
where can i download linux MLPPP and Bell's throttling

Posted by gbuchana(a)teksavvy(dot)c om - 2009/07/23 04:59

I have seen suggestions that switching to MLPPP service would somehow enable one to side-step Bell's traffic shaping and presumably any other non-neutral network management they might be doing. Is this true? I would have thought that MLPPP traffic traverses the same Gateway Access Service as everything else and would get just as throttled. How does MLPPP change anything?

gbuchana(a)teksavvy(dot)com Gardner Buchanan
FreeBSD: Where you want to go. Today.

where can i download linux MLPPP and Bell's throttling

Posted by JF Mezei - 2009/07/23 04:59

How does MLPPP change anything? MLPPP is really PPPoE with a couple extra bytes in the header before the payload. So to Bell, it looks like PPPoE and it processes it like PPPoE. But its DPI equipment is programmed to peek at specific locations in the packet payload for certain strings/values. So with MLPPP adding (I think) 6 bytes to the header, the packet payload is 6 bytes further from the start of packet, so the DPI equipment does not find the various signatures it is looking for. If Bell's DPI equipment looks for a 19 byte string Bittorrent Protocol at byte 63 of the PPPoE packet, when you use MLPPP, the DPI equipment would see *&?!& Bittorrent Pr and thus not recognize that packet as being the opening salvo in a BitTorrent exchange.

where can i download linux MLPPP and Bell's throttling

Posted by Tony - 2009/07/23 04:59

I have seen suggestions that switching to MLPPP service would somehow enable one to side-step Bell's traffic shaping and presumably any other non-neutral network management they might be doing. Is this true? I would have thought that MLPPP traffic traverses the same Gateway Access Service as everything else and would get just as throttled. How does MLPPP change anything?

gbuchana(a)teksavvy(dot)com Gardner Buchanan
FreeBSD: Where you want to go. Today.

where can i download linux MLPPP and Bell's throttling

Posted by gbuchana(a)teksavvy(dot)c om - 2009/07/23 04:59

But its DPI equipment is programmed to peek at specific locations in the packet payload for certain strings/values. So you're saying that the equipment Bell is using either cannot (yet) or has been (so far) programmed not to mess with MLPPP traffic. It seems still within theoretical possibility and even reasonable likelihood that Bell would configure or upgrade their equipment to interfere with MLPPP on the GAS too.

gbuchana(a)teksavvy(dot)com Gardner Buchanan
FreeBSD: Where you want to go. Today.

where can i download linux MLPPP and Bell's throttling

Posted by JF Mezei - 2009/07/23 04:59

So you're saying that the equipment Bell is using either cannot (yet) or has been (so far) programmed not to mess with MLPPP traffic. Correct. Bell likely had to pay Ellacoya/Arbor some big money to have them develop the capability to parse a TCP packet in an IP packet in a PPPoE packet in an L2TP packet which is what its devices have to do when dealing with GAS traffic. For Sympatico traffic, the DPI boxes het IP packets. Bell would probably have to pay Ellacoya to develop additional filters to spot signatures in different locations of packets when there is MLPPP and Bell so far has not done so. Should Bell's throttling rights be reconfirmed at the conclusion of all the issues at the CRTC right now, perhaps Bell might spend the money to catch MLPPP. However, it is also quite possible that MLPPP traffic is small enough that it really isn't worth it for them at this point in time. But should it grow and become important, then it might be a different story. Should the CRTC come to its senses and declare that throttling is not legal on GAS

service, then all this is moot and MLPPP will be relegated to a very obscure niche of people bonding multiple lines together.

=====

where can i download linux MLPPP and Bell's throttling

Posted by gbuchana(a)teksavvy(dot)com - 2009/07/23 04:59

Bell likely had to pay Ellacoya/Arbor some big money to have them develop the capability. It would surprise me very much that the DPI vendors did not already have such a feature. PPPOE is a pretty common link tunneling protocol and I bet handling it and maybe even MLPPP is a feature that the vendor would add of their own accord, based on demand. Unpacking protocol layers is not that hard a problem, even at speed, and it does not have to be 100% accurate

=====

where can i download linux MLPPP and Bell's throttling

Posted by JF Mezei - 2009/07/23 04:59

Unpacking protocol layers is not that hard a problem, even at speed, and it does not have to be 100% accurate

=====

where can i download linux MLPPP and Bell's throttling

Posted by gbuchana(a)teksavvy(dot)com - 2009/07/23 04:59

In one setup, half the packet goes on link 1, the other half goes on link 2 and the router at the other end reassembles both into a single packet. This sounds a little fishy. Unless you pack multiple half frames into each of the two link frames, you're leaving bandwidth unused

=====

where can i download linux MLPPP and Bell's throttling

Posted by JF Mezei - 2009/07/23 04:59

I was told that equipment is able to scan HTTPS transactions. Again this is fishy. SSL is genuinely secure. Maybe they're just guessing what a session is being used for based on the target IP address, but if they're inspecting actual SSL traffic content, This isn't rocket science. If you HTTPS://www.mybank.ca then the DPI equipment can do exactly the same thing as your browser to get certificates, verify them and decrypt the communication. This is not the same as two peers who have previously exchanged keys and begin with an already encrypted connection. On those, the DPI equipment wouldn't be able to decrypt on the fly.

=====

where can i download linux MLPPP and Bell's throttling

Posted by Some Guy - 2009/07/23 04:59

... so the DPI equipment does not find the various signatures it is looking for. If Bell's DPI equipment looks for a 19 byte string Bittorrent Protocol at byte 63 of the PPPoE packet, when you use MLPPP, the DPI equipment would see *?!& Bittorrent Pr and thus not recognize that packet as being the opening salvo in a BitTorrent exchange. Is it necessary for the string BitTorrent to appear in the packet for the packet to be interpreted correctly by the destination machine? If I were to mung the string (as it leaves my own machine, assuming Bell/sympatico is my ISP) then would it still be correctly interpreted by the destination machine? Does Bell throttle BT in both directions, or only the upload direction (ie does it throttle BT packets leaving my machine, or being received by my machine)? What is the current Bell BT throttling strategy? I mean, does it kick in only during certain times of the day, or is throttling happening all the time? When it has kicked in, does it try to achieve a certain max UL or DL data rate - and if so what is that rate? Or do those questions depend on where in Ontario I am, or which CO I'm connected through?

where can i download linux MLPPP and Bell's throttling

Posted by JF Mezei - 2009/07/23 04:59

What is the current Bell BT throttling strategy? 16:30-18:00 60KB/s (in practice, less than 60) 18:00-01:00 30KB/s (in practice, less than 30) 01:00-02:00 60KB/s (in practice, less than 60).

=====

where can i download linux MLPPP and Bell's throttling

Posted by Some Guy - 2009/07/23 04:59

Does Bell throttle BT in both directions? Both directions. Whether a TCP session is initiated by the local or remote end users, Bell will catch it and cripple it. What is the current Bell BT throttling strategy? 16:30-18:00 60KB/s (in practice, less than 60) 18:00-01:00 30KB/s (in practice, less than 30) 01:00-02:00 60KB/s (in practice, less than 60). What happens between 2:00 and 16:30 ??? Is that for all subscribers of Bell residential DSL (formerly known as Sympatico) ? What about business clients? I am an infrequent BT user. When I do torrent, the material that I download is such that I usually don't see more than 5 to 10 seeds and a similar number of leechers per torrent (and rarely ever seem to connect to more than 50% of the stated total number of seeders and leechers). And I practically never achieve a DL rate of more than 10 kb/sec from any single seeder or leecher (1 to 5 kb/sec is more typical DL rate from any single seeder or leecher). I'm not as concerned about UL rates, but I find that even when as few as one or two leechers are DL from me, that I hardly ever see a sustained UL rate higher than 10 kb/sec to any single leecher (and that's not because of any rate-limiting settings I have in my BT client). With regard to this Bell throttling and BT, are the rates mentioned above an aggregate of my total UL and DL for my DSL connection, or are they with regard to per-client BT traffic? I.E - Bell is throttling my TOTAL BT UL/DL rate to all leechers and seeders for all the torrents I have open, or the throttle is taking place on per-torrent or even per leecher or per seeder basis? And is this BT throttling (and the associated BT data-rate targets as listed above) independent of any other non-BT data bandwidth I might be using on my connection at the same time (viop, video streaming, web-surfing, etc) ?

=====

where can i download linux MLPPP and Bell's throttling

Posted by gbuchana(a)teksavvy(dot)com - 2009/07/23 04:59

This isn't rocket science. If you [HTTPS://www.mybank.ca](https://www.mybank.ca) then the DPI equipment can do exactly the same thing as your browser to get certificates, verify them and decrypt the communication. This is not the same as two peers who have previously exchanged keys and begin with an already encrypted connection. On those, the DPI equipment wouldn't be able to decrypt on the fly. I suggest you read up on SSL. SSL uses Diffie-Hellman key exchange to generate a unique session key for each connection. Effectively, the two peers start with an already encrypted connection. Hypothically an attacker can go to the same IP address and port it sees you going to, but that would be a new connection with a new negotiated session key. It can never get the session key for the original connection that way. _____ Gardner Buchanan
gbuchana(a)teksavvy(dot)com FreeBSD: Where you want to go. Today.

=====

where can i download linux MLPPP and Bell's throttling

Posted by Warren Oates - 2009/07/23 04:59

Or do those questions depend on where in Ontario I am, or which CO I'm connected through? I doubt if it makes much difference where you are. Throttling would be based on the time of day, which it was when I used to see it

=====

where can i download linux MLPPP and Bell's throttling

Posted by JF Mezei - 2009/07/23 04:59

And is this BT throttling (and the associated BT data-rate targets as listed above) independent of any other non-BT data bandwidth I might be using on my connection at the same time (viop, video streaming, web-surfing, etc) ? Yes, as long as Bell doesn't erroneously get some of your other data (such as secure FTP).

=====

where can i download linux MLPPP and Bell's throttling

Posted by JF Mezei - 2009/07/23 04:59

I suggest you read up on SSL. SSL uses Diffie-Hellman key exchange to generate a unique session key for each connection. Effectively, the two peers start with an already encrypted connection. If my browser is able to connect to some HTTPS server, and connect to a certificate authority to validate the server's credentials, then the DPI equipment can peek at both connections and emulate the client in terms of decrypting the connection. In the case of Bell, the DPI equipment has not yet been programmed to generate content (Roger's has). Inserting or changing content in an SLL connection would be much more difficult. But peeking into one without changing it is easier.

=====

where can i download linux MLPPP and Bell's throttling

Posted by Some Guy - 2009/07/23 04:59

I am an infrequent BT user. When I do torrent, the material that I download is such that I usually don't see more than 5 to 10 seeds I am like you. And it is extremely frustrating to have a slow feed being slowed to a crawl by Bell. My point was that I usually don't reach the 30 or 60 kb/sec limits when I torrent, so I'm wondering what is really limiting my connection. Are you saying that Bell throttling happens all the time - or only when my BT traffic reaches / exceeds 30/60 kb/sec? And are we talking about UL/DL combined cap at 30/60 kb/s, or separate?

=====

where can i download linux MLPPP and Bell's throttling

Posted by Some Guy - 2009/07/23 04:59

(...) Do you have any comment about Tek Savvy's mlppp offer of \$4/month? I thought any end-user could, with enough hardware tinkering, could establish an mlppp connection themselves, without needing to pay their ISP an extra fee. Am I wrong?

=====

where can i download linux MLPPP and Bell's throttling

Posted by JF Mezei - 2009/07/23 04:59

Do you have any comment about Tek Savvy's mlppp offer of \$4/month? The ISP needs routers that have the MLPPP support, and have to have it enabled. In the past, they did this as a test, and a few geeks found it was successful to bypass the throttling and it grew to a point where it brought down their routers. So now they bought equipment dedicated to MLPPP and turned off MLPPP on their other routers. To gain access to the router that has MLPPP[enabled, you need to pay the big bucks. Hopefully, my submission for the R&V final comments due tomorrow will convince the CRTC to block bell from throttling its competitors and MLPPP wont be needed anymore.

=====

where can i download linux MLPPP and Bell's throttling

Posted by gbuchana(a)teksavvy(dot)com - 2009/07/23 04:59

If my browser is able to connect to some HTTPS server, and connect to a certificate authority to validate the server's credentials, then the DPI equipment can peek at both connections and emulate the client in terms of decrypting the connection. No, it can't. It flat-out cannot. Your browser session and the one the attacker sets up use different session keys, and knowing one session key tells you nothing about the other. Look, if the kind of trivial attack you suggest were possible, online commerce would have collapsed in a heap years ago. SSL/TLS, especially browser implementations, has its limitations, but is much stronger than you are making out here.

gbuchana(a)teksavvy(dot)com
FreeBSD: Where you want to go. Today.

where can i download linux MLPPP and Bell's throttling

Posted by JF Mezei - 2009/07/23 04:59

No, it can't. It flat-out cannot. Your browser session and the one the attacker sets up use different session keys, and knowing one session key tells you nothing about the other. You don't understand DPI. Your own traffic flows THROUGH the DPI equipment. It is essentially spying equipment that scans all that you transmit and receive. If your browser can decrypt what the remote server sends, then so can the DPI equipment because it will have seen all of the exchanges and can duplicate this internally without you being aware of it. The main purpose of HTTPS isn't so much to encrypt communications, it is to authenticate that you are connecting to the right server. That is what the certificates are for.

where can i download linux MLPPP and Bell's throttling

Posted by Aidan Van Dyk - 2009/07/23 04:59

connected through? From my experience, it *is* location dependent... Living in Rural ontario, with sympatico (first few months at fantastic rate), all my IP traffic hopped from ottawa on to futher locations (Montreal and Toronto and out). And I never expereince any throttling. But as soon as I switched to teksavvy, or just using another login for testing, there was throttling going on... But using an non-sympatico service, my first IP hop was much further way (in toronto). I'm assuming that means that the throttling is in their GAS, the back-haul between the isp and the dslam/concentrator. And from that, I'm hypothesizing that they didn't (or maybe just didn't yet) have anything throttling the link from my local DSLAM to the local Ottawa POP that my sympatico PPPoE was being terminated at, but they did have throttling somewhere in the GAS between my local DSLAM and the teksavvy PPPoE termination. But that was a while ago, and things could certainly have changed...

where can i download linux MLPPP and Bell's throttling

Posted by Aidan Van Dyk - 2009/07/23 04:59

to authenticate that you are connecting to the right server. That is what the certificates are for. Exactly - and more specifically, that the key the right server is asking you to negotiate with is actually the right server's key. And knowing that without the right server's corresponding private key, that public key is pretty much useless.... The whole point of signed certs (and similarly, SSH fingerprints) is that I won't accept just any public-side key that claims to be www.mybank.com, rather only ones that have been signed by a trusted source, and thus that when I'm talking to that signed site, the only one able to decrypt that is the right server.

where can i download linux MLPPP and Bell's throttling

Posted by Aidan Van Dyk - 2009/07/23 04:59

The whole point of signed certs (and similarly, SSH fingerprints) is that I won't accept just any public-side key that claims to be www.mybank.com, rather only ones that have been signed by a trusted source, and thus that when I'm talking to that signed site, the only one able to decrypt that is the right server.
