SOLUTION BRIEF

Understanding and Validating Packet De-Duplication Within Network Packet Brokers

Deployment Scenario: Out-Of-Band Visibility Architecture

There are two common ways to access network monitoring data – either by using network Taps or network switch SPAN ports. With either scenario, duplicate packets are typically created. Depending upon your specific data collection architecture and data access method, those duplicate packets can become excessive – up to 50% of the data traversing your network. Sending duplicate packets into analytics and compliance tools can create an extra burden on those tools and cost you extra money. One of the best solutions to the problem is to use a network packet broker (NPB) to remove the duplicate packets. However, how do you know the NPB is working correctly and removing the duplicate data, and only that duplicate data? The answer is that you need to test the NPB. This solution will help you do just that.

Solution Components

- Network packet broker solution
- Keysight IxNetwork

Benefits

- Increase tool efficiency potentially by 30 to 50% by validating de-duplication accuracy
- Validate that only unnecessary, duplicate data is being removed
- De-duplication can be used to reduce security and monitoring tool costs

Solution Overview

This network visibility solution allows you to:

- Use an NPB to remove duplicate packets caused by the network architecture and use of SPAN technology
- Reduce the amount of monitored data sent to tools using de-duplication
- Validate that your selected NPB actually removes only duplicate packets and not key monitoring traffic as well
- Validate that your selected NPB can actually perform multiple, concurrent functions

KEYSIGHT TECHNOLOGIES

What is Packet De-Duplication?

Duplicate packets of monitoring data can come from several sources, including the use of SPAN ports and the geographic location of data captures. For instance, a normally configured SPAN port (which is frequently used to connect monitoring tools to the network) can generate multiple copies of the same packet. These copies are exact duplicates of the original packet. Even when optimally configured, a SPAN port may generate between one and four copies of a packet and the duplicate packets can represent as much as 50% of the network traffic being sent to a monitoring tool. Eliminating this unnecessary data improves the capacity of pertinent data that your monitoring tools can process.

It also matters where you capture monitoring data. If you capture it at the ingress and then again in the core, you may have copied the same data twice. This double capture is in addition to whatever duplicates were made by the core switches themselves.

A standard NPB is capable of removing duplicate packets at full line rate before forwarding traffic to the monitoring tools. Multiple copies are simply dropped from the data stream with no effect on the tools. A large de-duplication window and the ability to configure the window size within the NPB makes the de-duplication feature extremely powerful.

Not all NPBs are created equal. Some cannot actually handle de-duplication at full line rate, even if the manufacturer claims it does. This is important at 40 and 100 Gbps.

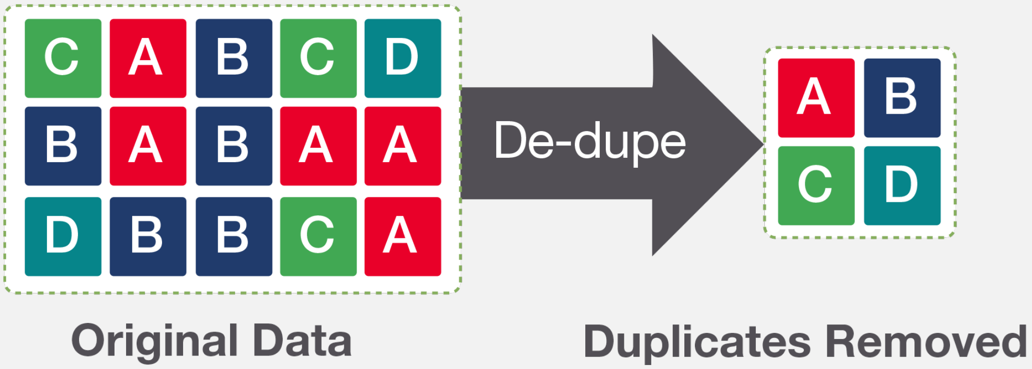

Figure 1. General De-Duplication Process

However, not all NPBs are created equal. Some cannot actually handle de-duplication at full line rate, even if the manufacturer claims it does. This is important at 40 and 100 Gbps. In addition, there may be packet size restraints or other restraints that make the NPB falter, even to the point that it may drop key pieces of monitoring data that you want to keep and analyze. The NPB may also not be able to handle multiple concurrent functions (e.g. packet slicing, load balancing, data masking, and header stripping) at line rate. This solution can answer those key questions.

Validation of NPB De-Duplication Capabilities

By setting up this test scenario, you can validate the performance of your NPB and even compare multiple NPB products. This solution exposes whether the de-duplication function in your network performance management (NPM) solution works, how well it works, whether it works at full line rate or not, and if there are any feature limitations.

Here is the basic process to validate that your NPB works correctly:

1. Connect a traffic generator (IxNetwork in this case) to the NPB and connect 40G of traffic (either four 10 Gbps ports or one 40 Gbps port) on the ingress ports and another 40 Gbps on the egress
2. Configure your NPB for de-duplication on the four ingress ports
3. Set the traffic generator to send 50% duplicate packets on the ingress, which means that only 20 Gbps traffic should come out of the egress
4. Validate that 20 Gbps of data come out the egress and that there are no duplicate packets
5. Rerun the test for 160 Gbps of traffic to test higher performance levels
6. Rerun the tests with multiple features like deduplication and packet slicing activated concurrently

Keysight packet brokers have been put to the test and these solutions do not drop traffic. In fact, depending upon the NPB model, it can handle de-duplication and other (simultaneous) features all the way up to 100 Gbps.

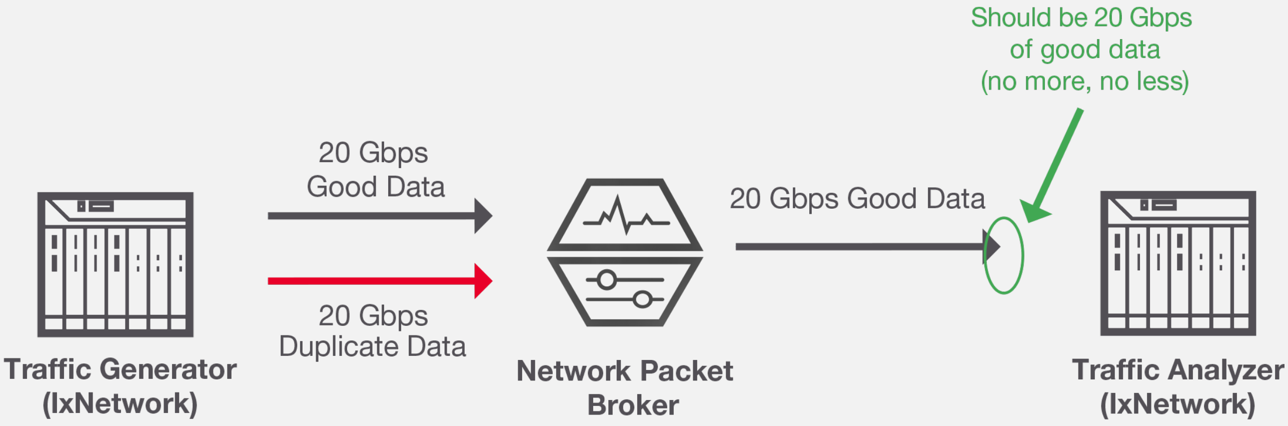

Figure 2. Configuration Set-Up

Summary

Networking devices that drop packets is a huge problem – especially if you don’t know that the data has been dropped. This test will shows that some NPB products on the market are dropping more than 80% of the packets while the Keysight solution doesn’t drop any. The loss within those NPBs increases as the bandwidth consumption increases to 160 Gbps and also as different frame sizes and even packet sizes (1518 byte, 256 byte, etc.) are used.

Keysight packet brokers have been put to the test and these solutions do not drop traffic. In fact, depending upon the NPB model, it can handle de-duplication and other (simultaneous) features all the way up to 100 Gbps per port without bandwidth limitations.

Visibility Architecture Solutions from Keysight

Keysight’s network visibility solution uses NPBs in conjunction with application intelligence and taps. Learn more about Keysight’s Network Packet Brokers, PacketStack, and IxNetwork Technology.

Learn more at: www.keysight.com

For more information on Keysight Technologies’ products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus