Deep Packet Inspection: What you need to know

All sorts of public and private entities would love to monitor your Internet browsing habits. It's now possible using "Deep Packet Inspection." Michael Kassner will shed some light on the technology involved and possible privacy issues.

Anyone who uses the Internet needs to be aware of Deep Packet Inspection (DPI), its uses, and potential misuses. You may recognize DPI as what ISPs use to conform to CALEA, the U.S. government-ordered Internet wire-tapping directive. If that's not enough, DPI, albeit behind the scenes, allows ISPs to block, shape, and prioritize traffic, which is now fueling the "Net Neutrality" versus traffic priority debate. So, what is DPI and how does it work?

Deep Packet Inspection

DPI is next-generation technology that's capable of inspecting every byte of every packet that passes through the DPI device, that means packet headers, types of applications, and actual packet content. Up until now, this wasn't possible with IDS/IPS systems or stateful firewalls. The difference being, DPI has the ability to inspect traffic at layers 2 through 7, hence the "deep" in DPI. A simple analogy would be that of snail mail. IDS/IPS firewalls would be the mail sorters who just read the letter's address, knowing nothing about the letter's content. Inspecting Internet traffic from layers 2 through 7 would correspond to the person who actually reads the letter and understands the contents.

To recap, DPI allows people controlling the device to know everything, including the payload of each packet in the data stream. For example, if an unencrypted e-mail is scanned, the actual body of the e-mail can be reassembled and read. Nate Anderson wrote an excellent Ars Technica article "Deep Packet Inspection Meets Net Neutrality, CALEA." The following quote appears in that article:

> *"Deep packet inspection refers to the fact that these boxes don't simply look at the header information as packets pass through them. Rather, they move beyond the IP and TCP header information to look at the payload of the packet. The goal is to identify the applications being used on the network, but some of these devices can go much further; those from a company like Narus, for instance, can look inside all traffic from a specific IP address, pick out the HTTP traffic, then drill even further down to capture only traffic headed to and from Gmail, and can even reassemble e-mails as they are typed out by the user."*

also explains what happens at layer 7:

> *"Layer 7 is the application layer, the actual messages sent across the Internet by programs like Firefox or Skype or Azureus. By stripping off the headers, deep packet inspection devices can use the resulting payload to identify the program or service being used. Procera, for instance, claims to detect more than 300 application protocol signatures, including BitTorrent, HTTP, FTP, SMTP, and SSH. Ellacoya reps tell Ars that their boxes can look deeper than the protocol, identifying particular HTTP traffic generated by YouTube and Flickr, for instance. Of course, the identification of these protocols can be used to generate traffic shaping rules or restrictions."*

What makes DPI all the more impressive is that the packet analysis happens in real time, with data stream throughput approaching 20-30 Gb. See where I'm going with this? With no loss of throughput, ISPs are able to insert these devices directly in their data streams, forcing all traffic to pass through the devices. Procera, Narus, and Ellacoya are front-runners in development of this technology, having placed equipment throughout the world.

DPI's potential uses

DPI technology is unique in that as of now it's the only way to accomplish certain governmental security directives. DPI also has the potential to do a great deal of good. For example, DDoS attacks are virtually impossible to thwart. Conceivably if DPI were in place and configured correctly it would detect the DDoS packets and filter them out. Some more potential uses are listed below:

- **Network security**: DPI's ability to inspect data streams at such a granular level will prevent viruses and spyware from either gaining entrance to a network or leaving it.
- **Network access**: DPI creates conditions where network access rules are easy to enforce due to the deep inspection of packets.
- **CALEA compliance**: DPI technology augments traffic access points (TAP) technology used initially for governmental surveillance equipment.
- **SLA enforcement**: ISPs can use DPI to ensure that their acceptable use policy is enforced. For example, DPI can locate illegal content or abnormal bandwidth usage.
- **QoS**: P2P traffic gives ISPs a great deal of trouble. DPI would allow the ISP to instigate traffic control and bandwidth allocation.
- **Tailored service**: DPI allows ISPs to create different services plans, which means users would pay for a certain amount of bandwidth and traffic priority. This one is controversial and affects Net Neutrality.
- **DRM enforcement**: DPI has the ability to filter traffic to remove copyrighted material. There's immense pressure from the music and movie industries to make ISPs responsible for curtailing illegal distribution of copyrighted material.

The above applications have the potential to give users a better Internet experience. Yet it wouldn't take much mission creep to create major privacy concerns. I would feel remiss if I didn't point them out and help everyone understand the ramifications.

Possible misuses of DPI

DPI is another innovative technology that has ISPs arguing with privacy advocates. ISPs and DPI developers are adamant that the technology is benign and will create a better Internet experience. However, privacy groups have two major concerns: little or no oversight and the potential for losing still more individual privacy. Many experts find the following uses of DPI to be especially troubling:

- **Traffic shaping**: Traffic shaping is where certain traffic or entities get priority and a predetermined amount of bandwidth. With the increasing number of bandwidth-hungry applications, ISPs are having to make decisions on whether to increase available bandwidth with infrastructure build out or increase control of the existing bandwidth. Installing a DPI system is usually the choice as it's cheaper and has a more predictable RoI. Albeit cheaper, it's riskier, and I suspect that's why the Net Neutrality debate is going on right now.
- **Behavioral targeting (BT)**: BT uses DPI technology for the sole purpose of harvesting user information anonymously (supposedly) and selling it to interested parties who use the information to create ads that are targeted to the individual.

Final thoughts

This is a very complex subject, having the potential to change everyone's view of the Internet. An optimist would say that DPI will help enhance the experience, even producing ads that are relevant to each individual user. Whereas a pessimist would say it's "big brother" technology that only benefits ISPs. I don't think anyone is sure how the Internet will look when the dust settles about DPI, but it should be interesting.I hope that I was able to increase awareness of how ISPs using a DPI device can intercept, read, and interpret every one of your Internet-destined packets.

There are options that you can use to avoid DPI scrutiny. VPNs, whether they are IPsec, L2TP, or SSL, will negate any effort by DPI to decipher the encrypted traffic. E-mail is another subject, and once again the only for sure way to ensure its privacy is to encrypt the message.