February 23rd, 2009

Mr. Robert A. Morin
Secretary General
Canadian Radio-television and Telecommunications Commission
Ottawa, ON
K1A 0N2

RE: Telecom Public Notice CRTC 2008-19
Review of the Internet traffic management practices of Internet Service Providers
Reference: 8646-C12-200815400

Please find enclosed my comments which should contribute to the discussion due to my different viewpoint as a technologist and industry observer.

I also wish to formally request participation in the upcoming public hearings in July. It is important that I be given at least a few minutes to address the Council members to ensure that the Council are made aware of the existence of my arguments and can question them further if necessary.

Best Regards,

Jean-François Mezei
Vaxination Informatique
86 Harwood Gate
Beaconsfield, Québec
H9W 3A3
jfmezei@vaxination.ca

Table of Contents

What is the Internet ?

1 The Internet is a telecommunications network which uses the IP protocol (RFC 791/STD 005) to route individual packets from a source to a destination. The IP protocol supports about 140 different subprotocols, with TCP and UDP being the most widely known. However, only the IP information is needed to deliver packets from one node to the other.

2 The subprotocols are used by and managed by the end nodes, outside of the Internet network. They are not needed by the actual Internet network. Optional statistics gathering software on routers such as Netflow are not necessary to operate the network and are not involved in the delivery of packets.

3 Similarly, the IP packets contain a source and destination port numbers. Those numbers are not needed to deliver packets on the Internet. They are used by a node's software to determine which application the packet needs to be delivered to. (The software acts like the receptionist at a switchboard, routing packets to the right extension in an office)

4 For instance, a packet arriving on a node with destination port 80 will typically be handed to that nodes's web server application. This is done inside the node, independently of the Internet.

5 **It is worth repeating that the GAS service offered by Bell Canada is NOT an internet service as it is not based on the IP protocol.**

6 The Internet is a collection of thousands of autonomous networks that have connections to one or more other networks allowing packets to flow from any node to any node on the internet.

7 A packet will typically travel first through its home network (the network responsible for the sender's IP address), followed by one of more transit networks until it reaches the network responsible for the destination IP address which will hand the packet to the destination node.

8 The scope of policies a transit provider can implement is very limited. It is paid to carry packets transparently towards the destination. It is measured by its reliability, speed and whether it has more congestion than acceptable. There is much competition between transit providers (especially in large cities) so poor service will cause a network to stop buying from it.

9 The other type of network is one which is responsible for either the sending or destination IP address. This network will generally have much greater scope of policies it can implement to manage its network. ISPs fall into this category. There are a number of widely acceptable practices. For instance, preventing users from sending emails without going through the ISP's central mail server is widely implemented to prevent Windows computers from sending billions of spam emails. The use of DPI is controversial and definitely not part of accepted practices.

10 **This CRTC process is really about defining what management practices are acceptable for an ISP.**

IP address: Peer , client or server ?

11 On the current internet, each node is identified by a 32 bit IP address. The dotted decimal notation is usually used to display an IP address, it breaks the address into 4 8 bit values separated by a period: for instance, the CRTC's web site IP address is currently 198.103.61.7 But this is really:

```
1100 0110  0110 0111  0011 1101  0000 0111
```

12 The IP address gives no clue on the nature of the node. It could be an industrial robot, home computer, office computer, cash register, small business server, large scale server, network router etc. All communications on the internet flow between 2 equal nodes. No IP address is superior to another.

13 **On the Internet, all end nodes are peers.**

14 **It is not possible for an ISP to know if an IP address belongs to a server, a client or a peer.**

15 One might be able to use other information to guess the nature of a node, but the IP address yields absolutely no clue.

16 This is significant in the context of this discussion because the CRTC and ISPs want to be able to discriminate between connections linking 2 peers and connections linking a client and a server.

17 It should also be noted that the ISP is not aware of connections. The IP protocol is connectionless.

Footnote 3, CRTC decision 2008-108 (CAIP vs BELL) :

18 P2P file-sharing applications are applications that use P2P networks, where multiple nodes (e.g. the computers of end-users) connect to form a network, in order to distribute files over the Internet. Unlike the traditional network distribution model, where multiple end-users download content from a central server, P2P applications allow end-users to download a single file from multiple end-users simultaneously, thus creating the potential for faster download speeds.

19 This is a significant issue to consider. An ISP cannot know if an IP address belongs to a giant server or a small end user. Some large server farms use P2P technologies to distribute content from multiple servers which distributes the load and provide fault tolerance. So DPI equipment, upon detecting the use of a P2P application protocol, may end up throttling a connection between an end user downloading from service with very large servers. And since P2P technologies offer a very efficient means of distributing content, such use will grow since it is more efficient.

20 The use of P2P also allows a small company to grow very rapidly and blocking P2P will prevent small Canadian content providers from easily distributing their content without massive investments they could never afford.

Network protocol vs application protocol

21 There is a need to have a clear understanding of the differences between the Internet network and applications which generate packets travelling on the network.

22 The IP protocol is standard and can carry a wide variety of packets. It is a connection-less protocol which handles the routing but un-guaranteed delivery.

23 The TCP protocol uses the IP protocol to allow 2 applications to establish a reliable connection between themselves. This protocol include logic to detect missing/corrupt packets and retransmit them, as well as automatically adapt to varying line speeds. This also allows connections to deal with varying levels of congestion on any of the links between the 2 nodes and dynamically adjust. All of this is done by each node at the end. The logic that controls the behaviour of TCP is within the nodes, not within the network.

24 ISPs are not aware of TCP sessions. They just see a stream of IP packets that flow through their network.

25 Application protocols exchange DATA between each other. Most applications use the TCP protocol because it provides a reliable path. But other applications use other protocols such as UDP because UDP is faster for simple transactions. All of an application's protocol is placed within the payload of packets.

26 The CRTC needs to understand that there are applications, and application protocols. One application may support multiple application protocols (for instance, Firefox supports SMTP, POP, IMAP, NNTP and maybe others).

27 And some application protocols support the delivery of multiple types of contents. For instance, HTTP (used by web browsers) can support delivery of HTML, images, movies, music, Flash content etc. YouTube uses large amounts of bandwidth and uses HTTP protocol to deliver content. Each YouTube transaction results in many TCP channels being opened, one for each of the components/images on the web page, and one of them will be for the flash content for the movie.

28 What is important to know that there is no standard "application header". Each application protocol has its own definition on how exchanges are made. Some applications allow textual commands to be assembled with multiple packets until a CR-LF is received, while others require that commands be embedded in a single packet with a strict packet format with non-readable bytes.

29 **There is no such thing as application headers.**

30 In the context of this discussion, there are 3 components: the IP header, the TCP header and the payload.

31 - Applications implement one or more application protocols.

32 - Application protocols use one of more sub protocols (TCP, UDP etc.)

33 - They all use IP at the core.

34 - The ISP provides IP connectivity.

35 All application protocols are contained wholly within the data payload of packets.

About port numbers

36 When an application wishes to contact an application on another node, it needs to specify a port number at the destination, and a port number where it can be reached on its own node. Port numbers are used by a computer's software to determine to which application a packet needs to be handed. Port numbers are not used inside the internet and are not needed by a network to deliver packets. They are convenience to allow the destination computer to know what to do with the packet.

37 For the Internet, there is a list of *well known ports*. Generally, well know ports below 1024 require privileges to be used. Many of the original Internet based applications were developed using those ports. This includes the HTTP protocol (web) which normally uses port 80.

38 So, when an ISP sees a packet with destination port number 80, it is a good **GUESS** that it is an HTTP connection. But it is not a foolproof conclusion. And not all HTTP transactions go to port 80. For instance, a printer management protocol uses HTTP transactions to port 631. And there are many web servers that also provide service on the 8080 port even though this port is not protected. (it bypasses some blocks put in by some ISPs). Encrypted HTTP (HTTPS) go to a different port.

39 Some applications, especially more recent ones, dynamically negotiate port numbers to use. They use what are essentially random port numbers. This makes it impossible for simple network gear to "snoop" on communications to make statistics. (and explains why carriers without DPI equipment have different usage statistics in the filings).

40 The problem arises with encrypted communications. Unless DPI equipment is set to decrypt all traffic flows, it finds only gibberish in the packet contents and may be set to throttle anything that is encrypted unless it uses a well known port (such as for VPN). This appears to be the case with Bell Canada as its DPI boxes happen to throttle secure FTP application as well because their connections for data transfers use random ports.

41 The conclusion is that it is impossible to have 100% foolproof way, even with DPI equipment to guess what application protocol is being used in a packet.

Growth of the Internet

42 All ISPs have been faced with continuous growth of internet usage. The rise in access speeds from the early days of dialup have transformed how the internet is used and have even transformed society. Not only are users now getting richer content, they are now also contributing rich content.

43 And every time ISPs have raised modem speeds, new possibilities have opened up. We are now at a point where movies can be downloaded and some services such as iTunes even offer HD content. Adoption rates lag behind speed increases as people get used to the concept.

44 So when ISPs now complain about a small proportion of users using a large amount of bandwidth, they are only seeing early adopters and as the concept of downloading large media files from the internet becomes more and more popular, the load on the ISP networks will grow.

45 This is a wave that cannot and should not be stopped.

46 Because the launch of commercial movie download services specifically serving the Canadian market are very recent, the statistics asked by the CRTC won't really reflect the upcoming growth. But it will happen.

47 The evolution of the DOCSIS standard over the last decade reflects the changing nature of the internet. While many will complain that cable systems have not kept up sufficiently, the DOCSIS updates from 1.0 to 1.1 to 2.0 and now 3.0 have all made increases in upstream capacity to reflect the fact that end users are now uploading ore and more content to the internet. And this trend will continue.

48 Some cable systems who have upgraded capacity in the USA are able to offer services to small business, including support for servers. One such service offers the possibility of symmetrical 30mbps:

http://www.optimumbusiness.com/online/packages.jsp

49 Where there is a will, there is a way. ISPs in other countries are able to give customers the bandwidth they are paying for.

Burst vs Download

50 In the early days, especially with slow downloads, the content being accessed was very light, mostly text HTML without megabytes of javascript code and without huge images, flash animations. And users would spend time reading the content before moving on to the next page, leaving network capacity for others to use at the same time. The odds of multiple users pressing "return" at the same time was low. And network infrastructure was built up to support such low average use.

51 However, today, with large media content and multiple downloads the bursty nature of early years has transformed itself into steady downloads and this changes the load on a network. This is not different from the heydays of dial-up where telephone line usage patterns changed dramatically with users spending all night on the phone when the telco's infrastructure had been built to support much shorter calls. Telcos adjusted to cope with this.

52 **ISPs must adjust their infrastructure to cope with changing usage patterns**

Competition and false advertising

53 With the disappearance of dial-up access as a viable option, the internet access business in Canada has been reduced to a duopoly of telco ADSL and Cable. Mobile telephony is not even in the running because no Canadian mobile company offers affordable internet access anymore.

54 With the CRTC 2008-108 decision (Bell vs CAIP) last November, the large ISPs don't even have to worry about independents stealing serious business anymore. In fact, Rogers has now admitted in intends to follow Bell's lead and throttle its wholesalers too.

55 The competition that is left is plays out on television and newspapers with Cable battling ADSL for whatever advantage they can advertise.

56 On the one hand, Bell has been bragging about how one can download videos and music as much as one wants without affecting neighbours (a jab against DOCSIS cable technology). Meanwhile, the cable companies know they can easily increase their cable modem speeds to outspeed the old copper based ADSL.

57 Bell has followed as much as it could, raising speeds for its ADSL modems from 1.1mpbs in early 2003 to 7 mbps in mid 2007. That is over a 600% increase.

58 Unfortunately , Bell Canada's 86 page filing of July 11th 2008 (CAIP vs Bell), reveals in a pretty graph that aggregation capacity grew by only 50% during roughly the same period.

59 The CRTC is now faced with a situation where ISPs have recklessly raised their advertised speeds in a race to outbid each other, without being able to actually deliver advertised speeds because they have not sufficiently invested in their infrastructure.

60 Allowing ISPs to throttle is giving them carte blanche to continue to raise speeds without being able to deliver the purchase bandwidth, essentially granting them immunity from false advertising accusations.

61 This is a serious commercial issue which must not be tolerated. If ISPs were able to deliver the service they sell, they would not need to throttle.

62 If an ISP advertises you can download movies and music without affecting neighbours, such usage should be considered fair and proportionate. But Bell Canada has successfully convinced the CRTC the opposite in the CAIP vs Bell issue last year, with the CRTC confirming that Bell could classify such users as preventing fair and proportionate use by others ad throttle them down to near dial-up speed.

63 When an ISP advertises a service, then customers who make use of that service as advertised cannot be punished. The ISP must be made to deliver the bandwidth which users have purchased or be accused of false advertising.

64 And ISP that has recklessly increased modem speeds to satisfy the marketing department's demands without matching infrastructure upgrades in now in a situation where it cannot deliver the advertised services.

The need for standards

65 ISP who throttle have only pretended to keep up with increasing demand by advertising higher modem speeds.

66 None of the statistics requested of the CRTC in its December 4th interrogatory are of much use, for one because they lack the average modem speed of users.

67 The reality of networking is that network almost always underprovision their networks because usage statistics show they will get away with it with very few periods where there would be congestion. And all of the internet is basically built this way.

67 However, we are now faced with a situation where Bell Canada is experiencing serious congestion 10 hours EVERY DAY to throttle users down to 30KB/s. This is some serious underprovisioning and should NOT be tolerated.

68 The CRTC should immediately request in another interrogatory that all telcos/cable companies provide PUBLIC numbers on:

69 • average modem speed (mbps)

70 • average unthrottled bandwidth usage per user during peak period (mbps)

71 • average aggregation network capacity per user (total capacity/# customers) . (mbps)

72 • average number of minutes per day an average user experiences congestion in aggregation network.

73 And this should be done using exact same periods for all participants.

74 Either Industry Canada or the CRTC should then set acceptable bandwidth provisioning standards and prevent ISPs from raising/setting speeds which they cannot reasonably provide.

75 This should be an ongoing process with adjustments as usage patterns change. If usage increases faster than the cost of bandwidth decreases, then the ISPs would have good reason to increase their prices or stop increasing speeds.

76 False advertising should not be tolerated.

77 The CRTC should require every carrier who uses DPI equipment in their service to mention this in any/all their advertising in a font size as large as that use to show their introductory price.

78 The CRTC should require every carrier who throttles any content to explicitly say so and list exactly what it throttles and down to what speed in every advertising it does for its service.

79 The CRTC should require every carrier to show both maximum burstable and average sustainable speeds on their service. This would allow consumers to choose the ISP who provide the most bandwidth in real terms.

79.5 These measures would motivate ISPs to build their infrastructure to match the promises made by their marketing departments because consumers could compare real performance of their ISP and not buy services from those who underprovision their infrastructure.

Is DPI the only feasible option ?

In its 2008-108 (CAIP vs Bell) decision, the CRTC stated:

80 *33. The Commission notes Bell Canada's submission that the traffic-shaping approach it has implemented is the only practical option that is technologically and economically suitable, at this time, for addressing congestion in its ADSL network.*

81 The Commission failed to note that the primary, most practical and most economically suitable option to manage this type of network is intelligent matching of ADSL modem speeds to aggregation network capacity. This is a capability which Bell Canada and other ISPs have had from day one and does not require installation of expensive or controversial DPI equipment.

82 As part of 2008-19, other carriers, namely Telus, have stated that they can manage their network without DPI by properly provisioning capacity to match demand.

83 In the USA, the FCC rendered a decision on the Comcast throttling issue. Access to Information Act documents for the CAIP vs Bell affair show that the Commissions was given information about how the FCC viewed Comcast's practices:

> *Comcast's practices do not constitute reasonable network management, have contravened industry standards and impede the user's ability to use applications and access content of their choice.*

85 **How could the Commission support Bell's opinion that DPI is the only acceptable option ?**

86 Furthermore, the same FCC decision also include the following text shown to the CRTC Council:

> *Submit a compliance plan that describes how it intends to transition from discriminatory to non-discriminatory network management practices by the end of the year.*

88 Considering that section 27 (2) of the Telecommunications Act does not allow discrimination which subjects any person to an undue or unreasonable advantage, it is hard to see how the CRTC could accept the throttling as an acceptable practice.

89 By looking at packet contents, DPI equipment guesses what application is generating packets. A person using a particular application to exchange information will be subjected to an unreasonable disadvantage (throttling) while a person using another application (such as Bell's Video Store) will not be subjected to this disadvantage, despite both using the same network protocol and the amount of bandwidth to download the content.

90 **How the CRTC could ignore this blatant discrimination boggles the mind.**

91 There are fundamental aspects of telecommunications which any regulator must uphold. A carrier's job is to deliver packets to their destinations. Packets with identical network features should all be treated equally. What application a customer uses is none of the network's business.

The myth of P2P using more bandwidth

92 Those ISPs who throttle have often made the claim that P2P applications overwhelm their networks and make it look as if P2P applications are able to overcome speed limits of the ADSL/cable modems.

93 This myth has to be killed once and for all and the CRTC needs to put its foot on the ground and no longer accept such propaganda.

94 ISPs only see/carry IP packets. Any ISP who claims that P2P's use of multiple TCP sessions results in increased bandwidth on their network should be tasked to prove this, and provide the exact equipment which allocates bandwidth for each TCP session.

•95 • When packets enter the ADSL/Modem, they are already TCP session agnostic and are just IP packets. They flow at whatever maximum speed the modem allows (or slower speed if there is congestion further down the network).

•96 • The arguments on the P2P using more bandwidth are only valid within one node/computer. For instance, if a user has 1 SMTP session and one FTP session running, that computer will allocate roughly 50% of the ethernet capacity to the SMTP and 50% to the FTP sessions.

97 • But if the user has one SMTP session and 9 BitTorrent TCP links, then the computer will (in general terms) give the SMTP session 10% and the 9 BitTorrent links 90% of the capacity at the computer level.

98 HOWEVER: IN BOTH CASES' THE COMPUTER WILL BE RECEIVING THE SAME AMOUNT OF TRAFFIC FROM THE INTERNET.

99 All TCP links, whether for SMTP, HTTP BitTorrent or any other application using TCP will behave exactly the same and will be designed to use all available bandwidth.

100 In the case of ADSL, the unshared nature of the last mile means that any upstream bandwidth used by a P2P application will not cause much congestion since upstream speeds are so small compared to available capacity. Again, no application can exceed the speed set by the telco on the modem. The use of P2P can have congestion issues for un-upgraded cable infrastructure, but cable companies need to respond to usage pattern changes instead of preventing them.

Section 36 of the Act

> 101 *36. Except where the Commission approves otherwise, a Canadian carrier shall not control the content or influence the meaning or purpose of telecommunications carried by it for the public.*

102 This is about section 36 of the **Telecommunications Act**, not the Applications Act. It is what happens to the data as it transits through a carrier's infrastructure that is in question, not whether applications at each end can recover from harm inflicted to packets during transit.

103 The CRTC itself has violated section 36 in the various documents it has published in this and in the Bell vs CAIP exercise.

104 By determining that "P2P" is "file-sharing" the CRTC is **influencing the meaning of a telecommunication**. These protocols are not designed solely for file sharing. They can be used for a variety of information distribution, including near-live coverage and streaming of content. In fact, the BBC uses P2P technology to stream content on the internet with its iPlayer application which distributes the load amongst many servers allowing more widespread deployment.

105 Secondly, by deciding that users of P2P can wait for their content because it is not important, the CRTC is most certainly **influencing the purpose of the telecommunication**.

106 How can the ISP or the CRTC possibly know that a telecommunication done by a user can wait days to complete (at 30KB/s that is what happens) ? How do they know that the user isn't working on a tight deadline and needs the document ASAP ?

107 Moreover, because the use of DPI involves, BY DEFINITION, looking at packet contents, this means that different treatment of IP packets based on their contents is **editorial control.**

108 This is made worse because the ISP *guesses* what application a user is running an if it doesn't like that application, it throttles the user.

109 Furthermore, the CRTC has not contemplated the actual throttling practice. In cases where it drops packets (Bell Canada) this causes a significant number of packets being retransmitted. Since this is about a telecommunications service, not an application service, what needs to be considered is what flows through the network, not what ends up being stored on the user's disk by the application.

110 Bell's action result in a greater flow of packets through the network (albeit at slower pace). For users of services which bill for usage, this means paying for packets never received because these packets are dropped after they have been counted (at least for GAS customers).

111 In the case of ISPs whose DPI boxes play tricks by modifying packets, this is clearly controlling the content.

What is throttling ?

Question 8 (c) of the CRTC's December 4th interrogatory asks :

112 *c) Describe in detail how the implemented technologies carry out traffic management. The response should include:*

113 And then goes on listing a variety of sub questions, none of which asking HOW the throttling is being done.

The original Public Notice announcement, at:

http://www.crtc.gc.ca/eng/archive/2008/pt2008-19.htm

Contains the following footnote 7:

114 *In the context of Internet traffic management, throttling can broadly be defined as slowing down the transfer rates of traffic by delaying certain data packets at certain points in the network.*

115 The CRTC has a serious case of misconception of how throttling works. The CRTC should not have the ability to rule on any thrittling issues until it understand how throttling is actually performed.

116 The CRTC ignored evidence in the CAIP vs Bell filing which indicated that Bell Canada drops a significant number of packets. Other carrier's equipment may achieve their goals with different techniques. Comcast's equipment (Sandvine) modified TCP headers to signal abrupt end of a TCP session. Ruling on throttling without knowing the exact nature of its implementation is not acceptable.

117 In an envrionment where *Quality of Service* has been implemented , packets with lower priority are the first to be dropped during periods of congestions. And "periods of congestion" tend to be short bursts or when there are problems with one failed link causing traffic to failover to the remaining links on a transit provider.

118 By imposing throttling on a continual basis during 10 hours of day, carriers like Bell have had intents far greater than dealing with congestion. They cannot be allowed to decide which new technology they will support and which technology they prevent.

119 THE CRTC MUST ASK THE CARRIERS HOW THEIR DPI EQUIPMENT IMPLEMENTS THOTTLING.