THE END OF END-TO-END?

One of the fundamental design principles of today's Internet is so basic and so important that few users have ever heard its name; they just assume its existence. It's called "end-to-end," and some disturbing new developments are putting it in jeopardy. The end-to-end principle asserts that information pushed into one end of the Internet should come out the other without modification: the Net should act like a big, fat, dumb, digital pipe.

End-to-end operates on many levels. When you try to download a news Web page, for example, the two ends might be CNN's server and your browser. End-to-end dictates that the Internet shouldn't modify CNN's data packets as they move through the network. It thus guarantees that the page you receive is the same one CNN sent. Who could argue with that?

Many people, it turns out. End-to-end pushes a lot of power to the endpoints, but it also saddles them with some important duties. One such responsibility is security. If some hacker sends you an "attack packet," it's the job of the network to deliver that packet, no questions asked. Too bad if you haven't installed the security patch. That sounds harsh, but it is preferable for users to have this kind of control than to cede it to network administrators.

For a good example of a network that's not end-to-end, think of today's cell-phone networks. When I call my friend Jesse's cell phone, I call a phone number that's out in San Francisco. But the network knows that Jesse is actually in Boston: the call gets routed out to California then back to Boston, and Jesse's phone rings. All of this involves a tremendous amount of work on the part of the network—too much work for end-to-end. When I talk, the network takes my voice, compresses it, turns it into packets, and sends those packets down a low-bandwidth digital wireless network to Jesse's phone. The quality of what he hears is determined by the network, not by our phones.

If the cell-phone network were end-to-end, my phone would use a registration server to find where Jesse's phone is located. It would then open up a channel to his phone, negotiate with his phone to find a mutually acceptable voice compression scheme, and the two phones would start exchanging digital packets. Suddenly the network is dumb and the cell phones are smart.

So what's the advantage of end-to-end? Innovation. With an end-to-end cell-phone system, Jesse and I could upgrade to a better voice compression system just by buying new phones: nothing else in the network would have to be modified. We could also add three-way or four-way or even five-way calling, just by sending out more packets. You can't do either of these with today's cell-phone networks.

Of course, if Jesse and I have end-to-end phones, we're not limited to using cell-phone networks. We could just as easily use the Internet through wireless Net access at a university or a Starbucks. And that's the real threat of end-to-end: by putting the intelligence in the endpoints, end-to-end turns the cell-phone network—or any other network—into a commodity.

On the Internet, end-to-end promotes competition by making it easy for users to switch from one network provider to another. If I don't like the service I'm getting from my broadband digital subscriber line (DSL) connection, I can swap it out for a high-speed cable modem. Sure, my computer's Internet Protocol address will change. But thanks to end-to-end, that address really doesn't matter.

End-to-end is such a basic principle that just about any tinkering with it is bound to cause problems. Consider those Internet service providers that have toyed with blocking unsolicited junk mail: a few customers wanted their spam and resented any e-mail filtering by the provider. Other customers discovered that some legitimate e-mail was accidentally being filtered out along with the tasteless promotions for Viagra and cheap refinancing *(see "Spam Wars," p. 32)*.

The basic principle underlying the Internet promotes competition and makes it easy for users to switch from one network provider to another. That's why some companies want to kill it.

Another way to break end-to-end is to modify packets so that they go somewhere other than their originally intended destinations. That's what the government of China did earlier this year when it ordered the country's Internet service providers to replace Google's home page with a China-based search engine. Packets were intercepted and rewritten on the fly. China was thus forcing the service providers to violate the end-to-end principle: it shouldn't be the job of the network to reroute your packets to a competing Web server or block them because the content is deemed illegal.

Nevertheless, most Internet service providers would like to be able to violate end-to-end as they see fit—blocking spam, filtering out viruses, and perhaps even suppressing advertisements. They would like to make customers dependent on these "enhanced" network services so that it would be harder than ever to switch providers. Then they might start dabbling in other end-to-end infringements, like rewriting the results of Google queries, inserting advertisements directly into your e-mail, and even mining your Web-browsing habits so that they can more easily target advertisements.

Whenever you hear a company bragging about the great services it can offer directly in its network, understand that it is trying to kill end-to-end. Personally, I'd rather have a dumb network, a pair of smart endpoints, and a future.