DPI Applications: Friend or Foe?

Deep Packet Inspection, or DPI, is a relatively new addition to the general telecom vocabulary. DPI is being promoted as a solution for many of the issues faced by fixed and mobile broadband operators. In fact, DPI as a concept has been around for a long time but it is only now coming to the forefront because the technology has reached a price and performance threshold where it is commercially viable for deployment – and because of certain controversial application areas where it might be used (more on that below).

DPI solutions promise to deliver better subscriber management, improved network efficiency, additional revenue, and better security – all for operators! But to understand whether DPI is a “friend” or “foe” for consumers, we need to look closer at the issues surrounding each of the benefits above, and in particular some of the more controversial areas such as policy enforcement and subscriber profiling for targeted advertising.

Current Context

Looking back, our telecom networks were largely separate silos of functionality: a circuit switched network carried voice, and a data network handled Internet access. VoIP traffic was also carried over the data networks, but often this involved dedicated paths or was highly managed to guarantee service levels.
When an operator ran out of bandwidth it simply threw more fiber at the problem in order to restore status quo.

In recent years, though, we have seen a dramatic increase in access speeds and now, particularly with IP Multimedia Subsystem (IMS) and Long Term Evolution (LTE), a single broadband IP network is delivering Internet access, entertainment, and voice telephony services. Balancing the demands of each of these application types to ensure consistent quality of service is imperative.

At the same time, the introduction of new applications – and the behavior of a minority of users – has started to consume disproportionate amounts of the (shared) bandwidth available, potentially spoiling everyone’s quality of service. Initially compressed music files, then short video snippets, and now full length films (including high definition versions) have caused demand for bandwidth to snowball out of control.

Managing Traffic

Operators have come to realize that throwing more bandwidth at the problem will not solve the situation in the long run; it merely pushes the problem forward into the future. Especially in an “unmanaged” network, the situation will always remain such that a relatively small number of users will be able to consume a disproportionate amount of bandwidth. To date this has been tolerated given the general public’s preference for flat rate billing plans.

Where this approach stops working, however, is when a heavy user significantly impacts the “value” (e.g., bandwidth) a regular, non-heavy subscriber is used to getting. This can be expressed as quality of service or price paid for the service. In fact, regular users are effectively subsidizing excessive users when operators have to hike flat-rate prices across the board to cover new equipment and capacity costs. In such a scenario subscribers are more likely to support the traffic management application of DPI to ensure that everyone gets a fair share of the bandwidth and pays a proportional price for what they use. The alternative is that perturbed subscribers can churn by moving to a rival a network where they feel they can get a fair deal – but this is what operators hope to avoid.

Netting Neutrality

Following this train of thought a little further, one might ask, “Why not just block peer-to-peer (P2P) traffic altogether, which is one of the main bandwidth-hogging culprits anyway?” Well, this topic takes us into the realm of net neutrality, where the argument is essentially, “If you block P2P today, what will get blocked next?” One person’s nuisance is another’s necessity. In other words, it is potentially the start of a slippery slope and net neutrality advocates seek to preserve a level playing field where all application and content types are treated equally.

The blocking (or throttling) of a specific P2P protocol is what originally sparked the net neutrality debate around DPI and started to taint its reputation with regulators, politicians, and consumers. Today the concept of totally blocking a specific P2P application is no longer considered acceptable – firstly because of the FCC ruling on Comcast but mostly because it won’t be effective: there are many P2P protocols and blocking one of these will merely result in users adopting a different application or churning to a different broadband vendor who doesn’t block their favorite file sharing application.

Most operators have therefore evolved their approach and now ensure “fair share” for all users by rate-limiting certain applications or users during busy hours but avoiding draconian measures such as completely blocking services.

The second aspect of net neutrality is a concern about anti-competitive behavior. An example might be a network operator favoring its own specific VoIP service over a more “universal” service from a competitor. DPI certainly has the capability to identify and prioritize one service or application over another, and I think there is indeed a legitimate concern regarding the application of DPI if it restricts consumer choice – which is rarely a good thing. What’s more, this “choice-limiting” approach is likely to be investigated by regulators and therefore in this scenario some consumers might view DPI as a foe. (Fig. 1).

Overall, traffic shaping and policy enforcement using DPI should be viewed as consumers’ friend resulting in fair share for all, and at a fair price. There are a few pitfalls of which to be aware, but with a sensible policy toward its application it will indeed benefit the consumer.
Making Money

Revenue generation is the second DPI-related area that we should consider. Network operators are under price pressure and looking to increase their revenue by offering new services enabled by DPI. Examples include “smart pipe” tiered service levels (i.e., you get what bandwidth you pay for) and enhanced services (such as a speed boost for a specific time/application). (Fig. 2)

It also includes “clean pipe” security services where traffic is screened for malware, viruses, etc. within the network before it is sent to a user. All of these are services with value to a certain demographic and are generally considered as consumer-friendly. (Fig. 3)

The controversial area regarding revenue generation is targeted advertising wherein network operators become part of the advertising value chain. It works like this: a consumer visits content providers’ sites and within these sites are advertisements – where the content provider is getting revenue from these placements. In the past, these adverts were placed with somewhat of a “shotgun” or “broadcast” approach and not targeted directly to specific consumers. For example, if a consumer went to a website that reviewed electronics, the consumer would indeed find adverts about electronics; however, the chances that the advert matched precisely what the consumer was looking for were slim, as the adverts were not tied to the precise context of the content being viewed.

Profiling Behavior

The logic goes that by profiling browsing habits and the interests of subscribers, it is possible to accurately understand (and predict) user behavior, and therefore to only display adverts in which they are (likely) interested, it should be better for the customer and more effective for the advertiser.

Right? Well, this is probably accurate to a certain extent, but it doesn’t address the core issues of privacy, how anonymity is assured, and how such profile data can be protected. Consumers are quite wary of profiles being assembled on them without their knowledge, consent, or editorial control.

For targeted advertising to be considered a friend, therefore, requires stringent safeguards regarding data protection, privacy, and very clear “best practices” regarding how customers may opt-in to (or opt-out of) the service.

We continue to see interest in this area and these concerns are certainly a focus for developers of the DPI platforms in this space. If the right balance is struck and privacy can be assured for users who opt-in, DPI-based profiling can be an efficient, positive service for network operators and consumers (although content providers may not agree as they may end up sharing their advertising revenue stream, but that is another issue...).
Summary

Overall, DPI has the potential to benefit consumers if it is employed sensibly, sensitively, and openly with the consensus of customers. It is going to be necessary for operators and the DPI ecosystem to quantify and explain the benefits to consumers. Prevailing in this public relations challenge is a near-term priority in order to ensure that customers view DPI in a positive light. While certain DPI applications have received negative press and therefore we in the industry cannot just focus on the network efficiency benefits it brings, we must also demonstrate to customers how DPI helps them get greater security, choice, and value.