An Enea White Paper

IMPROVING NETWORK PACKET BROKERS WITH DPI-BASED TRAFFIC CLASSIFICATION

By Erik Larsson, Senior Vice President of Marketing, Enea

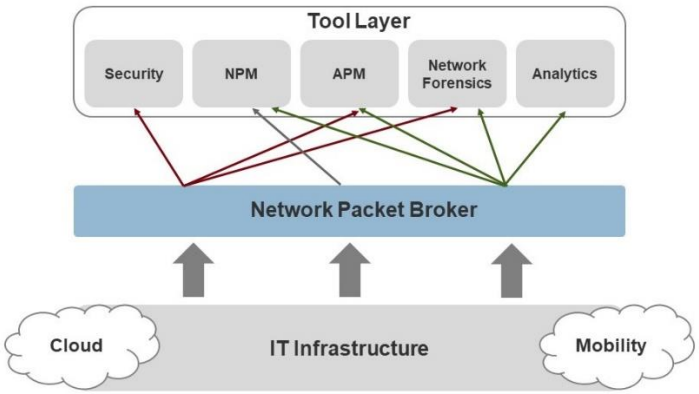
As networks become increasingly complex and virtualized, network packet brokers (NPBs) play a vital, central role by simplifying information distribution to third-party applications.

The integration of precise traffic classification based on Deep Packet Inspection (DPI), can create added value in next generation NPB solutions by increasing efficiency and adding advanced features such as real-time session filtering and traffic de-duplication. These mechanisms optimize the quantity and timing of data sent to external tools and can also be used to expand the range of NPB functions to include security, performance management and analytics capabilities. This new approach allows innovative NPB vendors to gain a competitive advantage and also capture part of the value delivered today by point-solution tools.

The Evolving Role of the Network Packet Broker

> "The advanced capabilities of next-generation NPBs are critical to the success of digital organizations. If an organization wants to move quickly, the limited feature set and manual nature of operations in traditional NPBs will hold the business back. Next-generation NPBs modernize the packet broker and align it with current trends."
>
> *- Zeus Kerravala, Network World* [(1)]

A Network Packet Broker (NPB) sits between a network's infrastructure and its tools, structuring and simplifying exchanges between the two. The aim is to improve network efficiency and increase network security while reducing operational costs.



The latest generation NPBs have strengthened capabilities and strategic value by adding intelligence, which means that a tool only receives the data it needs to perform its function. This significantly reduces the amount of processing the tool has to do, improving system efficiency and performance.

Some NPBs have also developed security-specific capabilities to optimize the effectiveness of security tools through pre-filtering capabilities. The ability to operate out-of-band enables security tools to perform tasks at line rate with no impact on the performance of applications.

NPBs are now playing a key role in simplifying the move to virtual networks and the addition of next-generation tools. This obviously requires vendors to adopt a new approach in the development of their NPBs and to integrate functions able to manage the end-to-end environment.

Raising the Bar

According to MarketsAndMarkets, the network packet broker market is expected to grow by USD 264 million over the next five years, reaching USD 849.4 million in 2023. Growth will be driven by the need for simplified data center management and automation, high demand for cloud services, and a surge in internet multimedia content and web applications.[(2)]

To capitalize on growth opportunities, NPBs must meet enterprise and Communications Service Provider demands for more efficient control of the volume and type of traffic sent to third-party tools and applications, and in particular that they:

- Reduce the amount of off-line traffic
- Eliminate duplication of data processing
- Minimize tool sprawl

In other words, NPBs are now expected to play an active role in controlling and optimizing the flow of data to third-party management and security tools. However, to do this they must also be capable of managing the relentless increase in network traffic, the multiplication and constant evolution of security tools as well as the increasing complexity brought by virtualization and cloud technologies.

New Challenges for NPB Developers

> "The network packet broker market is highly competitive due to the existence of a substantial number of players in the space."
>
> *- Network Packet Broker Market Share 2018-2024 Global Industry Report [(3)]*

To address these expanded requirements and remain competitive, vendors are looking for ways to raise the performance and capabilities of their solutions. One area of particular interest is the integration of application awareness that allows more intelligent data processing. This enables vendors to expand NPB functions to include security, performance management and analytics capabilities. This application-awareness is typically provided by a Deep Packet Inspection (DPI)-based classification engine, coupled with rule engines to deliver flexible traffic filtering.

DPI: A Highly Specialized Technology

Deep Packet Inspection (DPI) technology identifies data traveling over networks in real time, providing a highly detailed picture of traffic up to layer 7 through the identification of protocols and types of application, and the extraction of additional information in the form of metadata.

A DPI engine can be embedded in a NPB appliance or integrated as an external component. Some vendors choose to develop their own proprietary DPI engine while others buy it as a plug-and-play component from an external supplier. It is, however, a highly specialized technology that requires specific expertise and significant resources to develop. Before deciding whether to build or buy, it can be useful to understand some of the challenges associated with DPI engine development:

- Protocol and application coverage: the DPI engine needs to recognize the thousands of protocols and applications that can possibly transit on the network.
- Frequent updates to maintain accuracy and coverage: the DPI engine needs regular maintenance to ensure it recognizes new protocols and applications that emerge almost on a daily basis.
- Metadata processing: the DPI engine must be able to extract metadata but also perform some form of pre-processing to minimize the load on downstream applications such as firewalls, NPM/APM and analytics.
- Classification of encrypted traffic: the DPI engine must be able to classify encrypted traffic without decrypting it, using statistical methods and pattern recognition.
- Support for various line rates: the DPI engine must be able to classify traffic accurately at line rate without dropping any packets.
- CPU and memory consumption: the DPI engine must be able to perform at high speed with minimal impact on CPU and memory, especially if it is to be embedded in an appliance.

Any of these challenges can easily become a rabbit hole for NPB solution developers, delaying product releases and inflating development costs. This is why many vendors choose to source their DPI engine from a specialist supplier. It allows them to reduce the time-to-market for new products and functionalities while raising performance through regular updates and the reliability of tried and tested technology.

Encryption and Virtualization Create Additional Hurdles

Encryption on the public Internet is constantly rising, with current estimates showing that over 80% of web traffic will be encrypted by the end of 2019. In the enterprise space, more than 40% of traffic is currently encrypted due to a major shift towards cloud-based applications. Luckily, encrypted traffic can still be classified with great accuracy by a DPI engine without any decryption. However, this can only be achieved using heuristics and statistical methods based on expert knowledge of various application behaviors.

Virtualization and cloud-based architectures can also have an impact on the effectiveness of a DPI engine. The ability to identify sessions from end-to-end, regardless of the location and nature of physical resources being used, requires specific know-how and techniques and creates additional layers of development.

Qosmos ixEngine – An Example of a DPI Engine for Network Packet Broker Solutions

> "The below features define next-generation NPBs:
>
> - Metadata engine
> - SSL decryption
> - Application session filtering
> - Inline bypass."
>
> *- Zeus Kerravala, Network World* [(1)]

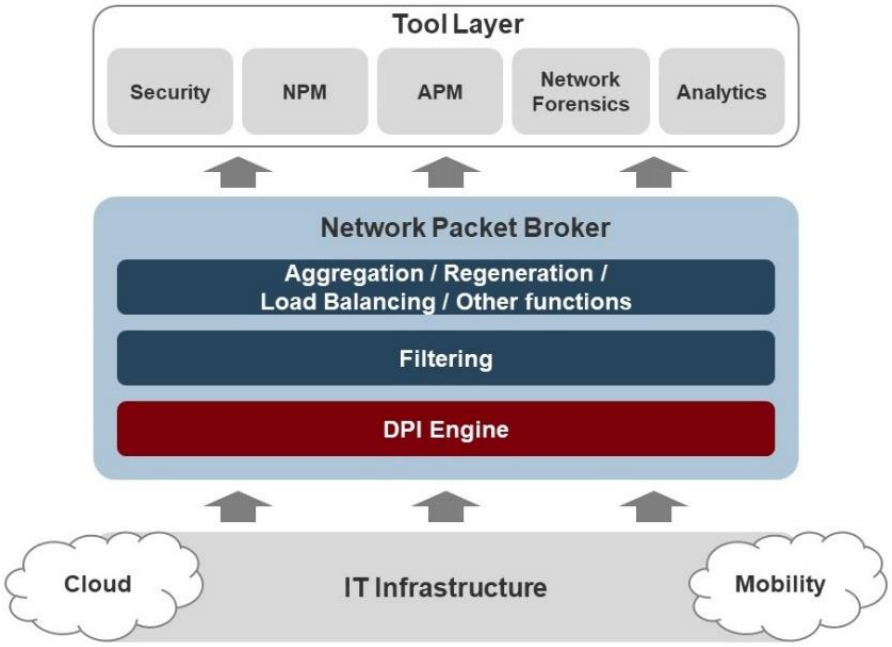
Enea's Qosmsos ixEngine has been specifically developed for software developers who need to integrate DPI into their solution. It is a software library that provides real-time classification and metadata extraction, up to Layer 7, based on application and user information. This information can be used to create integrated real-time filtering mechanisms based on:

- Application
- Session
- Flow
- User/Subscriber
- Device
- Raw or calculated metadata
- Rules-based business logic using any of the above information

By leveraging information from Qosmos ixEngine, NPB vendors can offer sophisticated filtering and other advanced features such as de-duplication to optimize the quantity and timing of data sent to any external tool. Obviously, this information can also be used to expand the range of NPB functions to include security, performance management and analytics capabilities. NPB vendors adopting this approach can gain a competitive advantage against other NPB solutions and also capture part of the value being delivered today by point-solution tools.

Qosmos ixEngine also solves issues related specifically to encryption and virtualization:

- Classifying traffic encrypted with SSL/TLS with 100% accuracy; classifying P2P traffic with 90% accuracy; classifying Skype traffic with up to 95% accuracy.
- Identifying entire sessions, from end-to-end, that use virtualized, physical and hybrid infrastructure.



Adding Value to NPB Solutions

The combination of a powerful classification engine with extension modules such as a rule engine allow NPB developers using Qosmos ixEngine to create traffic filtering logic for more intelligent, more accurate and more efficient classification and routing that improves the effectiveness of downstream applications.

Comprehensive Network Intelligence

Qosmos ixEngine provides the broadest range of protocol and application recognition in the telecom, enterprise and security markets:

- Ability to identify nearly all protocols and applications behind IP flows, on mobile and wireline networks, in any geography
- Full application decoding: classification, metadata extraction, content extraction, reconstruction of communications (e.g. Instant Messaging)
- Intelligent classification and routing
- Full protocol behavior analysis: for example full http decoding to handle http proxying
- Support of complex networking behavior such as GTP encapsulation, VXLAN and tunnels (GRE, L2TP, etc.)

Additional Modules for Advanced Functionality

Additional modules have been developed to provide greater data analysis. The following Qosmos ixEngine modules can be used for additional processing of classification results, enabling greater granularity in traffic filtering:

- Rule Engine: Execution of customer-defined rules at run-time (e.g. correlations, aggregations, etc.)
- Custom Signatures: Complement Qosmos Signatures with user-defined signatures for proprietary protocols or extensions

Conclusion

On the highly competitive NPB market, successful vendors will be those who offer products with capabilities that make it easier to deploy, operate and upgrade tools in both legacy and virtual environments. NPBs must therefore be able to manage the end-to-end environment, understand user behavior, and help businesses protect themselves. This has driven the need for a new approach in the development of NPBs and the integration of technologies, such as DPI, that raise the level of traffic visibility and therefore the intelligence and overall performance.

References:

(1) "The Rise of Next-Generation Network Packet Brokers," an article by Zeus Kerravala, Network World, 9 August 2018: https://www.networkworld.com/article/3295881/lan-wan/the-rise-of-next-generation-network-packet-brokers.html

(2) "Network Packet Broker Market by Bandwidth, End User and Geography - Global Forecast to 2023," a report published by MarketsAndMarkets:
https://www.marketsandmarkets.com/Market-Reports/network-packet-broker-market-229957221.html

(3) Global Market Insights presentation of the "Network Packet Broker Market Share 2018-2024 Global Industry Report", published September 2018
https://www.gminsights.com/industry-analysis/network-packet-broker-market

About the Author

Erik Larsson is Senior Vice President of Marketing at Enea, where he drives product marketing, demand generation, branding and communication. Erik's views on high-tech trends are regularly featured in articles, blog posts, webcasts, video interviews, and industry events.

To contact the author or for more information, click here.

About Enea

Enea develops the software foundation for the connected society, supplying solutions for mobile traffic optimization, subscriber data management, network virtualization, traffic classification, embedded operating systems, and professional services. More than 3 billion people around the globe rely on our technologies in their daily lives. Enea's leading DPI-based IP traffic classification and network intelligence software is embedded by vendors and integrators into their products sold to telcos, cloud service providers and enterprises. For more information on Enea's Qosmos DPI technology: www.qosmos.com.

www.enea.com