



Launchpaper Release 2.2 Allegro Packets

Management Summary

Software Release 2.2 of the measurement and analysis appliances developed by Allegro Packets provides the tools necessary to measure QoS, MPLS and interface bursts. This release supports Protocol 104 in a simple SCADA module for the first time, paying particular attention to the individual grouping of various IP parameters; the SSH Remote Tunnel Support and enhanced SIP and VoIP functions which contribute to faster error analysis and consequently to a reduction of time and costs in the VoIP operational environment.

Management Summary.....	1
IP-Groups.....	1
Ignoring VLAN-Tags in Connections.....	1
Quality of Service.....	2
SIP Extensions.....	3
MPLS.....	5
OPC Unified Achitecture.....	5
Controlled Packet Forwarding and Traffing Duplication.....	5
Remote Tunneling with SSH.....	6
Cluster Ring Buffers.....	6
Burst Analysis.....	7
Report: Port Usage per Subnetwork.....	8
About Allegro Packets.....	8

IP-Groups

With the 2.2 software release, groups of IP data packets (IPv4 and IPv6) can be combined for the first time enabling IP data from different IP servers, subnets, VPNs, clients, etc. to be aggregated. For example, if traffic from three servers needs to be simultaneously examined, these traffic streams are grouped together into a single IP group and all bundled IP statistics of these devices are then obtained. The detailed information shows the active IP addresses of the group, as well as the individual IP addresses contacted by the group.

Ignoring VLAN Tags in Connections

This latest software release allows packets from different VLANs (including packets without VLAN tags) to be considered as one connection if all other connection parameters (e.g. IP addresses, ports, Layer 4 protocols) are identical.

Such a setup may be required under the following conditions:

- Classic VLAN network configurations: Packets from one direction are received from a switch port with, for example, VLAN tag 1 on the mirror port.
- No VLAN has been configured on the terminal devices or switch ports associated with VLAN 1. Therefore, the packets are transmitted from this direction from the switch port to the mirror port without VLAN tagging.



Normally, the packets (with VLAN and without VLAN tags) would be considered as not belonging to a VLAN. The ability to ignore the VLAN tags in connections ensures that the VLAN can be displayed entirely in this special constellation.

Quality of Service

In the original design of TCP/IP protocols, Quality of Service (QoS) played a subordinate role. TCP/IP was solely intended for application data transport.

Networks based on Ethernet and IP are not generally suitable for real-time applications by their very nature. If required, networks can be made real-time capable by Quality of Service (QoS) mechanisms to provide the functionality needed for high-priority applications even during peak loads.

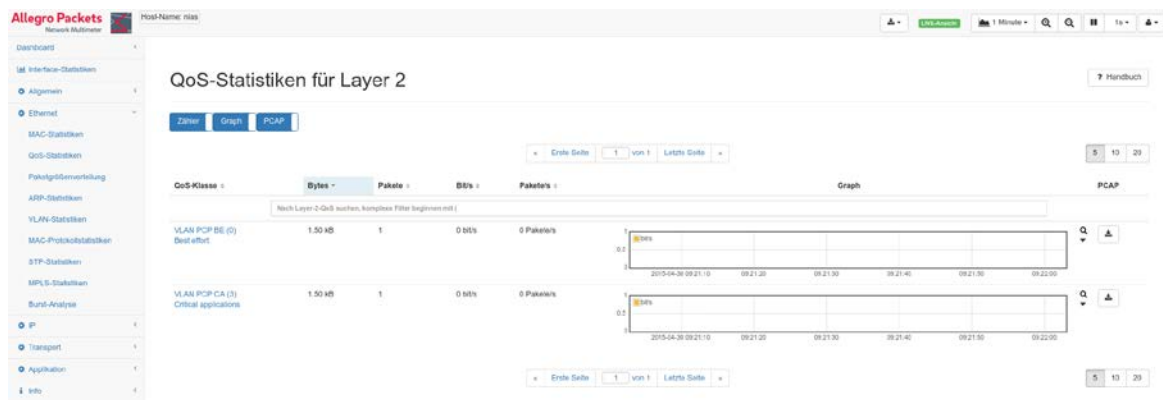


Figure 1: Representation of Layer 2 Prioritization

The QoS-related prioritization or parameterization of the data traffic, the data rate reservation, data rate limitation and packet optimization are included in Release 2.2 by the following mechanisms:

L2 QoS Extension in Release 2.2

With the QoS functions of the Allegro Network Multimeter integrated in Release 2.2, Layer 2 priorities (both in the VLAN tag and the TC bits in the MPLS header) and the corresponding data traffic can be displayed as a graph. In the QoS statistics window for Layer 2, all devices for a specific day are displayed.

L3 QoS Extension in Release 2.2

The QoS functions of the Allegro Network Multimeter integrated in Release 2.2 can be used to display the priorities on Layer 3 and the corresponding data traffic as a graph. The Layer 3 QoS statistics window displays all devices for a specific DSCP value.

L4 QoS Extension in Release 2.2

With the QoS functions integrated in Release 2.2, the list of ports on Layer 4 can be correlated with the QoS labels recognized in the network. The top 5 QoS labels are sorted according to the current traffic volume. (see also QoS Details).



L7 QoS Extension in Release 2.2

With the QoS functions integrated in Release 2.2, Layer 7 applications can be correlated with the QoS labels recognized in the network. The top 5 QoS labels are sorted according to the current traffic volume. (see also QoS Details).

QoS-Details

Using the QoS representations of Layer 4 and Layer 7, you can also display details for the ports and application protocols for each day.

A Layer 2 or Layer 3 list for each day can also be displayed in the IP details of an IP address. This visualizes the traffic associated with an IP address and the relevant day.

If you click on a QoS tag you get a corresponding IP connection list. A filter is automatically set and only the connections of the IP address concerned with the tag are displayed.

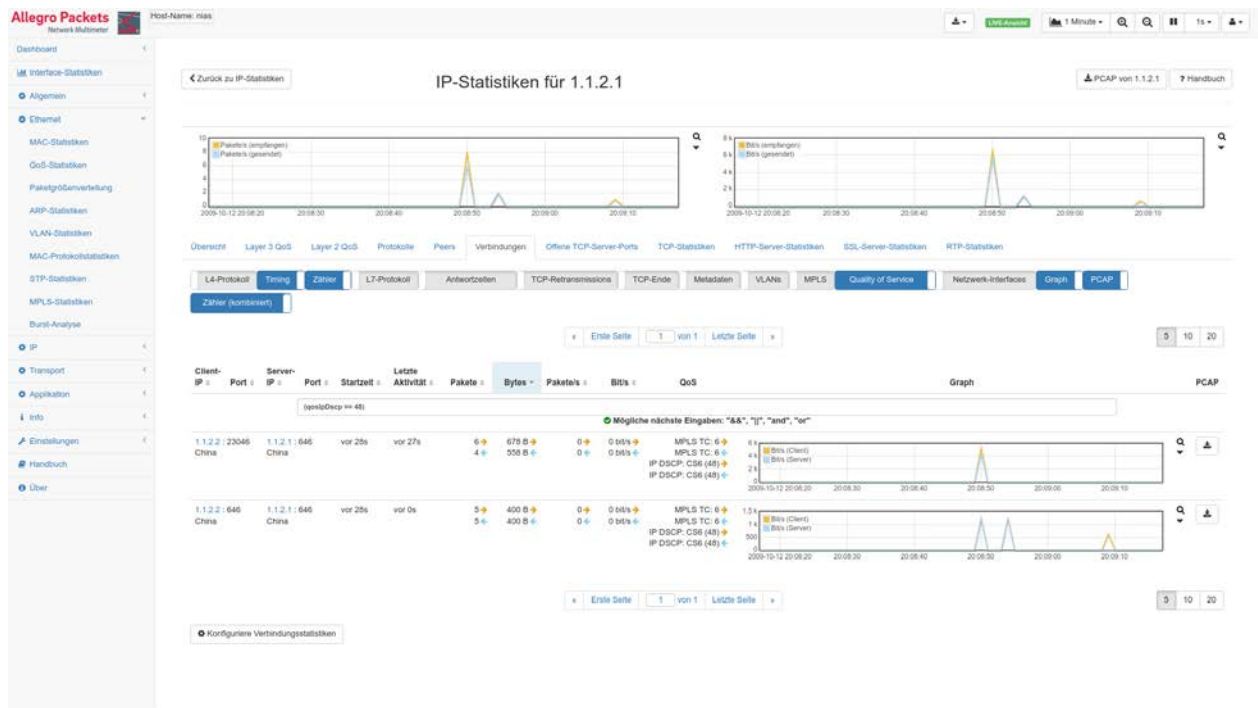


Figure 2: Display of the Quality Classes

SIP Extensions

In the previous release, measurement of Voice over IP (VoIP) flows was introduced for the first time. With the 2.2 Release, this functional area has been further expanded including a new and completely revised SIP dashboard with all associated SIP statistics. These include an overview of SIP:

- Overview of SIP, RTP and total traffic.
- RTP packet losses (general overview).
- RTP Jitter (general overview),



- SIP answer types.
- Number of simultaneous calls.

The associated (per call) RTP information is assigned to the SIP calls and displayed in detail in the 'SIP Calls' window. This includes:

- The caller and the called party.
- the RTP sender and receiver.
- Number of packets (in each transmit direction).
- Jitter (per transmissions direction).
- Mean Opinion Score (MOS) (per transmit direction).

In the SIP statistics, the Layer 4 endpoints of the connections initiated by SIP are displayed. Click on the magnifying glass icon to open the Events window with the SIP details for the specific connection.

SIP-Statistiken

? Handbuch

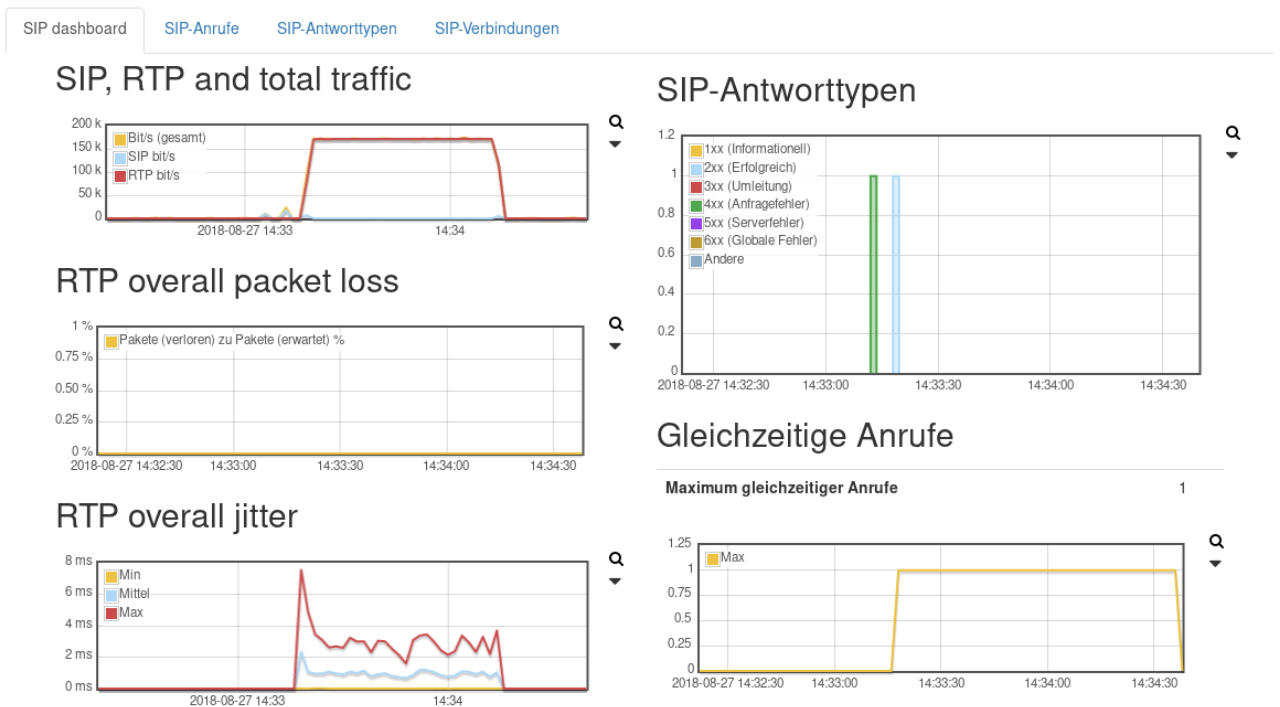


Figure 3: Display of SIP Information



MPLS

MPLS analysis has been enhanced in Release 2.2. All MPLS channels (single and double tagged) are displayed. In addition, the MAC addresses used to include graphs and PCAP extraction are displayed for each MPLS channel.

OPC Unified Achitecture

A new addition to Release 2.2 is the provision of measurement functions for the OPC UA binary protocol. OPC Unified Architecture (OPC UA) is used where sensors, controllers and controllers from different manufacturers form a common network. With OPC, it is necessary to develop one OPC-compliant driver for each device. OPC is divided into various sub-standards which can be implemented independently of each other for the respective application. OPC can thus be used for real-time data (monitoring), data archiving, alarm messages and, more recently, directly for control (command transmission). The OPC UA elements are published as IEC standard (IEC 62541).

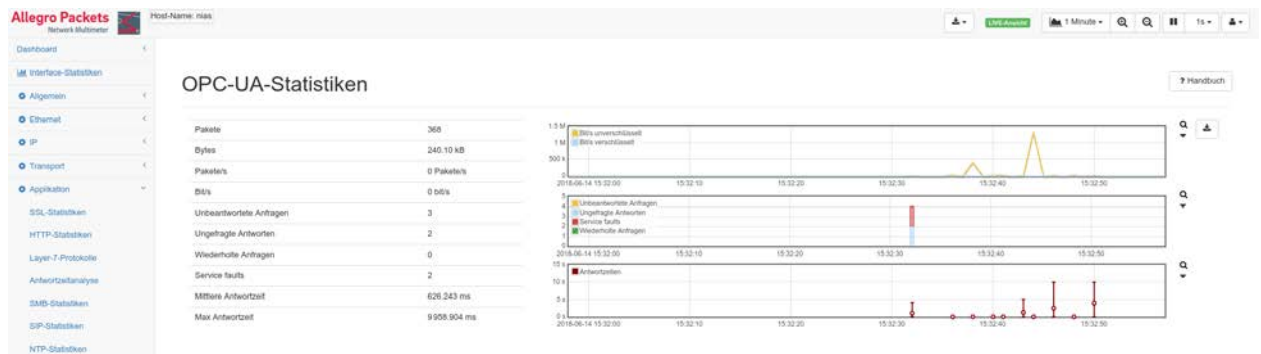


Figure 4: OPC UA Screenshot

Controlled Packet Forwarding and Traffic Duplication

Previously, data could only be stored in a Pcap and this could be forwarded via the network to any terminal device. With the 2.2 Release it is now possible to forward any data stream (as raw Ethernet output) to any destination in the network. The data streams are not changed (or modified) but transported as native Ethernet bit streams.

These data streams can also be recorded and then transferred to the network. The data speeds can be set individually.

Centrally Installed Network Management Components

Certain network management systems require access to the data generated at the point of origin. For this reason, it may be necessary to duplicate these traffic flows and forward them to a centrally operated network management console. The Allegro Network Multimeter enables lossless multiplication of one data connection to many ports and aggregation of several data connections to just one port. This can save span ports on switches, routers, etc., for example.

The data is filtered out with appropriate filter mechanisms before it is rejected. For example, several 10GB/s lines can be evaluated with existing 1GB/s analysis tools, thus reducing the amount of data required for reliable analysis. Data that is not of interest is either discarded or sent to other tools for further analysis.



Aufzeichnungseinstellungen auswählen

Ein Filter für den Paketringpeicher ist aktiv. Einige Pakete wurden möglicherweise nicht gepuffert.

Startzeit: 2018-09-05 00:00:00

Gestern Heute Vor 1 Stunde Vor 10 min Jetzt In 10 min In 1 Stunde Morgen

Endzeit: 2018-09-06 00:00:00

Gestern Heute Vor 1 Stunde Vor 10 min Jetzt In 10 min In 1 Stunde Unbeschränkt

PCAP-Datei direkt auf die Festplatte schreiben statt Download: Aus

Versende aufgezeichnete Pakete auf Interface: An

Interface zum Versand der Pakete: 2

Versenden mit Geschwindigkeit: Echtzeitfaktor

Versenden mit Echtzeitfaktor: 1.0

Ausgewählte Aufzeichnungsdauer: 1 Tag

Abbrechen **Starte Aufzeichnung**

Figure 5: Forwarding a Data Stream to a Management Center

Remote Tunneling with SSH

If an Allegro Network Multimeter is installed behind a firewall and cannot be reached from outside (or from a foreign network), the firewall ensures that all incoming connections to the local network are blocked. The 2.2 software Release addresses this problem by supporting an SSH tunnel.

The network administrator now has the option to specify a server with which the Allegro Network Multimeter establishes a Secure Shell (SSH) tunnel using Public Key Authentication. The SSH mechanism provides secure and encrypted traffic to the remotely installed query station or jump server and forwards the Allegro Network Multimeter's HTTPS port to the SSH server. This server has the task of transparently connecting the SSL connection (port 443) from the external workstation to the in-use SSH tunnel (e.g. port 5000).

With this mechanism it is now possible for a network administrator to remotely analyze and resolve network problems in a secure and controlled manner as if they were on site.

Cluster Ring Buffers

The Allegro Network Multimeter 2.2 software Release can also create a ring buffer for up to 64 HDDs or SSDs. Here the packets are written alternately on the data carriers. Thus, both the memory



size and the write rate can be increased. This is applicable for both internal and external data storage devices via USB3.

Burst Analysis

In data communication, one speaks of a burst transmission as data bursts which can occur over a short period of time. Data bursts can occur for example when downloading data from the Internet at excessive speeds for a short period of time. Data bursts can also occur in a computer network in which data transmission is performed at intervals (normal behavior in packet-oriented networks).

Prior to the launch of software Release 2.2, the Allegro Network Multimeter only graphically displayed the bursts in the connected data channel. The graph aggregates the incoming traffic of all interfaces each second with a measurement interval of one millisecond. A burst that leads to a significant increase in traffic volume and has a sufficient duration is also referred to as a spike. The diagrams show the traffic per interface.

Release 2.2 of the Allegro Network Multimeter software allows configuration of the total bandwidth of the available data channel for burst measurement. If, for example, only 30 percent load is usually transmitted on a network link (300 MB/s), this value can be set as the upper limit of this subchannel and the average data bursts that occur can be examined and the respective values displayed. In this case, an burst of up to 105 percent is permitted. This indicates that the data burst in the respective data channel exceeded the planned usage limit.

In addition, these data bursts can be displayed for up to five MAC addresses. Two graphs are used to display the MAC addresses. The TX graph shows the data bursts in the transmit direction and the RX graph shows the data bursts in the receive direction.

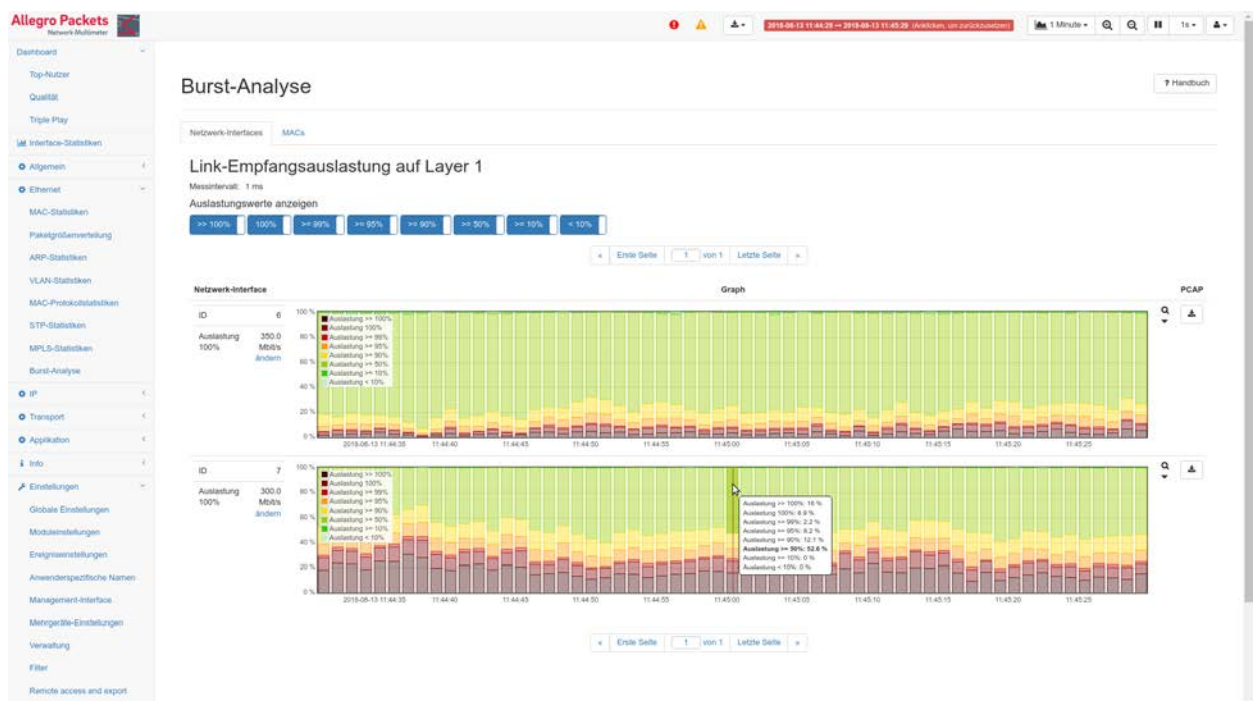


Figure 6: Burst Analysis Representation



Report: Port Usage per Subnetwork

With this function, the ports used (Layer 4) and the associated applications (Layer 7) can be displayed per subnet and the respective traffic volumes can be displayed.

Example. 192.168.1

192.168.1.10 TCP port 80 http rx 8GB tx 2GB

192.168.1.11 TCP port 43 https rx 7GB tx 1GB

192.168.1.200 UDP port 53 DNS rx 900MB tx 100MB

The Allegro Packets software Release 2.2 is now available. Information on prices and products can be obtained from Allegro Packets by sending an email to sales@allegro-packets.com.

About Allegro Packets

The network analysis specialist Allegro Packets offers innovative troubleshooting and analysis products to solve network issues with the Allegro Network Multimeter family of appliances. The innovative features of Allegro devices meet all requirements for information infrastructures. Customers include companies, data centers, IT service providers, system houses and ISPs. The Allegro Network Multimeter is developed entirely in Germany. This guarantees the customer efficient support and a swift, easy integration of new features.