Cisco路由器上CAR的工作原理及应用

贺春林
(西华师范大学计算机学院　南充637000)

摘　要　本文介绍了Cisco路由器上的承诺访问速率(CAR)的机制和实现方法,并提供了一些配置的范例和具体的应用,对于提高网络的带宽和利用率有一定的作用。

关键词　承诺访问速率,流量控制

The Work Mechanism and Application of CAR on the Cisco Router

HE Chun-Lin
(The College of Computer Science, China West Normal University, Nanchong 637002)

Abstract　This article introduces the mechanism of CAR and the methods of application on the Cisco router, also provides some examples of configuration and a specific way of application. It can improve the use of rate and increase the brandwidth of the network.

Keywords　Committed access rate, Rate-limit

1　前言

随着计算机技术的发展和网络应用的不断深入和软件的不断更新,网络上运行的应用软件越来越趋向多样化,并设有邮件服务和信息服务,这使得在网络上的带宽受到挑战。因此,在网络上保证应用软件的良好运行,流量控制就显得尤其重要。一种方法是购买流量控制的产品,如PacketShaper,但是这类产品价格比较昂贵,应用受到限制。另一种方法就是在路由器上采用流量控制策略,本文基于此,对Cisco路由器的CAR的工作机制及应用加以分析。

2　CAR的工作原理

2.1　CAR及其作用

CAR即承诺访问速率(Committed Access Rate),主要有两个作用:对一个端口或子端口(subinterface)的进出流量速率按某个标准上限进行限制;对流量进行分类,划分出不同的QoS优先级。

CAR只能对IP包起作用,对非IP流量不能进行限制,另外CAR只能在支持CEF交换(Cisco Express Forward)的路由器或交换机上使用。所以只有Cisco 2600系列以上的型号才可以使用CAR。以下这些interface上也不能使用CAR:Fast EtherChannel Interface、Tunnel Interface、PRI Interface。

2.2　CAR的运作机制

CAR可以是数据包分类识别(packet classification)和流量控制(access rate limiting)的结合。其工作流程如图1所示。

第一步　流量匹配(Traffic Matching)。首先从数据流中识别出感兴趣的流量,即用户希望对其进行流量控制的数据包类型。用户可以选择以下几种不同的方式来进行流量识别:

① 全部的IP流量,这样可以把所有的IP流量采用统一的流量控制策略。

② 基于IP前缀,此种方式是通过rate-limit access list来定义的。

③QoS分组。

④MAC地址,此种方式通过rate-limit access list来定义。

⑤IP access list,可通过standard或extended access list来定义。

第二步　流量衡量(traffic measurement)。CAR采用一种名为token bucket的机制来进行流量衡量(如图2)。

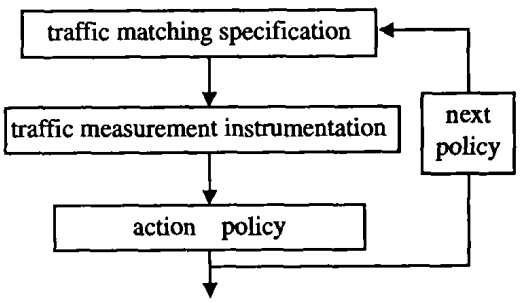

图1　CAR工作流程图

图2中token可以认为是第一步流量匹配所识别到的感兴趣流量,该种流量的数据包进入一个bucket内,该bucket的深度则由用户定义,在进入该token bucket后,以用户希望控制的流量速率(此流量速率并非该类流量的实际速率,而是用户希望该类流量的速率上限)离开该bucket,执行下一步操作(conform action)。在这里,对于实际流量速率的不同,可以看到会有两种情况发生:

① 实际流量小于或等于用户希望速率,这样,明显地,token离开bucket的实际速率将和其来到的速率一样,bucket内可以看作是空的。流量不会超过用户的希望值。

②实际流量大于用户希望速率。这样,token进入bucket的速率比其离开bucket的速率快,这样在一段时间内,token将填满该bucket,继续到来的token将溢出(excess)bucket,则CAR采取相应的动作(一般是丢弃或将其IP前缀改变以

改变该 token 的优先级)。这样就保证了数据流量速率保证在用户定义的希望值内。

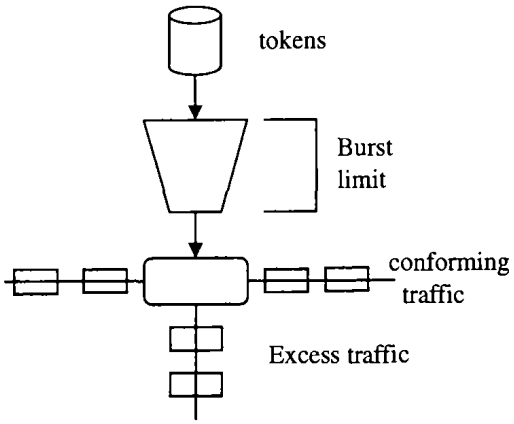

图2 CAR 的流量控制

3 配置 CAR

3.1 确定"感兴趣"的流量类型

可通过下列方式确定:(1)所有的 IP 流量;(2)基于 IP 前缀;(3)基于 QoS 分组;(4)基于 MAC 地址;(5)基于 standard 或 extended 的 IP access list。最常用的是第五种方式。用户可以使用 standard ip access list 来确定哪些进行访问(被访问)的 IP 的流量需要进行 rate-limit,也可以用 extended ip access list 来确定哪些访问(被访问)的 IP 的协议类型流量(如 HTTP,FTP)需要进行 rate-limit。例如想限制用户到内部网站上浏览网页的速度,则可以采用如下的 access list 来定义流量:

access-list 101 permit tcp any eq www any

值得注意的是在配置时要配成 any eq www any 而不是 any any eq www。因为主要的流量不是用户向 http server 发送的请求(这类请求流量的源端口号为随机,目的端口号为 80),而是 http server 收到用户的请求后发给用户方的网页内容的流量(这部分流量的源端口号为80,目的端口号为发起方的端口号),如果在这个小细节上不加注意则不能对下载的流量进行有效的限制。

3.2 在相应的端口配置 rate-limit

一般格式:

interface X

rate-limit {input | output} [access-group number] bps burst-normal burst-max conform-action action exceed-action action

其中,interface:用户希望进行流量控制的端口,可以是 Ethernet 也可以是 serial 口,但是不同类型的 interface 在下面的 input|output 上选择有所不同,需要注意一下。

input|output:用户希望限制输入或输出的流量。还是以限制浏览网页为例子,如果在以太网端口配置,则该流量为 output;如果在 serial 端口配置,则该流量为 input。

access-group number:number 是前面用户用 access list 定义流量的 access list 号码。

bps:用户希望该流量的速率上限,单位是 bps。

burst-normal burst-max:这个是指 token bucket 的大小,一般采用8000,16000,32000这些值,视 bps 值的大小而定。

conform-action:在速率限制以下的流量的处理策略。

exceed-action:超过速率限制的流量的处理策略。

action:处理策略,包括以下几种:①transmit:传输;②drop:丢弃;③set precedence and transmit:修改 IP 前缀然后传输;④set QoS group and transmit:将该流量划入一个 QoS group 内传输;⑤continue:不动作,看下一条 rate-limit 命令中有无流量匹配和处理策略,如无,则 transmit;⑥set precedence and continue:修改 IP 前缀然后 continue;⑦set QoS group and continue:划入 QoS group 然后 continue。

需要指出,在一个 interface 内,可以配置多条 rate-limit 命令,如果 action 里面有 continue,则顺序执行下一条 rate-limit 命令,若某种流量在 continue 之后没有被某条 rate-limit 命令丢弃,则它将进行传输。一个端口最多可配20条 rate-limit 命令。

那么对于进行 http 限制的例子,相应的配置为:

interface e0

rate-limit output access-group 101 128000 16000 16000 conform-action transmit exceed-action drop

这里把下载的流量定义在128kbps,token bucket 的大小为16000字节。如果把 token bucket 定得太小,则用户端的速率将显得不够平滑。

3.3 检查 CAR 是否在相应端口起作用

采用命令 show interface XX rate-limit 可以检查端口 XX 的 CAR 实际效果,实例如下:

```
fddi2/1/0
  input
    matches: access-group 101
      params: 80000000 bps, 72000 limit, 72000 extended limit
      conformed 0 packets, 0 bytes; action: set-prec-transmit 5
      exceeded 0 packets, 0 bytes; action: set-prec-transmit 0
      last packet: 4738036ms ago, current burst: 0 bytes
      last cleared 01:02:05 ago, conformed 0 bps, exceeded 0 bps
    matches: all traffic
      params: 50000000 bps, 64000 limit, 64000 extended limit
      conformed 0 packets, 0 bytes; action: set-prec-transmit 5
      exceeded 0 packets, 0 bytes; action: set-prec-transmit 0
      last packet: 4738036ms ago, current burst: 0 bytes
      last cleared 01:00:22 ago, conformed 0 bps, exceeded 0 bps
  output
    matches: all traffic
      params: 80000000 bps, 80000 limit, 80000 extended limit
      conformed 0 packets, 0 bytes; action: transmit
      exceeded 0 packets, 0 bytes; action: drop
      last packet: 4809528ms ago, current burst: 0 bytes
      last cleared 00:59:42 ago, conformed 0 bps, exceeded 0 bps
```

此命令用于检查配置 CAR 的实际效果,若发现没有 conform 的流量,则可能是 traffic matching 的规则设置有问题,或者是在 interface 上的 input output 设得不正确。

3.4 CAR 的其他用途

CAR 可以用来限制某种流量的速率之外,还可以用来抵挡某些类型的网络攻击。

DOS 网络攻击的一个特征是网络中会充斥着大量带有非法源地址的 ICMP 包,在路由器上对 ICMP 包通过配置 CAR 设置速率上限的方法来保护网络。例如:

interface xy

rate-limit output access-group 2020 3000000 80000 80000 conform-action transmit exceed-action drop

access-list 2020 permit icmp any any echo-reply

这样可以限制 ICMP 包的转发速率和大小,减少对网络和主机造成的破坏。

结束语 Cisco 路由器上应用非常广泛的路由器,通过 CAR 控制网络的流量,可以满足各种用户对网络流量和带宽的要求,这对提高网络带宽的利用率和提高网络性能有一定应用价值,当然,通过路由器也可实现网络控制和网络安全管理等方面的功能。

VPN 技术应用研究

杨永斌
(重庆工商大学计算机科学与信息工程学院　重庆400067)

摘　要　随着网络经济、电子商务、电子政务、远程教育等的迅猛发展，各单位对外联系业务及合作范围越来越广，传统的联网方式已难以适应现代业务发展的需求。VPN 技术可以让各单位利用 Internet 来建立自己安全的内部网，将其分散在各地的网络通讯通过现有的公网安全地连接起来。本文介绍了 VPN 的概念、技术、优势，并探讨了 VPN 在券商广域网备份系统中的应用。

关键词　虚拟专用网，隧道技术，身份验证，加密，广域网，备份

The Research of VPN Technique Application

YANG Yong-Bin
(College of Computer Science and Information engineer, Chongqing Technology and Business University, Chongqing 400067)

Abstract　With the rapid development of network economy, E-Business, E-Government, distance education, etc., and with the ever-enlarging scope of business and cooperation, it is difficult for the tradition way of linking network to adapt to the requirements of the developing modern business. VPN technique enables network users to establish their secure Intranets based on the Internet, linking securely together notwork in different places. This paper focuses on the VPN concept, technique and its advantages, and discusses about its application in backup system of WAN of security companies.

Keywords　Virtual Private Network (VPN), Tunnel technique, Identity validate, Encrypt, WAN, Backup

1　引言

随着网络经济、电子商务、电子政务、远程教育等的迅猛发展，各单位对外联系业务及合作范围越来越广。面对业务数据流量的不断增长，单位对网络的灵活性、安全性、经济性和可扩展性等方面提出了更高的要求，使得传统的基于固定地点的专线(DDN、ATM/帧中继)联网方式已难以适应现代业务发展的需求，尤其对于一些特殊应用更加力不从心，如：野外作业和远程作业的人员向办公室传输数据等情况。VPN 技术价格低廉、灵活、安全的联接方式，非常适合中小规模单位低成本扩展自身业务。

根据预测，国内分支机构间使用 VPN 将为用户节省的20%～80%的通讯费用，跨国公司使用 VPN 节省的国际通信费用比例则更高。随着 VPN 技术的不断发展和完善，用户中许多业务完全可以承载于 VPN 中，这都为 VPN 的广泛应用奠定了坚实的基础。

2　VPN 概述

虚拟专用网技术(Virtual Private Network，VPN)是利用开放性网络作为信息传输的媒体，通过加密、认证、封装以及

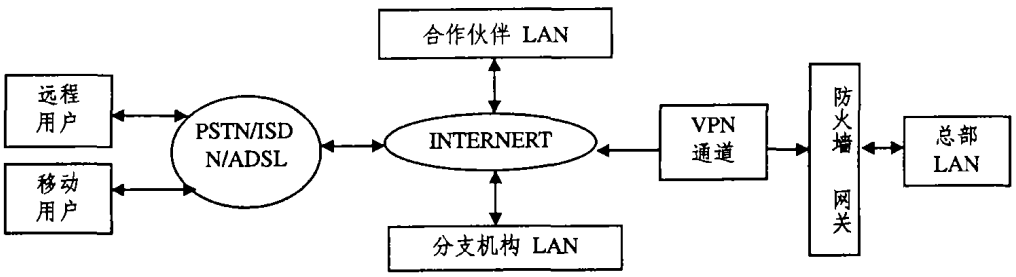

图1　典型的 VPN 系统组成

杨永斌　讲师，主要研究方向：计算机算法、计算机网络、数据库技术、网络教育。

参考文献

1　Ballew S M 著，夏昊，洪峰译. CISCO 路由管理[M]. 北京：中国电力出版社，2000
2　Helo G L, Hundley K 著，前导工作室译. CISCO 访问表配置指南[M]. 北京：机械工业出版社，2000
3　CISCO SYSTEMS 公司著，希望图书创作室译. 网络核心技术内幕—CISCO 网络安全解决方案(上、下)[M]. 北京：北京希望电子出版社，2000
4　CISCO SYSTEMS 公司著，希望图书创作室译. 网络核心技术内幕—网络协议解决方案(上、下)[M]. 北京：北京希望电子出版社，2000
5　张琳，李璇华著. 网络组建、原理与安全[M]. 北京：人民邮电出版社，2000
6　Mcqueny A 著，谈利群，胡爱民译. 组网用网：CISCO 网络设备互联解决方案[M]. 北京：电子工业出版社，2001