Per Vices Corporation
73 Strathcona Avenue Toronto Ontario M4J1G9 Canada

Technical Brief

Bypassing Throttling Using Protocol Encryption

Version	Date	Author(s)	Notes
0.01	2008 07 08	Victor Wollesen (*Applied Research*) Yi Yao (*Research and Development*)	The following brief provides instructions on how to configure a sample bit-torrent client to bypass the throttling measures enforced by Bell Canada. Sample clients (uTorrent, ktorrent) are configured to strictly apply protocol encryption and use the VPN port for transferring content.
0.02	2008 07 08	Victor Wollesen (*Applied Research*)	Added additional step (rebooting DSL modem (hypothesized that reconnecting renews dynamic IP). Confirmation this works on the Bell Canada Network. Thanks to Superhero Smith for the additional feedback.
0.03	2008 07 08	Victor Wollesen (*Applied Research*)	Corrected typo in port numbering (should be 1723). Thanks to imis for the notice.
0.04	2008 07 09	Victor Wollesen (*Applied Research*)	Added notes with our hypothesis on why this works for some people and not for others.
0.05	2008 07 14	Victor Wollesen (*Applied Research*)	Added additional notes based on filings made by Bell Canada on 11 July 2008.
0.06	2008 07 20	Victor Wollesen (*Applied Research*)	Added additional port TCP/500 based on information provided by Marc.
0.07	2008 11 22	Victor Wollesen (*Applied Research*)	Updated to include Ktorrent v3.1.4 client. Modified recommended utorrent DHT settings based on information provided by drjp81. Updated end notes based on additional information, including use of tunnelling protocols.
0.08	2009 01 07	Victor Wollesen (*Applied Research*)	Renamed Brief. Added information in overview concerning additional possible ports based upon information provided by grendel. Added information on Tomato/MLPPP in Notes section.

Overview

In general, there are two steps to enabling peer-to-peer communication over the Bell Canada DSL Network. It is first necessary to force protocol encryption for all connections. Then, select a VPN port to route your bit torrent traffic over.

The selection of the port seems to have become more important. We have included a list of the most common TCP and UDP ports and encourage you to select one at random: if the ports you choose don't work, try experimenting and using different ones.

At this point, it may be necessary to renew your IP address. Assuming you have a dynamic IP, this could be accomplished as simply as reconnecting to your DSL service, or rebooting the DSL modem. If you have a static IP, it may be necessary to wait an unknown period of time, or else request a new one.

This may not work for everyone. If this does not work for you, please see the notes following the example configurations.

TCP Ports: 50, 500, 1701, 1723, 10000

UDP Ports: 50, 51, 500, 2746, 4001, 10000

Examples

uTorrent

The following has been tested to work to uTorrent v1.7.7. Reference screen shots of the uTorrent configuration settings have been included at the end of this procedure.

1. Launch uTorrent.

2. Select **Options** then **Preferences**.

3. Click on **BitTorrent** from the preference tree.

4. Under the **Protocol Encryption** heading, select **Forced**. Ensure that the **Allow incoming legacy connections** box is **unchecked**.

5. As uTorrent seems to dynamically assign DHT ports, it seems necessary to disable them: Under Additional BitTorrent Features, disable DHT by **unchecking** the boxes for **Enable DHT Network**, and **Enable DHT for new torrents**.

6. Click on **Connection** from the preference tree.

7. Under the **Listening Port** heading, select the **Port used for incoming connections**, and set it to one of the *TCP* ports listed in the overview (our example uses **1723**).

8. Ensure that the **Randomize port each time uTorrent starts** box is **unchecked**.

9. Click on OK, and reconnect to your DSL service or reboot your DSL modem.

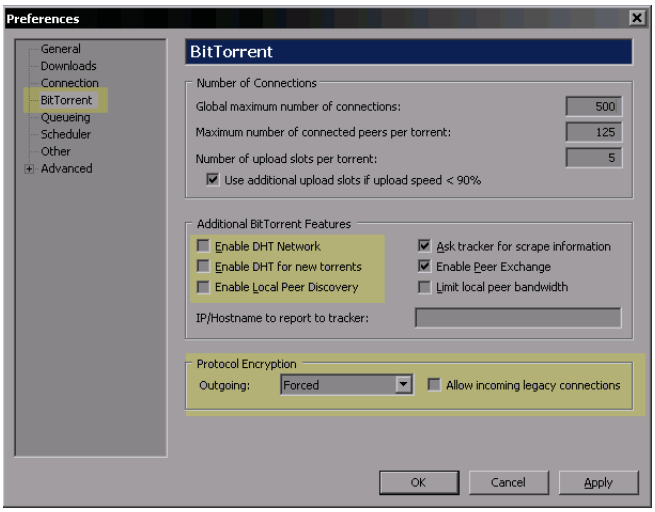

Illustration 1: The preference settings box showing the BitTorrent section settings.

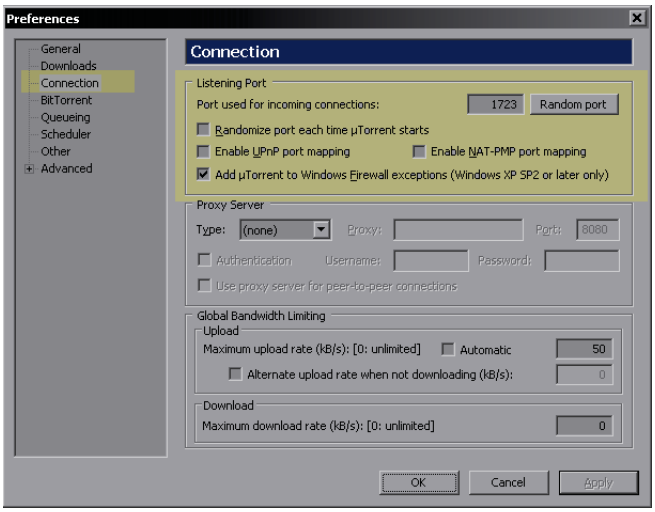

Illustration 2: The preference settings box showing the connection section settings.

KTorrent

The following has been tested to work to KTorrent v2.2.6, and v3.1.4. Reference screen shots of the Ktorrent v.2.2.6 configuration settings have been included at the end of this procedure. No screen shots have been included for the v3.1.4 settings.

As the configuration steps between the two versions is essentially identical, we have only included one proceedure – where section or header names vary, we have first indicated the v2.2.6 name immediately followed by the v3.1.4 name in square brackets and italicized, like so: **old v2.2.6 name** [***v3.1.4 name***].

1. Launch KTorrent.

2. Select **Settings**, then **Configure KTorrent**.

3. Click on the **Download** [***Network***] section.

4. Under the **Preferences [*Ports and Limits*]** header, set the **Port** to one of the *TCP* ports listed in the overview (our example uses **1723**), and the **UDP tracker port** to one of the *UDP* ports listed in the overview (we chose **50** for our example).

5. Click on the General [BitTorrent] section.

6. Under the **DHT** header, select the **UDP port for DHT communications**, and select a *UDP* port from the list in the overview section (we used **51**).

7. Type **OK**, and reconnect to your DSL service or reboot your DSL modem.

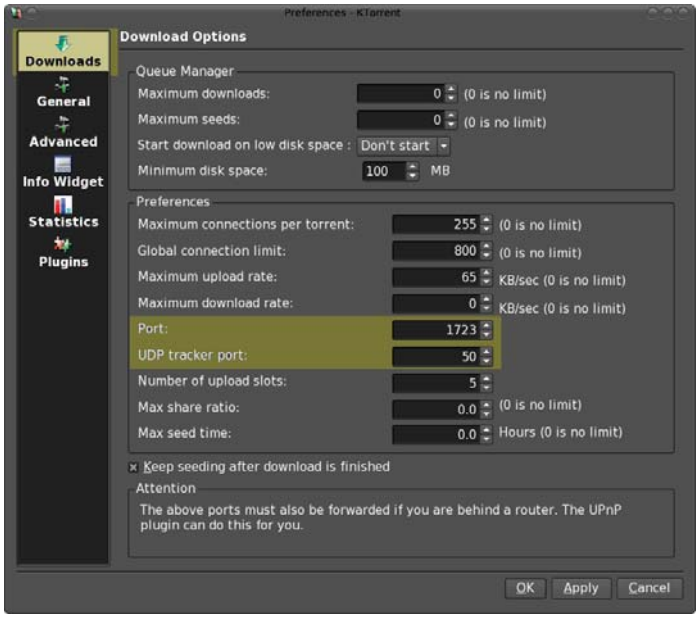

Illustration 3: The download section of the Ktorrent v2.2.6 configuration box.

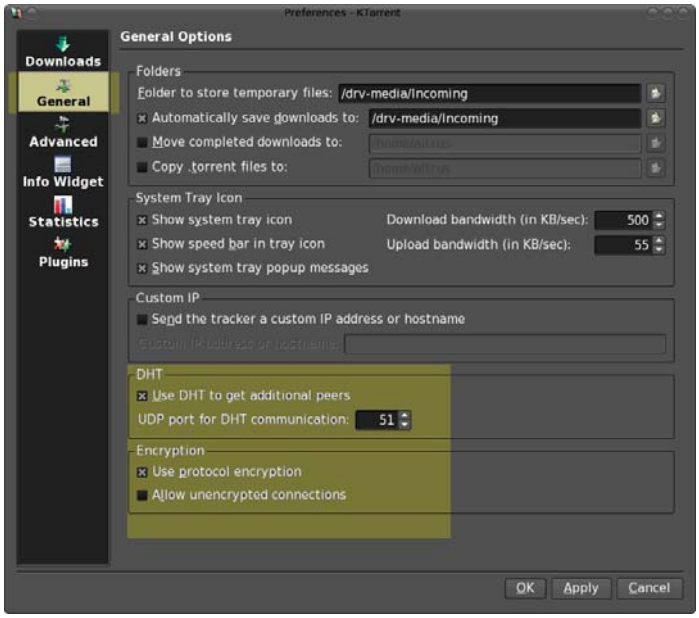

Illustration 4: The general section of the Ktorrent v2.2.6 configuration box.

Notes

Very little public information exists as to the specific methods or techniques used by Bell Canada to throttle traffic. While this method has been tested over the network of a third party ISP, and has been independently confirmed to work on some retail Sympatico customers, it does not work for everyone. We do not know why it does not work for everyone.

If you have not been successful using our method, there is an alternative available using Tomato/Multilink Point to Point Protocol (MLPPP). This requires your ISP to support MLPPP (which Bell does not support), and a Linksys WRT54GL router. Although more complex, and requiring you to purchase a new router if you have not already, it currently works works where this guide does not. More information is available here:

http://fixppp.org/index.php?p=documentation

The remainder of this note speculates on the mechanics of how Bell Canada throttles traffic, and on why we believe our method works. Without access to appropriate technical documentation, we cannot guarantee the accuracy of our claims. If you have additional information, or feel we are in error, we encourage you to email us using the contact information found on our site[1].

When Bell Canada first began throttling traffic, some VPN[2] users experienced a decrease in their connection bandwidth which they associated with being throttled by Bell. In their CRTC filing, Bell refuted the claim and emphasized that properly configured clients are not affected. They noted that the majority of clients using the correct ports are not throttled. As VPN traffic is encrypted, the DPI device is unlikely to be able to immediately read the packet contents, perhaps causing it to default to a rule based algorithm to decide whether or not to throttle a particular stream.

This also suggests a special configuration or procedure in place allowing VPN users unthrottled access. It also leaves the open the possibility for Bell to conduct traffic pattern analysis in order to determine likely the content type. As such analysis is statistical in nature, we assume conservative heuristics to minimize false positives.

Bell states that the majority of VPN users have unthrottled access. Although it is plausible to assume they configure the DPI devices differently depending on the area being served, we assume a standard rule set across the network, white listing VPN traffic. In their commission filings[3], Bell Canada notes as much;

1 http:// www.pervices.com
2 A Virtual Private Network (VPN) may be used by employees to access internal corporate networks outside their office.
3 ANSWER BELL CANADA 11 JULY 2008, paragraph 116

> *Therefore, the VPN signatures in the DPI are created leveraging the standard protocol ports and basic signatures based on the specification of the VPN vendor. As long as the customer's VPN port is correctly setup and there are no alterations to the VPN client, VPN traffic will not be shaped. In the Company's experience, issues arise because the VPN client is incorrectly setup or not setup to the specifications of the VPN vendor.*

This suggests that Bell Canada uses port and protocol data to to apply rule based signatures that exclude VPN traffic from being throttled. Depending on the completeness and aggressiveness of the rule set, this may eventually require modification of the bit torrent engine or protocol to effectively defeat throttle application.

It is our hope that the follow guide is of use in restoring full connectivity. If you have any further information you feel may be of use, we encourage you to contact us through our website.

Applied Research
Per Vices Corporation