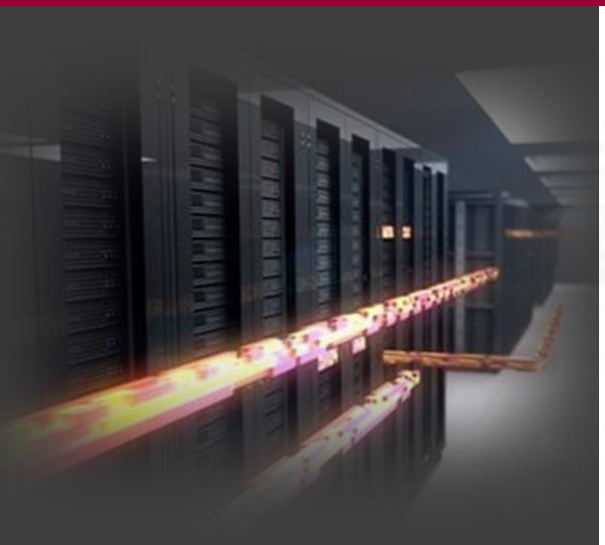
Joint Solution Brief



Improving Network Intelligence with Intelligent Traffic Aggregation and Optimization

Highlights

- Efficiently monitor massive volumes of network traffic for improved network visibility at scale
- Terabytes of aggregation and scalable packet-flow traffic optimization to reduce unwanted and unmonitorable traffic to optimize monitoring efficiency
- Maximize security and monitoring tool performance for more efficient traffic processing
- Extend monitoring and security tool life and defer future upgrades
- Intelligently reduce packet capture volume to speed forensic analysis, reduce storage requirements and increase packet retention times
- Achieve optimized visibility into encrypted traffic without expensive decryption
- Optimize packet-flow backhaul traffic to increase transport capacity and reduce WAN costs

The Problem

As network traffic grows exponentially and 100G and higher network speeds proliferate, security and monitoring tools are overwhelmed and continually challenged by the massive amount of traffic to monitor. This unrelenting data explosion forces the security and network operations teams to add incremental monitoring, analytics, and packet storage capacity just to keep up. This is not only excessively expensive, but in many cases futile, as an increasing amount of network traffic being delivered to upstream tools is unwanted and has low analytics value.

Consequently, the days of collecting 'everything' and letting the analytics layer 'sort it out' are no longer viable. To keep up with critical network traffic intelligence, the security and network operations teams still need to collect everything, but now must intelligently identify and deliver only relevant and monitorable traffic to the upstream tools to streamline analysis and optimize historical storage resources.

Optimizing network traffic not only reduces unwanted packets from reaching the analysis and storage layers. It enables organizations to extend the useable life of existing lower speed 10G and 40G tools and delay the need to upgrade the monitoring infrastructure to support 100G links and the ever-growing network traffic volumes. In addition, for organizations with multi-site monitoring infrastructures, traffic optimization is an essential requirement to reduce the volume of packets to be backhauled to centralized collection points to lower WAN bandwidth requirements and better control transport costs.

The Joint Solution

The network packet broker (NPB) has become an essential and ubiquitous tool for both network and security operations teams to achieve pervasive visibility into everything flowing across the network. By combining the Garland Technology PacketMAX™ Network Packet Brokers with the NetQuest Packet Services Broker™ as an Intelligent Service Node™, SecOps and NetOps teams can create an Intelligent Aggregation Layer™ that more efficiently collects, aggregates, and optimizes network traffic based upon granular user-definable policies for delivery to upstream tools and packet storage platforms.

Joint Solution Brief

The Intelligent Aggregation Layer off-loads the burden of prioritizing traffic for analysis and storage at the lower cost traffic collection layer by automating the identification and delivery of only relevant packets for analysis and forensic activities. This enables organizations to improve the value and integrity of monitored network traffic to maximize security and network visibility. This, in turn, extends the deployment life of existing tools, thereby delaying the need to add additional resources and storage capacity.

Together the joint Garland Technology and NetQuest Intelligent Aggregation Layer empowers organizations to break-through the performance barriers, packet processing limitations and the high costs of smart packet broker systems. By combining cost-effective Garland PacketMAX platforms with NetQuest ultra-scale packet processing, the combined solution delivers higher capacity with more optimization services at a lower cost than comparable products from alternative vendors.

Garland Technology PacketMAX Family

Garland Technology ensures complete 360-degree network visibility with a comprehensive family of network access solutions. Enabling complete network visibility, Garland's TAP-to-Tool™ architecture includes purpose-built Network Packet Brokers, Advanced Traffic Aggregators, Breakout TAPs, Regeneration TAPs, Advanced All-In-1 Filtering TAPs, Inline Edge Security Bypass TAPs, Hardware Data Diodes and Cloud Access Solutions.

The Garland PacketMAX enables high-scale acquisition of network traffic with wire-speed traffic replication that enables collecting, aggregating, and distributing all network traffic to any monitoring tool, analytics system, or packet storage platform. The Garland PacketMAX platform delivers market-leading performance and scales packet-flow access to significantly lower the cost of network traffic acquisition while optimizing the ability to cost-effectively monitor more links across an increasingly complex network environment.

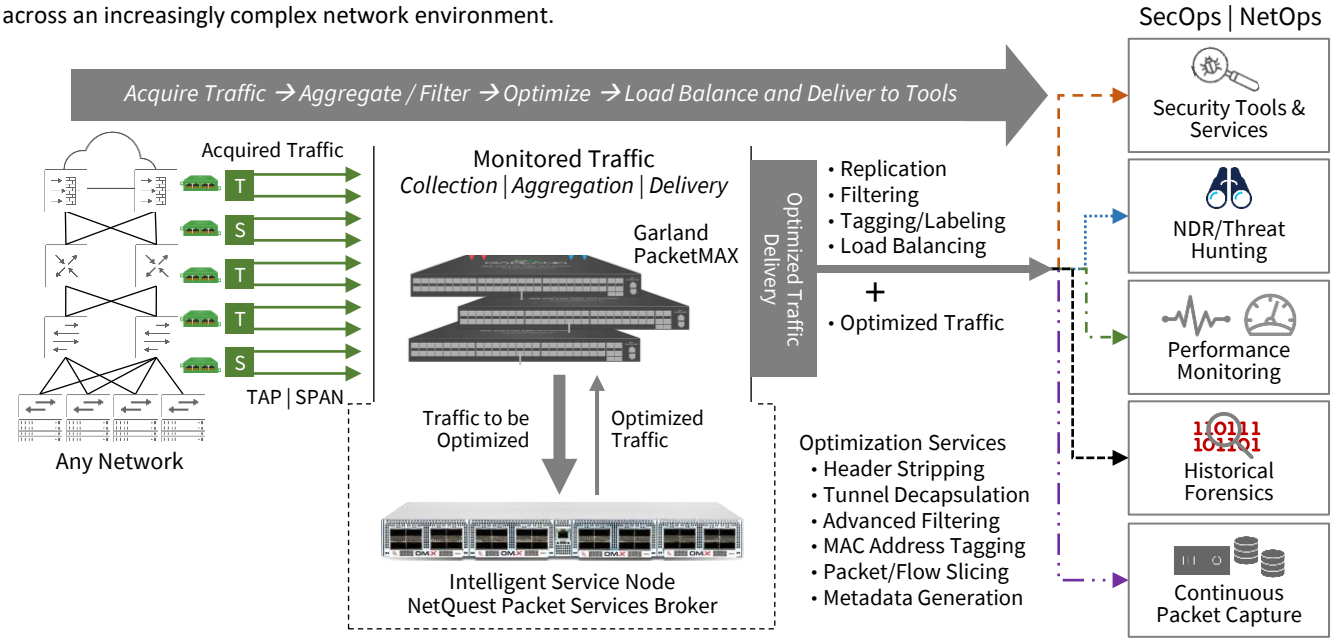
NetQuest Packet Services Broker

The NetQuest Packet Services Broker delivers multi-terabit, wire-speed advanced packet processing services for high-performance network monitoring environments that rely on accurate and reliable network packets. The Packet Services Broker provides the density, performance and packet optimization capabilities needed to inspect and optimize Petabytes of network packets per hour for both clear and encrypted traffic.

Leveraging the NetQuest OMX™ platform's software-defined architecture enables feature flexibility and support for multiple operational modes on common hardware across high-density 10G, 25G, 40G, 100G and 400G ports. The OMX platform's unique distributed pipeline processing architecture allows all packet optimization services to be activated simultaneously at wire-speed, with sustained performance at scale for the most demanding packet processing requirements. The NetQuest Packet Services Broker delivers more than 4x higher density, throughput, and packet processing power per rack unit (RU) than alternative smart packet service brokers at a significantly lower cost with a smaller footprint.

Plug-and-Play Integration

The Packet Services Broker quickly and easily integrates with the Garland PacketMAX to add advanced packet optimization services for any monitoring environment. The Garland PacketMAX collects and aggregates network traffic and, based upon user-defined policies, feeds the targeted traffic to the Packet Services Broker. The Packet Services Broker performs the desired optimization services and returns the conditioned traffic back to the Garland PacketMAX to redistribute packets to the targeted tools. The Packet Services Broker can retain or drop any tagging added by PacketMAX, and if needed, can further tag traffic to identify source port or specific tool destinations.



Intelligent Traffic Optimization

The Packet Services Broker efficiently identifies, prioritizes, and optimizes packet-flow traffic at wire-speed to deliver only relevant packets to reduce the upstream tool processing burden, facilitating faster analysis, and enable more efficient packet recording to reduce storage requirements and extend packet retention time. Depending on the network traffic profile and analysis goals, intelligent packet optimization can eliminate up to 50-80% of unwanted packet-flow traffic. The NetQuest Packet Services Broker optimization services include:

- **Header stripping and protocol de-encapsulation** – Remove headers and tunnels to deliver inner packets
- **Multi-stage adaptive filtering** – enables granular control over traffic to be sent
- **High-Scale Prefix and Port Filtering** - High-scale prioritization of traffic classes and IP address to send or drop
- **Packet slicing** – remove unwanted elements from packets for better tool efficiency or compliance
- **Adaptive flow slicing** – truncate specific flow-types, such as encrypted traffic, to remove payloads that are unmonitorable or undesirable
- **Encrypted traffic optimization** – identify and optimize encrypted traffic without expensive decryption
- **Packet deduplication** – remove duplicate packets collected from different monitoring points
- **Time stamping** – add time stamps to traffic for upstream tools
- **Source labeling** – identify source of optimized traffic, including preserving or removing tags inserted by the PacketMax
- **Flow metadata generation** – High scale 1:1 IPFIX metadata generated from the same optimized traffic

High-Capacity Advanced Filtering

The Packet Services Broker provides high-scale, real-time traffic classification with advanced packet parsing and filtering capabilities for defining precise parameters to identify traffic that is to be discarded or forwarded. Configurable rule-based priorities assure traffic integrity is not compromised, and analysis resources are used efficiently. Advanced Deep Packet Inspection algorithms step-through each packet to analyze and account for all relevant parameters including beyond protocol headers and when packets are encapsulated within transport tunneling protocols. Up to 7 layers of headers and tunnels can be stripped before the traffic is forwarded, enabling tools to receive the desired inner traffic for analysis.

The cornerstone of the NetQuest Packet Services Broker is its high-capacity, real-time traffic policy engine that performs advanced traffic classification and filtering.

High-scale IP prefix lists, with over 1.2 million filters, enable sophisticated precision traffic prioritization for services, IP addresses, and IP CIDRs. This allows sending specific traffic classes or source IP addresses, such as traffic destined for critical services or traffic originating from suspect locations identified by correlated threat intelligence feeds to the tools for analysis.

Encrypted Traffic Optimization

As much as 80% of network traffic is now encrypted, presenting many challenges for monitoring and analysis activities. The Packet Services Broker recognizes encrypted traffic and automates flexible user definable actions to discard or optimize encrypted traffic for upstream tools. Configurable policies allow the Packet Services Broker to drop all traffic classified as encrypted. Alternatively, the Packet Services Broker can identify, and forward only encrypted traffic with specific algorithms, such as SSH, TLS and QUIC, and drop all other encrypted traffic. To support sophisticated threat hunting missions, Adaptive Flow Slicing allows forwarding only packet headers and handshake details and discarding the unmonitorable encrypted payloads.

Encrypted traffic optimizations enables advanced threat hunting and NDR tools to receive important fingerprints, signatures, and heuristics to quickly identify emerging threats and pinpoint indicators of compromise without the need for slow and expensive decryption. Eliminating low-value, unanalyzable encrypted packets significantly reduces traffic volumes and the packet processing burden on analysis tools.

Similar optimizations can be applied to streaming services traffic, such as voice and video. The Packet Services Broker can detect streaming traffic and can forward session set-up and tear-down packets and drop the remaining streaming content packets, or simply drop all streaming content flow packets.

Simultaneous Flow Metadata Generation

When flow metadata is needed, the Packet Services Broker can simultaneously act as a high-scale Network Flow Sensor to generate and deliver 1:1 unsampled IPFIX metadata from the same optimized packet-flow traffic. When activated, metadata is created as the packet traffic is processed and can include standard layer 2/3/4 NetFlow-like metadata or can be enriched with layer 4-7 advanced application, protocol, and encrypted traffic details.

Flow metadata is delivered as a separate IPFIX output stream and can be distributed, and load balanced to up to 16 different flow collectors to support multiple monitoring platforms and use cases. The optional metadata creation capabilities further extends the operational value of the NetQuest Packet Services Broker while reducing the TCO and operational complexities associated with managing multiple probes and sensors.

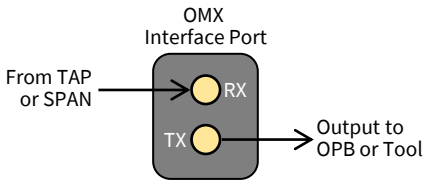
Joint Solution Brief

High-Scale Single-Pass Processing

All Packet Services Broker optimization services are applied in a single pipeline process for each input packet flow – so there is no need for recirculating traffic back and forth when multiple optimization services are needed. This significantly increases throughput and performance and eliminates undesirable packet service latency. Multiple Garland PacketMAX Packet Brokers can be connected directly into the same physical Packet Services Broker system while maintaining the integrity of the source data. The interconnection link speed between the Packet Services Broker and Garland PacketMAX is determined by the peak volume of traffic to be processed – so, a single or multiple 100G link can be used to support high volumes of traffic for multi-service conditioning.

Half-Duplex Ports Double Port Capacity

Depending on the Operational Mode deployed, the Packet Services Broker can receive, process, and return optimized packets on the same physical port – allowing each physical port to be operated as two distinct and separate interfaces. As a result, each physical port is receiving traffic to be optimized on the RX side and is using the TX side to send optimized traffic back to the Garland PacketMAX Packet Broker for redistribution.



This doubles the Packet Services Broker capacity to up to 32x 40/100G input ports (ingress traffic) and 32x 40/100G conditioned traffic output ports (egress traffic) – providing up to 64x 40/100G ports with 6.4 Tbps of aggregate bi-directional wire-speed throughput in a single rack unit (RU).

High-Scale Optical WAN Monitoring

The OMX platform can be leveraged to monitor high-speed optical links and high-density fiber optic cables, such as DWDM, OTN and SONET/SDH, by connecting to the optical fiber pairs. OMX auto-discovers and identifies all traffic traversing the fiber and converts the WAN traffic to IP Ethernet Packets or metadata suitable for traditional monitoring tools – eliminating the need for expensive specialized optical monitoring systems. The WAN traffic, now converted to standards-based IP packets or metadata, can be conditioned in the same manner as native IP packet traffic and delivered to the PacketMAX for distribution to monitoring tools.

The Value Realized

The combined Garland Technology - NetQuest solution integrates two industry-leading technologies to provide organizations with an ultra-high-scale, lower-cost approach enabling the construction of a powerful and flexible Intelligent Aggregation Layer. When compared to other well-known smart packet broker systems, the combined Garland and NetQuest solution delivers significantly higher density with more capacity and functionality and greater performance at scale than alternative solutions in its class to meet the most demanding monitoring requirements.

About Garland Technology

Garland Technology is an industry leader delivering network products and solutions for enterprises, service providers, and government agencies worldwide. Since 2011, Garland Technology has developed the industry's most reliable test access points (TAPs), enabling data centers to address IT challenges and gain complete network visibility. For more information or learn more about the inventor of the first bypass TAP, visit: GarlandTechnology.com or @GarlandTech.

About NetQuest

NetQuest provides market-leading Ethernet and WAN Flow and Packet-Based traffic monitoring solutions that deliver the highest levels of accuracy, capacity, and performance at scale. Monitoring solutions from NetQuest are deployment-proven across thousands of network segments in enterprise, carrier, government, and defense agency networks across the globe, empowering security operations teams with high-scale visibility and actionable traffic intelligence.

NetQuest Corporation
523 Fellowship Road, Suite 205
Mount Laurel, NJ 08054 USA
+1-856-866-0505 | sales@netquestcorp.com
www.netquestcorp.com