Allegro Packets
Network Multimeter

WHITE PAPER

In-Memory DB and Packet Ring Buffer
Two Databases for Different Purposes

The Allegro Network Multimeter is a powerful real-time network multimeter for detecting network problems. It measures many performance parameters from Layer 2 to Layer 7 and is used for troubleshooting and network analysis.

All information recorded by the device is available in real-time, including traffic history graphs (per MAC address, IP address, protocol, per connection). In addition, the graphics can be clicked to zoom into a specific time window and display the results only for this time window. The Allegro Network Multimeter uses two different databases to display and process the recorded information:

- the in-memory database and
- the packet ring buffer on the hard disk or SSD.

This white paper explains the different application areas and their use in practice.

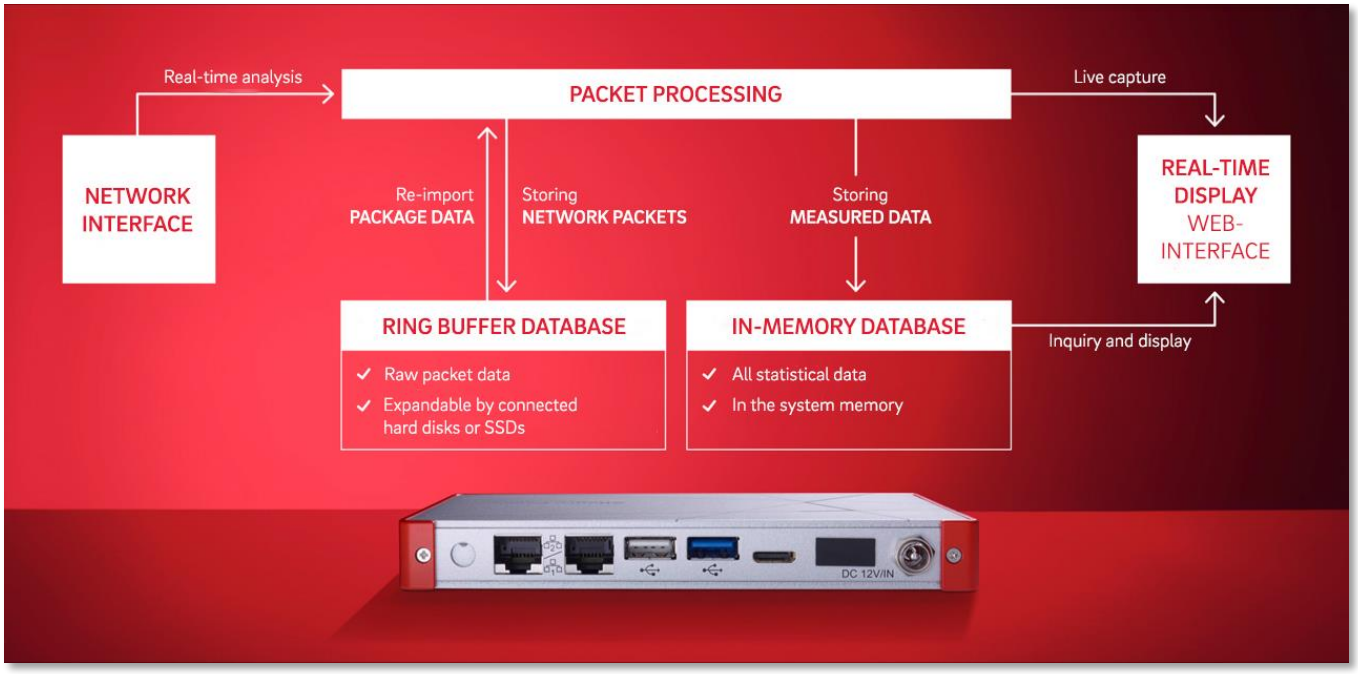

Figure 1: Architectural concept of the Allegro Network Multimeter

Figure 1 shows a simplified representation of the functional components of packet processing, enabling network packets to be analysed in depth. Metadata such as IP addresses, connection information, packet counters, etc. are stored in the main memory (= in-memory). The values displayed in the Web-based interface are derived from the main memory. To enable deeper historic analysis, these packets are stored in a cyclical ring buffer on a hard disk/SSD to allow detailed examination of captured requests at a later point in time.

In-Memory Database

The Allegro Network Multimeter uses an in-memory database to store the metadata of the processed packets. This means that all recorded measurement data is available without time-consuming disk access and can be called up for instant searches.

The Allegro Multimeter can operate without an internal or external hard disk and only use in-memory for the metadata, i.e. no data is written to the hard disk.

The in-memory database capacity varies between 2 GB and 1.5 TB depending on the model. As an approximation, the history of about 150,000 connections and their aggregations can be stored per gigabyte in-memory database.

The Allegro Network Multimeter adapts its memory configuration to the quantity of traffic. It always stores all data. If the memory is full, the longest inactive connections and IP addresses are deleted. This means that in smaller networks the device stores historical data for a longer period, while in larger networks the device stores more IP addresses and associated information, but only for a shorter period of time.

The Allegro system's memory fills up automatically over time (except for a memory reserve) to provide measurement data for as long as possible. Afterwards, old data is automatically deleted to ensure optimal system memory.

In the Web interface of the Allegro Network Multimeter, the system info page in the »Info« submenu shows the current memory usage and the period for which the data is available. The storage time depends on the type of data traffic.

By default, all graphs display network traffic with one second resolution. The level of detail for older recorded network traffic is automatically reduced to up to one minute. The administrator has the option of adjusting both graphic resolutions and reduction values in the system settings. These settings can result in either more detailed graphics or longer data storage times. Graphics resolution can be reduced to one millisecond.

The metadata stored in the in-memory database is lost when the Allegro Network Multimeter processing is stopped (update, shutdown, restart, reboot). Metadata is also lost in the event of a power failure.

Since the Allegro Network Multimeter does not permanently store network information, the device can be used in security-sensitive areas. If you want to restore the recorded information or extract individual packets from the past, we recommend the use of a packet ring buffer.

Ring buffer

If a packet ring buffer is used, the packets are stored on a connected storage medium. The following systems can be used for this purpose:

- Internal hard disks or SSDs (Allegro 500 and higher),
- External hard disks via USB3 (all Allegro Multimeters),
- iSCSI systems via the management port (all Allegro Multimeters).

The ring buffer makes it possible to create a fixed size packet buffer on which all recorded packets are stored - on one or more external storage devices. When the buffer is full, the oldest packets in the buffer are replaced by new packets.

In-memory database

- ✓ Direct access to all measurement data
- ✓ Fast problem search and correlation across network layers
- ✓ Access to all previous connections
- ✓ For evaluations relevant to data protection

Ring buffer

- ✓ Permanent, automatic recording of raw data
- ✓ Targeted extraction of network packets from the past
- ✓ Retrospective analysis of stored network packets without the need for network access
- ✓ Access to all functions of the in-memory database by re-analysing stored packets

The ring buffer can also be created over several hard disks. Up to 64 hard disks with a ring buffer of several petabytes are supported. Additionally, a data redundancy with 0 up to 3-fold redundancy is supported.

To prevent misuse, the storage device can be formatted with AES256 encryption (Caution: subsequent access to the disk without a password is not possible).

The packet ring buffer can also be used to analyse packet capture files. In addition, the packet ring buffer is also used for the analysis of pcap files to simplify the extraction of packets. Please note that all previous contents of the packet ring buffer will be deleted. This behaviour must therefore be explicitly enabled in the file analysis dialog to prevent unintentional deletion.

Use Case 1
Historical Pcap Extraction

By using the packet ring buffer on the Allegro Network Multimeter hard disk, it is possible to extract traffic from the past and create a pcap from it. The packet ring buffer can be set up on both internal and external storage devices. When the Allegro Network Multimeter is shipped with a storage device, the ring buffer is preconfigured and uses 75 % of the available capacity. Otherwise, the ring buffer can be created directly on a formatted storage device on the corresponding page in the Web interface.

The »packet ring buffer« statistics page displays information about the use of the ring buffer and multiple graphs of the stored traffic (**Figure 2**). Filters can be used to set which packets are stored in the ring buffer. By default, all packets are stored.

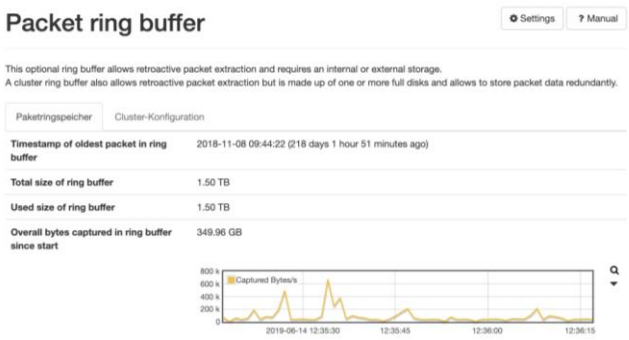

Figure 2: Statistics and configuration of the packet ring buffer

The capture function accesses the contents of the ring buffer and can extract data traffic from the past. On every page on the Web interface there are pcap symbols. Click on the pcap icon next to the statistic whose packets you wish to extract.

This will open a corresponding dialogue window, which suggests a reasonable time period and some options. You can change the period and the proposed options. If the start time of the recording is before the start time of the packet ring buffer, the start time of the recording is automatically adjusted and a message is displayed (**Figure 3**).

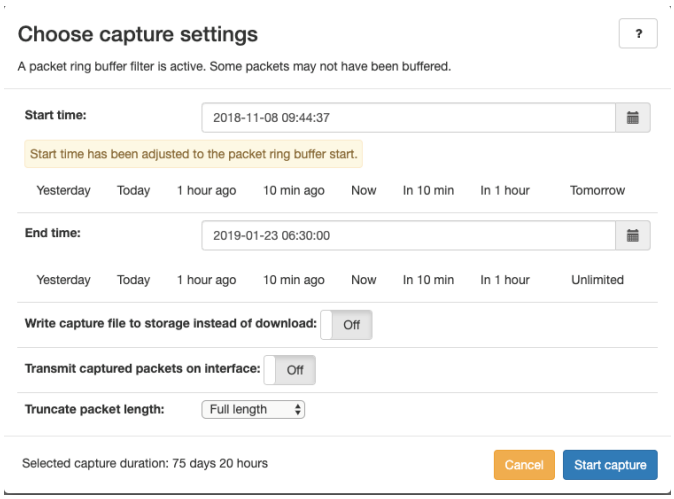

Figure 3: Capture dialogue with time adjustment to the available time interval in the ring buffer

If the ring buffer is activated, the behaviour of the pcap capture buttons changes in the entire system: If the user interface is in live mode and a capture is started, a dialogue appears in which you can specify when the capture should be started. This makes it possible, for example, to capture the traffic of an IP address from a certain time. If the user interface is in »back-in-time« mode (where a defined period of time from the past is selected), a dialogue box appears when a capture is started, confirming that the capture covers exactly the selected period of time. The capture stops automatically after the selected time span has been processed.

With additional options it is possible to save the pcap file directly to the hard disk or to transfer only the beginning of the packets. Both are especially helpful if there is only a limited bandwidth to the Allegro Network Multimeter, e.g. via a VPN tunnel. Here, a capture can first be stored on the memory and then be downloaded via **General -> Data carrier** (**Figure 4**).

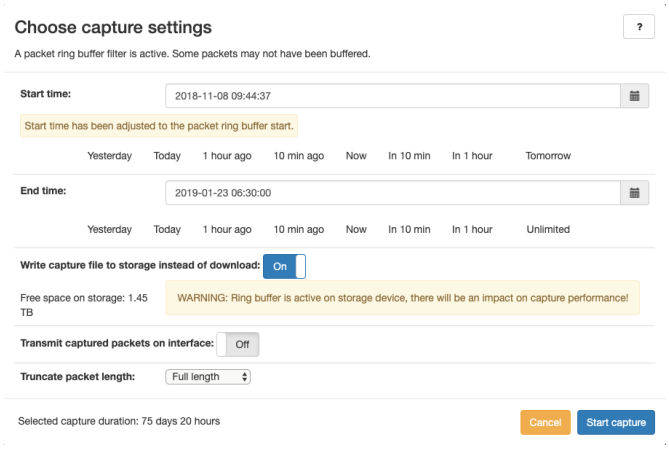

Figure 4: Alternative recording on data medium instead of download

The Allegro Packets tools can also return historical traffic to a network interface. This is very useful for reimporting an error in a network for analysis purposes. In **Figure 5** all traffic is replayed on port 4 with 10 MBit/s bandwidth. The traffic can also be played back in real-time at configurable speeds.

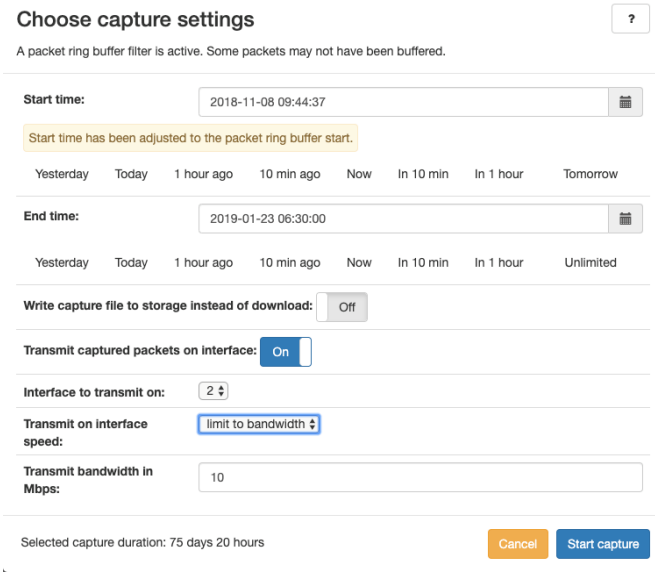

Figure 5: Repeated playback of network traffic on port 4

Use Case 2
Prefilter for the Packet Ring Buffer

The data of a device, a group of devices or applications are to be recorded and stored in the ring buffer. This can be configured in the Allegro system on the page "Packet Ring Storage" under "Statistics". A prerequisite for this is that the connected storage device has previously been formatted and a ring buffer has been created on it. The Allegro Packets tools provide the following filter functions, for example:

- Only certain parts of the data stream are to be recorded, e.g. the data of one device or an application are to be recorded and stored in the ring buffer.
- Only the lower three layers of the data stream are required for analysis or further processing.

In the first case, the Allegro Network Multimeter rules prevent certain packets from being stored in the packet ring buffer.

In the second case, rules can be configured that define the recording length of the packets to be stored in the packet ring buffer. In this case, the information about the original length of a packet is retained in the captures.

When creating a ring buffer filter rule, the following options are provided:

- **Rule condition:** All packets or a specific MAC or IP address, TCP/UDP port, VLAN tag or interface correspond to a specific value.
- **To negate:** A previously defined restriction is checked vice-versa (e.g. instead of recording a specific IP address, a specific IP address is now excluded).
- **Action:** Defines what to do with the appropriate packages:
  - Recording length: The packet is recorded with the maximum length specified in the input field. If the packet is larger, the remaining bytes are discarded.
  - Discard: The entire package is not recorded.
  - Full length: The entire packet is recorded.
  - Header: Only the packet header is recorded. If the value »L3« is selected, the Layer 2 and Layer 3 headers are stored, i.e. MAC and IP information. If »L4« is selected, Layers 2, 3 and 4 are saved, including TCP or UDP headers.

Example: A fully loaded 10 GBit/s link is analysed. The connected hard disk can record a maximum of 1 GBit/s. In addition, not all data is necessary. Instead, only one SIP server and its connections should be recorded. For this, the following two rules are defined for the ring buffer (**Figure 6**).

- **Rule 1:** IP address from SIP server -> full packet length,
- **Rule 2:** all (other) packets are not recorded.

The advantage of these rules is that the Allegro Network Multimeter can process higher link bandwidths and buffer them retroactively for longer.

In the second step, rule 2 can be changed so that only the data up to Layer 4 is stored. This means that all communication including the L4 header is available and allows writing to memory with a significantly lower bandwidth. With an average packet size of 700 bytes, the data rate reduction here is approx 80 % - 90 % and allows links with more than 1 GBit/s to be analysed on a relatively slow USB3 HDD.

Note: If not all packets are stored in the ring buffer, the metadata is still available in memory for all traffic.

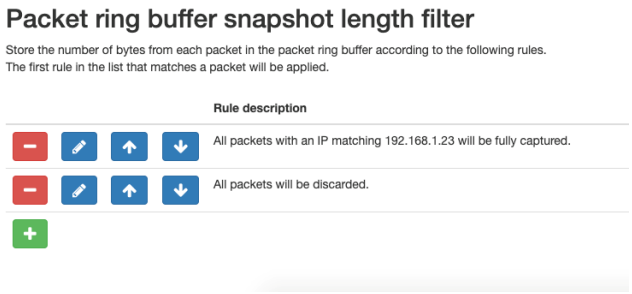

Figure 6: Filter rules to completely record IP 192.168.1.23 and discard all other packets

Use Case 3
Forensic (subsequent) Analysis of the Ring Buffer

Suppose the packet ring buffer of the Allegro Network Multimeter is activated during data analysis. All packets are stored in the packet ring buffer. If the Allegro Network Multimeter is switched off after the analysis has been completed, the metadata obtained from the measurement data is deleted from the main memory. However, the data recorded in the packet ring buffer is retained even after the device is switched off.

If the device is switched on again, the administrator can start the analysis of the packet ring buffer. This is initiated via the Web interface **General -> Packet Ring Store -> Analyze Packet Ring Store** (**Figure 7**). All packets stored in the packet ring buffer will be analysed by the Allegro Network Multimeter and all metadata will be generated again. It must be ensured that all time measurements and time stamps correspond exactly to the time of the recording and that all response time measurements also contain the time values that are in the packet.

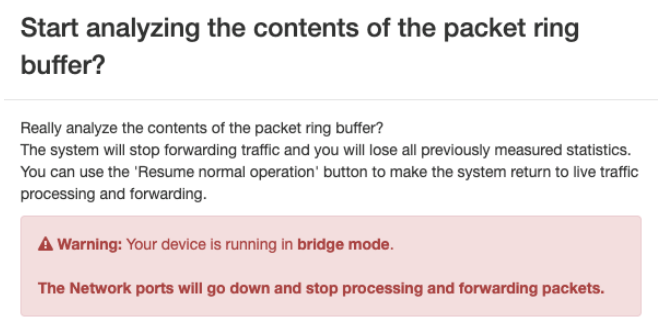

Figure 7: Re-analysis of previously recorded packets in the ring buffer

Example: The Allegro Network Multimeter is sent by mail to a branch office and connected by an employee. Only the network connections are connected to the prepared and preconfigured ports. A connection to the management port is not necessary. After switching on the device, all data packets are written to the ring buffer in real-time.

At the end of the trial period, the Allegro device is turned off and returned to central IT facility.

The device is switched on again in the laboratory or test environment in the central IT facility. Here however, the management port is used and all data / statistics stored in the packet ring buffer are restored using **General -> packet ring memory -> Analyse packet ring memory**.

The administrator can then perform all analyses (as with real-time data) and extract the corresponding pcaps if required.

Use Case 4
Planned records

The Allegro Network Multimeter can be used for scheduled recordings. For example, if the administrator wishes to schedule the recording in advance for a planned operation such as an update to a server.

To achieve this, the Allegro Network Multimeter starts a recording for the selected traffic, such as an IP or MAC address or the entire link. The desired start and end time can then be selected using the calendar icon (**Figure 8**).

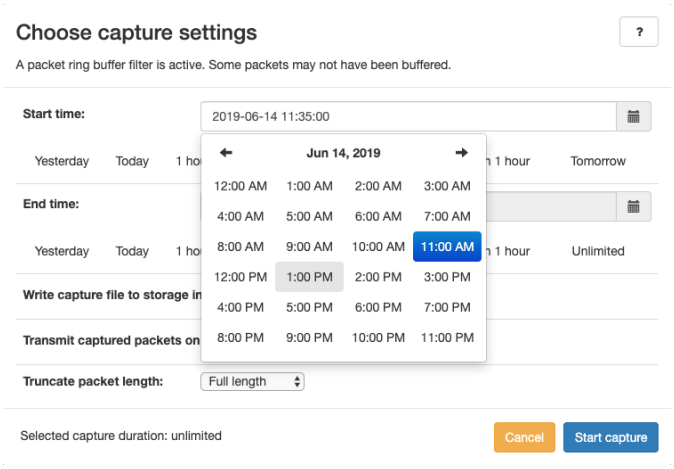

Figure 8: Configuration of a planned recording via calendar

It is recommended to write the capture directly to the hard disk (**Figure 9**). If a high-bandwidth capture is to be conducted, it is recommended to disable the ring buffer during the capture so that the hard disk does not have to write twice to the ring buffer and to the file.

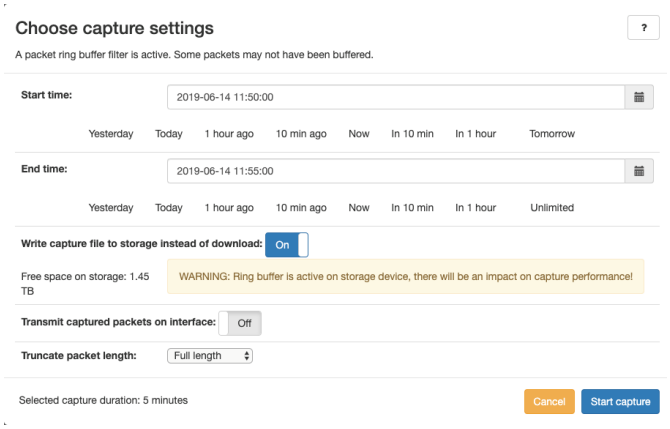

Figure 9: Planned recording to hard disk

Since the capture function runs in the background, the normal measurement and analysis functions of the Allegro Network Multimeter are not affected and the Allegro can continue to be used normally. Up to a total of four recordings can be run simultaneously.

For further questions about the Allegro Network Multimeter in general or about the in-memory database and ring buffer in particular, please feel free to contact us at any time.

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.