Title

A Framework for Classification of Traffic Management Practices as Reasonable or Unreasonable

Permalink
https://escholarship.org/uc/item/3ng6r1fw

Journal
ACM Transactions on Internet Technology, 10(3)

Author
Jordan, Scott

Publication Date
2010-10-01

DOI
10.1145/1852096.1852100

Peer reviewed

A Framework for Classification of Traffic Management Practices as Reasonable or Unreasonable

SCOTT JORDAN and ARIJIT GHOSH
University of California, Irvine

Traffic management practices of ISPs are an issue of public concern. We propose a framework for classification of traffic management practices as reasonable or unreasonable. We present a survey of traffic management techniques and examples of how these techniques are used by ISPs. We suggest that whether a traffic management practice is reasonable rests on the answers to four questions regarding the techniques and practices used. We propose a framework that classifies techniques as unreasonable if they are unreasonably anticompetitive, cause undue harm to consumers, or unreasonably impair free speech. We propose alternatives to unreasonable or borderline congestion management practices.

Categories and Subject Descriptors: C.2.3 [**Computer-Communication Networks**]: Network Operations; K.4.1 [**Computers and Society**]: Public Policy Issues; K.5.2 [**Legal Aspects of Computing**]: Governmental Issues

General Terms: Economics, Legal Aspects, Management

ACM Reference Format:
Jordan, S. and Ghosh, A. 2010. A framework for classification of traffic management practices as reasonable or unreasonable. ACM Trans. Intern. Techn. 10, 3, Article 12 (October 2010), 23 pages. DOI = 10.1145/1852096.1852100. http://doi.acm.org/10.1145/1852096.1852100.

1. INTRODUCTION

The traffic management practices of Internet Service Providers (ISPs) have become an issue of public debate. In 2007, Comcast started using reset packets to terminate selected peer-to-peer connections [Comcast Corporation 2008].

Portions of this work appeared in the 2009 IFIP/IEEE International Symposium on Integrated Network Management and in the 2009 International Conference on Computer Communications and Networks.
This work has been supported by National Science Foundation.
Author's address: S. Jordan, Department of Computer Science, University of California, Irvine, CA 92697; email: sjordan@uci.edu.

This practice, when uncovered by a few users, generated a firestorm of debate, largely because it dovetailed into an existing debate over net neutrality [Weitzner 2008].

Net neutrality represents the idea that Internet users are entitled to service that does not discriminate on the basis of source, destination, or ownership of Internet traffic. Proponents of net neutrality argue that without a prohibition on discrimination, ISPs may charge application providers discriminatory prices for access to dedicated bandwidth or for quality of service (QoS), or may outright block access to certain applications or Web sites, and that such activity will inhibit development of new Internet applications [Jordan 2009]. To proponents of net neutrality, Comcast's practices seemed like blocking of certain applications; to Comcast, however, its practices seemed like reasonable traffic management designed to limit network congestion.

The debate centers not only on Comcast's practices, but also on the wider use of deep packet inspection techniques which allow ISPs to identify and control traffic streams on the basis of transport and application layer information. An increasing number of vendors offer equipment that can be placed in the network to implement a variety of traffic management practices using packet classification and packet filtering.

In response to the early net neutrality debate in the United States, in 2005 the Federal Communications Commission (FCC) issued a set of principles [FCC 2005b]. The principles express the sentiment that consumers should be entitled to connect devices and to access content and applications of their choice. In a footnote, the FCC commented that these principles are subject to "reasonable network management," but did not yet define what this term means. In response to the discovery of Comcast's traffic management practices, a few organizations petitioned the FCC to rule that an ISP is violating these principles (and thus not practicing reasonable network management) when it intentionally degrades a targeted Internet application such as peer-to-peer [Free Press, Public Knowledge et al. 2007] and to adopt rules that would prevent such practices [Vuze Inc. 2007].

The FCC asked for public input on whether this practice and other traffic management practices are reasonable forms of network management [FCC 2007]. They asked whether ISPs use traffic management practices to prioritize latency-sensitive applications, to block unwanted traffic, to implement parental controls, to improve network performance, or to gain advantage over competitors. They also asked whether these practices are helpful or harmful to consumers and whether they are reasonable. In 2008, the FCC concluded that Comcast violated a principle concerning users' rights to access lawful Internet content and use applications of their choice, and that its practices did not constitute reasonable network management [FCC 2008].[1] As of the time of writing of this article, the FCC has proposed a set of rules that would delineate reasonable network management and is asking for public comment [FCC 2009]. They propose the following definition: "Reasonable network management consists

[1] As of the time of writing, this FCC Order is under review by the courts. However the authority, or lack thereof, of the FCC to issue this Order is outside the purview of this paper.

of: (a) reasonable practices employed by a provider of broadband Internet access service to: (i) reduce or mitigate the effects of congestion on its network or to address quality-of-service concerns; (ii) address traffic that is unwanted by users or harmful; (iii) prevent the transfer of unlawful content; or (iv) prevent the unlawful transfer of content; and (b) other reasonable network management practices." Many groups on both sides of the net neutrality issue have commented that this definition is too vague and have recommended revision.

These questions have largely gone unanswered by the academic networking community. Most networking technologists would have some concern about violations of layering such as that involved in deep packet inspection. However, there is no consensus about when layering violations are warranted or how to respond to them.

There have been only a few attempts in the networking literature to go beyond the technical aspects of traffic management and to consider the social and legal implications. Weitzner [2008] discusses the Comcast incident and the connections to net neutrality. Peha [2007] discusses the incentives that ISPs may have for using discriminatory practices, and the benefits and damages that may accrue from these practices. He also gives examples of what should be allowed and prohibited, but does not give a framework that allows one to classify practices. Frieden [2006] similarly gives examples of what he believes to be permissible and impermissible traffic management practices, and suggests a few best practices (including limitations on blocking and degradation) that ISPs should adopt. He similarly does not present a framework for classification, but instead proposes that the FCC should impose reporting requirements on ISPs and assess practices on a case-by-case basis. Lehr et al. [2007] discuss strategies that end-users may adopt in response to ISP discrimination, including technical counter-measures.

However, we have found no literature that proposes a method for classification of traffic management practices as reasonable or unreasonable. In this article, we present such a framework for traffic management by Internet service providers within the United States. We restrict our attention to traffic management policies as a subset of a larger class of network management policies. We consider traffic management to mitigate the effects of congestion, to address QoS, to address unwanted traffic, or to address traffic potentially harmful to the user. We do not consider here network management techniques employed by broadband Internet access providers to address illegal traffic or traffic harmful to the network, or other techniques not intended to address traffic management. To build the framework, we focus both on the technical aspects of traffic management techniques and on the goals and practices of an ISP that uses these techniques. The framework classifies traffic management practices as reasonable or unreasonable on the basis of the *technique* used and on the basis of *who* decides when the techniques are applied. The framework results in classifying practices as unreasonable when they are unreasonably anticompetitive, cause undue harm to consumers, or unreasonably impair free speech.

The article proceeds as follows. Section 2 presents a survey of traffic management techniques. In Section 3, we suggest that whether a traffic management practice is reasonable largely rests on the answers to four questions regarding the techniques and practices used. Section 4 considers examples of how these techniques are used by ISPs, and how the answers to these four questions collectively affect the degree to which a traffic management practice is reasonable. Based on these questions, in Section 5 we propose a framework that classifies techniques as unreasonable if they are unreasonably anticompetitive, cause undue harm to consumers, or unreasonably impair free speech. In Section 6, we propose alternatives to unreasonable or borderline congestion management practices that block or degrade performance for selected packets. In Section 7, we propose alternatives to unreasonable or borderline QoS practices that enhance performance for selected packets.

2. TRAFFIC MANAGEMENT TECHNIQUES

Traffic management is applied to implement a variety of functions, at a variety of layers, by a variety of actors, in a variety of manners, for a variety of purposes. To delineate these components, define a *traffic management technique* as a specific function that is offered at a specific layer. The function should determine whether traffic is transmitted and/or the rate[2] at which traffic is transmitted, or should enable such functions in other techniques. Define a *traffic management practice* as a collection of traffic management techniques, used by a specific type of actor, in a specific manner, for a specific purpose. This section presents a survey of traffic management techniques to display the range of techniques used. In Section 4, we will turn to traffic management practices, which consist of these techniques in conjunction with the actor, manner, and purpose.

Many traffic management techniques are standardized.[3] We consider them here by the layer at which they operate. Standardized *application layer* protocols such as the Real-time Transport Protocol (RTP) and the Real-time Transport Control Protocol (RTCP) collect information about the Quality of Service (QoS) experienced by a stream; this information can be used by other application layer traffic management techniques such as streaming (discussed in the following).

Transport layer traffic-management techniques control the rate at which sources transmit. In the Transmission Control Protocol (TCP), the Datagram Congestion Control Protocol (DCCP), and the Stream Control Transmission Protocol (SCTP), the source dynamically modifies the rate at which it attempts to transmit based on feedback from the destination, recent round-trip times, and dropped packets or acknowledgements. The Integrated Services (IntServ)

[2] Throughout the article, the term *rate* is used to loosely refer to how much traffic is transmitted over a period of time, not the instantaneous transmission rate at the physical layer; the length of the period depends on the context.

[3] Internet standards can be found at Internet Engineering Task Force [2010]. IEEE standards can be found at IEEE [2010].

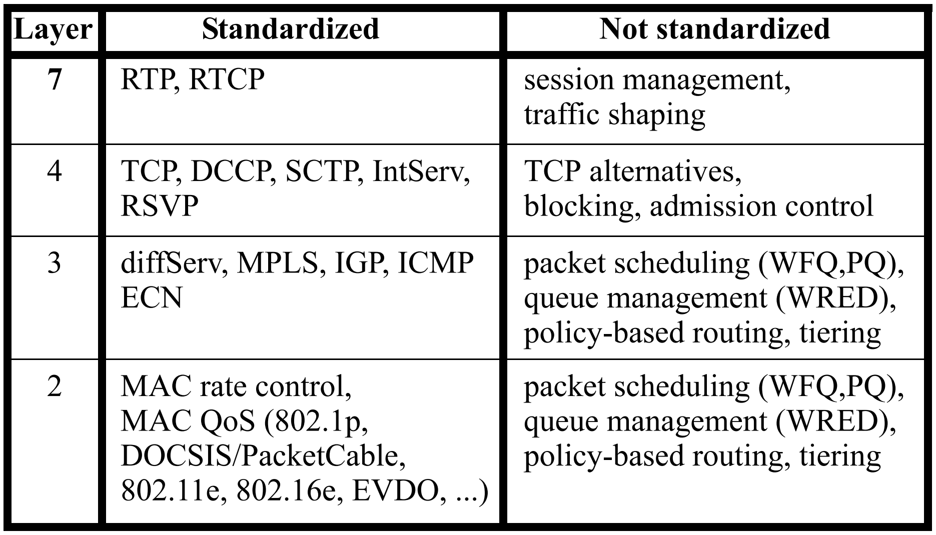
architecture, including the Resource ReSerVation Protocol (RSVP), allows for reservation of network resources and for requesting QoS; it can be used with access control, packet scheduling, queue management, and routing techniques (discussed below) to form an end-to-end QoS implementation.

Network layer traffic-management techniques affect the rate at which packets are transmitted through a network layer device such as a router. The Differentiated Services (diffServ) architecture allows for priority marking of packets and for requesting QoS; it can be used with packet scheduling, queue management, and traffic shaping techniques (discussed below) to form a QoS implementation within an Autonomous System (AS) or potentially end-to-end. Multi Protocol Label Switching (MPLS) allows for priority treatment of certain packets; it can be used in conjunction with the Interior Gateway Protocol (IGP) to provide QoS routing and/or with the IntServ architecture to provide QoS within an AS or end-to-end. Other techniques, including the Internet Control Message Protocol (ICMP) source quench message and Explicit Congestion Notification (ECN) provide information to application or transport layer protocols that can be used to modify source rates.

Data link layer traffic-management techniques determine when each individual packet can be transmitted, and often include QoS provisions. All standardized data link layer protocols, for example, IEEE 802.3 Ethernet, IEEE 802.11 Wi-Fi, and DOCSIS, incorporate algorithms that influence the rate at which a source can transmit packets. Many data link layer algorithms include functions that allow for QoS. The IEEE 802.1p protocol allows for priority marking of Ethernet packets. The DOCSIS standards implement flow prioritization and traffic shaping, and PacketCable standards add admission control and resource reservation capabilities [Miller et al. 2001]. The IEEE 802.11e protocol for Wi-Fi includes methods for admission control and prioritized transmission. The IEEE 802.16e protocol for WiMax supports QoS classes. The cell phone EV-DO standard supports QoS packet scheduling.

Many other traffic management techniques are not standardized. At the application layer, many applications incorporate proprietary traffic management techniques to control the rate at which an instance of the application transmits. Audio and video streaming applications, such as Windows Media Player, RealPlayer, and Quicktime, include proprietary algorithms that control the rate at which streams are transmitted; decisions are often based on information obtained via RTCP and RTP. Peer-to-peer protocols, such as BitTorrent DNA, and many peer-to-peer implementations of gnutella and eDonkey, include bandwidth usage algorithms. Voice over IP (VoIP) implementations such as Skype and Vonage include proprietary admission control and rate control techniques.

Also operating at the application layer, some proprietary traffic management products, such as Sandvine, use session management techniques, including termination of selected TCP connections [Sandvine Incorporated 2004]. In addition, a number of traffic management products, such as PacketShaper, include proprietary algorithms for traffic shaping which delay the transmission of selected packets and hence slow down the rate at which selected streams are forwarded through the device [Packeteer Incorporated 2007]. These products



Layer	Standardized	Not standardized
7	RTP, RTCP	session management, traffic shaping
4	TCP, DCCP, SCTP, IntServ, RSVP	TCP alternatives, blocking, admission control
3	diffServ, MPLS, IGP, ICMP ECN	packet scheduling (WFQ,PQ), queue management (WRED), policy-based routing, tiering
2	MAC rate control, MAC QoS (802.1p, DOCSIS/PacketCable, 802.11e, 802.16e, EVDO, ...)	packet scheduling (WFQ,PQ), queue management (WRED), policy-based routing, tiering

Fig. 1. Traffic management techniques.

often use Deep Packet Inspection (DPI) which involves looking at transport and application layer headers and sometimes at the application payload itself.

At the transport layer, alternatives to TCP such as Fast TCP [Wei et al. 2006] can be used to increase the rate at which sources transmit. In addition, other application and/or transport layer methods involve blocking of streams. Firewalls decide whether to forward or drop each packet based on information in the network and transport layer headers, and sometimes based on information in the application layer headers. Admission or access control techniques may decide whether to allow a new connection to be established.

At the network layer, routers implement many traffic management techniques whose operation are widely understood but have not been standardized. Packet scheduling techniques, including weighted fair queuing (WFQ) and priority queuing, determine the order in which packets are transmitted and often serve as basic building blocks for offering QoS through either the IntServ or diffServ architectures [Stiliadis and Varma 1998]. Queue management techniques, such as weighted random early detection (WRED), determine which packets are dropped and often similarly support IntServ or diffServ [Floyd and Jacobson 1993]. Policy-based routing algorithms can determine packet routes based on QoS criteria. Rate limits can be imposed to support tiering of access rates.

These traffic management techniques are summarized in Figure 1 for reference.

Which of these techniques are reasonable? We argue that a traffic management technique is not by itself acceptable or unacceptable, and that this determination must take into account how the technique is used. In the next section, we begin to consider their use.

3. KEY QUESTIONS ABOUT TRAFFIC MANAGEMENT TECHNIQUES AND PRACTICES

The previous section surveyed a wide variety of examples of traffic management techniques. In the next section, we will consider examples of how these techniques are used by ISPs to form traffic management practices. First, however, in this section we suggest that whether a traffic management practice is reasonable largely rests on the answers to four questions regarding the techniques and practices used. The first two questions apply to traffic management *techniques*, because they are directed at the layer ("where") and functionality ("what"). The second two questions apply to traffic management *practices*, because they are directed at the actor ("who") and the manner and purpose ("when").

The first question is:

(1) WHERE: Where in the network, and at which layer, is the traffic management technique applied?

We propose that the pertinent distinction should be (a) whether the technique is applied (i) at or above the transport layer versus (ii) at or below the network layer; and (b) whether the technique is applied (i) at an endpoint versus (ii) at a transit node. If a technique is applied at or above the transport layer, then good network layering practice recommends that it be applied only at an endpoint. Therefore, techniques that are applied at or above the transport layer *and* in a transit node likely violate layering; although this violation is not sufficient to make a traffic management practice unreasonable, it should raise a red flag. None of the standardized traffic management techniques discussed in the previous section is intended to be used in a manner that violates layering.[4] However, a number of nonstandardized traffic management techniques do violate layering. Proprietary products such as Sandvine [Sandvine Incorporated 2004] or PacketShaper [Packeteer Incorporated 2007] are used in transit nodes and involve DPI; this violates layering since transit node devices should not inspect transport or application layer headers or the application layer payload. Firewalls also violate layering if they are placed in transit nodes.

If a technique is applied below the transport layer, then layering allows implementation at transit nodes. For instance, guaranteed QoS can only be provided by offering QoS in every portion of the network that may experience congestion. Thus, the reasonableness of traffic management practices implemented below the transport layer may also depend on whether such techniques are available at transit nodes.

Are these practices reasonable? The answer to the "where" question alone is not sufficient to make this determination; other questions must be considered.

The second question is:

(2) WHAT: What type of traffic management functionality is applied?

[4] RSVP is a transport protocol that requires work by transit nodes, but the traffic management itself is applied at lower layers. Similarly, transport layer protocols using ECN aren't a violation of layering, since ECN is applied at the network layer.

We propose that the pertinent distinction should be whether the functionality of the traffic management technique is (i) blocking or termination of a session versus (ii) enhancement or degradation of QoS. Blocking or termination is a severe form of traffic management and should raise a red flag. In contrast, enhancement or degradation of QoS is much less severe if applied in moderation. The majority of the traffic management techniques discussed above use enhancement or degradation. A few, however, use blocking or termination. The IntServ architecture includes provisions to block new connections if adequate resources are unavailable. VoIP applications may block or terminate connections if sufficient QoS cannot be maintained. Sandvine's traffic management products can terminate selected TCP connections [Sandvine Incorporated 2007]. Firewalls are intended to block selected connections. The red flag raised by the use of blocking, therefore, is not sufficient to determine whether a practice is reasonable; other questions must be considered.

The third question is:

(3) WHO: Who decides whether the traffic management practice is applied?

We propose that the pertinent distinction should be whether the traffic management practice is applied (i) directly by a user or by an ISP only when a user desires this action versus (ii) by an ISP independent of a user's wishes. Actions taken by a user or under the user's direction are generally not deemed to be unreasonable. However, actions taken unilaterally by an ISP should raise a red flag, worthy of further investigation. Examples of each of these are given in the next section.

The final question is:

(4) WHEN: On what basis is it decided to apply the traffic management practice?

Traffic management can be used in various manners and for various purposes. Rather than relying on case-by-case analysis, we propose that the pertinent distinction should be whether the traffic management practice is applied to certain traffic on the basis of (i) the application, (ii) the source and/or destination, (iii) service provider, and/or (iv) payment. Practices applied to certain applications may be reasonable if they are done in a nondiscriminatory manner. Practices applied to traffic based on source and/or destination, however, are likely to raise a red flag out of anticompetitive concerns. Similarly, practices applied only to traffic carried by certain service providers are likely to raise a red flag for the same reason. In contrast, the reasonableness of practices applied on the basis of payment is likely to rest on the reasonableness of the payment amount. Examples of each of these are given in the next section.

4. TRAFFIC MANAGEMENT PRACTICES

In the previous section, we proposed four questions that affect the degree to which a traffic management practice is reasonable or unreasonable. In this section, we consider five examples of traffic management practices and discuss how the answers to these four questions affect their reasonableness. In the next section, we will use the lessons learned here to construct a framework for determination of whether a traffic management practice is reasonable.

First, consider the use of session management techniques that started this debate over traffic management practices. Sandvine's traffic management products are capable of identifying and terminating file-sharing connections [Sandvine Incorporated 2004; 2007]. In 2008, Comcast used products such as Sandvine to terminate TCP connections carrying BitTorrent packets used for uploading files from a Comcast subscriber to a destination outside the Comcast network, when the Comcast subscriber was not simultaneously downloading files [Comcast Corporation 2008]. For this traffic management practice, the answers to the four questions are as follows.

—*Where*: at or above the transport layer, in a transit node (red flag).
—*What*: termination (red flag).
—*Who*: by an ISP independent of a user's wishes (red flag).
—*When*: on the basis of the application and the destination (possible red flag).

This practice raises at least three red flags: (1) it violates layering, because a transit node operates at or above the transport layer; (2) it involves termination of a connection; and (3) it is done independent of a user's wishes. With so many red flags, we easily find this practice to be unreasonable. The principal reason is that causes undue harm to consumers, since as we will discuss in Section 6, there are more direct and transparent manners to limit traffic from a user. Indeed, the FCC concluded that the practice is unreasonable, by relying on the following aspects of the practice: blocking, anticompetitive harm, lack of disclosure, and lack of tailoring of the practice to combat network congestion [FCC 2008].

Next, consider another class of practices that involves blocking or termination of connections—firewalls. The answers to the four questions for firewalls are as follows.

—*Where*: at or above the transport layer (ok), at the endpoint or in transit nodes (red flag).
—*What*: blocking (red flag).
—*Who*: directly by a user or by an ISP only when a user desires this action (ok), or by an ISP independent of a user's wishes (red flag).
—*When*: on the basis of the application and/or the source and/or destination (possible red flag).

The use of firewalls as a traffic management practice can thus also raise several red flags. First, firewalls can be implemented in endpoints (e.g., Windows Firewall) or in transit nodes (e.g., in wireless routers or network gateways). When implemented in transit nodes, this is a layering violation which raises a red flag. In addition, firewalls such as parental control software can be used to block traffic from certain sources, which raises another red flag. However these uses of firewalls are universally accepted as reasonable forms of traffic management. Why? The answer is that such firewalls are under the control of the end user. In contrast, firewalls have sometimes been used by ISPs independent of a user's wishes. In 2005, Madison River Communications blocked ports used by VoIP applications, which the FCC concluded is unreasonable traffic management [FCC 2005a].

Currently, many ISPs block connections to or from specific ports to combat spam (e.g., blocking outgoing SMTP traffic to port 25) or to prohibit residential servers (e.g., blocking incoming traffic to selected server ports). While combating spam is a worthy goal, port blocking without user consent is problematic. First, an ISP is making an assumption about the application transmitting a packet when it bases the estimate upon the port. If the packet is not destined for the ISP itself, then this assumption may be incorrect. For instance, port 25 can be used by applications other than email. Second, port blocking can be anticompetitive. A subscriber may desire to send email via a port 25 SMTP server other than that of the ISP. If the ISP blocks all port 25 traffic emanating from its subscribers, this reduces competition amongst email servers. Third, there are more direct and transparent manners to limit traffic to and from a user (discussed in Section 6). Hence, we conclude that the use of firewalls in this manner is a traffic management practice that should be used only with the consent of the user. An ISP may avoid this prohibition by obtaining consent of the user. This may be done either via opt-in or opt-out techniques. Thus it is reasonable for an ISP to block outgoing port 25 traffic providing that a subscriber may opt out of such blocking.

Similarly, while ISP contracts may prohibit operation of a residential server, there are more direct and transparent manners to limit traffic to and from a user (discussed in Section 6), and this practice should be considered unreasonable. We conclude that if the "who" question is resolved in favor of user choice, then the other red flags do not matter.

What about traffic management practices that involve limited degradation of traffic without blocking or termination? Many products offer proprietary traffic shaping techniques, and a number of ISPs use these techniques to limit file-sharing traffic. The answers to the four questions for this practice is are as follows.

—*Where*: at or above the transport layer, in a transit node (red flag).

—*What*: degradation (possible red flag).

—*Who*: by an ISP independent of a user's wishes (red flag).

—*When*: on the basis of the application (possible red flag).

Many educational institutions implement this practice by configuring products such as PacketShaper to limit the network bandwidth used by file-sharing applications [Packeteer Incorporated 2008]. The practice delays the transmission of file-sharing packets and hence slows down the rate at which these streams are forwarded through the device. This type of traffic shaping could be implemented at the network layer if low-priority packets were labeled by the user. However, without the user's involvement to identify low-priority packets, products such as PacketShaper use DPI to determine which packets belong to file-sharing applications. Use of DPI classifies this practice as an application layer practice; because an application layer practice is applied at a transit node, it violates layering, which raises one red flag. A second red flag is raised because the practice is typically applied without the consent of the user. This type of practice is less severe than blocking of termination; opinions differ as to whether these two red flags are sufficient to classify the practice as unreasonable. Since there are more direct and transparent manners to limit traffic from a user (discussed in Section 6), we are reluctant to classify such techniques as acceptable. However, because these alternative practices involve different business models that may require some time to be accepted by the public, we recommend classifying traffic shaping for file-sharing traffic as a borderline traffic management practice that could be used for a limited period of time if properly disclosed in the user contract.

Next, consider another class of practices that involves limited degradation – tiering. The answers to the four questions for tiering are as follows.

—*Where*: at or below the network layer, in a transit node (ok).

—*What*: degradation (possible red flag).

—*Who*: by an ISP on the basis of a user's wishes (ok).

—*When*: on the basis of consumer payment (ok).

Tiering is typically accomplished in transit nodes (the user modem and/or ISP routers) at the data link and network layers by limiting the user download and upload rates to the maximum rates dictated in the user contract. This is a form of degradation, since the equipment is capable of transmitting at higher rates. However, since this practice is applied on the basis of user choice (and clearly displayed in user contracts), this is universally considered to be reasonable traffic management.

Finally, consider an example of a traffic management practice that involves enhancement of QoS. Currently, this is commonly used to support an ISP's own offering of VoIP or video-over-IP.

—*Where*: at or below the network layer, in transit nodes (ok).

—*What*: enhancement (possible red flag).

—*Who*: by an ISP on the basis of a user's wishes (ok).

—*When*: on the basis of the application and the service provider (possible red flag).

Enhanced QoS for real time applications such as voice and video typically requires the use of traffic management techniques that offer QoS in the data link and/or network layers in every portion of the network where congestion may occur (see, e.g., Cox Communications [2004]). When an ISP uses enhanced QoS for its own VoIP and/or video-over-IP offerings, it uses these practices within its own network. In the case of VoIP, the traffic is then transited onto the public switched telephone network which offers similar QoS. In the case of video-over-IP, the video source usually resides on the ISP's network, so the entire network path (up to the subscriber premises) is under the control of the ISP. Although the practice is applied without the ability for a user to decline this enhancement, presumably no user would desire their voice or video service to have a lower QoS. This practice does, however, raise one red flag because it is applied only to voice and/or video service offered directly by the ISP. We do not object to the use of QoS, nor to charging for QoS; however, we do believe it is an acceptable traffic management practice only if the ISP offers the same QoS service for services offered by other providers at a rate that is not unreasonably discriminatory [Jordan 2009].

5. A FRAMEWORK FOR DETERMINATION OF WHETHER A TRAFFIC MANAGEMENT PRACTICE IS REASONABLE

In the previous two sections, we proposed four questions that affect the degree to which a traffic management practice is reasonable or unreasonable, and investigated the reasonableness of five examples of traffic management practices on the basis of the answers to these questions. In this section, we propose a framework for determination of whether a traffic management practice is reasonable.

We remind the reader that we consider here only traffic management to mitigate the effects of congestion, to address QoS, to address unwanted traffic, or to address traffic potentially harmful to the user. We do not consider here network management techniques employed by broadband Internet access providers to address illegal traffic or traffic harmful to the network, or other techniques not intended to address traffic management.

The order in which the questions are considered is important. Start with one part of the “where” question, the location in the network where the traffic management technique is applied. If the technique is applied at an endpoint, we propose that it be classified as a reasonable traffic management practice regardless of the answers to the other questions. One endpoint is the user; practices applied directly by the user are not in question. The other endpoint is the entity with which the user is communicating. When this entity is an ISP, the ISP is acting in the role of an application provider. Common examples of this situation are ISPs that offer email and/or Web hosting services. However, a user can (or should be able to) receive such application services from a large number of potential providers. Since this market is competitive, practices applied at an endpoint that negatively impact the user’s experience may drive users to change application providers, buy they need not change their ISP. Therefore, any traffic management practice applied at an endpoint should be classified as reasonable. In contrast, if the traffic management practice is applied at a transit node, we must consider the remaining questions.

Next consider the “who” question, namely who decides whether the traffic management practice is applied. If the traffic management practice is applied directly by a user or by an ISP only when a user desires this action, we propose that it should be classified as a reasonable traffic management practice because the user has control over whether the practice is applied. Such practices are common, and include many firewalls, parental control software, and tiering. If an ISP were to provide enhanced QoS for voice or video purely on the basis of consumer payment, then this payment for QoS would not be discriminatory and we propose that it be classified as a reasonable traffic management practice. In contrast, if the traffic management practice is an action taken unilaterally by an ISP, then it is worthy of further investigation. If a practice is used without user consent, then we believe it should be disclosed in sufficient detail in the user contract. If so disclosed, then we must consider the remaining questions to determine if it is a reasonable practice.

Before progressing to these remaining questions, however, we should limit the scope of the traffic management practices considered here. We consider only techniques that are applied to networks such as the the Internet that use a public right-of-way; private networks are free of such regulation. We consider only techniques that affect Internet applications; if an ISP offers a voice service under Title II of the Communications Act (which regulates common carriers) or offers a video service under Title VI of the Communications Act (which regulates cable communications), then these restrictions need not apply. We consider only lawful uses; ISP rights to detect and interfere with illegal uses are addressed elsewhere in law. We consider only nonharmful uses of the network; security measures may require special considerations. We do not consider issues of privacy, which intersect with many of the techniques discussed here but which require considerations beyond those detailed here. Finally, prohibition of unreasonable practices should implemented only where sufficient competition does not exist; Title I of the Communications Act includes a provision which instructs the FCC to forbear from applying regulations unless they are in the public interest and required to ensure just and reasonable practices. Toward this end, regulation of reasonable traffic management should only apply to access networks, specifically to the portions of an ISP's network which must be transversed to form routes from the Internet to its subscribers.

The next aspect to be considered is the "what" question, in particular whether the practice involves blocking or termination of a session versus enhancement or degradation of QoS. If the practice involves blocking or termination, we propose to classify it as unreasonable. Blocking or termination practices that are applied at a transit node without user choice are unreasonably anticompetitive, cause undue harm to consumers, or unreasonably impair free speech. When blocking is applied at a transit node without user choice on the basis of the source or destination or on the basis of the speech within the packet, the practice unreasonably impairs free speech; this type of blocking includes blocking of specific Web pages or blocking on the basis of the content of the speech. When blocking is applied at a transit node without user choice on the basis of the application, the practice is unreasonably anticompetitive and/or causes undue harm to consumers; this type of blocking includes blocking of specific applications (e.g., blocking or terminating VoIP or file-sharing connections) and blocking of specific ports (e.g., SMTP or server ports). There is no reasonable justification for the use of these techniques. In some cases, the ISP's goal may be to limit congestion, reduce spam, or implement security; however, such goals can be implemented either through less severe methods that do not involve blocking or with the consent of the user. If a traffic management practice is implemented in a transit node, without user choice, but does not block or terminate connections, we must consider the remaining questions.

Practices that enhance or degrade QoS in a transit node without user choice are the concern of the remainder of this section of the article. To address such practices, consider the "when" question, which asks on what basis is it decided to apply the traffic management practice. This question considers the manner and purpose of the practice. We propose that the pertinent distinction should be whether the traffic management practice is applied to certain traffic on the basis of (i) the application, (ii) the source and/or destination, (iii) service provider, and/or (iv) payment.

First, consider using *source and/or destination and/or service provider* as the basis. A common example of this practice is an ISP that provides enhanced QoS for its own VoIP service, but does not provide this same QoS to competitors VoIP packets. Another example of an exclusive arrangement would occur if an ISP were to provide access to enhanced or degraded QoS to some third party application providers but not others. Use of source and/or destination and/or service provider without user choice involves the use of exclusivity. Such exclusive arrangements are unreasonable, since they tilt the playing field between application providers through use of Internet infrastructure. Thus, we propose that these traffic management practices be classified as unreasonable, because they are unreasonably anticompetitive.

Next, consider using *payment* as the basis for the decision of when an ISP uses enhanced or degraded QoS. For instance, an ISP could charge a consumer for enhanced QoS for all packets to or from that subscriber. Alternatively, an ISP could charge an application provider for enhanced QoS for all packets to or from that application provider. Consumer payment for QoS places the use of the practice under the control of the user, and hence this framework would already have classified such practices as reasonable. We thus only need consider charging of application providers. We considered this case in detail in Jordan [2009]. If the price is not unreasonably discriminatory (e.g., if an ISP sells QoS to all application providers at the same price as it passes on to its own applications that require QoS), then we argued in Jordan [2009] that the practice is reasonable. However, if prices for QoS are unreasonably discriminatory, then a traffic management practice that uses such prices as the basis is unreasonable since the practice is unreasonably anticompetitive.[5]

Finally, consider cases in which the practice is applied on the basis of the *application*. In these cases, if the practice is applied entirely *at or below the network layer*, then we propose that the practice be classified as reasonable. Enhancement or degradation of QoS is thus applied to specific packets identified by the user, for instance if an ISP chose to give enhanced QoS to all packets identified using diffServ codepoints by the user as VoIP.

[5] We understand that recouping infrastructure costs through favoring one's own services is a common idea. However, we disagree with it, since this tilts the playing field between the ISP and its application competitors. We believe that an ISP should recoup the costs of QoS through reasonable charges for QoS, both to itself and to others. A level playing field requires wide availability of QoS. Our vision is that this is most easily achieved through the incorporation of QoS into peering and transit agreements. An application provider could thus pay its own ISP for QoS, and this ISP would be responsible not only for ensuring QoS within its own network but also ensuring that QoS is honored by downstream ISPs. Further discussion of this can be found in Jordan [2009].

The last remaining case consists of practices that are applied at or above the transport layer at transit nodes without user consent and enhance or degrade QoS on the basis of the application. Practices of this sort use DPI to identify which packets should receive high or low priority or dedicated bandwidth. A common example of this practice is traffic shaping for file-sharing. Because DPI is used (rather than user identification of these packets), this practice violates layering. The question is whether this violation of layering is severe enough to cause this practice to be classified as unreasonable. There are more direct techniques that can be used that rely on user identification of packet priorities and that do not violate layering, as discussed in the next section of this paper. However, because these alternative practices involve different business models that may require some time to be accepted by the public, we recommend classifying any such practice that uses DPI to apply QoS as a borderline traffic management practice that could be used for a limited period of time if properly disclosed in the user contract.

The resulting framework is summarized by the flowchart in Figure 2.

6. ALTERNATIVES TO UNREASONABLE OR BORDERLINE CONGESTION MANAGEMENT PRACTICES

In the framework proposed in the previous section, several types of practices were classified as unreasonable. Unreasonable practices are those that are implemented at transit nodes without user choice and that either block or terminate sessions or apply QoS on an exclusive or unreasonably discriminatory basis. In addition, we classify practices that use DPI to apply QoS as borderline.

ISPs that currently use unreasonable or borderline practices typically give one of the following reasons.

(1) The traffic management practice is required to ensure security.

(2) The traffic management practice is required to relieve congestion.

(3) The traffic management practice is required to ensure adequate QoS for selected traffic.

The first rationale (ensuring security) is often used to justify practices that block traffic. We believe this rationale should be divided into two categories—traffic management to address traffic potentially harmful to the user versus network management techniques employed by broadband Internet access providers to address traffic harmful to the network. With respect to the security concerns for the end user, we believe that all such practices should be subject to subscriber choice. Individual users may elect to implement their own security practices and/or to have their ISP implement these practices for them. In contrast, network management to ensure the security of the network itself, for example, distributed denial of service attacks upon the network, fall outside the scope of this article and would likely be considered to be reasonable network management.

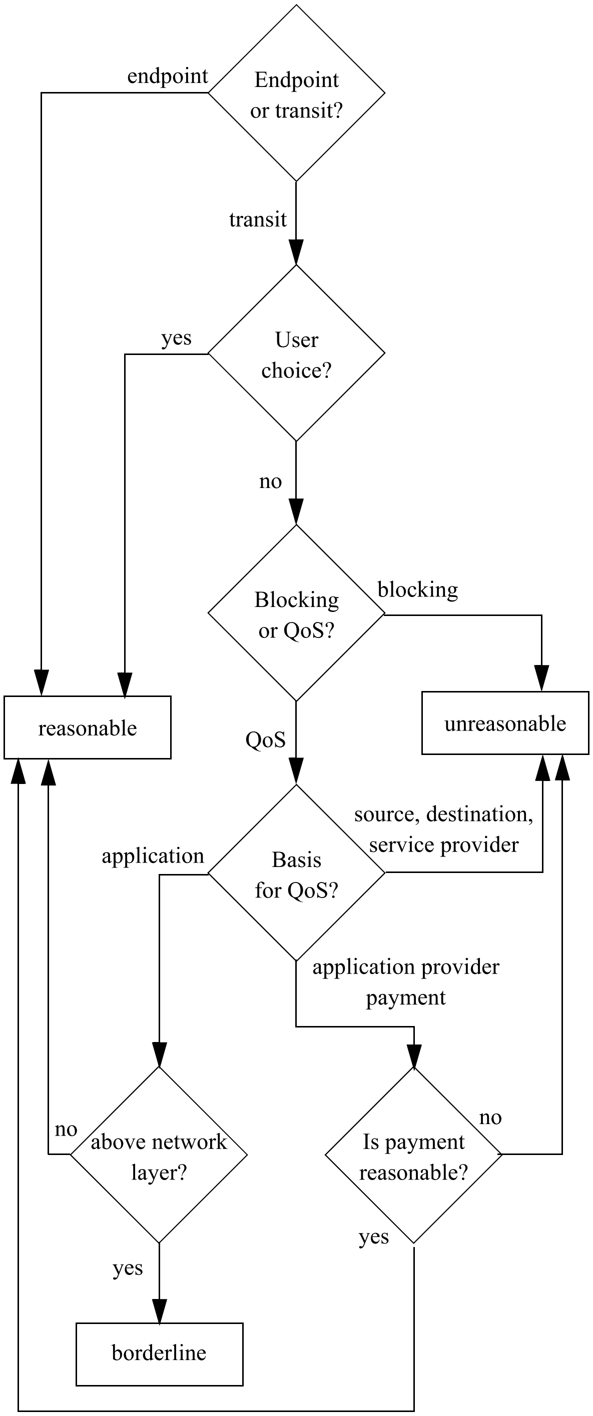


Fig. 2. The framework.

We consider the second rationale (relieving congestion) in this section, and we consider the third rationale (ensuring QoS) in the next section. The second rationale (relieving congestion) is often used to justify ISP traffic shaping on file-sharing traffic. Many congestion management practices would be classified by our framework as reasonable. However, if the practice involves blocking without user choice, for example, Comcast's termination of TCP connections carrying BitTorrent packets, we classify it as unreasonable. In addition, if the practice involves degrading performance based on the application using DPI without user choice, we classify it as borderline. In this section, we propose alternative congestion management practices that would be classified as reasonable and that achieve the same congestion management goals.

Recall that each traffic management *practice* is composed of traffic management techniques, used by a specific actor in a specific manner for a specific purpose. Blocking without user choice is unreasonable because of the combination of the technique (blocking) and the manner (without user choice). Degradation based on application using DPI without user choice is borderline because of the manner (DPI, without user choice). We start by considering alternative techniques to blocking, and we return to consideration of the manner below.

Alternative techniques for dealing with congestion are well known in the networking literature—these involve some combination of admission control, flow control, and resource allocation. We consider admission control in the next section on QoS, since it is primarily intended to protect the QoS of streams that require a minimum level of performance. The most common alternative congestion management to blocking is to delay transmission of excess traffic. To formalize this technique, let the random process $X(t)$ denote the aggregate user flow (in bps) demanded of the bottleneck link with capacity c in an access network. Denote by $\mathbb{A}$ the class of policies that reduce the aggregate user flow to c (bps) whenever it exceeds the capacity c, by discarding traffic or blocking connections. Assume that blocked traffic is cleared, that is, it does not resubmit itself to the network at a later time.[6] Note that $\mathbb{A}$ contains multiple policies that differ according to *which* excess traffic is blocked. Under any policy in $\mathbb{A}$, the aggregate user flow would thus be $Y(t) = \min(X(t), c)\ \forall t$.

Denote by $\mathbb{B}$ the class of policies that reduce the aggregate user flow to c (bps) whenever it exceeds the capacity c, by queueing traffic.[7] Note that $\mathbb{B}$ contains multiple policies that differ according to *which* excess traffic is queued, and the order in which queued traffic is transmitted. Denote the queue by $Q(t)$, which is dictated by $Q'(t) = X(t) - c$ when $Q(t) > 0$ and $Q'(t) = \max(X(t) - c, 0)$ when $Q(t) = 0$. Under any policy in $\mathbb{B}$, the aggregate user flow would thus be $Z(t) = c$ when $Q(t) > 0$ and $Z(t) = X(t)$ when $Q(t) = 0$.

For any policy $a \in \mathbb{A}$, our objective is to show that there exists a policy $b \in \mathbb{B}$ such that b is *feasible* and more *desirable* than a. We say that a policy (in $\mathbb{B}$)

[6] This assumption is reasonable for traffic that is time sensitive or that will be rerouted when blocked. Traffic generated by incoming p2p requests for popular files are likely to fit this assumption, since such requests will quickly be rerouted to alternative peers.

[7] Queueing may be explicitly implemented using a queue near the bottleneck link, or it may be implicitly implemented using flow control methods that queue the traffic at the source and allow it to be retransmitted at a future time.

that queues excess traffic is *feasible* if the queue is stable, that is, if $\mathbf{P}(Q(t) = 0) > 0$. Let $EX(t)$ be the long-term average traffic flow, defined by

$$EX(t) = \lim_{T\to\infty} \frac{1}{T} \int_0^T X(t)dt.$$

Under reasonable assumptions, the queue will be stable if $EX(t) < c$, since the capacity exceeds the average demand. We consider here the case in which $EX(t) < c$; the opposite case $EX(t) \geq c$ would mean that the access link is undersized and that traffic management must include not just traffic shaping but also blocking.

The question is how to turn this traffic queueing technique into a reasonable practice. Tiering is already a widely implemented use of pricing to differentiate users. Tiering, however, is currently defined in most contracts solely as a maximum transmission rate or throughput. The problem is that setting a maximum transmission rate does not adequately limit congestion. Indeed, ISPs often state that their networks were dimensioned on the assumption that users' duty cycles are very low and that file-sharing applications violate this assumption. A potential solution to congestion caused by file-sharing traffic is to define tiers in terms of *not only* maximum transmission rate but also the maximum volume transmitted during a specified period of time.

Suppose a subscriber can choose one of two tiers. The first tier allows transmission of up to c_h high-priority bytes per month for $\$d_h$ per month. The second tier allows transmission of up to c_h high-priority bytes per month plus up to c_l low-priority bytes per month for $\$d_h + \$d_l$ per month. The second tier may be of interest to heavy file-sharing users; the contract should state that the ISP may apply traffic shaping practices to low priority packets to time shift their transmission to uncongested times. The ISP can choose c_h, c_l, d_h, and d_l so that high-priority packets will be transmitted without queueing and that the queue is stable. Clearly, the resulting policy would be a member of class $\mathbb{B}$.

In order to define *desirability*, we need to consider users' satisfaction. In economics, *utility* is a measure of the relative satisfaction from or desirability of consumption of various goods and services. The fundamental assumption in utility theory is that the decision maker always chooses the alternative for which the expected value of the utility is maximum. If that assumption is accepted, utility theory can be used to predict or prescribe the choice that the decision maker will make, or should make, among the available alternatives.

To show that a queueing policy b is more desirable than a blocking policy a, we want to compare the aggregate utility of users under policies in $\mathbb{A}$ versus policies in $\mathbb{B}$. Suppose that user i under policy α transmits a proportion $p_i(\alpha)$ of its presented traffic without queueing and transmits a proportion $q_i(\alpha)$ of its presented traffic with finite queueing. It is reasonable to assume that user i's utility $u_i(p_i(\alpha), q_i(\alpha))$ is non-decreasing in both $p_i(\alpha)$ and $q_i(\alpha)$.[8]

[8] This simple model assumes that the queueing delay is not so long as to be unacceptable. If the link is saturated for a long period of time, then admission control will be required, as discussed in the next section.

Consider a particular policy $a \in \mathbb{A}$. Now there exists a policy $b \in \mathbb{B}$ such that $p_i(b) = p_i(a)\ \forall i$ and $q_i(b) \geq q_i(a) = 0\ \forall i$; policy b would simply queue the same traffic that was blocked under policy a. Let $U(\alpha)$ denote the aggregate utility of all users under policy α, that is, $U(\alpha) = \sum_i u_i(p_i(\alpha), q_i(\alpha))$. Then it follows that $U(b) \geq U(a)$, namely that policy b is at least as good as policy a and hence, at least as desirable. We conclude that there exist queueing practices that achieve the same goals as blocking practices (i.e., they are feasible), and that make the users at least as happy (i.e., they are at least as desirable).

In 2007–2008, Comcast adopted a highly controversial traffic management policy. During congestion, when $X(t) > c$, the policy blocked upstream p2p connections of the heaviest users by using a `TCP RST` packet. It is evident that such a policy roughly falls into class $\mathbb{A}$.[9] In 2009, Comcast adopted a traffic management policy that appears to fall within $\mathbb{B}$. At times of local congestion, this policy queues traffic for users who during the previous 15 minutes used at least 70% of their tier's maximum rate. The queue is cleared anytime there is an opportunity to do so. The former traffic management practice resulted in a huge consumer outcry resulting in the FCC's intervention. The latter has been adopted as a reaction to a demand by the FCC to adopt a policy that only throttles traffic when congestion occurs and to apply it in a protocol-agnostic manner, and has so far been successful.

Intuitively, we can see why traffic shaping would typically be preferable to blocking. For heavy users of p2p applications, arbitrary connection resets degrade the user's download experience because of the *tit-for-tat* strategy commonly employed in most p2p applications. A tiered traffic shaping policy, on the other hand, would the user to judiciously select the priority of his traffic, thereby improving the overall efficiency of the network and the experience of the user. For light users, blocking policies can decrease their utility if their occasional use of p2p based applications, for example *Software-as-a-Service*,[10] is arbitrarily reset. With traffic shaping, however, users are assured of a minimum level of service during peak periods.

It remains to consider practices that degrade performance based on application using DPI without user choice, and which we thus classified as borderline. Such traffic shaping practices raised red flags because they are implemented above the network layer. A layering violation occurs because the ISP is using DPI to identify the packets to prioritize. Layering could be respected, however, if users provide the identification themselves. Let a function $M_i(\alpha)$ denote a priority assignment function that marks each packet as either high-priority or low-priority, with a limited flow of high-priority packets (defined so that, in the absence of low-priority packets, the high-priority packets by themselves never trigger the network to queue them). The idea is to let the users decide the

[9] More precisely, it is unclear if TCP resets were only applied when congestion occurred, and to which users Comcast applied this technique.

[10] Software as a Service (SaaS) is a model of software deployment where an application is licensed for use as a service provided to customers on demand.

marking function, rather than the ISP. In this manner, the practice now allows user choice, and hence it moves from a classification of borderline to one of reasonable.

The challenge with relying on user identification of packets is one of motivation. What would induce a user to properly mark packets for congestion management? The research literature has long discussed the use of pricing for this purpose (see, e.g., Jiang and Jordan [1995]). The two-tier model proposed above can be used to accomplish this. For users who select the second tier that allows marking, modify the users' utility function to incorporate the marking, as $u_i(p_i(\alpha), q_i(\alpha), M_i(\alpha))$. Since the user can transmit only a limited amount of high-priority traffic and since presumably high-priority traffic will be more expensive, that is, $d_h/c_h > d_l/c_l$, the user will be motivated to mark as high-priority those packets for which priority transmission would be valuable. Specifically, consider a policy $a \in \mathbb{A}$ in which the ISP arbitrarily assigns priority to packets. Compare this policy to a policy $b \in \mathbb{B}$ that queues only low-priority packets, where the priority of a packet is decided by the user. It follows that $U(b) \geq U(a)$, since users will be happier with their own priority assignments than with the ISP's random priority assignment. We conclude that there exist congestion management practices that allow user choice (and hence are reasonable), that achieve the same goals as practices that involve use of DPI by an ISP (i.e., they are feasible), and that make the users at least as happy (i.e., they are at least as desirable).

7. ALTERNATIVES TO UNREASONABLE OR BORDERLINE QOS MANAGEMENT PRACTICES

In the previous section, we proposed alternatives to unreasonable or borderline congestion management practices that block or degrade performance for selected packets. In this section, we propose alternatives to unreasonable or borderline QoS practices that enhance performance for selected packets.

The framework proposed above treats QoS provided by an ISP differently depending on how which traffic receives QoS. The first set of QoS practices that were classified as unreasonable are those in which QoS is provided on the basis of source, destination, or service provider without user choice (e.g., if an ISP provides QoS only for its own VoIP service). We classified such practices as unreasonable since this results in an uneven playing field between the ISP and its application competitors. ISPs should not refuse to sell QoS to competing application providers, and they should not strike exclusive deals to sell reserved bandwidth to selected providers. The alternative is for an ISP to provide QoS on a nonexclusive basis. This can be done by letting the user determine which traffic should receive QoS, by giving QoS to all applications that require it, and/or by selling QoS to other application providers. We consider each of these alternatives in the following.

The second set of QoS practices that were classified as unreasonable are those in which QoS is provided on the basis of application provider payment and the payment itself is deemed unreasonable. ISPs should be prohibited from providing Internet infrastructure services to competing application providers at inflated prices in order to favor the ISP's own application offerings. The alternative is simply to adjust the payment to be reasonable. Essentially, the ISP should sell QoS to competing application providers at the same price it charges its own applications, and the price should be set according to demand and supply. This is required to again ensure a level playing field between the ISP and its application competitors.

It remains to consider QoS practices that were classified as borderline, due to their use of QoS based on DPI without user choice. A superior reasonable practice can be constructed by placing the application identification in users' hands. We start with the technique itself. Rather than using DPI, we suggest that ISPs should use either reservations (e.g., IntServ) or priorities (e.g., diffServ). While exclusive QoS mechanisms do indeed use either reservations (e.g., bandwidth limits) or priorities (e.g., PacketCable QoS), layering violation occurs because the ISP is using DPI to identify the packets to prioritize. Layering could be respected, however, if users provide the identification themselves, which both IntServ and diffServ allow.

The technique can be transformed into a reasonable practice by constructing a QoS tier, defined by a period of time and/or amount of traffic that can receive enhanced QoS. A user that subscribes to a VoIP service offered by an application provider other than the user's ISP may wish to receive QoS for that VoIP traffic. That user may purchase an option offered by the user's ISP that ensures a specified limit on delay and loss for packets marked by the user as high priority, for up to a specified number of high priority bytes per month. This practice allows user choice, and thus is deemed reasonable.

Admission control is thus implemented either through the reservation system (e.g., IntServ) or through the QoS tier (e.g., diffServ). In the former case, the user decides whether to start a connection that requires QoS in part based on whether there is capacity to support that QoS. In the latter case, the user decides whether to start a connection that requires QoS in part based on the limits the ISP has placed on the number of such QoS contracts it sells.

In closing, we note that some practices may involve a combination of bases for determining which packets receive enhanced QoS. As an example, for a period of time Canadian ISP Shaw Communications offered a tier to its users that, for $10/month, entitled its users VoIP packets to enhanced QoS in the Shaw network, regardless of the VoIP provider. If Shaw did not also offer its own VoIP service, this practice would be reasonable. However, Shaw does also offer its own VoIP service, and it gives enhanced QoS to its own VoIP packets. This vertical integration brings up the question of whether the $10/month charge is reasonable. Shaw undoubtedly included a charge for QoS in it's own VoIP service; if this charge to its own service is less than $10/month, then the consumer charge is unreasonable and thus the practice is unreasonable.

We conclude that there exist practices that are reasonable, that can achieve the same goal of ensuring QoS, and that result in user satisfaction at least as high as unreasonable or borderline practices. In addition, there are several advantages to expanded tiering over traffic management practices that involve DPI or exclusive use of QoS. First, expanded tiering does not violate layering, since packets are identified for prioritization by the user, not by the ISP.

Second, the traffic management practice becomes transparent, with the ISP applying techniques that have been agreed to by the user. Third, expanded tiering can easily accommodate future applications without requiring revision to user contracts, since the contracts specify only priority levels rather than specific applications.

8. CONCLUSION

ISPs use a wide variety of traffic management techniques in a wide variety of manners. Some of these practices are unreasonable, but it has been difficult to identify what makes a practice acceptable or unacceptable.

At the time of writing, the FCC has proposed a set of rules that would delineate reasonable network management and is asking for public comment [FCC 2009]. They seek comment on their proposed definition of reasonable network management. They ask whether it is reasonable for an ISP to temporarily limit the bandwidth to individual users in a congested neighborhood, to charge users based on usage, and/or to use QoS. They ask how QoS assignments might be determined, and when blocking is reasonable.

Whereas the FCC proposed definition is based on the intended purpose of a practice and on the reasonableness of that practice, we have proposed that reasonableness involves the layer (“where”), the functionality (“what”), the actor (“who”), and the manner and purpose (“when”). We have presented a framework that classifies a traffic management practice on the basis of answers to these four questions. We also proposed alternatives to unreasonable or borderline congestion management practices that block or degrade performance for selected packets and QoS practices that enhance performance for selected packets.

At the time of writing, the FCC is expected to likely issue final orders after further public comment. However, the FCC’s authority is also being determined by the courts. If the courts determine that the FCC does not have authority to issue such an order, it will fall to Congress to address these issues.

REFERENCES

Comcast Corporation. 2008. Comments of Comcast Corporation before the Federal Communications Commission in the matter of broadband industry practices (WC docket no. 07-52). http://fjallfoss.fcc.gov/.ecfs/document/view?id=6519840991.

Cox Communications. 2004. Voice over Internet protocol: Ready for prime time. White paper. http://cox.mediaroom.com/index.php?s=43&item=241.

FCC. 2005a. DA 05-543, Madison River communications consent decree. http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-05-543A1.pdf.

FCC. 2005b. FCC 05-151, Internet policy statement. http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-151A1.pdf.

FCC. 2007. FCC 07-31, Broadband Market Practices Notice of Inquiry. http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-31A1.pdf.

FCC. 2008. FCC 08-183, Comcast Order. http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-08-183A1.pdf.

FCC. 2009. FCC 09-93, Open Internet NPRM. http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-09-93A1.pdf.

Floyd, S. and Jacobson, V. 1993. Random early detection gateways for congestion avoidance. *IEEE/ACM Trans. Netw. 1*, 4, 397–413.

FREE PRESS, PUBLIC KNOWLEDGE ET AL. 2007. A petition before the Federal Communications Commission for declaratory ruling that degrading an Internet application violates the FCC's Internet Policy Statement and does not meet an exception for "reasonable network management." http://www.fcc.gov/broadband_network_management/fp_et_al_nn_declaratory_ruling.pdf.

FRIEDEN, R. 2006. Network neutrality or bias?—Handicang the odds for a tiered and branded Internet. In *Proceedings of the 34th Research Conference on Communication, Information, and Internet Policy (TPRC)*. TPRC.

IEEE. 2010. IEEE Standards. http://standards.ieee.org/.

INTERNET ENGINEERING TASK FORCE. 2010. IETF request for comments. http://www.ietf.org/rfc.html.

JIANG, H. AND JORDAN, S. 1995. The role of price in the connection establishment process. *Euro. Trans. Telecomm. 6*, 4, 421–429.

JORDAN, S. 2009. Implications of Internet architecture upon net neutrality. *ACM Trans. Intern. Techn. 9*, 2, 5:1–5:28.

LEHR, W. A., GILLETT, S. E., SIRBU, M. A., AND PEHA, J. M. 2007. Scenarios for the network neutrality arms race. *Int. J. Comm. 1*, 607–643.

MILLER, E., ANDREASEN, F., AND RUSSELL, G. 2001. The PacketCable architecture. *Comm. Mag. 39*, 6, 90–96.

PACKETEER INCORPORATED. 2007. Best practices: Monitoring and controlling peer-to-peer (p2p) applications. http://www.zdnet.co.uk/white-papers/view/network-management/best-practices-monitoring-and-controlling-peer-to-peer-p2p-applications-260084034/.

PACKETEER INCORPORATED. 2008. Packeteer education customers. http://www.bluecoat.com/solutions/industry/education/highereducation.

PEHA, J. M. 2007. The benefits and risks of mandating network neutrality, and the quest for a balanced policy. *Int. J. Comm. 1*, 644–668.

SANDVINE INCORPORATED. 2004. Session management: BitTorrent protocol, managing the impact on subscriber experience. http://web.archive.org/web/20080608162137/http://www.sandvine.com/general/getfile.asp?FILEID=21.

SANDVINE INCORPORATED. 2007. Sandvine DPI-based policy solutions. http://www.presh.com.mx/res/Sandvine_Solutions_Overview.pdf.

STILIADIS, D. AND VARMA, A. 1998. Latency-rate servers: A general model for analysis of traffic scheduling algorithms. *IEEE/ACM Trans. Netw. 6*, 5, 611–624.

VUZE INC. 2007. A petition before the Federal Communications Commission to establish rules governing network management practices by broadband network operators. http://fjallfoss.fcc.gov/ecfs/document/view?id=6519811711.

WEI, D. X., JIN, C., LOW, S. H., AND HEGDE, S. 2006. FAST TCP: Motivation, architecture, algorithms, performance. *IEEE/ACM Trans. Netw. 14*, 6, 1246–1259.

WEITZNER, D. 2008. Net neutrality... seriously this time. *IEEE Intern. Comput. 12*, 3, 86–89.

Received June 2009; revised February 2010; accepted August 2010