in-memory database supports troubleshooting. The ERSPAN feature also makes the appliance flexible for centralized installations in complex network environments. (un@ix.de)

Score

⊕ High-performing web GUI and search function due to in-memory database
⊕ Comprehensive VoIP analysis for both SIP and RTP
⊕ Use as a target of an ERSPAN tunnel
⊕ Development and support entirely in Germany

⊖ Documentation incomplete and only available in English
⊖ Only conditionally suitable for long-term analyses
⊖ no passive through-connection of the integrated ports in bridge mode in the absence of power supply (only via additional boards)

Data and Prices

Manufacturer	Allegro Packets GmbH
Model	Allegro 1000
Current version	3.5 (im Test 3.4.1)
Dimensions (W × H × D)	264 mm × 43 mm × 226 mm
Platform	Super Micro Server, Debian Linux
Scaling	Capture and analysis up to 20 GBit/s, history up to 4 million connections (16 GByte RAM)/128 million connections (512 GByte RAM), up to 1 million open connections
Monitoring ports	3 × 1 GE, 2 × 10 GE (Cu), 2 × SFP+
Options	Bypass card for fiber (2 × 10GBase-SR) or copper ports (4 × 1000Base-T), 2 x 10GE with nBase-T, SFP28, QSFP, QSFP28, GPS measurement card

Benjamin Pfister

is Head of the Networks and Telecommunications of the City of Kassel and owner of Pfister IT-Beratung.