身 份 证 130425198708092057 ， 210181199209046813 ， 222302197312260017 ，
350128197311050034 ，410611197403020058
联通手机号 18575414999 ，13026844666
电信手机号 18919628498 ， 18919628499
移动手机号 18756500265 ，18555918746 15665541872
邮箱 zhangsan@163.com ，lisi@qq.com
银行卡 6216610200016587010 ， 6221882600114166800
财务报表
内部数据
内部资料
保密
秘密
机密
密码口令
超级用户
家庭地址
Chapter 27 CAR 流量管理
27.1 CAR 流量控制
27.1.1 令牌桶模型
令牌桶有 4 个关键参数，
1． 平均速率或者承诺信息速率，CIR，单位 Bit/s
2． 顺从突发量 Bc，瞬间可以超过令牌桶的流量。有时候也称作常规突发量
3． 扩展突发量 BE，
4． 时间间隔：Ti=Bc/CIR
流量控制有 CAR 提供，CAR 主要提供了 2 个功能，通过设定 IP 优先级来描述分组和限制速率
作为一种流量控制功能,CAR 并不将通信保存到缓冲区或使其平稳,当超过允许的突发流量时就会
丢弃分组.
rate-limit <input/ouput> access-group rate-limit # "CIR""conformed burst" "extended burst" conform-action "action desired"exceed-action "action desired"
流量限制分为 3 个过程, 如下图:
1. 流量匹配(Traffic Matching)
流量匹配通常可以定义很多匹配方式,
1. 匹配所有通信
2. 使用速率限制访问列表匹配某个 IP 优先级
3. 使用速率限制访问列表匹配某个 MAC 地址
4. 使用 IP 标准或扩展访问列表进行匹配
2. 流量检测
流量检测采用令牌桶模型, 标准的令牌桶结构如下
令牌桶按用户设定的速度向桶中放置令牌，并且用户可
以设置令牌桶的容量，当桶中令牌的量超出桶的容量的时候，
令牌的量不再增加；当报文被令牌桶处理的时候，如果令牌桶
中有足够的令牌可以用来发送报文，则报文可以通过可以被继

续发送下去，同时令牌桶中的令牌量按报文的长度做相应的减
少，当令牌桶中的令牌少到报文不能再发送时，报文被丢弃。
令牌桶是一个控制数据流量的很好的工具，当令牌桶中充满令
牌的时候，桶中所有的令牌代　表的报文都可以被发送，这样
可以允许数据的突发性传输，当令牌桶中没有令牌的时候报文
将不能被发送，只有等到桶中生成了新的令牌报文才可以发送，
这就可以限制报文的流量只　能是小于等于令牌生成的速度，
达到限制流量的目的。

令牌桶能保存的最大令牌数目等于 Bc.
标准令牌桶 Be = Bc　没有扩展突发功能 ,令牌不够用直接丢弃
扩展突发功能的令牌桶 Be > Bc,它允许流量暂借根多的令牌.然后采用随机丢弃的策
略, 缓慢的丢弃流量.
27.1.2　　流量控制操作
对于 ISP 来说对用户送入网络中的流量进行控制是十分必要的。对于企业网，对某些应用的流量
进行控制也是一个有力的控制网络状况的工具，网络管理者可以使用约定访问速率　CAR 来对流量进行
控制。CAR 利用令牌桶（Token Bucket, TB）进行流量控制。如下图：
上图所显示的是利用 CAR 进行流量控制的基本处理过程，首先根据预先设置的匹配规则来对报
文进行分类,如果是没有规定流量特性的报文就直接继续发送,并不需要经过令牌桶的处理;如果是
需要进行流量控制的报文，则会进入令牌桶中进行处理，如果令牌桶中有足　够的令牌可以用来发送报
文，则允许报文通过，报文可以被继续发送下去；如果令牌桶中的令牌不满足报文的发送条件则报文
被丢弃，这样就可以对某类报文的流量进行控制。
在实际应用中 CAR 不仅可以用来进行流量控制，还可以进行报文的标记（mark）或重新标记
（re-mark），具体来讲就是 CAR 可以设置 IP 报文的优先级或修改 IP 报文的优先级，达到　标记报文的
目的。例如当报文符合流量特性的时候可以设置报文的优先级为 5，当报文不符　合流量特性的时候可
以丢弃，也可以设置报文的优先级为 1 并继续进行发送，这样后续的处　理可以尽量保证不丢弃优先级
为 5 的报文。在网络不拥塞的情况下也发送优先级为 1 的报文。　　当网络拥塞时首先丢弃优先级为 1 的

报文。然后才丢弃优先级为 5 的报文。
配置实例：
一个 Internet 提供商使用 IP 由县级为客户提哦能够不同等级的奖赏服务,确保网络主干由县

处
理这些信息
1．使用 CAR 的优先级
interface Hssi 0/0/1
rate-limit access-group 1 input 45000000 22500 22500 conform-action
set-prec-transmit 5 exceed-action set-prec-transmit 5
rate-limit input 45000000 22500 22500 conform -action set-prec-transmit 4
exceed-action set-prec-transmit 4
access-group 1 permit 215.215.215.0 0.0.0.255
2．使用 PBR 的 IP 优先级
interface Hssi 0/0/1
ip policy route-map tasman
route-map tasman permit 10
match ip address 1
set ip precedence 5
route-map tasman permit 20
set ip precedence 4
access-group 1 permit 215.215.215.0 0.0.0.255
3． 使用 QPPB 的 IP 优先级 ,Cisco 的 CEF 快速转发支持对 IP 优先级的识别.
interface Hssi 0/0/1
ip address 217.217.217.1 255.255.255.252
bgp source ip-prec-map
router bgp 10
table-map tasman
neighbor 217.217.217.2 remote-as 2345
route-map tasman permit 10
match ip address 1
set ip precedence 5
route-map tasman permit 20
set ip precedence 4
access-group 1 permit 215.215.215.0 0.0.0.255
修改 QoS 组
1．使用 CAR
interface Hssi 0/0/1
rate-limit access-group 1 input 45000000 22500 22500 conform-action

set-qos-transmit 3 exceed-action drop
rate-limit input 45000000 22500 22500 conform -action set-qos-transmit 0 exceed-action drop
access-group 1 permit 215.215.215.0 0.0.0.255
2．使用 QPPB
interface Hssi 0/0/1
ip address 217.217.217.1 255.255.255.252
bgp source ip-qos-map

router bgp 10
table-map tasman
neighbor 217.217.217.2 remote-as 2345
route-map tasman permit 10
match ip address 1
set ip qos-group 3
route-map tasman permit 20
set ip qos-group 0
access-group 1 permit 215.215.215.0 0.0.0.255
CAR 可以为不同类别的报文设置不同的流量特性和标记特性，即首先对报文进行分类，然后不
同类别的报文有不同的流量特性和标记特性，此外 CAR 的策略还可以进行串联处理。例如可以对所有
的报文限制一个总的流量，然后在总的流量中再限制部分报文的流量符合某 个流量特性。
CAR 通常使用在网络边界路由器的接口上，用来限制进入或离开该网络的流量速率。每个接口可
以配置多个 CAR 策略，当数据包进入使用了多个策略的接口时，路由器将检查每个策略，直到数据包
和某个策略相匹配；如果没有找到匹配的策略,默认操作是转发该数据包。
CAR 的使用限制：
第一、 CAR 只能对 IP 流量限速。
第二、 CAR 不支持快速以太网信道(FastEtherChannel)
第三、 CAR 不支持隧道接口
第四、 CAR 不支持 ISDN PRI 接口。
27.1.3 CAR 配置过程
nimokaka(config-if)#rate-limit {input|output} {CIR Bc Be} conform-action {action}
exceed-action {action}
output|input 指输出或者输入的流量。
CIR 配置的是承诺接入速率，它的值的范围是在 8000-2000000000 bit 每秒。
Bc 是普通突发，它的值应在 1000-512000000byte，
Be 是最大突发，其值范围为 2000-1024000000bytes.
conform-action 后面规定的是遵从条件时候的动作，
exceed-action 后面规定的是超出时的动作，
{action}
continue 继续执行下一条 CAR 语句
drop 丢弃该数据包
set-prec-continue {precedence} 设置 IP 优先级并继续执行下一条 CAR 语句
set-prec-trasnmit {precedence} 设置 IP 优先级并转发该数据包
set-dscp-continue {dscp} 设置 IP DSCP 值并继续执行下一条 CAR 语句
set-dscp-trasnmit {dscp} 设置 IP DSCP 值并转发该数据包
set-qos-continue {group ID} 设置 QoS 组 ID 并继续执行下一条 CAR 语句
set-qos-transmit {group ID} 设置 QoS 组 ID 并发送该数据包

transmit 转发该数据包
基本上就是这些，但是我们发现好像这样做是管理整个接口的流量，也可以对某一个流量进行 CAR 管理。或者针对 IP 优先级或者根据 DSCP 进行管理。
针对于 DSCP 值进行 CAR
nimokaka(config-if)#rate-limit {input|output} [dscp dscp] {CIRBc Be}
conform-action{action} exceed-action {action}
针对于 ACL 进行 CAR
nimokaka(config-if)#rate-limit {input|output}access-group {ACL}
{CIRBc Be}conform-action {action} exceed-action {action}
针对于限速 ACL 进行 CAR
nimokaka(config-if)#rate-limit {input|output} access-group rate-limit
{ACL} {CIR Bc Be} conform-action {action} exceed-action {action}
限速 ACL 是一种特殊的 ACL，其实也没啥特殊的，就是一个调用关系
nimokaka(config)#access-list rate-limit {ACL}
{precedence|mac-address}
ACL 是限速 ACL 的号码，可以匹配优先级，也可以匹配源 mac 地址
27.1.4 CAR 配置实例
基于接口的流量控制
interface Hssi0/0/0
rate-limit input 15000000 2812500 2812500 conform-action transmit exceed-action drop
ip address 200.200.14.250 255.255.255.252
rate-limit output 15000000 2812500 2812500 conform-action transmit exceed-action drop
hssi 高速串口是 45M 的带宽， 但是 ISP 的接入承诺信息速率为 15M，
并且限定普通突发大小为 2812500，最大突发大小也是 2812500
基于 DSCP 的流量控制
interface Serial1
ip address 10.0.0.1 255.255.255.252
rate-limit output dscp 1 20000000 24000 32000 conform-action transmit exceed-action
drop
基于 ACL 的流量控制
1. 所有的 www 流量都得发出，而且 web 中遵从第一个速率策略的流量设置 ip 优先级为 5,不遵从的就把

ip precedence 设为 0(尽力而为的传输)。
2. ftp 流量遵从第二个速率策略的 ip precedence 设置为 5,如果 ftp 超出速率策略就扔包。
3. 其他剩余流量限制到 8m，普通突发大小为 16000byte,最大突发大小为 24000byte；遵从策略的流
量设 ip precedence 为 5,超出的流量扔包。
interface hssi0/0/0
rate-limit out put accees-group 101 200000000 24000 32000 conform-action set
prec-transmit 5 exceed-action set-prec-transmit 0
rate-limit output access-group 102 10000000 24000 32000 conform-action set-prec-tranmit

5
exceed-action drop
rate-limit output 8000000 16000 24000 conform-action set-prec-transmit 5
exceed-action drop
ip address 10.1.0.9 255.255.255.0
!
access-li 101 per tcp any any eq www
access-li 102 per tcp any any eq ftp
基于 IP 地址前缀的流量控制
interface Serial1
ip address 10.0.0.1 255.255.255.252
rate-limit output access-group 1 20000000 24000 32000 conform-action transmit
exceed-action drop
!
access-list 1 permit 192.168.0.0 0.0.0.255
基于 IP 优先级匹配的流量控制
interface Serial1
ip address 10.0.0.1 255.255.255.252
rate-limit output access-group rate-limit 1 20000000 24000 32000 conform-action transmit
exceed-action drop
!
access-list rate-limit 1 mask 07
对于 Mask 的解释如下, 优先级为 7 是 10000000 6 是 0100000 …
Mask 是一个 16 进制数, 07 代表 00000111,表示匹配优先级 0,1,2
匹配源 MAC 地址
如图所示,需要将 ISP X 的流量限制到 30Mbps,ISPY 的流量限制为 40Mbps

interface Fddi1/0/0
ip address 162.111.10.1 255.255.255.192
rate-limit input access-group rate-limit 110 30000000 15000 15000 conform-action transmit
exceed-action drop
rate-limit input access-group rate-limit 120 40000000 40000 40000 conform-action
continue exceed-action drop
rate-limit input access-group 100 4000000 40000 40000
conform-action drop exceed-action drop
access-list rate-limit 110 0000.0c10.7819
access-list rate-limit 120 0000.0c89.6900
access-list 100 permit ip any any
防止 DOS 攻击
interface Hssi1/0
rate-limit input access-group 100 256000 8000 8000 conform-action
transmit exceed-action drop
access-list 100 permit icmp any any

Show command
1、查看限速 ACL：　　nimokaka#show access-lists rate-limit [ACL]
2、查看接口的限速信息：　　nimokaka#show interfaces [interface] rate-limit
#show interface hssi1/0 rate
Hssi1/0/0
Input
matches: all traffic
params: 30000000 bps, 15000 limit, 15000 extended limit
conformed 0 packets, 0 bytes; action: continue
exceeded 0 packets, 0 bytes; action: drop
last packet: 338617304ms ago, current burst: 0 bytes
last cleared 00:11:11 ago, conformed 0 bps, exceeded 0 bps
matches: access-group 101
params: 15000000 bps, 10000 limit, 10000 extended limit
conformed 0 packets, 0 bytes; action: set-prec-transmit 4
exceeded 0 packets, 0 bytes; action: set-prec-transmit 0
last packet: 338617201ms ago, current burst: 0 bytes
last cleared 00:11:11 ago, conformed 0 bps, exceeded 0 bps
matches: all traffic
params: 15000000 bps, 10000 limit, 10000 extended limit
conformed 0 packets, 0 bytes; action: set-prec-transmit 4
exceeded 0 packets, 0 bytes; action: set-prec-transmit 4
last packet: 338617304ms ago, current burst: 0 bytes
last cleared 00:03:30 ago, conformed 0 bps, exceeded 0 bps

27.1.5　基于 Policy-Map 配置
如上操作是针对接口设置的 CAR，CAR 同时也可以作用在 policy-map 上
nimokaka(config-pmap-c)#police {CIR Bc Be} conform-action {action}exceed-action {action}[violate-action {action}]
把 rate-limit 改成了 police，后面增加了一个 violate-action，违规操作，也就是超过了 Be 流量之后的操作 Action 的操作命令
continue　　继续执行下一条 CAR 语句
drop　　丢弃该数据包
set-prec-continue {precedence}　设置 IP 优先级并继续执行下一条 CAR 语句
set-prec-trasnmit {precedence}　　设置 IP 优先级并转发该数据包
set-dscp-continue {dscp}　　设置 IP DSCP 值并继续执行下一条 CAR 语句
set-dscp-trasnmit {dscp}　　设置 IP DSCP 值并转发该数据包
set-qos-continue {group ID}　　设置 QoS 组 ID 并继续执行下一条 CAR 语句
set-qos-transmit {group ID}　　设置 QoS 组 ID 并发送该数据包
transmit　　转发该数据包
show command
1.查看 policy map:　　nimokaka#show policy-map [policy-name]
2.查看接口的 policy map 信息:　　nimokaka#show policy-map interface

27.1.6 基于 Policy-Map 配置实例

限制来自 192.168.0.0/24 的进站数据包的平均速率为 8000bps，突发流量(Bc)为 2000 字节，额外突
发流量(Be)为 4000 字节。对突发流量和额外突发流量分别采取转发和设置 QoS 组 ID 为 25 的策略;
对违反突发流量和额外突发流量的数据流量采取丢弃的策略:

```
!
class-map match-all nimokaka match access-group 1
!
policy-map kiss class nimokaka
police 8000 2000 4000 conform-action transmit exceed-action set-qos-transmit 25
violate-action drop
!
interface Serial1
ip address 172.16.0.1 255.255.255.252
service-policy input kiss
!
access-list 1 permit 192.168.0.0 0.0.0.255
```