BT 流量对校园网络造成的影响及其对策

The effects on Campous network by BT cuweat and the counterpolocy

卢东祥 于建江 (盐城师范学院计算机系 江苏盐城 224002)

摘要:本文只要针对 BT 流量在高校校园网络上应用所造成的影响和对策进行探讨,以抛砖引玉。

关键词:BT 流量控制 端口控制

1 引言

BT 下载以其独特的优势受到广大用户的喜爱,它在下载的同时还为其他用户提供上传,因此下载的人越多,它的速度越快。因此,在高速的校园网络上下载巨大的音乐、电影文件是非常流行和普遍的。不过,麻烦也随之而来,由于 BT 软件的出现,使得网络带宽一下子变得不够用了。据国际互联网流量监控公司最新统计发现 BT,KAZAA 和 EMULE 等 P2P 软件所占用的带宽超过了传统的 HTTP 80 端口并且已经超过了 60%。这对于以太网接入等共享带宽的校园网络提出了很大的挑战,大量的使接入层交换机的端口长期工作在线速状态,严重影响了用户使用正常的 Web、E-mail 以及视频点播等业务。本文试图就 BT 流量所造成的影响、BT 流量的控制以及宽带高校校园网络运营的对策做点探讨。

2 BT 对网络产生的影响

2.1 BT 下载增加了网络流量

当校园网络的用户开始使用 BT 下载,入站的流量就会从互联网经过广域网入口到达校园网络内部网。用户通常使用 BT 下载大量的多媒体文件,包括 MP3 格式的音频文件、CD 镜像、压缩的电影文件,以及光盘镜像(ISO)、大型软件。这些文件小则 4~5M,大则 600~700M,甚至上 G,全部数据均通过广域网出口流入。大量的 BT 下载必然造成很大的入站流量。

根据 BT 的原理可以知道,使用 BT 下载的主机同时也充当了上载的服务器。不管使用 BT 的用户是否知道这个原理,BT 下载带来了大量的出站流量。另外,在下载的任务结束之后,执行 BT 下载的主机将作为一个种子(Seed),将已经下载完成的文件提供给其他的 BT 用户使用,此时,网络流量基本上都是出站流量。这些流量会和其他的应用争夺有限的广域网出口出站带宽资源,增加了校园网络的负担。

2.2 改变了校园网络流量构成

BitTorrent(简称 BT,俗称 BT 下载、变态下载)是一个多点下载的源码公开的 P2P 软件,使用非常方便,就像一个浏览器插件,适合新发布的热门下载。其特点简单的说就是:下载的人越多,速度越快。目前校园网络大多使用广域网来连接互联网,由于 BT 大量的使用,会造成网络带宽被尽情的消耗。BT 所占用的带宽远远超过了传统的 HTTP 80 端口并且已经超过了 60%,严重破坏了广域网的出口带宽资源分配,彻底改变了校园网络流量构成。

2.3 造成网络拥挤,使校园网络关键业务明显延迟

BT 下载流量具有很大的侵略性。为了更有效率的交换文件,BT 下载程序在启动时会建立数量巨大的连接,这些连接会使得网络流量突然迸发,进而在相当一段时间内维持很大的网络流量。这种情况会带来很严重的问题。在校园网络中间,BT 下载不是唯一的应用程序,其他关键应用同样运行在这个网络上,并且使用了同一个广域网出口。

校园网络关键业务,如网络办公系统、远程教育系统、视频点播系统等等,这些应用会和 BT 下载共享校园网络带宽。而这些业务系统通常都是对反应时间要求很高的。在 BT 下载运行时,操作人员会明显地感觉到这些业务系统反应变慢,甚至没有反应。其他对反应时间要求不是很高的应用,如电子邮件、数据备份、数据库数据同步等等,也很容易遭受到带宽的威胁。

3　BT 下载的“堵”与“疏”

每个校园网络的管理者对管理的网络都有不同的理解，因此，对于 BT 下载的控制方式也不尽相同。但归根结底无非是两种做法，一是：“堵”即通过技术手法隔离 BT，杜绝一切 BT 流量；二是：“疏”即在特定的范围、时间内可以使用 BT，允许流量通过，满足大家的需求。

3.1　堵隔 BT 流量

（1）限制浏览 BT 网站。BT 网站很多，但考虑到 BT 下载的特点：下载的人数越多，速度越快；Seed 越多，速度越快。只有比较热门 BT 网站的 Torrent 文件下载的人才会比较多，一般的 BT 网站去的人就比较少，下载的人数也少，除非他能忍受每秒几 K 的速度。因此针对比较热门的 BT 网站，获得服务器地址后就可以到核心服务器上对该地址进行封锁。以 Cisco 设备为例，具体命令为：

access – list 102 deny tcp any 202.103.9.83 0.0.0.0

这种方法使用 access – list 命令来控制，实现起来比较容易。但由于 BT 网站比较多而且层出不穷，因而 access – list 命令的条数会因为 BT 服务器的数量增加而增加，随着 access – list 命令条数的增多路由器的负荷也随之增加。从实际操作上来看，BT 的种子网站众多，而且无需固定的服务器，要想监控，难度也很大，技术上难以实现。

（2）封闭 BT 下载端口。解决 BT 对局域网的危害，最彻底的方法是不允许进行 BT 下载，BT 一般使用 TCP 的 6881～6889 的端口，网络管理员可以根据网络流量的变化进行判断，在网关中将特定的种子发布站点和端口封掉，在 BT 下载软件中的 Track 中可以获得这些信息；但是现在大多数 BT 软件可以修改端口号，因此网管可以根据实际情况，利用访问控制列表在不影响正常业务的情况下尽可能将封闭的端口范围扩大，把一些特定的种子发布站点和端口进行封闭。以 Cisco 设备为例，具体命令为：

access – list 101 deny tcp any any range 6880 6890
access – list 101 deny tcp any range 6880 6890 any
access – list 101 permit ip any any

接着进入相应的端口，输入 ip access – group 101 out 使访问控制列表生效配置之后，网络带宽就会马上释放出来，网络速度得到提升。

这种方法也使用 access – list 命令来控制，实现起来比较容易。但是由于 BT 可以自由变换端口这样一来，势必要封堵大量的端口，封闭了端口必然影响了网络的应用。有的网络管理员甚至仅仅打开 80、53、21、25、110 等常用端口而封闭其他所有端口。

（3）加载 PDLM 模块。使用 CISCO 公司出品的 PDLM 模块可以省去我们配置路由策略的工作，封锁效果非常好. 上文介绍的两种方法。一个是对数据包的目的地址进行封锁，一个是对数据包使用的端口进行封锁，虽然在一定范围内有效，但不能起到全面禁止 BT 的作用，通过 PDLM + N BAR 的方法来封锁 BT 就存在这个问题了。

CISCO 在其官方网站提供了三个 PDLM 模块，分别为 KAZAA2. pdlm，bittorrent. pdlm. emonkey. pdlm 可以用来封锁 KAZAA，BT，电驴，在此我们就封锁 BT 下载为例：

建立一个 TFTP 站点，将 bittorrent. pdlm 复制到该站点，在核心路由器中使用 ip nbar pdlm tftp：//TFTP 站点的 IP/bittorrent. pdlm 命令加载 bittorrent. pdlm 模块

接下来设置路器策略，具体命令如下：

class – map match – any bit
//创建一个 CLASS_MAP 名为 BIT
match protocol bittorrent
//要求符合模块 bittorrent 的标准！
policy – map limit – bit
//创建一个 POLICY – MAP 名为 LIMIT – BIT
class bit
//要求符合刚才定义的名为 BIT 的 CLASS – MAP
drop
//如果符合则丢数据包！
interface gigabitEthernet0/2
//进入网络出口那个接口
service – policy input limit – bit
//当有数据包进入时启用 LIMIT – BIT 路由策略
service – policy output limit – bit
//当有数据包出的时候启用 LIMIT – BIT 路由策略

如果不想每次启动路由器的都要手工加载 TFTP 上的 bittorrent. pdlm，可以把这个 PDLM 文件上传到路由器的 FLASH 中，然后选择 TFTP 服务器的 IP 地址即

可。值得提醒大家的是封锁 KAZAA 或者是 EDONKEY 时,在路由器配置中将" match protocol 后的 bittorrent 替换为 KAZAA2 或者 EDONKEY 即可,其它配置和封锁 BT 一样,通过 NBAR 加载 PDLM 模块法封锁 BT 软件后,已经完全断绝了 BT 流量,网络速度也恢复到以前的稳定值了。

(4) 采用 NAT 的单用户连接数限制。在 Cisco IOS 12.3(4)T 后的 IOS 软件上支持 NAT 的单用户限制,即可以对做地址转换的单个 IP 限制其 NAT 的表项数,因为 p2p 类软件如 bt 的一大特点就是同时会有很多的连接数,从而占用了大量的 NAT 表项,因此应用该方法可有效限制 bt 的使用,比如我们为 IP 10.1.1.1 设置最大的 NAT 表项数为 200;正常的网络访问肯定够用了,但如果使用 bt,那么很快此 IP 的 NAT 表项数达到 200,一旦达到峰值,该 IP 的其他访问就无法再进行 NAT 转换,必须等待到 NAT 表项失效后,才能再次使用,这样有效的保护了网络的带宽,同时也达到了警示的作用。

例如限制 IP 地址为 10.1.1.1 的主机 NAT 的条目为 200 条,配置如下:

ip nat translation max – entries host 10.1.1.1 200

如果想限制所有主机,使每台主机的 NAT 条目为 200,可进行如下配置:

ip nat translation max – entries all – host 200

(5) 使用 HTTP 代理对应用层协议进行过滤。当 BT 客户端下载时,必须进行 Tracker 查询,Tracker 通过 HTTP 的 GET 命令的参数来接收信息,而响应给对方(下载者)的是 Bencoded 编码的消息。在 HTTP 请求报文中,携带了 BT 的特征值 User – Agent:BitTorrent。

网络管理员针对该情况,可以通过一些安全管理设备以及流量管理设备,甚至网络管理系统软件,过滤特定的应用层数据包(如 HTTP 数据包),然后根据 BT 数据包中的关键字(BitTorrent),从 HTTP 数据包中过滤 BT 数据包。

3.2 疏通 BT 流量

(1) 将整体 BT 下载的流量控制在某个范围内。如整个校园网络可以使用的 BT 下载流量设定为 1Mbps。校园网络剩余的其他网络带宽资源可以给关键业务或者其他非关键业务使用,有效地防止 BT 下载侵吞大量网络带宽资源。以 Cisco 设备为例,具体命令为:

access – list 130 remark bt

access – list 130 permit tcp any any range 6881 6890

access – list 130 permit tcp any range 6881 6890 any

rate – limit input access – group 130 712000 8000 8000 conform – action transmit exceed – action drop

rate – limit output access – group 130 712000 8000 8000 conform – action transmit exceed – action drop

(2) 限制或者禁止在特定时间段内的 BT 下载。校园网络工作时间内限制或者禁止 BT 下载,这样工作时间内不会有 BT 下载流量和关键业务竞争,也充分保护了校园网络关键业务。同时,在非工作时间,校园网络也可以自行利用高速的网络络资源。以 Cisco 设备为例,具体命令为:

time – range test

periodic daily 20:00 to 23:00

access – list 130 permit tcp any any range 6881 6890 time – range test

access – list 130 permit tcp any range 6881 6890 any time – range test

(3) 将校园网络关键业务划分到专用动态带宽中间,BT 下载使用剩余带宽,避免两者竞争。某些特定校园网络会使用 BT 下载提供服务。对于这样的校园网络,由于 BT 下载具有很高的侵略性,因此需要使用保护机制来保障其他关键业务的正常运行。网络管理员可以通过一些管理软件或者网络硬件配置,针对应用流进行较细粒度的速率限制,例如将 BT 用户下载的优先级限制为 5(0 最高,7 最低),带宽限制为 64 kbps。这样可以确保 BT 软件使用的同时不会影响其他业务的开展,充分保护这些应用。剩余的网络资源可以全部提供给 BT 下载使用。

4 结束语

最近一段时间里,网络上关于"封杀 BT"问题上的争论,仁者见仁,智者见智。总的来说,BT 是 P2P 技术在解决大容量文件的问题上是一种很好的解决方案,它代表着网络发展的一种趋势,是网络资源共享的一种倾向。至于如何对待,在不同的单位不同的场合因该具体情况具体分析,封杀不是唯一的办法,更不是最终的解决方案。