SWCP Portal
May 2012

How the Net Works VI

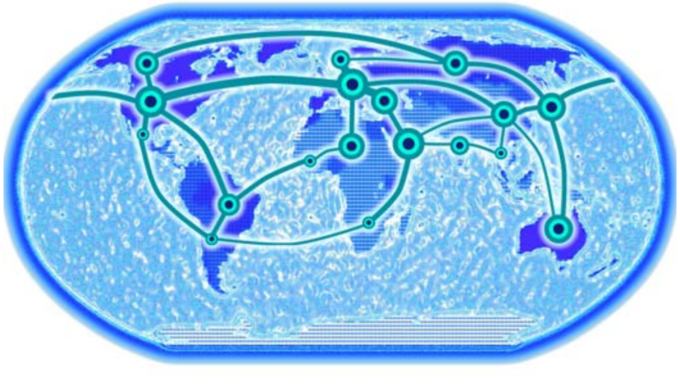
TCP/IP Makes the Net Go

Money may make the world go round, or love, or maybe just momentum, but the world of the Internet moves by a small set of rules embedded in software. Found in every computer, server, router, and Internet-enabled device from smartphones to gaming consoles to ereaders, most users know little about them and care less. Yet it is no exaggeration to say that modern life is largely now dependent on them, and will be even more so in the future.

The set of rules is referred to as the "**Internet Protocol Suite**", because that's what it operates. The "Internet" is, of course, the worldwide system of linked computing devices, a "protocol" is an agreed-upon method of doing things, and "suite" means a collection of protocols that work together. The Internet Protocol Suite, then, is simply the established ways of connecting computers. The suite contains all the methods for which the Net can be used, from moving files to Web-surfing to email to a raft of specialized services that users generally never see.

But virtually all of them (with few exceptions) depend entirely on a pair of protocols that work closely together, called "**TCP/IP**", the inelegantly named "*Transmission Control Protocol/Internet Protocol*," a real mouthful that may explain their unfamiliarity. But as the basis of all means later devised to do things, these rules are simple, rugged, and brilliant.

The real measure of their cleverness is that TCP/IP is **entirely independent** of the actual technology that connects one machine to another. TCP/IP doesn't care what sort of computer it’s in or if it's linked by a copper wire, fiber cable, radio or whatever. That's the business of some other part of the computer.



TCP/IP is the same everywhere. It performs an identical function on every machine from supercomputers to Blackberries because the Internet is not really linked by phone lines. Of all things, the Internet is actually based on the **Post Office**.

Phones v. postal models

As many people know, the Internet was invented by the US Army, through what was then called "**ARPA**", the *Advanced Projects Research Administration*, which funded university researchers. The military were big on rockets and A-bombs, both of which took huge amounts of data. It was clear that crunching numbers in their giant mainframe computers for these projects would be easier and faster if the machines could easily share the information.

The brains behind the effort, **Vint Cerf** and **Bob Kahn**, realized that just stringing wires between the boxes was insufficient. They knew the military would like to put computers everywhere - not just big mainframes in labs, but on ships, planes, even rockets. Furthermore, they realized the system would have to be open-ended, so that other devices could be plugged in or removed anywhere at any time without bringing the whole network to a screeching halt.

There were few models at that time as to how to connect large numbers of things that way. There were railroads, telephones and telegraphs, radio and the postal system. Each had advantages, but each was inefficient in different ways. Railroads were limited to one train going in one direction at a time while all others waited; telephones required a constant, open circuit to work; radio scattered information far and wide which could be intercepted or jammed.

That left the post office. While the earliest, most primitive networking solution seems the least likely choice of all, it was also the most rugged and flexible. The postal system had an overwhelming appeal to military planners during the Cold War, too, as the only network that just might survive a nuclear war.

Even if most of the country was smoking rubble, they believed that some mail would still get through. Much would be lost and many packages would have to be re-routed, but the system could still function

Continued on back

Continued from front

even if only a fraction of post offices were left standing. And to the system, it didn't matter how the mail was moved - planes, trucks, or pony express.

It was not the easiest model to emulate. The idea of "**packet switching**", that is, dividing data into small blocks like packages instead of constant streams had been around since 1961. The first experimental network between two computers across the country over the phone system in 1965 proved that sharing worked but that the telephone system was totally inadequate even under the best conditions.

1972 was a key year: email was invented by Cerf and colleagues, and ARPANET, the first packet-switching network, was demonstrated by Kahn. Shortly afterwards, Kahn developed one of the foundational concepts of the Internet, that of "**open architecture networking**". Each network could stand on its own, with no global control, and inter-network communications would involve ways of resending lost packets, but no information about the flow was kept by the boxes in between. The network would neither know nor care what kinds of information were in those flying bundles of bits.

From these simple principles stem most of the potential and the problems of the Internet. Along with the promise of a **free flow** of uncensored information from one end to the other, the lack of rigorous identification and central control allows abuse. Hence our modern world with every imaginable interest online, where rebels in the Mid-East can tweet about their struggle while hackers threaten the Pentagon and users are drowned in spam.

As Cerf put it in an interview for *Wired* recently, they wanted "a future-proof protocol" - one that wouldn't be made quickly obsolete by new gizmos. So they deliberately designed the TCP/IP structure so that it didn't know how the information was being sent. All it knew was how to take the data apart and put it back together again and send it on its way.

IP and TCP handle the addressing and transport of packets. Together they work like a very busy post office, dividing information into bundles, addressing them, sending them off and receiving them, rebuilding the data, and if any are missing, sending requests and acknowledgements. This happens on the fly, for every webpage, picture, text or voice message.

It took a long time to develop and work out the bugs, but because the protocol was not tied to any one technology, it can easily work with all. So TCP/IP will remain the basis for the Net in the foreseeable future.

Freedom of information with all its benefits and risks is **hardwired** into the very roots of the Internet by TCP/IP. All measures to monitor or limit content or access - for good or ill - are therefore **added-on applications** and thus may be vulnerable to other apps. And that's something worth remembering.

Coworking Spaces Coming Soon...

In these economically volatile times we're seeing a number or interesting new trends towards smaller businesses, sometimes made up of one or two people. These new light weight businesses have different requirements. Long term leases and expensive office space is just not something that's viable for them.

But working from home or in a noisy coffeeshop is difficult as well. It's easy to feel isolated, and cramped. Any IT problems like a broken printer or a failing network steals time from working on what you're really trying to do. And worst of all is there is no-one to bounce ideas off.

In many of the larger cities across the US and in Europe we're starting to see a new trend, called the **coworking space**. It's a comfortable place you can go for a couple of days a week to get some serious work done. High speed wifi, printers, copiers, fax machines, a break area with good coffee, and other interesting people, freelancers, entrepreneurs, and consultants to chat with. These coworking spaces usually have quiet offices if you need to meet a client, and conference rooms with white boards and projectors for group meetings.

SWCP is putting together a coworking space across the hall from our offices. We plan to open in a few weeks. If you're interested in idea of coworking and have ideas about it, please feel free to drop us a line at **coworking@swcp.com**.

FBI Server Shutdown Coming

Windows and Mac users whose machines are infected with a Trojan called "**DNS Changer**" have until **July 9** to fix their machines or else they will lose all access to the Internet.

This virus directed browsers to fake websites. It also blocked access to antivirus websites that could have eliminated it. But last year, the servers to which the browsers had been redirected were seized by the FBI.

The FBI set up safe surrogates which will be shut down this summer. To check if you have the virus, go to the DNS Changer Checkup, **www.dns-ok.us**, for an instant diagnosis and to the DNS Changer Working Group, **www.dcwg.org/fix** for repair.

Portal *editor/chief writer, Jay Nelson* **jnelson@swcp.com**