Deep packet inspection meets 'Net neutrality, CALEA

By <u>Nate Anderson</u> | Last updated July 25, 2007 11:10 PM

Net neutrality, traffic shaping, and the "coming exaflood"

Let me put my cards on the table: I loathe the word "exaflood." It sounds like the sort of concept that would surface in a bad science fiction novel, one involving a sentient artificial intelligence, aliens who speak only in clicks, and a hard-boiled ex-space Marine with a shotgun. I'm not going to use it again, but if you're not familiar with the term (it's generally used not in any technical sense, but simply to mean "a whole lot of data"), check out this <u>*Wall Street Journal* article</u> or this <u>freely-available reprint</u>.

The idea here, from the perspective of the DPI vendors, is that the Internet now generates and streams more data than the current transmission network can handle without shaping or throttling. Senator Ted Stevens (R-AK) may have been widely ridiculed for his "series of tubes" analogy, but Internet connections *are* like tubes—each link can only transmit so much data at once (though "Internet tubes" can gain capacity over time, as fiber optic lines, DSL links, and cable lines have all done; this is part of Isenberg's point about why it's just cheaper to boost capacity). Given the voracious appetite of P2P users and streaming video watchers, this sort of content alone could cause delays for content that is arguably more critical and time-sensitive for an ISP's customers than an illicit Hollywood release or a video of a kid wiping out on a dirt bike: e-mail, instant messages, traditional web browsing.

Seen in these terms, the DPI vendors argue that ISPs which "do nothing" to shape traffic on their networks have actually made a choice. In this case, the choice is in favor of chaos and bottlenecks at peak periods. No matter how much bandwidth is currently thrown at the problem, P2P, Usenet, FTP, and streaming video will fill it (Ellacoya's CEO told me that "throwing bandwidth at the problem can't solve it"). Handling this ~~exaflood~~ data surge responsibly means using traffic shaping, at least during the periods of highest use.

This argument fits together nicely with another common one that I heard from DPI vendors: we help to make networks "fair." This was one of the claims made by plus.net (see the previous page); why should it be fair for a few ultraheavy users of the network to drag down performance for everyone else? Traffic shaping gear is all designed to integrate easily with billing systems, making it easy to charge more money for heavier use. The corollary is that prices for more modest users should actually go down (whether that actually happens is another story).

Concerns over managed traffic

Now, this entire approach to managing traffic doesn't sit well with some folks who call for neutrality on their networks. Recent research has shown that a nondiscriminatory network will in fact require up to twice the peak bandwidth of a tiered and shaped network, but this doesn't necessarily mean that this is the more expensive approach. Pundits like David Isenberg have argued that <u>simple overprovisioning is cheaper</u> in the long run than investing in all the new DPI gear and the manpower to maintain and monitor it.

The debate is made complicated by the fact that "network neutrality" has a hundred differing definitions, making it something of a hundred-headed hydra. In the *Journal* article linked above, the author talks repeatedly about net neutrality as something that will force network providers to lease out access to competitors at government-dictated rates. Whatever else this idea might be, it's not what most people talk about when they refer to "net neutrality."

For a thoughtful definition, consider the one <u>given by Daniel Weitzner</u>, who cofounded the Center for Democracy & Technology, teaches at MIT, and works for the W3C. He lays out four points that neutral networks should adhere to:

1. Non-discriminatory routing of packets
2. User control and choice over service levels
3. Ability to create and use new services and protocols without prior approval of network operators

4. Nondiscriminatory peering of backbone networks.

Savetheinternet.com has spearheaded the network neutrality drive in Congress, and it has a shorter <u>definition available</u>: "Put simply, Net Neutrality means no discrimination. Net Neutrality prevents Internet providers from speeding up or slowing down Web content based on its source, ownership, or destination."

If that's not clear enough, they provide an example. "When we log onto the Internet, we take a lot for granted. We assume we'll be able to access any Web site we want, whenever we want, at the fastest speed, whether it's a corporate or mom-and-pop site. We assume that we can use any service we like—watching online video, listening to podcasts, sending instant messages—anytime we choose."

It's not hard to see why these particular constructions of "openness" run headlong into the business plans of the traffic-shapers. Companies like Ellacoya and Procera argue that this sort of "never discrimate" policy isn't much more than unworkable idealism. Such a network will in fact fill up with data; companies that don't filter or shape packet flows have then made a default decision to allow things like VoIP, videoconferencing, and online gaming to get "laggy" and e-mail to get delayed as BitTorrent and YouTube packets clog the tubes. Downloading an 800MB video, even if the movie in question is legal, is hardly the sort of application that is mission critical, and few customers are going to abandon ship because their YouTube videos take an extra two seconds to buffer. But customers do care if their VoIP service consistently goes glitchy or has tremendous lag, if *World of Warcraft* becomes unplayable, or critical e-mails and IMs are delayed in transit.

The argument of the vendors is generally that "the market will decide" and that what's important is for companies simply to be upfront about the kinds of restrictions they have in place. We agree that transparency in these matters is a good idea, but the basic problem in the US is that if you don't like the policies your ISP has in place, it can be difficult to switch. We've been pointing out for years that Americans are generally locked into one or two providers, so most people are hardly spoiled for choice.

Where you come down on these questions may vary depending on where DPI gear is deployed; many people have less problems with its use by last-mile ISPs who interact directly with consumers. Throttling P2P traffic to keep the network open for other uses might be fine, but the concern is magnified when such gear is rolled out by the backbone operators, like AT&T and Verizon. With last-mile ISPs, at least (most) customers have *some* options for switching if they don't like the terms.

But there are so few backbone operators, and they wield so much power, that the truly scary stuff from a net neutrality perspective is if backbone providers start looking at Google and say, "If you want decent transport over my pipes, then you have to pay my toll." When that type of demand comes from an upstream provider, from a network economics standpoint that's a whole different ball game than Comcast trying to soak Google by threatening to slow down access to Google.com.

That's because there's no way for the end users to vote "no" on the policy; all of the users of the multiple last-mile ISPs who are downstream from that backbone will see their access to Google start to suck, but there's not much they can do about it because it's not really their ISP's fault. In other words, the backbone providers have a more insular, more monopolistic, non-consumer-facing position in the Internet hierarchy, so if they decide to ditch neutrality and start squeezing websites and online service providers, then there's not much that can be done.

These are deep waters, and there are complex arguments to be made here (for a detailed engineering discussion of the issues facing "best effort" routing on a congested network, take a look at this <u>IETF Internet-Draft</u> by Sally Floyd and Mark Allman). DPI gear makes plenty of objectionable behaviors possible, but it also opens the door to network virus

scans and DDoS defense mechanisms that could do real good. By making it possible to purchase access only to the specific services or protocols that one needs, DPI could also make the Internet cheaper for casual web and e-mail users. Like most technologies, the gear itself enables a great range of uses, and it's up to the operator to be responsible.

In fact, the Center for Democracy & Technology, which stands up for freedom of expression and privacy on the Internet, has no problem with many of DPI's projected uses. In its <u>FCC comments regarding network neutrality</u>, the group laid out a host of possible practices along with its thoughts on them (pp. 7-10). Blocking security threats, spam, and illegal content is unobjectionable to the CDT, as is prioritizing any content requested by the subscriber and prioritizing traffic based solely on the type of application (like VoIP). But blocking any traffic or actively degrading it would be off limits, as would priority given to traffic from specific ISPs or web site operators who have paid an additional fee.