PB100G24AC Time Stamping

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

The PB100G24AC 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 DestMAC address. The time stamp Layer 2 header is defined (right) as follows:

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>length</th>
<th>info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>2015-05-30 16:04:05</td>
<td>192.168.100.10</td>
<td>192.168.100.12</td>
<td>IPv4</td>
<td>64</td>
<td>hop-by-hop option (0x00)</td>
</tr>
</tbody>
</table>

For questions, please contact Garland Technical Support at:
8 AM – 9 PM (CST) Monday – Friday (except for observed US Holidays)
+1.716.242.8500  |  support@garlandtechnology.com

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 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.

Note: When Layer 3 routing or filtering is to be performed, the additional Time Stamp header needs to be removed. Contact Garland Technology for a Wireshark plugin that will capture and display these packets.

Setting up the PB100G24AC to Time Stamp packets:
1) Configure the new MAC addresses and the new EthType:
Switch(config)# timestamp-over-ether x.x.x y.y.y 0xff12 (where x.x.x is the new DMAC, and y.y.y is the new SMAC)

2) Configure a time stamp group:
Switch(config)#tap-group tap_test_ts

3) Configure the ingress/egress ports:
Switch(config)#ingress eth-0-1
Switch(config)#egress eth-0-2 timestamp

4) Use the show tap-group command to verify time stamping is enabled:
Switch(config)#show tap-group
TAP-group ingress flowname mark-src egress
----------------------------------------+----------------++---------+---------------
tap_test_ts      eth-0-1                                      eth-0-2[Ts]

5) Use Wireshark and the plugin to parse and display the new time stamped packets.