15. Packet Loss

Packet loss typically occurs at an interconnecting device such as a switch, a router, a NAT device, or a network firewall. When a TCP host notices packet loss (based on an unexpected TCP sequence number or no acknowledgment within the Retransmission Time Out), the host begins a recovery process. A UDP-based application must be written to detect packet loss and begin its own recovery process.

If the number of packets dropped is small and the recovery process is quick, the packet loss may go unnoticed. If many sequential packets are lost, however, users will likely feel the impact and complain.

When your trace file indicates packets have been lost, you must move your capture point across interconnecting devices to locate the point where packet loss begins.

Be aware that in some situations Wireshark may trigger a packet loss warning when packets are simply out of order.

Possible Symptoms

- Expert Infos Warning: Previous Segment Not Captured
- Expert Infos Note: Duplicate ACKs
- Expert Infos Note: Fast Retransmission
- Expert Infos Note: Retransmission
- IO Graph: Drops in throughput

16. High Path Latency

A single low speed (high delay) link along a path or the delay between geographically disbursed peers can inject a level of path latency that affects performance.

Possible Symptoms

- Capture at client: Large delays between the outbound SYN and the inbound SYN/ACK of a TCP handshake (**`tcp.time_delta`**).
- Capture at server: Large delays between the SYN/ACK and the ACK of a TCP handshake (**`tcp.time_delta`**).