Application Performance Management and Lawful Interception
Table of Contents

A New Approach Unifies Two Disciplines to Drive Mutual Performance, Efficiency and Results .............................................. 4

New, Internet-Based Applications Bring Change and Challenge to Lawful Interception .......................................................... 4

A Snapshot of Network Performance Management ........................................ 4

The Changing Face of Network Performance Monitoring .......................... 5

Passive Access, a Common Thread .......................................................... 5

The Shared Technology of Deep Packet Inspection ................................ 6

The Problem of Speed ........................................................................... 6

Are KPIs a Positive Consequence of the New APM Paradigm? ............... 7

How Network Performance Management Supports LI Objectives .......... 8

Conclusion ............................................................................................. 9
A New Approach Unifies Two Disciplines to Drive Mutual Performance, Efficiency and Results

New, Internet-Based Applications Bring Change and Challenge to Lawful Interception

Customarily seen as disparate areas, network performance management and lawful interception (LI) have recently begun to converge. In concept this should be no surprise, as the two disciplines share a common foundation: LI involves examining network traffic to identify and collect specific content, while network performance management examines network traffic to identify specific performance parameters. However, despite a common approach, this convergence is relatively recent, as both disciplines have begun to draw upon one another for mutual benefit.

For clarity and definition, the following is a brief, high-level overview of both lawful interception and network performance monitoring.

Lawful interception has long been regulated by the strict conventions of governments and law enforcement agencies. LI’s non-commercial nature has caused it to evolve largely behind closed doors, addressing the specific needs of law enforcement in carrier and service provider environments. Historically, LI has involved identifying and inspecting voice traffic, i.e., ‘phone-tapping.’ While voice remains a vital component of LI, the challenges driven by the rise of data now require a new approach.

Almost all Internet communication today uses TCP/IP as the underlying protocol. Recent diversification of Internet communication techniques now pose unique challenges to LI. Numerous and varied methods for transferring messages over the Internet have arisen. Email and instant messaging, along with the near-infinite array of information-sharing and transfer mechanisms—peer-to-peer networks, web-based file repositories, Voice over IP (VoIP) telephony—and exploding numbers of social media sites such as Facebook and Twitter, all provide an immense field for information-sharing and communication.

The adaptation of LI to this new world of Internet-based applications is difficult. Many new Internet-based communication methods are no longer point-to-point, meaning that LI cannot simply examine a known stream of data to identify and collect traffic. Further, much data is cross-jurisdictional—extending across international borders—which makes identification of targets difficult at best. Lastly, applications that transfer information are often encapsulated within other protocols in order to conceal their appearance and bypass traditional lawful interception techniques.

A Snapshot of Network Performance Management

For its part, network performance management has historically focused on identifying such performance metrics as throughput, volume and loss of data packets traversing the network. Network equipment vendors supplied detailed statistics in their network elements to allow third-party network monitoring tools to collect and analyze performance data. This was, and to some extent still is largely done using dedicated management protocols such as the Simple Network Management Protocol (SNMP), RMON and NetFlow.

Of course, the network equipment vendor’s primary concern is to ensure that equipment is operating and performing optimally. Similarly, carriers and service providers deploy...
network monitoring to ensure that network bearers and servers are performing at level that avoid service degradation to end users. Accordingly, the majority of network performance-monitoring tools were designed to assess performance of network elements and carrier links regardless of traffic type carried over the network.

Thus, network performance monitoring tools typically provided information about how much and how fast in regards to traffic, as opposed to who or what actually generated the traffic—which would have interested LI. This disparate focus distinguished traditional network performance monitoring from LI, with little or no overlap of techniques.

The Changing Face of Network Performance Monitoring

Change in application deployment, particularly in the enterprise space, is now exerting pressure to extend that traditional network monitoring focus of ‘how much’ and ‘how fast’ to include ‘who’ and ‘what’. This trend is driven by the fact that most enterprises depend heavily on network infrastructure for delivery of basic business services—a situation that is intensifying with the rapid deployment of cloud-based and Software as a Service (SaaS) applications.

Increasingly, enterprise-wide business applications are critical to commerce for all size enterprises. Companies make large investments in their enterprise software, but maintaining those applications after deployment can profoundly influence overall productivity and cost-efficiency for the entire company. In actuality, application problems are the single largest source of IT downtime.

To manage new, network-based applications, from a network performance perspective, we must examine not only how much and how fast the network is running, but also who and what is generating traffic. Visibility of specific applications and users across the network is now critical to ensure business continuity, enable effective troubleshooting and reduce Mean Time To Resolution (MTTR). Visibility is also critical to allow ongoing capacity management from both a network and application viewpoint.

There can be no argument that solving application-related concerns calls for in-depth network traffic visibility down to the application level. In truth, we can no longer rely on the carriers or network element vendors to provide the fundamental data. Rather, we need to start inspecting the traffic itself, deploying deep packet inspection (DPI) techniques that enable us to grab information from within the payload of each packet where applications themselves are carried.

For these reasons, the world of network performance monitoring needs to shift its view from networks to applications and users behind them.

Passive Access, a Common Thread

LI vendors have long used passive techniques to access the primary data streams running across the network. Devices such as simple network taps or fiber splitters provide a ‘mirror image’ or copy of network traffic to various LI applications.

The beauty of using dedicated passive access hardware devices, as opposed to leveraging the capability of network elements to mirror the traffic itself, is that dedicated passive access devices impose no performance overhead to the monitored network. Perhaps even
more importantly, they are totally transparent and undetectable to end users—and often even to network operators. This simplicity, along with their additional functionality, has made passive access devices a common foundation for lawful interception deployments.

Of course as networks have become more complex, the passive access layer has also evolved to meet the requirement of more complex topologies and higher bandwidths. Vendors such as Net Optics have released a comprehensive set of higher density and fully featured passive access products to meet the demand for fundamental visibility across carrier and enterprise networks both physical and virtual.

Though the requirements of LI often drive implementation of a dedicated passive access layer, this is not always the case. The same level of visibility is required by application and network performance monitoring tools, and indeed for other emerging areas such as security and network forensics. Certainly in the enterprise space, where LI is not typically a requirement, the implementation of passive access devices is driven solely by the need of network monitoring and security tools for visibility into underlying data streams.

The cost of deploying a passive access layer into a complex, high-speed network can be significant. Therefore, it makes perfect sense to leverage the functionality available in these platforms across a range of LI, network monitoring and security tools. Thus, the passive access layer becomes the common thread between lawful interception and network performance monitoring.

**The Shared Technology of Deep Packet Inspection**

Lawful Interception and application performance monitoring can use the same passive access layer as the fundamental data source. So it is not surprising that they can also share the same fundamental DPI inspection technique to analyze traffic streams.

DPI looks inside the payload of TCP/IP frames to gather information. In the case of LI, this technique is applied to gather content of the underlying communication relating to persons of interest, whereas in application performance monitoring, DPI serves to collect important data about specific applications.

Whatever the requirement, both LI and network performance management share a need for fast, effective DPI techniques. A quick word of caution: the term Deep Packet Inspection is often misused within the industry, with no clear definition, resulting on wild claims by many vendors in this space.

Accordingly, some vendors claim DPI functionality when in effect all they are doing is collecting and storing full packets from the wire—simple packet capture, if you will. True DPI involves much more sophisticated functionality relating to identification and collection of unique and proprietary application information from within the application layer payload of TCP/IP frames.

It is this more comprehensive, ‘true’ definition that we are referring to here when speaking of DPI. This definition of DPI is also that required by LI vendors to effectively deploy their solutions across Internet and network-based applications.

**The Problem of Speed**

Compounding the challenge of deploying effective DPI is the perennial issue of ever-increasing network throughput. It doesn’t seem long ago that we were contemplating the
monumental increase from a 9600 baud modem to a full 128Kbps ISDN connection—and wondering how we would ever keep pace with such high bandwidths!

The same problem exists today, but rather than talking of a jump to 128Kbps we now confront the ramifications of deploying LI and network performance monitoring in 10 Gigabit and 100 Gigabit networks. Just as we had to adapt in the past, the transition to such high-speed networks will drive fundamental changes in the way that we implement LI and monitoring solutions within carrier, service provider and enterprise environments alike.

Such velocity makes the old fashioned “brute force” approach of streaming all packets to disk for later analysis impossible. Even if the disk technology were available today to cope with such high speeds, the sheer volume of storage required makes this approach prohibitive both logistically and financially.

We need a smarter approach to the identification and collection of data, as well as a seamless mechanism to strip out only information of interest. To do this we must still examine all the data, but once we have identified the target, we need the ability to selectively capture only those streams of interest.

For application monitoring solutions, rather than trying to collect and retain every packet, we need to use DPI to collect only pertinent application-specific metrics (better known in the industry as Key Performance Indicators or KPIs) relating to each application. These KPIs represent a relatively small set of data in comparison to the brute force packet streaming approach and as such can be undertaken more efficiently and at much higher speeds.

Based on analysis of the collected KPIs, it is relatively simple to identify specific traffic or streams of interest. In the enterprise space, this identification is primarily used to pinpoint performance or perhaps security issues—but from the LI perspective, it can identify potential targets or communications of interest.

Specifically, leaving jurisdictional privacy issues aside, a network performance monitoring platform can provide a high-level view of all traffic by gathering KPIs across a wide range of applications. Because KPIs are relatively small in volume, compared to the originating traffic, it is simple to search for keywords or patterns within the KPIs themselves. This approach makes it possible to search all email subject lines for a specific term, or website URLs for a particular pattern or monitor an applications’ behavior based on its specific KPIs.

LI solutions can leverage the capability of application performance monitoring to provide detailed KPIs via DPI. This capability enables more comprehensive security monitoring at a far lower cost than the traditional brute force packet capture approach.

This tripartite approach between the passive access layer, application performance monitoring and LI provides the most comprehensive, cost-effective solution to cope with emerging high-speed networks and diverse Internet communication modes.

Are KPIs a Positive Consequence of the New APM Paradigm?

As we have discussed, modern performance management solutions need to incorporate DPI in order to effectively identify and classify network-wide application performance.
Unlike traditional SNMP or even flow-based monitoring, those metrics required to monitor networks at an application level are application-specific. That is, metrics that define one application’s performance differ from those that define another’s.

This is a subtle concept, illustrated with this example: If we are interested in email performance, we might collect pertinent statistical data such as ‘To’ and ‘From’ address, attachment name and size, time taken for the email to send and so on. In monitoring VoIP traffic, however, we collect a different set of metrics such as caller/callee identifiers, jitter, MOS score and volume. Thus, while some metrics are common across many applications, others are application-aware. This is why DPI is important, to dig into the payload of each packet and extract application specific data.

It is the collection of these application-aware metrics—or KPIs, as we have named them—which is of most interest to the new breed of network performance solutions. The KPIs go well beyond traditional performance measures such as volume and throughput, to include information traditionally the domain of policy or security managers. Identifying the ‘sender’ from an email does not, strictly speaking, pinpoint application performance issues, but this information could be very useful from a security or policy management point of view. This information is also likely to be very important to LI.

This capability represents a convergence of physical infrastructure, in the form of the passive access layer, with technology used to collect information via DPI. Plus, the commonality of KPIs or application-specific data represents a significant overlap between LI and application performance management. While network performance monitoring is less concerned with collecting actual content, LI can nevertheless leverage KPI data to assist in identifying and collecting traffic of interest.

How Network Performance Management Supports LI Objectives

Increasing network bandwidth is one issue that is unlikely to go away soon. But other LI challenges may be resolved by the emerging network performance management platforms.

As alluded to earlier, much Internet communication is not point-to-point in the same fashion as traditional voice conversations. In the LI arena, it is often incumbent on the local carrier or ISP to provide identification information on a particular target or person of interest. This may take the form of a locally held IP address or username that a local law enforcement agency may compel an ISP or carrier to reveal.

The global nature of the Internet makes it very easy to house data, and in fact transfer information with scant regard to international borders or jurisdiction. This global environment poses unique unique challenges for LI by allowing retention of data across multiple jurisdictions. Coincidentally this mirrors the challenge faced by network performance monitoring solutions as applications become distributed in a cloud environment. This environment may be housed on networks that are no longer private and which encapsulate application data in common Internet protocols.

For example, consider a situation in which a user wishes to communicate with absolute anonymity—that is, with little or no traces or record of conversation made available to local authorities. The Internet provides a wide range of free email and file-sharing solutions to fit these needs. The user can easily open an account on a free email server known to be hosted outside the local jurisdiction. By doing so, this user ensures that local law enforcement authorities will have difficulty compelling a foreign company to reveal his
or her details. Or the user can create an account and login, and then type a message as an email. Rather than actually sending that email, the user simply saves it as a ‘draft’ on the remote server itself, then passes login details to another party, who logs in to the same remote mail account, looks at the saved draft and updates accordingly. In this fashion, it is possible to have a complete conversation without the content of the communication ever being transmitted across the Internet. The entire communication is stored on the local mail server housed in a foreign country.

From a law enforcement perspective, it is almost impossible to acquire the login details from the remote email server provider, given that it is likely housed in a remote jurisdiction. The content of the communication is only ever transmitted as an HTTP or SMTP stream and is never stored outside the local mail server. Of course it would be possible for a local law enforcement agency to inspect the target’s Internet traffic, but it is a far more complex proposition to be able to gather and then decode the HTTP or SMTP stream to gain access to the communication itself.

This is where the new application performance tools that support sophisticated DPI can help. Rather than relying on the ability to identify a specific target and analyze all subsequent traffic, the new APM approach allows for all traffic to be analyzed and for searches to be set up for specific keywords or addresses. That is, we take a global, high-level view of all traffic rather than a macro detailed view of just some. Once we have identified specific areas of interest, then we can simply deploy the traditional macro lawful interception techniques for detailed analysis and content collection.

This approach may not be suitable in all jurisdictions owing to privacy and regulatory concerns, but it does allow for a more comprehensive view of network traffic, as well as providing the ability to capture data that would have previously gone unnoticed.

**Conclusion**

It is clear that the traditionally disparate disciplines of lawful interception and application performance management are converging; that they now share common technologies and can be seen as complementary in implementing comprehensive, total solutions.

This overlap of technology is largely due to the increasing deployment of DPI application identification techniques within application performance management solutions. In addition, the technology is assisted by implementing a passive access layer infrastructure throughout many carrier and service provider networks.

This passive access layer provides an ideal foundation for seamlessly and transparently mirroring data streams to LI and network performance monitoring solutions alike. Modern passive access solutions also provide the ability to implement complex filtering that allows for specific streams of interest to be forwarded. This negates the requirement for LI solutions to deal with the ever-increasing bandwidths associated with carrier networks.

As time goes on and these techniques continue to evolve, we will see a continuing convergence of the passive access hardware layer with both network performance management and lawful interception, further negating the traditional approach of relying on feeds from network equipment vendors.