思科认证:通过路由器设定来控制带宽流量占用Cisco认证考试
 BT是近年来比较热门的基于P2P技术的分布式数据共享与传播软件，不同的人对这类应用有不同的看法。支持的人说它完满地体现了我为人人，人人为我的思想，任何一个人都可以在网络上向别人提供自己的文档或软件下载，当下载的人越多时它的下载的速度也越来越快；反对的人说它侵犯了软件作者的版权以及耗费了大量的网络带宽，应该给予禁止。不管人们对这个软件的看法如何，作为一个主要从事教育的大学来讲，首先要保护作者的知识产权不会受到侵犯，另外还要保证学校的网络资源能够被合理利用，以保障教学及其它应用的正常开展。对任何一所大学来说它的网络带宽资源是十分宝贵的，但是BT软件的使用耗费了大量的带宽，使得原来一些需要保证的应用受到影响，使用理论的说教往往不能使喜欢这类软件的人放弃这种喜好，所以有必要对此类软件从技术手段上进行限制。下面来分析一下BT下载类软件的工作原理，找到可以用来限制此类应用的依据，然后再进行限制。 首先BT类下载软件一般使用的端口是固定的一个范围，常用的范围是：6881～6890，如果我们能够在路由器中对这一段的端口进行限制，就可以对此类软件进行限制了。但是也有一些BT软件，可以自动更新端口。此类软件有一个共同的特点是在工作时占用的带宽很大，往往要超过正常的应用，所以我们从两个方面对此类软件进行限制：一个是限制它应用的端口，一个是对异常的流量进行限制。下面就这两个方面进行配置

：一．使用基于类的路由策略进行控制 1．端口限制： access-list 101 deny tcp any eq range 6881 6890 any range 6881 6890 access-list 101 permit any any 2．流量限制： class-map match-all bt_updown match access-group 101 policy-map 0drop-bt_updown class bt_updown police 1024000 51200 51200 conform-action 0drop exceed-action 0drop violate-action 0drop 二．使用上述的基于类的策略在对付自动变更端口的BT类软件时有些力不从心。为此，CISCO路由器提供了专门的PDLM（Packet Description Language Module）包描述语言模块从协议层上进行对此类软件使用的协议进行了描述。因此，路由器可以对数据包使用的协议进行分析，当传输的数据包符合该协议的描述时路由器可以识别，配合相应的类策略对数据进行控制（如允许通过或丢弃等），从而根本上解决了动态端口的控制弊病。但是由于PDLM模块属于非公开资源，CISCO公司对该资源的下载和传播进行了严格的控制，必须具有CCO资格的路由器用户方可下载使用。由于该 PDLM不属于路由器的启动加载项，所以重新启动路由器时，必须通过TFTP进行进行手动加载： ip nbar pdlm tftp://192.168.100.2/bittorrent.pdlm //bittorent.pdlm为下载的pdlm模块文件名 class-map match-all bt_updown //定义类bt_updown match protocol bittorrent //匹配bittorrent协议 policy-map limit-bt //定义策略图limit_bt class bt_updown //将类bt_updown加载到策略图中作为触发事件 police cir 240000 conform-action transmit exceed-action 0drop //定义符合和超载传输流大小为240000 bits police cir 8000 conform-action transimit exceed-action 0drop 在路由器相应端口上加载服务策略： service-policy input limit-bit //限制下载，流

入 service-policy output limit-bit //限制上传，流出 2001年出现的尼姆达病毒（Nimda）、红色代码病毒均是蠕虫病毒，这些病毒借助于网络进行传播，传播的速度快，对感染的计算机破坏强。用户一旦感染了这种病毒，只要所处的网络中存在有此类的病毒，一般情况下是很难清除的。这里不想对病毒的工作原理及如何清除这些病毒进行过多的。 论述，而主要讨论这些病毒的网络行为如何在路由器中被识别出来并且使用相应的策略对这些数据包加以阻止或丢弃。 尼姆达病毒在网络中传播的主要特征有： 1、利用病毒宿主通过网络短时间内发送大量的含有 “ readme.exe ” 附件的 “ readme.eml ” 电子邮件； 2、搜寻以前的IIS蠕虫病毒留下的后门程序曾经或已经感染红色代码病毒（Code Red）并留下了病毒后门，尼姆达病毒就会利用后门程序进行漏洞扫描； 3、通过大量含有病毒的电子邮件的发送和扫描将导致网络服务产生拒绝服务（DoS）。 在分析尼姆达病毒的主要特征后，可以在路由器上有针对性进行配置以防范和阻止尼姆达病毒的传播： a.阻塞端口 access-list 101 deny tcp any eq 25 any eq 25 //阻塞SMTP协议端口 access-list 101 deny tcp any eq 69 any eq 69 //阻塞TFTP端口 access-list 101 deny tcp any eq 135 any eq 135 //阻塞NetBIOS协议 access-list 101 deny tcp any eq 445 any eq 445 //阻塞NetBIOS协议 access-list 101 deny tcp any eq range 138 139 any range 138 139 //阻塞NetBIOS协议 access-list 101 permit any any b.配置策略图 class-map match-all nimda //定义类nimda match protocol http url "*.ida*" //匹配HTTP协议中的url地址中含有.ida关键词 match protocol http url "*cmd.exe*" //匹配HTTP协议中的url地址中含有cmd.exe关键词 match protocol http url

"*root.exe*" //匹配HTTP协议中的url地址中含有root.exe关键词 match protocol http url "*readme.eml*" //匹配HTTP协议中的url地址中含有readme.eml关键词 policy-map block_nimda //定义策略图block_nimda class nimda //将类nimda加载到策略图中作为触发事件 police 512000 128000 256000 conform-action transmit exceed-action 0drop violate-action 0drop //定义路由器速率限制策略 结束语： 上述所有基于QoS的路由器配置在思科2621XM路由器上测试通过。通过测试，不但可以明显减轻BT、Nimda等病毒对网络的冲击和对网络资源的大量消耗，保护正常计算机用户对网络资源的需求，同时也可以有效防止其他类似的网络蠕虫病毒的攻击，实际价值非常明显；但是如果你想将BT完全封掉，可以考虑购买专门的P2P限制软件，国内诸如聚生网管（http://www.grabsun.com）之类的网管软件，在控制P2P方面非常不错，可以将BT完全封掉；实际测试中，我们还发现思科的路由器在控制新兴的P2P软件方面不是十分有效，如迅雷（包括web迅雷），下载速度远远超过传统的P2P软件，是当前下载速度最快的P2P软件，由于采用了多协议交叉下载的方式，所以通过规则匹配的效果不是十分明显。在这方面聚生网管较为强悍，可以将迅雷完全封掉，在国内还是比较领先的。 