Out-of-Order Packets

Display Filter Value

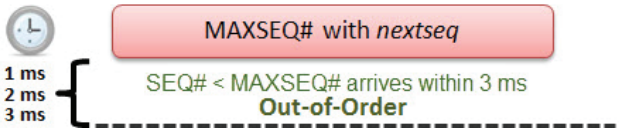
```
tcp.analysis.out_of_order
```

Traffic Analysis Overview

Out-of-order packets may not affect performance if there is very little time between their expected arrival and their actual arrival. For example, if two packets arrive in reverse order, but the packets both arrive within 1 ms, it is unlikely this will cause a problem.

If out-of-order packets arrive after quite a delay, or there are many out-of-order packets, there may be a noticeable degradation in performance. TCP cannot pass received data up to the application until all the bytes are in the correct order.

Wireshark marks a packet as out of order based on the fact that it (a) contains data, (b) does not advance the sequence number value, and (c) arrives within 3 ms of the highest sequence number seen. There may be one or more ACKs seen between the Previous Segment Not Captured point and the Out-of-Order packet.



What Causes Out-of-Order Packets?

Out-of-order packets can be caused by a stream using multiple different speed paths to reach the target (such as traffic traveling through the Internet), poorly configured queuing along a path or even asymmetric routing configurations.

In the case of queuing along a path, out-of-order packets can be caused when the queuing device does not forward packets in a first-in/first-out (FIFO) order.

In the image that follows, a queuing device has reordered the packets upon forwarding. Packets 1 and 2 would be marked as Out-of-Order if the packets arrive within 3 ms of each other. No network issue may be noticed if the total delay would be 6 ms in this case, however.

COLOR IN EBOOK VERSION ONLY