In the earliest days of the Internet, many of us who participated had no way to explain what we were doing and why it was important. Now decades later we can put “Internet service” into our budget plans or tell our families we have to travel to an “Internet meeting” and we will be understood. But as late as the year 1990 that was not possible, because the word “Internet” had no general meaning. Most of us in the industry at that time hid our companies’ Internet activities in our phone bills and, if we were up all night fixing the Internet, our explanation to our spouses would be something like “the e-mail server had a bug and I had to rewrite some of it again.”

My own early work on the Internet was in writing, fixing and enhancing the Berkeley UNIX (BSD) software used by Internet connected computers. When in 1984 I first encountered BSD UNIX and the Internet, the phrase “Open Source Software” did not exist. Much of the operating system source code for BSD UNIX was at that time copyrighted by AT&T and when programmers like myself wrote software and gave it away we called it “free software” or “public domain software”. There was no thought at first of building a career or a business around this technology: we worked on it because it was a fascinating intellectual challenge. I chose to work on the Domain Name System (DNS) because it was the first time I had heard of a hierarchical distributed autonomous reliable database and the very existence of such a thing seemed to break all the rules I knew. The Domain Name System (DNS) is the Internet’s way of translating between names like “www.caspers.it” and the underlying Internet addresses needed to actually reach Caspur’s web servers. Before DNS, this type of translation required a central database containing all known Internet names. Now that the Internet has billions of connected devices, such a central database is completely impractical. So in DNS the database where we register names like “caspers”
is in the top level IT registry. No other database operator has to know or act in order to facilitate this name, yet any user on the Internet can quickly and reliably look up the resources associated with this or with any other name among hundreds of millions of names.

Now it is both refreshing and wonderful, and also mundane and terrible, to be a part of the Internet in these days where everyone on our planet knows what an Internet is and why it’s important. The days of not being able to explain what we’re working on or to write a job description describing the skills we are looking for are gone. Instead of hiding a company’s Internet costs in the phone bill we can now request competing proposals from vendors of access, firewalls, cloud backups, spam filtering, content distribution and so on. While new categories of Internet services are always being introduced, it’s nearly always possible to explain to one’s boss why the company will benefit from buying whatever it is.

In spite of this broad growth of the knowledge and awareness on the topic, the basic infrastructure of the Internet has not changed at all. It’s still a common expense, it’s still very hard to explain and it still depends on cooperation from everyone. Every company’s and every university’s and every end user’s Internet experience will be determined by not only their own investments but also everyone else’s investments. There is no way to unilaterally improve one’s own Internet service level by investment, since to be “on the Internet” means to be connected to a network of networks where every other network determines its own level of investment. Fortunately there’s a loophole: it is not possible to unilaterally improve your own Internet service level, but it is possible to unilaterally improve everyone’s Internet service level. As a case in point, any network operator can install a DNS name server but only a few network operators can install a new DNS root name server. By “DNS root name server” I mean one of the name servers for the root zone, responsible for keeping track of all top level domains (such as .COM, .NET or .IT). There are thirteen root name server identities, each having a single letter name from “A” to “M”. My own experience is with the “F” root name server (f.root-servers.net) which is operated by Internet Systems Consortium (ISC), of which I am the Chairman and Founder. Beginning in 2002, ISC began installing and operating anycast copies of F-root in locations throughout the world. This type of anycast operation for root name servers is now fairly common, but ISC was the first root name server operator to try it. Our motivation was to make the F-root service resistant to distributed denial of service (DDoS) attacks, and we now operate about fifty copies of F-root.

The Internet overall and most services on the Internet remain quite vulnerable to DDoS attacks, by which a set of hundreds or thousands of personal computers become infected with a software virus which causes them to act in concert by transmitting Internet packets toward a single victim’s address. No victim is strong enough to withstand all possible DDoS attacks because the victim depends on their connections to other networks, and those connections and those other networks have finite capacity. On the Internet, if some criminal out there wants to prevent you from communicating or to prevent your service from being reachable by your customers, then they can unilaterally impose a DDoS attack which can almost always succeed. In order to build a DDoS-resistant Internet service it is necessary to create many identical server computers and to install these computers in diverse locations around the world. This is called anycast and it works by dividing the traffic toward your service into many small traffic flows, each answered by a local Internet server which is in the same region as the customer.

By operating fifty or so anycast copies of F-root world wide, ISC can ensure that no single DDoS attack can affect more than one or two of F-root servers. Therefore any DDoS attack against F-root will be effective in only one or at most several regions – but the service itself will never be truly “down” and most Internet users will see no service interruption for F-root no matter what kind of DDoS attack is launched or how long it lasts. This level of resiliency is necessary for the health of the Internet and for the safety of the Internet investment climate. Some things, like root name service, must always work. Any compromise on the resiliency of basic Internet in-
Infrastructure such as root name service would have chilling and far reaching effects on the Internet’s relevance in all human societies.

Since root name service is an honorable contribution to the Internet with no separate funding, the cost of creating, installing, and operating the fifty or so copies of F-root can only be by contribution. Since ISC is a non-profit public benefit company we rely on the community’s support for all of our activities including the operation of F-root. For F-root we rely on a network of sponsors around the world – including CASPUR and NaMeX – to provide the equipment, services, and financial support that makes F-root possible. Each F-root sponsor donates rack space, remote hands, power, Internet connectivity, equipment, and financial support to make it possible for ISC to operate an F-root anycast instance in their location. By reaching out to a broad worldwide audience in this way, ISC ensures that F-root’s continued resiliency is a matter of community action and not merely ISC action. This also makes it possible for responsible and community minded companies around the world to focus their energies through ISC to jointly create a root name server - F-root – that is stronger than any server that any one company could ever build.

DNS was the Internet’s first distributed application, in which location independent servers could be operated by disparate teams but still able to cooperate using a common protocol and to thus create a global information asset. Later examples of distributed Internet applications include the World Wide Web (WWW), Voice over IP (VOIP), peer to peer file sharing and Cloud Computing. All of these later distributed systems use DNS as their naming and discovery framework and, in that sense, the Domain Name System (DNS) is the bridge between the cooperative connectivity between Internet Service Providers (ISPs) and their customers and the services offered by Google, Amazon, Apple and thousands of other companies who have made the Internet their home.

I am proud of ISC’s accomplishments in helping to create and maintain the Internet and we at ISC strive to be worthy of the faith and charity shown to us by our many sponsors and customers. The Internet ecosystem must be made sustainable and must be sustained, which can only happen through the kind of cooperation that is exemplified by ISC and F-root and a worldwide network of fellow travelers.

BASIC BIBLIOGRAPHY