PacketStack+



NextGen Network Packet Broker Offers Advanced Line-Rate Packet Processing at Chip Level

Advanced packet processing is one of the most important features of a Network Packet Broker (NPB). Many security tools cannot work efficiently without the help of a NPB to perform some levels of advanced packet processing like packet deduplication, protocol header stripping, packet trimming or a combination of many, performed as a cascaded operation. It's one of the Key Performance Indicators (KPI) to consider when evaluating and selecting a packet broker. Traditional NPBs implemented the features either via dedicated CPU or dedicated FPGA. NextGen NPB offers the feature via switch silicon, allowing advanced packet processing at line rate on all ports with unprecedented scalability.

Solution

To date, there are two general types of NPB implementation for advanced packet processing: Hardware FPGA-based or software CPU-based.

FPGA hardware accelerates the packet processing of the NPB and offers significant architectural benefits including accelerated advanced packet processing with zero packet-loss at line-rate, independent of packet size. Keysight legacy platforms, including Vision X, Vision ONE, Vision E10S offer this capability.

In contrast, NPBs that rely on onboard software-based CPU processing commonly drop packets as traffic volumes increase and more often than not, cannot use all features simultaneously because of limited CPU power. This significantly slows down application detection and reporting and requires ongoing investment in additional modules.

KEYSIGHT

Keysight offers a third implementation option: using P4 programming language to write the advanced packet processing engine from ground up for Tofino-based NPB family, including patented technology for packet deduplication. This offers unprecedented scalability and allows advanced packet processing functions available on all ports and at line rate. Currently, the feature is offered thru PacketStack+ software stack and is available on Vision E400S and Vision 400 platforms.

Highlights

- Protect monitoring tools so they operate more effectively by removing all duplicated packets, at full line rate with no loss. Up to 9.2Tbps deduplication capability per chassis
- Enable tools to analyze encapsulated payload by removing encapsulation headers such as FabricPath, ETag, VNTag, GTP, LISP, MPLS L2VPN, MPLS L3VPN, MPLSoGRE, MPLSoUDP, VxLAN, GENEVE, L2GRE, L3GRE, IPinIP, or ERSPAN
- Boost tool performance and retain only needed header bytes by trimming payload to a user configurable length of bytes
- Hide MAC addresses (aka MAC rewrite) or IP addresses, before sending the data to your analysis tools
- Terminate L2GRE, VxLAN or ERSPAN tunnels from CloudLens vTap and deliver plain Ethernet traffic to your tools
- Originate L2GRE or VxLAN tunnels with user configurable KEY or VNI values so tapped traffic can reach remote tools with security
- Enable monitor tools to measure latency and jitter, with nanosecond resolution, by replacing source MAC with timestamp derived from local, NTP, PTP or 1PPS+ToD(G.8271) for greater accuracy, in a packet by packet basis

PacketStack+ Capabilities

Capability	Description
Packet de-duplication 	Packet duplicates occur in networks when a packet traverses multiple taps or SPAN ports that generate multiple copies of the same packet. De-duplicating packets reduces the amount of redundant data sent to security and monitoring tools, directly improving tool efficiencies and preserving their integrity. Deduplication is offered by PackeStack+ via Dedup+ feature set in order to differentiate it from FPGA-based Dedup. Dedup+ is a patented technology to utilize certain TCP/UDP/SCTP packet header fields, including TCP/UDP checksums, to perform hashing and derive packet signature as a result. In contrast, FPGA-based Dedup performs hashing and signature calculation based on packet payload.
Protocol header stripping 	Monitoring tools, legacy or even modern ones, cannot analyze traffic encapsulated inside of an unsupported protocol. This feature enables tools to monitor all required data by removing the encapsulation header. Supported protocols include: ETag, VNTag, Fabric Path, GENEVE, L2GRE, L3GRE, VxLAN, GTP, LISP, MPLS L2VPN with or without CW, MPLS L3VPN, MPLS over GRE, MPLS over UDP, ERSPAN, IPinIP. Up to two protocol headers can be removed in one data pass (one at Network Port, and one at Dynamic Filter/Tool Port). If incoming data contains more than 2 protocol encapsulation headers, loopback ports can be used to remove as many protocol headers as needed (cascaded stripping).
Native tunnel termination 	Traffic coming from remote site or virtual environment usually is encapsulated with certain protocols such as L2GRE, VxLAN, ERSPAN, GENVE, or MPLS. It's required for the NPB ingress port to actively terminate these protocols before going thru filtering, load balancing or other functions to reach locally attached tool. All protocols supported by header stripping are also supported by tunnel termination. This is implemented thru a generic Network Interface on all Network Ports to allow destination IP specification and enablement of ARP/PING.
L2GRE and VxLAN tunnel origination 	Tapped traffic, after NPB processing, sometimes need to be delivered to tools at remote site or in the cloud. For security reasons, it's often required for the NPB to initiate L2GRE or VxLAN tunnel in order to deliver the tapped traffic safely to the remote tools. The tunnel origination feature allows user to define one tunnel per Tool Port, L2GRE or VxLAN, with user configurable KEY or VNI values. Multiple tunnels per Tool Port is also supported.
Packet trimming 	Many monitoring tools, especially legacy ones, only need to analyze packet headers and/or some portions of packet payload. In other monitoring applications, regulatory compliance requires tools to remove sensitive data from captured network traffic. The Packet Trimming function can remove payload data from the monitored network traffic, which boosts tool performance and keeps sensitive user data secure.
Data masking 	Data masking offers secrecy for MAC address and/or IP address by rewriting the entire MAC or IP with a single byte pattern per user's specification. Data masking on the Dynamic Filter level also allows MAC rewrite (source or/and destination) with 6 bytes of unique values.
Time stamping 	Network operators require high-accuracy timestamps on packets to correlate events with other device logs in low-latency financial data centers and to correlate traffic events across a WAN. PacketStack+ Timestamping replaces Source MAC with a high-accuracy timestamp into every packet at ingress or egress. Timestamping with 48 bits nanosecond representation is supported at either ingress or egress by regular Priority/Intersection Image. Timestamping with 16/32 second/nanosecond format is supported at ingress only by the Finance Image. Timestamp source can come from local, NTP, PTP, or 1PPS+ToD(G.8271) with two independent 1PPS SMA/SMP front inputs for greater accuracy.

Ordering Information

PacketStack+ features are available for Keysight Vision E400S and Vision 400

Part number	Vision E400S
LIC-VE400S-PSPL	Keysight Vision E400S. Fully featured PacketStack Plus features activated on every port. (993-0324)
SUB-VE400S-PSPL	Keysight Vision E400S. One year subscription for fully featured PacketStack Plus features activated on every port. (993-0357)
LIC-VE400S-MASK	Keysight Vision E400S. PacketStack Plus feature for fixed length masking, activated on every port (993-0323)
SUB-VE400S-MASK	Keysight Vision E400S. One year subscription for PacketStack Plus feature for fixed length masking, activated on every port (993-0356)
LIC-VE400S-STRP	Keysight Vision E400S. PacketStack Plus feature for header stripping and tunnel termination, activated on every port (993-0325)
SUB-VE400S-STRP	Keysight Vision E400S. One year subscription for PacketStack Plus feature for generic header stripping, activated on every port (993-0358)
LIC-VE400S-TMSP	Keysight Vision E400S. PacketStack Plus feature for Timestamps PTP/NTP and 1PPS/G.703, activated on every port (993-0326)
SUB-VE400S-TMSP	Keysight Vision E400S. One year subscription for PacketStack Plus feature for Timestamps PTP/NTP and 1PPS/G.703, activated on every port (993-0359)
LIC-VE400S-TUNL	Keysight Vision E400S. PacketStack Plus feature for L2GRE/VxLAN tunnel origination, activated on every port (993-0327)
SUB-VE400S-TUNL	Keysight Vision E400S. One year subscription for PacketStack Plus feature for tunneling, activated on every port (993-0360)
LIC-VE400S-DDUP-E	Keysight Vision E400S. PacketStack Plus feature for packet deduplication, activated on 4 ILB ports. Perpetual license (993-0392)
SUB-VE400S-DDUP-E	Keysight Vision E400S. One year subscription for PacketStack Plus feature for deduplication, activated on 4 ILB ports (993-0394)
LIC-VE400S-DDUP-U	Keysight Vision E400S. PacketStack+ feature for packet deduplication, extend from ILB port support only to full support on all ports (993-0397)
SUB-VE400-DDUP-U	Keysight Vision V400. One year subscription for PacketStack+ feature for packet deduplication, extend from ILB port support only to full support on all ports (993-0394)
LIC-VE400S-TRIM	Keysight Vision E400S. PacketStack Plus feature for packet trimming, activated on every port. Perpetual license (993-0393)
SUB-VE400S-TRIM	Keysight Vision E400S. One year subscription for PacketStack Plus feature for trimming, activated on every port (993-0395)

Part number	Vision 400
LIC-V400-PSPL	Keysight Vision 400. Fully featured PacketStack Plus features activated on every port. (993-0308)
SUB-V400-PSPL	Keysight Vision 400. One year subscription for Fully featured PacketStack Plus feature activated on every port. (993-0355)
LIC-V400-TUNL	Keysight Vision V400. PacketStack Plus feature for L2GRE/VxLAN tunnel origination, activated on every port. Perpetual license (993-0327)
SUB-V400-TUNL	Keysight Vision V400. One year subscription for PacketStack Plus feature for tunneling, activated on every port (993-0431)
LIC-V400-DDUP-E	Keysight Vision V400. PacketStack Plus feature for packet deduplication, activated on 4 ILB ports. Perpetual license (993-0421)
SUB-V400-DDUP-E	Keysight Vision V400. One year subscription for PacketStack Plus feature for deduplication, activated on 4 ILB ports (993-0428)
LIC-V400-DDUP-U	Keysight Vision V400. PacketStack+ feature for packet deduplication, extend from ILB port support only to full support on all ports (993-0422)
SUB-V400-DDUP-U	Keysight Vision V400. One year subscription for PacketStack+ feature for packet deduplication, extend from ILB port support only to full support on all ports (993-0422)
LIC-V400-TRIM	Keysight Vision V400. PacketStack Plus feature for packet trimming, activated on every port. Perpetual license (993-0423)
SUB-V400-TRIM	Keysight Vision V400. One year subscription for PacketStack Plus feature for packet trimming, activated on every port
LIC-V400-STRP	Keysight Vision V400. PacketStack Plus feature for header stripping and tunnel termination, activated on every port. Perpetual license (993-0420)
SUB-V400-STRP	Keysight Vision V400. One year subscription for PacketStack Plus feature for header stripping, activated on every port (993-0427)
LIC-V400-MASK	Keysight Vision V400. PacketStack Plus feature for fixed length masking, activated on every port. Perpetual license. (993-0419)
SUB-V400-MASK	Keysight Vision V400. One year subscription for PacketStack Plus feature for fixed length masking, activated on every port (993-0426)
LIC-V400-TMPS	Keysight Vision V400. PacketStack Plus feature for Timestamps PTP/NTP and 1PPS/G.703, activated on every port. Perpetual license (993-0418)
SUB-V400-TMPS	Keysight Vision V400. One year subscription for PacketStack Plus feature for Timestamps PTP/NTP and 1PPS/G.703, activated on every port (993-0425)

Support

Keysight's Visibility industry-best products are backed by our industry-leading expertise. Our comprehensive product support does more than ensure uptime – it ensures a competitive edge. The Keysight support team partners with customers to:

- Avoid downtime and keep schedules on track
- Implement according to industry specifications
- Develop best practices to meet individual needs and objectives
- Maximize efficiency and reduce operating expenses
- Protect and maximize investments in test and visibility

In addition to above, Keysight customers registering for the secure area and access to the Support Site will also be able to view and download our product Security Advisories.

Access Keysight Visibility Support

About Keysight Visibility

Connect and secure the world with dynamic network intelligence

The need for always-on networks is pervasive, and expectations are high when it comes to keeping them connected and secure. As technologies advance, edge computing, cloud environments, sophisticated security threats, increasing bandwidth requirements, and demanding compliance regulations make it challenging to extract actionable insight from your network.

Keysight can help. Customers rely on our solutions to deliver rich data about network traffic, applications, and users across any networking environment. This deep insight is what we call dynamic network intelligence. It helps you continuously innovate, meet aggressive service level agreements, and keep applications running smoothly and securely.

Learn more about Keysight Visibility Solutions

Keysight enables innovators to push the boundaries of engineering by quickly solving design, emulation, and test challenges to create the best product experiences. Start your innovation journey at www.keysight.com.

KEYSIGHT

This information is subject to change without notice. © Keysight Technologies, 2020 – 2024, Published in USA, May 17, 2024, 3120-1039.EN