OVERVIEW

Scalable Visibilty Fabric

Network Packet Brokers (NPB)

In today's environments with significant investment in security and monitoring tools, understanding and maintaining control of your network is a constant, uphill battle. With the increase in network virtualization, BYOD, and the growing number of security threats, network monitoring is more important than ever. It's well documented that the foundation of any good visibility fabric comes from using Network Test Access Points (TAPs), but then where does all that tapped traffic go?

What is a Network Packet Broker?

Network Packet Brokers (NPBs) are devices that do just what the name suggests, they "broker" incoming network traffic to any number of security, application performance monitoring, or network forensic tools. The need to "broker" packets before they're sent to tools comes from 2 major driving forces:

1. **The throughput of tools is limited.**
2. **Every tool requires a different subset of traffic to maximize performance.**

NPBs are designed to deliver only the traffic of interest required by any specific tool. NPBs achieve this by using a variety of filtering and load balancing options, acting as the man-in-the-middle between TAP/SPAN ports and the tool layer.

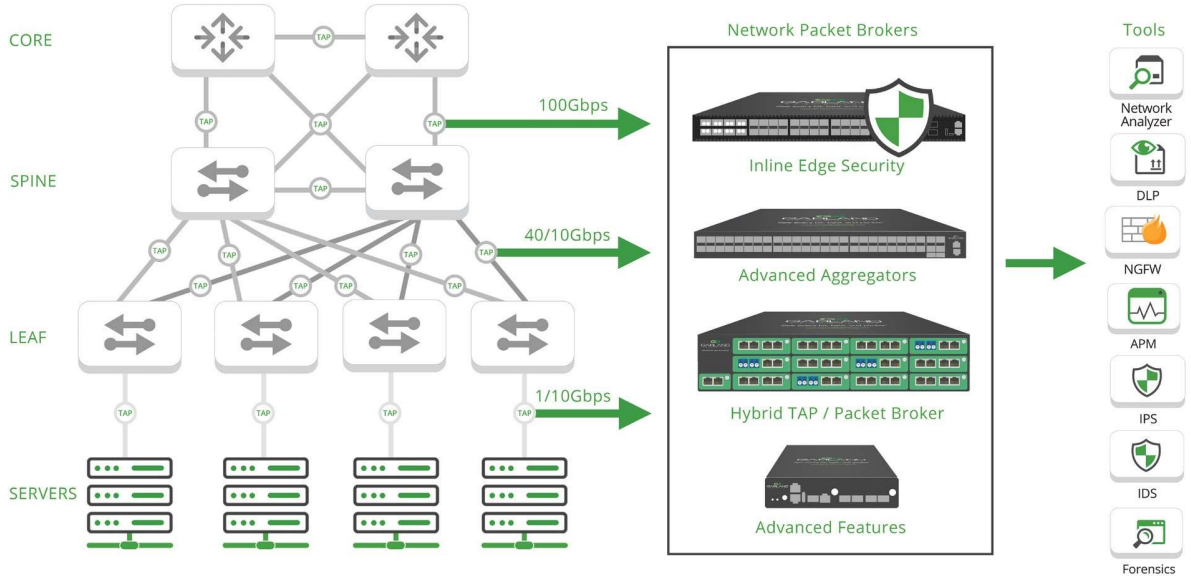


Figure 1: Data center topology with packet broker architecture

Packet Broker Aggregation

Network Packet Brokers are designed to manage TAP aggregation and speed conversion. Intelligent TAP aggregation ensures each tool receives only the data it needs to perform its function, which reduces the processing the tools have to do.

Garland's Advanced Aggregators provide aggregation and load balancing, and are also capable of pre-filtering traffic prior to sending out to NPBs for advanced filtering, or taking the place of packet brokers in applications where only L2-L4 filtering is required.

Network Packet Brokers (NPB)

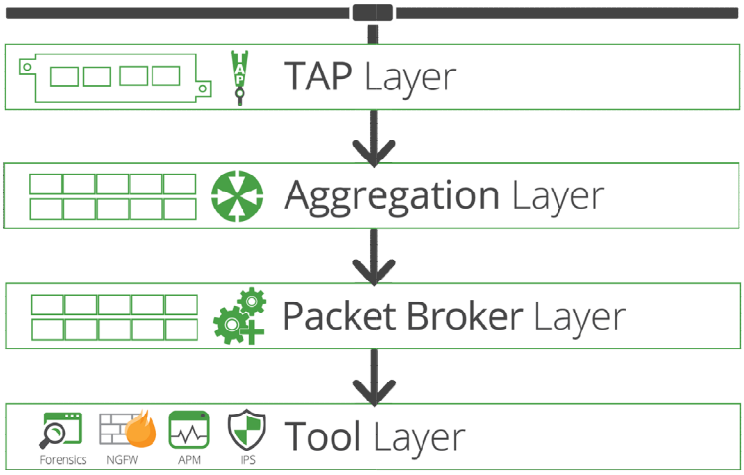
Packet Broker Advanced Features

Full-featured NPBs have functionality that includes filtering, aggregation, load balancing, deduplication, header stripping, GRE / L2GRE Tunnels, and time stamping.

Garland's Advanced Features system provides those advanced features to the Packet Broker layer for both inline and out-of-band applications. The system supports deep window deduplication, NTP time stamping, and configurable packet slicing, which extends the feature set of any product. The Advanced Features system aims at reducing the overall volume of traffic sent to security and monitoring tools, which decreases the possibility of oversubscription, while providing greater reliability and scalability than a full-featured NPB.

Today's Visibility Fabric Layers

With the addition of an aggregation layer, today's 4-tier approach includes the TAP Layer, Aggregation Layer, NPB Layer and the tools. The benefit to this architecture lies with increasing the efficiency of the full-featured NPB, making sure ports at near capacity and fully utilized. Adding an aggregator can free up ports on the packet broker, which either pushes out the time to purchase additional NPBs, or improves ROI by reducing the total cost of licensing fees and processing power leading to better efficiency of existing infrastructure.



Garland recognizes the need for a cost effective solution that allows the flexibility and speed that is required for the networks of the future. Get the advantages of full-featured NPBs at a significantly less cost. We take the approach of providing solutions that are flexible and scalable for future on-demand growth with excellent ROI.

Garland's "deconstructed packet brokers" offer a specialized device for each of your needs:

- **Filtering, aggregation and load balancing**
- **Advanced features like deduplication and time stamping**
- **Hybrid NPB's with TAP integration**
- **Inline Edge Security solutions**
- **Easily reuse and repurpose devices as needs shift**

Have Questions? sales@gch-services.com | +44 (0) 1628 559980 | www.gch-services.com