

Who Will Control Tomorrow's Internet?

Net Forecasts – Peter J. Sevcik

BCR Volume 33, Number 9

September 2003

The Internet was born and has grown on a constant diet of innovation. But today, the momentum of technology deployment has slowed. If you shrug this off as an inevitable consequence of technical maturity and the sheer size of the Net, think again: Staying innovative is essential to avoid stagnation and eventual irrelevance. Important technologies are ready for deployment, and we'll regret letting them rot on the sidelines. Two examples are discussed below.

Internet Protocol version 6 (IPv6)

IPv6 was developed to prevent the Internet from running out of IP address space. And it does just that -- it increases the address space from 4×10^9 to 3×10^{38} . Moreover, it also improves security and support for mobile users.

But instead of embracing IPv6, the Internet community continues to put a patchwork of fixes into IPv4 -- for example, Classless Interdomain Routing (CIDR), Network Address Translation (NAT) and the private address re-use of the huge Class A address 10.0.0.0. Inertia has prevented us from making improvements.

But powerful groups *outside* the Internet are beginning to assert themselves. Sony and Panasonic have started hardwiring an IPv6 address into every product they make. And Microsoft also has well thought-out plans -- aka Project Teredo -- for IPv6. Its Teredo architecture is ostensibly a v4-to-v6 transition technology, but it also puts Microsoft in the driver's seat with a solution that tunnels v6 packets over v4 networks. The architecture specifies new functions including Teredo addresses, Teredo packet structures, Teredo clients, Teredo relays and Teredo servers.

This is not pie in the sky -- Microsoft's Windows XP Peer-to-Peer Update includes a Teredo client and the relay functionality comes in Windows XP Service Pack 1. Microsoft's claims that as "...IPv6 connectivity become ubiquitous, Teredo will be used less and less until finally it is not

used at all." Very collegial, a position Microsoft can afford to take, because Ipv6 is not moving. The Microsoft solution looks like it's here to stay.

Beyond IPv6, another important phenomenon is occurring. While the Internet was great at connecting people and computers, a new Internet of *things* is emerging. The technology of radio frequency identification (RFID) tags has been around since World War II, but Moore's law has brought the cost of the tags down to 15 cents and they'll soon be less than 5 cents each.

The basic research is finished, the standards are in place and the Auto-ID Center has been formed to lead the deployment. Big companies -- really big companies, like Wal-Mart, Gillette, Procter & Gamble, Pepsi, Johnson & Johnson -- are behind the movement to put an RFID on every product.

Auto-ID and its technology are in the hands of the Uniform Code Council (UCC), the industry group that brought us the Universal Product Code (UPC) bar codes and the RosettaNet. The Auto-ID standard defines a 96-bit format for encoding the manufacturer, object or product class, and serial number of anything a company may choose to tag. There are 88 bits of information fields, thus yielding a potential Internet of 3×10^{26} things. The RFID network will use the Internet for communications, and the value will come from both tracking and eventually more intelligent use of the RFID on the tagged device. For example, the tag could let someone know a product's location, whether it's been opened or whether it's no longer working.

The common thread in the discussion above is that the fate of IP and of other addressing structures is migrating out of the control of the traditional Internet community. When an overlay network operates and controls its own address space, it is in control of its destiny. Controlling addressing is the ultimate power (which is why the phone companies fight number portability).

The Internet of Things (based on RFIDs or burned-in IPv6 addresses) will have more "users" than today's Internet, and the IETF, ISPs and Internet vendors have virtually no influence on it.

Domain Name Service Security Extension (DNSSEC)

The domain name service (DNS) has been the most successful distributed database application in the history of computing. However, it has one big flaw: A computer can masquerade with a false name, which is one of the ways spammers hide their identity.

As we all know, spamming has turned into a huge problem. At a recent party, I was with a group of folks who were among the 'Net's earliest users but, because of spam, these pioneers use the Internet less and less. This ultimately will hurt commerce and the exchange of information, and while legislators are starting to get involved with the spam problem, their track record isn't reassuring (see "Unexpected Consequences").

More to the point, there is a technology -- DNSSEC -- that the IEFT developed more than 10 years ago and which, while it won't eliminate spam, could be a truly distributed, ubiquitous, key-distribution system, upon which a system of email authentication could be built. There currently are two credible sources of products -- a commercial implementation by Nominum, and an open-source version in BIND9 from the Internet Software Consortium -- but deployments are rare. A combination of inertia and complacency keep DNSSEC on the sidelines.

The Consequence of a Stagnant Edge

To be sure, some new Internet technologies are moving into deployment and the mainstream. MPLS is one example, and SIP is starting to displace H.323 for VOIP. These, however, are essentially for the network core; I'm worried about inertia at the network edge. If the edge does not get smarter, we lose ground.

Unexpected Consequences

If you think that Congress gets it, think again. In the early 1980s, I was working on a network design for the Air Force Strategic Air Command, and my task was to figure out how to meet the performance requirements for communications to airplanes permanently in the air somewhere over the Arctic Circle.

The communications was, you could say, "mission critical;" they conveyed instructions to the pilot about dropping nuclear bombs on the Soviet Union. These instructions took the form of a complex set of key exchanges that had to be perfectly synchronized, and it was very difficult to execute. I told the Air Force that it could be done, but only after an upgrade to the terrestrial part of the network from 2400-bps to 9600-bps modems.

I was told that couldn't be done, because Congress, in its wisdom, had written a requirement into the appropriations that no circuit could operate faster than 2400 bps. The rationale: A congressional aide was worried about the Air Force wasting taxpayers' money trying to push the state-of-the-art. He remembered reading in college that Claude Shannon, at Bell Labs, had showed the limit to *signaling* over a voice-grade line was 2400 baud, and so the aide set that limit into the appropriations bill. Unfortunately, he didn't know the difference between signaling rate and *data rate*. He also seemed oblivious to the fact that 9600 bps modems were commercially available, as were 56-kbps modems.

And so, my job was to make this application work at 2400 bps. I did, but am grateful that the President of the United States never had to really test my math.

To a certain extent, this is inevitable; as technologies change, so do power centers. Back in the days when the Internet started, we all relied on dumb circuits from the telephone company. The phone network had been around for a long time, but it focused on voice; most folks working for the phone companies didn't think that helping computers communicate was a problem worth solving. The new kids on the block called themselves Net-heads, while the old, slow technology guys were dubbed Bell-heads.

Today there is a next generation of Value-heads, who are building real application and financial benefits on top of what has become a now stogy Internet. Once the Value-heads get control of the address space that people, things and money care about, the Net-heads' hey-days will end.

Again, this cycle isn't new. Samuel Morse, the father of the telegraph, saw his creation grow, prosper and become hugely important before it fell into obsolescence. Morse experienced that entire cycle during adult lifetime; don't think it can't happen to you.

Companies Mentioned

Internet Software Consortium (www.isc.org)
Microsoft (www.microsoft.com)
Nominum (www.nominum.com)
Panasonic (www.panasonic.com)
Sony (www.sony.com)
Uniform Code Council (www.uc-council.org)

Peter Sevcik is president of NetForecast and is a leading authority on Internet traffic, performance and technology. Peter has contributed to the design of more than 100 networks, including the Internet, and holds the patent on application response-time prediction. He can be reached at peter@netforecast.com.

NetForecast provides custom consulting services on the value of new network technology. Our seasoned consultants draw on decades of experience to help clients worldwide choose new technologies, improve performance, and align infrastructure to business. We have helped leading enterprises, service providers, and vendors navigate the changing competitive landscape of the Internet economy. Please call us to discuss how we can help your information network succeed.

