用网络应用识别技术管理 P2P 应用

赵 毅 别 牧
(重庆交通学院 重庆 400074)

摘 要 P2P是互联网上的最新应用,但BT下载等应用严重影响网络的正常运行。利用NBAR(网络应用识别)技术,深度、准确识别网络中的P2P数据流,能够合理地使用P2P应用。本文介绍了NBAR原理及特性,给出一个NBAR具体应用的实例,并对应用NBAR对路由器性能的影响作出分析,展望管理P2P应用发展的方向。

关键词 P2P, NBAR, BT,识别, 下载

On Managing P2P Application with NBAR Technology

ZHAO Yi BIE Mu
(Chongqing Jiaotong Uiniversity,Chongqing 400074)

Abstract P2P is the latest application in the Internet while these applications like BT download would greatly endanger normal network application. Concise identification of the P2P data flow with the application of NBAR technology can reasonably apply to P2P. The paper introduces the principles and the features of NBAR by presenting specific examples of the application. It also analyses the influence of Router and the future direction of managing P2P application.

Keywords P2P, NBAR, BT, Recognition, Download

互联网上的对等连接P2P应用发展迅速,BitTorrent(简称BT)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,很适合新发布的热门下载。其特点是:"我为人人,人人为我",下载的人越多,速度越快。但是,由于BT大量的使用,会造成网络带宽被尽情地消耗,导致一些企业和单位的关键业务不能正常运行,所以有必要对BT流量进行一定的控制。

网络管理员采用了限制访问BT网站,封闭BT下载端口,限制用户带宽等多种方法对BT下载进行控制,其中一些办法不能完全奏效,彻底封杀BT这种新的应用也是不合适的。采用网络应用识别技术对协议进行深度识别,能有效控制BT的合理应用。

1 NBAR网络应用识别技术

1.1 网络应用识别技术原理

网络应用识别(NBAR)是Cisco IOS Software中的新特性,能够为基础设施提供智能网络分类。NBAR是一种新的分类引擎,能够识别多种应用,包括基于Web的应用,以及动态分配TCP或UDP端口号的客户机/服务器应用。完成应用识别后,网络可以为该应用提供相应的服务。目前,NBAR与服务质量(QoS)特性配合使用,能够最合理地使用网络带宽,实现企业目标。这些特性包括:保证主要应用的带宽,限制其它应用的带宽,有选择地丢弃分组以避免出现拥堵,给分组作上标记以便网络和服务供应商的网络能够端到端提供QoS。

例如,在Oracle数据库服务器上的公司数据库中查询订单状态时,客户服务需要快速答复。但是,如果网络上的其他人正在使用VDOLive等高带宽应用,或者查看大型GIF文件,则对Oracle数据库的SQL*NET事务处理可能被延迟。而NBAR就能解决这个问题,因为它能够对应用分类,然后一面为SQL*NET查询提供足够的带宽,一面执行其它应用。该解决方案如图1所示。

不同于netflow技术,利用NBAR,能分析网络3层到7层数据(如图2),对网络上的企业能够实施智能分类,并对当今的关键业务应用实施QoS策略。NBAR支持多种网络协议,包括在NBAR出现之前难以识别的以下状态化协议:按URL、主机和MIME类型实施HTTP分类;Oracle SQL*NET;Sun RPC;Microsoft Exchange;VDOLive;RealAudio;Microsoft Netshow;文件传输协议(FTP);StreamWorks。另外,NBAR还能对传统的静态端口协议进行分类,以便支持多种解决方案。

通过思科开发的数据包描述语言模块(PDLM),可以轻松、快速地添加新协议。PDLM包含NBAR用于识别的规则,多数情况下,不需要新Cisco IOS软件镜像,甚至不需要重新启动就能实现加载。

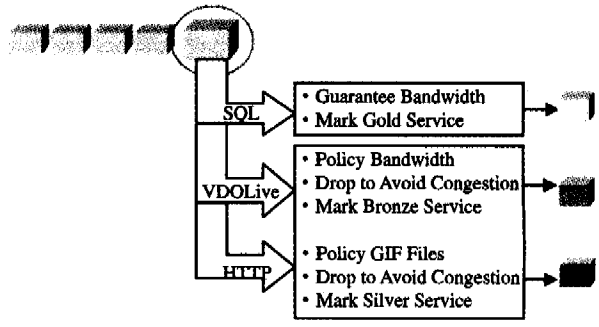

图1 NBAR能够提供智能网络分类

对应用进行智能分类之后,网络可以应用以下QoS特性:利用基于等级的加权公平排序(CBWFQ)保障带宽;通过

赵 毅 硕士生,主要从事计算机网络安全研究。

监控实施带宽限制；在IP报头中使用服务类型(ToS)位或Diff Serv代码点(DSCP)给与众不同的下行服务或来自服务供应商的服务作上标记；通过丢弃避免拥堵。

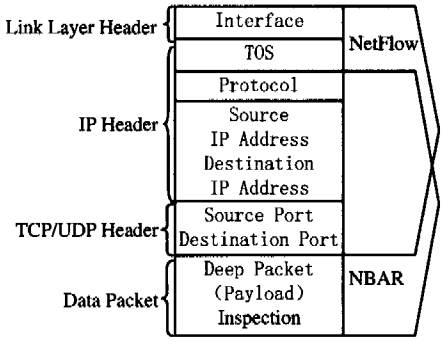

图2 NBAR对IP数据包的深度识别

1.2 网络应用识别技术的优点

保证关键业务应用的性能 Oracle、Citrix、Microsoft Exchange等关键业务应用或者新型Web应用必须连续正常运行才能保证企业在快速发展的电子商务环境中取得成功。许多地方都有可能出现瓶颈，包括网络。即使花巨资为每个应用提供了过量的带宽，也有可能出现瓶颈。其原因是，员工通常会使用新型互联网应用，例如流音频和视频，或者下载新程序。这些应用都会很快耗尽企业的WAN带宽。遗憾的是，这些并不是企业希望优先处理的关键业务应用。如果能够智能地识别应用，NBAR将能够使网络为每种应用提供不同的服务。对于Oracle等关键业务应用，或者在某个Web页面上运行的应用，企业可以给予绝对的优先处理，并提供足够的带宽。与此同时，企业还可以限制"带宽猪"对带宽的消耗，使用户能够以最低的延迟访问关键业务应用，而企业则不需要进行昂贵的WAN链路升级，也不需要切断经常使用但非关键业务应用的连接。

缩减WAN开支 过去十年里，WAN成本一直在下降，尤其是在非管制市场上。但是，在世界上许多地区，尤其是在国家之间，电信链路仍然比较昂贵。这使网络经理陷入了两难境地：一方面，企业必须提供对新型客户机-服务器和互联网应用的访问；另一方面，又需要控制WAN服务成本。为解决这个问题，NBAR提供了一种解决方案，使企业能够以智能方式利用WAN带宽，以便以最低的带宽提供可以接受的服务水平。NBAR能够识别关键业务应用，以便为其分配更高的优先级或足够的带宽，避免非关键应用占用这些比较慢的国际链路，阻碍关键业务流量的传输。

增强Web响应能力 目前，无论是对内部交流，还是外部交流，Web都已经成为许多企业的关键业务资源。员工、合作伙伴和客户必须能够正常访问所需要的Web页面，而不能出现下载缓慢或Web应用失效等问题。利用NBAR，企业能够识别企业认为重要的Web页面和Web内容，例如：访问销售订单页面的客户应得到优先处理，以免客户在销售点不耐烦。销售工具也应给予绝对的优先处理和足够的带宽，以保证销售人员不需要因另一名员工正在使用流视频浏览公司最新推出的电视广告而长久等待产品报价。基于Web的应用一般加载比较慢，利用NBAR，可以按MIME类型识别应用，并给予优先处理。JPEG图片等内容占用大量带宽，但不属于基于Web的关键信息。在这种情况下，可以控制这些"带宽猪"占用的带宽。

改善虚拟专用网的性能 虚拟专用网(VPN)不但能降低联网成本，还能提高灵活性。遗憾的是，VPN中的服务质量很难保证。同时在同一台路由器中运行NBAR和VPN能够解决这个问题，因为这样可以在加密之前识别关键业务流量，并允许网络使用适当的QoS控制。另外，通过同时运行VPN和NBAR，我们还能保证以正常的顺序处理分组，以提高安全性，实现相应的QoS。当远程员工访问关键的企业资源规划(ERP)应用时，NBAR将进行包识别，作上"金色服务"标记，然后放入高优先级序列。然后，VPN流程对分组进行加密，并继续在新分组上作"金色服务"标记。当传输到在网络上提供多种服务的服务供应商的网络上时，ERP应用将在穿过VPN的过程中得到优先处理。与之相反，同一员工访问的非关键应用则只能得到低优先级服务。

提高多服务性能 利用多服务网络，可以将数据、话音和视频信息聚合到同一个网络上。遗憾的是，不同的服务需要不同的网络特性。NBAR能够以智能方式识别分组的种类，并提供适当的网络特性。

2 控制BT下载的一般方法

BitTorrent下载工具软件可以说是一个最新概念P2P的下载工具，常用的软件还有：eDonkey，BitComet，PTC(Personal Torrents Collector)，Sharcaza等等。它采用了多点对多点的原理，每个用户既是客户端又是服务端，产生大量的网络连接，对网络交换机造成很大的压力，也占用大量的出口带宽，使正常应用无法进行，常用的控制方法有以下几种：

2.1 限制浏览热门BT网站及Tracker服务器

在路由器、防火墙、计费服务器等设备上，都可以配置相应的URL过滤规则，限制内网用户对热门的BT网站进行访问。但BT网站越来越多，不可能完全限制所有的BT网站。

2.2 封闭BT软件下载端口

BT软件一般使用TCP的6881-6889的端口，可以在路由器中用访问控制列表封掉相应的端口，但是现在很多BT软件其应用端口会根据应用端口的可用性，随机更改当前的应用端口，使访问控制列表失效。

2.3 限制最大连接数

每个BT下载都会产生大量的TCP连接，一般一个热门的下载会产生100～150个TCP连接。因此，网络管理员可以根据这个特点，在交换机、防火墙或者计费服务器上，限制每个用户对外产生的最大网络连接数，从而减轻交换机的压力，控制BT对网络带宽的占用。

2.4 限制用户的带宽

BT之所以会危害到局域网，是因为它占用了大量用户带宽。因此，限制每个用户使用的网络带宽，可以明显缓解BT对网络的危害，完全禁止BT使用是不合理的，限制每个BT的使用带宽是一个比较好的选择。现在的网络交换机一般都能在接入端口上对接入带宽进行控制。

3 网络应用识别技术应用

3.1 NBAR控制BT下载配置实例

NBAR是新版本cisco ios内置的功能(cisco 7200和7100系列平台从12.0(5)XEZ开始支持，2600和3600系列从12.1(4)T开始支持)，并提供对大多数常见应用协议的支持，要实现对BT流量的控制，就要在思科路由器上实现对PDLM的支持。PDLM是Packet Description Language Mod-

ule 的缩写，意思是数据包描述语言模块。它是一种对网络高层应用的协议层的描述，例如协议类型，服务端口号等。它的优势是让 NBAR 适应很多已有的网络应用，像 HTTP URL，DNS，FTP，VoIP 等，同时它还可以通过定义，来使 NBAR 支持许多新兴的网络应用。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，具体配置步骤如下：

① 使用 TFTP 把 bittorrent. pldm 文件拷贝到路由器的 FLASH 中

② 加载 pdlm 模块：

ip nbar pdlm bittorrent. pdlm

③ 建立 BT 特征码相关的 class-map "denybt"：

class-map match-any denybt

match protocol bittorrent

④定义符合 bittorrent 特征的数据包处理方式 policy：

policy-map bittorrent-policy

class denybt

drop

⑤ 然后在你的路由器内网端口配置中添加 service-policy

interface f 1/1

ip address 202. 202. 240. 65 255. 255. 255. 0

ip nat inside

service-policy input bittorrent-policy

\\定义对进入的数据包执行策略检查

service-policy output bittorrent-policy

\\定义对外出的数据包执行策略检查

duplex full

3.2 启用 NBAR 对路由器性能的影响

现在企业的路由器除了完成路由寻址，数据转发功能外，还承担许多其它的功能，比如：利用访问控制列表实现一些安全功能，地址转换功能，IP 与 MAC 绑定等等。路由器的负荷相当重，路由器已经是网络中的瓶颈。

启用 NBAR 当然会对路由器的使用增加一些负担，通常情况下，和访问控制列表一样，会增加路由器 CPU 利用率的 11%～38%，不同的平台影响的大小不一样，越高端的平台影响就越小，另一方面和路由器的配置及网络中流量的类别也有关系，主要是以下几个方面：需要匹配协议的数量；使用配置匹配规则的数量；所检测数据流的复杂度；数据流种类的多少；持续时间长的数据流开销较小；静态端口协议开销较小。而路由器端口的速度，是否在多个端口上应用 NBAR 不会对路由器的性能产生影响。

图 3 是在 cisco 3745 路由器上的测试结果图，在 60%负载无掉包(NDR)情况下，模拟企业实际应用数据流，在不开启 NBAR，开启 NBAR 协议匹配，开启 NBAR 协议发现，既开启协议匹配又开启协议发现四种状况下的测试，我们可以看到，开启 NBAR 协议发现后，CPU 的利用率增加了 32%。同样的情况，在 cisco 7500 平台上 CPU 的利用率增加只有 2%。

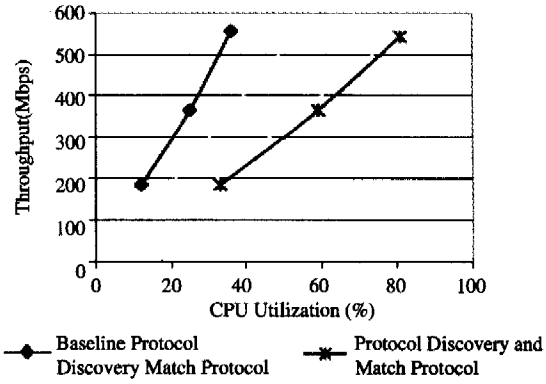

图 3 cisco 3745 NBAR 性能测试图

结束语 P2P 应用的迅速发展，对带宽，网络设备提出更高的要求，甚至成为危害网络安全稳定的因素，但 P2P 是符合互联网平等精神的应用，是未来发展的方向，所以我们不能完全禁止这种新技术的使用。使用 NBAR 技术对网络的数据流进行深度准确的识别，从而更好地管理网络，合理地使用。对 P2P 应用数据流的正确识别，是合理使用 P2P 的基础。

目前，各网络设备商推出许多新的技术，增加深度识别的方法和提高设备对数据深层解析的性能，如：Cisco 公司的安全智能网络方案，华为 3com 公司基于 XRS 的产品，锐捷公司集自动防御、自动修复与自动学习于一体的 GSN 全局安全解决方案等。最终网络将形成统一的识别标准，对应用层更加精细的控制和处理，包括根据不同的应用采取不同的策略，实现全网资源的统一调配和优化。

参 考 文 献

1 http://www. cisco. com Network-Based Application Recognition Overview

2 http://www. cisco. com Network-Based Application Recognition Q&A

3 邹仁明，李吉祥，彭隽. 出口流量的分析与管理. 中国教育网络[J]. 2005，09：22～25

4 春丽. 防火墙控制 BT 的几种方法[N]. 网络世界. 2005，16：40～40

5 李梅. P2P 遭遇阻击与控制. 计算机世界[N]. 2005，32：B1-B3

6 http://www. cisco. com Network-Based Application Recognition Performance Analysis