Deep packet inspection meets 'Net neutrality, CALEA

By Nate Anderson | Last updated July 25, 2007 11:10 PM

Peeking beneath the 7th layer

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.

Much like virus scanners, the boxes generally make use of "application signatures"—telltale ways of sending and receiving information that can be used to link a particular packet with a particular application. Procera's version is called Datastream Recognition Definition Language, and just like virus signatures, DPI gear needs regular updates to stay on top of new developments.

DPI vendor Allot Communications has produced a nice whitepaper that describes the different forms that this signature analysis can take. Port analysis is the simplest way to identify an application, but as we've already mentioned, it's notoriously inaccurate. Adding string matches can help, but not all applications use identifiable strings of characters. Kazaa does so, however, embedding its own name in the "user-agent" field of HTTP GET requests. Searching packets for the string "Kazaa" can turn up these requests and let the ISP know that a particular user currently has the application running. Numerical properties are another good way to craft application signatures, using patterns like payload length or specific response sequences.

Looking this closely into packets can raise privacy concerns: can DPI equipment peek inside all of these packets and assemble them into a legible record of your e-mails, web browsing, VoIP calls, and passwords? Well, yes, it can. In fact, that's exactly what companies like Narus use the technology to do, and they make a living out of selling such gear to the Saudi Arabian government, among many others.

Texas disaster recovery and managed services company Data Foundry objects to network operators doing this deep level of inspection. In a recent FCC filing, the company charged that "broadband providers' AUP/TOS/Privacy Policies, in combination with Deep Packet Inspection, allow intrusive monitoring of the content and information customers transmit or receive. This contractual and technical capability interferes with and may well eliminate all sorts of privileges presently recognized under law... Broadband service providers have no justifiable reason to capture this information."

But vendors like Ellacoya and Procera aren't so interested in capturing private data, and it's not the focus of their devices. An Ellacoya rep reassures me that most applications can be identified without actually looking through all the data in a packet payload. Still, concern over the technology has been growing as its rollout has accelerated.

DPI can also be used to root out viruses passing through the network. While it won't cleanse affected machines, it can stop packets that contain proscribed byte sequences. It can also identify floods of information characteristic of denial of service attacks and can then apply rules to those packets.

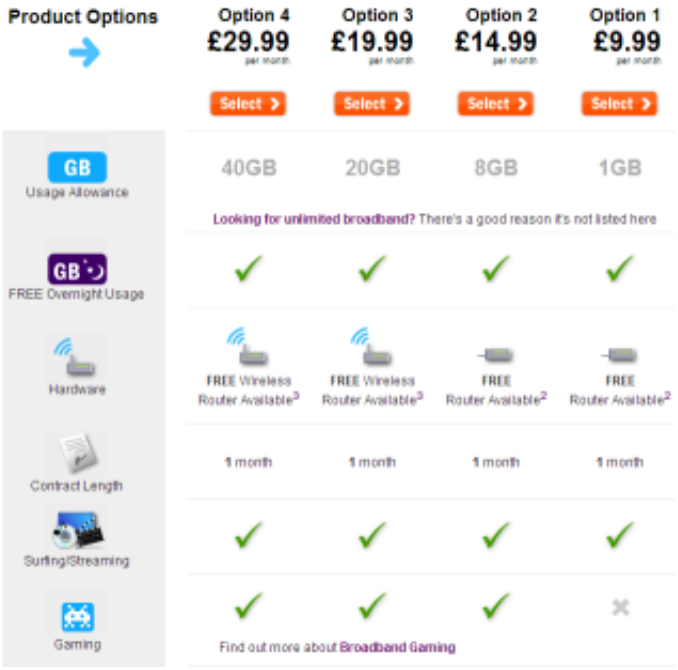
Some of these things can be done by looking at a single packet, but many cannot. DPI gear can generally extract information from traffic that varies by application type: IP addresses and URLs from HTTP traffic, SIP numbers from VoIP calls, filenames of P2P files, and chat channels for instant messages. Grabbing this information requires a look at a whole set of initial packets until the necessary information is gained, referred to as examining the "flow." Procera in particular makes a big deal about this, referring to their technology as "deep flow inspection" rather than deep packet inspection.

Nickel-and-diming?

All of this technology can be applied in a highly granular fashion. Surveillance rules can be created that are specific to each individual subscriber, and traffic shaping and quality of service can also be applied differently to every connection in the network. Without this sort of individual shaping technology, it has generally been easiest for ISPs to simply offer subscribers unfettered access to the Internet. Bandwidth caps are simple to implement without using DPI, but DPI does make it simple to tier levels of service—purchasing access to the web, but not to VoIP for instance. Based on the capabilities I've been describing, this sort of thing can go even further, with companies marketing low-cost data plans that might include web access *except* for streaming video or VoIP calls but no online gaming.

Such scenarios aren't a fantasy; they're happening right now. In the US, Internet access is still generally sold as all-you-can-eat, with few restrictions on the types of services or applications that can be run across the network (except for wireless, of course), but things are different across the pond. In the UK, ISP plus.net doesn't even offer "unlimited" packages, and they explain why on their web site.

"Most providers claiming to offer unlimited broadband will have a fair use policy to try and prevent people over-using their service," they write. "But if it's supposed to be unlimited, why should you use it fairly? The fair use policy stops you using your unlimited broadband in an unlimited fashion—so, by our reckoning, it's not unlimited. We don't believe in selling 'unlimited broadband' that's bound by a fair use policy. We'd rather be upfront with you and give you clear usage allowances, with FREE overnight usage."



Plus.net's plans

What that means in this is that you pay by the gigabyte and by the service. Plans start at £9.99 (around $20) a month for just 1GB of data, though use after 10 PM appears not to count for this quota. The lowest price tier also does not support gaming and places severe speed controls on FTP and P2P use (allowing only 50Kbps at peak periods). Plus.net says that the lowest tier will not work adequately with online games or corporate VPNs. Paying £29.99 (around $60) a month provides 40GB of data transfer and fast P2P and FTP speeds, along with 240 VoIP minutes from the company. All of these tiers feature downloads speeds of up to 8Mbps.

How do they do it? With Ellacoya gear.

This can sound like nickel-and-diming, creating new ways to charge people for things (online gaming) that used to be free. But plus.net and Ellacoya both argue that it's actually a better deal for consumers because it lowers the price for those who need fewer features. According to this argument, users who don't want to play online games or download massive P2P files should not have to pay a share of the bandwidth for those who do. Traffic shaping can be used to set up a whole host of data packages to provide increased customization and, ultimately, lower costs for lighter users. Heavy

users might actually see their fees increase as they're no longer subsidized by others on the network.

In fact, modern DPI gear can allow each individual subscriber to select services and speeds that are of most benefit to them, and every single user on the network can have a different set of rules in place (and pay a different price). Ellacoya's new marketing buzzword for this capability is "the Personal Internet."

Now, if all this talk of throttling and service restrictions hasn't yet cause you to think the words "network neutrality," you haven't been paying attention, because this is exactly the sort of talk that some people find offensive. "The 'Net was built on open access and non-discrimination of packets!" they argue, to which DPI vendors say, "ISPs must prepare for the exaflood."