

H3C WA 系列用户流量限速 CAR 功能典型配置举例

关键词：CAR

摘要：IP 网络应用日益繁多的今天，宝贵有限的网络带宽资源越来越成为开展众多业务应用的瓶颈；而提高网络带宽代价昂贵，这就要求在现有基础上更有效的利用这些网络资源。而 QoS 可以根据不同的业务的不同要求，通过为不同业务提供区分的 QoS 服务，从而使有限的网络资源得到更好的利用，满足客户对不同业务的不同需求。本文介绍了如何使用 CAR 流量监管技术，对用户访问网络时所占用的带宽进行流量监管。

缩略语：

缩略语	英文全名	中文解释
QoS	Quality of Service	服务质量
CAR	Committed Access Rate	承诺访问速率

目 录

1 特性简介	1
2 应用场合	1
3 注意事项	1
4 配置举例	2
4.1 组网需求	2
4.2 配置思路	3
4.3 使用版本	3
4.4 配置步骤	4
4.4.1 FAT AP的配置	4
4.4.2 L2 交换机的配置	7
4.4.3 验证结果	7
5 相关资料	9
5.1 相关协议和标准	9
5.2 其它相关资料	9

1 特性简介

随着计算机网络的高速发展，越来越多的网络接入 Internet。Internet 无论从规模、覆盖范围和用户数量上都拓展得非常快。越来越多的用户使用 Internet 作为数据传输的平台，开展各种应用。

除了传统的 WWW、e-mail、FTP 应用外，用户还尝试在 Internet 上拓展新业务，比如远程教学、远程医疗、可视电话、电视会议、视频点播等。企业用户也希望通过 VPN 技术，将分布在各地的分支机构连接起来，开展一些事务性应用：比如访问公司的数据库或通过 Telnet 管理远程设备。

这些新业务有一个共同特点，即对带宽、延迟、抖动等传输性能有着特殊的需求。比如电视会议、视频点播需要高带宽、低延迟和低抖动的保证。事务处理、Telnet 等关键任务虽然不一定要求高带宽，但非常注重低延迟，在拥塞发生时要求优先获得处理。

新业务的不断涌现对 IP 网络的服务能力提出了更高的要求，用户已不再满足于能够简单地将报文送达目的地，而是还希望在转发过程中得到更好的服务，诸如支持为用户提供专用带宽、减少报文的丢失率、管理和避免网络拥塞、调控网络的流量、设置报文的优先级。所有这些，都要求网络应当具备更为完善的服务能力。

增加网络带宽是解决资源不足的一个直接途径，然而它并不能解决所有导致网络拥塞的问题。

解决网络拥塞问题的一个更有效的办法是在网络中增加流量控制和资源分配的功能，为有不同服务需求的业务提供有区别的服务，正确地分配和使用资源。在进行资源分配和流量控制的过程中，尽可能地控制好那些可能引发网络拥塞的直接或间接因素，减少拥塞发生的概率；在拥塞发生时，依据业务的性质及其需求特性权衡资源的分配，将拥塞对 QoS 的影响减到最小。

CAR (Committed Access Rate) 作为一种常用的 QoS 流量监管技术，它可以对进入设备的特定流量的规格进行监管。当流量超出规格时，可以采取限制或惩罚措施，以保护运营商的商业利益和网络资源不受损害。

2 应用场合

为了有效地利用有限的网络资源，需要对用户访问网络时所占用的带宽进行相应的限制，从而保证每个用户的利益。

CAR 适用于接入网络，即在用户接入网络时，就对用户可以占用的网络带宽进行监管。

3 注意事项

在无线产品的配置中，CAR 通过 QoS 的流行为来实现的，下面首先介绍一下 QoS 策略。

QoS 策略包含了三个要素：类、流行为、策略。用户可以通过 QoS 策略将指定的类和流行为绑定起来，方便地进行 QoS 配置。

1. 流分类

流分类是用来识别流的。

流分类的要素包括：流分类的名称和流分类的规则。

用户可以通过命令定义一系列的规则，来对报文进行分类。同时用户可以通过命令指定规则之间的关系：**and** 或者 **or**。

- **and**: 报文只有匹配了所有的规则，设备才认为报文属于这个类。
- **or**: 报文只要匹配了类中的一个规则，设备就认为报文属于这个类。

2. 流行为

流行为用来定义针对报文所做的 **QoS** 动作。

流行为的要素包括：流行为的名称和流行为中定义的动作。

用户可以通过命令在一个流行为中定义多个动作。

3. 策略

策略用来将指定的类和指定的流行为绑定起来。

策略的要素包括：策略名称、绑定在一起的类和流行为的名称。

用户可以通过命令在一个策略中定义多个类与流行为的绑定关系。

下面将要介绍的用户流量限速 **CAR** 功能就是通过上述 **QoS** 策略实现的。

在配置过程中，需要注意以下几点：

- 配置正确的流分类策略，以保证所要监管的流量能进入相应的流行为
- 配置正确的流行为，这里主要是 **CAR** 规则
- 在 **QoS** 策略中匹配流分类和流行为
- 在相应的接口应用 **QoS** 策略

4 配置举例

4.1 组网需求

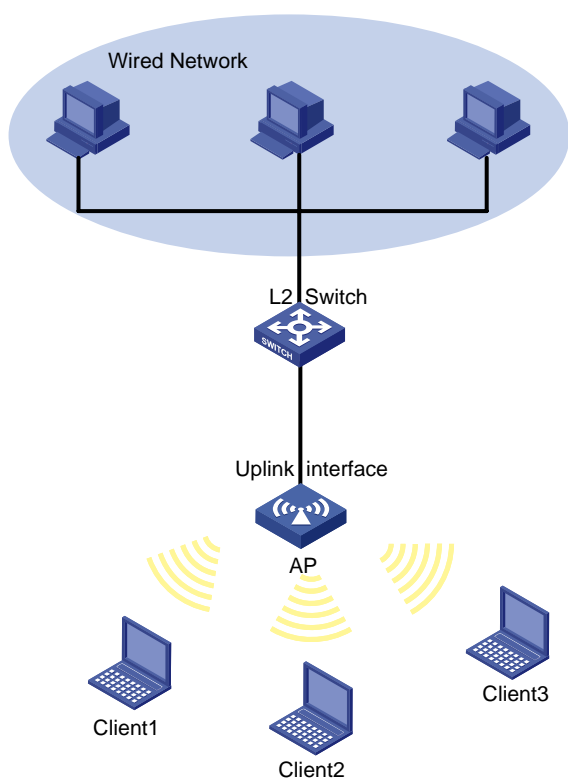


说明

本配置举例中的 AP 使用的是 **WA2220X-AG** 无线局域网接入点。

在下面的配置举例中，通过在 **FAT AP** 的 **WLAN-BSS 1** 口的出方向(**outbound**)和入方向(**inbound**)同时配置 **QoS** 策略 (**CAR**)，限制无线用户可以访问网络的带宽。

图4-1 用户流量限速 CAR 组网图



4.2 配置思路

用户流量限速 CAR 功能的配置目前是通过 MQC 实现的，即先配置用于流分类的 ACL，再配置流分类和流行为及 QoS 策略，最后在无线接口上应用 QoS 策略。

4.3 使用版本

```
<AP> display version
H3C Comware Platform Software
Comware Software, Version 5.20, Beta 1103P01
Copyright (c) 2004-2008 Hangzhou H3C Tech. Co., Ltd. All rights reserved.
WA2220X-AG uptime is 0 week, 0 day, 0 hour, 5 minutes
CPU type: AMCC PowerPC 266MHz
64M bytes SDRAM Memory
8M bytes Flash Memory
Pcb          Version:  Ver.B
Basic BootROM Version:  1.07
Extend BootROM Version: 1.07
[SLOT 1]CON          (Hardware)Ver.B, (Driver)1.0
[SLOT 1]ETH1/0/1     (Hardware)Ver.B, (Driver)1.0
[SLOT 1]ETH1/0/2     (Hardware)Ver.B, (Driver)1.0
[SLOT 1]RADIO1/0/1   (Hardware)Ver.B, (Driver)1.0
[SLOT 1]RADIO1/0/2   (Hardware)Ver.A, (Driver)1.0
```

4.4 配置步骤



说明

以下配置均是在实验室环境下进行的配置和验证，配置前设备的所有参数均采用出厂时的缺省配置。如果您已经对设备进行了配置，为了保证配置效果，请确认现有配置和以下配置不冲突。

4.4.1 FAT AP 的配置

1. 配置信息

```
<AP> display current-configuration
#
version 5.20, Beta 1103P01
#
sysname AP
#
domain default enable system
#
telnet server enable
#
acl number 4001
rule 0 permit source-mac 0012-f0cc-3a2f ffff-ffff-ffff
rule 5 permit dest-mac 0012-f0cc-3a2f ffff-ffff-ffff
rule 10 deny
#
vlan 1
#
domain system
access-limit disable
state active
idle-cut disable
self-service-url disable
#
traffic classifier client1 operator and
if-match acl 4001
#
traffic behavior client1
car cir 1000 cbs 62500 ebs 0 green pass red discard
#
qos policy clientpolicy
classifier client1 behavior client1
#
local-user admin
password simple h3capadmin
service-type telnet
level 3
#
```

```

wlan rrm
 11a mandatory-rate 6 12 24
 11a supported-rate 9 18 36 48 54
 11b mandatory-rate 1 2
 11b supported-rate 5.5 11
 11g mandatory-rate 1 2 5.5 11
 11g supported-rate 6 9 12 18 24 36 48 54
#
wlan service-template 1 clear
  ssid H3C
  authentication-method open-system
  service-template enable
#
interface NULL0
#
interface Vlan-interface1
  ip address 192.168.0.50 255.255.255.0
#
interface Ethernet1/0/1
#
interface Ethernet1/0/2
#
interface WLAN-BSS1
  qos apply policy clientpolicy inbound
  qos apply policy clientpolicy outbound
#
interface WLAN-BSS2
#
interface WLAN-Radiol/0/1
  service-template 1 interface wlan-bss 2
#
interface WLAN-Radiol/0/2
  channel 1
  service-template 1 interface wlan-bss 1
#
user-interface con 0
user-interface vty 0 4
  authentication-mode scheme
#
return
<AP>

```

2. 配置步骤

(1) 设备采用缺省配置启动。

(2) 配置用于流分类的 ACL。

```
<AP>system-view
```

```
System View: return to User View with Ctrl+Z.
```

创建一个序号为 4001 的二层 ACL。

```
[AP]acl number 4001
```

设置一条规则允许源 MAC 地址为 0012-f0cc-3a2f 的报文通过。

```
[AP-acl-ethernetframe-4001]rule permit source-mac 0012-f0cc-3a2f ffff-ffff-ffff
```

设置一条规则允许目的 MAC 地址为 0012-f0cc-3a2f 的报文通过。

```
[AP-acl-ethernetframe-4001]rule permit dest-mac 0012-f0cc-3a2f ffff-ffff-ffff
```

设置一条规则禁止所有报文通过。

```
[AP-acl-ethernetframe-4001]rule deny
```

```
[AP-acl-ethernetframe-4001]quit
```

显示 ACL 4001 中配置的规则。

```
[AP]display acl 4001
```

```
Ethernet frame ACL 4001, named -none-, 3 rules,
```

```
ACL's step is 5
```

```
rule 0 permit source-mac 0012-f0cc-3a2f ffff-ffff-ffff
```

```
rule 5 permit dest-mac 0012-f0cc-3a2f ffff-ffff-ffff
```

```
rule 10 deny
```

(3) 配置流分类。

定义一个名为 client1 的类。

```
[AP]traffic classifier client1
```

定义类匹配 ACL4001。

```
[AP-classifier-client1]if-match acl 4001
```

```
[AP-classifier-client1]quit
```

(4) 配置流行为。

定义一个名为 client1 的流行为。

```
[AP]traffic behavior client1
```

为流行为配置流量监管，承诺信息速率为 1000kbps。

```
[AP-behavior-client1]car cir 1000
```

```
[AP-behavior-client1]quit
```

```
[AP]
```

(5) 配置 QoS 策略。

定义一个策略 clientpolicy 并进入策略视图。

```
[AP]qos policy clientpolicy
```

在策略 clientpolicy 中为类 client1 指定采用流行为 client1。

```
[AP-qospolicy-clientpolicy]classifier client1 behavior client1
```

```
[AP-qospolicy-clientpolicy]quit
```

(6) 在 WLAN-BSS 1 口上应用 QoS 策略，这里是在 WLAN-BSS 1 口的入方向和出方向都应用了相同的 QoS 策略。

```
[AP]interface WLAN-BSS 1
```

```
[AP-WLAN-BSS1]qos apply policy clientpolicy inbound
```

```
[AP-WLAN-BSS1]qos apply policy clientpolicy outbound
```

```
[AP-WLAN-BSS1]quit
```


(7) 查看 WLAN-BSS 1 口的 QoS 策略。

```
[AP]display qos policy interface WLAN-BSS 1
  Interface: WLAN-BSS1
  Direction: Inbound
  Policy: clientpolicy
  Classifier: client1
    Matched : 0(Packets) 0(Bytes)
    Operator: AND
    Rule(s) : If-match acl 4001
    Behavior: client1
    Committed Access Rate:
      CIR 1000 (kbps), CBS 62500 (byte), EBS 0 (byte)
      Green Action: pass
      Red Action: discard
      Green : 0(Packets) 0(Bytes)
      Red   : 0(Packets) 0(Bytes)

  Direction: Outbound
  Policy: clientpolicy
  Classifier: client1
    Matched : 0(Packets) 0(Bytes)
    Operator: AND
    Rule(s) : If-match acl 4001
    Behavior: client1
    Committed Access Rate:
      CIR 1000 (kbps), CBS 62500 (byte), EBS 0 (byte)
      Green Action: pass
      Red Action: discard
      Green : 0(Packets) 0(Bytes)
      Red   : 0(Packets) 0(Bytes)

[AP]
```

4.4.2 L2 交换机的配置

L2 交换机采用缺省配置，无线用户上线后，和有线网络都在同一个 VLAN 中。

配置文件略。

4.4.3 验证结果

在无线网络中，QoS 策略需要在无线用户上线之前配置，无线用户上线后相应的 QoS 策略才会生效。在完成上述配置后，可通过以下方式验证上述配置：

(1) 通过命令 `display qos policy interface WLAN-BSS 1` 查看接口的 QoS 统计信息

因为无线用户在上线后就有 ARP 或其它报文收发，从下面可以看到，已经有报文被 ACL 匹配。

```
<AP>display qos policy interface WLAN-BSS 1
  Interface: WLAN-BSS1
  Direction: Inbound
  Policy: clientpolicy
  Classifier: client1
```

```
Matched : 19(Packets) 1732(Bytes)
Operator: AND
Rule(s) : If-match acl 4001
Behavior: client1
Committed Access Rate:
  CIR 1000 (kbps), CBS 62500 (byte), EBS 0 (byte)
  Green Action: pass
  Red Action: discard
  Green : 19(Packets) 1732(Bytes)
  Red   : 0(Packets) 0(Bytes)
```

Direction: Outbound

Policy: clientpolicy

Classifier: client1

```
Matched : 29(Packets) 2576(Bytes)
Operator: AND
Rule(s) : If-match acl 4001
Behavior: client1
Committed Access Rate:
  CIR 1000 (kbps), CBS 62500 (byte), EBS 0 (byte)
  Green Action: pass
  Red Action: discard
  Green : 29(Packets) 2576(Bytes)
  Red   : 0(Packets) 0(Bytes)
```

<AP>

(2) 在打流量 1 分钟后，通过命令可以看到，有更多的报文被匹配上。

<AP>display qos policy interface WLAN-BSS 1

Interface: WLAN-BSS1

Direction: Inbound

Policy: clientpolicy

Classifier: client1

```
Matched : 2790(Packets) 174698(Bytes)
Operator: AND
Rule(s) : If-match acl 4001
Behavior: client1
Committed Access Rate:
  CIR 1000 (kbps), CBS 62500 (byte), EBS 0 (byte)
  Green Action: pass
  Red Action: discard
  Green : 2790(Packets) 174698(Bytes)
  Red   : 0(Packets) 0(Bytes)
```

Direction: Outbound

Policy: clientpolicy

Classifier: client1

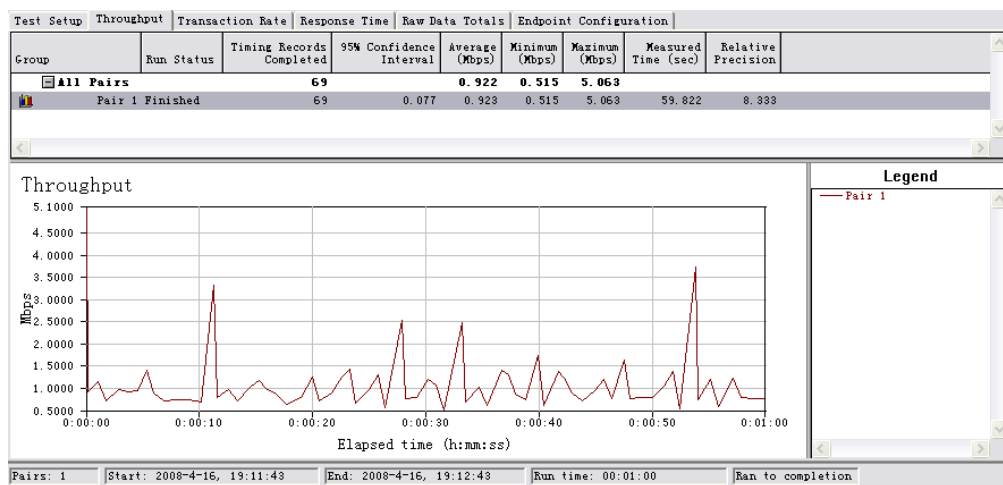
```
Matched : 5705(Packets) 8461266(Bytes)
Operator: AND
Rule(s) : If-match acl 4001
Behavior: client1
Committed Access Rate:
```

```

CIR 1000 (kbps), CBS 62500 (byte), EBS 0 (byte)
Green Action: pass
Red Action: discard
Green : 5016(Packets) 7428973(Bytes)
Red   : 689(Packets) 1032293(Bytes)
<AP>display acl 4001
Ethernet frame ACL 4001, named -none-, 3 rules,
ACL's step is 5
rule 0 permit source-mac 0012-f0cc-3a2f ffff-ffff-ffff(2881 times matched)
rule 5 permit dest-mac 0012-f0cc-3a2f ffff-ffff-ffff(5624 times matched)
rule 10 deny(76 times matched)
<AP>

```

- (3) 如果是用 IxChariot 打流量，通过 IxChariot 的流量图，就可以更加明确地看出无线用户的流量被限制在 1M 左右。



5 相关资料

5.1 相关协议和标准

TCP/IP Routing, 第二卷; Routing TCP/IP, Volume II

5.2 其它相关资料

《H3C WA 系列无线局域网接入点设备 用户手册》“QoS 分册”。

《H3C WA 系列无线局域网接入点设备 用户手册》“安全分册”中的“ACL”。