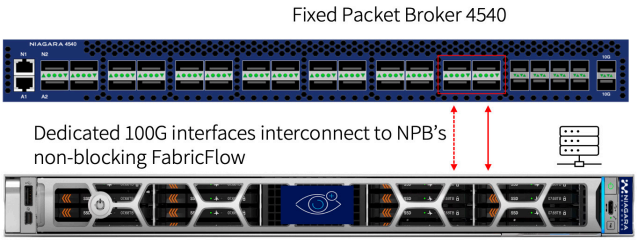
Your path to an Intelligent Visibility Layer

Niagara Networks has recognized that the exponential growth in data rates and the increasing sophistication required from network monitoring and security tools have created a widening gap in effective processing capacity. To address this challenge, the visibility layer must evolve into an intelligent processing layer capable of offloading computationally intensive tasks from network appliances.

The ePacketron Acceleration Appliance Series powers Niagara Networks' advanced packet broker architecture with deep packet intelligence spanning from the network to the application layer. It enables data inspection and manipulation, traffic optimization, and precise packet data intelligence delivery for NOC and SOC environments - streamlining complex packet operations, ensuring scalable network visibility, and empowering NetSecOps teams to route the right traffic to the right tools.

Niagara's Network Intelligence achieves this through the ePacketron solution - an external packet processing appliance that extends the capabilities of Niagara's packet brokers. The ePacketron operates on off-the-shelf hardware and connects via 100G interfaces to the Niagara Packet Brokers. It performs advanced visibility and traffic optimization functions such as deduplication, packet slicing, NetFlow/IPFIX generation, application filtering, header stripping, data masking, regular expression–based filtering, flow slicing, and subscriber-aware visibility.



NPB <--> ePacketron combo.
Extending packet broker performance with advanced processing intelligence and application-layer agility.

Through this architecture, Niagara's Network Intelligence efficiently offloads heavy packet processing from security and monitoring tools to the visibility layer - delivering scalability, flexibility, and enhanced performance across high-bandwidth environments.

NPB + ePacketron Power Multiplier

Combining Niagara's Network Packet Broker (NPB) with the ePacketron Acceleration Appliance creates a true power multiplier- delivering a more capable and intelligent visibility solution than either component alone. The ePacketron introduces a wide selection of Network Intelligence applications, enabling NetSecOps teams to dynamically select and deploy the specific functions required per hardware module to meet their operational and architectural needs.

The NPB ePacketron synergy not only enhances performance but also reduces operational expenditure (OPEX) and total cost of ownership. The ePacketron's flexible, pay-as-you-grow model ensures investment protection and scalability as traffic demands evolve. With the ePacketron's processing power, the network visibility layer gains the ability to handle deduplication, advanced header stripping, and filtering across a broad range of encapsulations and tunneling protocols - including ERSPAN, FabricPath, GENEVE, GRE, NVGRE, VXLAN, VLAN, VN-Tag, PPPoE, GTP, MPLS (GRE/IP/L2/UDP), and many more - empowering precise, application-aware visibility and streamlined NetSecOps operations.

The ePacketron Value Proposition

Enable Ultra Packet Intelligence for NetSecOps

- Wide range of network intelligence applications
- Enhanced packet manipulation for complete visibility up to L7
- Precise packet data delivery for NOC / SOC environments

Scalable Performance

- High-performance packet acceleration in a compact 1RU form factor
- 6 x 100Gb interfaces - up to 600Gbps processing performance
- Fully compatible with fixed Niagara NPB models

De-coupled software architecture

- Upload or update ePacketron software without affecting the host NPB firmware
- Supports multiple instances and third-party applications under VMware hypervisor

Intuitive Configuration

- Apply ePacketron applications to any selected flow via an intuitive, web-based interface
- ePacketron applications are seamlessly integrated with Niagara's intent based FabricFlow™ technology

ePacketron Integration and Processing Architecture

Applications running on the ePacketron automatically and seamlessly benefit from the aggregation, replication, filtering, load balancing, and other traffic manipulation capabilities of a fully featured Network Packet Broker (NPB).

By connecting the ePacketron hardware model directly to the NPB's non-blocking switching fabric, traffic from any ingress port to any egress port can leverage ePacketron's advanced packet intelligence applications.

A Network Packet Broker is powered by a high-performance switching fabric designed to process and forward packets up to Layer 4. The ePacketron appliance, connected through dedicated high-speed interfaces on the packet broker, extends this capability to Layer 7, enabling sophisticated application-level processing across packets, sessions, and flows.

As part of the Niagara 55xx Series, the ePacketron offers multiple processing capacity options. Actual performance depends on the selected hardware configuration, CPU cores, and the number or type of applications running simultaneously.

With its modular, field-replaceable design, users can easily scale and select the optimal processing configuration to meet their specific visibility and application needs.

Niagara's ePacketron Architecture Advantages

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, or different profiles can be applied, based on deployment needs, to the same traffic flow.

Passthrough

Passthrough mode is a unique user configurable option where the Niagara ePacketron Architecture is able to dynamically detect levels of congestion and forward packets through the ePacketron 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.

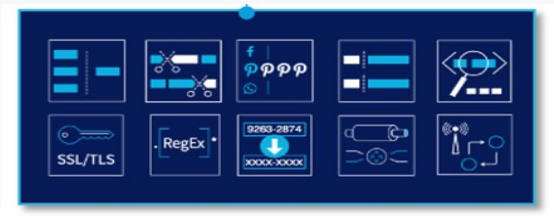
Optimal Core Efficiency

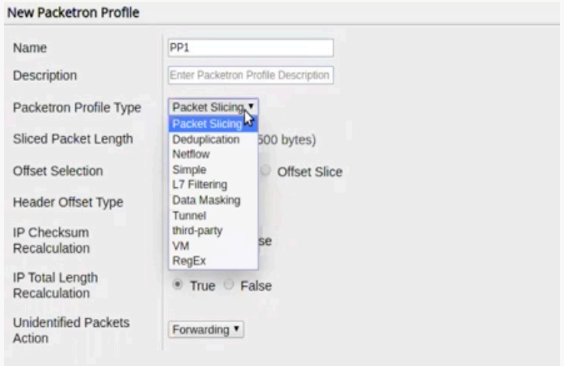
When running multiple packet processing functions and applications on a ePacketron, the number of cores allocated for data traffic processing needs to be optimized.

The Niagara ePacketron 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 cumbersome 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 'stand-alone' modes that are user selectable based on their deployment needs.

Deployment Hub

Use thePacketron as a deployment hub for multiple Network Intelligence (NI) utility processing applications. Network Intelligence Applications will be applied at a user defined logical sequence on the data traffic. Applying Network Intelligence applications in sequence on the data traffic is intuitive and does not require additional complex manual configurations.





Network Intelligence Functions Enabled by the Packetron Acceleration Solution

Niagara's ePacketron-powered architecture transforms the visibility layer into a true Network Intelligence platform. Each application listed below is seamlessly deployable through the ePacketron Acceleration Solution, extending the traditional Packet Broker's capabilities beyond traffic distribution into application-level and subscriber-aware visibility.

Function / Application	Description	Operational Benefit	Enabled Use Case
Packet Deduplication	Removes duplicate packets before forwarding to tools.	Reduces tool overload and eliminates redundant data for higher tool efficiency.	Network forensics, NDR/IDS optimization, compliance logging, and storage reduction.
Packet Slicing	Truncates packets to retain only headers or metadata as needed.	Saves bandwidth and processing power while preserving analytical context.	Compliance monitoring, metadata-based analytics, and encrypted traffic inspection.
Flow Slicing	Captures only the first few packets of each flow while discarding the rest.	Maintains session context while minimizing data volume.	Threat hunting, behavioral analytics, anomaly detection, and application performance monitoring.
Header Stripping	Removes multiple encapsulation or tunneling headers (GRE, VXLAN, GTP, MPLS, ERSPAN, PPPoE, NVGRE, etc.).	Simplifies analysis for downstream L2–L7 tools by exposing original payloads.	Multi-tenant cloud visibility, mobile core monitoring, SD-WAN and service chaining analysis, encapsulated traffic analytics, and virtualized network functions visibility.
Application Filtering	Filters traffic by application or protocol type.	Enables focused monitoring and analysis for specific applications.	SOC/NOC segmentation, compliance-driven traffic isolation, and targeted tool feeds..
Regular Expression Filtering	Filters or masks packets based on defined regex patterns or payload content.	Provides deep inspection flexibility and customizable policy control.	Data loss prevention (DLP), content inspection, and regulatory compliance enforcement.
Data Masking	Masks sensitive data (e.g., PII, credentials) within packet payloads.	Ensures privacy and compliance with data protection standards.	SOC/NOC operations under GDPR/CCPA, financial transaction monitoring, healthcare data inspection.
NetFlow / IPFIX Generation	Generates flow metadata (NetFlow v9, IPFIX) from raw packet traffic.	Enables scalable flow analytics and long-term performance visibility.	Capacity planning, anomaly detection, and traffic profiling for enterprise or carrier NOC/SOC.
Subscriber-Aware Visibility	Correlates GTP sessions for full subscriber-level flow visibility and filtering.	Enables 3G/4G/5G mobile subscriber-aware analytics and selective traffic steering.	Mobile core SOC/NOC, carrier-grade visibility, and 5G edge security monitoring.
Protocol Reporting*	Identifies and reports traffic composition by protocol and usage volume.	Delivers network-wide visibility into traffic distribution and utilization.	Network capacity management, SLA monitoring, and performance baselining.
Packet Capture*	Records selected packets for in-depth offline analysis.	Enables retrospective investigation and forensic reconstruction.	Incident response, law enforcement, troubleshooting, and post-breach analysis.

* Future software release

Part Number	ePacketron - system licenses
P-BASE-LC	ePacketron base license to use one physical server as an ePacketron host. This license must be paired with an EP-VSYS license and one or multiple EP-PORT licenses. Multiple EP-VSYS licenses can be installed to deploy additional ePacketron instances on a single ePacketron server
EP-VSYS-LC-100	ePacketron virtual appliance license for use with 100Gbps data ports. License must pair with one EP-BASE license and one or multiple EP-Port-100 license(s).
EP-PORT-LC-100	ePacketron license to compliment the EP-VSYS license with 2x 100G ports (speed enforced). All ports in a VSYS must have the same speed. Up to four licenses can be installed for a full 8 x 100G deployment

Part Number	Network Intelligence Applications - Feature Licenses
KTRN-LC-PSL-100	Packet Slicing, Removes user defined payload part of a packet. Perpetual ePacketron instance license enabling 33 PB/month of Packet slicing. Multiple licenses can be applied to a single ePacketron instance, ePacketron server and system licenses are not included.
EPKTRN-LC-DDUP-100	Deduplication, Removes duplicate packets from a data flow. Perpetual ePacketron instance license enabling packet deduplication of 33 PB per month. Multiple licenses can be applied to a single ePacketron instance, ePacketron server and system licenses are not included.
EPKTRN-LC-NETFL-100	Netflow generation. Perpetual ePacketron instance license enabling netflow generating for 33 PB of data per month. Multiple licenses can be applied to a single ePacketron instance, ePacketron server and system licenses are not included.
EPKTRN-LC-APPFLT-100	Application Filtering. Enables advanced applications traffic filtering. Filtered applications can be applied for monitoring and inline deployments. Perpetual ePacketron instance license enabling application filtering for 33 PB of data per month. Multiple licenses can be applied to a single ePacketron instance, ePacketron server and system licenses are not included.
EPKTRN-LC-RXS-100	Regular expression search. Expansion for filtering and data masking capabilities. Define any pattern through a regular expression and perform advanced packet filtering, advanced masking and advanced session filtering. Perpetual ePacketron instance license enabling regular expression search for 33 PB of data per month. Multiple licenses can be applied to a single ePacketron instance, ePacketron server and system licenses are not included.
EPKTRN-LC-HSTP-100	Generic header stripping. Remove multiple tunnel headers from the ethernet packet. Perpetual ePacketron instance license enabling header stripping for 33 PB of data per month. Multiple licenses can be applied to a single ePacketron instance, ePacketron server and system licenses are not included.
EPKTRN-LC-FSL-100	Flow Slicing, forward a user defined amount of packets after which subsequent packets of the same flow are discarded. Perpetual ePacketron instance license enabling flow slicing for 33 PB of data per month. Multiple licenses can be applied to a single ePacketron instance, ePacketron server and system licenses are not included.

Part Number	Network Intelligence Applications - Feature Licenses
EPKTRN-LC-DMASK-100	Data masking of specified byte(s) length in the packet. Multiple masks supported. Perpetual ePacketron instance license enabling data masking for 33 PB of data per month. Multiple licenses can be applied to a single ePacketron instance, ePacketron server and system licenses are not included.
EPKTRN-LC-PCAP-100*	Packet capture, Capture packets from the network for traffic analysis. Perpetual ePacketron instance license enabling packet capture for 33 PB of data per month. Multiple licenses can be applied to a single ePacketron instance, ePacketron server and system licenses are not included.
EPKTRN-LC-PRPT-100*	Protocol Reporting, report on the protocols and their traffic amounts for the analyzed traffic flow. Perpetual ePacketron instance license enabling protocol reporting for 33 PB of data per month. Multiple licences can be applied to a single ePacketron instance, ePacketron server and system licenses are not included.
EPKTRN-LC-MS4GTP-100	Mobile Subscriber-aware Visibility. Correlated filtering and load balancing. Uncorrelated load balancing. Perpetual ePacketron instance license enabling 3G, 4G and 5G NSA correlation and filtering for 33 PB of data per month. Multiple licenses can be applied to a single ePacketron instance, ePacketron server and system licenses are not included.
*Notes: * future software release*	

About Niagara Networks

Niagara Networks is a Silicon Valley-based company delivering high-performance, reliable network visibility and traffic delivery solutions for mission-critical environments. Our solutions empower Security and Network Operations Centers (SOC/NOC) with complete visibility and actionable intelligence across physical, virtual, and cloud networks. As a former division of Interface Masters, we provide all the building blocks for an advanced Visibility Layer, including packet brokers, bypass switches, network TAPs, and unified management software, offering a single pane of glass for simplified visibility infrastructure.

For more information please visit us at www.niagaranetworks.com

NIAGARA NETWORKS

48430 Lakeview Blvd,
Fremont, CA 94538, USA

www.niagaranetworks.com
info@niagaranetworks.com

Tel: +1 408 622 0354
Fax: +1 408 213 7529