Packet Timestamping

- About Packet Timestamping, on page 1
- Guidelines and Limitations, on page 3

About Packet Timestamping

Packet timestamping enables precise, scalable traffic monitoring. It helps to detect congestion spots on routers or devices in the network.

Every participating switch can add one or more timestamp shims, and the decision is based on local configuration.

Timestamping consists of:

- Per-port or Per-flow timestamping
- Insert up to two timestamps at the end of the frame (pre-enqueue and post-dequeue)
- Convey a notion of source identifier that accompany every timestamp record (path topology)

The following figure provides a graphical representation of packet timestamping.
Per-Port Timestamping

An advantage of per-port timestamping is that you can save IFP entries and all packets get timestamped. Each port can be configured to enable timestamping in this way:

- Packets entering ports with timestamping enabled get an ingress timestamp.
- Packets that leave timestamp-enabled ports get an egress timestamp.

To enable per-port timestamping on ingress and egress of port ethernet1/1 using the CLI in NX-OS:

```
configure terminal
interface ethernet1/1
timestamp ingress id source_id egress id source_id
```

To disable per-port timestamping on port e1/1 using the CLI in NX-OS:

```
no timestamp
```

Per-Flow Timestamping

Per-flow granularity is achieved in timestamping by defining new action fields for the IFP policy table.

Captured Data

Following is an example of captured date without packet timestamping:

```
0000 00 00 01 00 00 01 00 10 94 00 00 02 08 00 45 00
0010 00 52 d2 ee 00 00 ff fd 66 67 c0 55 01 02 c0 00
```
Following is an example of captured date with packet timestamping in ingress and egress enabled:

```
0000  00 00 01 00 00 01 00 10 94 00 00 02 08 00 45 00
0010  00 52 81 ef 00 00 ff fd b7 66 c0 55 01 02 c0 00
0020  00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0030  00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0040  00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00
0050  54 df 93 d4 cd 46 97 80 2c 89 f1 0e 50 33 0c d9
0060  9b e9 fc 50 00 00 b1 cc e0 6e 00 00 01 54 00 00
0070  00 00 00 00 b1 cc e2 24 00 00 01 77
```

### Guidelines and Limitations

Following are the guidelines and limitations for the timestamping feature:

- The timestamping feature is supported only on Cisco Nexus 3132C-Z and Cisco Nexus 3264C-E switches.
- Timestamp is not part of the L3 packet. Any checks that assume that the L3+ packet length field represents the total frame length will not be accurate. Systems that need to subject packets to such checks must disable timestamping for the corresponding system or port of flow.
- Header length fields or checksum fields (for example, UDP checksum) will not be updated with the insertion of the timestamp.
- IEEE 802.3 frames (for example, SNAP LLC) are not supported.
- Features that rely on the I2E_CLASSID and HG_CLASSID extended header will not co-exist with packet timestamping.
- No switches across the timestamping path should do pad-stripping or otherwise adjust frame content based on the IP header `payload_len/total_len` field for Ethernet II frames.
- Timestamping is not available for:
  - Mirrored copy
  - SOBMH packets
  - Truncated packets
  - Ingress of HiGig port
  - RCPU