Allegro Packets

Network Multimeter

Rethinking
Network Troubleshooting

Allegro Network Multimeter

Rethinking Network Troubleshooting

- Mobile appliance for 1 to 100 GBit/s
- Clear display of complex network structures
- Intuitive web interface for fast troubleshooting
- Analysis and correlation of all metadata on layer 2–7
- Selective and retroactive pcap extraction
- Real-time analysis straight after installation
- Development and support from Germany

Fast troubleshooting

The Allegro makes both real-time and historical analysis of network traffic possible. It analyzes and correlates all data across the network layers 2 to 7, allowing network problems or unexpected traffic to be detected in seconds. The appliance is available in different versions: as a mobile or rack version, for small data centers, large ISPs, but also for the local company network.

Addition to Wireshark

The troubleshooting appliance shows both the big picture as well as the finer details. Network or application problems can be searched for, pre-filtered and then extracted as a pcap. This simplifies the Wireshark analysis because only a fraction of the total traffic needs to be analyzed. The Allegro's integrated pcap ring buffer (standard in Allegro 1000/3000 Series) makes this possible even for operations that have happened in the past.

Quick diagnosis

Click-through structures and selective pcap extraction help you to find the content you need quickly. The web interface search function allows you to sort, search and filter by MAC or IP addresses, ports, VLANs, TCP handshakes, HTTP latencies and more. You get the results in a fraction of a second, enabling immediate analysis.

Comprehensive analyses

The Allegro includes many different analysis modules for L2 to L7. Search and extract all the different Ethernet types such as LLDP on L2, for instance, or automatically search for microbursts on the link. For example, you can use L4 TCP to analyze retransmissions globally or per IP endpoint, and L7 to identify potential VoIP quality problems in SIP and RTP streams. Allegro Packets is constantly working to extend these modules.

Uncomplicated startup

The Allegro can be integrated quickly and easily anywhere in your network. You don't need to install any extra software. Access data via the browser-independent web interface, also remotely. You can install the Allegro as needed: on the mirror port, tap or as a bridge.

A real-world example in troubleshooting

Troubleshooting in IT often requires quick access to the relevant data. Here's a typical problem:

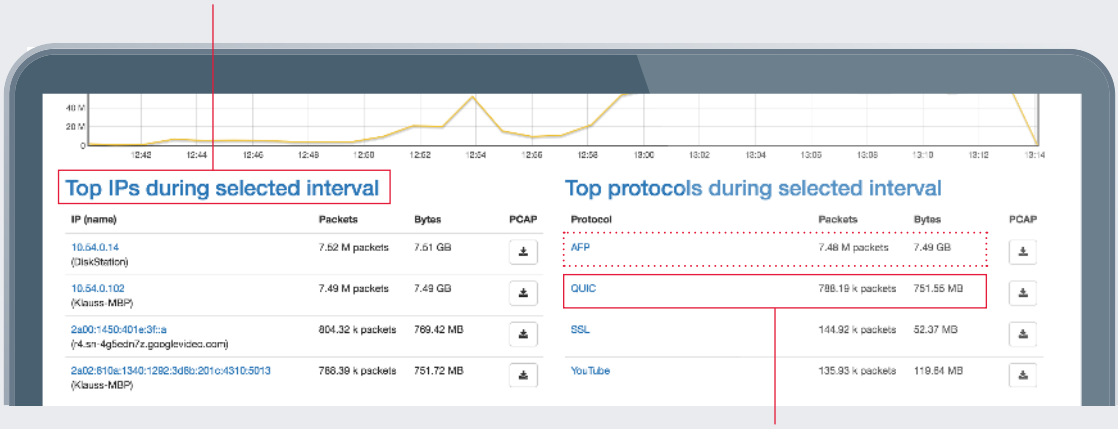
»I tried to access the file server an hour ago and it was very slow. I couldn't get on with my work. It's working better now, but it has wasted a lot of my time and I don't want it to happen again.«

- What traffic was there at a certain point in the network at a certain time?
- Was there any other data transfer going on, such as a backup or an update?
- Was there a bandwidth problem? If so, who or what caused this?
- How can this past traffic be examined in detail?

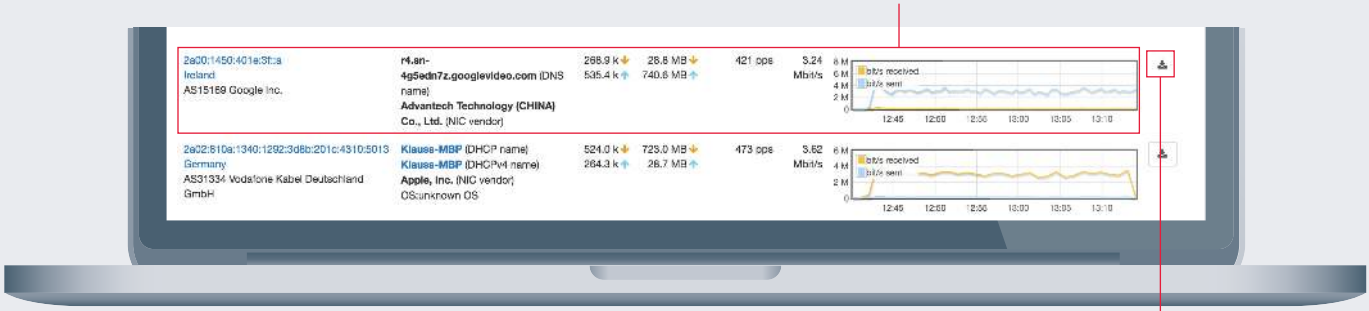
The Allegro Network Multimeter can help you to answer the questions quickly and easily.

In detail

The dashboard displays the TOP-IPs and protocols of a specific time interval with just one click. This allows you to quickly determine whether it was one event in particular such as a large update or just a Youtube stream that generated a load at that time. Use it to view the TOP-IPs per protocol immediately on the dashboard.



Use our dashboard to take a closer look at an L7 protocol or an IP. TOP connection partners are also displayed on the dashboard. You'll see in the screenshot that the AFP protocol was used for backup and QUIC. AFP is intended to be part of this network, but QUIC will be further investigated here. By clicking on QUIC the TOP QUIC-IPs are displayed in the interval.



Using the pcap button, all packets of an IP communication over a protocol can be extracted and analyzed, e. g. with Wireshark.

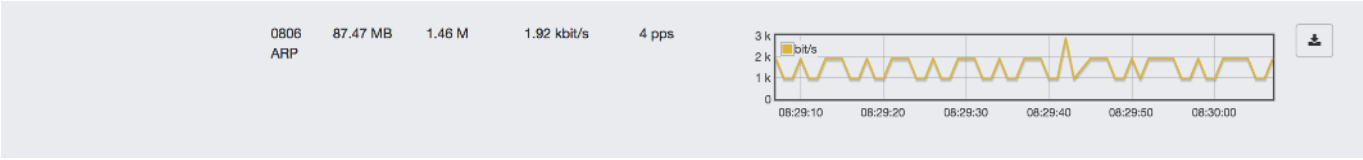
The additional load of approximately 5 MBit/s was generated by a Google video server via IPv6. This clarifies the cause and allows further actions to be taken.

Excerpt of several analysis modules

Allegro provides you with a wide range of analyses on layers 2 to 7 which it can display both in real time as well as retroactively for a given time interval. In addition, it can be used to display a lot of information for each IP and MAC, such as the decoded DNS, DHCP or HTTP host name or the SSL Common Name. The tables can also be filtered for correlated information.

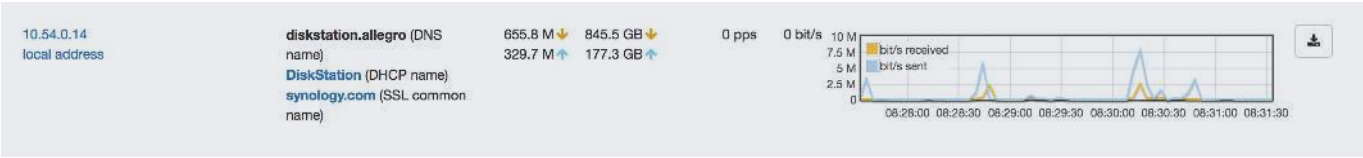
LAYER 2

- Analysis of all Ethernet types occurring on L2
- MAC address analysis with L7 protocols, connection partners and IPs used per MAC
- VLAN analysis: display of all VLANs per trunk, also for Q-in-Q, display of all MACs per VLAN
- Utilization analysis: bandwidth measurement in the millisecond range with automatic alerting when threshold values are exceeded
- QoS analysis



LAYER 3

- IP analysis: display of all IPv4/v6 addresses, each with L7 protocols, connection partners and used MAC addresses, TCP return transmissions , QoS classes, etc.



LAYER 4

- TCP retransmission: time-based analysis of retransmissions, both globally and per IP
- TCP: handshake, response time, flags, zero window
- Port analysis: used TCP and UDP ports

LAYER 7

- Protocol analysis: used protocols based on signatures, TOP-IPs per protocol
- HTTP/SSL analysis: temporal analysis of an HTTP request or SSL handshake both globally and per IP
- SIP analysis: analysis of a SIP telephone call incl. status code, RTP correlation, RTP jitter and packet loss
- Generic response time analysis: measured using patterns in the request or response

All statistics can be viewed with a freely configurable time interval.

Overview appliances

Appliance	Virtual Edition	Allegro 200	Allegro 500
Monitor ports	1 x virtual mirror port	2 x 1000Base-T	4 x 1000Base-T
Maximum throughput	About 1 GBit/s (CPU dependent)	2 GBit/s	4 GBit/s
Internal database memory	Unlimited	2 GB	4 – 8 GB
Integrated ring buffer	Unlimited	–	0.5 – 1 TB
Versions	Virtual	Portable	Portable
Weight	–	260 g	1 kg
Packaging	–	Portable soft shell case	Portable soft shell case
Area of application	Cloud	Office or small data center	

Appliance	Allegro 1000 / 1200	Allegro 3000 / 3200	Allegro 3500 / 5500
Monitor ports	3 x 1000Base-T 2 x 10GBase-T 2 x SFP+ 1 extension slot	3 x 1000Base-T 2 x 10GBase-T 2 x SFP+ 1 extension slot	5 extension slots: SFP+, QSFP, QSFP28 etc.
Maximum throughput	20 GBit/s	40 GBit/s	50 – 100 GBit/s
Internal database memory	16 – 256 GB	64 – 256 GB	96 – 1536 GB
Integrated ring buffer	Up to 10 TB	Up to 10 TB	Up to 360 TB
Versions	Portable / 1 U	Portable / 1 U	4 U
Weight	2 – 4 kg	2 – 4 kg	40 – 80 kg
Packaging	Portable soft shell case/ server cardboard	Portable soft shell case/ server cardboard	Server cardboard
Area of application	Office building or data center		Big data center

Some of our customers

Allegro Packets GmbH
Fockestr. 6 | 04275 Leipzig

Phone +49 341 59 16 43 53
Email info@allegro-packets.com
Internet allegro-packets.com

Faster network troubleshooting with Allegro Network Multimeter.
The Allegro revolutionizes the market for network analysis. For the first time ever, it is possible to analyze a huge volume of packets with a mobile device. The development is based on Allegro Packets' mission to provide a debugging tool that combines the advantages of previous solutions. The result is a device that's as mobile as a software and as powerful as a full-blown server.