Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

06-Apr-2007

English - Or. English

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY

DSTI/ICCP/TISP(2006)4/FINAL
Unclassified

Working Party on Telecommunication and Information Services Policies

INTERNET TRAFFIC PRIORITISATION: AN OVERVIEW

JT03225145

English - Or. English

FOREWORD

This report was presented to the Working Party on Communication Infrastructures and Services Policy in May 2006 and was declassified by the Committee for Information, Computer and Communications Policy in March 2007.

The report was prepared by Mr. Taylor Reynolds of the OECD's Directorate for Science, Technology and Industry. It is published on the responsibility of the Secretary-General of the OECD.

TABLE OF CONTENTS

FOREWORD....2
NO TABLE OF CONTENTS ENTRIES FOUND.MAIN POINTS....4
INTRODUCTION....6
TECHNICAL BACKGROUND: TRAFFIC PRIORITISATION....7
Traffic prioritisation (unhindering/delaying)....8
Traffic shaping policy....10
Traffic shaping points of control....13
KEY ISSUES AND POLICY DEBATES....16
Incentives....16
Building new networks....16
Introducing new QoS applications....16
Innovation at the edges of the network....17
Production of new content....18
Maintaining access....19
Anti-competitive behaviour....20
Unhindered access to information....21
Security benefits of traffic control....21
Bandwidth ownership....22
The role of bandwidth....22
Are the lines paid for?....22
Who provides the lines?....24
Bandwidth entitlement....25
Privacy issues....26
Packet shaping and encryption....26
Personally identifiable information....27
POLICY CONSIDERATIONS....28
Level of competition....28
Negotiations between content providers and infrastructure operators....29
Market-based consumer protection under a multi-tiered Internet....30
Consumer protection and information disclosure....32
Government involvement to protect consumers....33
Mobile network neutrality....35
NOTES....37

Boxes

NO TABLE OF CONTENTS ENTRIES FOUND.MAIN POINTS

The Internet is very efficient for quickly routing large amounts of data but it was not designed to provide the guaranteed quality of service or security that many current Internet applications now require.

Network administrators who manage networks have powerful tools that allow them to control, prioritise or block specific data transmissions. Traffic prioritisation is one tool that can be used to improve quality of service on their network but could also potentially be employed in an anti-competitive manner to block or disadvantage competing services.

Traffic prioritisation is typically used to minimise latency and allocate bandwidth on data networks. Traffic prioritisation is often discussed in the debates surrounding “network neutrality”, although there is no universally accepted definition of “network neutrality”.

There is likely a wide range of future innovations that will require better quality of service than the current Internet can provide. Certain Internet providers have even put forward that they believe traffic prioritisation is inevitable for the future functioning of the Internet. The ability to designate priority to certain applications will be a boon for consumers and providers as long as there is sufficient competition in the market.

The debate over traffic prioritisation should focus on whether competitive market forces provide sufficient consumer safeguards on network operator behaviour. There are several factors that will affect network operators' incentives and behaviours. Market analysis should examine if these incentives and behaviours are likely to affect consumers adversely. These factors include the level of competition in the broadband access market, the capabilities of traffic prioritisation technology and the range of service offerings from providers in the market.

In analyzing competitive conditions, policy makers need to consider consumer demands, the relevant technologies, and how technologies are applied in the marketplace. Indeed, there may not be a single “broadband Internet access market” but rather a variety of smaller service markets. Policy makers must carefully consider the bandwidth demands and quality of service needs of different services and the bandwidth limitations of wired and wireless technologies when making market definitions.

Open-access fibre networks, such as those where the physical infrastructure is owned by a co-operative or municipality, could play an important role in the debate over traffic prioritisation. Open access networks that separate the provision of physical infrastructure from service delivery could significantly reduce anti-competitive traffic shaping incentives by allowing a variety of providers to offer video, voice and data services in the same market over the same physical infrastructure. Municipalities and governments could also promote wired infrastructure development by making duct or pole space available to all interested providers.

A market-based solution is preferable to intervention in the market as a way to deal with issues regarding traffic prioritisation. However, it may be helpful for governments to publish a set of general principles for market participants. If problems occur, *ex-post* remedies can be used. The decision to apply *ex-ante* regulation will depend on whether regulators find evidence of persistent problems in the context of

traffic prioritisation and if market forces or *ex-post* solutions are unable to sufficiently protect consumers. There is considerable debate about whether significant anti-competitive problems will appear in markets. There is little evidence of anti-competitive conduct to date and problems have typically been resolved quickly via market forces or through quick regulatory intervention in markets where they have appeared.

Consumers need to be protected *a priori* from non-transparent behaviour by network operators. In this context enhancing competition can help. There are several steps policy makers could take to increase competition in markets as a way to reduce incentives for anti-competitive behaviour and proactively protect consumers:

i) Reducing entry barriers that inhibit entry in the broadband Internet access market.

ii) Re-examining existing competition laws to ensure they can address any abusive practices that could appear under a multi-tiered Internet structure.

iii) Ensuring that subscribers can switch operators easily.

iv) Improving disclosure to broadband consumers of how their broadband Internet service is affected by packet prioritisation.

From the current state of the discussions it seems premature for governments to become involved at the level of network-to-network traffic exchange and demand neutral packet treatment for content providers. The concerns of smaller, start-up firms might be addressed through the pooling of demand for Internet access via a common ISP.

Under the current Internet architecture routers have no need to routinely examine the payload of packets traversing the network before passing them on. However, the introduction of packet shaping throughout the network could require the routers to examine the payload of packets that were associated with IP addresses. In certain jurisdictions these practices may raise privacy concerns.

If consumers face high switching costs they will be reluctant to pay to leave one broadband provider for another. Regulators can consider imposing rules that protect consumers and allow them to quickly and effectively change providers, at minimal or no expense and without service disruption if their operator's routing policies change to degrade or block services that were unaffected when the subscriber signed up for service.

It is important to clarify which bandwidth should be included in the discussion of traffic prioritisation since cable and FTTH networks may already use a majority of their available “bandwidth” for services other than Internet access. Traffic prioritisation debates should focus on the frequencies reserved and advertised for Internet data communications.

INTRODUCTION

Long known for its open architecture which gives transmissions equal priority, the Internet should, according to some market players, evolve into a network where users and companies could pay to increase the priority of their transmissions over others. Under such a system Internet access could be broken into several tiers of service quality where the data of those who pay more traverse the network faster (with higher priority) than the data of those who do not. To others, the ability to pay for prioritised data handling on the Internet is viewed as a distortion of the basic elements of equality and openness promoted by the Internet. This proposition of prioritising certain types of data has resulted in a debate which has evoked strong emotions.

The aim of this paper is to provide background for national debates by examining the policy and regulatory issues surrounding traffic prioritisation.

TECHNICAL BACKGROUND: TRAFFIC PRIORITISATION

The Internet's original design is based on what is known as the "end-to-end principle" as a way to maximise the efficiency and minimise the cost of the network. This has arguably been one of the key elements of its success. The end-to-end principle explains the relationship between the network and its end points and has its origins in a seminal paper in 1981 by Jerome Saltzer, David Reed, and David Clark. In their paper, the authors propose a model where the intelligence and processing power of a network reside at the outer edges while the inner network itself remains as simple as possible.[1]

The Internet's original designers adhered to this principle as they developed the protocols and technologies that have become what we know as the Internet today. Computers communicate with each other over the Internet by means of IP addresses (used to identify different computers connected to the Internet) and small packets of data sent serially. Users on different networks can pass along information to one another because of network devices (routers) that examine the destination IP address on incoming data packets and resend them on, ever-closer to the destination computer.

At its inception, the Internet kept the processing requirements of routers at a minimum. This allowed routers to handle a large amount of traffic with a minimal amount of computation and at the fastest speed. As the Internet has grown, this initial design of the Internet has allowed for huge amounts of data to be routed without the need for massive processing power within the network.

While the Internet's current design is very efficient for quickly routing large amounts of data, it currently does not provide the quality of service or security that many currently-envisioned Internet applications would require. Internet protocols, as they are implemented today, do not provide functionality that could guarantee quality of service for time-sensitive applications such as real-time voice and live video. This has meant that the quality of real-time voice and live video delivered over the Internet is tied to the level of general Internet traffic and network congestion. Despite these challenges, content providers have found innovative ways to improve response times and delivery quality without explicit traffic prioritisation. For example, content providers commonly use caching and content distribution services from companies such as Akamai that deliver content from servers closer to users. Content providers also commonly negotiate peering or transit agreements directly with Internet providers.

The current Internet may lack some of the quality of service functionality that future applications may demand but engineers did build elements of traffic prioritisation into the original Internet protocol specifications (IP)[i]. This functionality has not been used extensively and research has suggested that this is a result of the complexity of quality of service protocols and the difficultly of implementing such systems.[2] Instead, quality of service guarantees are commonly provided using virtual private network (VPN) technologies such as IP MPLS which essentially mimic a dedicated circuit on an IP network. Internet

[i] For example, the header of an IP packet allocates one byte for recording the "type of service" of the packet. Of this byte, three bits are used to set the precedence of the packet – essentially allowing for a priority ranking between 0 and 7. The "type of service" header has been available in the protocol but has not been used extensively. Subsequently the IETF proposed and standardised various protocols that could provide quality of service controls on IP networks. For example, the IETF proposed an architecture called DIFFSERV that would reuse this byte. DIFFSERV has also not been widely used since its development in 1998.

service providers commonly offer VPN services to businesses and these have not caused noticeable disruption with other Internet traffic.

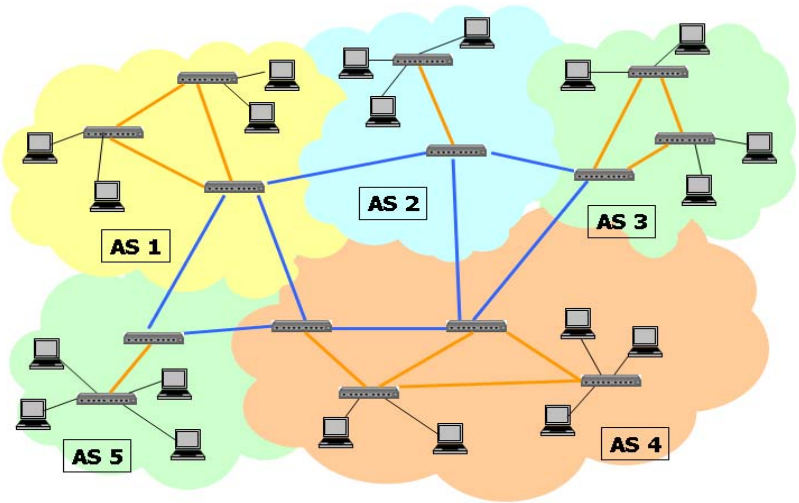
Some commentators view differentiated levels of service as an opportunity to build quality of service into networks and provide very-high-quality connectivity for time-sensitive applications such as voice and video. To others, changes to the current architectural model threaten to destabilize many of the business models that have been successful on the Internet or worse, create anti-competitive incentives for Internet service providers to block or slow certain types of competitive traffic.

Traffic prioritisation (unhindering/delaying)

Since the beginning of the Internet, network administrators have had to manage Internet traffic. When the Internet's users offer traffic loads in excess of the routing and transmission capabilities of the network, administrators must accommodate this by: sending packets along an alternative route, delaying packets in a buffer, or dropping packets completely. This queuing may be done on a "first come, first served" or some other basis – without particular regard to the source or character of the packets, or some other method. Any changes in queuing procedures (prioritisation) on the Internet have to be made on a technical level by network administrators. These administrators have powerful tools available which allow them some control over the data flowing over their networks. One of the main tools they have at their disposal is the ability to "shape" and manage data traffic flows.

Traffic shaping (also known as packet shaping or traffic structuring) is a technical tool that controls and manages data traffic on a network. It provides network administrators with the ability to control the flows of data coming onto the network as well as to identify types of traffic (data packets) and handle them differently. Administrators can then give certain applications or services priority handling over others. Certain types of traffic shaping technologies have long been available to network administrators for controlling data flows on networks. For example, administrators have implemented traffic shaping to smooth out traffic flows and prevent bottlenecks, typically in an effort to improve the user's experience. Administrators have not had equipment available to do high-speed, deep-packet inspection and prioritisation until now. This is one of the reasons why prioritisation debates are moving to the forefront now even though "type-of-service" classification has been possible for decades with IP.

Figure 1. Network relationships for passing along traffic



Source: http://lecture.ecc.u-tokyo.ac.jp/~gnakao/images/internet-topology.png

Currently, most large network routers pass traffic amongst themselves on a first-come-first-served basis. However, some of the arguments in the current "network neutrality" debates are about whether these routers should continue to pass along packets, such as e-mail, on equal terms or if network administrators should be allowed to offer different priority for packets along the journey.

Figure 1 shows a very simplified diagram of how smaller networks can be interconnected to form a piece of the Internet. Each Autonomous System (AS) number represents a single network or collection of networks administered by the same entity that likely uses the same routing methodology. Essentially every network administrator can set their own priority levels for different types of traffic traversing their networks. It is worth noting that network managers cannot provide quality of service for traffic on the Internet to a given customer unilaterally since most Internet communications traverse multiple networks. Network operators can only control for quality of service within their own networks unless they have agreements with other networks to honour each other's prioritisation on their own networks. In Figure 1, a user on the network marked AS 1 would need to traverse network AS 2 or AS 4 in order to reach content on AS 3. This means the operators of AS 1 could provide increased quality of service for traffic within their network but likely would not have agreements in place to offer increased quality along the whole route from AS 1 to AS 3. In the future, enhanced quality of service may require co-ordination across multiple networks and application-specific handoffs between the networks.

Administrators are able to "shape" and "prioritise" traffic at the router level by installing software/hardware that examines the destination IP address, port and contents of the IP packet to determine its "payload" before passing it along. This traffic shaping software allows network operators extensive flexibility in determining which packets and traffic receive priority on a given network.

Current traffic shaping tools are very powerful and give network administrators the ability to view and prioritise a wide range of applications and data. Table 1 gives a sample of some of the more than 500 applications and data types that just one manufacturer advertises that its product can detect and control on a wide area network. Hardware solutions for monitoring, controlling and prioritising traffic are available for large carrier networks as well. For example, carrier-grade equipment such as the Cisco Service Control Engine (SCE) 2000 can do deep packet inspection at "multi-gigabit and 10 gigabit speeds".[3] Cisco's SCE 2000 recognises over 600 protocols and applications and is capable of performing application-layer stateful-flow inspection of IP traffic, and controlling that traffic based on configurable rules.[4]

Table 1. Sample of applications that can be monitored, controlled and prioritised

Peer-to-Peer	Voice over IP	Multimedia	Gaming	Messaging
Aimster	CiscoCTI	Abacast	Asheron's Call	AOL (IM,
Apple-iTunes	Clarent	Motion Video using	Battle.net	Talk, Image,
AudioGalaxy	CUSeeMe	DIGStream	Diablo II	File, ISP)
Bit Torrent	Dialpad	MPEG (Audio, Video)	Doom	iChat
Blubster	H.323	Multi-cast NetShow	EverQuest	ICQ
DirectConnect	I-Phone	NetMeeting	Half-Life	IRC
EarthStation V	iChat	Ogg over HTTP	Kali	Lotus IM
EDonkey	MCK Commun.	QuickTime	LucasArts (Jedi)	MSN
Emule	Megaco	RadioNetscape	MSN Zone	Messenger
Gnutella	Micom VIP	Real (Audio, Video)	Mythic	Windows-
Grokster	MGCP	RTP	Quake I, II, & III	POPUP
Groove	Net2Phone	RTSP	SonyOnline	Yahoo!
Hopster	RTP	SHOUTcast	Tribes I, II	Messenger
Hotline	RTCP	Streamworks	Unreal	
iMesh	SIP	VideoFrame	Warcraft III	
Limewire	Skinny (SCCP)	WebEx	WorldofWarcraft	
KaZaA	Skype	WinampStream	XboxLive	
KaZaA Lite	T.120	WinMedia	Yahoo! Games	
Morpheus	VDOPhone			
Napster	Vonage			
Napigator				
+ 50 others				

Source: Packeteer at http://www.packeteer.com/resources/prod-sol/ApplicationDiscovery.pdf

Essentially, an Internet service provider or network operator could identify any of the services or applications in Table 1 and decide whether to block or allow it. In cases where the service is allowed, operators can then assign levels of priority to specific services or programs or even allocate a block of available bandwidth to the service. For example, an Internet service provider may offer a premium level of service to avid gamers and allocate a dedicated amount of bandwidth to specific games in the gaming list. Internet providers could also advertise broadband connections that block peer-to-peer file sharing as a way to ensure faster bandwidth for all customers who may not see a need for such services. Many traffic shaping products allow network operators to set parameters on an application or a per-user basis.[5] These can also be the same tools that ISPs use to filter spam or block malicious intrusions to their customers' computers.

Packet shaping technologies are currently available to ISPs and network operators, but routers across the Internet generally are not configured to examine the contents of packets. It is likely that network operators will continue increasing their use of packet shaping tools in the future, largely to meet commercially-driven demands.

Traffic shaping policy

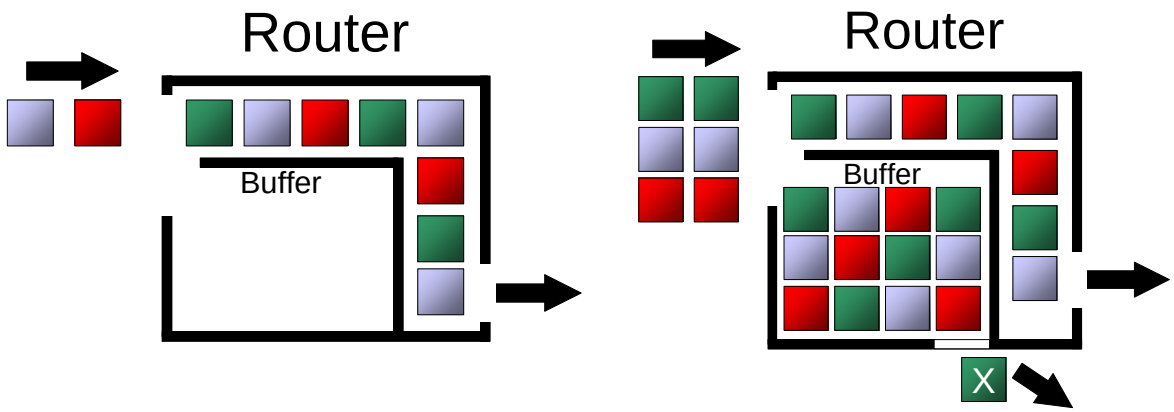
Once network administrators have installed traffic shaping technologies within the network they must set internal policies prescribing the treatment of different types of packets. These internal routing policies can be assigned to three broad categories: Best effort, needs-based prioritisation and active prioritisation (see Table 2).

Except in cases of active prioritisation, the decision of whether to drop or delay packets will be triggered and applied during times of network congestion at the router. As Felten and Halderman have

highlighted, the buffering mechanisms of the router play a key role in this process.[6] Buffers built into the routers are used to accommodate sudden surges in traffic over a given link because they can temporarily accept incoming packets even when there is not sufficient outgoing capacity to immediately send them on. In times of low traffic volume the router is able to pass on traffic immediately as it arrives (see Figure 2 – left). Best effort transmissions are all handled on a first-come, first-served basis when there is sufficient network capacity and there is no delay imposed on any packets traversing the router as a result.

In times of congestion however, the router cannot forward on all the packets it is receiving and must set some aside in a buffer to be forwarded later when network demands are lower. This buffering works well during temporary periods of high traffic but can quickly encounter problems when there are sustained and heavy network demands and the router runs out of buffer memory.

Figure 2. Different traffic flow states at the router – fluid (left) and congested (right)



The router's policies must dictate what action to take with additional packets that arrive at the moment the buffer is completely full (see Figure 2 – right). The router must either write over some data in the buffer to make space or block any new packets from entering. Routing policies typically begin by writing over the oldest packets in the buffer and creating space for new packets that arrive. It is worth noting that this is not necessarily a problem for current Internet protocols since applications on the receiving end can detect that packets are being lost and request the originating computer to either slow down the rate at which it is sending packets (with UDP) or to resend any packets for which it has not received a confirmation of delivery (TCP)[ii]. Some of the most important policy questions surrounding a multi-tiered Internet are which packets the routers delete first.

[ii] A glossary of acronyms is provided at the end of the document.

Table 2. Routing policy categories

1. Best effort	2. Need-based prioritisation	3. Active prioritisation
When packets enter the router faster than they can be sent on the packets are stored in a buffer until traffic lightens. If the buffer runs out of space then packets are dropped based on the amount of time they have spent in the buffer, not on the type of data traffic they contain.	Packets are again temporarily stored in the buffer when there is not sufficient outbound bandwidth. Once the buffer is full packets are deleted according to preferences assigned by the network operator. Packets carrying less-valued traffic are dropped first.	Packets can be detained or deleted in a buffer even when outgoing bandwidth is available on the line. An operator could allocate a small percentage of the line's total traffic for certain applications, creating a self-imposed traffic constraint. Finally, traffic destined to certain ports can be blocked altogether.
All packets are treated on a first in, first out basis (FIFO). No priority is given for different packet contents. In periods of congestion packets of all types can be dropped.	Packets are treated on a first in, first out (FIFO) basis until there is traffic congestion. At that point certain packets are given priority and essentially move to the front of the queue.	Packets are examined as they enter the router and are prioritised even in cases where sufficient bandwidth on the outbound link exists.

Source: OECD, Felten and Halderman.

Network administrators can choose to treat all traffic as "best effort" and simply delete the oldest packets in the buffer that are waiting for their turn to be forwarded on. The drawback with a strict interpretation of best effort is that it does not leave flexibility for users to determine different levels of priority for their own traffic on the network. Users may want voice traffic to be given priority over simple web browsing when the router is forced to drop packets.

As mentioned above, users may have applications such as VoIP where packet delivery is time critical. Network operators may then choose to implement router policies that give priority to certain types of incoming packets over others instead of increasing the overall capacity of the network. These routing preferences would only come into play when there was congestion on the outbound link of the router. The network administrator could assign priority to certain packets that were deemed to be the most in need of timely and steady packet delivery. This type of routing policy falls into the second category of "needs-based prioritisation" since packets are only assigned priority when network congestion necessitates it.

Finally, the third category of "active prioritisation" refers to routing policies that can detain or block packets even when sufficient bandwidth is available on the outbound link. Network operators have the ability to allocate a portion of bandwidth to specific applications. For example, packets sent by peer-to-peer (P2P) applications could be limited to 5% of total traffic on a given line. Once the P2P packets had saturated the 5% limit any additional packets would be placed into a buffer or dropped altogether. The remaining 95% of the line's capacity may still be available for use but the routing policy would impose a bandwidth constraint on certain applications and their packets.

Prioritisation among types of packets is not limited to dropping packets altogether. Routers can have policies that move prioritised traffic to the head of the queue, even before buffers are full, displacing lower-priority packets that may have arrived earlier. Routers could move packets from a voice telephone call to the front of the queue and displace web browsing requests that could tolerate delays better. This displacement would only occur when a delay for some packets was necessary given constraints on the outbound path from the router. Active prioritisation is also possible and would delay or stagger the retransmission of all low-priority packets even if an outbound link were available.

One of the key questions in the debate is who determines which packets, applications or ports are deemed time sensitive and receive priority. One way users could clearly benefit from "needs-based prioritisation" is if they were able to assign different levels of priority to different applications. To some extent this is already possible using home routers/switches which offer packet shaping capabilities on their

local networks (see Box 1). It is worth highlighting that the control an end user has over traffic shaping is limited to the home network and has no effect on the network operator's infrastructure – with the exception of the rate at which the home router passes along outbound traffic to the broadband line and the rate at which it accepts incoming packets.

Box 1. Traffic structuring initiated by end-users

Home equipment manufacturers (*e.g.* modem/router) have introduced devices that allow users to set bandwidth priority levels for applications and services they commonly use. These devices are particularly popular with gamers and VoIP users since they allow certain applications to have priority through the router and out to the modem over other time-insensitive Internet traffic.

Users can typically assign priority based on MAC address of the device or via a range of ports a specific application commonly uses. This control is limited to the user's premises. Users can take control of their Internet connections up until the point the connection leaves their modem and it is passed on to the Internet service provider. At that point the data flowing over the network has traditionally been “best effort” with no service level guarantees.

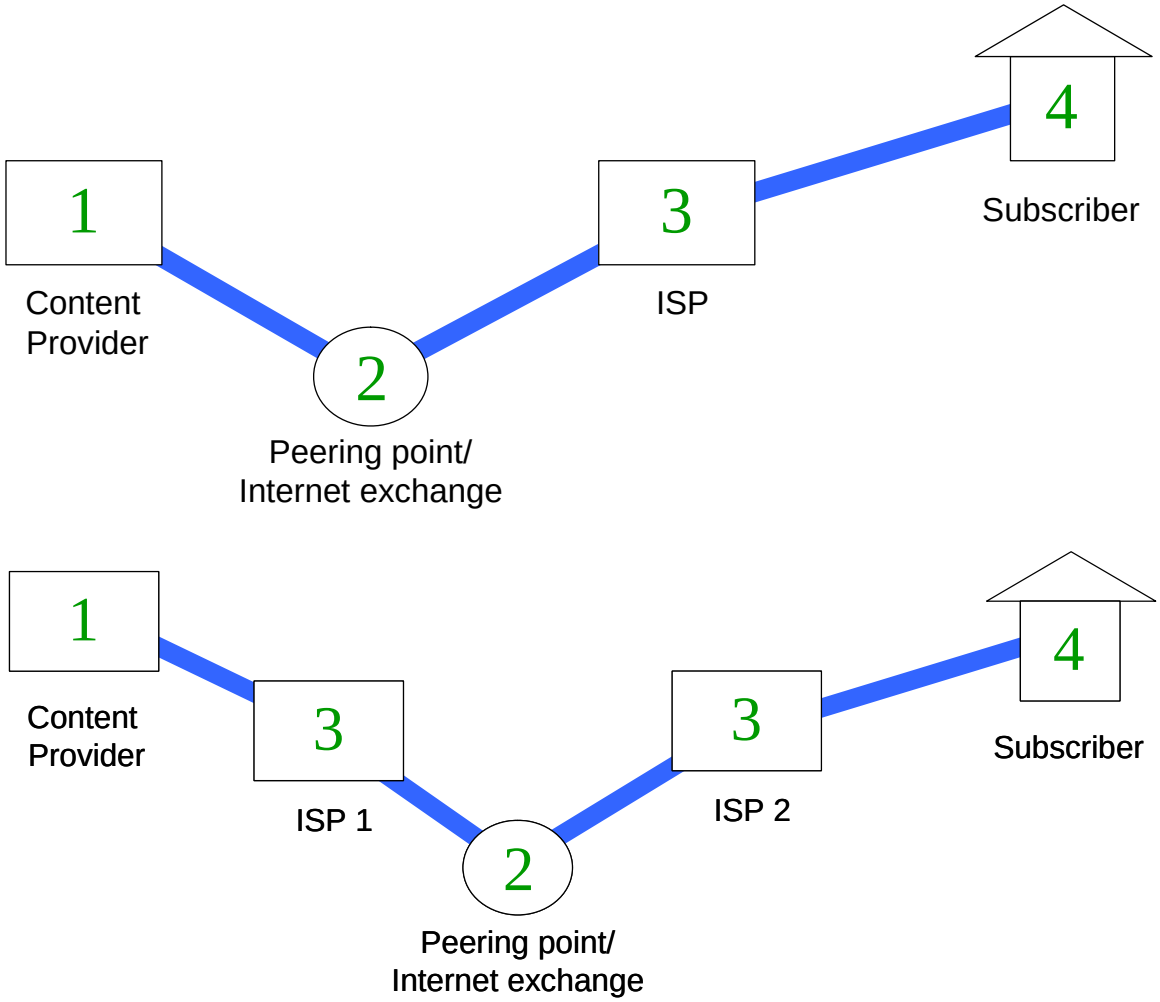
Experienced users may have no trouble navigating the process for assigning priority to their connections but less-sophisticated users could find the process daunting. Even though the process may be too technical for some users, the introduction of traffic shaping tools into home routers shows how traffic shaping can be an effective tool towards improving QoS on a broadband connection, particularly if it is under the user's control.

Traffic shaping points of control

Traffic shaping can be applied at any router along the path of a packet's transmission. However, there are four key points of control where structuring could be applied the most efficiently to change how packets are delivered from a content provider to an end user. Figure 3 gives two hypothetical examples of an external content provider delivering video data to a subscriber. The relationships between the parties indicated in Figure 3 are determined by contracts that typically only cover the exchange and delivery of content but not levels of priority. These are the key points where discussion will take place on how traffic is prioritised.

It must be noted that the four points of control highlighted in Figure 3 are a very simple breakdown of what is commonly a much more complex route that data packets travel. A typical data connection may traverse 10 to 20 routers between a content provider and an end user. The delivery of content with guaranteed quality of service will require co-ordination across the entire path of the packets.

Figure 3. Four key points of control for traffic shaping



In the example shown in Figure 3 (top), the content provider sends video over the Internet to the end-user. The subscriber may or may not pay the content provider for the video but it would be possible for the content provider to sell a differentiated level of video service by controlling how video traffic leaves its network. Requests from paying subscribers could be given priority over requests from non-paying customers. This first point of control (labelled 1) represents the relationship directly between the content provider and the subscriber.

In the example, the content provider needs a relationship with the subscriber's ISP in order to be able to deliver the video. This can be either a direct or indirect relationship where the content provider connects directly to the end-user's ISP (top figure) or connects to an ISP that in turn, has a connection to the end-user's ISP (bottom figure). It is at this second point of control (labelled 2) that the content provider's video passes onto the network of the subscriber's ISP. This second point of control has been the subject of intense debate because it is here that ISPs could require content providers to pay for prioritised access to the ISP's subscribers. This hand-off between networks has traditionally been performed on a best-effort basis. Discussions about Internet peering and paid-transit already take place at the second point of control and any new negotiations about prioritised data could begin to encompass traffic prioritisation as well.

The third point of control is the ISP's own internal network. The ISP controls how data is routed inside its own network. Network administrators could have the network essentially pick up data marked

“best effort” at the second point of control and assign it a certain priority to the user's premises. This third point of control is likely where a large amount of traffic shaping would take place since operators would be able to set parameters once for all routers on the operator's own network.

Finally, the modem/router at the end-user's premises represents the fourth key area of control for packet prioritisation and will likely be the key focus for user-specified traffic shaping. All data flowing between the end-user and the content provider must traverse the modem/router provided by the ISP. This allows the network operator to shape traffic directly from the modem or set-top box at the user's premises. Home users do have some ability to prioritise packets on their internal networks on the subscriber side of the modem's connection.

These four points of control represent a simplified breakdown of network traffic. There are other more complicated scenarios for data transmission and delivery that include caching systems or transit across multiple network operators.

KEY ISSUES AND POLICY DEBATES

While the previous section looked at the key technical aspects, this section will examine the key debates and issues under discussion regarding Internet traffic prioritisation. Most issues fall into one of four categories: Incentives, maintaining access, bandwidth ownership/control and privacy. There is a section dedicated to each.

Incentives

Building new networks

One of the key priorities of telecommunication policy is to create a competitive environment that promotes infrastructure investment. As decreasing voice revenues have hit telecommunication firms, many operators are looking for new revenue streams to tap to make up the difference, particularly as they consider large investments in fibre. Broadband revenues have more than offset shortfalls in voice revenue for many operators but downward pressure on broadband prices from competition has left many operators searching for new revenue. Most telecommunication operators are either providing or preparing multiple play offers that bundle voice, Internet access and video.[7] Another potential source of revenue operators have suggested is the ability to charge content providers and users an additional fee for improved quality of service. In some cases operators have claimed a linkage between their ability to charge for differentiated levels of service and the level of infrastructure investment they are willing to undertake.

What is not as clear, however, is the link between the level of investment in infrastructure and any policy decisions regarding traffic prioritisation. There is considerable debate among experts about the determinants of investment in telecommunications infrastructure. Many network operators feel that traffic prioritisation is a more economical way to deal with increasing bandwidth demands than adding large amounts of raw capacity. At present, operators are continuing to invest large amounts in infrastructure improvements despite the absence of any firm regulatory decisions regarding traffic prioritisation. Economies with healthy competition should continue to see strong levels of investment as operators invest to better compete against one another.

Introducing new QoS applications

There is likely a wide range of new innovations on the horizon that will require better quality of service than the current Internet can provide. The ability to designate priority to certain applications will be a boon for consumers as well as providers as long as there is sufficient competition in the market. The debates should not focus on whether packet structuring for QoS should be allowed but rather on how consumers should be safeguarded from anti-competitive behaviour, whether consumers maintain their ability to choose the services they want and how much control the end user may have over determining which packets receive better transmission.

One likely innovation would be operators selling different prioritised services to different users. For example, an operator could sell one broadband connection that was optimised for VPN access to and from an office for teleworkers. The same operator could also sell services to avid gamers that optimised

ping/response times for online multi-player games. This new range of services could improve the overall Internet experience for a large number of users.

Proponents of a multi-tiered Internet have highlighted that emergency services could receive prioritised transmissions over the Internet. Examples include e-mail and voice traffic during a natural disaster or the connections between vital medical equipment in a patient's home and the hospital. These applications could certainly benefit from the increased quality of service that a prioritised VPN could offer.

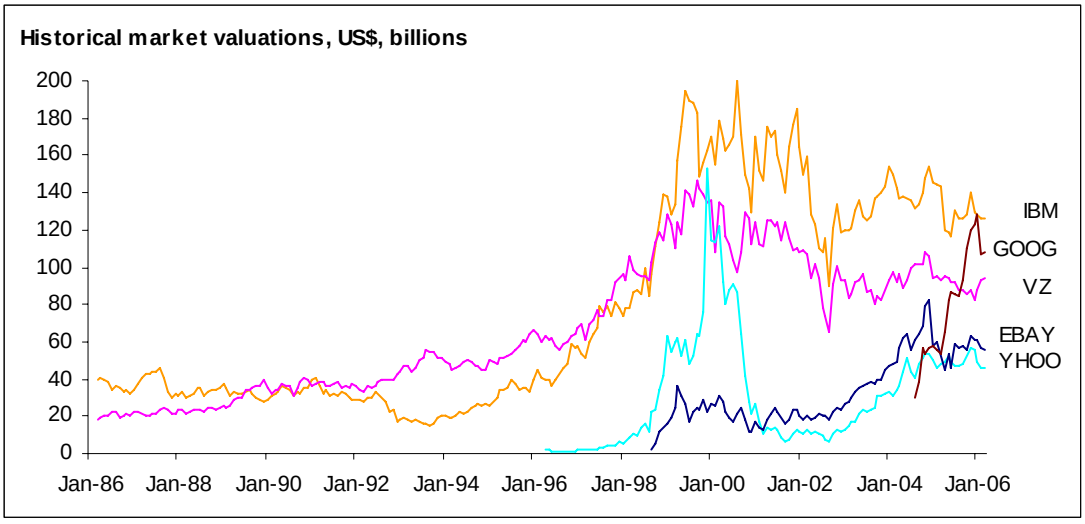
Quality of service enhancements are an important way to promote new services and improve the Internet experience in general for users. However, a key issue with QoS improvements is if they are used to enhance or reduce consumer welfare.

Innovation at the edges of the network

Some opponents of a multi-tiered Internet have expressed concerns that it could diminish innovation at the edges of the network. Some of today's largest Internet companies started out as student projects that flourished under an Internet architecture that provided them the same unfettered access to customers as was available to large, powerful media companies. The concern is large media firms will be able to pay for prioritised transport while small developing firms may not.

Clearly the Internet's current structure has reduced barriers to entry for start-up companies, allowing them to quickly grow and compete alongside long-established firms. Successful companies built on the edges of the Internet include Yahoo, EBay and Google. The market capitalisations of these young companies have grown to rival IBM and telecommunication firms such as Verizon (see Figure 4).

Figure 4. Historical market valuations of new and old technology firms



Ebay, Yahoo, Google and Amazon were able to enter their respective markets on a scale that was not possible before the Internet. The Internet has reduced barriers to large-scale market entry in many consumer markets and this has increased competition and consumer welfare across sectors. Now, some commentators are worried that a multi-tiered structure would introduce a new barrier to entry and stifle innovation at the edges. Any increased barriers to entry will reduce the amount of competitive entry into the market. It is not clear though how the access to higher-speed delivery would be priced and the amount of burden it would place on new firms. On the other hand, the introduction of higher-quality, guaranteed connections could also spur innovation for services that require such connectivity.

It is important to note that firms already make price-based web hosting decisions that limit their potential exposure to consumers and the introduction of prioritised traffic handling may have little effect on small websites. Under the current Internet system, small websites face technical and economic obstacles to doing e-business at a competitive level with established Internet firms. First, small businesses on the Internet rarely host their own content to make it available on the web. Instead, they pay for web hosting services from third parties through an ISP. Website owners and administrators already must decide how much bandwidth they need for their website and pay accordingly subject to market forces.

There are instances where a website suddenly receives a lot of interest, quickly reaches its maximum bandwidth allowance and then ceases to function (sometimes referred to as the "Slashdot" or "Digg" effect). In such cases the site's administrators must pay for a more expensive hosting plan that accommodates the large amount of traffic the site receives. By contrast, established Internet firms often manage their own networks and enter into peering or transit arrangements directly with large Internet providers.

Page load times will likely be unaffected for small firms with "light" web pages under a multi-tiered Internet infrastructure. However, the differences could be much more pronounced for small firms providing time-sensitive, high bandwidth services such as video or voice. For example, companies offering video chat services or high-bandwidth video delivery would likely need to upgrade to higher tiers of service.

Production of new content

The rapid rollout of broadband connections throughout the OECD and the rest of the world has increased demand for content on the Internet. Media companies are moving online with their content but individual subscribers are also producing and developing their own content to put online for others to see. Policy makers are keen to foster this increased participation by subscribers and so discussions about traffic prioritisation must consider the effect of these policies on the Internet's end-users as content creators.

Analysts are now debating where all this new content will be stored and how will it be accessed in the future. There has been speculation that content storage and Internet publishing will be delivered from home networks instead of third-party Internet hosting sites. Under such a scenario users will store all their music, video and photographs on their home computer – or a dedicated home server – that they could then access from anywhere on the Internet and over a number of devices. This model of content storage and delivery would place large demands on the home user's Internet connection because a computer on the home network would become the hub/server for all access to the user's own content.

One potential stumbling block is that most broadband providers currently prohibit end-users from running server software on their computers, effectively blocking the retransmission of material on a home computer outside to the Internet. This could be easily enforced by traffic structuring technologies. Comcast, the largest broadband provider in the United States with 9.3 million subscribers, strictly prohibits users from running home content services which are visible from the outside Internet. Their acceptable use policy states:

> "Prohibited uses include, but are not limited to, using the Service, Customer Equipment, or the Comcast Equipment to: run programs, equipment, or servers from the Premises that provide network content or any other services to anyone outside of your Premises LAN (Local Area Network), also commonly referred to as public services or servers. Examples of prohibited services and servers include, but are not limited to, e-mail, Web hosting, file sharing, and proxy services and servers[8]",

These prohibitions have forced users to find third-party websites that can host their content and make it available on the web. Flikr (digital photographs) and YouTube (video) are examples of websites that aggregate user content and make it available to others for free. These sites both work well for short clips and a relatively small number of photos but they do not address the desire for users to effectively have access to all their digital media from home.

ISPs could respond in a number of ways. They could embrace the idea of consumers accessing their home networks over the Internet and could even offer new services that provided quality of service guarantees and prioritised traffic for any connections to and from the user's home server. It would also be logical to envision broadband plans that would offer "burstable" broadband speeds to users for certain home server applications. In these ways the introduction of a multi-tiered model could benefit home users wishing to access content from their home networks while away.

One of the potential drawbacks of such an arrangement under a multi-tiered Internet is that there may be little incentive for vertically integrated Internet providers to introduce prioritised bandwidth to media content on home servers, particularly if it enables competition directly with their own video or other content offerings on fixed or mobile networks.

Again, the debate reverts back to the level of competition in the market. Efficient markets will allow new ISPs to appear and cater directly to the needs of home subscribers who want guaranteed access to a home server. Providers that may block such a service would be under competitive pressure to change their policies if their competitors offered them. Facilities-based competition and competitive access over the last kilometre, in the areas where it has been granted, may help increase the level of competition by allowing upstart providers to tailor a broadband network to the needs of the user, not necessary those simply of the ISP.

Maintaining access

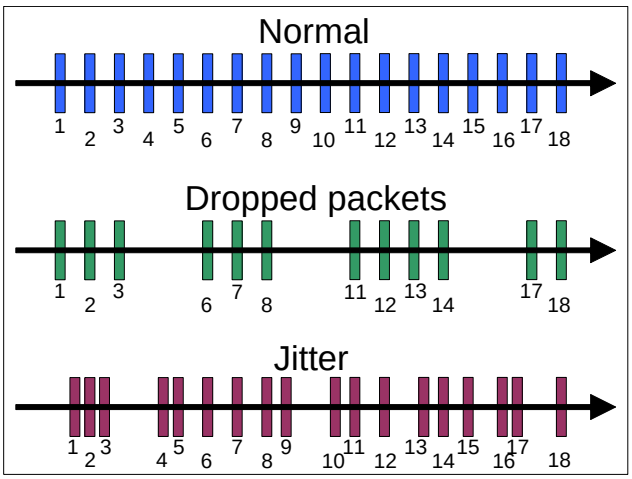
This section will examine how traffic shaping tools could be used in anti-competitive ways to disrupt or block certain communications. The purpose of the section is not to imply that such behaviour will appear in OECD countries. There have been only a few cases of reported anti-competitive behaviour and this is likely due to the high level of competition seen in most OECD markets. Instead, this section is meant to provide an introduction to the type of behaviour regulators and policy makers may need to watch for and monitor.

Some of the applications that could benefit the most from increased QoS on the network are also those that would be the most susceptible to anti-competitive traffic shaping. These applications include remote desktop connection applications, online gaming, live video conferencing and voice communication over the Internet (VoIP).

VoIP calls in particular can be severely disrupted by jitter – a network state defined by packets arriving without a synchronised rhythm (see Figure 5). Packets may arrive early or late for a number of reasons and the "bursty" nature of Internet traffic is one of them. "Bursty" describes data flows characterised by high bandwidth demands for a few seconds and then longer periods of network inactivity.

Voice over Internet services require very low latency and stable traffic steams. Variations in one or more signal characteristics (*e.g.* amplitude, the interval between pulses, or the frequency or phase of successive cycles) can cause jitter that can easily disrupt VoIP streams and render the phone service unusable.[9] Typically a half-second gap in voice traffic is distinguishable to the human ear.[10]

Figure 5. Packet transmissions and VoIP



Network jitter can occur naturally in data networks but can be largely remedied by introducing traffic shaping and packet prioritisation on the network. Traffic shaping technologies can smooth out the flow of data to avoid congestion at routers and even assign priority to the voice traffic. However, jitter could also be introduced in an anti-competitive fashion using the same technologies. This could be accomplished by placing VoIP packets at the back of the queue and upsetting the transmission rhythm of the voice conversation. Users may not be able to determine the cause of the problem easily since other applications will continue to function normally. Even voice calls through an encrypted VPN could be affected. An ISP intent on interfering with other VoIP applications may not be able to determine the contents of an encrypted VPN connection but could still introduce jitter to the transmission and degrade VoIP services if they were being used in the tunnel.[11]

Anti-competitive behaviour

Many of the discussions surrounding traffic prioritisation have focused on the potential anti-competitive threats from network operators who also provide services and can easily configure their networks in such a way as to put other operators at a disadvantage. Some commentators have highlighted the risks[12] while others have claimed such analysis is simply a "solution in search of a problem".[13] Several commentators[14] and regulators[15] as well have sounded a note of caution against introducing regulatory restrictions without sufficient evidence of anti-competitive behaviour.

Under certain circumstances, last-kilometre bottlenecks in all network industries can provide operators incentives to block or limit competing services if there is not sufficient competition in the market.

While there have been relatively few claims of anti-competitive behaviour using packet shaping the potential for some types of anti-competitive behaviour is real and has been highlighted in previous OECD research.[16] The risk is most acute in areas with limited broadband competition although isolated traffic shaping complaints have appeared even in highly competitive markets. For example, the second largest ISP in Korea, Hanaro Telecom, has complained that other ISPs are blocking access to its streaming television service, HanaTV. The service delivers video-on-demand via the Internet to a set-top box. In October 2006 the *Korea Times* reported that major cable providers Curix, C&M and HCN were either blocking the service outright or reducing bandwidth to the site. The provider LG Powercomm also blocked the service. Hanaro estimated that 3 million Korean broadband subscribers could not access the service due to ISPs' restrictions.[17] In December, the Korea Communications Commission ruled that LG Powercomm had to

allow access to the service but also that Hanaro violated its contract with Powercomm by not consulting Powercomm before offering a pay service.[18]

Port blocking, as one form of anti-competitive behaviour, is relatively easy to detect and would quickly receive the attention of users, the national regulatory body or the competition authorities if it were done for anti-competitive reasons. Indeed, there have been relatively few examples of anti-competitive traffic shaping in the OECD so far that have not been quickly resolved. However, detecting degradation of a service, rather than the outright blocking of traffic could be much more difficult since users are not accustomed to guaranteed quality of service in their Internet applications. At times of peak usage pages may load more slowly than usual. However, users may have a very difficult time determining the cause of the slowdown and this may render competition laws more difficult to apply.

There has also been discussion that operators could use prioritised data treatment as an indirect "tax" on their competitors. ISPs may decide to charge for quality of service guarantees for live voice and video applications but include it for free with their own services. The ISP's pricing of the service and the level of quality that was given to non-upgraded live streaming services could effectively determine whether subscribers could economically use competitive providers. In countries where dominant ISPs are regulated they are often subject to non-discriminatory obligations which may prohibit such differentiated treatment.

Regulators may want to focus on less-competitive markets, particularly if there is evidence that network operators have the incentive and capability to engage in anti-competitive behaviour in a way that is not readily discernible to end-users. As an example, operators could favour individual packets simply by sending them over a more direct route to the destination than other packets without affecting queuing. A competitive broadband market with low transaction costs for changing network providers will help discourage anti-competitive behaviour if it does indeed appear.

Unhindered access to information

Some commentators have raised concerns that packet analysis at the router level could be used to curtail free speech or limit access to information.[19] While packet shaping technologies can obviously be beneficial, free speech advocates fear that the technologies could also be used to suppress access to information that governments or ISPs could want to keep out of the hands of users.

The OpenNet Initiative (ONI), a partnership between the University of Toronto, Harvard, Cambridge and Oxford universities, has compiled a series of case studies that examines how Internet blocking and filtering is taking place in certain countries around the world. ONI finds that packet filtering technology at the router level is playing a key role in blocking access to information in China for example. ONI reports that the routers China is using on the backbone network are capable of filtering content bi-directionally at the packet level, imposing up to 750 000 different filtering rules simultaneously.[20]

The amount of competition in OECD countries and an unencumbered press make the likelihood of any ISP blocking political speech through packet snooping or structuring only a remote possibility. However, regulators should be aware that the technology does exist and is currently used for this purpose in some countries outside the OECD.

Security benefits of traffic control

While port blocking and traffic structuring could theoretically be used in anti-competitive ways, these techniques may also be used to enhance security for users. For example, many ISPs have blocked outbound TCP traffic on port 25 as a way to reduce spam being sent out knowingly or unknowingly from users' computers. Instead, mail users must authenticate and are only allowed to send out mail through the ISP's

own mail server. Traffic shaping technologies can also be used as a way to help diffuse the effects of a distributed denial of service attack.

Bandwidth ownership

The role of bandwidth

Bandwidth plays a central role in the debates over network neutrality because bottlenecks in access networks are commonly the trigger that starts packet prioritisation. Those against a multi-tiered Internet structure argue that introducing tiered services will necessarily reduce the quality of service for all other best-effort services if bandwidth remains constant. These claims rest on the assumption that there will be congestion in the last-kilometre network, although this need not be the case. Contention problems may also occur in "back haul" routes in cases where network operators may "over subscribe" bandwidth.

It is important to clarify which bandwidth should be included in the discussion of traffic prioritisation. Cable and FTTH networks may already use a majority of their available "bandwidth" for services other than Internet access. Cable television networks reserve most of the network's capacity for television signals and use only the space of a few channels for Internet access. Fibre optic-based networks may even use separate lasers for video and data services. As a result, policy makers must first decide which measure of bandwidth to choose for analysis. Traffic prioritisation debates should probably focus solely on the frequencies reserved and advertised for Internet data communications. FTTH providers may have 1 Gbit/s of connectivity into a household but only advertise Internet data speeds of 50 Mbit/s. Therefore, the 50 Mbit/s portion of the line should be the key component of the regulatory analysis.

The impact of most types of data prioritisation is linked to the amount of bandwidth available. Broadband connections of 100 Mbit/s in Korea and Japan are likely large enough that assigning prioritised access to certain applications will have almost no effect on the remaining services. However, in September 2005, the incumbent operator's best broadband offer was slower than 3 Mbit/s in 13 of the 30 OECD countries and slower than 10 Mbit/s in 25 of the 30. In these cases, prioritised access to certain applications could have a profound effect on competitive services that rely on best-effort transmission.

In addition, increasing the bandwidth linking end users could decrease the effects of two of the three types of packet shaping. User's whose data traffic was subjected to either best-effort or needs-based prioritisation routing policies would benefit from increased bandwidth across the network. Buffer usage would fall as the outbound capacity of routers increased. Needs-based packet shaping or dropping would only occur during times of excess traffic so bandwidth growth could mitigate its effects.

Increases in bandwidth across the network would not, however, necessarily improve the situation for users on networks subjected to active prioritisation. Network administrators could allocate additional bandwidth on the network to services, applications or ports of their choosing. This means there would not necessarily be an improvement across the board for all Internet applications when more bandwidth was available.

Arguments that traffic prioritisation will become irrelevant as the amount of bandwidth available increases assume that network operators are engaging in either best-effort delivery or need-based prioritisation on the network. Regulators and policy makers should bear in mind that increasing bandwidth may have no effect on certain services under an active prioritisation scenario.

Are the lines paid for?

The debate over multi-tiered levels of Internet service began to make headlines after the head of an incumbent telecommunications operator in the United States was quoted as saying that content providers

should not be allowed to use the ISP's network for "free".[21] However, the current economic system behind data transfer on the Internet is already determined by financial negotiations between different network operators and content providers, either directly or indirectly.

For typical broadband subscribers the Internet appears to be a seamless connection between the user's computer and the rest of the world connected to the Internet. The simplicity of the experience for the user betrays the true complexities and the economics behind data movement on the Internet. Recent OECD work has shown that the movement of data requires a very sophisticated series of peering and transit agreements between the disparate networks that make up the Internet.[22]

The Internet appears seamless to Internet users only because of continuing negotiations between different network operators on how they will carry each other's traffic. If both networks are of similar size or considered equally valuable to one another, they may decide to "peer" with one another and terminate traffic from the other's network for a fee or without payment. If a smaller network wants access to the entire Internet through interconnection with a larger carrier it can also do so but will have to pay for the privilege. This exchange is called "transit" because one network is paying a fee to interconnect to the entire Internet through a larger or more in-demand network.

Figure 6. No "free ride" for Internet data

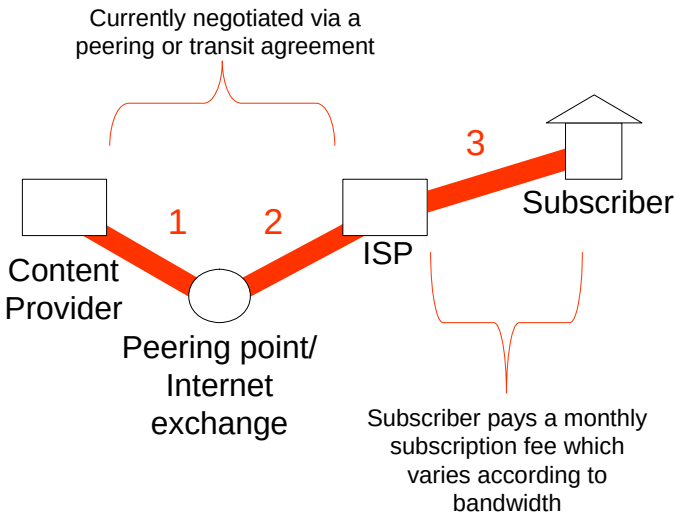


Figure 6 shows a theoretical exchange in the network segments marked "1" and "2". A popular content provider and the ISP decide to exchange traffic between each other by means of an Internet exchange or peering point. Before physically connecting the lines to the exchange they must come to a financial agreement on how traffic will be billed. The content provider may offer search and other services that are likely very attractive to the ISP's subscribers. The ISP has an incentive to have a fast and low-cost connection to the content provider – if its sites are popular among the ISP subscribers. The content provider may also have an incentive to interconnect in order improve its response time to the ISP's subscribers and to be able to serve ads and services more effectively.

When the content provider and the ISP enter negotiations they examine historical and potential traffic flows before deciding if they will both benefit from a peering arrangement or if the situation merits paid transit. During the course of the negotiations the ISP may determine that the content provider, needs direct access to the ISP more than the ISP needs direct access to the content. If this is the case, the content provider would be required to pay transit to have a direct connection to the ISP's subscribers. However, the counter situation is that as a popular content provider rolls out more services the ISP's subscribers in turn

may demand better access from the ISP back to the content provider. This will make the content provider a more attractive peering partner.

The important point is that the peering/transit discussions already consider the different traffic flows between providers, even if these current agreements do not include quality of service differentiation. Payments are made when the assets of one network are seen as more valuable than those from the other. The direction of payments for prioritised traffic will depend on the respective level of competition in both the content and ISP markets, as well as the attractiveness of each respective network. A mechanism already exists for content providers and ISPs to negotiate the transfer of data between networks and the system works well.

Who provides the lines?

Platform competition for broadband varies greatly throughout the OECD. Some markets have strong DSL/cable competition while others are struggling just to upgrade the telephone network to DSL. Subscribers in countries relying on platform-based competition have typically been limited to two or fewer very-high-speed providers, although other platforms may be emerging. The roll out of municipal and regional fibre networks to subscribers has introduced much-needed connectivity in some under-served areas and improved competition in areas with relatively few broadband choices. These networks are graining ground in several OECD countries. In the United States, for example, there are 936 communities in 47 states served by fibre to the home (FTTH) with 671 000 active connections and 4 million homes passed.[23] A growing number of these fibre lines in the United States are provided by municipal and community networks. The total number of municipal fibre subscribers may still be low as a percentage of total broadband in the OECD but there is growing interest in fostering competition through such open-access networks.

Even within a given country the level of platform competition may vary considerably between rural and urban areas. Competition over the local loop is particularly important in markets lacking a developed facilities-based competitor.

Debates over traffic prioritisation have also renewed interest in finding new ways to finance, build and manage last-kilometre networks. There is increasing interest in open-access networks where the provision of physical infrastructure and services is separated. Open access networks[24] may be run co-operatively, by public utilities or by a municipality, or through a public-private sector partnership. Their key benefit is that they can allow a range of competitors to offer services over the same physical infrastructure. Some of the renewed interest in open-access networks is the result of a lack of efficient platform-based competition on the last kilometre.

The city council of Amsterdam in the Netherlands has approved an open-access project called Citynet (http://www.citynet.nl) that will install fibre-to-the-premises in the city using a public/private sector partnership. The network will be “open access”, meaning that any competitive operator would be allowed to interconnect and sell services over the network. Public utility companies have also entered into the market for broadband services in some OECD countries and provide an extra layer of competition in the market. A Danish power utility SEAS-NVE is building out a fibre-optic network to users that should extend to 50% of its subscribers in the next ten years. Consumer-owned utility companies such as SEAS-NVE have been able to take advantage of their comparative advantage in building out public infrastructure such as the electricity grid and apply it to the planning and rollout of fibre infrastructure.

Open access municipal networks could play a key role in the debate over prioritisation because they provide a platform for service-level competition that could significantly reduce any anti-competitive effects of a multi-tiered Internet structure. An open-access policy allows a variety of providers to offer

video, voice and data services in the same market and over the same physical infrastructure. This increased competition reduces the ability of any one provider to block services or demand excessive fees for prioritised data traffic while still providing the benefits of QoS offered by a multi-tiered system. Another promising development is the opening of existing ducts or the building of new open-access ducts or pole systems by governments which can be used by firms wishing to roll out or expand networks. These approaches have been referred to as "passive" infrastructure since they are operator-neutral and simply rent out space for an operator's own physical equipment. Examples include CERIU in Montreal[25], Canada and the government's 22@ Barcelona project in Barcelona, Spain.[26]

A growing number of cities across the OECD are beginning to plan and build-out municipal Wi-Fi networks that are either free or low cost to consumers. These networks could also increase competition in the market and reduce the power of individual firms to charge excessive fees for data prioritisation. However, municipal Wi-Fi and WiMAX networks cannot offer similar speeds to fibre and competitive access over the lines would be more difficult. Subscribers to Wi-Fi networks will not be able to access all the same types of services as users on dedicated wire connections. For example, HDTV streaming over fibre is available in the Netherlands[27] but many Wi-Fi rollouts only offer average speeds of 1 Mbit/s[28] – roughly one tenth the speed needed for one HDTV stream. Therefore, the bandwidth available to users over a municipal Wi-Fi or WiMAX network will likely be considerably lower than for FTTH deployments and will complement, rather than replace, home broadband wired Internet service.

Municipal access networks are a subject of intense debate in several countries. For example, the European Commission has opened an investigation under EC Treaty state aid rules into the Citynet project in Amsterdam. Over the past two years, the Commission has issued a series of state aid decisions finding aid was justified in rural and remote access areas to promote broadband. The Commission has been more cautious however in assessing state-funded projects in metropolitan areas where broadband services are already available under competitive conditions. Some telecommunication providers have also expressed concern that the provision of municipal-owned networks could inhibit existing and future investment by the private sector.

Bandwidth entitlement

There is a significant level of confusion within the debate over traffic prioritisation as to what type of connectivity subscribers are entitled to have over their broadband connections. Broadband plans are commonly sold with unlimited data transfers, although excessive use often goes against published acceptable use policies and may not be tolerated for long. In March 2006, for example, BT sent letters to more than 3 000 customers who had been downloading between 100 and 200 gigabytes of data per month, notifying them that they needed to pay more for their higher use or risked having their contracts terminated.[29]

Operators in some OECD countries have introduced bit caps on broadband connections. These are often limiting and require subscribers to pay higher monthly fees for unlimited usage. In countries such as Australia, users typically select a monthly broadband plan based on the amount of traffic they plan on using rather than by the speed of the connection. Low-use subscribers can opt for bit caps in exchange for lower monthly subscription rates. For example, Telstra's Bigpond subscribers pay AUD 29.95 for 200 MB of traffic per month or double the price for unlimited data traffic.[30]

Bit caps are typically put in place to discourage heavy bandwidth users from taking too large a share of overall network resources. Some analysts have said that a multi-tiered Internet could be used in a similar way to help solve this "tragedy of the Internet commons" where overuse of bandwidth by a few applications can slow down connectivity for all other services. They suggest that requiring users to pay for higher quality of service can help ensure that they essentially "pay" for the true costs of the bandwidth they

are using. Others counter that many of these problems can be dealt with through clear acceptable use policies.

From an economic perspective, "all-you-can-surf" broadband plans are built around the assumption that the average user will consume only a moderate amount of bandwidth per month. There are broadband users who consume a disproportionately large amount of bandwidth and are subsidised by users who may simply use broadband as a way to download their e-mail more quickly. The low bandwidth users essentially subsidise the high bandwidth subscribers through their identical monthly fees.

Proponents of a multi-tiered Internet claim that such a system could allow operators to charge prices for service that are more in line with actual usage. Low bandwidth users could be given priority treatment for their e-mails in exchange for unused bandwidth each month. High bandwidth users may be willing to forgo priority on all traffic in exchange for keeping bandwidth usage allowances high. This would allow more equitable terms for all subscribers without introducing bit caps that tend to discourage Internet use. Opponents of a multi-tiered system argue that such differentiated services are simply another way to segment markets and recapture consumer surplus.

It is clear that consumers would benefit from better information about what they are buying each month when they pay their broadband bill. They need to know if they are purchasing unlimited access to the Internet at a given bit rate or if there are actually undisclosed usage caps that will trigger the termination of the user's service at some point. Many of the debates over traffic prioritisation could be clarified if ISPs provided more guidance to users about the limitations on use of their connections.

Privacy issues

Packet shaping and encryption

As highlighted in the technical section, routers have the ability to examine the contents of packets traversing the network and process rules to determine how they will be handled. Some of the prioritisation decisions that routers make will require the router to examine the contents of entering packets. This phenomenon is sometimes referred to as "packet snooping" or "packet sniffing" and it allows the router to determine the contents of the packet before assigning it a certain priority level.

Encryption technologies give users the ability to protect the contents of their packets from being read by routers (or other computers on the network) during transmission. However, network operators can still examine information in the IP header such as origination and destination IP addresses and port information, all which could be used in decisions to block or prioritise packets.

In addition packet shaping technologies do not necessarily need to be able to see inside a tunnel to make a good determination of what type of traffic the tunnel is transmitting. Packet shaping equipment, for example, may be able to detect a steady stream of packets that was roughly the same size flowing in both directions with a metronome-like regularity over the connection and impute that there is a voice call taking place.[31]

Distributed encrypted networks such as Tor (The Onion Router), I2P and Freenet could help prevent others, including an ISP, from determining the content *or* final destination of packets sent out on to the network. Encrypted tunnels only encrypt the data contents (payload) of the packet but the header information, with port and IP address information is in plain text and easily readable. This means that packet sniffing technologies could still learn a lot about the contents of the packets by observing where they were going and from which IP address they were sent.

ISPs could also slow down traffic from certain domains and would not need to rely on being able to see the contents of the packets in order to discriminate against certain traffic. Distributed encrypted network routers such as Tor routers work around this by routing all packets through a series of computers to masque the final destination of the packet. Data packets on the Tor network follow a random pathway through several servers so no single point on the network knows where the packet originated or where it is going.[32] Tor routing could prevent ISPs from blocking access to certain ports or IP address. However, Tor may also be used to circumvent certain security measures or beneficial traffic blocking, such as sites with malicious content. They can also be used to masque illegal activity.

Personally identifiable information

Packet shaping technologies give network operators the ability to examine header information and the payload of packets before making decisions on how the packets are then delivered. Network operators have long had the ability to examine data in the packets flowing over their networks but the proposition of a multi-tiered Internet significantly increases the number of routers that would actively be examining packets.

The original architecture of the Internet provided less incentive for operators to install packet shaping technologies across their networks because their implementation would reduce the amount of traffic that a router was able to pass on in a given period of time. However, if proposals for a multi-tiered Internet do go forward then there will be an economic incentive for operators to equip more routers throughout the network with technology to examine packets more closely.

Anytime technologies gather data, particularly those that could be personally identifiable, there may be a need for oversight on how that data is gathered, stored and used. Under the current Internet architecture routers have no need to routinely examine the payload of packets traversing the network before passing them on. However, the introduction of packet shaping throughout the network would require the routers to examine the payload of packets that were associated with IP addresses, which in some OECD jurisdictions may be considered to be personally identifiable information and raise privacy concerns.

There is no indication that network operators have any plans to gather and store personally identifiable information at the router level but policy makers should be aware that the wide spread adoption of packet shaping technologies at least gives operators the ability to flag packets based on the payload (contents) of the packet and the IP address of the user. This could, in turn, raise fears that data could be easily processed for purposes unrelated to traffic routing. The privacy issues may be complex under a multi-tiered Internet structure and could warrant particular attention by privacy specialists.

POLICY CONSIDERATIONS

This section on policy considerations has three parts. The first section deals with the key role competition plays in the debate and provides a short analysis on what market structure analysis should consider. The next section covers specific policy suggestions tailored for situations where policy makers decide to allow market forces to guide traffic prioritisation decisions. The suggestions contained in the section focus solely on helping markets function more effectively and improving transparency to end users. This section does not put forward suggestions for cases where markets may be deemed insufficiently competitive and may require regulatory intervention. Instead the section concludes with some possible questions that regulators may face in less-competitive markets.

Level of competition

This paper has emphasised that consumers in markets with strong and effective broadband Internet access competition will likely benefit most from the introduction of quality of service and may be at the least risk of any anti-competitive traffic shaping behaviour by ISPs. Anti-competitive behaviour can appear in all types of markets, even those judged to be competitive. However, the risk of anti-competitive behaviour will typically decline as the number of effective competitors in a market increases.

Therefore, the level of competition in the broadband market will be one of the most important determinants of whether regulators need to implement safeguards against anti-competitive traffic prioritisation. Defining the market and determining the level of competition are not as simple in broadband Internet access markets as in other network industries such as electricity, water and rail. Data services may be available over multiple platforms (*e.g.* dial-up, DSL, cable, 3G) but different data rates may mean they are not easily substitutable. Therefore, regulators cannot simply count the number of data providers in a given region and assume that the market is sufficiently competitive. Regulators may need to undertake a careful market analysis to determine whether households have effective choices for substitutable broadband Internet access. Which Internet access technologies constitute substitutable broadband will be a key issue in determining market competition.

As an example, 3G technologies, including forthcoming High Speed Packet Access (HSPA) are capable of a maximum bit rate of 14.4 Mbit/s per user on a cell. However, the UMTS Forum estimates that the typical throughput of one of these technologies, High Speed Downlink Packet Access (HSDPA) will be 500-700 kbit/s with a maximum of 40 users per cell.[33] At the other end of the bandwidth scale, FTTH network operators in Japan and Korea currently offer users 100 Mbit/s connections, while Hong Kong, China's HKBN Limited now offers 1 Gbit/s (1 000 Mbit/s) connections. There will indeed be some market overlap for 3G and FTTH but the technologies might instead be more complementary than substitutable.

Policy makers may want to distinguish between lower speeds available over wireless networks and higher speeds possible over wired broadband. This distinction is vital because some of the services at greatest risk of anti-competitive packet degradation are those that require faster bandwidth than current, and even future wireless technologies may be able to support. For example, HDTV will require roughly 10 Mbit/s of bandwidth capacity for each channel streamed to a home, based on today's available compression rates. 3G and other mobile wireless technologies such as WiMAX will not be able to provide that amount of bandwidth to individual subscribers.[34]

After defining the relevant market, policy makers can then determine if there is sufficient competition for consumers. Many OECD markets do have healthy competition for high-speed broadband Internet access through infrastructure-based competition, local loop unbundling or both. In some countries, competitive access to the local loop supplements infrastructure-based competition between cable and DSL, and, in some instances, fibre. Countries with both types of competition such as Korea, the Netherlands, Denmark and Belgium thus are likely to have the most competitive markets to counterbalance any anti-competitive packet shaping incentives from individual ISPs.

Competition for connections over the last kilometre keeps the market power of Internet service providers in check. There are, however, some OECD countries where consumers are limited to one, or possibly two operators providing high-speed Internet services. In these cases Internet service providers may have sufficient market power to pursue anti-competitive objectives.

A number of other OECD countries have strong competition on one type of infrastructure but lack an extensive parallel broadband network that is capable of providing broadband services to consumers today or in the near future. In such cases policy makers must examine the level of competition on the single line, typically the local loop, and determine if competition is strong enough that regulators can take a "hands-off" approach to traffic shaping technologies in the last kilometre. While unbundling has encouraged competition in many OECD countries there can be situations where local loop unbundling is mandated but the market is still not deemed competitive.

There remain a few countries in the OECD that rely solely on infrastructure-based competition in the high-speed Internet market. Policy makers in these countries should take special care when evaluating the progress of parallel infrastructure development, keeping in mind that wireless technologies are not perfectly substitutable for physically wired connections and that some subscribers will only have access to one or two providers who could offer connections faster than 10 Mbit/s in the foreseeable future. Game theory analysis should be a key component of the decision, particularly in regard to markets with a duopoly market structure.

Negotiations between content providers and infrastructure operators

One of the key questions raised during ongoing traffic prioritisation debates is whether ISPs should have the ability to charge additional fees to content providers in exchange for higher priority for their packets. ISPs and large content providers may already be in negotiation for peering or paid transit so prioritised packet treatment could simply be an extension of these discussions, even if historical negotiations have been for "best effort" traffic handling. The relative bargaining power of the ISP will be related to a variety of factors such as the number of subscribers on its network, the type of customers on its network (residential, end-user businesses, content providers), and the geographic scope of its network.

From the current state of the discussions it may be premature for governments to become involved at the level of network-to-network traffic exchange and demand neutral packet treatment for content providers. The concerns of smaller, start-up firms could be addressed through the pooling of demand for Internet access via a common ISP. Start-up content firms may not have the means to bargain favourably with large broadband providers but their own ISPs may. It would not seem far-fetched for large ISPs to agree to peer traffic at higher levels of priority amongst themselves.

If governments can effectively address competition issues at the local loop level then the need for regulation at the backbone level of the network would likely diminish. The solution is not yet clear and for the time being it may be better for policy makers to focus on fostering competition access in the last kilometre.

Market-based consumer protection under a multi-tiered Internet

The most effective way to ensure that traffic prioritisation does not distort competition is to ensure that broadband markets remain or become competitive. There are several steps policy makers could take to further increase competition in markets where competitive forces are determined to be sufficient to protect consumers from anti-competitive packet prioritisation.

Since competition serves to protect consumers from unfair traffic shaping, government policy makers could consider additional steps to reduce barriers to entry in broadband markets. Many OECD countries have found local loop unbundling to be effective because it allows new entrants to run networks that are managed differently than the incumbent's and adds a competitive threat to any provider considering anti-competitive packet shaping. It also helps ensure that consumers can switch away from an ISP using traffic prioritisation that effectively limits access to content and services that the consumer wants.

Governments should also promote infrastructure-based competition and there are various approaches policy makers can take. First, governments can decrease entry barriers by facilitating better right-of-way (RoW) access to new entrants. New providers should be able to collaborate with existing RoW holders such as water and electrical companies to jointly connect homes. Governments, particularly at the local level, can also look for innovative ways to help facilitate new infrastructure rollout by allowing easier access to ducts and existing poles. Introducing new wireless spectrum could increase competition for some services but not those that require very high bandwidth.

There may be considerations other than the number of substitutable broadband providers in a market. If consumers face high switching costs they will be reluctant to pay to leave one broadband provider for another. This consumer “stickiness” gives operators more leeway to unfairly prioritise their own services over competitors. Regulators can consider imposing rules that protect consumers and allow them to quickly and effectively change providers, at minimal or no expense and without service disruption if their operator's routing policies change to degrade or block services that were unaffected when the subscriber signed up for service.

Often high switching costs for consumers are the result of high switching costs for providers. Operators may provide heavily discounted installations and modems in exchange for a specified contract duration. Any regulatory change allowing consumers to terminate a contract early due to changes in the service may push ISPs to re-evaluate their marketing and business plans with regard to service installations. Competitive operators may have additional costs connecting a customer since they often must pay large up-front fees to incumbents to take over or give back an unbundled line. Competitive operators are reluctant to pass along these costs in installation fees (as they discourage new subscriptions) and would much rather recoup them as disconnection fees (as they discourage cancellations). These fees could have a detrimental effect on users' ability to switch operators and create high enough transaction costs that operators may have an incentive to implement unfair packet shaping. Therefore, any reduction in fees that subscribers must pay to switch broadband operators will increase competitiveness amongst providers.

Other safeguards that policy makers could consider include encouraging or requiring ISPs to clearly state their broadband packet shaping policies to consumers before they sign up for broadband and keeping existing subscribers aware of any changes. Rules could be applied to ISPs requiring them to provide real, achievable broadband speeds estimates and what portion of the connection was dedicated to best-effort service. These could be similar to line-test information already provided by some DSL providers when potential subscribers verify service availability. Notifications similar to those shown in Figure 7 could be encouraged or required in advertisements for broadband services. The “reserved by ISP” portion reflects any active prioritisation policy that assigns bandwidth to the ISP's own services supplied over the data

connection that is not automatically released when the subscriber is not using the service. ISPs could be required to list applications that are traffic shaped, restricted or disadvantaged by routing policies.

Figure 7. Example of the type of disclosure that ISPs may be required to provide consumers

Bandwidth

Total	Effective
20.0 Mbit/s ↓	12.0 Mbit/s ↓
	Reserved by ISP
2.0 Mbit/s ↑	0.8 Mbit/s ↑

Applications/Services

Application	Status
Web browsing	Open
Video	Restricted
Audio	Restricted
Peer-to-peer	Restricted
Gaming	Open
VPN	Open

Some ISPs have moved ahead and clarified their traffic shaping policies to consumers. While this may initially lead to some consumer backlash when policies are announced, such transparency is ultimately better for consumers and the market as a whole. For example, the Australian ISP Exetel announced that it has begun "de-prioritising" peer-to-peer traffic between the hours of noon to midnight.[35] Another example is the ISP PlusNet in the United Kingdom which publishes the priority it assigns to various types of traffic on its website (See Table 3).

Table 3. Making traffic-shaping policies public: PlusNet (United Kingdom)

Priority category	Services, protocols affected	Level of priority
Gold	HTTP/HTTPS, SMTP, IMAP, POP3, PlusTalk	Priority Traffic
Silver	Gaming, VPN, network services, other VoIP services, FTP, SSH, Instant Messaging, IRC, other TCP/UDP/other traffic, P2P/Usenet for PAYG/Lite accounts. 15GB of Usenet traffic. Text only news from PN's server and external text usenet servers.	No slow downs except in emergency, such as a pipe failure.
Bronze	P2P for all accounts bar PAYG/Lite, BB+ usenet, Usenet traffic over 15GB offpeak hours	
256 kbit/s	Usenet traffic over the 15GB limit during daytime and peak time hours.	8 AM and Midnight

Source: http://usergroup.plus.net/shaping.php, 10 January 2006.

Increased transparency, as highlighted by the Australian ISP, can also lead to more efficient use of network resources. Users who understand the policy have an incentive to shift legitimate peer-to-peer downloads to off-peak hours on the network to obtain higher speeds. This parallels experiences with electrical networks and peak-load pricing where users may schedule large electrical appliances such as water heaters and dishwashers to run late at night to take advantage of lower electricity prices.

In an effort to increase transparency, regulators could encourage or require ISPs to make public their traffic shaping policies and then help publicise this information. In the absence of any consumer-oriented sites highlighting the information, the regulator could create a consumer-focused website for broadband where operators were required to update detailed lists of which applications or services were blocked, shaped or prioritised. ISPs could be required to provide updated information to the regulator when there were significant changes to routing policy. Any new reporting requirements would need to be very simple so as to not unduly increase the demands on industry or regulatory staff.

Some regulators already have websites in place that could include new traffic prioritisation information. The Irish regulator ComReg has an interactive site where consumers can compare the cost of personal/non-business mobile, home phone and broadband price plans (http://www.callcosts.ie). The Swedish National Post and Telecom Agency is working actively on the production of comparative quality information for consumers.[36] In other cases, market mechanisms have encouraged private sector companies to produce similar outputs. The French research group Ariase produces a matrix of VoIP termination prices across all telecommunication operators in France.[37]

Policy makers may also need to re-examine existing competition laws to ensure they can address any abusive practices that could appear under a multi-tiered Internet structure. Competition authorities will need a strong and effective competition law that will be able to address the intricacies of network traffic. Consumers must also have a simple way to lodge complaints if they suspect anti-competitive behaviour and there must be a mechanism in place to investigate allegations. Competition law will likely be one of the key mechanisms governments use to stop anti-competitive traffic shaping if it appears.

Consumer protection and information disclosure

Many of the potentially negative issues associated with a multi-tiered Internet structure could be addressed by better information disclosure and consumer protection rules. Consumers will be much better protected in markets where they can make informed choices between competing broadband providers and are free to switch quickly and inexpensively in the event that detrimental traffic shaping occurs.

Table 4. Broadband "burn rates" – October 2006

How quickly consumers will reach published ISP bit caps if downloading at advertised maximum speed

	Down (Mbit/s)	Bit cap (Megabytes)	Minutes to reach bit cap	Implied contention ratio (x:1)
Optus (Australia)	9 900	100	1	32 522
Optus (Australia)	9 900	300	4	10 841
Woosh (New Zealand)	1 600	200	17	2 628
Optus (Australia)	9 900	2 000	27	1 626
BT (United Kingdom)	8 000	2 000	33	1 314
Woosh (New Zealand)	1 600	500	42	1 051
Bigpond (Australia)	1 500	500	44	986
Tele2 (Belgium)	512	250	65	673
Telecom (New Zealand)	2 000	1 000	67	657
Slovak Telecom (Slovak Republic)	1 024	600	78	561
Vodafone (Iceland)	6 000	4 000	89	493
Optus (Australia)	9 900	7 000	94	465
BT (United Kingdom)	8 000	6 000	100	438
Bigpond (Australia)	256	200	104	420
Telecom (New Zealand)	256	200	104	420
Bigpond (Australia)	512	400	104	420
Belgacom (Belgium)	512	400	104	420
AON (Austria)	1 024	800	104	420
Internode (Australia)	24 000	20 000	111	394

Consumers need to know exactly what they are buying when they sign up for broadband. The introduction of traffic shaping technologies on broadband networks creates a difficult information gap that needs to be addressed in Internet markets. This conveyance of information is important because there is

evidence that some broadband subscribers may not choose optimal plans when signing up for broadband services. In October 2006, the OECD gathered pricing and offer characteristics on 373 broadband Internet access offers across the 30 OECD countries. A number of offers available to subscribers stood out because of how quickly users would reach the ISP-imposed bit caps if the connection were operating at advertised speeds. Table 4 shows a sampling of how many minutes of downloading at the advertised speed would be possible before reaching the subscription's monthly bit cap. In the most extreme case, a user would reach the bit cap after just one minute of downloading at full speed. At that point, the provider then reduces the connection to dial-up speed for the remainder of the month. In such a case subscribers either should look for a less-expensive/slower speed connection or one with a higher bit cap. This type of mismatch between download speeds and bit caps highlights the information gap that many consumers face when approaching the various offers from ISPs.

As Table 4 has highlighted, some consumers do not understand the limitations of their broadband offers even when advertised speeds and bit caps are published as part of the original offer. The information gap is then likely more severe for traffic shaping policies since broadband providers, particularly those who already engage in traffic shaping, typically do not make public the types of traffic that are blocked, the amount of bandwidth assigned to specific applications, and whether their routing policies rely on best effort, needs-based, or active prioritisation. Certainly a large number of ISPs have been alleged to shape certain traffic such as BitTorrent[38] but very few ISPs make this type of information public.

Regulators should consider encouraging or requiring better disclosure from ISPs of the types of traffic shaping they may use. ISPs should also inform consumers when there are services that are blocked or degraded to an extent that performance could suffer. This information should also be publicly and easily accessible for consumers before they enter into contracts with providers. The need to provide consumers with adequate and accurate information about commercial transactions is a core element of consumer protection law and policy in OECD countries. The OECD *Guidelines for Consumer Protection in the Context of Electronic Commerce* (1999) cover online contracts and include provisions to ensure transparency regarding the terms and services of business-to-consumer transactions. New protections for consumers may also need to be considered to allow them to terminate contracts free of charge where post-purchase (traffic shaping/service blocking) changes occur.

Some regulators are already taking steps in the direction of ensuring that consumers have good information about the services they are subscribing to and are able to switch providers easily. In April 2006 the regulator in the United Kingdom, OFCOM, announced that it was undertaking a study of the process of signing up for and switching broadband providers.[39]

Government involvement to protect consumers

Quality of service will require some packet prioritisation on networks, even in a regulatory environment that puts restrictions on traffic prioritisation. Initially, policy makers may want to consider putting forward a set of guidelines establishing some fundamental principles that network operators should follow when implementing data prioritisation (see Box 2).

Box 2. United States Federal Communications Commission Policy Statement

The United States Federal Communications Commission (FCC) released a policy statement concerning the Internet and broadband in September 2005. The statement consists of four points that are tailored to "ensure that broadband networks are widely deployed, open, affordable, and accessible to all consumers". The Commission adopted the following four principles:

- *To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet*, consumers are entitled to access the lawful Internet content of their choice.
- *To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet*, consumers are entitled to run applications and use services of their choice, subject to the needs of law enforcement.
- *To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet,* consumers are entitled to connect their choice of legal devices that do not harm the network.
- *To encourage broadband deployment and preserve and promote the open and interconnected nature of the public Internet,* consumers are entitled to competition among network providers, application and service providers, and content providers.

Source: http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-05-151A1.pdf.

Guidelines, such as those put forward by the FCC, could form a policy basis for any *ex-post* action that may be required if problems are not solved by market mechanisms alone. Policy makers could still allow both need-based and active prioritisation as long as consumers had a clear choice on how prioritisation would be applied on their line. In this sense the "neutrality" of the network could be achieved by allowing consumers to decide which services were assigned different levels of priority.

In other cases, existing regulatory tools may be applied to dominant firms. For example, the European Union regulatory framework requires dominant operators to offer access to their competitors as a way to promote competition. The European Commission has also recently highlighted the role of national regulatory authorities (NRAs) in protecting consumers from certain forms of unwanted traffic prioritisation. As part of its review of the EU Regulatory Framework for electronic communications networks and services, a Commission staff working document has stated:

> In general, a competitive market means that if one supplier seeks to restrict user rights, another can enter the market with a more 'open' offer. In Europe, the regulatory framework allows operators to offer different services to different customer groups, but does not allow those who are in a dominant position to *discriminate* between customers in similar circumstances. However, there is a risk that, in some situations, the quality of service could degrade to unacceptably low levels. It is therefore proposed to give NRAs the power to set minimum quality levels for network transmission services in an NGN environment based on technical standards identified at EU level.
>
> The existing provisions for NRAs to impose obligations on operators with significant market power, and the powers for NRAs to address access and interconnection issues could be used to prevent any blocking of information society services, or degradation in the quality of transmission of electronic communication services for third parties, and to impose appropriate inoperability requirements.[40]

If market mechanisms and existing safeguards fail to offer sufficient protections to consumers then regulators may consider a set of policies on traffic prioritisation. ISPs could also take certain steps voluntarily and proactively as a way to reduce the need for any government intervention.

This paper focuses only on cases where market mechanisms are left to guide the development of traffic prioritisation. However, there are several key policy questions that regulators will face if they indeed decide that a market is not sufficiently competitive to protect consumers from anti-competitive traffic shaping and that it may require regulatory intervention.

i) Which parts of a provider's network may be subject to regulatory intervention? Would traffic shaping restrictions be sufficient if they were only applied over the last-kilometre of a connection or would they need to be applied deeper in an operator's network (*e.g.* the "middle kilometre" or backhaul segment between points of presence and Internet exchange points?).

ii) Would it be possible to still allow traffic prioritisation on the network but give consumers considerable control over which applications received priority over their last-kilometre connection?

iii) How would traffic shaping connected to the security and basic functioning of the network be treated? For example, would ISPs still be allowed to block ports commonly used for SMTP as a way to control the release of spam e-mail messages from bot-infected computers?

iv) How would an operator's video services be treated? Should a telecommunications operator using separate lasers for video transmissions over fibre be subject to traffic prioritisation restrictions in the same way as an operator providing IPTV streamed over a standard data connection would? If video were streamed by the operator over the basic data connection should users be able to "reclaim" that bandwidth for their own uses if they decline the service or switch off the set-top box?

v) Would requiring operators to offer the option of a basic, unshaped subscription to consumers help alleviate some of the anti-competitive issues or could traffic shaping in the "middle kilometre" still be an issue?

Mobile network neutrality

This paper examines the debates surrounding traffic prioritisation on wired networks but many of these issues are migrating to mobile data networks as well. Indeed, traffic prioritisation is much more prevalent on mobile networks than fixed networks, in part due to rigid bandwidth constraints. Many mobile data networks already block heavy bandwidth applications such as peer-to-peer file sharing. Others have blocked VoIP and streaming data services as well.

Many of the consumer protection and information disclosure issues highlighted for the fixed network should carry over to mobile networks as well. Indeed, as more users subscribe to 3G data services there is a need for clarity on what users can and cannot do with their connections.[41] This paper has also highlighted how mobile and fixed broadband may need to be considered as separate markets. As a result policy makers should not assume that decisions regarding traffic prioritisation can be directly applied to mobile networks. Indeed, this is an area that may warrant future research.

GLOSSARY

Acronym	Description
3G	Third-generation mobile network
ADSL	Asymmetric Digital Subscriber Line
ADSL2+	Asymmetric Digital Subscriber Line 2 plus
AH	Authentication Header
AS	Autonomous System
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
ESP	encrypted security payload
FCC	Federal Communications Commission
FIFO	First In, First Out
FTTH	Fibre To The Home
Gbit/s	Gigabits per second
HDTV	High Definition Television
HSDPA	High Speed Downlink Packet Access (HSDPA)
HSPA	High Speed Packet Access
IP	Internet Protocol
IPSEC	Internet Protocol Security
IPTV	Internet Protocol Television
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISP	Internet Service Provider
JPEG	Joint Photographic Experts Group
KB	Kilobyte
kbit/s	Kilobits Per Second
LAN	Local Area Network
MAC	Media Access Control
MB	Megabyte (roughly 1 000 kilobytes)
Mbit/s	Megabits per second
ONI	Open network initiative
P2P	Peer to Peer
PVR	Personal Video Recorder
RSS	Really Simple Syndication
TCP	Transmission Control Protocol
Tor	The Onion Router
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunications System
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
Wi-Fi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access

NOTES

[1] JH Saltzer, DP Reed and DD Clark, "End-to-end arguments in system design", at: http://web.mit.edu/Saltzer/www/publications/endtoend/endtoend.pdf.

[2] Bell, Gregory, "Failure to thrive: QoS and the culture of operational networking", Proceedings of the ACM SIGCOMM workshop on Revisiting IP QoS: What have we learned, why do we care?, Karlsruhe, Germany, 2003.

[3] Cisco data sheet, Cisco SCE 2000 Series Service Control Engine, http://www.cisco.com/en/US/products/ps6151/products_data_sheet0900aecd801d8574.html.

[4] Cisco Service Control Application for Broadband User Guide, Rel 3.0.5 (HTML) at: http://www.cisco.com/en/US/products/ps6135/products_user_guide09186a008078a9fd.html.

[5] St. Sauver, Joe, "Basics of traffic shaping", at: http://cc.uoregon.edu/cnews/winter2002/traffic.html.

[6] Felten, Edward and J. Alex Halderman, Freedom to Tinker, Entries: "Nuts and Bolts of Network Discrimination Thursday, March 2nd, 2006"; "Nuts and Bolts of Net Discrimination, Part 2, Tuesday, March 7th, 2006"; "Discrimination, Congestion, and Cooperation

Monday, March 13th, 2006", available at: http://www.freedomtotinker.com

[7] See, "Multiple Play: Pricing and Policy Trends", OECD, DSTI/ICCP/TISP(2005)12/FINAL, at http://www.oecd.org/dataoecd/47/32/36546318.pdf .

[8] Comcast acceptable use policy as of February 2005, emphasis added, at: http://www.comcast.net/terms/use.jsp.

[9] "Jitter", Wikipedia Entry, 30 March 2006, at: http://en.wikipedia.org/wiki/Jitter.

[10] "Review: Voice over Wireless LAN", Network World, 10 January 2005, at: http://www.networkworld.com/reviews/2005/011005rev.html?page=1.

[11] For a detailed discussion of this pheonomenon see "Nuts and Bolts of Net Discrimination: Encryption", Felten, Ed and J. Alex Halderman, Freedom to Tinker Blog, 21 March 2006, at: http://www.freedom-to-tinker.com/?p=995.

[12] Van Schewick, Barbara, "Towards an Economic Framework for Network Neutrality Regulation", Paper presented at the 33rd Research Conference on Communication, Information and Internet policy, 23-25 September 2005, Arlington, VA.

[13] USIIA White Paper: Network Neutrality and Tiered Broadband, US Internet Industry Association (USIIA), 06 February 2006, at: http://www.usiia.org/nlcurrent/alert0601.txt.

[14] Yoo, Christopher S., "Promoting Broadband Through Network Diversity", 04 February 2006 at: http://policycouncil.nationaljournal.com/NR/rdonlyres/B745CF87-C00E-4BE6-8D96-57DD91F1EA39/34908/Yoo2020Network20Diversity202606.pdf.

[15] Marilyn Geewax, "Battle Emerges On Future Of Net," *The Atlanta Journal-Constitution*, 27 January 2005.

[16] "The implications of WiMAX for competition and regulation", OECD, DSTI/ICCP/TISP(2005)4/FINAL, at: http://www.oecd.org/dataoecd/32/7/36218739.pdf.

[17] "Cable TV Operators Block HanaTV", *The Korea Times*, 22 October 2006, at: http://times.hankooki.com/lpage/biz/200610/kt2006102219434911890.htm.

[18] "하나TV서비스 호차단 관련 이용자이익저해행위 등 제136차 통신위원회 회의 결과", Korea Communications Commission, 18 December 2006, at (in Korean): http://www.kcc.go.kr/main3_1_2.php?kcc_idx=177&rank=1". See also Hanaro press release in English at: http://www.hanaro.com/eng/pr/press_info_view.asp?keynum=89.

[19] "Keep network neutrality", *The Minnesota Daily*, 31 January 2005, at: http://www.mndaily.com/articles/2006/01/31/66882.

[20] "Internet Filtering in China in 2004-2005: A Country Study, OpenNet Inititative, at: http://www.opennetinitiative.net/studies/china/.

[21] "At SBC, It's All About "Scale and Scope", *BusinessWeek*, 07 November 2005, at: http://www.businessweek.com/@@n34h*IUQu7KtOwgA/magazine/content/05_45/b3958092.htm.

[22] "Internet Traffic Exchange: Market Developments and Measurement of growth", DSTI/ICCP/TISP(2005)11/FINAL.

[23] "U.S. Optical Fiber Communities" List", TIA and FTTH Council Press Release, 26 April 2006, at: http://www.tiaonline.org/business/media/press_releases/2006/JointPR06-03.cfm.

[24] Roberto Battiti, Renato Lo Cigno, Frederik Orava, Bjorn Pehrson, Mikalai Sabel, "Wireless LANs: from WarChalking to Open Access Networks", Mobile Networks and Applications, 01 January 2005, pages 275-287, vol. 10.

[25] Centre for Expertise and Research on Infrastructures in Urban Areas (CERIU), *Infrastructures*, Vol 8, No. 7, September 2001, at: http://www.ceriu.qc.ca/shared/utils/download.asp?folder=download&subfolder=public/bulletinelectronique&file=septembre2001.pdf.

[26] 22@ Barcelona Project, "Presentation of the 22@ Barcelona Project, September 2005 at: http://www.bcn.es/22@bcn/pdf/22@_state_execution.pdf.

[27] Lijbrandt Telecom offers of HDTV over fibre are available at: http://www.kadaka.nl/hillegom_tarieven.php.

[28] "Detailed analysis of EarthLink-San Francisco contract", MuniWireless, 06 January 2007 at: http://muniwireless.com/municipal/1576.

[29] "BT goes after broadband gluttons", BBC, 24 March 2006, at: http://news.bbc.co.uk/1/hi/technology/4841132.stm.

[30] ADSL pricing was obtained on 21 February 2006 from: http://www.bigpond.com/internet-plans/broadband/adsl/default.asp. The unlimited traffic plan allows 10 GB of traffic downloaded at 256 kbit/s. After 10 GB, the speed of the connection drops to 64 kbit/s.

[31] "Nuts and Bolts of Net Discrimination: Encryption", Felten, Ed and J. Alex Halderman, Freedom to Tinker Blog, 21 March 2006, at: http://www.freedom-to-tinker.com/?p=995.

[32] "Tor: Overview", Electronic Frontier Foundation, http://tor.eff.org/overview.html.en.

[33] "HSPA: High Speed Wireless Broadband - From HSDPA to HSUPA and Beyond", UMTS Forum at: http://www.umts-forum.org/servlet/dycon/ztumts/umts/Live/en/umts/MultiMedia_PDFs_Papers_White-Paper-HSPA.pdf.

[34] "The implications of WiMAX for Competition and Regulation", OECD, DSTI/ICCP/TISP(2005)4/FINAL, at: http://www.oecd.org/dataoecd/32/7/36218739.pdf.

[35] Excetel Forum, 13 October 2006, at: http://forum.exetel.com.au/viewtopic.php?t=17721.

[36] Swedish IT Policy Strategy Group, "Broadband for growth, innovation and competitiveness", http://www.regeringen.se/content/1/c6/07/38/23/a695375c.pdf.

[37] "Cost of VoIP calls – Telephony over ADSL", Ariase, 18 October 2006, at: http://www.ariase.com/fr/observatoire/telephone-adsl.html.

[38] One of the most popular BitTorrent clients, Azureus, has a Wiki which allows users to categorise ISPs by the way they allegedly shape peer-to-peer traffic. http://www.azureuswiki.com/index.php/Bad_ISPs. The information is submitted by users so may or may not reflect the ISPs true traffic shaping situation.

[39] "Broadband – switching, migration and connection processes", OFCOM Press Release, 13 April 2006, at: http://www.ofcom.org.uk/media/news/2006/04/nr_20060413.

[40] "Communication from the commission to the council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on the review of the EU Regulatory Framework for electronic communications networks and services [COM(2006) 334 final], European Commission staff working document, SEC(2006)816, 28 June 2006, at: http://europa.eu.int/information_society/policy/ecomm/doc/info_centre/public_consult/review/staffworkingdocument_final.pdf.

[41] "Verizon Limits Its "Unlimited" Wireless Broadband Service", *Consumer Affairs*, 25 July 2006 at: http://www.consumeraffairs.com/news04/2006/07/verizon_unlimited.html.