What is Packet duplication and what causes a packet to be duplicated?

A packet can be duplicated on a network in a number of different ways, here’s a few ways which are very common:

- If a router is plugged in to a single network segment and if multiple SPAN ports are connected to a single aggregator, identical traffic will be presented out of each of the SPAN ports. Your monitoring system will then have collected multiple copies of the same packet.

- Placing multiple passive TAPs in a series of point-to-point links, to copy the traffic from each of the desired points in a network, will also result in duplicates of the same packet being tapped from each of these points.

- With an aggregator, if you are monitoring traffic from several points in a network, you’ll end up with multiple copies of the same packet as it traverses each link. An identical packet doesn’t necessarily mean that it has to be 100% the same, since layer 2 information (e.g. MAC, VLAN) may change, but the remainder of the packet from layer 3 upwards is identical.

Why is this an issue?

If you have multiple identical packets being provided by the monitoring system / traffic visibility / network monitoring infrastructure, an analytics tool has to do more work. The tool becomes less effective - essentially costing more - as you have to buy more tools to detect and remove duplicate packets at line-rate as well as analyze the same amount of data. On top of that, there could be issues with the analysis results since the same packets are arriving with different delays respective to each other which can cause different / un-repeatable results and lack of precision with the results. Also, issues with a network could be hidden, because the tool can’t correctly analyze the data, since the underlying issue is being effectively hidden by the duplicated packets.
How to avoid this issue?

With a Network Intelligence Optimization system from VSS Monitoring, you can guarantee your analytic tools are running at their peak efficiency, no more duplicated packets to waste processor cycles are presented to the tool. A series of settings allow you to configure exactly what is and what is not a duplicated packet.

Tool results become more reliable, accuracy and precision are maximized since the tool receives only the data it is expecting. Next time you are looking for a network monitoring system, make sure it has a capability to remove duplicated packets at line-rate.