Allegro Packets

Network Multimeter

Netzwerk-Troubleshooting **neu gedacht**

Allegro Network Multimeter

Netzwerk-Troubleshooting neu gedacht

- Mobile Appliance für 1 bis 100 GBit/s
- Übersichtliche Darstellung komplexer Netzwerkstrukturen
- Schnelle Fehlersuche durch intuitives Webinterface
- Analyse und Korrelation aller Metadaten auf Layer 2–7
- Selektive und nachträgliche Pcap-Extraktion
- Echtzeitanalyse sofort nach Inbetriebnahme
- Entwicklung und Support in Deutschland

Der Troubleshooter

Das Allegro ermöglicht die Analyse von Netzwerkverkehr in Echtzeit und in der Vergangenheit. Es analysiert und korreliert alle Daten über die Netzwerkschichten 2 bis 7. Netzwerkprobleme oder unerwarteter Verkehr können so sekundenschnell erkannt werden. Die Appliance ist in verschiedenen Ausführungen erhältlich: als mobile oder Rack-Variante, für kleine Rechenzentren, große ISPs, aber auch für das lokale Firmennetz.

Ergänzung zu Wireshark

Die Troubleshooting-Appliance dokumentiert das große Ganze ebenso wie das exakte Detail. Netzwerk- oder Applikationsprobleme können gesucht, vorgefiltert und im Anschluss als Pcap extrahiert werden. Dies erleichtert die Wireshark-Analyse, da nur noch ein Bruchteil des Gesamtverkehrs untersucht werden muss. Mit dem teils standardmäßig integrierten Pcap-Ringpuffer ist dies auch für weit zurückliegende Vorgänge in der Vergangenheit möglich.

Schnell zur Diagnose

Mithilfe von Click-Through-Strukturen und selektiver Pcap-Extraktion finden Sie schnell die für Sie relevanten Inhalte. Mit der Webinterface-Suchfunktion können Sie nach MAC- oder IP-Adressen, nach Ports, VLANs, TCP-Handshakes, HTTP-Latenzen u.v.m. sortieren, suchen und filtern. Die Ergebnisse werden in Sekundenbruchteilen angezeigt und ermöglichen so eine Analyse ohne Wartezeiten.

Umfassende Analysen

Das Allegro beinhaltet viele verschiedene Analysemodule für L2 bis L7. Sie können etwa auf L2 alle verschiedenen Ethernet-Typen wie z.B. LLDP untersuchen und extrahieren oder automatisch nach Mircobursts auf dem Link suchen. Auf L4 TCP können z.B. Retransmissions global oder pro IP-Endpunkt analysiert, auf L7 mögliche VoIP-Qualitätsprobleme in SIP- und RTP-Strömen gefunden werden. Diese Module werden von Allegro Packets ständig erweitert.

Unkomplizierter Einstieg

Das Allegro kann an jeder Stelle im Netzwerk schnell und unkompliziert eingebunden werden. Eine Installation ist nicht nötig. Der Zugriff erfolgt über das browserunabhängige Webinterface und ist auch remote möglich. Je nach Bedarf kann das Allegro am Mirror-Port, Tap oder als Bridge installiert werden.

Praxisbeispiel in der Fehlersuche

Troubleshooting in der IT benötigt oft schnellen Zugriff auf die relevanten Daten. Eine typische Problemstellung mit grundlegenden Fragen ist:

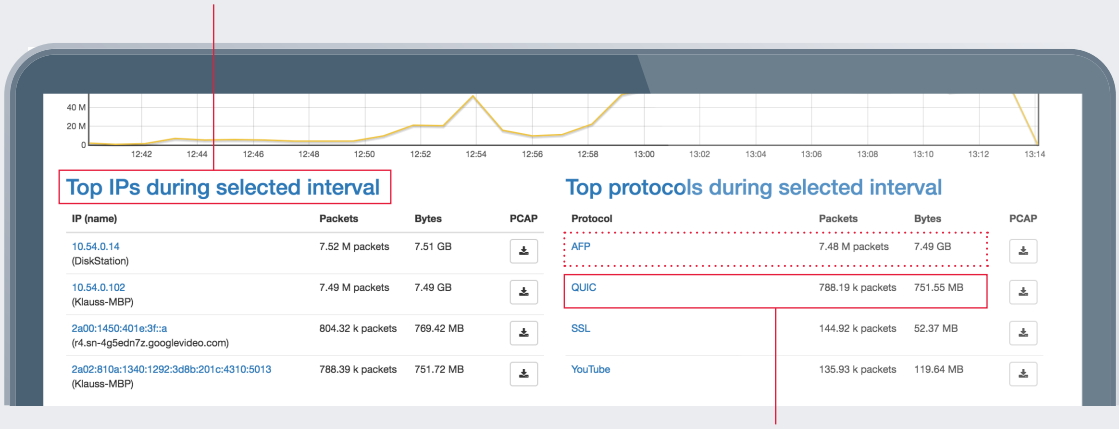
»Vor einer Stunde war der Zugriff auf den Fileserver sehr langsam und ich konnte nicht arbeiten. Jetzt funktioniert es wieder besser, aber es hat mich viel Zeit gekostet und es soll bitte nicht nochmal vorkommen.«

- Welchen Verkehr gab es zu einem bestimmten Zeitpunkt an einer Stelle im Netzwerk?
- Gab es anderen Datentransfer, wie ein Backup oder ein Update in diesem Zeitintervall?
- Gab es ein Bandbreitenproblem? Wenn ja, wer oder was hat dies verursacht?
- Wie lässt sich dieser vergangene Verkehr genauer untersuchen?

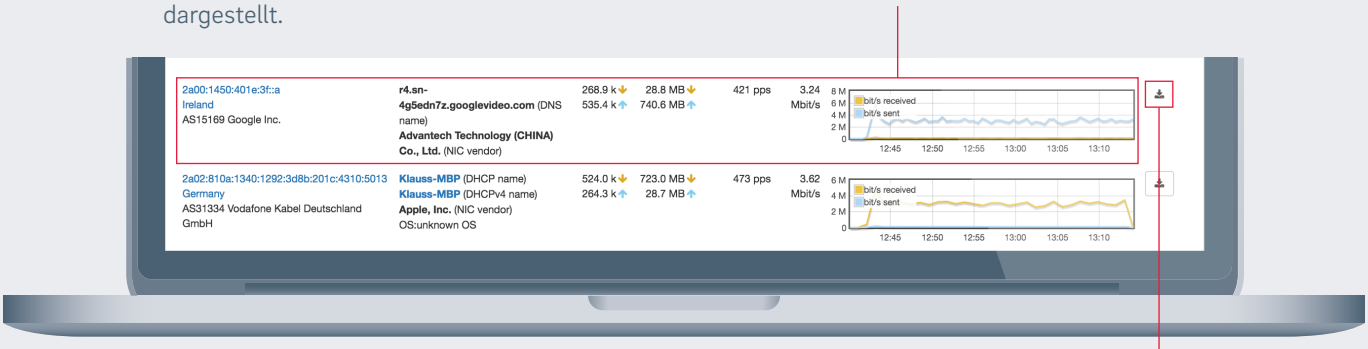
Alle diese Fragen lassen sich sehr schnell und einfach mit dem Allegro Network Multimeter klären.

Im Detail

Das Dashboard zeigt hierbei mit nur einem Klick die TOP-IPs und Protokolle eines Zeitintervalls. Damit kann schnell geklärt werden, ob zu dieser Zeit ein bestimmtes Ereignis eine besondere Last erzeugt hat, wie z.B. ein großes Update oder einfach nur ein Youtube-Stream. Hier werden unmittelbar die TOP-IPs pro Protokoll angezeigt.



Hier lässt sich nun direkt ein L7-Protokoll oder eine IP untersuchen. Ebenso können die TOP Verbindungspartner angezeigt werden. In dem Screenshot wurde das Protokoll AFP (Apple Filing Protocol) zum Backup und QUIC genutzt. AFP ist gewollt in diesem Netzwerk, QUIC hingegen soll hier weiter untersucht werden. Durch Klicken auf QUIC werden die TOP QUIC-IPs in dem Intervall dargestellt.



Hier können nun über den Pcap-Knopf rückwirkend alle Pakete der Kommunikation einer IP über ein Protokoll extrahiert und zur weiteren Analyse mit z. B. Wireshark untersucht werden.

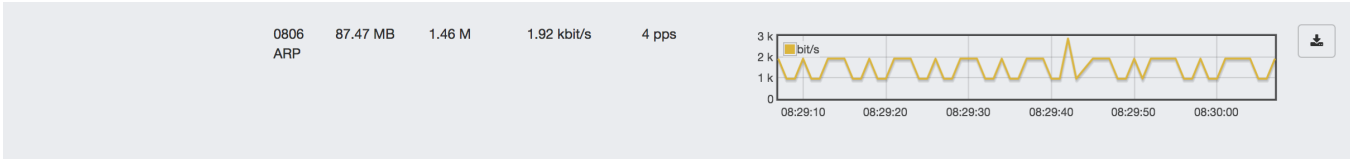
Die zusätzliche Last von ca. 5 MBit/s wurde also durch einen Google-Videoserver über IPv6 erzeugt. Damit ist die Ursache geklärt und es können weitere Aktionen vorgenommen werden.

Auszug einiger Analysemodule

Das Allegro liefert Ihnen vielfältige Analysen auf Schicht 2 bis 7. Diese liegen alle in Echtzeit mit Graphen vor, können aber auch rückwirkend für ein Zeitintervall dargestellt werden. Zudem werden pro IP und MAC viele Informationen korreliert dargestellt, wie z.B. der dekodierte DNS-, DHCP- oder HTTP-Hostname oder der SSL Common Name. Zudem kann in den Tabellen frei nach den korrelierten Informationen gefiltert werden.

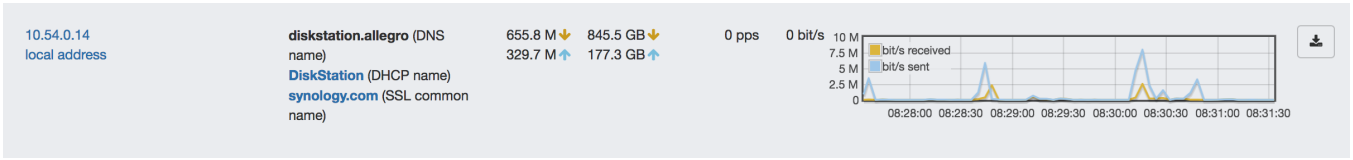
SCHICHT 2

- Analyse aller auf L2 auftretenden Ethernet-Typen
- MAC-Adressen-Analyse mit L7-Protokollen, Verbindungspartnern und genutzten IPs pro MAC
- VLAN-Analyse: Anzeige aller VLANs pro Trunk, auch für Q-in-Q, Anzeige aller MACs pro VLAN
- Auslastungsanalyse: Bandbreitenmessung im Millisekundenbereich mit automatischer Alarmierung bei Überschreitung von Schwellwerten



SCHICHT 3

- IP-Analyse: Anzeige aller IPv4/v6-Adressen, jeweils mit L7-Protokollen, Verbindungspartnern und genutzten MAC-Adressen, TCP-Retransmissions etc.

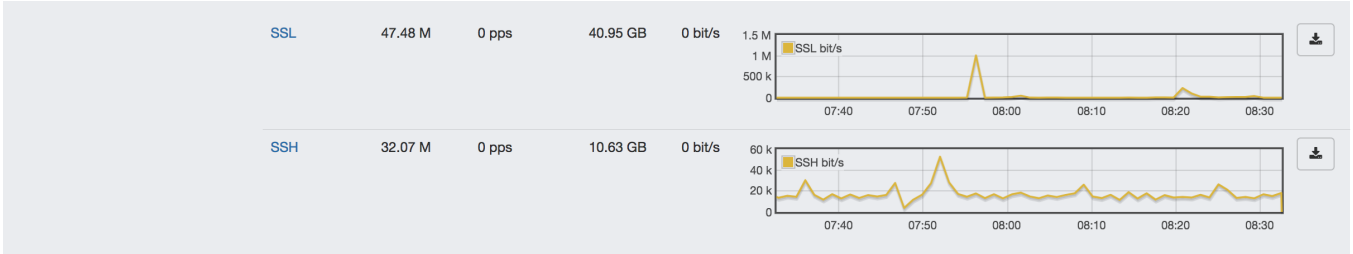


SCHICHT 4

- TCP-Retransmissions: zeitliche Analyse von Retransmissions, sowohl global als auch pro IP
- TCP-Handshake: zeitliche Analyse des TCP-Handshakes, sowohl global als auch pro IP
- Portanalyse: verwendete TCP- und UDP-Ports, TOP-IPs pro Port

SCHICHT 7

- Protokollanalyse: verwendete Protokolle anhand von Signaturen, TOP-IPs pro Protokoll
- HTTP/SSL-Analyse: zeitliche Analyse eines HTTP-Requests bzw. eines SSL-Handshakes sowohl global als auch pro IP
- SIP-Analyse: Analyse eines SIP-Telefonates inkl. Status-Code, RTP-Korrelation, RTP-Jitter und Packet-Loss
- Generische Antwortzeitanalyse: vermessen anhand von Patterns im Request oder in der Response



Alle Statistiken lassen sich für ein frei konfigurierbares Zeitintervall abrufen.

Übersicht Appliances

Allegro 200

Das Allegro 200 ist, mit 260g, eine ultra portable Appliance, die kaum größer als ein Smartphone ist. Dabei kann es den Datenverkehr von bis zu 50 PCs bzw. Servern und Datenraten bis zu 1 GBit/s full duplex sofort nach Inbetriebnahme inline oder am Mirror-Port analysieren.

Das Allegro 200 ist als portable Variante erhältlich, optional mit externem Ringpuffer.

Allegro 1000 Serie

Die Appliances der Allegro 1000 Serie zeichnen sich durch eine kostengünstige Einstiegsversion für Gigabit-Verkehr und eine Analyse für bis zu 10.000 Server aus. Dabei können alle Appliances um SFP+ Ports, Ringpuffer und zusätzlichen In-Memory-Datenbankspeicher erweitert werden.

Als Versionen gibt es das portable Allegro 1000 und das Allegro 1200 als 1U-Rack Unit.

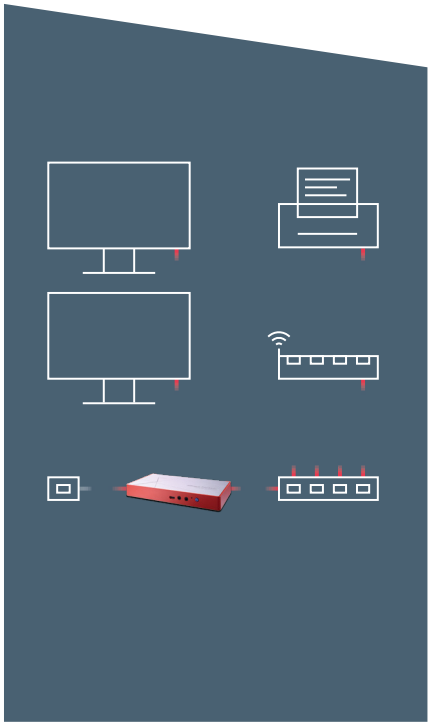
Allegro 3000 Serie

Die Allegro 3000 Serie ist die High-End-Version mit Unterstützung von QSFP28-Anschlüssen für 40- und 100 GBit/s. Das Allegro eignet sich hervorragend für ISPs, große Rechenzentren und große Unternehmensnetze zur Linkanalyse an Knoten mit hoher Last. Hierbei ist die Echtzeit- und historische Analyse für bis zu 40 GBit/s möglich.

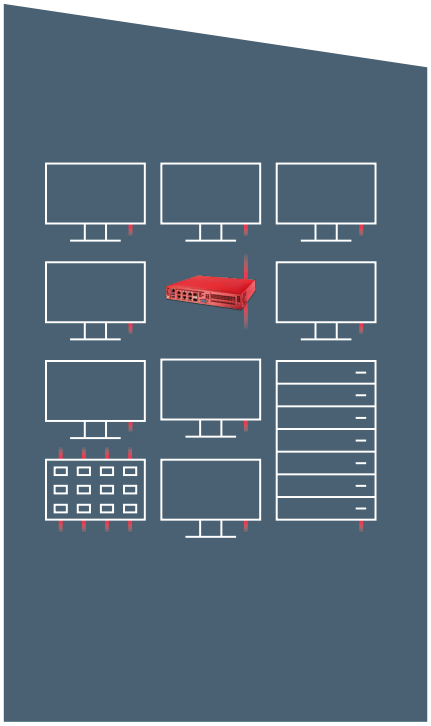
Die 3000 Serie ist neben dem 1U-Gerät (Allegro 3200) zudem auch als portable Version (Allegro 3000) erhältlich.

Einsatzszenarien der Allegro Network Multimeter

Büro



Bürogebäude im Rechenzentrum



Großes Rechenzentrum

Einige unserer Kunden

arvato
BERTELSMANN

Hochschule für den öffentlichen Dienst in Bayern
Fachbereich **Polizei**

Kreiskliniken Günzburg-Krumbach

BITMARCK®

FESTO AG

Allegro Packets GmbH
Richard-Wagner-Platz 1 | 04109 Leipzig

Telefon +49 341 59 16 43 53
E-Mail info@allegro-packets.com
Internet allegro-packets.com

Schnelleres Netzwerk-Troubleshooting mit dem Allegro Network Multimeter.
Das Allegro revolutioniert den Markt der Netzwerk-Analysen. Zum ersten Mal gelingt es, ein riesiges Paketvolumen mobil zu analysieren. Grundlage der Entwicklung ist der Anspruch von Allegro Packets, ein Debugging-Tool anzubieten, das die Vorteile bisheriger Lösungen vereint. Das Ergebnis ist so mobil wie eine Software und ebenso leistungsstark wie ein ausgewachsener Server.