NIAGARA NETWORKS

Packetron – Enabling Network Intelligence from Layer 4–7

Network Intelligence Functions Powered by the Packetron Acceleration Solution

Niagara's Packetron-powered architecture elevates the visibility layer into a true Network Intelligence Platform. Each function listed below is seamlessly deployable through the Packetron Acceleration Solution, extending the traditional Packet Broker's role beyond traffic distribution - into application-level, subscriber-aware, and content-aware visibility.

Function / Application	Description	Operational Benefit	Enabled Use Case
Packet Deduplication	Removes duplicate packets before forwarding to tools.	Reduces tool overload & 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 & 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, NVGRE, GENEVE 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 NFV 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 (NSA) mobile subscriber-aware analytics & selective traffic steering.	Mobile core SOC/NOC, carrier-grade visibility, and 5G edge security monitoring.

** future release*