NIAGARA NETWORKS

Packetron

Your path to an Intelligent Visibility Layer

NI

Network Intelligence

Niagara Networks has recognized that the increase in data speed and the increase in sophistication required from network tools and applications is creating an expanding gap in the effective processing of the network tool’s performance.

To meet this challenge the network visibility layer and the security visibility layer need to provide network intelligence. Niagara's Network Intelligence will efficiently offload processing tasks from the network appliances to the visibility layer and introduce new speciality capabilities in decryption and threat detection not commonly associated with the visibility layer.

Niagra's Network Intelligence is fulfilled by the Packetron. The Packetron - a packet acceleration module - is designed to meet these challenges. The Packetron's packet processor module is based on x86 architecture and can be optionally offered in the N2 modular packet broker series.

NPB ⟷ Packetron combo power multiplier

Combining the Packetron with the NPB provides a power multiplier, achieving a more powerful solution than each one of the solutions independently.

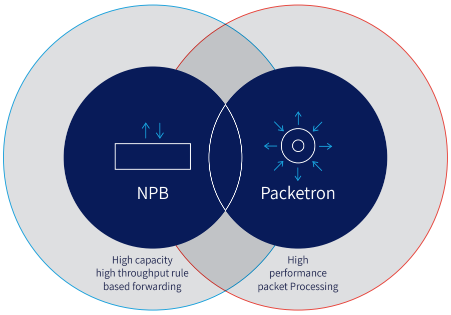
NPB
Packetron
High capacity high throughput rule based forwarding
High performance packet Processing

Figure 1 - NPB<-->Packetron combo. Combining Packet broker functionality with Application layer agility

Packetron offers a wide selection of Network Intelligence applications, combining both in-house applications developed on top of the Niagara Packetron Architecture with the applications that are part of the Open Packetron Partnership. Open Packetron enables the user to load and run best-of-breed 3rd party partner applications on the Packetron. The user can select which applications will be loaded on each Packetron hardware module to meet their deployment needs.

The NPB ⟷ Packetron combo also reduces opex and total cost of ownership. Without the Packetron the user would potentially need to deploy multiple boxes with the additional wiring and maintenance complexity and increased vulnerability. Moreover the Packetron facilitates pay-as-you-grow deployment scenarios and investment protection. Dedicated software applications with advanced capabilities in cyber security or monitoring, performance and troubleshooting can added dynamically added as you need them.

With Packetron, Niagara Networks continues its excellence in expanding the network visibility layer. With the Packetron, users can truly get the right traffic to the right tool. With the power of the Packetron your network visibility layer will be able to handle TLS decryption, Deduplication and more.

The Packetron Difference

Packet acceleration in a single bay module

- Xeon D1577 - 16 cores.
- 32GByte RAM (up to 64GByte optional).
- 32GByte SSD (up to 1TByte optional).

Scalable Performance

- Up to 4 Packetron modules can be deployed with the N2 2847 for 320Gbps processing
- Up to 2 Packetron modules in the 2845 for 160Gbps

De-coupled software architecture

- Upload new software to the Packetron without impacting the host NPB software.

Open Packetron Partnership

- Supports 'open garden' application architecture where
- 3rd party partners can deploy and offer their applications

Intuitive Configuration

- Apply available Packetron applications in a hassle-free intuitive user interface on any selected flow.
- All Packetron applications are seamlessly integrated with Niagara’s FabricFlow technology that provides intent-based method of defining traffic flow relationships between source and destination ports.

Applications running on the Packetron automatically and seamlessly benefit from aggregation, replication, filter, load balance, inline bypass and other traffic manipulation capabilities of a fully featured NPB. By connecting to the non-blocking switching core, traffic from any port and to any port can be easily accomplished.

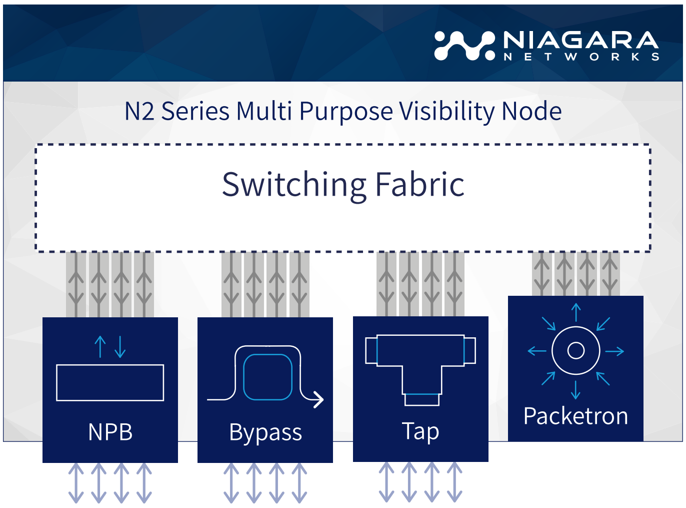

Figure 2 - The Packetron module occupies a single bay in the N2 series modular multi purpose packet brokers. This provides superior packet processing density per form factor. Input traffic from packet broker ports, bypass ports or tap ports via the nonblocking switching fabric, enables the Packetron to provide Network Intelligence application for both out-of-band monitoring deployments and for inline deployments.

A Network Packet Broker is powered by a switching fabric that is able to deliver great processing and forwarding capabilities on packets, up to Layer 4. The Packetron module is directly connected to the host packet broker switching fabric. The Packetron is able to handle sophisticated application level and L7 level processing on packets, sessions and flows.

The Packetron has a nominal processing capacity of 80GbE. Though actual performance may vary based on the application and or number of applications that are run simultaneously on a single Packetron module. As a modular, field replaceable module, users can add Packetron modules to satisfy their processing needs.

Niagara Packetron Architecture Applications

As part of the Niagara Packetron Architecture we offer the following Network Intelligence applications:

- Packet Slicing
- NetFlow/IPFIX and metadata
- Deduplication

The Niagara Packetron Architecture offers important common to all if its applications:

Profiles - users can define multiple profiles of application configurations. These profiles can then be selectively applied as part of the FabricFlow on to different traffic flows. The same Profile can be applied to multiple flows, or different NetFlow profiles can each be applied based on deployment needs, to different traffic flows.

Passthrough - passthrough mode is a uniques user configurable option where the Niagara Packetron Architecture is able to dynamically detect levels of congestion and forward packets through the Packetron rather than process the packet and potentially have it dropped because of resource constraints. This may be especially important where the user's priority is to minimize the risk of dropping packets at a tradeoff of certain application processing.

Optimal Core Efficiency - when operating in a multicore multi-GbE port environment, the number of cores allocated for data traffic processing needs to be optimized. The Niagara Packetron Architecture is able to dynamically load balance incoming traffic so that traffic throughput processing will be maximized and optimized. This is done 'behind the scene' without burdening the user with fixed manual configurations and compromised performance. Moreover, in specific applications significant performance improvement can be achieved by parallel processing and reassignment of cores. For those applications we offer 'dedicated-mode' that is user selectable based on their deployment needs.

Packet Slicing

Packet Slicing reduces the volume of data to be forwarded for analysis and processing by a network appliance by reducing the packet length. This is especially useful for network applications that only require header analysis and or a defined set of bytes from each packet. Packet length is reduced based on user configurable rules.

Relative offset - users can define the number of bytes from which slicing will take place relative to a Layer2 or Layer3 header.

Fixed offset - users can define the number of bytes from which slicing will take place from the beginning of the packet.

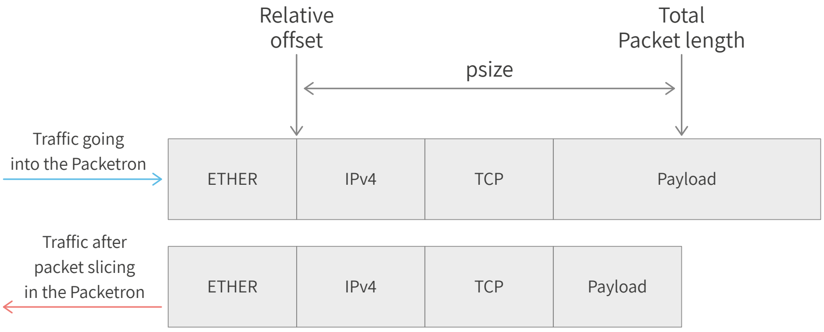
Relative offset
Total Packet length
psize
Traffic going into the Packetron
ETHER
IPv4
TCP
Payload
Traffic after packet slicing in the Packetron
ETHER
IPv4
TCP
Payload

Figure 3 depicts the use of packet slicing using relative offset

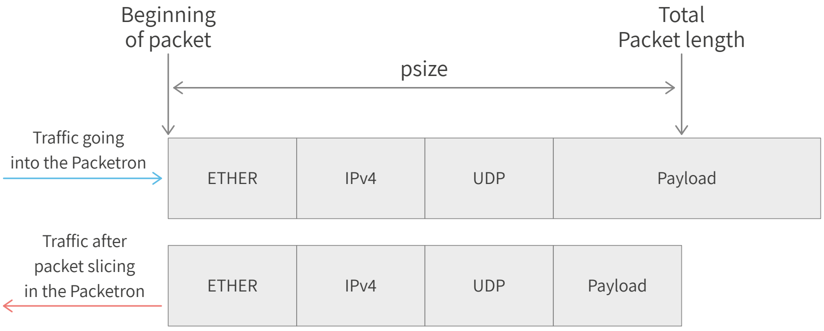

Figure 4 depicts packet slicing using fixed offset

NetFlow/IPFIX and metadata

Traffic metadata reports are used for monitoring and security network appliances and for other network tools that cannot ingest raw traffic data. Often, metadata reports are generated by the network element itself like a switch or a router. However, as metadata generation is not the primary objective of the network device, metadata performance may be degraded in times of congestion. One manner often used by network elements, to address congestion is by sampling the traffic, instead of taking into account every packet in the flow.

With Niagara Networks, NetFlow/IPFIX and metadata offer the following advantages:

- Compliant with RFC 3954, RFC 5101, RFC 5102, RFC 5153, RFC 7011, RFC 7012 and other IETF recommendations.
- Supports Netflow version 5 and 9 and IPFIX (v10).
- Supports unsampled 1:1 generation on every packet, or user configured 1:N sampling.

The following metadata report attributes are supported:

destinationIPv4Address	flowStartSysUpTime	icmpTypeCodeIPv6	maximumIpTotalLength	selectorAlgorithm
destinationIPv6Address	flowStartMicroseconds	ingressInterface	maximumTTL	sourceIPv4Address
destinationMacAddress	flowStartMilliseconds	ipClassOfService	meteringProcessId	sourceIPv6Address
destinationTransportPort	flowStartNanoseconds	ipDiffServCodePoint	minimumLayer2TotalLength	sourceMacAddress
dot1qCustomerVlanId	flowStartSeconds	ipHeaderLength	minimumIpTotalLength	sourceTransportPort
dot1qVlanId	httpContentType	ipPayloadLength	minimumTTL	systemInitTimeMilliseconds
egressInterface	httpMessageVersion	ipPrecedence	nextHeaderIPv6	tcpAcknowledgementNumber
flowEndMicroseconds	httpReasonPhrase	ipTTL	octetDeltaCount	tcpControlBits
flowEndMilliseconds	httpRequestHost	ipVersion	packetDeltaCount	tcpHeaderLength
flowEndNanoseconds	httpRequestMethod	layer2FrameDeltaCount	payloadLengthIPv6	tcpSequenceNumber
flowEndReason	httpRequestTarget	layer2FrameTotalCount	postIpClassOfService	tcpUrgentPointer
flowEndSeconds	httpStatusCode	layer2OctetDeltaSumOfSquares	protocolIdentifier	tcpWindowSize
flowEndSysUpTime	httpUserAgent	layer2OctetTotalSumOfSquares	samplingPacketInterval	vlanId
flowLabelIPv6	icmpTypeCodeIPv4	maximumLayer2TotalLength	samplingPacketSpace	udpMessageLength

Additional metadata attributes and customized report templates can be added

Deduplication

Deduplication is intended to identify and remove duplicate packets from being sent to a network appliance. While duplicate packets may occur on the network from backup and failovers, the more common occurrence is with the use of SPAN ports that are feeding to a network appliance. When a network appliance handles duplicate packets, the duplicate packets consume the tools limited processing resources, and may affect the accuracy and results reported. On the other hand having to network appliance handle deduplication on its own, may reduce its performance by as much as 30% or more.

Packet Deduplication

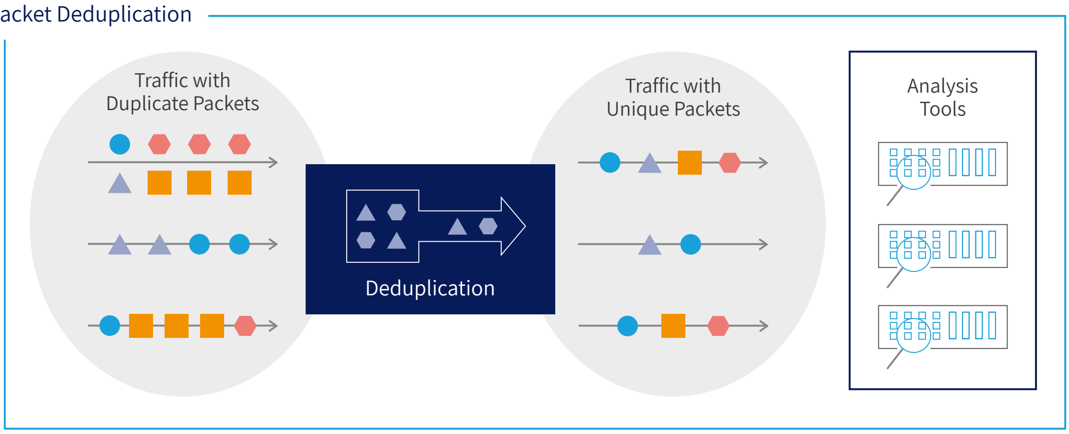

Figure 5 depicts the function of deduplication. Effective deduplication is impacted by user configurable window size, the ability to perform full packet comparison and the ability to refine the packets based on header attributes

Packetron offers the following Deduplication advantages:

Full packet comparison - our deduplication engine performs full packet comparison on every packet within the window selected by the user, versus only header comparison that leads to many false positive hits (i.e the removal of packets that were misidentified as duplicates while they were not really duplicate packets)

Customizable Window size - user can select the desired window size in which duplicate packets will be examined

Header Attribute Elimination - the user can select header attributes that will be included in assessing if two packets are duplicates. If for example, packets may be duplicates even though they have different destination IP address, by selecting the attribute of DST IP Address - it will be excluded from the algorithm determining duplicate packets. And the users deployment objective will be met.

Stats Mode - in some cases user may prefer to first assess how duplicate are in his setup without removing them. In this mode duplicates are only counted, but not removed. Of course full and detailed statistics are provided and deduplicated packets when that mode is active

Dedicated Mode - to boost performance, the user can select to operate in Dedicated Mode. In Dedicated mode, only dedup will be available on the selected Packeron hardware. With Dedicated Mode deduplication of up traffic up to 50GbE can be achieved.

Part Number	Description
N2-SG-PKTRN-A-S	Packetron module hardware. Single bay module. 32GB RAM, 32GB SSD. Includes Packet Slicing software licensing
N2-LC-PKTRN-PCKSL	Slices packet payload based on user selected configuration. Included with Packetron module hardware
N2-LC-PKTRN-DDUP	Removes duplicate packets. License required per each Packetron hardware module. Packetron module hardware sold separately
N2-LC-PKTRN-NETFL	Generates Netflow report to Collectors. License required per each Packetron hardware module. Packetron module hardware sold separately

About Niagara Networks

Niagara Networks provides high performance network visibility solutions for seamless administration of security solutions, performance management and network monitoring. Niagara Networks products provide advantages in terms of network operation expenses, downtime, and total cost of ownership.

A former division of Interface Masters, Niagara Networks provides all the building blocks for an advanced Visibility Adaptation Layer at all data rates up to 100Gb, including Taps, bypass elements, packet brokers and a unified management layer. Thanks to its integrated in-house capabilities and tailor-made development cycle, Niagara Networks are agile in responding to market trends and in meeting the customized needs of service providers, enterprise, data centers, and government agencies.