Comments on Petition by *Free Press et al.* Regarding Reasonable Internet Network Management Practices

Joseph Tucek

I, Joseph Tucek, file these comments in response to the FCC's Public Notice requesting comment on the Petition for Declaratory Ruling submitted by Free Press, *et al.*, regarding "reasonable network management". I recommend that the FCC stricty prohibit Internet Service Providers (ISPs) from considering, in any sense, the content of network traffic from making their management decisions, and that any management policy other than packet queuing or discard be carefully regulated. Modifying or forging any traffic, including RST (reset) packets, should specifically be forbidden due to the harmful effects such techniques pose, and ISPs should be strongly encouraged to use "leaky-bucket" or "token-bucket" traffic management, through packet discard, to control bandwidth usage. Finally, the Commission should be aware of, and regulate, the extent of underprovisioning (or "overselling") in Internet service, as it is the underlying cause for requiring network management.

1 Summary & Introduction

Internet access has become a fundamental element of our society. More and more, people rely on the Internet for their news, entertainment, business and personal communications, and other everyday activities [1]. One could say that Internet access, escpecially high speed access, is more important than POTS service for nearly all Americans. Because of this ubiquity of the Internet in

[1] E.g. submitting comments such as this to certain government agencies

our everyday personal and business lives, there is a compelling government interest in ensuring the smooth functioning of Internet service.

Recently, there has been a controvesy regarding the bandwidth management policies of some Internet Service Providers (ISPs)[2] Specifically, in an attempt to reduce the bandwidth usage of their "bandwidth hogs", many providers have targeted peer-to-peer (P2P) applications. P2P applications are considered to constitute a heavy drain on provider resources; hence they have been especially targetted. There are both technical and social implications to this. The technical means by which some ISPs have attempted to regulate P2P traffic represent a shortsighted and ill-advised solution to this "problem". Specifically, some ISPs have begun forging of RST (reset) packets, terminating individual P2P transfers. This intrusive forging of packets violates the design principles of the Internet, and encourages the development of alternate protocols which will ultimately be more harmful. Socially, restrictions on P2P traffic reduce the utility of the Internet, limit free discourse, and (as currently practiced by ISPs) are unfair/desceptive.

I recommend that the FCC favorably consider the petition filed by Free Press *et al.*. Additionally, I recommend the following course of action:

- The FCC should prohibit any network management practice that considers the content of network traffic. It should not be allowed to consider what the characteristics of the traffic is: video, voice, or text; legal or illegal; P2P, client-server, encrypted, plaintext, UDP, TCP, or other protocol.

- The FCC should prohibit any ISP from modifying or forging traffic, for any purpose. Of special interest is the use of forged RST packets, but other forged, modified, or inserted packets should also be forbidden.

- . The FCC should encourage the use of "leaky-bucket" or "token-bucket" traffic management, and discourage other management techniques.

- The FCC should pay attention to, and if necessary regulate, the extend of underprovisioning/overselling in Internet service. Excessive underprovisioning causes a need for intrusive

[2]Especially, but not limited to, Comcast Corporation.

network management, and entails an unfair/fraudulent practice by ISPs.

2 Technical Concerns

The Internet is built on a set of protocols. Because all of the computers follow the same protocol (speak the same language), their ability to communicate is ensured. These protocols have been carefully designed, and represent a well thought out attempt to ensure that the network as a whole functions in a wide variety of conditions. Most traffic today consists of Transmission Control Protocol (TCP), which allows reliable, in-order communication between computers. TCP is resilient to packet loss, delay, and re-ordering, and strives to limit excessive congestion. It is a far more important backbone than the physical networks themselves.

2.1 RST Forging Considered Harmful

Some ISPs have decided to manage their traffic by sending forged RST packets to both side of a TCP connection. These forged packets cause the TCP connection to terminate. Each side, when recieving the RST packet, believes that the other is no longer interested in continuing communication, and ceases transmission. As many high-bandwidth applications make use of long-lived TCP connections, such forged RST packets will reduce bandwidth usage.

However, the use of forged RST packets cannot be recommended. To make an analogy, forging RST packets is like a POTS operator interupting a call and shouting “shut up and go away” to both sides. It would clearly be outrageous if a POTS operator did this; because the RST packets are dealt with automatically, a more insideous effect occurs. Each side of the TCP connection is left believing that the other wants to terminate communication, even though both in fact would like to continue communicating.

Forged RST packets appear to both sides as a failure. The applications built above TCP respond as such, and will act as if the other host has encountered a problem. For P2P applications, this means attempting to continute the connection with an alternate peer. A well-designed P2P applications encouraged communication between “nearby” hosts; terminating these connections

causes them to use non-optimal peers which are further away, increasing the total amount of Internet traffic.

For non-P2P applications, these forged RST packets are interpeted as a real failure. For instance, consider a user using SSH to tunnel a secure remote connection. The RST packet will cause the tunnel to be closed, and the user will be informed that a the server is down (in turn, the other side will be led to believe that the user has crashed). However, both hosts are in fact functioning, and have been tricked. The application as a whole fails for no reason other than the ISPs fraudulent packets.

2.2 Potential Backlash

The authors of P2P applications are sophisticated in their understanding of networks. They will react to the inavailability of TCP by switching to other protocols. It is likely that they will use UDP as an underlying protocol, and provide reliablity themselves. However, correctly implementing congestion control is difficult, and the authors of P2P applications have no reason to do so. Without congestion control, P2P traffic will not respond to the natural indicators that the network is busy, and continue sending too much traffic. As a result, the network will become even more congested, completely negating any beneficial effect of network management.

2.3 "Reasonable Network Management"

There are traffic management techniques besides forging RST packets. Leaky bucket filtering[3] has been known for decades, and has been shown to be an effective tool for meeting any quality of service requirement[4]. Also called token bucket management, leaky bucket filtering only allows traffic to be sent if a user has sufficient "tokens"; if sufficient tokens are not available, they are queued (to a limit) until enough tokens have accumulated. Tokens are given to a user at a constant rate,

[3]Turner, J. S. "New Directions in Communications (or Which Way to the Information Age?)" IEEE Communications Magazine, vol. 24, no. 10, pp. 8-15, October 1986.

[4]Cruz, R. L. "A Calculus for Network Delay, Part I: Network Elements in Isolation" IEEE Transactions on Information Theory, vol. 37, no. 1, pp. 114-131, January 1991.

and stored in a fixed size bucket. If a user doesn't use their tokens, they overflow the bucket and "fall on the floor". The rate that tokens are added provide a limit to long-term average bandwidth use, while the size of the bucket limits the length of any "burst" traffic. Several such filters chained together allow traffic to be managed as desired.

Because excessive traffic causes congestion, which leads to increased and inefficient packet loss, TCP has been designed to reduce the speed at which traffic is sent if congestion is detected. The two primary mechanisms for detecting congestion is measuring increased latency, and measuring increased packet loss. Leaky bucket filtering, besides actually reducing the rate of traffic, triggers both congestion control mechanisms in TCP. Hence hosts will naturally reduce their traffic, while maintaining their connections. The network continues to operate as intended, with reduced total traffic.

This traffic control mechanism has been long studied, and represnts a reasonable means of controlling network traffic. Rather than work against the underlying protocols, it works with them. It does not cause applications to incorrectly conclude that a failure has occured, and is the recommended mechanism for controlling traffic.

3 Social Concerns

Briefly, I will consider non-technical concerns.

3.1 Network Neutrality

P2P applications allow individuals to transmit data amongst themselves for low cost. If many people find content interesting, they will themsleves bear the cost of transmitting it, using the bandwidth they have paid for. This has social benefits, similar to those found in the printing press, by allowing the cheap distribution of ideas. it is, for society, a good thing.

Some ISPs double as content providers. P2P content, and other Internet distributed content, competes with them in this regard. By limiting P2P traffic, or by otherwise degrading the ability of others to provide Internet content, they can make their own offerings more attractive. This is dis-

tasteful to an open society, and should be considered when determining of a network management practice is reasonable.

3.2 Consumer Rights

Network operators, by and large, are profit-seeking entities; they're in it for the money. They want to minimize their costs while maximizing their income. If they can advertise a high-speed connection without backing it up with actual infrastructure, they can make more money.

However, if they promise far more bandwidth than they are able to provide, ISPs will find themselves with a congested network which is useful for nobody. Hence, they turn to network management. By preventing their customers from using the product which they purchased, they can make it appear as if they have a high speed network, when in fact they do not. This is fradulent, and unfair to consumers.

4 Conclusions

The means by which ISPs manage their traffic should be carefully considered. Certian technicam measures are clearly improper. Further, it is important to consider the free and open spirit of the Internet when deciding if a network management practice is acceptable.