

#221118

March 2021

Commissioned by

Keysight Technologies

Network Packet Broker Performance & Features

Keysight Vision X

EXECUTIVE SUMMARY

Network visibility is essential to network security and performance management. In practical terms, visibility relies heavily on a packet broker's ability to process tapped traffic reliably and intelligently. All tapped traffic from switched port analyzer (SPAN) and test access point (TAP) ports must have duplicate packets eliminated and be delivered without loss to network security tools. Another key to complete visibility is application intelligence. Network packet brokers (NPB) are required to detect, report, filter and present application metadata to security monitoring tools in a reliable and consistent way.

Keysight commissioned Tolly to report on the advanced packet processing capability (deduplication, in particular) and the application intelligence of its Vision X network packet broker.

Throughout the testing described, Keysight Vision X demonstrated high packet processing of 2Tbps systemwide combined with no-drop packet deduplication and rapid, accurate detection of applications.

THE BOTTOM LINE

Keysight Vision X delivers:

- 1 Innovative design and memory optimization
- 2 System-wide advanced packet processing capacity of 2Tbps
- **3** High performance packet deduplication with no packet drop
- **4** Accurate application detection within seconds under load
- **5** Patented filter compiler to resolve overlap rules seamlessly





Solution Architecture & System Capacity

The system is built around Broadcom's Tomahawk II switching silicon that provides a maximum of 128 logical ports and 4K general rules. Keysight's implementation provides a combination of flexibility and resource optimization. See Figure 1 & Table 1.

Breakout Port Flexibility

Datacenters can consist of any combination of 10/25/40/50/100GbE ports. Flexible breakout of ports is an important consideration when choosing next-gen packet brokers where each port is ideally capable of five speeds to take advantage of highly condensed network design.

Some packet brokers only allow specific ports to break out (fan out). By contrast, Vision X allows any port from a pipeline to be fanned-out regardless of its physical location and each port is 5-speed capable. A single module support up to 64 breakouts and two modules support 108 breakouts with 20 ports being internally reserved for advanced packet processing.

Filter Memory Optimization

Test results demonstrated the benefits of Keysight's unique filter memory optimization technique. This leverages unused system memory to increase the number of filter rules supported. In the test example, 75% of filter memory was consumed prior to optimization. After optimization, only 4% of filter memory was consumed. (See Sidebar.)

Switch Control Card

The switch control card is where the switching silicon resides and provides backplane switching capability. As a result, it is mandatory for the chassis

to operate. Keysight implemented its switch card with an additional 12 ports capable of five speeds.

Overview of Keysight Vision X System Features

Rack Space	3U
Switch Silicon	Broadcom Tomahawk II
Backplane Capacity	6.4 Tbps
Open Slots (for provisioning ports)	4 + 1 (one rear slot)
Filter Memory	4K rules in main table + memory optimization to allow double or triple amount of rules
Max. rules per slot	2K per open slot; 4K for switch card
Max. 10G Ports	108
Max. 40G Ports	76
Max. 100G Ports	60
Max. 25G/50G Ports	108/108
Advanced Packet Processing Capacity Per Module	400 Gbps
Advanced Packet Processing Capacity Per System	2 Tbps

https://www.keysight.com/us/en/assets/3120-1029/data-sheets/Vision-X Network-Packet-Broker.pdf capacity.

Source: Keysight Data Sheet, August 2020

Table 1

More importantly, the Keysight switch card is connected to 4 pipelines from the switch silicon; making it a fully functional module with full access to 4K memory rules.

Sidebar: Filter Optimization Example

In this case, one of the 4 quadrants is 75% full (25% available) before optimization is triggered and it becomes only 4% full (96% available) after optimization is completed. Total saving is 71% for the same number of rules.





Advanced Processing Capacity

Of particular interest is the advanced packet processing capacity. Keysight implemented its advanced packet processing functions using dedicated hardware/FPGA. As a result, there is significant processing capacity on both a per module basis (400G) and per chassis basis (2Tbps). Most importantly, Keysight's hardware-based implementation doesn't drop packets. Vendors implementing software-based processing can exhibit performance that varies with packet sizes.

Smart Filtering

It is not at all uncommon for multiple tools to require different subsets of the traffic being generated by a single span port. These overlapping rules can be difficult to configure in some products. According to Keysight, its U.S. patented Dynamic Filter Compiler allows for overlapping filters that can be configured simply. In this test, the offered traffic for VLAN 1-3 was 3,000 frames per second (1,000 FPS for each VLAN), for TCP (no VLAN) it is also 3,000 FPS and for VLAN 3-6 it is 4,000 FPS so each VLAN ID has 1000 FPS. See Figure 2.

Note that there is no manual effort involved in the resolution of overlapping rule. The expected output is: Tool1 = 4,000 FPS; Tool2 = 6,000 FPS; Tool3 = 5,000 FPS. As expected, the Keysight solution delivered accurate results – all tools received their expected number of packets.

Packet Deduplication Performance

Removing duplicated packets from a packet stream is an essential task of an NPB. This test involved sending a 50/50 mix of unique/duplicate traffic via a 100GbE port. The test was run with six packet sizes from 64- through 1518-bytes and also using a mixture of packet sizes (IMIX).

Keysight Technologies		
Vision X Packet Processing Performance Evaluation	Tolly.	
	Tested August 2020	

The system was configured to deduplicate the traffic and forward only unique packets. To perform packet deduplication, a system must buffer all packet signatures (a.k.a hashing digest). For each incoming packet, the system must calculate its signature and compare to those stored in the buffer. Only packets without a matching signature are considered unique and subsequently forwarded.

It is important to understand how a system behaves in cases where its packet deduplication processing limit is reached.





Packet Deduplication Processing Performance 50/50 Mix of Unique/Duplicate Traffic (100GbE Ports)

Input Packet Size (Bytes)	Max Deduplication & Forward Rate	Dropped
64	80%	0%*
128	100%	0%
256	100%	0%
512	100%	0%
1024	100%	0%
1518	100%	0%
IMIX Tolly	100%	0%

Note: *Deduplication buffer that is used for storing packet signature is full and duplicate packets are not removed but forwarded to egress without drop. In this case, egress port receives more packets than it is expected (duplicates fail to be removed) and no packet drop occurs.

Source: Tolly, August 2020

Specifically, what happens to the packets that are beyond the limits of the deduplication engine? Are those packets forwarded or are they dropped (lost)?

With Vision X, packets in excess of the maximum forwarding limit are not dropped but forwarded along with other, deduplicated packets. The maximum

forwarding rate for most packet sizes is 100%.

Table 2

In this test, Vision X was able to deduplicate and forward 100% of packets for all packet sizes except 64-bytes packets. With those, Vision X was able to deduplicate and forward 80% of incoming packets before reaching its limits. At this point, the signature buffer is full and packets are forwarded without being deduplicated so the remaining 20% at the egress is filled up with duplicates. No packets were dropped even at this extreme corner case. See Table 2.

Application Detection and NetFlow Generation Performance

Recognizing applications is another essential task of NPBs. This test focused on how quickly and accurately applications could be recognized by each solution both under light and heavy traffic loads. Engineers also noted the information presented by each solution's dashboard. Engineers also evaluated each solution's capabilities with respect to generating NetFlow application metadata. See Table 3 for all the results for this group of tests.

Application Detection Speed

When confronted with network issues, it is safe to assume that "time is of the essence." Thus, a rapid and complete presentation of application information is desirable.

Application Detection & NetFlow Generation Performance

(as observed by Tolly)

Test	Scenario	Result
Application Detection Speed	First application	10 seconds from start
	All applications	10 seconds from start, all apps displayed together
Application Detection Accuracy	Light Traffic Load (0.5Gbps)	Accurate app identification and statistics
	High Traffic Load (50Gbps)	Accurate. Performance steady and consistent over time
NetFlow Generation	Light Traffic Load (0.5Gbps)	Consistent
	High Traffic Load (50Gbps)	Consistent and stable over time
NetFlow Export	Network Characteristics	Smooth (smaller packets)

Note: Application detection run using ten applications.

Source: Tolly, August 2020

Table 3



For this test, engineers presented a light load containing streams of ten different applications and recorded how much time was required before the NPB identified the first application and then all applications.

Keysight identified all ten applications simultaneously only ten seconds after the start of the test.

Engineers noted that Keysight's dashboard contained ten different information modules that provided additional insights for network technicians. For example, geolocation display could reveal an imminent attack if your company never does business with certain countries yet the dashboard clearly shows heavy traffic from those countries. See Figure 3.

Application Detection Accuracy

It is important for applications to be detected accurately not only when the

network is lightly loaded but also under heavy traffic conditions.

Engineers re-ran the application detection test using the same mix of application streams but at a higher traffic rate. The light load traffic was generated at 0.5Gbps and the high load traffic was generated at 50Gbps.

Keysight's performance remained stable under load. At the load tested, there were no dropped packets and CPU usage did not impact the App Engine and application identification remained accurate. See Figures 4A & B.

NetFlow Generation & Export

Network analysts often require metadata such as NetFlow, which provides a description of network traffic, rather than a full sample of the network traffic itself. NetFlow is a long-established mechanism for delivering that data. In these tests, engineers confirmed that Keysight delivered NetFlow data as requested and performance is steady and consistent throughout the test.

Test Methodology

Solution Under Test

The Keysight Vision X network packet broker was evaluated. Software modules and versions are found in Table 4.

Solution Architecture & System Capacity

This information was based primarily on the published specifications along with the published specifications of the Broadcom Tomahawk II switching silicon¹.



¹ https://www.broadcom.com/products/ethernet-connectivity/switching/strataxgs/bcm56970-series



To quantify the benefits of rule optimization, rules were generated and memory usage measured. Then, the rules were moved to optimized memory and memory usage was measured again.

Smart Filtering

The methodology was explained in the test results section.

Packet Deduplication

A Keysight Novus and CloudStorm packet generator was used to generate traffic of the specified packet size at up to 50% utilization. This traffic was replicated by the packet broker using loopback ports. The traffic on the loopback ports are merged so that the input traffic going to deduplication engine on the input side would consist of line rate (100%) traffic of which 50% was unique and 50% duplicate packets. For a logical diagram of the flow, see Figure 6.

Packet sizes: 64-, 128-, 256-, 512-, 1024-, 1518-bytes. The IMIX Tolly was also tested which consists of traffic with the following packet size/weight characteristics: 64:55, 78:5, 576:17, 1518:2.





Application Detection and NetFlow Generation Performance

For this test, a total of 10 apps were constructed on a tester and sent to the NPB under test for app detection, filtering, and meta data generation. As with prior tests, this test was run first with a light load (0.5Gbps) and then, again, with a high load (50Gbps) to determine behavior under different load conditions. Figure 5A & B illustrate the flow of input traffic and, when appropriate, NetFlow metadata.



Source: Tolly, August 2020



Page 7 of 8

Figure 5A & B



About Tolly

The Tolly Group companies have been delivering world-class IT services for more than 30 years. Tolly is a leading global provider of third-party validation services for vendors of IT products, components and services.

You can reach the company by E-mail at <u>sales@tolly.com</u>, or by telephone at +1 561.391.5610.

Visit Tolly on the Internet at http://www.tolly.com

Terms of Usage

This document is provided, free-of-charge, to help you understand whether a given product, technology or service merits additional investigation for your particular needs. Any decision to purchase a product must be based on your own assessment of suitability based on your needs. The document should never be used as a substitute for advice from a qualified IT or business professional. This evaluation was focused on illustrating specific features and/or performance of the product(s) and was conducted under controlled, laboratory conditions. Certain tests may have been tailored to reflect performance under ideal conditions; performance for their own networks.

Reasonable efforts were made to ensure the accuracy of the data contained herein but errors and/or oversights can occur. The test/ audit documented herein may also rely on various test tools the accuracy of which is beyond our control. Furthermore, the document relies on certain representations by the sponsor that are beyond our control to verify. Among these is that the software/ hardware tested is production or production track and is, or will be, available in equivalent or better form to commercial customers. Accordingly, this document is provided "as is," and Tolly Enterprises, LLC (Tolly) gives no warranty, representation or undertaking, whether express or implied, and accepts no legal responsibility, whether direct or indirect, for the accuracy, completeness, usefulness or suitability of any information contained herein. By reviewing this document, you agree that your use of any information contained herein is at your own risk, and you accept all risks and responsibility for losses, damages, costs and other consequences resulting directly or indirectly from any information or material available on it. Tolly is not responsible for, and you agree to hold Tolly and its related affiliates harmless from any loss, harm, injury or damage resulting from or arising out of your use of or reliance on any of the information provided herein.

Tolly makes no claim as to whether any product or company described herein is suitable for investment. You should obtain your own independent professional advice, whether legal, accounting or otherwise, before proceeding with any investment or project related to any information, products or companies described herein. When foreign translations exist, the English document is considered authoritative. To assure accuracy, only use documents downloaded directly from Tolly.com. No part of any document may be reproduced, in whole or in part, without the specific written permission of Tolly. All trademarks used in the document are owned by their respective owners. You agree not to use any trademark in or as the whole or part of your own trademarks in connection with any activities, products or services which are not ours, or in a manner which may be confusing, misleading or deceptive or in a manner that disparages us or our information, projects or developments.