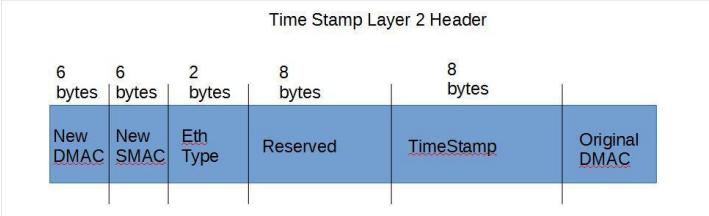
In traditional data center applications, devices are used to sample network traffic. As traffic increases, there is a growing requirement for extended performance monitoring.

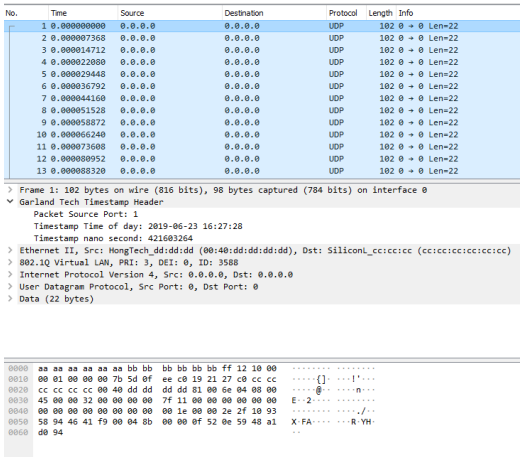
The Advanced Features provides a flexible packet time stamping function. The time stamp function is set up to insert a new 30 byte Layer 2 header before the original DMAC address. The Time Stamp Layer 2 header is defined as follows.



The time stamping is performed before the packet enters the switching chip. This function supports the standard Time of Day format and is accurate down to 8 nano-second resolution. Software can distinguish these packets by the new EthType that has been added into the packet. The Time Stamp EthType is defined as 0xff12.

When Layer 3 routing or filtering is to be performed, the additional Time Stamp header needs to be removed.

Garland Technology has produced a Wireshark plugin that will capture and display these packets as shown below.



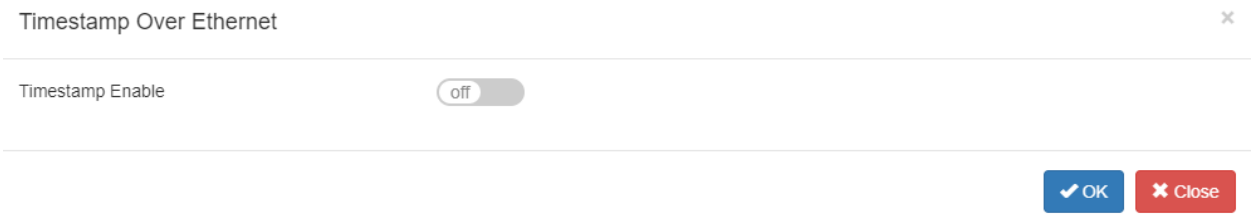
This document discusses the procedure to enable Timestamp. The procedure to apply Timestamp is discussed in the TAP group guide.

Copyright © 2023 Garland Technology, LLC. All rights reserved.

Enable Timestamp

1. Select TAP Management.
2. Select TAP Group Table.
3. Select Timestamp.

The Timestamp over Ethernet panel will appear.



4. Select Timestamp Enable.

5. Enter the Dst-mac for the new Time Stamp L2 segment.
6. Enter the Src-mac for the new Time Stamp L2 segment.
7. Enter the Ether Type for the new Time Stamp L2 segment, (0xff12).
8. Select OK.

Timestamp may be applied to any egress port(s) when a TAP Group is created.

Copyright © 2023 Garland Technology, LLC. All rights reserved.