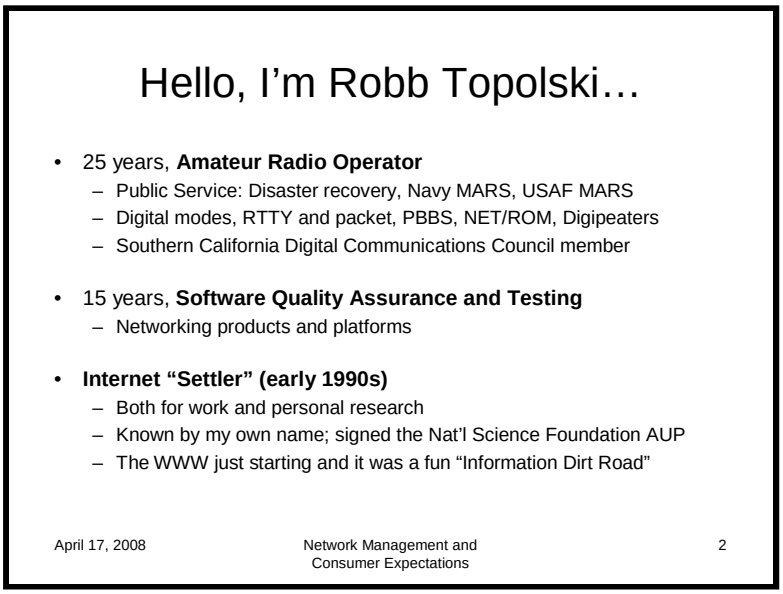
Network Management and Consumer Expectations

Robert M. “Robb” Topolski
robb@funchords.com



Thank you for inviting me to speak on this panel.

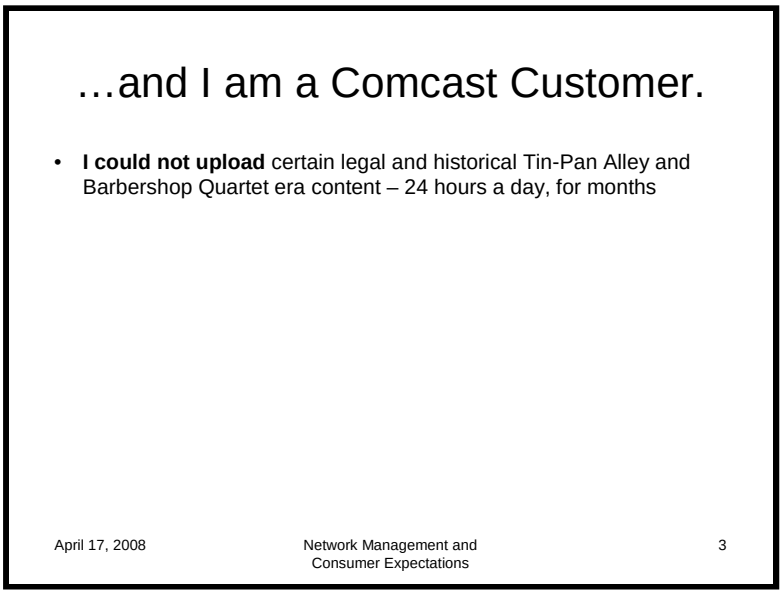
I owe my interest in technology and networking to Amateur Radio, where as a teen I was supervised by mentors "Elmers" who introduced me to digital modes over radio. Indeed, my interest in communications, protocols, and networking "physics" is deeply rooted in the concepts that I learned in those first days as a "Ham."

For the last 15 years, I've been working on Networking products and platforms, ranging from "Video Phone" software to scalable data-center servers.

(Note: My professional bio is on file with the original *Free Press, et. al.* filings in this case.

Not surprisingly, then, I took those basics with me when I became interested in an emerging medium known as the "Internet." I didn't invent it, nor were any of my innovations one of the Internet's core protocols. But when I arrived, it wasn't yet the "World-Wide-Web" or an "Information Superhighway," either. We all used our real names, many of us signed a National Science Foundation agreement promising to keep to certain standards. One of my favorite pages sat on a server called akebono.stanford.edu – known either as Jerry's List or Yet Another Hierarchical Officious Oracle – later to change its name to, simply, YAHOO. So perhaps you might think of me as an stagecoach Settler.

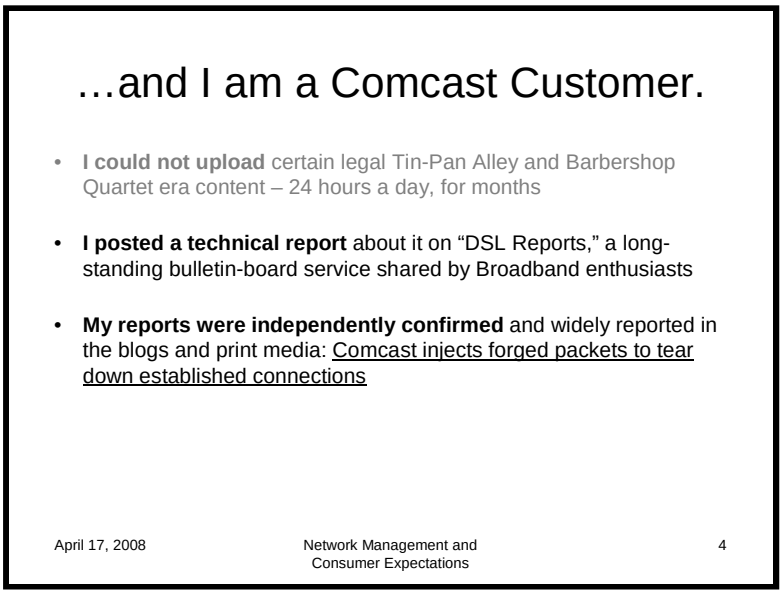
One of my first projects on the Internet was the commercial development of the NCSA Mosaic browser. Most recently, I was responsible for oversight of multiple development and testing projects concerning datacenter servers. Over the years, I have been responsible for ensuring that my company's numerous networking products behaved according to established Standards.



My work is also one of my hobbies. I have been a presenter at several software quality and testing conferences, I've worked on anti-spam and anti-phishing projects. I have helped numerous end-user consumers put together their wireless networking projects.

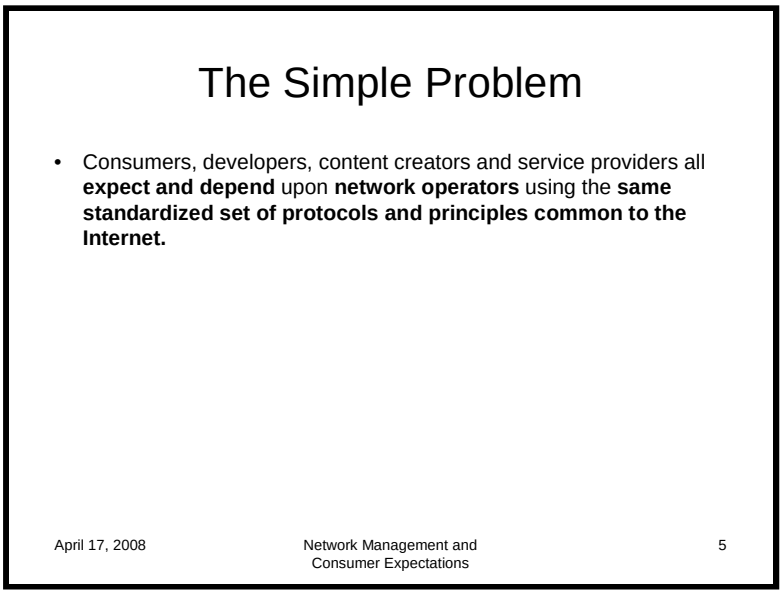
Another hobby of mine is music. Since coming to Oregon. Nine months out of the year, people in my part of the Pacific NorthWET look for ways to stay dry. I became interested in four-part barbershop harmony.

Over the years, I had collected some nice samples of printed and recorded musical history, in the old-time Barbershop Quartet style. While trying to use the Peer-to-peer networks to share this with others, I found that I was completely unable to upload any of it on the Gnutella network. This confused me, because, months earlier, an earlier attempt to share other files like these worked fine.



At first, I suspected that something new about my own configuration was at fault (I'm always changing things). After applying a packet-sniffer to the line, I found that there were several incoming Gnutella requests to download my files, but that these requests were immediately being Reset. After repeating my tests over a secure tunnel to another ISP, I found that Comcast was the common denominator. I also found that their method was one known to be associated with severe policy management – such as that used by "The Great Firewall of China" – and that a policy-management company known as Sandvine recently broke news by signing a big customer, analysts whispering the name Comcast.

As technologists are apt to do, I publically posted about my findings (http://preview.tinyurl.com/yqyow2) and the story was later picked up by blogs and news media. My findings have since been independently verified, have been covered in thousands of news articles, and are the heart of these hearings.

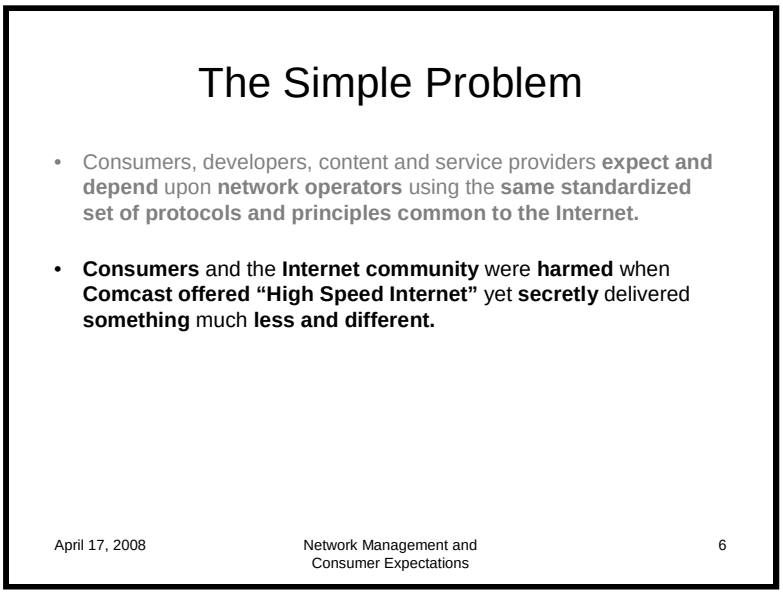


As I told the Free Press when I agreed to sign on to their FCC filing, the implications of an ISP behaving this way strikes at the heart of the freedom to innovate on the Internet.

On February's technical panel, Dr. David P. Reed said it very well: "Providing Internet Access implies adherence to a set of standard technical protocols and technical practices that are essential for the world-wide Internet to work for all its users."

I have to know, as a developer, that the Web Browser that I am developing in a lab in Santa Monica, California will work on an ISP anywhere in Africa. As a consumer, I expect that Slingbox, which was developed in Israel, will work on my Cable ISP in Hillsboro, Oregon. Each of these may have certain minimum System Requirements about the connection speed, but world-wide, developers assume that the word "Internet" means that same set of protocols and operating principles.

When you pull into a station, and fill your tank with Unleaded Gasoline, you need only concern yourself with the volume and the price. You need not concern yourself with the fundamental formula. Otherwise, the job of owning, manufacturing, repairing, or making products for cars would be much more complicated. The "Internet" has a similar quality. Since the consumers, developers, content providers, and network service providers all share a common understanding of the "Internet," there is no need to define it any further. Network requirements for currently-shipping products need not mention the various protocols presumed to be allowed across the 'net.



But, one day we did have a problem with gasoline. Dealers and suppliers toyed with their fuel sources, the formula, and their pumps. In such cases, the dealer secretly evaded gasoline taxes or the consumer received less volume, and/or a lower-quality product than expected. The ripped-off public, however, was usually none-the-wiser as all of the clues of such a scam are quite hidden from them. When the damage is done, it is too late.

Likewise, this has happened with Broadband. When Comcast offered High Speed Internet at certain "tiers" or levels of service, it secretly deployed technology to stop delivery of the upload portion of that service to some. Most non-technical customers did not notice, which was by design – Sandvine even goes as far as to warn ISPs not to go too far with its product lest it be noticed by the consumers.*

Consumers and the Internet community were harmed when Comcast offered "High Speed Internet" yet secretly delivered something much less and different.

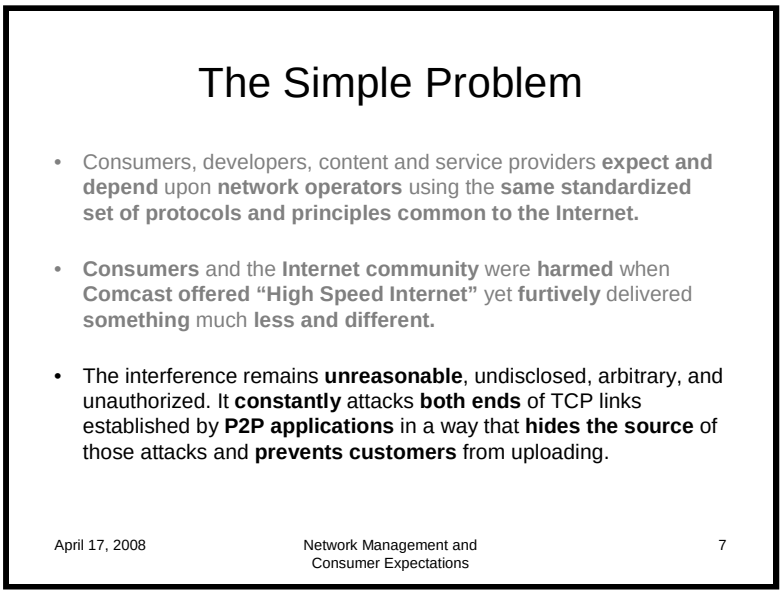
Consumers obviously got less product than their subscription called for. Developers were also harmed, who were chasing their tails as the issues reported by their users could not be reproduced.

---

*http://fjallfoss.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6519855453 (see quoted text in point 8)

RFC 1087 (dated 1989, but historically relevant – an Internet "Federalist Paper" if you will):

The […Internet Architecture Board of The Internet Society, (and the oversight board of the IETF), views…] as unethical and unacceptable any activity which purposely: (a) seeks to gain unauthorized access to the resources of the Internet, **(b) disrupts the intended use of the Internet**, (c) wastes resources (people, capacity, computer) through such actions, **(d) destroys the integrity of computer-based information**, and/or (e) compromises the privacy of users.



That denial of service, man-in-the-middle attack continues today. Using a very detailed scheme* of packet forgery that both hides the source of the attacks and rewriting certain counters to ensure that the forged packet is accepted by the end-users' networks, Comcast tears down its customers' uploading connections. This attack is presumably without regard to network congestion, as it happens regardless of the time of day or day of the week. The only common factor in these attacks is that it was a TCP connection transporting an openly-defined P2P application protocol and the application was in an uploading mode on that connection.**

One thing that was made crystal clear at the last FCC hearing on this matter, nobody sees using RST flags to tear down established and working TCP connections is an extreme act, having no place in Reasonable Network Management.

---

*__*Sandvine US Patent App 20040006643-"TCP proxy providing application layer modifications"*__ :

•[0097] State machine 100 will on occasion need to generate segments, for example when:

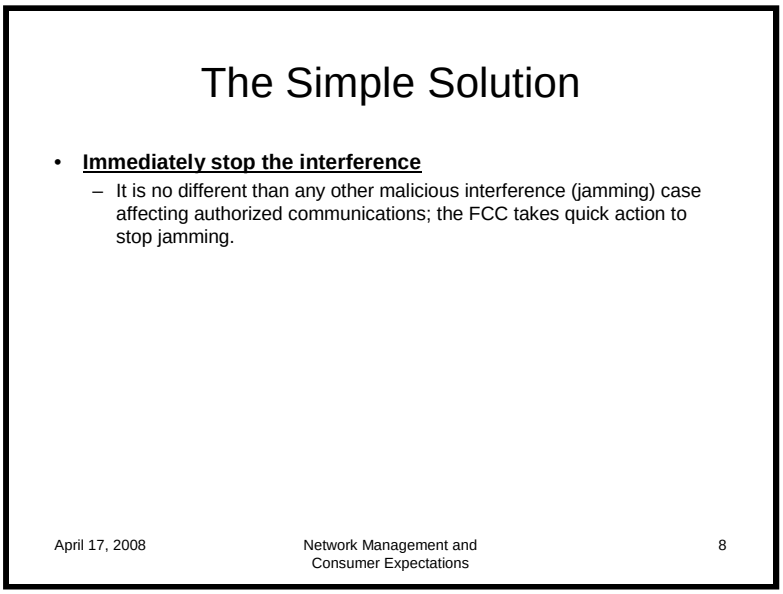
•[0098] a) sending ACK segments to the sender to force the sender's rapid re-transmit algorithm to activate;

•[0099] b) sending ACK segments to the sender when entire segments are deleted by application layer analysis module 104; and

•*[0100] c) **sending RST segments in both directions** when the flow is forcibly terminated by application layer analysis module 104.*

•[0101] This generation of segments is handled by segment generation module 106.

**http://fjallfoss.fcc.gov/prod/ecfs/retrieve.cgi?native_or_pdf=pdf&id_document=6519870563 explains about how most of Comcast's assertions are technically inaccurate.

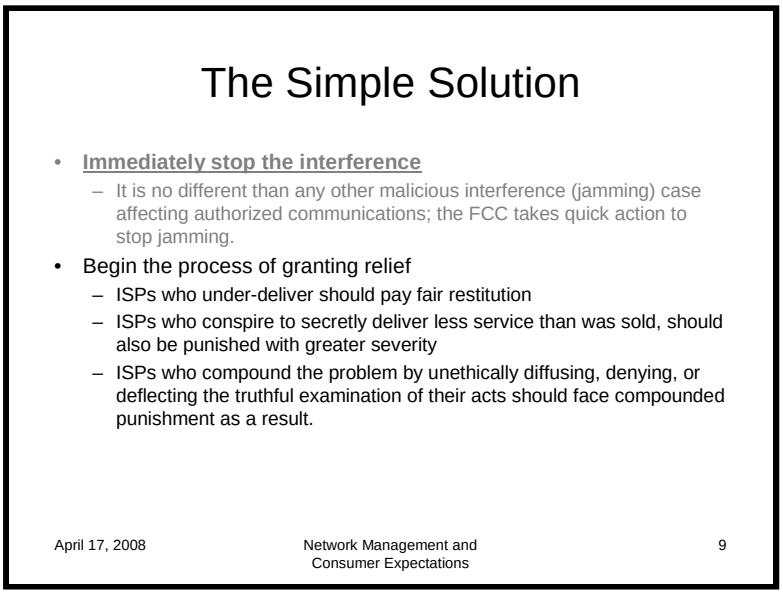


As a ham radio operator, I see this simply as – without regard to the Network Neutrality implications – a jamming complaint.

The FCC usually does a fantastic job of putting active jamming activity on the top of their list, however this period of jamming has continued from sometime in 2006 until present day – and the "Jammer" assures us that he'll stop when he's damned good and ready to change his ways – hopefully by the end of the year. This is both unprecedented and unacceptable.

The FCC probably should have acted already. Nevertheless, the FCC should take immediate action, today if possible, to enjoin Comcast from employing this technology any longer.

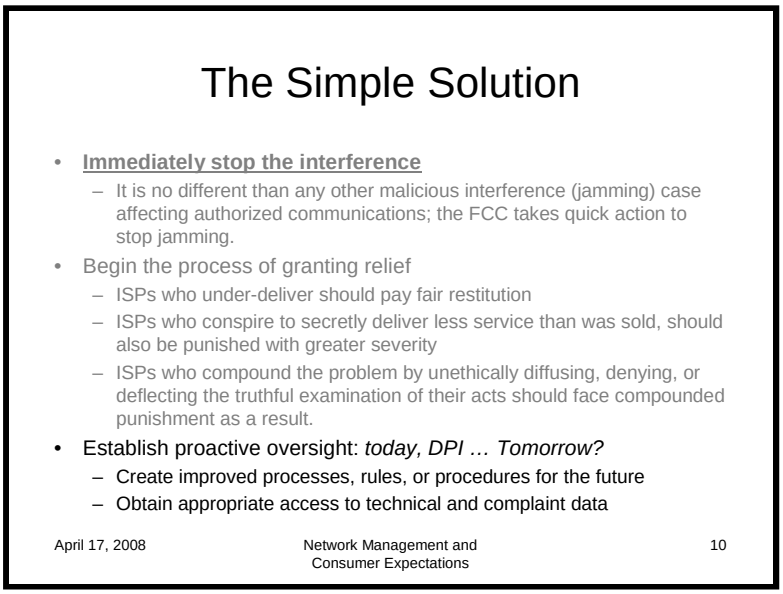
Just as there is no reasonable excuse for intentionally jamming authorized communications, forging RSTs to tear down authorized, working communication links between peers is likewise without excuse.



Aside from stopping the interference, the various complainants in this case have asked for certain relief. Considering those requests seems to be the appropriate and logical next steps in this case.

In such that we have a case of under-delivery of services – regardless if malicious or not – capture and restitution of customers' subscription fees is in order.

The government should duly investigate and determine if there are further findings of a violation of certain assurances Comcast provided to the government, or criminal acts committed, or securities-related ethical lapses, and upon such finding deliver appropriate consequences.



Finally, the FCC needs to understand that the advent of high-speed Deep Packet Inspection hardware opens up a whole new set of capabilities –

Some are good. Deep Packet Inspection might be employed by a lab or a business to prevent employee theft of Intellectual Property by looking for key words in incoming or outgoing communications. It might be specifically requested by customers who want additional parental controls to monitor participation in chat rooms and to avoid dangerous content.

It's when these new abilities challenge the bedrock principles of the Internet that require the FCC to prepare. These devices are still very new, but are currently being tested and marketed for:

a. Intercepting a subscribers' incoming web pages and changing their content, such as an ISP inserting their own ads or messages so that they appear within the web pages fetched by the consumer.
b. Passively monitoring the activity of users, without their explicit consent, and selling that information and/or delivering customized marketing campaigns based on the results.

Situations like these are extremely difficult for an end user to detect, and they're appearing in the marketplace now. A grass-roots concern known as the Network Neutrality Squad (www.nnsquad.org) is collecting such reports.

For the integrity of the Internet "product," the FCC needs to have sufficient access to the appropriate business and complaint records as well as access to "the product" to determine the validity of those complaints.