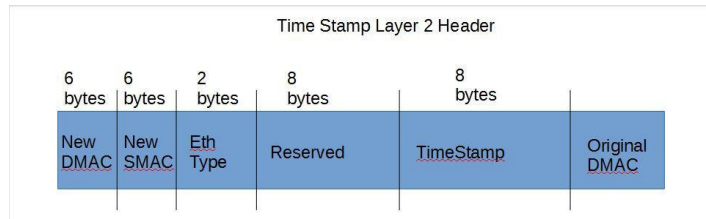


In traditional data center applications, devices are used to sample network traffic. As traffic increases, there is a growing requirement for extended performance monitoring.

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.

```

No.    Time           Source            Destination      Protocol  Length  Info
-----
1 0.000000000 0.0.0.0          0.0.0.0          UDP       102    0 → 0 Len=22
2 0.000007368 0.0.0.0          0.0.0.0          UDP       102    0 → 0 Len=22
3 0.000014712 0.0.0.0          0.0.0.0          UDP       102    0 → 0 Len=22
4 0.000022080 0.0.0.0          0.0.0.0          UDP       102    0 → 0 Len=22
5 0.000029448 0.0.0.0          0.0.0.0          UDP       102    0 → 0 Len=22
6 0.000036792 0.0.0.0          0.0.0.0          UDP       102    0 → 0 Len=22
7 0.000044160 0.0.0.0          0.0.0.0          UDP       102    0 → 0 Len=22
8 0.000051528 0.0.0.0          0.0.0.0          UDP       102    0 → 0 Len=22
9 0.000058872 0.0.0.0          0.0.0.0          UDP       102    0 → 0 Len=22
10 0.000066240 0.0.0.0          0.0.0.0          UDP       102    0 → 0 Len=22
11 0.000073608 0.0.0.0          0.0.0.0          UDP       102    0 → 0 Len=22
12 0.000080952 0.0.0.0          0.0.0.0          UDP       102    0 → 0 Len=22
13 0.000088320 0.0.0.0          0.0.0.0          UDP       102    0 → 0 Len=22

> Frame 1: 102 bytes on wire (816 bits), 98 bytes captured (784 bits) on Interface 0
Garland Tech Timestamp Header
  Packet Source Port: 1
  Timestamp Time of day: 2019-06-23 16:27:28
  Timestamp nano seconds: 421603264
  > Ethernet II, Src: HongTech_dd:dd:dd (00:40:dd:dd:dd:dd), Dst: Silicon_cc:cc:cc (cc:cc:cc:cc:cc:cc)
  > 802.1Q Virtual LAN, PRI: 3, DEI: 0, ID: 3588
  > Internet Protocol Version 4, Src: 0.0.0.0, Dst: 0.0.0.0
  > User Datagram Protocol, Src Port: 0, Dst Port: 0
  > Data (22 bytes)

0000  aa aa aa aa aa bb bb bb bb ff 13 10 00  .....-...!
0010  00 01 00 00 00 75 5d ff  ee c0 13 21 77 c0 cc cc  .....{}...
0020  cc cc cc cc 00 40 dd dd dd dd 81 00 6e 04 08 00  .....@.....
0030  45 00 00 32 00 00 00 00  7f 11 00 00 00 00 00 00  E-2.....
0040  00 00 00 00 00 00 00 00  00 1e 00 00 2a 2f 10 93  .....-.../...
0050  58 94 46 a1 f9 00 04 8b  00 00 0f 52 0e 59 48 a1  X:FA....R:YH
0060  d0 94  ..

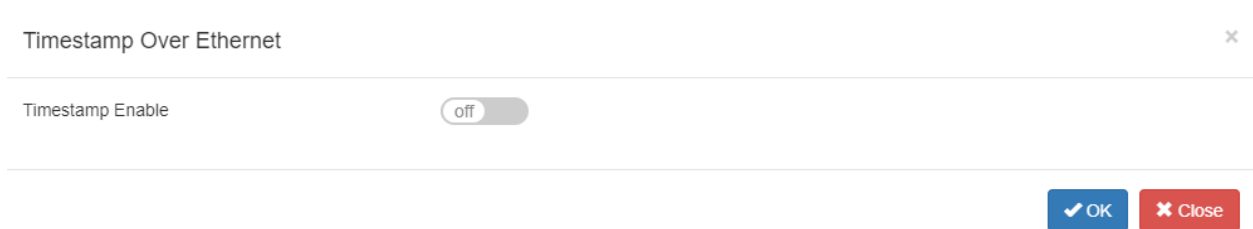
```

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

Enable Timestamp

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

The Timestamp over Ethernet panel will appear.



Timestamp Over Ethernet

Timestamp Enable off

OK Close

4. Select Timestamp Enable.



Timestamp Over Ethernet

Timestamp Enable on

Dst-mac f093.c5a1.a1a1 Src-mac f093.c5b2.b2b2 Type 0xff12

OK Close

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.