

July 3, 2008

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

**RE: CRTC file: 2008-04-03 - #: 8622-C51-200805153
CAIP vs Bell Canada, Throttling and Deep Packet Inspection
of ADSL GAS/5410 data service [TN6767]**

Bell Canada has installed Deep Packet Inspection equipment which cripples certain services offered by Sympatico's competitors despite the later purchasing the bandwidth to support their services.

This a serious issue in terms of 5410 tariff enforcement since service providers are not getting the bandwidth they are paying for, and Bell has decided to change the tariff (and even announced usage based billing) without CRTC consultations.

The type of equipment installed has capabilities that are considered *service management* instead of *network management* and a common carrier has no business dictating service features of its customers and preventing customer from offering features they are paying for.

DPI equipment is designed for and sold to Internet Service Providers. The CRTC must consider the Telecommunications Act implications of these devices residing on common carrier infrastructure because the type of features offered by DPI equipment are incompatible with the core concepts of a common carrier.

One measure of competition is whether competitors can differentiate themselves with different services and features. Bell Canada has decided to intervene and manage the service of its competitors to prevent them from differentiating themselves from Sympatico.

The CRTC must also consider the precedents that would be set should it allow a common carrier to inspect and manage data flows by looking at the data beyond the protocol header of the service it provides. This has serious privacy implications.

Bell Canada's introduction of DPI on common carrier services is unique as DPI equipment used in other democracies is limited to ISPs who cannot affect competitor's services. Condoning a common carrier's inspection of private data, discrimination of service level based on the contents and non provision of purchased bandwidth is not something you would expect of a democratic government such as we have in Canada.

Because Bell Canada's official responses to the CRTC, as well as Bell's public relations efforts have introduced many factual errors, we are forced to spend considerable time explaining basic network concepts in this document because Bell's legal department clearly did not spend the time to learn about their own services, and the CRTC must not make a decision based on erroneous Bell Canada propaganda.

Regards
Jean-François Mezei
Vaxination Informatique
jfmezei@vaxination.ca

Table of Contents

Why Did Bell Canada deploy DPI equipment ?	3
A look at DPI capabilities	4
The slow ramp up of all DPI functions	5
Not a Bell White Label Service	7
Overall Network Topology	9
The Life of a Packet	12
The PPPoE Protocol	13
What is P2P ?	14
Peer-to-Peer versus Client-Server	16
Is Bell Looking at Private Data or Not ?	18
What Congestion ?	22
How Does Bell Canada perform its throttling ?	23
What is Fair Use ?	24
The Myth of Co-Located DSLAMs	25
General Policy Issues	26
Recommendations	27
Appendix 1- The IP Header	28
Appendix 2- The TCP Header	29

Why Did Bell Canada deploy DPI equipment ?

In its interrogatory questions, the CRTC has asked Bell Canada to justify the use of DPI equipment. Bell may claim congestion necessitates use of DPI equipment, but consider the following conflicting statements from Bell:

April 15th: 080415 - CAIP Part VII - Answer - App 2.pdf

QUESTION: Why did Bell implement Traffic Management?

Like other Internet providers, Bell's network is strained by applications that use up a lot of bandwidth, like on-line video and peer-to-peer file-sharing programs. Bell decided to ease network congestion by limiting the bandwidth of one application, peer-to-peer file sharing

Note the use of the term "Internet provider" even though Bell should know full well that GAS-5410 does not provide internet connectivity.

May 15th: Bell Canada 15May08-1 CAIP Part VII page 2:

The DPI devices were originally deployed with the intention of introducing customer usage data collection functionality for Bell Canada's usage billing.

So, which is which ? In the April 15th filing, Bell Canada assured us that it did not buy this equipment to collect any information. A month later, it admits it was the primary purpose. If Bell Canada were under oath, what would it respond to the same questions ? And since GAS/5410 does not provide for usage billing, the May 15th statement should be challenged by the CRTC: Was Bell going to unilaterally change GAS tariffs without telling the CRTC ? If this was meant to be Sympatico-only system, it should have been installed on links that serve only the Sympatico service.

Bell Canada totally misunderstood the concept of convergence during the dot-com boom and wasted billions of dollars so it could imitate the AOL-Time Warner fiasco. Reading Bell's submissions, it is clear that Bell Canada's upper management do not understand the nature of the GAS/5410 service and that they do not understand what an internet service provider does. The conflict of interest between Bell Canada as a common carrier and Sympatico as an ISP may explain part of this. However, Bell's misunderstanding of the situation warrants many fears that Bell may have pink dreams of using DPI equipment to develop new revenue possibilities and prevent customer churn by screwing competitors.

When one goes through the web sites of the most popular DPI equipment vendors, namely Ellacoya (Arbor Networks), Sandvine and pCube (Cisco), it is clear that the main thrust of their sales pitch is not network management, but the possibility of generating new revenues (service management).

Network Management is very different from Service Management. DPI equipment is designed to manage services. As a common carrier, Bell Canada does not have the right to interfere with the service provider's ability to define their own services. Its role is to carry packets from A to B.

One thing is certain. Bell Canada did not purchase sophisticated DPI equipment to solve a localised short term congestion problem that would go away with upgrades already in the works.

A look at DPI capabilities

Bell Canada did not purchase this type of equipment to use only a tiny subset of its capabilities. And since Bell Canada has not been forthcoming and trustworthy in its responses, one must look at the full capabilities of such devices and consider worst case scenario where Bell would want to eventually enable all those features.

Going through the websites of the major DPI providers, one clear constant is the ability to generate additional revenue.

- Ability to tie IP traffic to a specific customer and apply custom policies for that customer. This allows ISPs to block or unblock features on a per-customer basis.

Note: Bell Canada would have no problem obtaining profiles for Sympatico customers, but it does not have access to profiles of independent ISP customers. Changes to tariff would be required to force independent providers to load Bell's RADIUS servers with their private customer information so that Bell could activate/block features on a customer by customer basis.

- The ability to identify an application or data type being transferred being used by a customer enables many possible features such as accounting data (different usage rates based on what type of data transferred).
- By throttling most traffic, it frees up bandwidth to those willing to pay for higher performance. Those wanting to use their Playstation to play internet-connected games could purchase an option that would unlock the playstation data stream and allow unthrottled access.
- Customer profiling taken to an extreme with Bell knowing exactly how a customer uses the internet, what application he uses, what web sites he visits, how much time he spends on the web, downloading files etc.

Note: There is absolutely no need for DPI equipment to provide basic usage data (monthly data transfer amounts). Sympatico, and independent ISPs have been doing it without DPI equipment. Again, if one is to believe Bell's May 15 claims, one must ask what type of usage data was Bell seeking to collect with those DPI devices that it doesn't already have.

- The above opens the door to a redefinition of what an ISP service is. Bell Canada could provide a basic package that has all services throttled to dial-up speeds, and some of the key web sites enabled at full speed. Customers would then pay extra to have various features enabled, allowing them full speed access to different sites and applications.
- The list of web sites being granted high speed access in the "basic" offering could be determined by which web sites would be willing to pay Bell Canada to be included in the core list of web sites. (again, additional revenue).
- Like Cable or Satellite TV, Bell could then offer "packages" that grant full speed access to a block of web sites. There could be an "adult" package that would unlock access to any sites with "adult content" tags in the HTML for instance.
- Collect usage information and sell HTTP statistics to advertising firms such as Nebuad.
- Insert advertising in HTTP responses coming from other sites, again generating extra revenue. The equipment installed by Rogers is designed to do that.

One must carefully consider the implications of a common carrier doing the above to the independent providers. **Selling competitor's usage data to advertising firms is despicable.**

The slow ramp up of all DPI functions

One can easily argue that nobody today would ever tolerate an ISP implementing the types of features described in the previous page. It wasn't that long ago that Americans would fume at the mere thought of a national identity card. Yet, there wasn't even a debate when they passed a bill that included neatly hidden identity card requirements.

It is all about HOW you pitch it to customer.

The first step is to claim some legitimate technical requirement and implement it in a way that does not seem nefarious. Bell Canada claims congestion due to an application portrayed as being used solely for illegitimate purposes. Rogers has installed equipment capable of insert advertising in HTTP content, but it only inserts a warning to certain customers when they approach their monthly download limits. Once the equipment has been installed and all the initial debate and criticisms go away, they can slowly move towards their eventual goals.

Bell can legitimately claim it isn't blocking the service, and because the P2P applications have been under constant assailment by the RIAA, Bell can claim it is helping the fight against illegal copying which makes it easier to swallow by the mass market consumers who have lower understanding of the Internet.

Next, they will throttle any adult material, claiming that they are protecting their customers from such materials and offering customers the option to purchase access to those sites. Bell will quote some parents thanking Bell for protecting their kids from all the nasty porn on the web.

And in the end, they will produce statistics showing the number of illicit web sites out there, phishing sites, sites that could load a virus on Windows machines if you make a typing error in a URL etc. and claim that by providing access to only approved web sites, Bell is protecting their customers from all the nasty web sites out there.

While they do this, they also block other protocols, and then provide customers with "à la carte" subscription model. They can then claim that they are lowering the price for the average user who only reads emails and accesses a few web sites.

Consider how quickly some USA ISPs decided to agree to stop offering Usenet access as a means to tell politicians they were doing something about child porn. Instead of blocking the newsgroups containing the child porn, they blocked the whole application and then got customer to pay extra to purchase unrestricted access to Usenet.

Bell will claim the above is all speculation, and they will be right. Speculation is all we can make because Bell has not been forthcoming and has very little credibility with its statements, especially when you consider all the errors and misrepresentations in Bell's official filings to the CRTC.

Furthermore, one must also question why Bell Canada installed this equipment on a CRTC regulated portion of network that is used by competitors of its Sympatico. Had this equipment been installed on links used exclusively by Sympatico, this issue would not be in front of the CRTC because it would be a simple Internet Service Provider debate.

The educated explanation to this is that Bell Canada knows very well that Sympatico will lose a percentage of customers due to the crippling of certain applications. Crippling competitors makes them less appealing to Sympatico customers thinking of defecting.

Another explanation is that Bell's upper management are so misinformed that they truly do believe that the independent service providers merely resell a white label Sympatico service. In that mindset, Bell would naturally think that if it provides 100% of the ISP service, it would have 100% control of the features and provide service management any way it wishes. You will see in this document that this is absolutely NOT the case.

In a "white label" reseller mindset, Bell`s upper management probably see no problem with Bell Canada capturing data from its competitors and selling it for advertising revenue since all customers would essentially be Sympatico customers. You will see in this document that this is absolutely NOT the case.

Not a Bell White Label Service

- 1.1 Bell Canada officials have been telling the media that independent ISPs were merely reselling a Bell Canada *while label internet service*. Bell's official filings with the CRTC reflect this mentality and it is crucial that the record be set correctly as this defines what type of network management Bell can and cannot do for that service.

A newspaper does not resell ink. It buys ink in bulk to make its final product, and the ink provider has no say in what can and cannot be printed on the newspaper.

- 1.2 **GAS/5410 provides no access to the Internet.** It is a communications service which links customers to their service providers, much in the same way that banks buy telecommunications services to link branches to their data centre(s).

- 1.3 **GAS/5410 is defined as a PPPoE based service.** It is **not** based on the Internet Protocol (IP). Bell chose PPPoE as its mainstream offering by pricing HSA (5420) out of the market. This protocol is defined by RFC 2516 at <ftp://ftp.rfc-editor.org/in-notes/rfc2516.txt>

RFC 2516 Abstract: The Point-to-Point Protocol provides a standard method for transporting multi-protocol datagrams over point-to-point links.

- 1.4 **GAS/5410 does not specify what the payload of the PPPoE packets is.** Bell Canada's role is merely to transport PPPoE packets and has no right to inspect, restrict or otherwise manage carriage of packets based on their contents. The PPPoE payload is opaque to Bell Canada and it has no say on what data can and cannot be carried inside the PPPoE packet. Management of the network cannot go beyond PPPoE header contents.

- 1.5 The **point-to-point** nature of PPPoE means that packets must be transported transparently between the 2 end points once a PPPoE session is established (the equivalent of a switched virtual circuit).

Every service is a managed service. But one needs to fully define at what level the service is managed. Bell's role is to manage up to the PPPoE level. The ISP is responsible to manage at the IP level and beyond. Since GAS/5410 does not provide IP connectivity, Bell Canada has no right to claim this is an IP managed service and thus must not be allowed to look/manage beyond the PPPoE header. The responsibilities are clearly delimited, and the CRTC must ensure Bell Canada not overstep its boundaries.

- 1.6 **ISP's are the ones who provide each of their customers with an IP address.** This is contrary to Bell's statements in multiple documents filed so far. This is a critical issue, and it is very difficult to explain why Bell's legal department could have allowed such serious misrepresentation of facts to be filed with the CRTC.

Independent ISPs are assigned a block of IP addresses they can hand to their own customers. In North America, ARIN (American Registry for Internet Numbers) is the body which distributes blocks of IP addresses to ISPs. ISPs do not get their blocks of IP addresses from Bell.

These IP blocks are associated to an Autonomous System Number (ASN). This is a network identification number defining who has responsibility for the IP block(s) and their routing throughout the Internet. ISP's have different ASN's than Bell Canada, so Bell Canada is not involved in any way with the routing/management of the ISP's IP address blocks.

When a Internet network carries a packet where neither the source nor destination IP addresses belong to itself, it is considered a transit provider. Transit providers have no mandate to implement packet content policies. Their role is to look at the IP header and route the packet on its way to the destination's network. Transit providers get paid for bandwidth provided, and they provide the bandwidth for which they are paid. They do not care about what is being carried in packets.

When the source or destination IP addresses belongs to a network, that network can implement its own policies. This is because that network has a direct relationship with its customer who has consented to the ISP's policies (implicitly or explicitly).

Since it is the ISP which gives the customer an IP address, it is the ISP and not Bell which has the identity of the customer attached to an IP address.

The ISP manage its IP blocks as it wishes, and can provide different services based on what IP was given to a customer. For instance, an ISP may grant a range of IP addresses the right to access a usenet service, and issue those IP addresses only to customers who purchase the usenet option.

The ISP can also offer a fixed-IP address to customers who purchase that option. This allows the customer to define a domain name pointing to this fixed IP address. Sympatico does not offer this to residential customers, but independent ISPs can do this if they choose (and many do)

The ISP can also decide to prevent use of certain applications. For instance, many ISPs will block packets destined to port 25 on a remote host in order to prevent spam from emanating from their network. However, for trusted customers, the ISP may decide to unblock port 25 so he may run his own SMTP (mail) server.

The ISP also offers its own e-mail servers and defines what anti-spam services/policies are to be implemented. Such services are absolutely independent from Bell or Sympatico. There are vast differences in the quality of the e-mail service provided by different ISPs, and this illustrates very well that ISPs do not merely resell a Bell/Sympatico service.

Bell's filings often make references to Sympatico activities, confusing them with GAS ones. Sympatico provides absolutely no services to the independent ISPs and is not involved with the provision of GAS/5410.

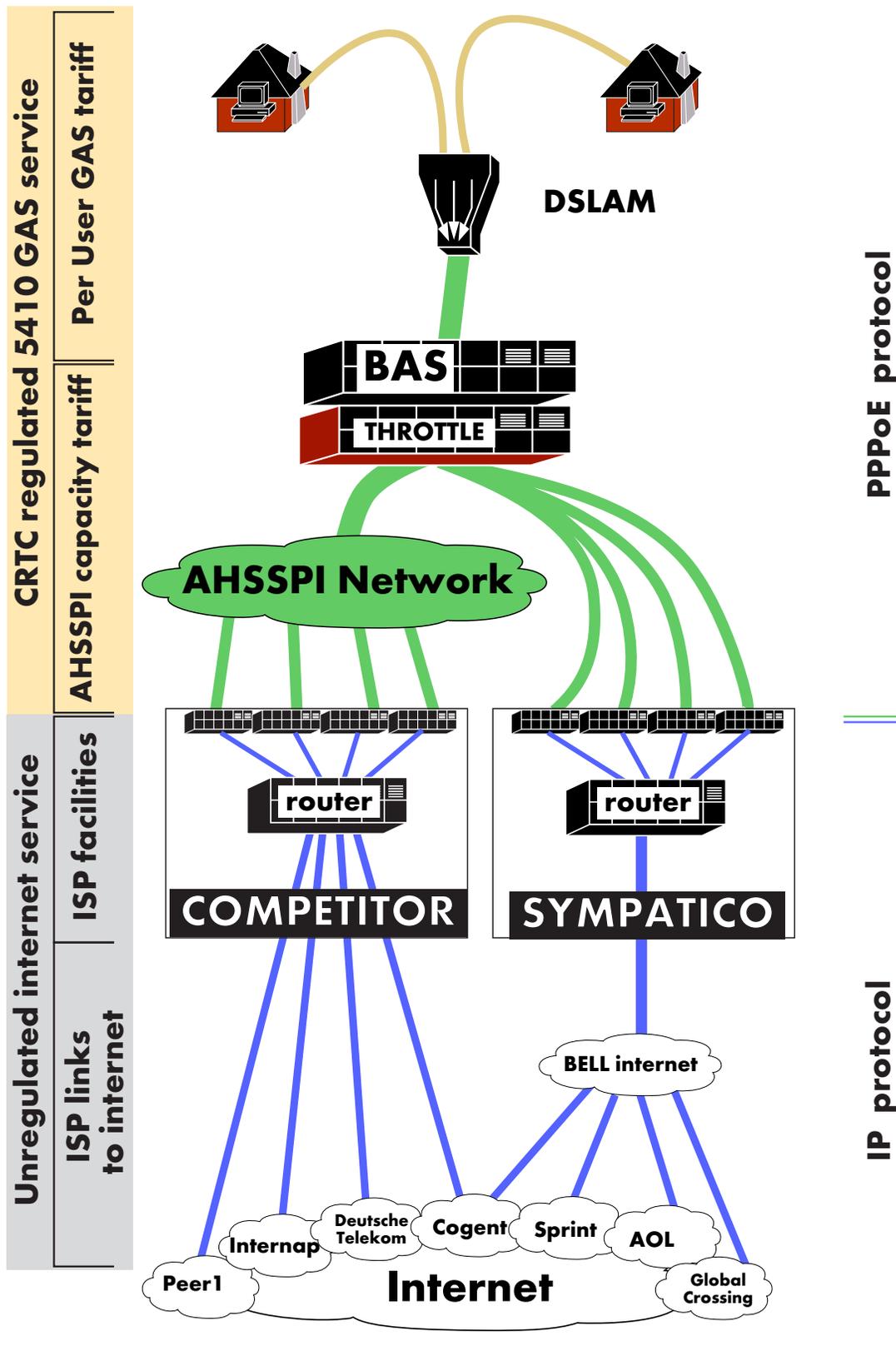
In fact, Sympatico does not even have its own network number. The IP addresses handed to Sympatico customers belong to AS577 which is Bell Canada's Internet connected network. Sympatico no longer has its own email service, it has pointed its customers to a free Microsoft email service (Hotmail). Sympatico long ago shut down its usenet service, and its web site is operated by Microsoft.

Because of the lack of transparency on the relationship between Sympatico and Bell Canada, it is hard to know if Sympatico even pays Bell Canada its fair share for the operation of the ADSL infrastructure. For all we know, the independent providers end up subsidising Sympatico's use of ADSL.

The independent service providers do not resell a Bell Canada IP service, they just buy the raw PPPoE service and build and manage their own complete IP based service which has no relationship with Bell or Sympatico.

Once it is understood that Bell Canada does not provide an IP service in the context of GAS/5410, you can strip off a lot of the text in Bell's filings since they refer to the provision and management of an IP service.

Overall Network Topology



ADSL *Asynchronous Digital Subscriber Line.* ADSL runs on the copper telephone wires between the residence/office and the DSLAM. Bell Canada has been upgrading Sympatico customers to 7mbps speed, while competitors are still limited to 5mbps. The Upload speed is limited to 800kbps. (mbps: megabits per second, kbps: kilobits per second)

DSLAM *DSL Access Multiplexer.* This device drives the ADSL signals for multiple telephone lines and aggregates the data streams into a trunk line going to a BAS. Originally found in the telephone central switches (CO), Bell has been deploying DSLAMs in the neighbourhood remotes. This not only accommodates the growing demand, but also reduces the distance between the DSLAM and the end user. Shorter distances allow higher ADSL speeds. Sympatico customers are given priority to the DSLAM ports installed in remotes. It is estimated that there are roughly 10,000 DSLAMs installed in the Bell Canada territory.

BAS *Broadband Access Server.* This device combines data streams from many DSLAMs and distributes packets to their respective service providers via data "tunnels". To achieve this, the BAS maintains a table of current PPPoE sessions that link each subscriber to his service provider. Once the session is established, the BAS need only look at the session ID in the 8 byte PPPoE header to perform its job. Packets to Sympatico infrastructure are switched to an internal network. Packets to competing service providers are sent via the AHSSPI network. There are an estimated 250 BAS on the Bell Canada territory. Some documents use the term BRAS (Broadband Regional Access Server). ISPs often call those the "LAC" which is the L2TP term for the node which originates a tunnel to them.

AHSSPI *Aggregated High Speed Service Provider Interface.* This service uses Bell's core network to funnel end user packets from each BAS into fast links to the ISPs. The "pipes" at the narrow end of the funnel are currently limited to 1 giga bits per second (gbps). Additional capacity is obtained by purchasing multiple AHSSPI links. Each ISP purchases sufficient AHSSPI capacity to handle the peak throughput demand of its customer base. Should an ISP not buy sufficient AHSSPI capacity, then the bottleneck happens at the narrow end of the funnel, a portion of the network which only affects that ISP and has no impact on other ISPs or Sympatico.

Note: The AHSSPI uses the L2TP protocol (Layer 2 Tunnelling Protocol). L2TP frames are carried in IP-UDP packets, thus making AHSSPI an IP based intranet; it is not connected to the Internet. The 5410 and 5420 tariffs mention that the service providers must provide Bell with a number of IP addresses. These addresses are used to establish the private L2TP tunnels between each BAS and each ISP. They are not distributed to end users, nor do end users ever see those IP addresses.

ISP FACILITIES

The PPPoE sessions are established between the end user and the ISP's AHSSPI-facing routers. Packets are meant to travel transparently between those 2 points. Once packets arrive at the ISP's facilities, the PPPoE payloads are extracted and inserted into the ISP's IP network and begin their journey through the Internet.

The ISPs are in charge of providing mail servers, spam filtering equipment, routing and connections to the internet. ISPs are also responsible for web hosting, access to NNTP, SMTP, DNS servers. They define their own TCPIP policies, such as routing and/or port blocking. These services are completely independent from those provided by Bell Canada and/or Sympatico.

THE INTERNET

The Internet consists of separate but interconnected IP networks. Transit providers are commercial networks that sell access to the internet on a capacity basis. Each transit provider connects to some other transit providers and this allows packets to find some path via a number of networks to reach any destination on the Internet. Transit providers differ from each other in pricing, reliability, performance, number of connections to other networks, geographical footprint and number of points of presence in the areas covered. Routing protocols between networks allow packets to choose the best available route to a destination.

ISP CONNECTIONS TO THE INTERNET

Each ISP purchases links from transit providers who have a point of presence in their city. ISPs can extend their own network, via dedicated links, to a larger city where they can choose from more transit providers. In large cities such as Toronto, there are enough transit providers to provide a very competitive field. The ISP will buy sufficient capacity from one or more transit providers to meet the demand generated by its customers. The selection of providers, and routing policies that manage multiple connections to the internet is all done by the ISP with no involvement from Bell Canada.

There is also the concept of peering arrangements where two networks can get a direct connection to each other without using transit capacity (reducing transit costs). These are negotiated by the ISPs with no involvement from Bell.

As an ISP's customer base grows and/or average usage increases, the ISP will need to purchase additional AHSSPI capacity and additional Internet transit capacity. ISPs that offer generous usage plans do so because they have found affordable Internet transit providers and purchase sufficient AHSSPI capacity to provide good service at profitable levels. They are fully paying for the GAS/AHSSPI service they use. ISPs have their own Internet network. For instance, one ISP often mentioned in this dossier is Teksavvy and its network is AS 5645

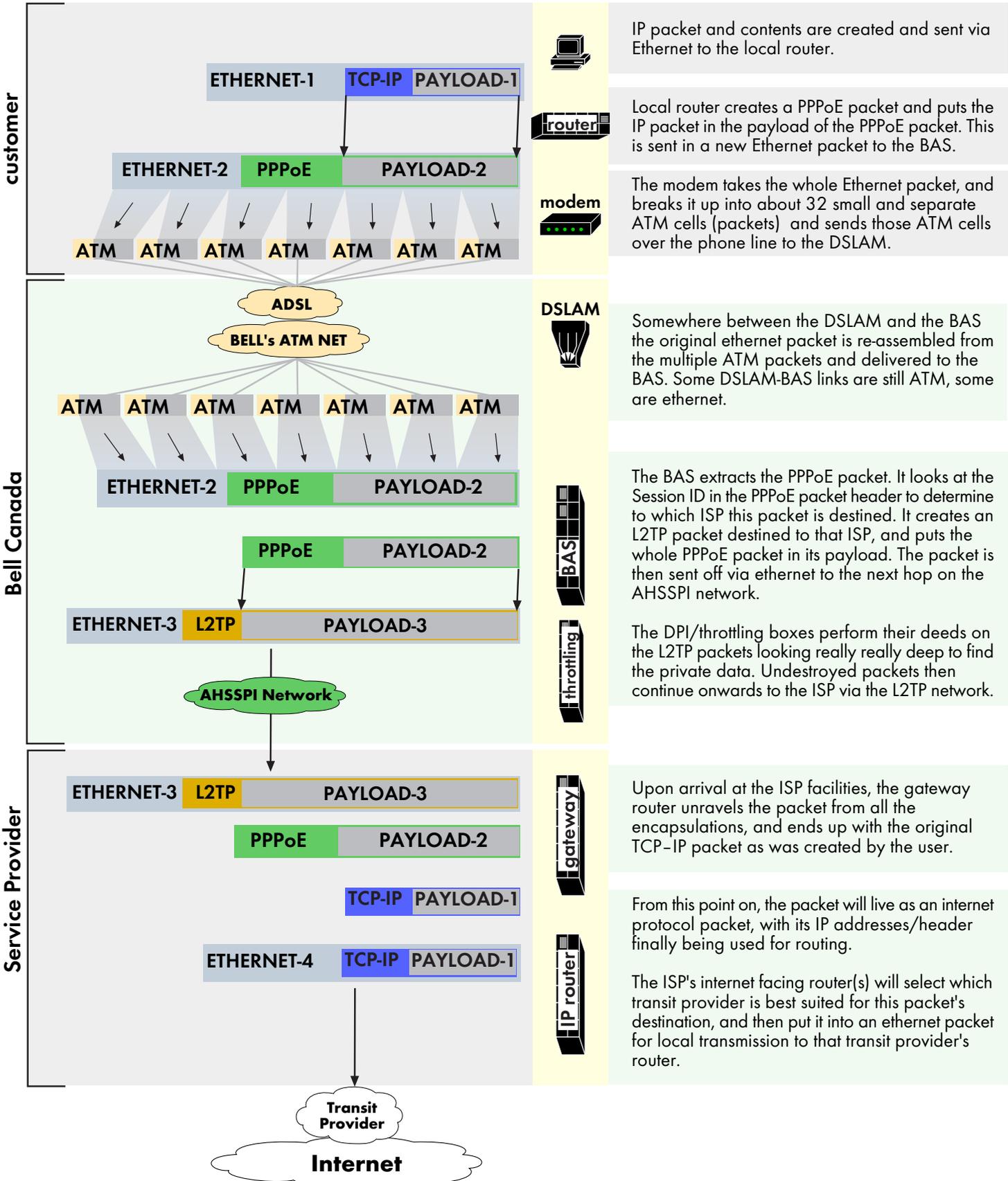
Bell Canada has its own Internet-connected network with its own connections to various transit providers. In technical terms it is known as AS 577 and is completely separate from the GAS/HSA/AHSSPI networks. Bell also uses that network to sell Internet transit to a number of large corporations in Canada. Few independent ISPs buy internet transit from Bell Canada because it is not considered competitive.

Sympatico does not have its own network. Its customers are handed IP addresses that belong to Bell Canada's internet network (AS 577). This means that Bell Canada makes all IP network management/routing decisions, selects and negotiates with transit providers and does capacity planning for Sympatico.

Bell Canada provides Sympatico with the ADSL access network at one end, and Internet connectivity at the other as well as providing IP network management. For the independent service providers, Bell Canada provides only the ADSL access network.

Many comments in the documents filed by Bell Canada for this issue fail to make this very important and very critical distinction. Needless to say, it is not comforting to realise how little key Bell Canada employees know about their own services and network.

The Life of a Packet



The PPPoE Protocol

The PPPoE protocol, as defined in RFC 2516 and STD51 (PPP) is a session oriented protocol. When the end user establishes a session the following happens (simplified)

- The user's router sends an ethernet broadcast out to Bell.
- The BAS responds with an offer of service, Session ID, and the user's router learns the ethernet address of the BAS that can be used for all further packet exchanges. Low level connection between the user and BAS has been established.
- From that point on, higher level PPP protocols are used to complete the session establishment, they follow the "LENGTH" field of the PPPoE header.
- The user's router sends the authentication request (user@realm + password) . Upon receiving it, the BAS can associate the Session ID to the ISP (based on the name specified in the "realm"), and forward the authentication packet to the ISP. Upon receiving the packet, the ISP verifies the credentials of the user using its own user database and responds positively or negatively to the authentication request.
- From that point on, the PPPoE connection has been made, the PPPoE CODE becomes zero, and private data exchanges between the 2 end points can begin with the BAS only needing to look at the SESSION ID to do its job.
- The ISP then uses the PPP protocols (STD 51 same as the old dialup) to supply the user with an IP address and other configuration data provided by the ISP. None of this configuration data is provided by Bell.
- Once established, the PPPoE session is, by design, totally transparent and packets flow from one end to the other without any expectation of Bell performing any action on those packet or their contents.

PPPoE	VERSION	4 bits	always set to 0001
	TYPE	4bits	always set to 0001
	CODE	8bits	Defines the state of the PPPoE session (various stages of session establishment, or "0" once the session is established and data is being exchanged.
	SESSION ID	16bits	Identification of the session which links the customer with his ISP.
	LENGTH	16bits	The length of the data that follows it. Officially, the PPPoE header is 6 bytes (48 bits) and is followed by a payload of up to 1494 bytes that contains a PPP packet.
PPP	PROTOCOL	16 bits	In practice, because it is the only PPP field that remains once data exchanges begin, the PROTOCOL is often included in the PPPoE header description for simplicity's sake. But technically is part of the PPPoE payload.
	PAYLOAD	many	up to 1492 bytes of data. When 1492 bytes of payload are transmitted, the LENGTH field indicates 1494 because the PROTOCOL field is considered a PPPoE payload.

The PPPoE header contains absolutely no hint on the nature of the payload. There is no way for Bell Canada to know what type of application is being used by looking only at the PPPoE envelope.

What is P2P ?

Throughout its documents, Bell Canada has been using the "P2P file sharing" terminology without ever defining it. In fact, nobody has been able to get any straight answer from Bell Canada on exactly what they are throttling.

How are independent ISPs supposed to define their service for their customers if Bell won't tell them exactly what it is doing to their own traffic ?

Definitive discussion is not possible unless we have access to the exact filter configuration of Bell's DPI equipment. One well known P2P protocol is BitTorrent, and we know that it is definitely crippled by Bell for both the clear text and encrypted links.

BitTorrent is an application level protocol which resides fully in the data portion of packets and which was written by what is now the BitTorrent corporation. The protocol specification were released to the open source community and are documented at

<http://www.bittorrent.org>

There are now many different applications which have implemented this protocol. It is used by a number of commercial operations which distribute legitimate content such as BitTorrent.Com, Vuze.com, and there is a lot of legitimate software distributed with this protocol (for instance Linux)

BitTorrent is a legitimate corporation which sells legitimate movie download service along with others such as Vuze. Thus, Bell Canada is crippling services which compete against Bell's own video store.

How does BitTorrent work ?

If I wish to distribute a large file to 3 friends, this is what will happen: The file is first broken up into a large number of small segments. When peers connect to each other, they exchange information on their status, and which segments they already have. They can then request segments from any other peer.

In this case, I would send 3 different segments to the 3 peers. As soon as those are received, each peer announce the segment it has just received. The others, not having this segment, will request it. Meanwhile, I will now be sending 3 more segments to the peers.

The end results is that instead of having to send one full copy to each peer (3 full copies in total), I end up sending 1/3 of a copy to each peer (one copy in total) and while this happens, the peers use their own upstream to send their portion to each other.

If I send data to 3 people, the effective rate is $800/3 = 266\text{kbps}$ per recipient so each peers gets the 1/3 of the file I and sending him at 266kbps. But because the peers also upload to each other, they will each get data from 2 peers, each peer sending to another peer at 400kbps. The total is then 266kbps from me, and 400 from each of the other 2 for a total of 1066kbps.

The end result is that I send 1/3 as much data (1 copy instead of 3), and recipients get the file at 1 megabits per second instead of 266kbps.

It is a very elegant and efficient philosophy that makes use of otherwise idle upload bandwidth at each peer. In practice the numbers are not so clean cut, but the above illustrates the philosophy.

The simplicity and flexibility of the protocol also allows content providers to easily distribute their products from a small farm of servers with and implicit load balancing (because of the protocol's flow control mechanisms) and automated failover and more importantly, their customers help reduce the load by also providing portions of the content to others.

And yes, the software was designed to make full use of available bandwidth, but then again, most software is designed this way. But the software is different in that it uses both the built-in TCP flow control mechanisms as well as its own detection of when links become chocked.

Now, lets compare this with the client/server approach where one very large server feeds content to many customers. This server needs very large "pipes" to the internet. But it will feed data to its customers at whatever full speeds its customers can accept the data.

You will find on the next 2 pages graphs showing that for Bell, whether data is coming from a BitTorrent "swam" or from a server such as Bell's Video Store, it makes no difference because all Bell sees are PPPoE packets flowing at whatever rate the end user's ADSL line has.

A test was conducted in early June during peak hours. A movie was purchased from the Bell Video Store and downloaded:

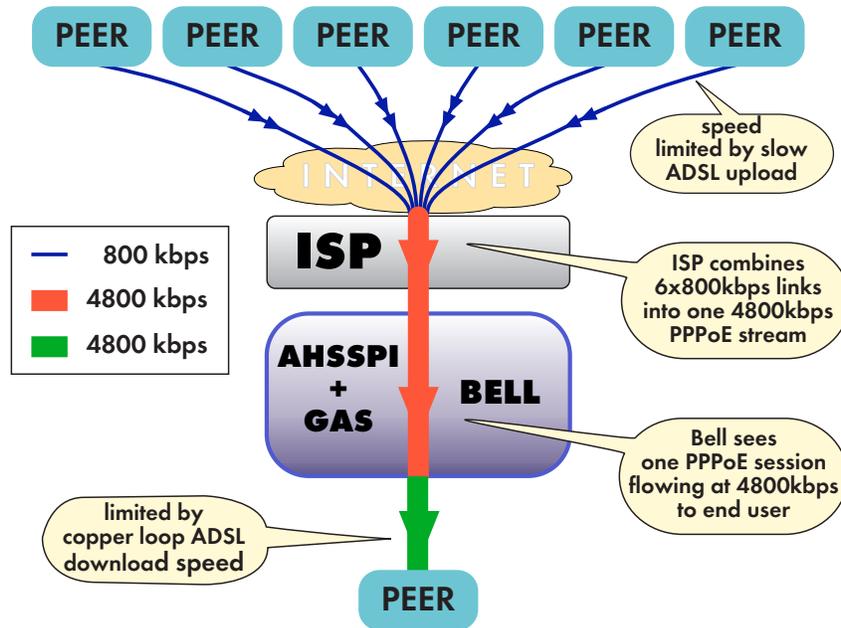
1.62 gigabytes downloaded in 65 minutes resulting in a rate of 415.4 KB/s (kilobytes/second) which is close to the maximum for a line at 5.0 megabits/second when consider PPPoE and ATM overhead.

Another attempt soon after the Bell Video Store was made available, done on a line with better quality, reached average throughput of roughly 480 KB/second (kilo bytes/second).

It is very clear that the Bell Video Store will make full use of a end user's ADSL capacity, in the very same was as a BitTorrent download would. It makes no difference to Bell Canada.

Why should BitTorrent be crippled when the Bell Video Store has the same impact on the GAS infrastructure ?

Peer-to-Peer versus Client-Server



Bell Canada claims that the BitTorrent protocol generates a heavy load on its network. This page and the next page will show that this is not the case and that it is no different than other protocols.

When considering traffic flowing towards one customer, this is what happens:

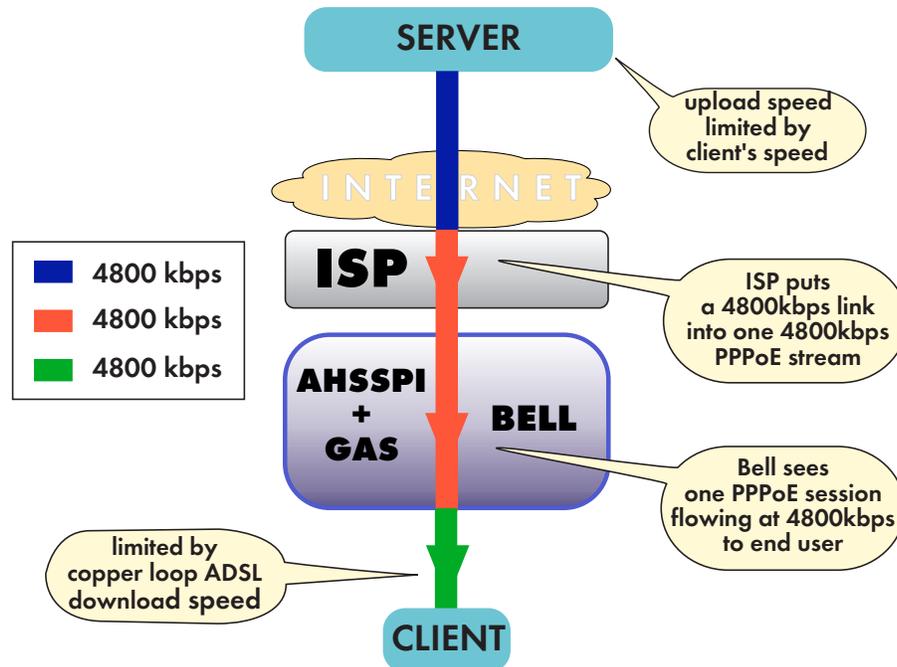
-data from various peers flows to the ISP via the Internet. The ISP puts each packet in a PPPoE frame to be sent to the end user. The flow rate is limited by the end user's relatively slow ADSL speed. The TCP flow control mechanisms adapt to this and each peer at the other end will be sending only at a rate that the receiving peer can acknowledge.

-In the above case, 6 peers sending at 800kbps will generate a flow of PPPoE packets over the ADSL line of 4800kbps. (not counting overhead to make things simpler).

Bell Canada has claimed that because the end user can have TCP-IP connections with over 100 peers, that it puts undue strain on its network. Bell Canada, under the GAS tariff, sees only PPPoE packets. Whether a PPPoE packet contains an IP packet that originated in India while the next one originated in New Zealand makes absolutely no difference Bell Canada provides a PPPoE service and all TCP-IP features are in the opaque payload of the PPPoE packet and thus of no concern to Bell.

Bell Canada gets 4800kbps worth of data to deliver to the end user. It is all in PPPoE packets.

Peer-to-Peer versus Client-Server



Here we have a situation where the user is downloading from a large single server. Lets take the Bell Video Store as an example. A single TCP-IP connection might be established between the server and the end user. The commercial server has a huge pipe to the internet and could pump data at many gigabits per second.

Once the data starts to flow towards the client, the TCP mechanisms adjust the rate of flow and the server will only be pumping data at a rate where the client acknowledges receipt. So in the end, the server will end up sending at 4800kbps.

Just as in the case with the peer to peer example, the ISP will get 4800bps worth of data and package it into PPPoE packets and send it at the same speed to the AHSSPI cloud to be delivered to the end user.

Bell Canada will therefore be receiving roughly the same number of PPPoE packets as if the same content had been sent via BitTorrent.

The big difference is that with BitTorrent, you do not need to connect to massive servers in order to download at your ADSL speed, you can connect to a torrent that will provide enough peers that each contribute a small amount of bandwidth which adds up to the speed your ADSL line allows.

Is Bell Looking at Private Data or Not ?

Bell Canada has made the claim that it does not look at private user data, despite admitting to the use of DPI equipment, which, by definition, looks at user data.

First and foremost, this is a PPPoE service and Bell Canada must only have access to the PPPoE header. This is a core data communications principle that cannot be ignored.

THERE IS NO INFORMATION IN THE PPPoE HEADER THAT CAN ASSOCIATE A PACKET TO ANY APPLICATION.

From a common carrier point of view, the payload of a PPPoE payload must remain opaque. And the debate should stop here. However, since Bell Canada has made claims, and since this is an important issue, I will demonstrate just how deeply Bell Canada must dig to detect a BitTorrent protocol connection.

Assuming Bell Canada has access to the IP header: (see Appendix 1)

The IP header contains information that allows a packet to go from one IP address to another. It has absolutely no information on the type of contents or the application that created those contents.

Assuming that Bell Canada has access to the TCP header: (see Appendix 2)

The TCP protocol uses ports as a sub-address (like telephone extensions in an office). Upon receiving a TCP packet the IP stack on that computer will lookup a table to determine which application on that computer gets the packet. There are well known ports, registered ports and dynamically used ports.

The official list of port numbers is at: <http://www.iana.org/assignments/port-numbers>

This list makes no mention of BitTorrent since BitTorrent does not use pre-defined port numbers.

Well known ports are between 0 and 1023.

Well known ports are defined for well established older applications. For instance, port 80 has been defined for the HTTP protocol (the "web"). By default, if you do not specify a port number in a HTTP: URL, it will connect to the destination's port 80. But the application listening for calls on port 80 could be anything and could be BitTorrent. The known ports are just convention, not a "rule".

Registered ports are similar, except that they are less secure from the operating system point of view. (one needs privileges to become the official listener for well known ports such as SMTP (port 25) for mail.)

Dynamic ports are used in two ways: First, when a process makes an outgoing call (for instance to a remote web server), it needs to have a port so it can receive the data the web server will be sending. Those ports are essentially random ports.

The second way dynamic ports are used is when they are application driven. This is the case for BitTorrent. The user specifies a range of port numbers in a preference panel. The application will listen for incoming connections on the first port in that range, and when announcing itself to other peers, it will include a "to contact me, specify port XXXX". And when individual connections are established with other peers, other ports in that range will be used.

Therefore, Bell Canada's DPI equipment

CANNOT IDENTIFY BITTORRENT BY LOOKING AT PORT NUMBERS.

Furthermore: <http://www.ellacoyanetworks.com/products/ipservicecontrolsystem.pdf>

(a document well worth reading)

Unlike most policy-based network devices, the Ellacoya switch can identify traffic based on application signatures in addition to standard TCP/IP header information. This allows the switch to identify port-hopping applications and apply the correct policies, even when they use the well-known ports of other applications (e.g. port 80).

Application signatures are found ONLY in the data payload of a packet.

In other words, confirmation that the DPI equipment goes beyond the port number to identify the application.

If the equipment can spot a BitTorrent running on port 80, means that it must scan all port 80 communications. And the only way to distinguish if a connection is using HTTP or BitTorrent on port 80 is to scan the PAYLOAD to see if there are HTTP or BitTorrent "commands" in the data.

And there is no "masquerading". If a company decides that dialing "0" leads to the janitor and you need to dial 1 1 1 to get to the switchboard receptionist, it may not be according to convention, but there is no masquerading.

And HTTP transactions can be found in many different ports. Some web servers listen to port 8080, and there are devices such as printers and routers and switches which can be configured via HTTP transactions that may need to use an strange port number (for instance for printing, port 631 is common).

Furthermore: From: http://www.bittorrent.org/beps/bep_0003.html

BitTorrent's peer protocol operates over TCP. It performs efficiently without setting any socket options.

In other words, confirmation that there are no special TCP options which would identify BitTorrent protocol. None of the other fields in the TCP header contain any information which could identify a packet being used for BitTorrent in any way shape or form.

THERE IS NO INFORMATION IN THE PPPoE HEADER TO IDENTIFY BITTORRENT

THERE IS NO INFORMATION IN THE IP HEADER TO IDENTIFY BITTORRENT

THERE IS NO INFORMATION IN THE TCP HEADER TO IDENTIFY BITTORRENT

So, where does Bell Canada get the idea that its boxes merely look at packet headers ?

Here is a hint: For BitTorrent, when a conversation is initiated, the first few bytes of the USER DATA contain:

one byte set to the value 19, followed by the string "BitTorrent protocol". This is the BitTorrent signature, but it isn't in the header, it is in the payload. (and it requires repeating that in a PPPoE service, Bell Canada must not look beyond the PPPoE header and it doesn't have the right to look at the IP or TCP headers and certainly not the user data portion.

In: docs-911097-Part VII - Responses to interrogatories - Bell Canada - Attachment 15May08-7.DOC

Bell States: DPI is used to examine each of the protocol headers that wrap the content, in order to identify the type of package being transmitted. It is called "Deep Packet Inspection" because it looks beyond the routing addresses, deeper into the packet headers,

Any IP router, even home routers, can look at IP,TCP,UDP headers. There is no such thing as "deeper into the packet headers:". You are either in the header or in the payload. It is black or white. DPI equipment [looks for strings or patterns in the payload of the packet.](#)

I have already established that there is no special "signature" in the IP and TCP headers which identify a BitTorrent flow. The special signatures are in the data payload of the TCP-IP packet.

And it is time to remind readers that GAS/5410 is a PPPoE service, so Bell Canada can only look at the PPPoE header and has no business looking at the IP and/or TCP headers which are contained in the PPPoE payload.

Bell states: The closest identifier to an individual subscriber that the DPI currently does maintain and store is a "subscriber id" which is actually Bell Canada's user ID assigned by network authentication in order to bind a user ID to an assigned IP address.

The Ellacoya documents clearly state that they are capable of accessing a full user profile from a RADIUS server and collect information on a per user basis, as well as applying service management profile to each individual user. (aka: which sites/applications are throttled etc.). If I can find this information on the Web, how come Bell Canada, who have purchased a whole bunch of those boxes wouldn't know ? And since Bell Canada has stated it has intentions to use these boxes for usage based accounting, these boxes would be pretty useless if they couldn't associate traffic to a specific customer (which the Ellacoya documentation confirms it can).

Why does Bell Canada go out of its way to mislead the CRTC ?

Would the CRTC tolerate Bell using voice recognition equipment on its telephone service ? It could unilaterally decide that teenage girls overload the network by talking too fast and program its boxes to insert static on conversations after it has detected a female saying "Oh My God!", forcing each person to stop talking during the periods of static.

That is what Bell Canada is doing on the GAS/5410 service.

In a telecommunications environment, there is no such thing as an application. There is a pipe between 2 points, and the role is to take data from one point and bring it to the other point. The applications do not run on the network, they run on computers at either ends of the pipe. Only raw data is being exchanged in packets.

Different applications format their data differently. And this creates signatures. But those signatures are part of the data, and the carrier has absolutely no business looking at them

Bell Canada gets PPPoE packets to carry from point A to point B. It has no management to perform once the session has been established and as a common carrier, certainly has no business implementing service management to prevent certain types of data from flowing at the speed which is being paid for.

Use of DPI by an ISP is questionable. But use of DPI by a monopoly common carrier is criminal.

A monopoly imposing its own service philosophy on competitors is intolerable.

What Congestion ?

The ADSL system is already equipped with a natural throttling mechanism: the speed of ADSL connection. It is the weakest link. Any increase in ADSL speeds will automatically increase demand on the backbone. This has been demonstrated in recent years as ADSL speeds have gone from 1.3 to 1.7 to 3.0 to 5.0 mbps.

In August 2007, Bell Canada started to advertise 7mbps service for Sympatico customers. Competitors' customers continue to be limited to 5mbps.

In October 2007, Bell Canada starts to throttle Sympatico customers.

In August 2007, Bell Canada would have been quite advanced in the planning of the installation of the DPI equipment.

If Bell was forecasting so much congestion that it had to install DPI equipment, why then did Bell increase Sympatico's marketed speed by 40% (from 5 to 7mbps) ?????

In essence, Bell Canada can now raise ADSL speeds to any level it wants/can, and use the throttle machines to prevent people from actually using those speeds.

A few points to consider in Bell's number:

- Since it takes roughly 32 ATM packets to build one PPPoE packet, the loss of 1 packet has the same impact as the loss of 32 consecutive ATM packets since the whole PPPoE packet will need to be retransmitted. So one must take Bell's numbers with a grain of salt.
- Modern DSLAMS are capable of handling all ports at their ADSL speeds. Bell should provide an explanation on why there would be congestion at a DSLAM. Perhaps lost ATM cells are really cells that were lost while on the copper loop (line noise, lightning etc.).
- The line between the DSLAM and the BAS location would be shared with HSA 5420 service. Yet, HSA is not throttled. Congestion numbers given by Bell cannot be fully considered without HSA numbers as well.
- Bell claims that ATM equipment is expensive for upgrades. This is a good indication that moving from legacy to Ethernet not only drastically increase line capacity, but also decrease costs. Bell conveniently omits to mention that as it upgrades ATM segments to ethernet, the ATM equipment could be used to upgrade ATM segments that are oversubscribed (instead of having to buy more ATM equipment).
- Bell's numbers do not show congestion for ATM and Ethernet segments separately. Since ATM segments would not remain in the long term, it would be wrong to use this short term excuse to install long term DPI equipment.

How Does Bell Canada perform its throttling ?

So far, the issue of HOW Bell Canada achieves the level of crippling has been dealt with. It is an important issue. Certain ISPs have systems that modify packets (notably changing the RST flag of the TCP header which orders the receiving peer to abruptly abort the connection with its peer.

I have used data tracing tool (Wireshark) to examine what happens to BitTorrent data transfers. This is a long and tedious process.

The TCP-IP protocol was built with withstand network problems. In particular, networks who have occasional congestion are expected to drop packets. The TTL mechanism of the IP header will also cause an automatic packet loss if it cannot be delivered to destination within the specified deadline. The receiving system detects a missing packet (because of the gaps left between sequence numbers) and the sender will eventually resend the packet when an ACK has not been received. This disrupts the flow of packets.

Looking at transfers during a 10 minute period:

To the local computer:

18299 packets received.

3962 packets were retransmissions, indicating 21.6% rate of packet loss.

Looking at individual streams (flows to use Bell terminology), the packet loss rate ranged from 3.1% up to 32.3%. There was no "free" period since the packet loss applied to very short streams ("I have nothing that interests you" exchanges), as well as longer exchanges (where the percentages comes close to the 21% mark).

What this means is that the throttling is applied as soon as the DPI equipment sees the application signature in the user data. And this means that Bell's statements to the media that those who use BitTorrent for small transfers are not affected is FALSE.

In practice, instead of getting a throughput of roughly 420 KB/s (kilobytes/second), one gets only between 25 to 30 KB/s. This is why the word "crippling" is used in this document because it means that downloading a legal movie takes over 10 times as long when purchasing a movie from a competitor to the Bell Video Store. Not everyone can afford to leave computers running 7/24 to complete downloads that are artificially crippled by Bell.

Furthermore the type of actions taken by Bell Canada harms end users:

While the end user does not packets killed by Bell, those packets have been processed by the ISP and counted towards the monthly download caps. So when the packet is retransmitted, it is counted twice by the ISP even though the end user has only seen it once. This means that Bell Canada is causing end users to reach their monthly download limit 20% faster.

This is a systematic killing of a large number of packets based on "racial" features of the data in the packet that Bell has decided it does not like. Therefore, Bell's throttling should be called:

PACKET GENOCIDE

What is Fair Use ?

In an interview with Mr. Bibic by Roberto Rocha, April 11, Montreal Gazette.

01:53: Q: What is the measure of a heavy user ?

A: More, you know, well it's around more than 30 kilobits per second
(...)

Q: More than 30 kilobits per second at any given time or constantly ;
what constitutes heavy usage ?

A: Well, it's more than 30 kilobits per second, I don't know if is at any given time or constantly
or average, I don't know.

The 5410 Tariffs, which should be an inviolable bible provide 2 points where speed is measured:

- The ADSL loop. Due to technical limitations (copper loop length), line speeds cannot all be set to the marketed standards. The tariff takes this into consideration. But there is no text that states that using the line at its speed for more than a few seconds is not acceptable.
- The AHSSPI capacity.

ISPs purchase sufficient capacity to handle the full aggregated load from their customer base. The Tariff defines speeds that are "burstable up to x". But there is no definition of what average use or acceptable use should be. I believe most ISPs aim for average utilisation rate of roughly 60%.

Unless the tariffs change, Bell Canada should be forced to provide the ADSL speed capacity between the DSLAM and the BAS, and fill the AHSSPI pipes up to the level purchased by the ISP.

Yes, internet usage is growing rapidly as new applications are developed and richer media is being exchanged. At the same time, telecommunications costs are going down, and Bell Canada has plenty of fibre laid. Other countries such as Japan are coping nicely. Bell's shenanigans are not due to congestion, they are about their vision for what type of service they wish to offer in the long term.

If Bell Canada feels that the GAS/AHSSPI rates do not cover the costs, then let Bell Canada argue its case to the CRTC. Otherwise Bell Canada must be made to provide the bandwidth and continue with its current upgrade programme which has worked well.

The Myth of Co-Located DSLAMs

Retail internet access was originally developed by smaller entrepreneurial companies. Legacy telcos eventually realised the need to be in this business and gained a large portion of market share mainly through acquisition of small ISPs. During the initial years of ADSL service, one CRTC decision circa 1997/1998 stated that dialup still provided sufficient competition to the ADSL services. This stopped being the case and GAS/5410 became a regulated service to ensure proper competitive environment existed.

Modern applications have now made dialup irrelevant, so the need for competitive high speed access is stronger than ever. Competitive access via cable companies has not developed significantly.

- The copper loop is the true bottleneck of the service. Only a certain percentage of customers are close enough to a DSLAM to achieve the advertised speeds. Bell Canada has been handling growth in demand by adding DSLAMS to neighbourhood remotes. This has the added advantage of reducing the loop length, allowing a greater percentage of customers to reach the advertised speeds.
- It is not possible to co-locate a DSLAM on a remote. The co-location suggestions by Bell Canada restricts ISPs to having DSLAMs in Central Offices. Every advertised speed increase reduces the number of customers who can attain that new speed while connected to a Central Office DSLAM.
- The 5400 tariff for co-located DSLAMs, approved in the late 1990s has not succeeded in developing a competitive network of Co-Located DSLAMs. With Central-Office based DSLAM no longer adequate, and ADSL nearing its limits, there is no point in anyone developing a new competitive ADSL infrastructure.
- Competitive access via cable companies has not taken off, and has many technical and geographical limits that hinder provision of competitive access. Wireless access is either too expensive, and/or does not offer sufficient total bandwidth for large scale deployment.
- Therefore, at this point in time, GAS/5410 (and its 5420 cousin) is the only viable and comprehensive competitive access covering Québec and Ontario.

Until municipalities install Fibre-To-The-Home and make ADSL irrelevant, **the GAS/5410 service remains the only comprehensive and competitive option and must be considered essential to the maintenance of a competitive environment.**

General Policy Issues

- ISP buy bandwidth and they buy ADSL access. Bell must provide the service for which they pay for.
- Allowing Bell Canada to retain the DPI equipment on bulk data links would set dangerous precedents that might be used to justify using such equipment on similar links used by banks, retailers and others. The Telecommunications Act exists for a good reason, and the neutrality of common carriers must remain inviolable.
- In essence, the Telecommunication Act regulates the common carrier to ensure private exchanges are not regulated nor tampered by the common carrier.
- Bell Canada disregarded and broke the laws that apply to it and has unilaterally introduced its own regulations to be imposed on its competitors.

Anarchy: a state of lawlessness where government laws are not enforced and citizens devise and impose their own laws on whomever they can.

The ball is now in the CRTC's court.

Recommendations

- 1 The CRTC must order Bell Canada to immediately stop throttling independent service providers traffic.
- 2 The CRTC must order Bell Canada to physically disconnect AHSSPI network lines from the DPI equipment and plug them back into the BAS as it was before. This would remove the DPI equipment from the GAS/5410 service, but still allow Sympatico to deploy whatever features of the DPI equipment they wish without impacting competitors.
- 3 Independent auditors should be hired to ensure that Bell Canada has complied with the above 2 recommendations at all sites where DPI equipment has been deployed.
- 4 Should Bell Canada find some excuse to not comply with item •2, independent auditors must make regular and full audits of each DPI machine, including access to their full configuration to ensure that no throttling is being done, and more importantly that none of the other DPI functions are activated for GAS service customers, especially the collecting of any and all data, from usage on a per/user or per/application basis, or the collection of HTTP transaction to be sold to 3rd party advertisers.
- 5 The CRTC should instruct Bell Canada to develop a plan to be presented to the CRTC to ensure that Bell Canada's regulated common carrier services are fully separated from Bell Canada's retail internet service provider service (Sympatico) in order to ensure that Sympatico cannot influence the provision of the GAS and HSA services to competitors.
- 6 The CRTC must send a very strong message that it will uphold the Telecommunications Act and not allow a common carrier to look beyond the header of the protocol use for a particular service.
- 7 Bell Canada must not give preferential treatment to any one ISP when it comes to ADSL speed profiles, as well as access to ADSL ports in DSLAMs. This means that if Bell Canada wishes to increase ADSL speeds to 7mbps, all ISPs must be given access to this new speed. And it means that ADSL ports on DSLAM should be on a first come, first served basis without Bell deciding to reserve DSLAM ports in remotes to Sympatico users and putting customers of independent providers on the longer loops to the central office.
- 8 The CRTC should not tolerate that Bell Canada move to usage based billing (as mentioned in its filing of May 29) without first going to the proper procedure for a Tariff change with the CRTC.

Appendix 1- The IP Header

Version	4 bits	The Version field indicates the format of the internet header. IPv4 uses the value of 4.
IHL	4 bits	Internet Header Length is the length of the IP header length. Denotes the number of 4 byte words. A value of 5 indicates a header length of 20 bytes.
Type of Service	8 bits	The Type of Service provides an indication of the abstract parameters of the quality of service desired. This can be used to indicate to the network currently transporting the packet whether this is an high priority packet, bulk transfer packet etc. Not all networks support all options. This is within the IP header, and is set by the originator of the IP packet. Networks in between do not decide what packets are important and which are not, it is the originator of the packet which does.
Total Length	16 bits	Total Length is the length of the datagram, measured in octets, including internet header and data. (the TCP header is considered "data" in this context)
Identification	16 bits	An identifying value assigned by the sender to aid in assembling the fragments of a datagram. When a packet needs to travel over a link that can only handle shorter packet lengths, the router can break the packet in multiple parts that fit within that link's capabilities.
Flags	3 bits	Various Control Flags which control packet fragmentation.
Fragment Offset	13 bits	This field indicates where in the datagram this fragment belongs. This allows the reconstruction of a packet which was fragmented in transit even if the fragmented packets arrive out of order.
Time To Live	8 bits	This field indicates the maximum time (in seconds) the datagram is allowed to remain in the internet system. If this field contains the value zero, then the datagram must be destroyed. This field is modified in internet header processing and every IP router along the way typically decreases the value by 1. This would prevent a packet to remain in some routing loop forever. This field is not changed during transit through the GAS network.
Protocol	8 bits	This field indicates the next level protocol used in the data portion of the internet datagram. (for instance TCP or UDP. There are about 140 defined protocols.
Header Checksum	16 bits	A checksum on the header only. Since some header fields change (e.g., time to live), this is recomputed and verified at each point that the internet header is processed.
Source	32 bits	The source IP address (the IP address of the sender of the packet). This value is often written in what is called dotted decimal notation such as 72.14.205.99 where each number represents 8 of the 32 bits.
Destination	32 bits	The destination IP address.
Options	variable	The length of this optional field is the difference between the IP header length and the length of the data before it (20 bytes).

Appendix 2- The TCP Header

Source Port	16 bits	The port used by the application sending this packet. When the receiver wishes to respond to this packet, it will use this port as the destination port.
Destination Port	16 bits	This is like a an extension number in an office telephone system. Upon receiving the packet, the destination system will use this port number to hand the packet to the right process. Further discussion in the chapter dealing with the BitTorrent protocol.
Sequence Number	32 bits	This identifies the first data byte of the packet relative to the first byte transmitted in this TCP connection. Adding the length of data to this sequence number predicts the sequence number the next packet should have. The receive uses this mechanism to detect missing packets, and to reorder packets that arrive out of sequence. Equipment such as Rogers' which insert content in a stream have to find imaginative ways to resequence all of a data stream so the recipient does not notice the insertion of forged data into the stream.
Acknowledgement Number	32 bits	In a bidirectional exchange, the sender will use outgoing data packets to confirm reception of the incoming data packets. In unidirectional exchanges, the receiver will need to send packets with 0 bytes of data, but with the acknowledgement number set in order to let the sender know what has and what has not been received. This mechanism allows both to detect missing packets and implicitly request retransmissions.
Data Offset	4 bits	This defines the size of the TCP header, or how many bytes to skip to reach the start of the data. (this field contains the size of TCP header divided by 4)
Reserved	6 bits	Reserved for future use. Must be zero.
Control Bits	6 bits	URG: Urgent Pointer field significant RST: Reset the connection ACK: Acknowledgment field significant SYN: Synchronize sequence numbers PSH: Push Function FIN: No more data from sender In some cases, the DPI equipment modifies that user data packet to set this bit which forces the recipient to declare the connection to be dead without the other peer knowing about it. In the case of Bell Canada this does not appear to be the case. SYN and FIN and used during session start and tear down respectively.
Window	16 bits	This is used as part of flow control mechanism to indicate how much data can be sent before it has been acknowledged by the recipient. This value adjusts automatically during a session if link throughput changes.
Checksum	16 bits	This is a checksum to ensure integrity of the bytes contained in the TCP header, TCP data and some IP header fields. DPI equipment which modifies any field in the header must also recalculate the checksum.
Urgent Pointer	16 bits	Defines the location of Urgent data in the packets when the URG bit has been set.
Options:	variable	Provides for optional additional options. Commonly used to provide for widow sizes that would not fit in a 16 bit number, as well as automated flow control mechanisms.