White Paper

DPI & Traffic Analysis in Networks Based on NFV and SDN

Prepared by

Graham Finnie
Chief Analyst, Heavy Reading
www.heavyreading.com

on behalf of

www.qosmos.com

January 2014
Executive Summary

Traffic analysis based on deep packet inspection (DPI) and a wide range of other techniques is now well-established as a means for operators to better understand IP network traffic. This information is used for a widening range of purposes, including policy management, service assurance, security, customer experience management and development of new services.

DPI is now embedded in many types of equipment, including network gateways (e.g., GGSN and P-GW); policy enforcement appliances; service assurance elements such as network probes; load balancers; applications delivery controllers; analytics platforms, and others. However, the coming transformation of networks by ETSI NFV, SDN, and cloud services poses some new questions. In particular: What is the role of DPI and related techniques in a virtualized network and a cloud-based service delivery environment?

In this white paper, we examine these issues from the point of view of network hardware and software suppliers, drawing mainly on an exclusive survey conducted by Heavy Reading in October/November 2013. This survey asked executives from telecom suppliers a range of questions about DPI/traffic analysis, virtualization, and the relationship between the two.

The first part of the paper briefly discusses the background to this work, then considers the evolution of DPI and traffic analysis in networks and network equipment, looking at the main use cases, both established and emerging; the changing balance between internal development and third-party sourcing of DPI; and the impact of traffic encryption on DPI. In the second part, we explore vendor attitudes to virtualization, including their views on the impact of NFV, the growing potential to use standardized third-party components, and the impact of virtual switches, among other things. In the final part of the paper, Qosmos presents its own views on the findings presented here.

Key findings from the survey include the following:

- Two thirds of vendors now believe DPI is a must-have technology.
- The largest use case (by number of vendors citing it) is service assurance for QoS/QoE; the second largest is policy control (PCEF), which we believe is the largest use case by volume.
- The proportion of vendors choosing to source DPI from a third party is gradually rising, and a majority of those doing so prefer to use a pure-play supplier of DPI components.
- Half of respondents said that encryption of protocols is reducing the effectiveness of DPI. Packet metric analysis (heuristics) was identified as the main remedy.
- More than 90 percent said ETSI NFV would affect next-generation product design, and more than half said availability of standardized virtualized network function (VNFC) components would likely lead them to source more third-party components, including the proposed ETSI DPI VNFC.
- Most vendors expect to use several hardware platform types, including in some cases proprietary or ATCA platforms, as they shift to virtualization.
- More than two thirds said the virtual switch would be important in future product designs, and most also said it should be application-aware.
The Evolution of DPI & Traffic Analysis

Introduction to the Study

In September 2011, Heavy Reading conducted a survey on behalf of Qosmos that looked at the use of “embedded DPI” – which we defined as DPI that has been deployed in a wide range of telecom equipment, rather than in standalone dedicated DPI appliances. We concluded that use of embedded DPI is steadily spreading as both vendors and operators seek to embed traffic analysis techniques in a wider and wider range of network equipment.1

In a further paper published in 2012, we looked at the possible evolution of DPI in the context of SDN and network functions virtualization (NFV), arguing that DPI would likely continue to play an important (and perhaps more important) role in these types of networks, but that much still remained to be decided.2

In this new paper, we bring together these two themes in a further examination of the ongoing evolution of traffic analysis and its significance in a virtualizing network environment. The paper draws mainly on a new survey conducted during October and November 2013 that sought the views of executives working for hardware and software suppliers in the telecommunications industry.

Our survey drew 99 responses from executives working for a wide range of hardware and software suppliers. Among other things:

- 39 percent worked for companies based in the Americas, 41 percent in Europe and 19 percent in Asia.
- 12 percent worked in corporate management, 28 percent in product development, 20 percent in product management and 30 percent in sales and marketing roles.
- 49 percent worked for companies with revenues above $1 billion, 19 percent for companies with revenues of $200 million to $1 billion, and 31 percent for companies with revenues of less than $200 million.

The Evolution of Traffic Analysis

DPI has been widely deployed by network hardware and software vendors, meeting a wide range of established and emerging network operator requirements. In Heavy Reading’s September 2013 Policy Control & DPI Market Tracker, we calculated that the network operator DPI market had reached $609 million in 2012, and would grow to $715 million in 2013; a large majority of network operators has now deployed DPI for one purpose or another.

The principal catalyst for deploying DPI has been the rapid migration of network traffic to IP, and the related explosion in the use of applications and content delivered “over the top” to a widening range of devices, including smartphones and tablet computers. This has created new challenges for operators in managing traffic and customer quality of experience (QoE); understanding the nature of IP packet flows has become critically important to providing an acceptable level of service at an acceptable cost.

1 Embedded DPI: An Industry Survey
2 The Role of DPI in an SDN World
As Figure 1 reveals, about two thirds of equipment providers now regard DPI as a “must have” technology, with a further 17 percent classifying it as “nice to have.” This figure is nearly identical to that we obtained in our 2011 survey, which on the face of it suggests that the case for using DPI has not changed much in the intervening two-year period. However, closer analysis of the respondent base suggests that the 2013 survey attracted a larger number of responses from companies operating in product areas that do not yet use DPI, such as optical transport, home gateways and DSLAMs. Correcting for this, we believe that the proportion seeing DPI as a “must have” has risen slightly since 2011.

Figure 1: The Importance of DPI
Question: How important is DPI to your company?

Source: Heavy Reading survey of telecom hardware and software vendors, November 2013

To identify the use cases driving DPI deployment, we also asked respondents about the products or applications in which they used DPI. However, note that only respondents who reported that they used DPI today (82 in total) were included here, so the results shown in Figure 2 slightly overstate the use of DPI within the sample as a whole.

The results show that DPI is used across a wide range of use cases; the average respondent company using DPI reported just over four different use cases in our survey. The relatively large number of respondents working for large companies probably goes some way to explaining this, but this finding also suggests how embedded DPI is becoming in product portfolios.

Perhaps the most interesting finding here is the high score attained by “service assurance (QoS/QoE).” This broad category includes companies involved in monitoring and troubleshooting network equipment, such as Anritsu, EXFO, and NetScout. This category is a more recent adopter of DPI techniques than some others, and we might expect it to continue to grow in importance.
The second-largest category is policy control (PCEF) – a result that is consistent with our market tracker research, which shows that policy control – having grown sharply in carrier networks over the past five years – is now the largest DPI category by both value and volume. Again, we can anticipate that this application will continue to grow, along with the general growth we are forecasting in the use of policy management.

Interestingly, a quarter of respondents also reported support for the new Traffic Detection Function (TDF) recently standardized by 3GPP. Network operators have begun adding this to policy architecture specifications and RFPs: In a separate survey of network operators on policy management, conducted earlier in 2013, more than 40 percent said they expected to deploy or specify TDF in their networks, and this interest is confirmed in our new survey.

The third-largest category for DPI use is gateways; in mobile networks, DPI is now usually switched on in vendor packet gateways (P-GW) for 4G and increasingly in GGSNs for 3G; one major vendor that offered DPI as an option in its gateways told us that about 80 percent of customers used it, and a second vendor reported a similar percentage take-up.

Some gateway vendors now offer DPI as a standard feature, and in 4G networks, we can anticipate that nearly all operators will want to activate this software. Note, however, that the availability of DPI in gateways does not preclude its use elsewhere for other purposes; a typical mobile network might use DPI to do simple traffic management in the GGSN, then have a second package, perhaps in a

Figure 2: Products in Which DPI Is Used

<table>
<thead>
<tr>
<th>Category</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service assurance (QoS, QoE)</td>
<td>60%</td>
</tr>
<tr>
<td>Policy control (PCEF)</td>
<td>55%</td>
</tr>
<tr>
<td>Gateways (e.g., GGSN, P-GW, BNG)</td>
<td>45%</td>
</tr>
<tr>
<td>Subscriber analytics data source</td>
<td>40%</td>
</tr>
<tr>
<td>Service routers</td>
<td>35%</td>
</tr>
<tr>
<td>Load balancers / ADCs</td>
<td>30%</td>
</tr>
<tr>
<td>RAN congestion control</td>
<td>25%</td>
</tr>
<tr>
<td>3GPP TDF</td>
<td>20%</td>
</tr>
<tr>
<td>Other</td>
<td>5%</td>
</tr>
</tbody>
</table>

Source: Heavy Reading
standalone device or blade, used to perform more sophisticated analysis, for example to support an analytics operation. Operator views vary on the right balance to strike here.

The fourth-largest category is use of DPI as a feed for subscriber analytics systems. DPI has been routinely used by network and operations staff to analyze network traffic trends offline, but more recently there is an increasing desire to analyze trends at a subscriber level, primarily in order to develop better service packages that are suited to both customer preferences and network load/characteristics (hence a trend to real-time analytics is also taking place).

At the same time, analytics and exploitation of "big data" are seen as strategic priorities: There is a growing trend to specify "holistic" analytics systems that take feeds from a very wide range of sources, and then make these systems available to all of the different departments that might need them. Hence in the policy management area, to take one example, every significant vendor has added a standard or optional analytics package to its product in the past two years.

There is a degree of overlap between real-time subscriber data analytics and RAN congestion control – another emerging area in which DPI is starting to have a significant impact, with 30 percent in our survey citing this. Many operators would like to be able to control congestion at the RAN and cell level, and at the subscriber level, so as to provide customized or guaranteed QoE to certain customers (e.g., those with high-value packages or subscribing to particular services).

This poses some hard challenges to engineers, since congestion events are often fleeting, and QoE is affected by other factors such as radio signal strength. However, it is also an area of high innovation and investment at present. RAN congestion control also itself overlaps with service assurance, since probe vendors such as Tektronix can provide service assurance at the RAN level. Accurate real-time detection of applications and protocols is essential in these applications.

Load balancers and application delivery controllers (ADCs) are also an emerging but fast-growing sector for public network carriers. As reported elsewhere by Heavy Reading, vendors such as F5, Brocade, and A10 Networks have driven deployment of ADCs, which are usually located in data centers and decide how to balance loads based in part on identifying applications, and often include related functions such as firewalls.

**How Vendors Source DPI**

As in other areas, telecom hardware and software vendors can either develop DPI and traffic analysis capabilities in-house, or source it from third parties, usually on an OEM basis.

Initially, most vendors developed their own capabilities. But there are now several established third-party sources of DPI engines, and this is affecting the balance between internal development and outsourcing. As Figure 3 shows, although the majority mostly develops DPI internally, approximately one third now source their DPI from third parties. This compares to 27 percent in our 2011 survey, suggesting that third-party sourcing of DPI is gradually increasing. We should note that the proportion of large companies in our 2013 survey was considerably higher than in 2011; on a like-for-like basis, we believe that the proportion outsourcing would be higher in 2013 than is shown here, because small companies have a greater propensity to outsource DPI.
In a subsequent question, we asked those respondents sourcing or planning to source a DPI engine what type of supplier they preferred. As Figure 4 shows, there is now strong support for the use of a "pure play" supplier – i.e., those that are only selling DPI engines on an OEM basis – perhaps because of fears about competition, or because pure-play suppliers are perceived to be more focused on development and support of the engine itself.
The Impact of Encryption

One of the factors that might influence the way companies source DPI is the need to ensure that traffic analysis systems remain relevant, accurate and capable of detecting all that needs to be detected. This is a classic arms race in which suppliers of Web-based services seek to disguise their services to circumvent measures that network operators, among others, might apply to them.

As a result, more and more packet flows are encrypted, which prevents conventional DPI from identifying the protocol. As Figure 5 shows, slightly more than half of the sample thought this was making their DPI solution less effective, creating some internal challenges for designers. However, more sophisticated traffic analysis solutions already make heavy use of additional techniques beyond DPI, and these are now becoming more important than conventional DPI.
**Figure 6: Identifying Encrypted Protocols**

Question: How will your company address the growing number of encrypted protocols?

- **No need to address this issue because we base most of the classification on the SSL handshakes**: 22%
- **Packet metric analysis (size of the packets, spacing and frequency)**: 64%
- **Other**: 14%

Source: Heavy Reading
DPI in a Virtualizing World

DPI and other traffic analysis techniques must adapt to an ever-changing network and services environment. This includes adapting not only to continually mutating content and applications types, but also to changes in network infrastructure itself. These may include changes in the way the edge network and the gateway environment is configured (e.g., the shift from 3G to 4G), but also more profound architectural shifts. The most important of these in the medium term is the shift to virtualized network functions and componentized software.

The huge interest in these topics that has arisen in the past 12-18 months was clearly visible in our survey. For example, to gauge the impact of ETSI NFV, we asked our vendor respondents – who are responsible for a very wide range of different types of equipment – whether the ETSI specification would affect the design of next-generation network equipment. As Figure 7 shows, more than nine out of ten said it would.

But though interest is very high, the details of exactly how NFV might impact next-generation hardware and software designs are often still quite hazy. Take the hardware platform, for example: Because the main purpose of NFV is to split hardware from software (i.e., functions), most operators are expecting much lower hardware costs, with functions installed and virtualized as far as possible on generic COTS servers. In reality, however, the picture is more nuanced, with operators acknowledging that many functions may still be housed on “engineered” hardware platforms.

This reality is reflected in the replies to a more specific question we asked, about the impact of NFV on hardware platforms used. As Figure 8 shows, although respondents scored standard/generic COTS servers highest, and hybrid COTS servers third, they also gave a relatively high score to proprietary networking platforms – suggesting that many expect to continue to use these platforms for at least some of their products, even in a virtualized environment. It’s also noteworthy that the average respondent chose two of the four offered options, showing that a multi-platform approach may persist for some time.
Other Heavy Reading research has suggested that while operators are ready to shift many control layer and IT-centric functions to COTS hardware (for instance, charging systems, policy servers, and load balancers, which are often already on COTS hardware), there is more uncertainty about the right platform for mainstream data layer functions, especially routing.

Despite this, the response to another question on the impact of SDN and NFV on business models suggests that vendors are well aware that the impact on their hardware revenue streams could be significant. As Figure 9 shows, nearly half of all respondents thought that there would be a shift from an appliance-selling (hardware) model to a usage-selling (software license) model.
Figure 9: Impact on Vendor Business Models

Question: How will SDN/NFV change the current business models between equipment suppliers and telcos?

- From an “appliance-selling model” to a usage-selling model
- There will be a new ecosystem of suppliers
- Networking vendors will provide their virtual equipment per RTU only
- Don’t know

Source: Heavy Reading Survey of Network Equipment Vendors, 2013
Figure 10: Impact on Standardized Components

Question: Will ETSI NFV and the availability of standardized components influence your company to source more third-party components?

Source: Heavy Reading Survey of Network Equipment Vendors, 2013
This is a work in progress, with differing views among both vendors and operators about how and where extensions are used. Some vendors may regard this as a key part of their intellectual property and value in a software-centric market, but operators will be wary of proprietary extensions, especially if there are standardized or open-source alternatives.
The Road Ahead

There are major issues about the timing of the changes discussed in this paper, and about the telco appetite for true transformation, both of their technology supply chain and their networks. Heavy Reading’s broader research on this topic suggests that, at a high level, nearly all leading operators are becoming committed to applying the principles of virtualization and SDN to as much of their technology infrastructure as possible. The real issues, in our view, are around timing and the internal issues raised by this transformation, and operators are at different stages.

For example, those operators that have strong ICT businesses selling cloud-based services to enterprises and others are showing a much stronger appetite for SDN, with plans to apply it initially in data centers, both to cut hardware costs and to simplify operational environments. Insofar as these organizations are driving the company as a whole, this may drive application of SDN in network divisions as well. This in turn may help to transform network functions into assets that can be made available “as a service” in the cloud to third parties, and some operators are beginning to look at network functions in this way.

However, our research suggests a fairly high degree of caution about SDN within the network technology divisions of many operators at present, with most network CTOs and architects in no hurry to shift to SDN.

Network divisions are, however, showing a greater appetite for virtualization, which could be applied case-by-case and incrementally in the control layer. Even here, though, the broader potential of NFV to transform the operational environment raises many difficult organizational issues, around slimming down legacy OSS and reskilling remaining staff. This suggests to us that NFV will be a slow burn rather than a big bang for many. For suppliers in every part of the supply chain, it will be

---

**Figure 13: Making Virtual Switches Application-Aware**

Question: Should the virtual switch be made “application-aware” with embedded DPI for intelligent policy management?

- Yes: 67%
- Don't know: 24%
- No: 9%

Source: Heavy Reading Survey of Network Equipment Vendors, 2013
An Industry View From Qosmos

As described in the previous analysis, network operators deploying SDN and NFV-based networks can take advantage of the network intelligence delivered by DPI to offer new services and better manage bandwidth. DPI also gives operators more control over their networks by helping them identify and supervise the wide range of services and applications they carry. This is achievable with DPI technologies from Qosmos, designed to accelerate the development of networking equipment supporting SDN and NFV.

This survey confirms the strong move toward third-party sourcing of DPI components that we have witnessed in the past couple of years. We believe this trend will accelerate with the introduction of SDN and NFV, in line with the wider shift of the networking industry, which is adopting principles of the IT industry: more software-focused, more use of COTS hardware and leveraging of standardized components.

This leads to increased demand for DPI component products in different formats, from the existing DPI engines that can be embedded in applications, to new concepts such as a DPI plugin for virtual switch layers or a DPI engine in the form of a generic VNFC. Equipment makers and software vendors benefit from the general component approach, since they can leverage ready-to-use DPI technology to rapidly build application-aware solutions for service providers and enterprises.

Figure 14: Implementing DPI in an SDN Architecture

Source: Qosmos
In all cases, new DPI-based products provide the built-in application intelligence required for service-awareness in SDN and NFV environments. Technically, these DPI components can be implemented at three different points of an SDN architecture (see Figure 14):

1. **DPI engine VNF component**: Application running in VM and feeding applications through enriched protocols (packet tagging)
2. **DPI plugin for OVS**: Makes OVS application-aware, for e.g., efficient service chaining
3. **DPI plugin for controller**: Makes controller application-aware

Below, we describe the currently most discussed approaches in the industry.

**DPI Engine Virtual Network Function Component (DPI VNFC)**

The DPI engine as a VNFC is one of the official use cases specified by the ETSI ISG in July 2013. The product consists of a DPI engine-based component running in a virtual machine and using APIs and/or interfaces to feed protocol information and metadata to other components, together forming virtual networking equipment (VNFs) such as Service Router, GGSN, PCEF, B-RAS, ADC/Load Balancers, Network Analytics, NG Firewall, WAN optimization, etc.

**DPI Plugin for Virtual Open Switch (OVS)**

The objective of this type of infrastructure-based product is to accelerate time-to-market for open virtual switch-based developers, and enable service awareness into the virtualization host, so that service providers and enterprises profit from new solutions with integrated intelligence to optimize network services.

Technically, a DPI engine integrated with the open virtual switch can provide detailed, real-time traffic intelligence to all the guest virtual machines using packet-tagging approaches. The DPI engine classifies flows at the hypervisor level, and the resulting protocol information and metadata are either used directly by the virtual switch function (e.g., for enforcement or intelligent steering) or passed on to the guest (virtual) applications via APIs or ongoing standards. This product can consist of a DPI engine integrated with the Intel® DPDK Accelerated Open vSwitch, as demonstrated at the Intel® Developer Forum in September 2013. See the full description [here](#).

**Standardization of Components & APIs**

Standardization is key for a wide adoption of DPI as a component technology for SDN and NFV. In addition to the ETSI standard for a DPI VNFC, the ONF is working on how L4-L7 intelligence can be used in an SDN environment. On the API side, the IETF Service Function Chaining (SFC) working group is defining how mechanisms such as Network Service Header (NSH) tagging can be used to create network service paths and convey traffic information.