Blown to Bits

Your Life, Liberty, and Happiness After the Digital Explosion

Hal Abelson
Ken Ledeen
Harry Lewis

Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and the publisher was aware of a trademark claim, the designations have been printed with initial capital letters or in all capitals.

The authors and publisher have taken care in the preparation of this book, but make no expressed or implied warranty of any kind and assume no responsibility for errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of the use of the information or programs contained herein.

The publisher offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact:

This Book Is Safari Enabled

The Safari® Enabled icon on the cover of your favorite technology book means the book is available through Safari Bookshelf. When you buy this book, you get free access to the online edition for 45 days.

Safari Bookshelf is an electronic reference library that lets you easily search thousands of technical books, find code samples, download chapters, and access technical information whenever and wherever you need it.

To gain 45-day Safari Enabled access to this book:

- Go to http://www.informit.com/onlineedition
- Complete the brief registration form
- Enter the coupon code 9SD6-IQLD-ZDNI-AGEC-AG6L

If you have difficulty registering on Safari Bookshelf or accessing the online edition, please e-mail customer-service@safaribooksonline.com.

APPENDIX

The Internet as System and Spirit

This Appendix explains how the Internet works and summarizes some larger lessons of its remarkable success.

The Internet as a Communication System

The Internet is not email and web pages and digital photographs, any more than the postal service is magazines and packages and letters from your Aunt Mary. And the Internet is not a bunch of wires and cables, any more than the postal service is a bunch of trucks and airplanes. The Internet is a system, a delivery service for bits, whatever the bits represent and however they get from one place to another. It's important to know how it works, in order to understand why it works so well and why it can be used for so many different purposes.

Packet Switching

Suppose you send an email to Sam, and it goes through a computer in Kalamazoo—an Internet *router*, as the machines connecting the Internet together are known. Your computer and Sam's know it's an email, but the router in Kalamazoo just knows that it's handling bits.

Your message almost certainly goes through some copper wires, but probably also travels as light pulses through fiber optic cables, which carry lots of bits at very high speeds. It may also go through the air by radio—for example, if it is destined for your cell phone. The physical infrastructure for the Internet is owned by many different parties—including telecommunications firms in the

U.S. and governments in some countries. The Internet works not because any-
one is in charge of the whole thing, but because these parties agree on what
to expect as messages are passed from one to another. As the name suggests,
the Internet is really a set of standards for **inter**connecting **net**works. The indi-
vidual networks can behave as they wish, as long as they follow established
conventions when they send bits out or bring bits in.

In the 1970s, the designers of the Internet faced momentous choices. One
critical decision had to do with message sizes. The postal service imposes size
and weight limits on what it will handle. You can't send your Aunt Mary a
two-ton package by taking it to the Post Office. Would there also be a limit
on the size of the messages that could be sent through the Internet? The
designers anticipated that very large messages might be important some day,
and found a way to avoid any size limits.

A second critical decision was about the very nature of the network. The
obvious idea, which was rejected, was to create a "circuit-switched" network.
Early telephone systems were completely circuit-switched. Each customer was
connected by a pair of wires to a central switch. To complete a call from you
to your Aunt Mary, the switch would be set to connect the wires from you to
the wires from Aunt Mary, establishing a complete electrical loop between you
and Mary for as long as the switch was set that way. The size of the switch
limited the number of calls such a system could handle. Handling more simul-
taneous calls required building bigger switches. A circuit-switched network
provides reliable, uninterruptible connections—at a high cost per connection.
Most of the switching hardware is doing very little most of the time.

So the early Internet engineers needed to allow messages of unlimited size.
They also needed to ensure that the capacity of the network would be limited
only by the amount of data traffic, rather than by the number of intercon-
nected computers. To meet both objectives, they designed a *packet-switched
network*. The unit of information traveling over the Internet is a packet of
about 1500 bytes or less—roughly the amount of text you might be able to
put on a postcard. Any communications longer than that are broken up into
multiple packets, with serial numbers so that the packets can be reassembled
upon arrival to put the original message back together.

The packets that constitute a message need not travel through the Internet
following the same route, nor arrive in the same order in which they were
sent. It is very much as though the postal service would deliver only post-
cards with a maximum of 1500 characters as a message. You could send *War
and Peace*, using thousands of postcards. You could even send a complete
description of a photograph on postcards, by splitting the image into thou-
sands of rows and columns and listing on each postcard a row number, a col-
umn number, and the color of the little square at that position. The recipient

could, in principle, reconstruct the picture after receiving all the postcards. What makes the Internet work in practice is the incredible speed at which the data packets are transmitted, and the processing power of the sending and receiving computers, which can disassemble and reassemble the messages so quickly and flawlessly that users don't even notice.

Core and Edge

We can think of the ordinary postal system as having a *core* and an *edge*—the edge is what we see directly, the mailboxes and letter carriers, and the core is everything behind the edge that makes the system work. The Internet also has a core and an edge. The edge is made up of the machines that interface directly with the end users—for example, your computer and mine. The core of the Internet is all the connectivity that makes the Internet a network. It includes the computers owned by the telecommunications companies that pass the messages along.

An *Internet Service Provider* or *ISP* is any computer that provides access to the Internet, or provides the functions that enable different parts of the Internet to connect to each other. Sometimes the organizations that run those computers are also called ISPs. Your ISP at home is likely your telephone or cable company, though if you live in a rural area, it might be a company providing Internet services by satellite. Universities and big companies are their own ISPs. The "service" may be to convey messages between computers deep within the core of the Internet, passing messages until they reach their destination. In the United States alone, there are thousands of ISPs, and the system works as a whole because they cooperate with each other.

Fundamentally, the Internet consists of computers sending bit packets that request services, and other computers sending packets back in response. Other metaphors can be helpful, but the service metaphor is close to the truth. For example, you don't really "visit" the web page of a store, like a voyeuristic tourist peeking through the store window. Your computer makes a very specific request of the store's web server, and the store's web server responds to it—and may well keep a record of exactly what you asked for, adding the new information about your interests to the record it already has from your other "visits." Your "visits" leave fingerprints!

IP Addresses

Packets can be directed to their destination because they are labeled with an *IP address*, which is a sequence of four numbers, each between 0 and 255. (The numbers from 0 to 255 correspond to the various sequences of 8 bits,

from `00000000` to `11111111`, so IP addresses are really 32 bits long. "IP" is an abbreviation for "Internet Protocol," explained next.) A typical IP address is 66.82.9.88. Blocks of IP addresses are assigned to ISPs, which in turn assign them to their customers.

There are $256 \times 256 \times 256 \times 256$ possible IP addresses, or about 4 billion. In the pre-miniaturization days when the Internet was designed, that seemed an absurdly large number—enough so every computer could have its own IP address, even if every person on the planet had his or her own computer. Figure A.1 shows the 13 computers that made up the entire network in 1970. As a result of miniaturization and the inclusion of cell phones and other small devices, the number of Internet devices is already in the hundreds of millions (see Figure A.2), and it seems likely that there will not be enough IP addresses for the long run. A project is underway to deploy a new version of IP in which the size of IP addresses increases from 32 bits to 128—and then the number of IP addresses will be a 3 followed by 38 zeroes! That's about ten million for every bacterium on earth.
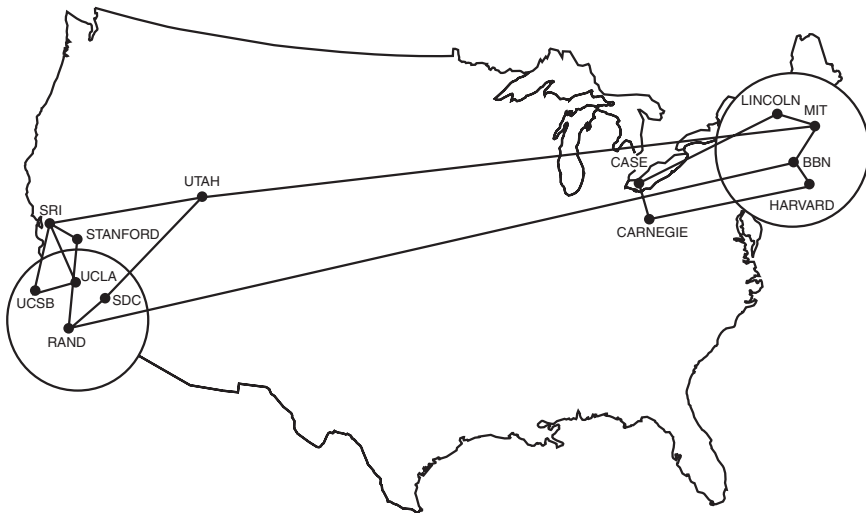
Source: Heart, F., McKenzie, A., McQuillian, J., and Walden, D., ARPANET Completion Report, Bolt, Beranek and Newman, Burlington, MA, January 4, 1978.

FIGURE A.1   The 13 interconnected computers of the December, 1970 ARPANET (as the Internet was first known). The interconnected machines were located at the University of California campuses at Santa Barbara and at Los Angeles, the Stanford Research Institute, Stanford University, Systems Development Corporation, the RAND Corporation, the University of Utah, Case Western Reserve University, Carnegie Mellon University, Lincoln Labs, MIT, Harvard, and Bolt, Beranek, and Newman, Inc.
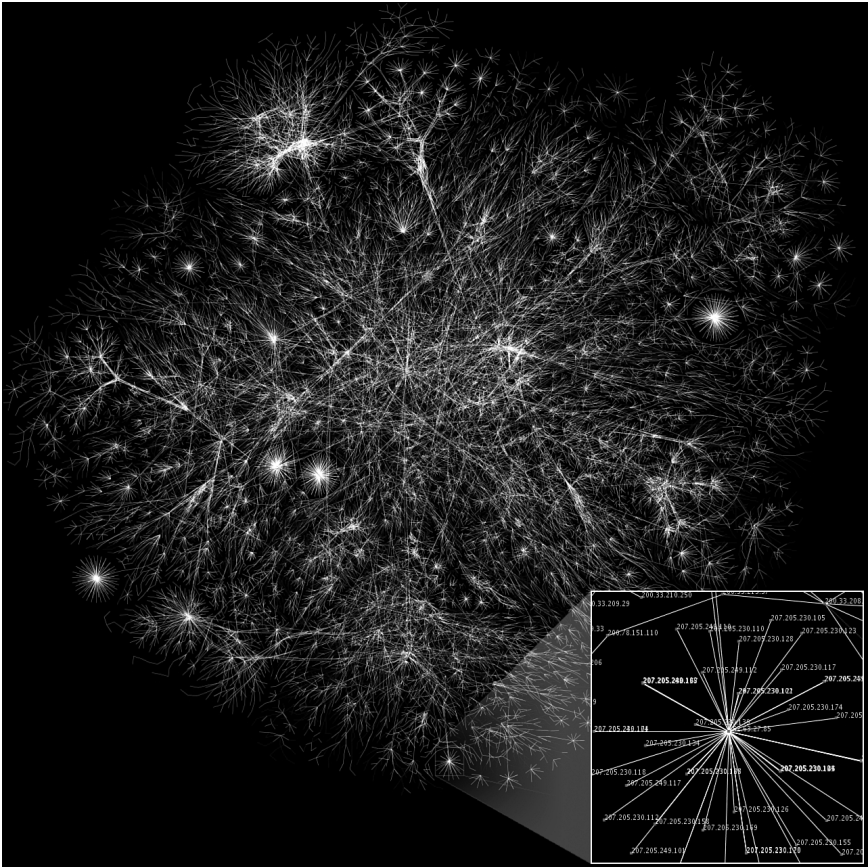
Source: Wikipedia, `http://en.wikipedia.org/wiki/Image: Internet_map_1024.jpg`. This work is licensed under the Creative Commons Attribution 2.5 License.

FIGURE A.2   Traffic flows within a small part of the Internet as it exists today. Each line is drawn between two IP addresses of the network. The length of a line indicates the time delay for messages between those two nodes. Thousands of cross-connections are omitted.

An important piece of the Internet infrastructure are the *Domain Name Servers*, which are computers loaded with information about which IP addresses correspond to which "domain names" such as harvard.edu, verizon.com, gmail.com, yahoo.fr (the suffix in this case is the country code for France), and mass.gov. So when your computer sends an email or requests a web page, the translation of domain names into IP addresses takes place before the message enters the core of the Internet. The routers don't know about domain names; they need only pass the packets along toward their destination IP address numbers.

> ### IP ADDRESSES AND CRIMES
>
> The recording industry identifies unlawful music downloads by the IP addresses to which the bits are sent. But an IP address is rarely the exclusive property of an individual, so it is hard to be sure who is doing the downloading. A provider of residential Internet service allocates an address to a home only temporarily. When the connection becomes inactive, the address is reclaimed so someone else can use it. If NAT is in use or if many people use the same wireless router, it can be impossible to establish reliably who exactly used an IP address. If you don't activate the security on your home wireless router, neighbors who poach your home network signal may get you in serious trouble by their illegal downloads!

An enterprise that manages its own network can connect to the Internet through a single gateway computer, using only a single IP address. Packets are tagged with a few more bits, called a "port" number, so that the gateway can route responses back to the same computer within the private network. This process, called *Network Address Translation* or *NAT*, conserves IP addresses. NAT also makes it impossible for "outside" computers to know which computer actually made the request—only the gateway knows which port corresponds to which computer.

The Key to It All: Passing Packets

At heart, all the core of the Internet does is to transmit packets. Each router has several links connecting it to other routers or to the "edge" of the network. When a packet comes in on a link, the router very quickly looks at the destination IP address, decides which outgoing link to use based on a limited Internet "map" it holds, and sends the packet on its way. The router has some memory, called a *buffer*, which it uses to store packets temporarily if they are arriving faster than they can be processed and dispatched. If the buffer fills up, the router just discards incoming packets that it can't hold, leaving other parts of the system to cope with the data loss if they choose to.

Packets also include some redundant bits to aid error detection. To give a simple analogy, suppose Alice wants to guard against a character being smudged or altered on a post card while it is in transit. Alice could add to the text on the card a sequence of 26 bits—indicating whether the text she has put on the card has an even or odd number of As, Bs, ..., and Zs. Bob can check whether the card seems to be valid by comparing his own reckoning with the 26-bit "fingerprint" already on the card. In the Internet, all the

routers do a similar integrity check on data packets. Routers discard packets found to have been damaged in transit.

The format for data packets—which bits represent the IP address and other information about the packet, and which bits are the message itself—is part of the *Internet Protocol*, or IP. Everything that flows through the Internet—web pages, emails, movies, VoIP telephone calls—is broken down into data packets. Ordinarily, all packets are handled in exactly the same way by the routers and other devices built around IP. IP is a "best effort" packet delivery protocol. A router implementing IP tries to pass packets along, but makes no guarantees. Yet guaranteed delivery is possible within the network as a whole—because other protocols are layered on top of IP.

Protocols

A "protocol" is a standard for communicating messages between networked computers. The term derives from its meaning in diplomacy. A diplomatic protocol is an agreement aiding in communications between mutually mistrustful parties—parties who do not report to any common authority who can control their behavior. Networked computers are in something of the same situation of both cooperation and mistrust. There is no one controlling the Internet as a whole. Any computer can join the global exchange of information, simply by interconnecting physically and then following the network protocols about how bits are inserted into and extracted from the communication links.

The fact that packets can get discarded, or "dropped" as the phrase goes, might lead you to think that an email put into the network might never arrive. Indeed emails can get lost, but when it happens, it is almost always because of a problem with an ISP or a personal computer, not because of a network failure. The computers at the edge of the network use a higher-level protocol to deliver messages reliably, even though the delivery of individual packets within the network may be unreliable. That higher-level protocol is called "Transport Control Protocol," or TCP, and one often hears about it in conjunction with IP as "TCP/IP."

To get a general idea of how TCP works, imagine that Alice wants to send Bob the entire text of *War and Peace* on postcards, which are serial numbered so Bob can reassemble them in the right order even if they arrive out of order. Postcards sometimes go missing, so Alice keeps a copy of every postcard she puts in the mail. She doesn't discard her copy of a postcard until she has received word back from Bob declaring that he has received Alice's postcard. Bob sends that word back on a postcard of his own, including the serial number of Alice's card so Alice knows which card is being confirmed. Of course,

Bob's confirming postcards may get lost too, so Alice keeps track of when she sent her postcards. If she doesn't hear anything back from Bob within a certain amount of time, she sends a duplicate postcard. At this point, it starts getting complicated: Bob has to know enough to ignore duplicates, in case it was his acknowledgment rather than Alice's original message that got lost. But it all can be made to work!

TCP works the same way on the Internet, except that the speed at which packets are zipping through the network is extremely fast. The net result is that email software using TCP is failsafe: If the bits arrive at all, they will be a perfect duplicate of those that were sent.

TCP is not the only high-level protocol that relies on IP for packet delivery. For "live" applications such as streaming video and VoIP telephone calls, there is no point in waiting for retransmissions of dropped packets. So for these applications, the packets are just put in the Internet and sent on their way, with no provision made for data loss. That higher-level protocol is called UDP, and there are others as well, all relying on IP to do the dirty work of routing packets to their destination.

The postal service provides a rough analogy of the difference between higher-level and lower-level protocols. The same trucks and airplanes are used for carrying first-class mail, priority mail, junk mail, and express mail. The loading and unloading of mail bags onto the transport vehicles follow a low-level protocol. The handling between receipt at the post office and loading onto the transport vehicles, and between unloading and delivery, follows a variety of higher-level protocols, according to the kind of service that has been purchased.

In addition to the way it can be used to support a variety of higher-level protocols, IP is general in another way. It is not bound to any particular physical medium. IP can run over copper wire, radio signals, and fiber optic cables—in principle, even carrier pigeons. All that is required is the ability to deliver bit packets, including both the payload and the addressing and other "packaging," to switches that can carry out the essential routing operation.

There is a separate set of "lower-level protocols" that stipulate how bits are to be represented—for example, as radio waves, or light pulses in optic fibers. IP is doubly general, in

IP OVER CARRIER PIGEON

You can look up RFC 1149 and RFC 2549 on the Web, "Standard for the Transmission of IP Datagrams on Avian Carriers" and "IP over Avian Carriers with Quality of Service." They faithfully follow the form of true Internet standards, though the authors wrote them with tongue firmly planted in cheek, demurely stating, "This is an experimental, not recommended standard."

that it can take its bit packets from many different physical substrates, and deliver those packets for use by many different higher-level services.

The Reliability of the Internet

The Internet is remarkably reliable. There are no "single points of failure." If a cable breaks or a computer catches on fire, the protocols automatically reroute the packets around the inoperative links. So when Hurricane Katrina submerged New Orleans in 2005, Internet routers had packets bypass the city. Of course, no messages destined for New Orleans itself could be delivered there.

In spite of the redundancy of interconnections, if enough links are broken, parts of the Internet may become inaccessible to other parts. On December 26, 2006, the Henchung earthquake severed several major communication cables that ran across the floor of the South China Sea. The Asian financial markets were severely affected for a few days, as traffic into and out of Taiwan, China, and Hong Kong was cut off or severely reduced. There were reports that the volume of spam reaching the U.S. also dropped for a few days, until the cables were repaired!

Although the Internet *core* is reliable, the computers on the edge typically have only a single connection to the core, creating single points of failure. For example, you will lose your home Internet service if your phone company provides the service and a passing truck pulls down the wire connecting your house to the telephone pole. Some big companies connect their internal network to the Internet through two different service providers—a costly form of redundancy, but a wise investment if the business could not survive a service disruption.

The Internet Spirit

The extraordinary growth of the Internet, and its passage from a military and academic technology to a massive replacement for both paper mail and telephones, has inspired reverence for some of its fundamental design virtues. Internet principles have gained status as important truths about communication, free expression, and all manner of engineering design.

The Hourglass

The standard electric outlet is a universal interface between power plants and electric appliances. There is no need for people to know whether their power is coming from a waterfall, a solar cell, or a nuclear plant, if all they want to

do is to plug in their appliances and run their household. And the same electric outlet can be used for toasters, radios, and vacuum cleaners. Moreover, it will instantly become usable for the next great appliance that gets invented, as long as that device comes with a standard household electric plug. The electric company doesn't even care if you are using its electricity to do bad things, as long as you pay its bills.

The outlet design is at the neck of a conceptual hourglass through which electricity flows, connecting multiple possible power sources on one side of the neck to multiple possible electricity-using devices on the other. New inventions need only accommodate what the neck expects—power plants need to supply 115V AC current to the outlet, and new appliances need plugs so they can use the current coming from the outlet. Imagine how inefficient it would be if your house had to be rewired in order to accommodate new appliances, or if different kinds of power plants required different household wiring. Anyone who has tried to transport an electric appliance between the U.S. and the U.K. knows that electric appliances are less universal than Internet packets.

The Internet architecture is also conceptually organized like an hourglass (see Figure A.3), with the ubiquitous Internet Protocol at the neck, defining the form of the bit packets carried through the network. A variety of higher-level protocols use bit packets to achieve different purposes. In the words of the report that proposed the hourglass metaphor, "the minimal required elements [IP] appear at the narrowest point, and an ever-increasing set of choices fills the wider top and bottom, underscoring how little the Internet itself demands of its service providers and users."
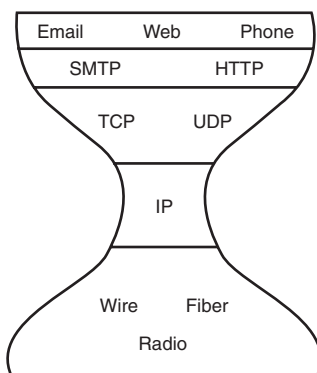

FIGURE A.3   The Internet protocol hourglass (simplified). Each protocol interfaces only to those in the layers immediately above and below it, and all data is turned into IP bit packets in order to pass from an application to one of the physical media that make up the network.

For example, TCP guarantees reliable though possibly delayed message delivery, and UDP provides timely but unreliable message delivery. All the higher-level protocols rely on IP to deliver packets. Once the packets get into the neck of the hourglass, they are handled identically, regardless of the higher-level protocol that produced them. TCP and UDP are in turn utilized by even higher-level protocols, such as HTTP ("HyperText Transport Protocol"), which is used for sending and receiving web pages, and SMTP ("Simple Mail Transport Protocol"), which is used for sending email. Application software, such as web browsers, email clients, and VoIP software, sit at a yet higher level, utilizing the protocols at the layer below and unconcerned with how those protocols do their job.

Below the IP layer are various physical protocol layers. Because IP is a universal protocol at the neck, applications (above the neck) can accommodate various possible physical implementations (below the neck). For example, when the first wireless IP devices became available, long after the general structure of the Internet hourglass was firmly in place, nothing above the neck had to change. Email, which had previously been delivered over copper wires and glass fibers, was immediately delivered over radio waves such as those sent and received by the newly developed household wireless routers.

Governments, media firms, and communication companies sometimes wish that IP worked differently, so they could more easily filter out certain kinds of content and give others priority service. But the universality of IP, and the many unexpected uses to which it has given birth, argue against such proposals to re-engineer the Internet. As information technology consultant Scott Bradner wrote, "We have the Internet that we have today because the Internet of yesterday did not focus on the today of yesterday. Instead, Internet technology developers and ISPs focused on flexibility, thus enabling whatever future was coming."

Indeed, the entire social structure in which Internet protocols evolved prevented special interests from gaining too much power or building their pet features into the Internet infrastructure. Protocols were adopted by a working group called the Internet

> **THE FUTURE OF THE INTERNET— AND HOW TO STOP IT**
>
> This excellent book by Jonathan Zittrain (Yale University Press and Penguin UK, 2008) sees the vulnerabilities of the Internet—rapidly spreading viruses, and crippling attacks on major servers—as consequences of its essential openness, its capacity to support new inventions—what Zittrain calls its "generativity." The book reflects on whether society will be driven to use a network of less-flexible "appliances" in the future to avoid the downsides of the Internet's wonderfully creative malleability.

Engineering Task Force (IETF), which made its decisions by rough consensus, not by voting. The members met face to face and hummed to signify their approval, so the aggregate sense of the group would be public and individual opinions could be reasonably private—but no change, enhancement, or feature could be adopted by a narrow majority.

The larger lesson is the importance of minimalist, well-selected, open standards in the design of any system that is to be widely disseminated and is to stimulate creativity and unforeseen uses. Standards, although they are merely conventions, give rise to vast innovation, if they are well chosen, spare, and widely adopted.

Layers, Not Silos

Internet functionality could, in theory, have been provided in many other ways. Suppose, for example, that a company had set out just to deliver electronic mail to homes and offices. It could have brought in special wiring, both economical and perfect for the data rates needed to deliver email. It could have engineered special switches, perfect for routing email. And it could have built the ideal email software, optimized to work perfectly with the special switches and wires.

Another group might have set out to deliver movies. Movies require higher data rates, which might better be served by the use of different, specialized switches. An entirely separate network might have been developed for that. Another group might have conceived something like the Web, and have tried to convince ordinary people to install yet a third set of cables in their homes.

The magic of the hourglass structure is not just the flexibility provided by the neck of the bottle. It's the logical isolation of the upper layers from the lower. Inventive people working in the upper layers can rely on the guarantees provided by the clever people working at the lower layers, without knowing much about *how* those lower layers work. Instead of multiple, parallel vertical structures—self-contained silos—the right way to engineer information is in layers.

And yet we live in an information economy still trapped, legally and politically, in historical silos. There are special rules for telephones, cable services, and radio. The medium determines the rules. Look at the names of the main divisions of the Federal Communications Commission: Wireless, wireline, and so on. Yet the technologies have converged. Telephone calls go over the Internet, with all its variety of physical infrastructure. The bits that make up telephone calls are no different from the bits that make up movies.

Laws and regulations should respect layers, not the increasingly meaningless silos—a principle at the heart of the argument about broadcast regulation presented in Chapter 8.

End to End

"End to End," in the Internet, means that the switches making up the core of the network should be dumb—optimized to carry out their single limited function of passing packets. Any functionality requiring more "thinking" than that should be the responsibility of the more powerful computers at the edge of the network. For example, Internet protocols could have been designed so that routers would try much harder to ensure that packets do not get dropped on any link. There could have been special codes for packets that got special, high-priority handling, like "Priority Mail" in the U.S. Postal Service. There could have been special codes for encrypting and decrypting packets at certain stages to provide secrecy, say when packets crossed national borders. There are a lot of things that routers might have done. But it was better, from an engineering standpoint, to have the core of the network do the minimum that would enable those more complex functions to be carried out at the edge. One main reason is that this makes it more likely that new applications can be added without having to change the core—any operations that are application-specific will be handled at the edges.

> **STUPID NETWORKS**
>
> Another way to understand the Internet's end-to-end philosophy is to realize that if the computers are powerful at the edge of the network, the network itself can be "stupid," just delivering packets where the packets themselves say they want to go. Contrast this with the old telephone network, in which the devices at the edge of the network were stupid telephones, so to provide good service, the switching equipment in the telephone office had to be intelligent, routing telephone signals to where the network said they should go.

This approach has been staggeringly successful, as illustrated by today's amazing array of Internet applications that the original network designers never anticipated.

Separate Content and Carrier

The closest thing to the Internet that existed in the nineteenth century was the telegraph. It was an important technology for only a few decades. It put

THE VICTORIAN INTERNET

That is the title of an excellent short book by Tom Standage (Berkley Books, 1999), making the argument that many of the social consequences of the Internet were seen during the growth of the telegraph. The content-carrier conflict is only one. On a less-serious level, the author notes that the telegraph, like the Internet, was used for playing games at a distance almost from the day it came into being.

the Pony Express out of business, and was all but put out of business itself by the telephone. And it didn't get off to a fast start; at first, a service to deliver messages quickly didn't seem all that valuable.

One of the first big users of the telegraph was the Associated Press—one of the original "wire services." News is, of course, more valuable if it arrives quickly, so the telegraph was a valuable tool for the AP. Recognizing that, the AP realized that its competitive position, relative to other press services, would be enhanced to the extent it could keep the telegraph to itself. So it signed an exclusive contract with Western Union, the telegraph monopoly. The contract gave the AP favorable pricing on the use of the wires. Other press services were priced out of the use of the "carrier." And as a result, the AP got a lock on news distribution so strong that it threatened the functioning of the American democracy. It passed the news about politicians it liked and omit-

MORE ON INFORMATION FREEDOM

The SaveTheInternet.com Coalition is a pluralistic group dedicated to net neutrality and Internet freedom more generally. Its member organizations run the gamut from the Gun Owners of America, to MoveOn.org, to the Christian Coalition, to the Feminist Majority. Its web site includes a blog and a great many links. The blog of law professor Susan Crawford, `scrawford.net/blog`, comments on many aspects of digital information freedom, and also has a long list of links to other blogs.

ted mention of those it did not. Freedom of the press existed in theory, but not in practice, because the content industry controlled the carrier.

Today's version of this morality play is the debate over "net neutrality." Providers of Internet backbone services would benefit from providing different pricing and different service guarantees to preferred customers. After all, they might argue, even the Postal Service recognizes the advantages of providing better service to customers who are willing to pay more. But what if a movie studio buys an ISP, and then gets creative with its pricing and service structure? You might discover that

your movie downloads are far cheaper to watch, or arrive at your home looking and sounding much better, if they happen to be the product of the parent content company.

Or what if a service provider decides it just doesn't like a particular customer, as Verizon decided about Naral? Or what if an ISP finds that its customer is taking advantage of its service deal in ways that the provider did not anticipate? Are there any protections for the customer?

In the Internet world, consider the clever but deceptive scheme implemented by Comcast in 2007. This ISP promised customers unlimited bandwidth, but then altered the packets it was handling to slow down certain data transmissions. It peeked at the packets and altered those that had been generated by certain higher-level protocols commonly (but not exclusively) used for downloading and uploading movies. The end-user computer receiving these altered packets did not realize they had been altered in transit, and obeyed the instruction they contained, inserted in transit by Comcast, to restart the transmission from scratch. The result was to make certain data services run very slowly, without informing the customers. In a net neutrality world, this could not happen; Comcast would be a packet delivery service, and not entitled to choose which packets it would deliver promptly or to alter the packets while handing them on.

In early 2008, AT&T announced that it was considering a more direct violation of net neutrality: examining packets flowing through its networks to filter out illegal movie and music downloads. It was as though the electric utility announced it might cut off the power to your DVD player if it sensed that you were playing a bootleg movie. A content provider suggested that AT&T intended to make its content business more profitable by using its carrier service to enforce copyright restrictions. In other words, the idea was perhaps that people would be more likely to buy movies from AT&T the content company if AT&T the carrier refused to deliver illegally obtained movies. Of course, any technology designed to detect bits illegally flowing into private residences could be adapted, by either governments or the carriers, for many other purposes. Once the carriers inspect the bits you are receiving into your home, these private businesses could use that power in other ways: to conduct surveillance, enforce laws, and impose their morality on their customers. Just imagine Federal Express opening your mail in transit and deciding for itself which letters and parcels you should receive!

Clean Interfaces

The electric plug is the interface between an electric device and the power grid. Such standardized interfaces promote invention and efficiency. In the

Internet world, the interfaces are the connections between the protocol layers—for example, what TCP expects of IP when it passes packets into the core, and what IP promises to do for TCP.

In designing information systems, there is always a temptation to make the interface a little more complicated in order to achieve some special functionality—typically, a faster data rate for certain purposes. Experience has shown repeatedly, however, that computer programming is hard, and the gains in speed from more complex interfaces are not worth the cost in longer development and debugging time. And Moore's Law is always on the side of simplicity anyway: Just wait, and a cruder design will become as fast as the more complicated one might have been.

Even more important is that the interfaces be widely accepted standards. Internet standards are adopted through a remarkable process of consensus-building, nonhierarchical in the extreme. The standards themselves are referred to as RFCs, "Requests for Comment." Someone posts a proposal, and a cycle of comment and revision, of buy-in and objection, eventually converges on something useful, if not universally regarded as perfect. All the players know they have more to gain by accepting the standard and engineering their products and services to meet it than by trying to act alone. The Internet is an object lesson in creative compromise producing competitive energy.

RFCs AND STANDARDS

The archive of RFCs creates a history of the Internet. It is open for all to see—just use your favorite search engine. All the Internet standards are RFCs, although not all RFCs are standards. Indeed, in a whimsically reflexive explanation, "Not all RFCs are standards" is RFC 1796.