



ON THE INTERNET

Part 2

By Vinton G. Cerf

In "Musings on the Internet," published in the September/October 2002 issue of *EDUCAUSE Review*, Vinton G. Cerf offered his ideas about what was happening, at that time, in the Internet world—its technology, policy, economics, and philosophy. Now, nearly two years later, he continues the discussion, touching on the topics of R&D, security, IPv6, RFID, telecom regulation, ICANN, and the Interplanetary Internet.

One of the main topics I'd like to discuss in this article is the role of higher education research and development (R&D)—particularly R&D into the issues and problems that industry is less able to explore. In addition to high-speed computer communications, broadband networking efforts, and the use of fiber, a rich service environment is equally important and is somewhat difficult for industry to explore. For example, the issues that colleges and universities encounter in wireless campus networks—dealing with security matters, with interference, with open spectrum—these are problems that industry is struggling with as well.

Vinton G. Cerf is Senior Vice President of Technology Strategy at MCI. Cerf is known as a "father of the Internet" for his work codesigning TCP/IP protocols and the architecture of the Internet.

Another example is the convergence between voice and data networking, this rich communications environment that's evolving. Higher education has an opportunity, if not an obligation, to understand and explore and try out different ways of implementing such developments. In industry today—unlike in higher education—it is very hard to find two competitors in the Internet world who have to interlink with each other or at least transfer data back and forth through, possibly, a third intermediary. Industry competitors have trouble offering end-to-end quality-of-service (QoS) capabilities or multicast or some of the other more elaborate services. Part of the reason is that the business model for this isn't too clear. If somebody is going to send you multicast packets and you're going to deliver them, you don't know the replicating effect of receiving one of these multicast packets and pumping it out. Keeping track of all the details is not very attractive. In the voice world, we do keep Call Detail Records (CDRs) and collect one hundred terabytes of data each month in order to do so. We used to have to keep these records for billing purposes, so it was just a cost of doing business, but as the competition heats up and as VoIP (Voice-over Internet Protocol) becomes a more visible part of the voice spectrum, people are beginning to look at fixed-price models. With a fixed-price model, we no longer need to collect CDRs. Setting aside the law enforcement's interest in CDRs and looking only from the service point of view, if you don't have to collect CDRs, you would rather not, because doing so costs a lot in terms of storage, transmission, and processing. And yet, if somebody sends me a high-priority packet, the question will be: does that consume more resources on my network than the best-efforts versions, and if it does, do I have to keep track of all that in order to make some kind of settlement, or can we work out a "sender keep all" kind of arrangement?

Higher education has an opportunity not so much to try out settlement arrangements in billing each other but at least to test the ability of multiple systems to deliver end-to-end QoS. There are all kinds of issues associated with this, of course. For one thing, it's not always clear that different vendors' equipment will interwork

in such a way as to produce an end-to-end QoS capability. Frequently, a vendor will say that it will provide QoS as long as both ends terminate on its network, where the vendor has some control over what's going on. That's a standard sales pitch. But can this be done through multiple networks, and if so, what are the side effects? The business questions are quite real. Even though it may not be part of the scientific community's responsibility to resolve these questions, perhaps college and university economics departments should take a look at these topics nonetheless.

Another area of interest concerns security. In the environment of a college or university campus, the notion of security and that of openness conflict with each other. Since campus facilities cost money to operate, they should be reserved for use by the people who pay for the facilities and education. On the other hand, the campus environment should be open and flexible. Clearly, there is much for higher education to explore here. And once again, this exploration can be quite beneficial to industry. Understanding what works and what doesn't work, particularly in the challenging and open environment of higher education (not counting, of course, the smart undergraduate and graduate students who will hack away into virtually anything anyway), is of real interest to industry.

In the original Internet design, the thinking was very open—which is not surprising, since the original design came out of the academic environment. The belief was that if you needed to have some kind of security, it ought to be on an end-to-end basis, and the two devices that needed to communicate securely should authenticate each other and should encrypt their traffic if exposure was an issue and should not rely on some notion of a security perimeter. In retrospect, this thinking is probably more correct than not for the simple reason that security perimeters don't seem to be working too well. For example, I sit on the board of Gallaudet University, and not too long ago, its network-

In the original Internet design, the thinking was very open—which is not surprising, since the original design came out of the academic environment.

ing people reported to the board about what had happened when some of the Internet worms had gotten loose. The thing that was most difficult for them was the "walk-in" worm. Somebody who got infected by being on the public Internet then came to the university with a laptop, plugged in behind the firewall, inside the security perimeter, and proceeded to infect everybody at the university with this worm.

Clearly, the security perimeter theory wasn't working very well in this case. But it does work for certain kinds of problems, which leads to some very interesting thinking about what I call *layered security*. The Internet operates in a layered fashion, and not all problems occur on the same layer. Security problems, in particular, occur on different layers, and therefore any mechanism that is intended to defend against various kinds of attack or other infection has to be mounted at the appropriate layer. A trivial example is somebody who goes to a lot of trouble to build an encrypted tunnel. Then, sitting in some hot spot somewhere in an airport, I build an encrypted tunnel back to the firewall that is supposed to be guarding the periphery of the campus network. I build this very solid pipe, with 128-bit or 256-bit key encryption—nothing is going to be exposed in that transmission—and I send over this pipe a piece of e-mail that has a worm attached to it. It goes through the tunnel beautifully. It is never exposed to anybody, it gets decrypted at the other end, and it then infects everything inside. Plainly, the original encryption didn't help. It's a terrible disservice to propose that encryption solves everything. It clearly doesn't. And it's a disservice to imagine that all protection can be done on one layer.

This doesn't even speak yet to things like intrusion detection and intrusion protection. There are any number of companies offering gadgets that will detect when an intrusion is taking place. But then there is this little problem of what to do with this information. Once you know that you're under attack, then what? Often some of the solutions turn out to be

academically interesting and difficult to implement. For example, suppose the router that the service provider mounts to face your campus is smart enough to look at the BGP exchanges, see which packets—which addresses—should be coming from you, and then, if there are any addresses that are coming from you and that you didn't announce as being deliverable, it would assume that's an attack with some fake-source IP addresses and would throw those packets away and raise an alarm. But how much processing power is available to apply to every packet that flows in from that interface? How much processing power is available to do packet forwarding, source-address validation, routing, and the miscellaneous other things that routers have to do? Some vintages of routers simply don't have enough processing power. So, looking at security from the research point of view, there is still much to be done.

Another topic of real importance to me is IP Version 6 (IPv6), which has taken quite a long time to go from its definition to deployment. Once again, the higher education community has an opportunity to help lead the way. The problem is not so much specification as it is implementation. There are many loose ends still associated with trying to get IPv6 fully deployed. Many pieces of software have to learn to speak v6 as well as v4. The industry has been very slow to move in this direction, partly because the consumer side has not been saying that it wants to have v6. The Defense Department has announced that it would like to be running v6 by 2008, and that certainly provides some stimulus to the industry. It would be very helpful to see worked examples, so there are initiatives under way in the United States and elsewhere to try to stimulate IPv6 deployment. But there are so many dangling participles that once again, we turn to the R&D community. Perhaps, within the subset of the Internet that colleges and universities are working with, higher education could blaze some trails showing how to get to the point of running a fully capable IPv6 system.

Of course, many might ask: "Why bother? V4 is working fine, and my NAT boxes are wonderful." My feeling is that NAT (Network Address Translation) boxes get in the way of end-to-end exper-

imentation. Plus, v6 also has this almost limitless address space. I probably should never say that, having thought that 32 bits was enough in 1977. But that was four years into the R&D program, and at the time, 4.3 billion terminations in this little four-network system struck me as being more than enough. The problem was that we didn't know we weren't going to build a production version after we demonstrated that the technology worked. The technology demonstration simply kept growing, and here we are in 2004, with a substantial amount of deployment and with a predictable expectation that at some point, we'll run out of address space. NAT boxes notwithstanding, I think the number of consumer appliances that are likely to show up with v6 capability will easily swamp the available v4 address space. Companies like Sony have asserted that they will have all of their consumer devices v6-enabled by around the end of 2005, and their consumer devices number in the tens of millions—if not hundreds of millions and eventually billions.

This brings me to another interesting phenomenon: RFID (Radio Frequency Identification) devices. These are becoming a fairly hot topic because they are already in use today, most typically for travel on toll roads. A burst of radio energy provides enough power that these little RFID devices can regurgitate some number, which can be detected by a sensory system. I admit that I always get a little nervous when I think about how this is supposed to work. There are about a half-dozen sensors, and you go through these tollbooths, and they're all radiating to get these RFID devices to spit out a number, and I think: "OK, so I'm headed down this lane, but these radio transmitters are on either side of the lane I'm in. How many other cars am I paying for as I go through this thing?" Apparently, a sophisticated piece of software figures out how to charge only one car and only one number going through each time.

I recently visited Wal-Mart and Tyson Foods, both located in Arkansas. At Wal-Mart, we started talking

about RFIDs. Wal-Mart has told its vendors that it wants all of its products to have RFID labels on them. This makes a lot of sense. Wal-Mart does \$248 billion in business every year (\$1.4 billion just for the day after Thanksgiving in 2003). Wal-Mart says that the fundamental problem limiting its rate of growth in income is getting people through the checkout stands and out the door. Here is what Wal-Mart wants: when the shopper walks through the checkout stand, pushing a cart, this big blast of radio energy will pick up all the RFID chips and figure out what to charge.

Setting aside the commercial aspect, let's think about shelf life. RFID sensors could conceivably be used to figure out when things should be taken off the shelves—which would be very useful, especially for pharmaceuticals. Hospitals, which distribute pharmaceuticals to lots and lots of people, would like to ensure that they don't deliver the wrong medication to a patient. An RFID chip could be placed on a plastic tag to match up with the RFID that is associated with the medication.

Tyson Foods is planning on putting these RFID chips onto every chicken that it ships. Tyson—one of the largest shippers of chicken, pork, and beef product—discovered that in big boxes full of chickens, the RFID signal did not penetrate the chickens that were on the inside because the chickens are 80 percent water and radio doesn't go through water very well. This is an interesting research topic: to see how radio propagates through chickens. We didn't solve the problem at Tyson, but I assume the solution will be a combination of the size of the box and how the chickens are packaged and which direction the RFID chips are facing when they are placed in the box.

RFID chips will lead to some interesting product developments. A refrigerator with an RFID chip could sense when something is placed in the appliance. If the refrigerator is Internet-enabled, it will surf the Net looking for recipes that use the ingredients that are inside the refrigerator, and it will

think the number of consumer appliances that are likely to show up with v6 capability will easily swamp the available v4 address space.

Value-added pricing will still be incurred, but basic services may eventually become just part of being on the Net.

show the recipes on a liquid crystal display. Or maybe the refrigerator will send out an e-mail that says: "Don't forget the marinara sauce. I've got everything else I need for a spaghetti dinner tonight."

Another topic I'd like to discuss is the telecom industry, which is in a state of enormous flux right now. The business models of yesterday will not apply tomorrow. One example is the history of voice telephony. Whereas we used to have time- and distance-sensitive charging, the industry is now going to fixed-price charges. More critically, as VoIP becomes a reality, there soon may not be any cost for voice service at all. When MCI started MCI Mail in 1983, it charged one dollar for each e-mail and was paid one dollar for each e-mail. Today, no one is willing to pay for e-mail, especially given that 70 percent of it is spam. E-mail became an adjunct to being on the Internet. The same is going to be true, I think, for many voice services, for conferencing, and for the other kinds of collaborative tools that need to identify multiple parties and have them all communicate in some secure fashion. Value-added pricing will still be incurred, but basic services may eventually become just part of being on the Net.

The reason this is an issue for higher education is that colleges and universities rely on some very fundamental transmission facilities in order to build all the elaborate systems they use on a day-to-day basis. If the business models of the telecom industry begin to fail, the telecom industry is going to have to adjust. Many in the industry are doing this by cutting staff and trying to improve the efficiency of operations, but at some point, the business model of simply cutting costs may not work. Colleges and universities thus need to be careful in their dealings with the telecom industry because by negotiating advantageous agreements, they may be accelerating the rate of failure for the current business model.

I am not saying that colleges and universities should not fight for the best price they can get. But I am saying that higher education should start thinking about what the future looks like in a telecom

world, which is dominated by IP-based communications and the natural inclination to pay nothing for any of the services that can be produced at the edge of the Net. Can we sustain the transmission industry without much value added? Industry, of course, is going to work very hard to provide more elaborate kinds of services, including things like grid computing.

A related point here is regulation. Historically, telecom regulation in the United States has been vertical in character. That is, the service and the underlying substructure are regulated as one thing. Telephone service, which is delivered over a twisted pair, is regulated separately from radio and television, which are delivered over the air and are regulated separately from cable television, which uses yet another transmission medium. But the vertical treatment of these different pieces of the telecom industry may no longer be the right model.

A new, proposed model recognizes that the Internet is layered and that as the Internet penetrates and becomes much more the common framework for most telecommunications, the equivalents of radio and television and voice telephony will be conducted over the Internet, just as Web surfing and e-mail and all these other applications are now done over the Internet. So we need to start thinking about what it means to regulate an industry that is IP-centric. We aren't there yet, and we won't be there for quite a long time. But the Internet-induced regulatory posture has some interesting characteristics. For one thing, the Internet packets don't care what the underlying transmission system is. They're happy to go over a satellite link or over an optical fiber or through a radio transmission or through a coaxial cable. They also don't care what they're carrying—whether it is a piece of video or voice or an e-mail or a Web page.

Thus, the idea of regulating by functionality is replaced by a layered structure. This leads to another important issue: regulation or enforcement at the wrong layer. For example, a court in Pennsylvania ordered MCI and other ISPs to block access to a particular Web site in Spain because

the site was alleged to have child pornography on it. None of the ISPs disputed the presence of that material, and none wanted it there, but the court order said that whoever was doing the packet-switching at the IP layer was supposed to block access. A better strategy would have been to go to the Spanish Web site and order it to take the pornographic pages out from the specific one of its 10,000 different Web services. But of course the Pennsylvania court doesn't have jurisdiction in Spain. So it looked for whoever was within its jurisdiction. MCI then had to explain that if MCI blocked that IP address, it would be blocked for everybody else in the world—not just for, maybe, people in Pennsylvania. Plus, if MCI blocked access to the site for Pennsylvania, it would also block access to everything else on that site. All 10,000 Web services and hundreds of thousands of Web pages, including the pornographic pages, would be inaccessible through the system if MCI blocked that IP address. This was the wrong layer in which to approach the problem.

We see similar problems involving concerns over copyright. I remember having a very public exchange with Jack Valenti, the head of the Motion Picture Association of America (MPAA), who wanted very much for the ISPs to detect copyrighted packets and to ring a bell whenever such packets went through the router. I said: "OK, Jack, so here's what you're asking me to do, basically. I see a packet go by, and it says, 'Call me,' and it goes on, and then a hundred packets later I get another packet that says, 'Ishmael.' I'm supposed to figure out that this is the beginning of *Moby Dick*, and then I'm supposed to figure out that it is copyrighted material, and then I'm supposed to find out whether the person who sent it had the authority to send the copyrighted material, and then I'm supposed to ring a bell. Right?" Jack said, "Yeah." And I said: "This is really hard to do, Jack. We hardly have enough horsepower just to push the packets through the system, let alone look at them and figure out all the combinations." He said: "Oh, you guys are smart. You can do it." I didn't win the round, but I will tell you that this is, again, the wrong layer in which to approach the problem.

Another matter close to my heart is ICANN (the Internet Corporation for

Assigned Names and Numbers). The two years leading up to the first World Summit on the Information Society (WSIS), held in Geneva in December 2003, were very interesting. Another summit will be held in Tunisia in November 2005. In Geneva, the discussion about how to move the world closer to an information society led to an oddly narrow focus in several debates. For example, one idea popular among the developing countries was to establish some kind of a global fund that the developed countries would contribute to, and that the developing countries would have access to, in order to further develop information technology and its use. On the surface, this sounds like a good idea. But how will the fund be administered, and where will the money go? Will the money stop at the administration, never making it to the places where it needs to be? And there are also the usual concerns over the United Nations and its rather complex structure and overhead.

Another topic of debate was the question of Internet governance. Though the phrase *Internet governance* is quite broad, it tended to get distorted into either one of two things: (1) whatever ICANN does is Internet governance; and (2) the only things that ICANN should do are Internet governance. Either ICANN is responsible for every aspect of Internet governance; or Internet governance is all that ICANN is supposed to do. Well, the fact is that ICANN is simply responsible for overseeing the domain-name system, for recording the various parameters that are needed for Internet standards, and for allocating the IP address space for v4 and v6 addresses. That's it.

These are no longer trivial duties, of course. The job was once a fairly straightforward, almost bookkeeping-like thing to do: Jon Postel, of the USC Information Sciences Institute, did the job for twenty-five years before he died in 1998. But it has become much more complicated now. For example, concerns over who should run the top level of the country codes are becoming major issues. Before, the countries didn't even know about the Internet, so they didn't care. Members of the academic community used to do this on a voluntary basis, and they still do with regard to the root servers, for example. But in terms of the top-level domains and the

domain-name system, governments are starting to want to have a say. The problem is that there seems to be little attention paid to the other things that are a part of Internet governance. For example, what taxation policy should be followed regarding either the use of the Internet or the transactions that take place over the Net? What if there is a dispute in some business transaction? What is the jurisdiction for dispute resolution? What are the mechanisms for it? Should arbitration or litigation be used, and in whose jurisdiction? What should we do about law enforcement? What should we do about fraud? What should we do about consumer complaints? What should we do about people who are defrauded by somebody on the Internet? Are these problems the responsibility of ICANN? Some people claim that ICANN should stop spam by revoking registration in the domain-name system for anybody who is caught sending spam. Of course, this suggestion takes the naïve view that the "from" address in the e-mail that arrives with spam is the actual source of the spam.

ICANN is trying to stay focused on its assigned roles and not grow its mandate, because some of these other issues are well beyond the ability of any one organization to deal with. I would like to suggest two things. One is that ICANN *should* stay small and should keep close, in terms of its mandate, to the technical side of the Internet: just trying to make sure that the domain-name system works and that everybody gets addresses when they need them. Second, I suggest that the other parts of governance should go to whatever appropriate national or international body can be created or already exists. We need to avoid mission creep at ICANN, and we need to make sure that we don't put governance issues such as taxation and law enforcement into what should be a technically driven aspect of Internet operation.

Finally, I'd like to give a quick update on the status of the Interplanetary Internet (IPN). I spent the last five years working, off and on, with the Jet Propulsion Laboratory. (By the way, MCI has

given me some time to do this, but MCI is not planning to build an interplanetary network.) Since 1998, I have been working with a small group of engineers on the design of an interplanetary extension of the Internet. In the process, we have had to unlearn virtually all of our intuitions about the design of protocols. For example, the notion of *now* actually means very different things, depending on distance. There really is no such thing as *now* because even at the speed of light, whatever is happening *now* is not going to be detectable for a while longer to somebody who is 35 million miles away. When Earth and Mars are at their closest, as they were recently, the round-trip time between the two is something like five minutes. And when they are the farthest apart in their respective orbits, the round-trip time is forty minutes. Think about doing TCP/IP with a forty-minute round-trip time. So much for flow control, right? If you say "Stop sending now" to someone on Mars, by the time the person hears you, you've been inundated. So, doing flow control in the conventional way just doesn't work.

The domain-name system is obviously not a good thing on an interplanetary basis either. For one thing, with these deep-space missions, the data rate for sending to the space platforms is much lower than the data rate for receiving from the platforms. Part of the reason for this is that the platform devices are physically smaller and have very little power. We've built these big, 70-meter dishes for receiving these wonderful transmissions from the Spirit and Opportunity rovers, but the rovers themselves have very tiny antennas. So we can send perhaps 10 to 100 kilobits per second outbound, whereas inbound we might be able to receive 1 megabit per second.

In addition, things don't stay connected. When a fiber is placed for an Internet backbone between Los Angeles and New York, the two cities don't get up and run around. Unless backhoes start digging, the fiber stays connected. But if things are in orbit around the planets, or if they are on the surface and the planets are turning,

ICANN
*should stay
small and
should keep
close, in terms
of its mandate,
to the technical
side of the
Internet.*


there is a normal disconnection from time to time because of the celestial motion. A similar situation on Earth is mobile operation. The problems in deep space—size, weight, and power, the three basic parameters for getting space platforms off the surface of Earth and out of the gravity field—are the same problems for mobility on Earth. How long can I go? How much power do I have? How long can I maintain the power? When you're carrying a laptop and a PDA and a pager and a cell phone, the last thing you want is to have to carry a 65-pound battery as well. You want lightweight stuff, and that means small amounts of power and limited lifetime.

So, we had to rethink the entire set of protocols. After we finished doing all this design for the interplanetary system, we looked at what we had done and said, "You know, this is interesting." The Interplanetary Internet is just one example of a generally delay-tolerant network, and it is also an example of an even more general disruption-tolerant network. The most recent outcome of the research has been to reapply the protocols and architecture to

terrestrial, tactical communication for the military. DARPA (Defense Advanced Research Projects Agency), which funded the original Internet work and the ARPANET and also funded the architecture of the interplanetary network, is now funding a fairly significant program in disruption-tolerant networking using some of the ideas that have come out of this research.

At this stage, the lowest two levels of the interplanetary protocols are on board the Spirit and Opportunity Mars rovers. These have been standardized, and they've gone through the CCSDS (Consultative Committee on Space Data Systems) community. We've begun looking at a Mars telecommunications orbiter, which is scheduled to be launched and put into orbit around Mars for 2009 and which we hope will contain the full suite of interplanetary protocols. We also plan to put a laser on board that spacecraft. This has a possibility of getting data at a rate of maybe one hundred megabits a second from Mars through the laser transmission instead of the standard RF transmission. Scientists can get a lot more in-

formation from Mars if we can just transmit it fast enough. So, the 2009 mission looks like an exciting possibility.

In conclusion, as a member of the vendor community, I would like to thank those of you in the higher education community for the R&D that you perform. We need as much light as possible shed on all the paths that we may go down. Only with this light can we hope to avoid existing traps and to succeed in delivering high-quality services to the public. 

RELATED RESOURCE



Emerging networking opportunities and issues, spanning the spectrum of academic and administrative areas in higher education, are the focus of Net@EDU. Information on working groups, meetings, events, and publications can be found on the EDUCAUSE Net@EDU Web site: (<http://www.educause.edu/netatedu/>).