H3C WA 系列无线接入点

QoS 配置指导

新华三技术有限公司
http://www.h3c.com

资料版本：6W100-20180921
产品版本：R2414

前 言

本配置指导主要介绍 H3C WA 系列无线接入点 WLAN QoS 配置以及 QoS 配置等内容。

前言部分包含如下内容：

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 命令行格式约定

格　式	意　义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从多个选项中仅选取一个。
[x | y | ...]	表示从多个选项中选取一个或者不选。
{ x | y | ... } *	表示从多个选项中至少选取一个。
[x | y | ...] *	表示从多个选项中选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1～n次。
#	由“#”号开始的行表示为注释行。

2. 图形界面格式约定

格　式	意　义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[ ]	带方括号“[ ]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。
	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 示例约定

由于设备型号不同、配置不同、版本升级等原因，可能造成本手册中的内容与用户使用的设备显示信息不一致。实际使用中请以设备显示的内容为准。

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：info@h3c.com

感谢您的反馈，让我们做得更好！

目 录

1 WLAN QoS

1.1 WLAN QoS简介

在 802.11 网络中，为了给不同的应用提供不同质量的接入服务，IEEE 802.11 工作组制定了无线网络的 QoS 技术 802.11e，基于此协议实现丰富的 QoS 功能。目前，设备支持的 WLAN QoS 功能包括 WMM、SVP、智能带宽保障功能和客户端限速功能。

1.1.1 WMM

1. WMM协议

Wi-Fi 组织为了满足不同 WLAN 厂商对 QoS 的需求，定义了 WMM（Wi-Fi Multimedia，Wi-Fi 多媒体）协议。WMM 协议用于保证优先发送高优先级的报文，从而保证语音、视频等应用在无线网络中有更好的服务质量。

在 802.11 协议中 DCF（Distributed Coordination Function，分布式协调功能）规定了 AP 和客户端使用 CSMA/CA（Carrier Sense Multiple Access with Collision Avoidance，载波监听/冲突避免）接入方式。在占用信道发送数据前，AP 或客户端会监听信道。当信道空闲时间大于或等于规定的空闲等待时间，AP 或客户端在竞争窗口范围内随机选择退避时间进行退避。最先结束退避的设备竞争到信道。在 802.11 协议中，由于所有设备的空闲等待时间、竞争窗口都相同，所以整个网络中设备的信道竞争机会相同。

WMM 协议通过对 802.11 协议进行改进，改变了整个网络完全公平的竞争方式，将 BSS（Basic Service Set，基本服务集）内的数据报文分为 4 个 AC（Access Category，接入类），高优先级 AC 中的报文占用信道的机会大于低优先级 AC 中的报文，从而使不同的 AC 获得不同级别的服务。

2. 基本概念

(1) EDCA

EDCA（Enhanced Distributed Channel Access，增强的分布式信道访问）是 WMM 定义的一套信道竞争机制，有利于高优先级的报文享有优先发送的权利和更多的带宽。

(2) AC

AC（Access Category，接入类），WMM 定义了四种接入类型，相应的有各自的优先级队列，这些队列按优先级从高到低的顺序分为 AC-VO（语音队列）、AC-VI（视频队列）、AC-BE（尽力而为队列）、AC-BK（背景队列）。越高优先级队列中的报文，抢占信道的能力越强。

(3) U-APSD

U-APSD（Unscheduled Automatic Power-save Delivery，非调度自动节能发送）是 WMM 定义的一种新的节能处理方式，可以进一步提升客户端的节能能力。

3. EDCA参数

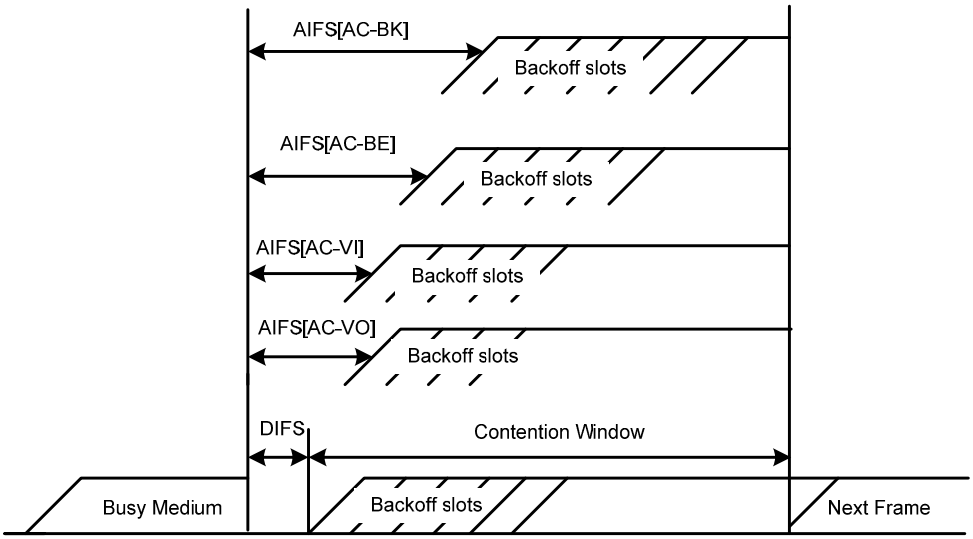
WMM 协议对每个 AC 定义了一套信道竞争 EDCA 参数，EDCA 参数的含义如下所示。

- AIFSN（Arbitration Inter Frame Spacing Number，仲裁帧间隙数）：在 802.11 协议中，空闲等待时长（DIFS）为固定值，而WMM针对不同AC配置退避前需要等待的时隙，AIFSN数

值越小，用户的空闲等待时间越短，即高优先级AC具有较高的信道竞争机会。AIFSN为 图 1-1 中AIFS时间段。

- ECWmin（Exponent form of CWmin，最小竞争窗口指数形式）和ECWmax（Exponent form of CWmax，最大竞争窗口指数形式）：决定了平均退避时间值。这两个数值越大，用户的平均退避时间越长。通过这两个值计算 图 1-1 中Backoff slots时间段。
- TXOP Limit（Transmission Opportunity Limit，传输机会限制）：用户每次竞争成功后，可占用信道的最大时长。这个数值越大，用户一次能占用信道的时长越大。如果是 0，则每次占用信道后只能发送一个报文。

图1-1 WMM 为每个 AC 赋予不同的信道竞争参数



4. U-APSD节能模式

U-APSD 是对传统节能模式的改进。在这种机制下，客户端不再定期监听 Beacon 帧，而是由客户端决定何时到 AP 上获取缓存报文。对于客户端的一次请求，AP 可以发送多个缓存报文给客户端，该机制显著改善了客户端的节能效果。

开启 WMM 功能后，就自动开启 U-APSD 节能模式。

5. ACK策略

ACK 策略有两种：Normal ACK 和 No ACK。

- Normal ACK 策略：对于每个发送的单播报文，接收者在成功接收到报文后，都要回复 ACK 进行确认。
- No ACK（No Acknowledgment）策略：在无线报文交互过程中，不使用 ACK 报文进行接收确认。在通信质量较好、干扰较小的情况下，No ACK 策略能有效提高报文传输效率。但是，在通信质量较差的情况下，如果使用 No ACK 策略，则会造成丢包率增大的问题。需要注意的是，对于 802.11n 客户端发送的 A-MPDU 报文，配置的 No ACK 不起作用。

1.1.2 智能带宽保障功能

在实际应用中，网络中的流量不会一直处于某个稳定的状态。当某个 BSS 的流量非常大时，会挤占其它 BSS 的可用带宽。如果直接对单个 BSS 的报文进行限速，在总体流量较小时，又会导致闲置带宽被浪费。

智能带宽保障功能提供了更灵活的流量控制机制，当网络未拥塞时，所有 BSS 的报文都可以通过；在网络发生拥塞时，每个 BSS 都可以获取最低的保障带宽。通过这种方式，既确保了网络带宽的充分利用，又兼顾了不同无线服务之间带宽占用的公平原则。例如，配置 SSID 1、SSID 2 及 SSID 3 的保障带宽占总带宽的比例分别为 25%、25%及 50%。当网络空闲时，SSID 1 可以超过保障带宽，任意占用网络剩余带宽；当网络繁忙、没有剩余带宽时，SSID 1 至少可以占有自己的保障带宽部分（25%）。


说明

智能带宽保障功能只能对由 AP 发送至客户端的流量进行控制。

1.1.3 客户端限速功能

每个 AP 提供的带宽由接入的所有客户端共享，如果部分客户端占用过多带宽，将导致其它客户端受到影响。通过配置客户端限速功能，可以限制单个客户端对带宽的过多消耗，保证所有接入客户端均能正常使用网络业务。

客户端限速功能有两种模式：

- 动态模式：配置所有客户端使用的速率总值，每个客户端的限制速率是速率总值/客户端数量。例如，配置所有客户端可用速率的总和为 10Mbps，当有 5 个用户上线时，每个客户端的可用带宽限制为 2Mbps。
- 静态模式：为所有客户端配置相同的限速速率，该配置对所有客户端生效。当接入客户端增加至一定数量时，如果所有接入客户端限制速率的总和超出 AP 可提供的有效带宽，那么每个客户端将不能保证获得配置的带宽。

1.1.4 协议规范

- 802.11e-2005, Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements, IEEE Computer Society, 2005
- Wi-Fi, WMM Specification version 1.1, Wi-Fi Alliance, 2005

1.2 配置WMM

1.2.1 WMM配置任务简介

WMM 配置任务如下：

(1) 开启WMM功能

(2) （可选）配置射频的EDCA工作参数

(3) （可选）配置射频和客户端的AC-BE或AC-BK协商参数

(4) （可选）配置射频和客户端的AC-VO或AC-VI协商参数

(5) （可选）配置信任的报文优先级类型和端口优先级

1.2.2 开启WMM功能

1. 功能简介

协议要求 802.11n、802.11ac 的客户端必须支持 WMM，所以当 Radio 工作在 802.11an、802.11gn 或 802.11ac 的情况下，WMM 功能必须开启，否则可能会导致关联后的 802.11n 或 802.11ac 的客户端无法通信。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 Radio 接口视图。

interface wlan-radio *interface-number*

(3) 开启 WMM 功能。

wmm enable

缺省情况下，WMM 功能处于开启状态。

1.2.3 配置射频的EDCA工作参数

(1) 进入系统视图。

system-view

(2) 进入 Radio 接口视图。

interface wlan-radio *interface-number*

(3) 配置 Radio 的工作参数。

edca radio { **ac-be** | **ac-bk** | **ac-vi** | **ac-vo** } { **ack-policy** { **noack** | **normalack** } | **aifsn** *aifsn-value* | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* } *

缺省情况下：如 表 1-1 所示。

表1-1 射频的 EDCA 工作参数缺省值

AC	AIFSN	ECWmin	ECWmax	TXOP Limit
AC-BK	7	4	10	0
AC-BE	3	4	6	0
AC-VI	1	3	4	94
AC-VO	1	2	3	47

1.2.4 配置射频和客户端的AC-BE或AC-BK协商参数

(1) 进入系统视图。

system-view

(2) 进入 Radio 接口视图。

interface wlan-radio *interface-number*

(3) 配置 Radio 和客户端的 AC-BE 或 AC-BK 协商参数。

edca client { **ac-be** | **ac-bk** } { **aifsn** *aifsn-value* | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax -value* | **txoplimit** *txoplimit -value* } *

缺省情况下，如 表 1-2 所示。

表1-2 射频和客户端的协商参数的缺省值

AC	AIFSN	ECWmin	ECWmax	TXOP Limit
AC-BK	7	4	10	0
AC-BE	3	4	10	0

1.2.5 配置射频和客户端的AC-VO或AC-VI协商参数

(1) 进入系统视图。

system-view

(2) 进入 Radio 接口视图。

interface wlan-radio *interface-number*

(3) 配置 Radio 和客户端的 AC-VO 或 AC-VI 协商参数。

edca client { **ac-vi** | **ac-vo** } { **aifsn** *aifsn-value* | **cac** { **disable** | **enable** } | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* } *

缺省情况下，如 表 1-3 所示。

表1-3 射频和客户端的协商参数的缺省值

AC	AIFSN	ECWmin	ECWmax	TXOP Limit
AC-VI	2	3	4	94
AC-VO	2	2	3	47

1.2.6 配置信任的报文优先级类型和端口优先级

1. 功能简介

没有配置信任的报文优先级类型时，设备信任端口优先级，使用端口优先级进行优先级映射。

2. 配置限制和指导

配置信任的报文优先级类型和端口优先级都只针对上行报文有效。

配置了信任的报文优先级类型后，端口优先级的配置不生效。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入无线服务模板视图。

wlan service-template *service-template-name*

(3) 配置信任的报文优先级类型。

qos trust { dot11e | dscp }

缺省情况下，信任端口优先级。

(4) 配置端口优先级。

qos priority *priority*

缺省情况下，端口优先级为 0。

1.3 配置智能带宽保障功能

(1) 进入系统视图。

system-view

(2) 配置指定射频类型的最大带宽参考值。

wlan max-bandwidth { **dot11a** | **dot11ac** | **dot11an** | **dot11b** | **dot11g** | **dot11gac** | **dot11gn** } *bandwidth*

缺省情况下，不同射频类型的最大带宽参考值如 表 1-4 所示。

表1-4 不同射频类型的最大带宽参考值

射频类型	dot11a	dot11b	dot11g	dot11an	dot11gn	dot11ac
最大带宽参考值	30000Kbps	7000Kbps	30000Kbps	250000Kbps	250000Kbps	500000Kbps

(3) 进入 Radio 接口视图。

interface wlan-radio *interface-number*

(4) 开启/关闭智能带宽保障功能。

bandwidth-guarantee { **disable** | **enable** }

缺省情况下，智能带宽保障功能处于关闭状态。

(5) 配置无线服务模板的保障带宽。

bandwidth-guarantee service-template *service-template-name* **percent** *percent*

缺省情况下，未配置无线服务模板的保障带宽。

1.4 配置客户端限速功能

1.4.1 功能简介

客户端限速功能可以基于无线服务模板、射频或用户类别进行配置。若配置动态模式，则每个客户端的限速速率为总限速速率/客户端总数，若配置静态模式，则所有客户端的限速速率为配置的值。如果同时配置多种方式或不同模式的客户端限速，则多个配置将同时生效，每个客户端的限速值为多种方式及不同模式中的限速速率最小值。

1.4.2 配置限制和指导

- 基于无线服务模板的客户端限速对使用同一个无线服务模板接入的所有客户端生效。
- 基于用户类别的客户端限速对所有客户端生效，每种类型的客户端的速率都不能超过配置的限速值。

1.4.3 配置基于无线服务模板的客户端限速功能

(1) 进入系统视图。

system-view

(2) 进入无线服务模板视图。

wlan service-template *service-template-name*

(3) 配置基于无线服务模板的客户端限速速率。

client-rate-limit { **inbound** | **outbound** } **mode** { **dynamic** | **static** } **cir** *cir* [**cbs** *cbs*]

缺省情况下，未配置基于无线服务模板的客户端限速速率。

1.4.4 配置基于用户类别的客户端限速功能

(1) 进入系统视图。

system-view

(2) 配置基于用户类别的客户端限速。

wlan client-rate-limit { **dot11a** | **dot11ac** | **dot11an** | **dot11b** | **dot11g** | **dot11gac** | **dot11gn** } { **inbound** | **outbound** } **cir** *cir* [**cbs** *cbs*]

缺省情况下，未配置基于用户类别的客户端限速。

1.5 WLAN QoS显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 WLAN QoS 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除 WLAN QoS 服务的统计信息。

表1-5 WLAN QoS 显示和维护

操作	命令
显示WMM客户端的统计信息	**display wlan wmm client** [**interface wlan-radio** *interface-number* | **mac-address** *mac-address*]
显示WMM射频的统计信息	**display wlan wmm radio** [**interface wlan-radio** *interface-number*]
清除WMM客户端的统计信息	**reset wlan wmm client** [**interface wlan-radio** *interface-number* | **mac-address** *mac-address*]
清除WMM射频的统计信息	**reset wlan wmm radio** [**interface wlan-radio** *interface-number*]

1.6 WLAN QoS典型配置举例

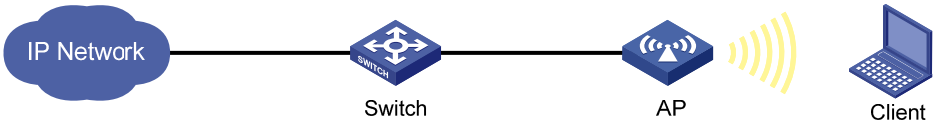
1.6.1 WMM基本服务配置举例

1. 组网需求

在 AP 上启用 WMM 功能，使 AP 和客户端在发送流量时能够区分业务优先级。

2. 组网图

图1-2 WMM 基本服务配置组网图



3. 配置步骤

配置服务模板，SSID 为 market。

```
<AP> system-view
[AP] wlan service-template market
[AP-wlan-st-market] ssid market
[AP-wlan-st-market] service-template enable
[AP-wlan-st-market] quit
```

将无线服务模板 market 绑定到 WLAN-Radio 1/0/1 接口上。

```
[AP] interface wlan-radio 1/0/1
[AP-WLAN-Radio1/0/1] undo shutdown
[AP-WLAN-Radio1/0/1] service-template market
```

开启 WMM 功能。

```
[AP-WLAN-Radio1/0/1] wmm enable
[AP-WLAN-Radio1/0/1] quit
```

4. 验证配置

完成以上配置后，可通过如下显示命令查看 WMM 射频的统计信息。

```
[AP] display wlan wmm radio
```

```
Radio : 1
Client EDCA updates : 0
QoS mode    : WMM
WMM status : Enabled
Radio max AIFSN         : 15           Radio max ECWmin : 10
Radio max TXOPLimit     : 32767        Radio max ECWmax : 10
```

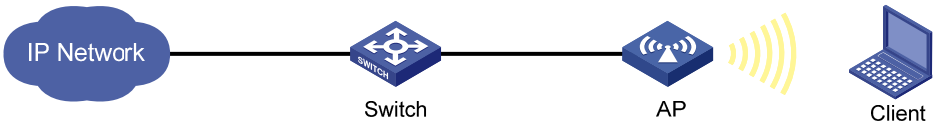
1.6.2 流区分配置举例

1. 组网需求

AP 将 Client 发送的 802.11 报文，经过端口优先级映射后，放入 AC-VO 队列。

2. 组网图

图1-3 流区分配置组网图



3. 配置步骤

配置服务模板，SSID 为 market，并开启服务模板。

```
<AP> system-view
[AP] wlan service-template market
[AP-wlan-st-market] ssid market
[AP-wlan-st-market] service-template enable
```

配置端口优先级映射，将 Client 侧发送的 802.11 报文，优先级变为 7。

```
[AP-wlan-st-market] qos priority 7
[AP-wlan-st-market] quit
```

将无线服务模板 market 绑定到 WLAN-Radio 1/0/1 接口上。

```
[AP] interface wlan-radio 1/0/1
[AP-WLAN-Radio1/0/1] undo shutdown
[AP-WLAN-Radio1/0/1] service-template market
```

开启 WMM 功能。

```
[AP-WLAN-Radio1/0/1] wmm enable
[AP-WLAN-Radio1/0/1] quit
```

4. 验证配置

完成以上配置后，在 AP 上使用 **terminal monitor** 命令允许日志输出到当前终端、使用 **terminal debugging** 命令开启当前终端对调试信息的显示功能、使用 **debugging wlan wmm all** 命令打开 wmm 所有报文调试信息开关，而后在客户端上使用 **ping** 命令测试 Client 与 Switch 的连通性。最终可查看到上行报文（AP 收到的从客户端发来的报文）的优先级更改为 7，而下行报文（经由 AP 发送给客户端的报文）不会修改优先级。

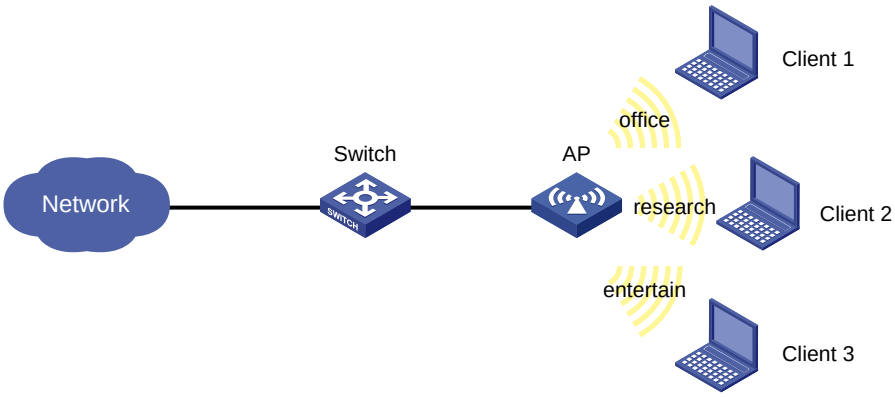
1.6.3 智能带宽保障配置举例

1. 组网需求

在某企业内，三个客户端分别通过名为 research、office、entertain 的 SSID 接入无线网络。为了满足企业网络正常运行的需求，要求在同一个 AP 内，保证无线服务 office 的带宽占总带宽的 20%，无线服务 research 的带宽占总带宽的 80%，无线服务 entertain 没有分配固定带宽。

2. 组网图

图1-4 智能带宽保障配置举例组网图



3. 配置步骤

配置无线服务模板 office，SSID 为 office。

```
<AP> system-view
[AP] wlan service-template office
[AP-wlan-st-office] ssid office
[AP-wlan-st-office] service-template enable
[AP-wlan-st-office] quit
```

配置无线服务模板 research，SSID 为 research。

```
[AP] wlan service-template research
[AP-wlan-st-research] ssid research
[AP-wlan-st-research] service-template enable
[AP-wlan-st-research] quit
```

配置无线服务模板 entertain，SSID 为 entertain。

```
[AP] wlan service-template entertain
[AP-wlan-st-entertain] ssid entertain
[AP-wlan-st-entertain] service-template enable
[AP-wlan-st-entertain] quit
```

配置 802.11ac 射频的最大带宽参考值为 10000Kbps。

```
[AP] wlan max-bandwidth dot11ac 10000
```

将无线服务模板绑定到 WLAN-Radio1/0/1 接口。

```
[AP] interface wlan-radio 1/0/1
[AP-WLAN-Radio1/0/1] undo shutdown
[AP-WLAN-Radio1/0/1] service-template office
[AP-WLAN-Radio1/0/1] service-template research
```

```
[AP-WLAN-Radio1/0/1] service-template entertain
```

开启智能带宽保障功能。

```
[AP-WLAN-Radio1/0/1] bandwidth-guarantee enable
```

配置无线服务模板 office、无线服务模板 research 的保障带宽占总带宽的百分比分别为 20%、80%。

```
[AP-WLAN-Radio1/0/1] bandwidth-guarantee service-template office percent 20
[AP-WLAN-Radio1/0/1] bandwidth-guarantee service-template research percent 80
[AP-WLAN-Radio1/0/1] return
```

4. 验证配置

如果 AP 向所有客户端发送的数据流量累计小于 10000Kbps，AP 向 Client 1～Client 3 发送的流量不会受限制。

如果 AP 向 Client 1 发送流量大于 2000Kbps，向 Client 2 发送流量大于 8000Kbps，由于为 research 无线服务和 office 无线服务配置了智能带宽保障功能，设备会优先发送 Client 1 和 Client 2 的流量。因此，AP 向 Client 1 和 Client 2 实际发送的流量分别为 2000Kbps 以及 8000Kbps 左右，向 Client 3 发送的流量会受到限制。

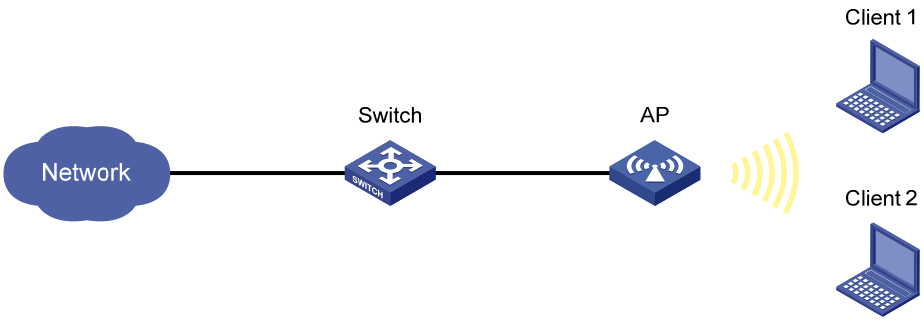
1.6.4 客户端限速配置举例

1. 组网需求

在 AP 上配置基于无线服务模板的客户端限速功能，AP 分别在入方向以静态模式、出方向以动态模式限制客户端的速率。

2. 组网图

图1-5 客户端限速组网图



3. 配置步骤

配置无线服务模板，配置 SSID 为 service。

```
<AP> system-view
[AP] wlan service-template service
[AP-wlan-st-service] ssid service
```

配置限制从客户端到 AP 方向和从 AP 到客户端方向数据传输的最大速率，使从客户端到 AP 方向的固定速率为 8000 Kbps，从 AP 到客户端方向的共享速率为 8000Kbps。

```
[AP-wlan-st-service] client-rate-limit inbound mode static cir 8000
[AP-wlan-st-service] client-rate-limit outbound mode dynamic cir 8000
[AP-wlan-st-service] service-template enable
[AP-wlan-st-service] quit
```

#将无线服务模板绑定到 WLAN-Radio1/0/1 接口上。

```
[AP] interface wlan-radio 1/0/1
[AP-WLAN-Radio1/0/1] undo shutdown
[AP-WLAN-Radio1/0/1] service-template service
[AP-WLAN-Radio1/0/1] return
```

目 录

1 QoS概述

QoS 即服务质量。对于网络业务，影响服务质量的因素包括传输的带宽、传送的时延、数据的丢包率等。在网络中可以通过保证传输的带宽、降低传送的时延、降低数据的丢包率以及时延抖动等措施来提高服务质量。网络资源总是有限的，在保证某类业务的服务质量的同时，可能就是在损害其它业务的服务质量。因此，网络管理者需要根据各种业务的特点来对网络资源进行合理的规划和分配，从而使网络资源得到高效利用。

1.1 QoS服务模型简介

通常 QoS 提供以下三种服务模型：

- Best-Effort service（尽力而为服务模型）
- Integrated service（综合服务模型，简称 IntServ）
- Differentiated service（区分服务模型，简称 DiffServ）

1.1.1 Best-Effort服务模型

Best-Effort 是一个单一的服务模型，也是最简单的服务模型。对 Best-Effort 服务模型，网络尽最大的可能性来发送报文。但对时延、可靠性等性能不提供任何保证。

Best-Effort 服务模型是网络的缺省服务模型，通过 FIFO 队列来实现。它适用于绝大多数网络应用，如 FTP、E-Mail 等。

1.1.2 IntServ服务模型

IntServ 是一个综合服务模型，它可以满足多种 QoS 需求。该模型使用 RSVP 协议，RSVP 运行在从源端到目的端的每个设备上，可以监视每个流，以防止其消耗资源过多。这种体系能够明确区分并保证每一个业务流的服务质量，为网络提供最细粒度化的服务质量区分。

但是，IntServ 模型对设备的要求很高，当网络中的数据流数量很大时，设备的存储和处理能力会遇到很大的压力。IntServ 模型可扩展性很差，难以在 Internet 核心网络实施。

1.1.3 DiffServ服务模型

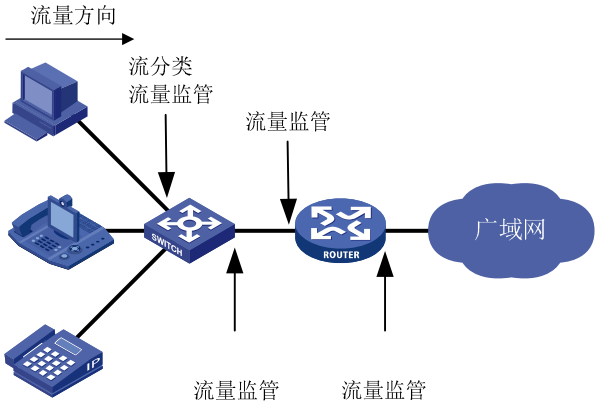
DiffServ 是一个多服务模型，它可以满足不同的 QoS 需求。与 IntServ 不同，它不需要通知网络为每个业务预留资源。区分服务实现简单，扩展性较好。

本文提到的技术都是基于 DiffServ 服务模型。

1.2 QoS技术在网络中的位置

QoS 技术包括流分类、流量监管等。下面对常用的技术进行简单地介绍。

图1-1 常用 QoS 技术在网络中的位置



如 图 1-1 所示，流分类、流量监管主要完成如下功能：

- 流分类：采用一定的规则识别符合某类特征的报文，它是对网络业务进行区分服务的前提和基础。
- 流量监管：对进入或流出设备的特定流量进行监管，以保护网络资源不受损害。可以作用在接口入方向和出方向。

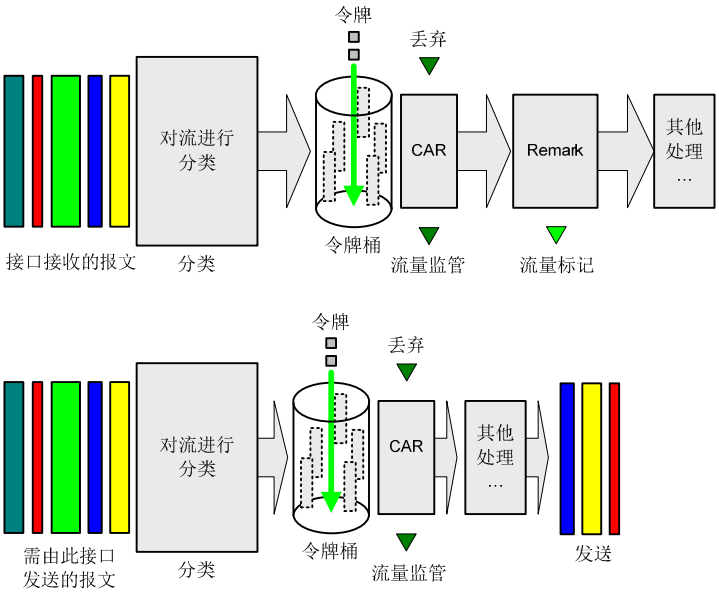
1.3 QoS技术在设备中的处理顺序

图 1-2 简要描述了各种QoS技术在网络设备中的处理顺序。

(1) 首先通过流分类对各种业务进行识别和区分，它是后续各种动作的基础；

(2) 通过各种动作对特定的业务进行处理。这些动作需要和流分类关联起来才有意义。具体采取何种动作，与所处的阶段以及网络当前的负载状况有关。例如，当报文进入网络时进行流量监管。

图1-2 各 QoS 技术在同一网络设备中的处理顺序



1.4 QoS配置方式

QoS 的配置方式分为 MQC 方式（模块化 QoS 配置，Modular QoS Configuration）和非 MQC 方式。

MQC 方式通过 QoS 策略定义不同类别的流量要采取的动作，并将 QoS 策略应用到不同的目标位置（例如接口）来实现对业务流量的控制。

非 MQC 方式则通过直接在目标位置上配置 QoS 参数来实现对业务流量的控制。

有些 QoS 功能只能使用其中一种方式来配置，有些使用两种方式都可以进行配置。在实际应用中，两种配置方式也可以结合起来使用。

2 QoS策略

2.1 QoS策略简介

QoS 策略由如下部分组成：

- 类，定义了对报文进行识别的规则。
- 流行为，定义了一组针对类识别后的报文所做的 QoS 动作。

通过将类和流行为关联起来，QoS 策略可对符合分类规则的报文执行流行为中定义的动作。

用户可以在一个策略中定义多个类与流行为的绑定关系。

2.2 QoS策略配置任务简介

QoS 策略配置任务如下：

(1) 定义类

(2) 定义流行为

(3) 定义策略

(4) 应用策略

- 基于接口应用QoS策略
- 基于上线用户应用QoS策略

2.3 定义类

(1) 进入系统视图。

system-view

(2) 创建类，并进入类视图。

traffic classifier *classifier-name* [**operator** { **and** | **or** }]

(3) 定义匹配数据包的规则。

if-match [**not**] *match-criteria*

缺省情况下，未定义匹配数据包的规则。

具体规则的介绍，请参见“QoS 命令”中的 **if-match** 命令。

2.4 定义流行为

(1) 进入系统视图。

system-view

(2) 创建流行为，并进入流行为视图。

traffic behavior *behavior-name*

(3) 配置流行为的动作。

缺省情况下，未配置流行为的动作。

流行为动作就是对符合流分类的报文做出相应的 QoS 动作，例如流量监管、流量过滤、重标记等，具体情况请参见本文相关章节。

2.5 定义策略

(1) 进入系统视图。

system-view

(2) 创建 QoS 策略，并进入策略视图。

qos policy *policy-name*

(3) 为类指定流行为。

classifier *classifier-name* **behavior** *behavior-name* [**insert-before** *before-classifier-name*]

2.6 应用策略

2.6.1 设备支持的策略应用位置

QoS 策略支持应用在如下位置：

- 基于接口应用 QoS 策略，QoS 策略对通过接口接收或发送的流量生效。
- 基于上线用户应用 QoS 策略，QoS 策略对通过上线用户接收或发送的流量生效。

2.6.2 策略应用限制和指导

QoS 策略应用后，用户仍然可以修改 QoS 策略中的流分类规则和流行为，以及二者的对应关系。当流分类规则中使用 ACL 匹配报文时，允许删除或修改该 ACL（包括向该 ACL 中添加、删除和修改匹配规则）。

2.6.3 基于接口应用QoS策略

1. 配置限制和指导

基于接口应用 QoS 策略时需要注意的是：

- 一个 QoS 策略可以应用于多个接口，但在接口的每个方向（出和入两个方向）只能应用一个策略。
- QoS 策略应用在出方向时，对设备发出的协议报文不起作用，以确保这些报文在策略误配置时仍然能够正常发出，维持设备的正常运行。常见的本地协议报文如下：链路维护报文、RIP、SSH 等。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 在接口上应用已创建的 QoS 策略。

qos apply policy *policy-name* { **inbound** | **outbound** }

缺省情况下，未在接口上应用 QoS 策略。

2.6.4 基于上线用户应用QoS策略

1. 功能简介

用户通过身份认证后，认证服务器会将与用户帐户绑定的 User Profile 名称下发给设备，设备可以通过 User Profile 视图下配置 QoS 策略来对上线用户的流量进行管理。User Profile 视图下的 QoS 策略只有在用户成功上线后才生效。

2. 配置限制和指导

一个策略可以应用于多个上线用户。上线用户的每个方向（发送和接收两个方向）只能应用一个策略，如果用户想修改某方向上应用的策略，必须先取消原先的配置，然后再配置新的策略。

3. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 User Profile 视图。

user-profile *profile-name*

(3) 在 User Profile 下应用 QoS 策略。

qos apply policy *policy-name* { **inbound** | **outbound** }

缺省情况下，未在 User Profile 下应用 QoS 策略。

参数	说明
inbound	表示对设备接收上线用户的流量（即上线用户发送的流量）应用策略
outbound	表示对设备发送给上线用户的流量（即上线用户接收的流量）应用策略

2.7 QoS策略显示和维护

在任意视图下执行 **display** 命令可以显示 QoS 策略的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除 QoS 策略的统计信息。

表2-1 QoS 策略显示和维护

操作	命令
显示QoS策略的配置信息	**display qos policy** { **system-defined**	**user-defined** } [*policy-name* [**classifier** *classifier-name*]]
显示接口上QoS策略的配置信息和运行情况	**display qos policy interface** [*interface-type interface-number*] [**inbound**	**outbound**]
显示用户上线后User Profile下应用的QoS策略的信息和运行情况	**display qos policy user-profile** [**name** *profile-name*] [**user-id** *user-id*] [**inbound**	**outbound**]
显示流行为的配置信息	**display traffic behavior** { **system-defined**	**user-defined** } [*behavior-name*]

操作	命令
显示类的配置信息	**display traffic classifier** { **system-defined** | **user-defined** }

3 优先级映射

3.1 优先级映射简介

优先级映射可以将报文携带的优先级字段映射成指定优先级字段值，设备根据映射后的优先级字段，为报文提供有差别的 QoS 服务，从而为全面有效的控制报文的转发调度等级提供依据。

3.1.1 优先级介绍

优先级用于标识报文传输的优先程度，可以分为两类：报文携带优先级和设备调度优先级。

报文携带优先级包括：802.1p优先级、DSCP优先级、IP优先级等。这些优先级都是根据公认的标准和协议生成，体现了报文自身的优先等级。相关介绍请参见“7.3 附录 C 各种优先级介绍”。

设备调度优先级是指报文在设备内转发时所使用的优先级，只对当前设备自身有效。设备调度优先级仅支持本地优先级（LP）。设备为报文分配的一种具有本地意义的优先级，每个本地优先级对应一个队列，本地优先级值越大的报文，进入的队列优先级越高，从而能够获得优先的调度。

3.1.2 优先级映射表

设备提供了多张优先级映射表，分别对应不同的优先级映射关系。

通常情况下，设备可以通过查找缺省优先级映射表（7.2 附录 B 缺省优先级映射表）来为报文分配相应的优先级。如果缺省优先级映射表无法满足用户需求，可以根据实际情况对映射表进行修改。

3.1.3 优先级映射配置方式

优先级映射配置方式包括：优先级信任模式方式、端口优先级方式。

1. 优先级信任模式方式

配置端口的优先级信任模式后，设备将信任报文自身携带的优先级。通过优先级映射表，使用所信任的报文携带优先级进行优先级映射，根据映射关系完成对报文优先级的修改，以及实现报文在设备内部的调度。

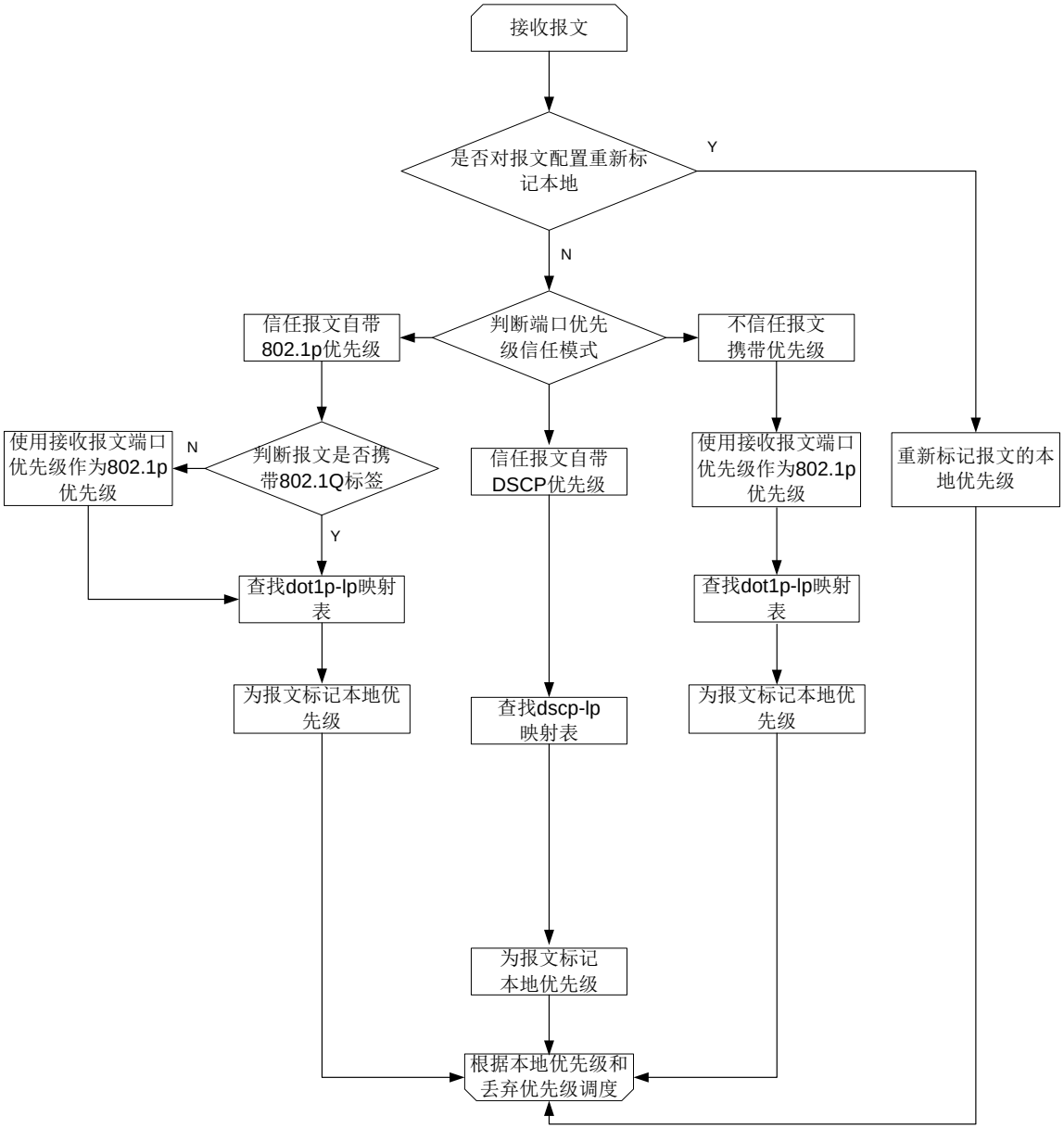
2. 端口优先级方式

未配置端口的优先级信任模式时，设备会将端口优先级作为报文自身的优先级。通过优先级映射表，对报文进行映射。用户可以配置端口优先级，通过优先级映射，使不同端口收到的报文进入对应的队列，以此实现对不同端口收到报文的差异化调度。

3.1.4 优先级映射过程

对于接收到的以太网报文，根据优先级信任模式和报文的 802.1Q标签状态，设备将采用不同的方式为其标记调度优先级。如 图 3-1 所示：

图3-1 以太网报文优先级映射过程



说明

关于重标记优先级功能的介绍，请参见 重标记。

3.2 优先级映射配置任务简介

优先级映射配置任务如下：

(1) （可选）配置优先级映射表

(2) 配置优先级映射方式。

- 配置优先级信任模式

3.3 配置优先级映射表

(1) 进入系统视图。

system-view

(2) 进入指定的优先级映射表视图。

qos map-table [**inbound** | **outbound**] { **dot11e-lp** | **dot1p-lp** | **dscp-lp** | **lp-dot11e** | **lp-dot1p** | **lp-dscp** }

(3) 配置指定优先级映射表的映射关系。

import *import-value-list* **export** *export-value*

缺省情况下，优先级映射表的映射关系请参见“**错误!未找到引用源。错误!未找到引用源。**”。

多次执行本命令，最后一次执行的命令生效。

3.4 配置优先级信任模式

1. 功能简介

配置优先级信任模式后，设备将根据报文自身的优先级，查找优先级映射表，为报文分配优先级参数。

在配置接口上的优先级模式时，用户可以选择下列信任模式：

- **dot1p**：信任报文自带的 802.1p 优先级，以此优先级进行优先级映射。
- **dscp**：信任 IP 报文自带的 DSCP 优先级，以此优先级进行优先级映射。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 配置优先级信任模式。

qos trust { **dot1p** | **dscp** }

缺省情况下，设备未配置优先级信任模式。

设备不信任报文携带的优先级，会使用端口优先级作为报文的 802.1p 优先级进行优先级映射。

(4) 退回系统视图。

quit

3.5 配置端口优先级

1. 功能简介

按照接收端口的端口优先级，设备通过一一映射为报文分配相应的优先级。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入接口视图。

interface *interface-type interface-number*

(3) 配置端口优先级。

qos priority *priority-value*

缺省情况下，端口优先级为 0。

3.6 优先级映射显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后优先级映射的运行情况，通过查看显示信息验证配置的效果。

表3-1 优先级映射显示和维护

操作	命令
显示指定优先级映射表配置情况	**display qos map-table** [**inbound** | **outbound**] [**dot11e-lp** | **dot1p-lp** | **dscp-lp** | **lp-dot11e** | **lp-dot1p** | **lp-dscp**]
显示端口优先级信任模式信息	**display qos trust interface** [*interface-type interface-number*]

4 流量监管

4.1 流量监管简介

如果不限制用户发送的流量，那么大量用户不断突发的数据只会使网络更拥挤。为了使有限的网络资源能够更好地发挥效用，更好地为更多的用户服务，必须对用户的流量加以限制。流量监管可以实现流量的速率限制功能，而要实现此功能就必须对通过设备的流量进行度量。一般采用令牌桶（Token Bucket）对流量进行度量。

4.1.1 流量评估与令牌桶

1. 令牌桶

令牌桶可以看作是一个存放一定数量令牌的容器。系统按设定的速度向桶中放置令牌，当桶中令牌满时，多出的令牌溢出，桶中令牌不再增加。

2. 用令牌桶评估流量

在用令牌桶评估流量规格时，是以令牌桶中的令牌数量是否足够满足报文的转发为依据的。如果桶中存在足够的令牌可以用来转发报文，称流量遵守或符合这个规格，否则称为不符合或超标。

评估流量时令牌桶的参数包括：

- 平均速率：向桶中放置令牌的速率，即允许的流的平均速度。通常配置为 CIR。
- 突发尺寸：令牌桶的容量，即每次突发所允许的最大的流量尺寸。通常配置为 CBS，突发尺寸必须大于最大报文长度。

每到达一个报文就进行一次评估。每次评估，如果桶中有足够的令牌可供使用，则说明流量控制在允许的范围内，此时要从桶中取走满足报文的转发的令牌；否则说明已经耗费太多令牌，流量超标了。

3. 复杂评估

为了评估更复杂的情况，实施更灵活的调控策略，可以配置两个令牌桶（分别称为 C 桶和 E 桶）。以流量监管为例。

单速率单桶双色算法

- CIR：表示向 C 桶中投放令牌的速率，即 C 桶允许传输或转发报文的平均速率；
- CBS：表示 C 桶的容量，即 C 桶瞬间能够通过的承诺突发流量。

每次评估时，依据下面的情况，可以分别实施不同的流控策略：

- 如果 C 桶有足够的令牌，报文被标记为 green，即绿色报文；
- 如果 C 桶令牌不足，报文被标记为 red，即红色报文。

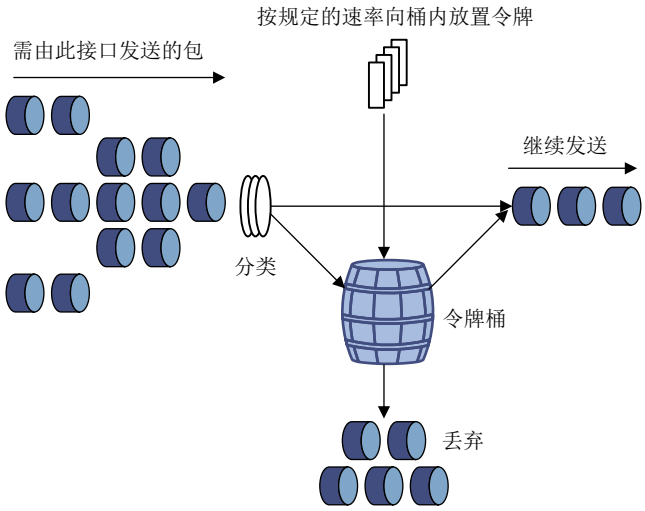
4.1.2 流量监管

流量监管分为入和出两个方向，为了方便描述，下文以出方向为例。

流量监管就是对流量进行控制，通过监督进入网络的流量速率，对超出部分的流量进行“惩罚”，使进入的流量被限制在一个合理的范围之内，以保护网络资源和运营商的利益。例如可以限制 HTTP

报文不能占用超过 50%的网络带宽。如果发现某个连接的流量超标，流量监管可以选择丢弃报文，或重新配置报文的优先级。

图4-1 TP 示意图



流量监管广泛的用于监管进入 Internet 服务提供商 ISP 的网络流量。流量监管还包括对所监管流量的流分类服务，并依据不同的评估结果，实施预先设定好的监管动作。这些动作可以是：

- 转发：比如对评估结果为“符合”的报文继续转发。
- 丢弃：比如对评估结果为“不符合”的报文进行丢弃。
- 改变优先级并转发：比如对评估结果为“符合”的报文，将其优先级进行重标记后再进行转发。

4.2 配置流量监管

4.2.1 流量监管配置方式介绍

可以通过 MQC 方式和非 MQC 方式配置流量监管，其中非 MQC 方式配置流量监管时基于上线用户的流量监管配置。

如果接口上同时采用了 MQC 方式和非 MQC 方式配置了流量监管，那么只有前者会生效。

4.2.2 配置流量监管（MQC方式）

1. 配置限制和指导

设备支持基于接口和上线用户应用 QoS 策略配置流量监管。

2. 配置步骤

(1) 进入系统视图。

```
system-view
```

(2) 定义类。

a. 创建类，并进入类视图。

traffic classifier *classifier-name* [**operator** { **and** | **or** }]

b. 定义匹配数据包的规则。

if-match [**not**] *match-criteria*

缺省情况下，未定义匹配数据包的规则。

具体规则的介绍，请参见“QoS 命令”中的 **if-match** 命令。

c. 退回系统视图。

quit

(3) 定义流行为。

a. 创建一个流行为并进入流行为视图。

traffic behavior *behavior-name*

b. 配置流量监管动作。

car cir *committed-information-rate* [**cbs** *committed-burst-size*] [**green** *action* | **red** *action* | **yellow** *action*] *

缺省情况下，未配置流量监管动作。

c. 退回系统视图。

quit

(4) 定义策略。

a. 创建策略并进入策略视图。

qos policy *policy-name*

b. 在策略中为类指定采用的流行为。

classifier *classifier-name* **behavior** *behavior-name*

缺省情况下，未指定类对应的流行为。

c. 退回系统视图。

quit

(5) 应用 QoS 策略。

具体配置请参见“2.6 应用策略”

缺省情况下，未应用 QoS 策略。

4.2.3 配置基于上线用户的流量监管

1. 功能简介

用户通过身份认证后，认证服务器会将与用户帐户绑定的 User Profile 名称下发给设备，设备可以通过 User Profile 视图下配置 CAR 策略来对上线用户进行流量监管：当用户数据流量符合承诺速率时，允许数据包通过；用户数据流量不符合承诺速率时，丢弃数据包，只要用户上线，认证服务器会自动下发相应的 User Profile，当用户下线，系统会自动取消相应的配置，不需要再进行手工调整。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 进入 User Profile 视图。

user-profile *profile-name*

(3) 在 User Profile 下应用 CAR 策略。

qos car { **inbound** | **outbound** } **any cir** *committed-information-rate* [**cbs** *committed-burst-size*]

缺省情况下，在 User Profile 下没有应用 CAR 策略。

4.3 流量监管显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后流量监管的运行情况，通过查看显示信息验证配置的效果。

说明

由于 WX2500H 系列和 WX3000H 系列无线控制器不支持 IRF 功能，因此仅支持独立运行模式的命令行参数。

表4-1 流量监管显示和维护

操作	命令
显示流量监管的相关配置信息	**display traffic behavior user-defined** [*behavior-name*]

5 流量过滤

5.1 流量过滤简介

流量过滤是指对符合流分类的流进行过滤的动作。例如，可以根据网络的实际情况禁止从某个源 IP 地址发送的报文通过。

5.2 流量过滤配置限制和指导

设备支持基于接口和上线用户应用 QoS 策略配置流量过滤。

5.3 配置流量过滤

(1) 进入系统视图。

system-view

(2) 定义类。

a. 创建一个类，并进入类视图。

traffic classifier *classifier-name* [**operator** { **and** | **or** }]

b. 定义匹配数据包的规则。

if-match [**not**] *match-criteria*

缺省情况下，未定义匹配数据包的规则。

具体规则的介绍，请参见“QoS 命令”中的 **if-match** 命令。

c. 退回系统视图。

quit

(3) 定义流行为。

a. 创建一个流行为，并进入流行为视图。

traffic behavior *behavior-name*

b. 配置流量过滤动作。

filter { **deny** | **permit** }

缺省情况下，未配置流量过滤动作。

如果配置了 filter deny 命令，则在该流行为视图下配置的其他流行为都不会生效。

c. 退回系统视图。

quit

(4) 定义策略。

a. 创建策略并进入策略视图。

qos policy *policy-name*

b. 在策略中为类指定采用的流行为。

classifier *classifier-name* **behavior** *behavior-name*

缺省情况下，未指定类对应的流行为。

c. 退回系统视图。

quit

(5) 应用 QoS 策略。

具体配置请参见“2.6 应用策略”

缺省情况下，未应用 QoS 策略。

(6) （可选）显示流量过滤的相关配置信息。

display traffic behavior user-defined [*behavior-name*]

6 重标记

6.1 重标记简介

重标记是将报文的优先级或者标志位进行设置，重新定义报文的优先级等。例如，对于 IP 报文来说，可以利用重标记对 IP 报文中的 IP 优先级或 DSCP 值进行重新设置，控制 IP 报文的转发。

重标记动作的配置，可以通过与类关联，将原来报文的优先级或标志位重新进行标记。

重标记可以和优先级映射功能配合使用，具体请参见“3 优先级映射”。

6.2 配置重标记

1. 配置限制和指导

设备支持基于接口和上线用户应用 QoS 策略配置重标记。

2. 配置步骤

(1) 进入系统视图。

system-view

(2) 定义类。

a. 创建一个类，并进入类视图。

traffic classifier *classifier-name* [**operator** { **and** | **or** }]

b. 定义匹配数据包的规则。

if-match [**not**] *match-criteria*

缺省情况下，未定义匹配数据包的规则。

具体规则的介绍，请参见“QoS 命令”中的 **if-match** 命令。

c. 退回系统视图。

quit

(3) 定义流行为

a. 创建一个流行为，并进入流行为视图。

traffic behavior *behavior-name*

b. 重新标记报文的动作。

具体重标记动作的介绍，请查看“QoS 命令”中的 **remark** 命令。

c. 退回系统视图。

quit

(4) 定义策略。

a. 创建一个策略，并进入策略视图。

qos policy *policy-name*

b. 在策略中为类指定采用的流行为。

classifier *classifier-name* **behavior** *behavior-name*

缺省情况下，未指定类对应的流行为。

c. 退回系统视图。

quit

(5) 应用 QoS 策略。

具体配置请参见“2.6 应用策略”

缺省情况下，未应用 QoS 策略。

(6) （可选）显示重标记的相关配置信息。

display traffic behavior user-defined [*behavior-name*]

6.3 重标记配置举例

6.3.1 重标记基本配置举例

1. 组网需求

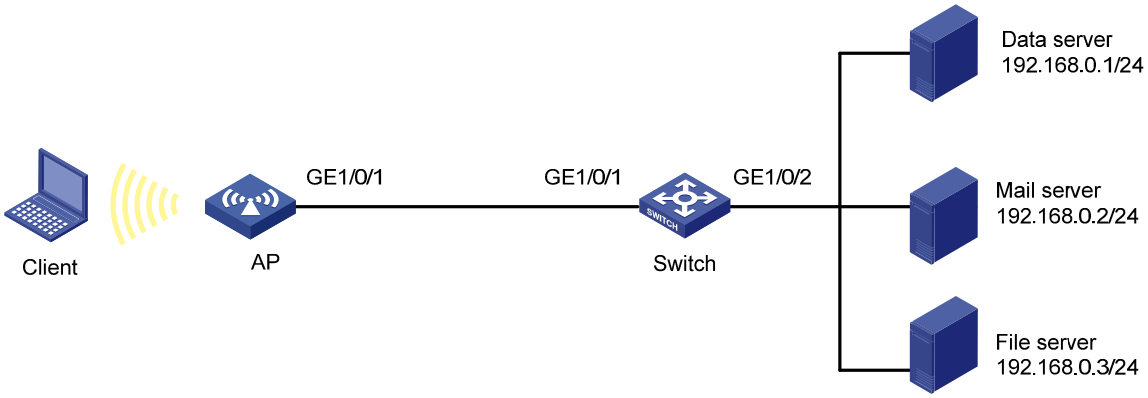
公司企业网通过 AP 实现互连。

通过配置重标记功能，在 AP 上实现如下需求：

- 优先处理 Client 访问数据库服务器的报文；
- 其次处理 Client 访问邮件服务器的报文；
- 最后处理 Client 访问文件服务器的报文。

2. 组网图

图6-1 重标记配置组网图



3. 配置步骤

定义高级 ACL 3000，对目的 IP 地址为 192.168.0.1 的报文进行分类。

```
<AP> system-view
[AP] acl advanced 3000
[AP-acl-ipv4-adv-3000] rule permit ip destination 192.168.0.1 0
[AP-acl-ipv4-adv-3000] quit
```

定义高级 ACL 3001，对目的 IP 地址为 192.168.0.2 的报文进行分类。

```
[AP] acl advanced 3001
[AP-acl-ipv4-adv-3001] rule permit ip destination 192.168.0.2 0
```

```
[AP-acl-ipv4-adv-3001] quit
```

定义高级 ACL 3002，对目的 IP 地址为 192.168.0.3 的报文进行分类。

```
[AP] acl advanced 3002
[AP-acl-ipv4-adv-3002] rule permit ip destination 192.168.0.3 0
[AP-acl-ipv4-adv-3002] quit
```

定义类 classifier_dbserver，匹配高级 ACL 3000。

```
[AP] traffic classifier classifier_dbserver
[AP-classifier-classifier_dbserver] if-match acl 3000
[AP-classifier-classifier_dbserver] quit
```

定义类 classifier_mserver，匹配高级 ACL 3001。

```
[AP] traffic classifier classifier_mserver
[AP-classifier-classifier_mserver] if-match acl 3001
[AP-classifier-classifier_mserver] quit
```

定义类 classifier_fserver，匹配高级 ACL 3002。

```
[AP] traffic classifier classifier_fserver
[AP-classifier-classifier_fserver] if-match acl 3002
[AP-classifier-classifier_fserver] quit
```

定义流行为 behavior_dbserver，动作为重标记报文的 DSCP 优先级为 4。

```
[AP] traffic behavior behavior_dbserver
[AP-behavior-behavior_dbserver] remark dscp 4
[AP-behavior-behavior_dbserver] quit
```

定义流行为 behavior_mserver，动作为重标记报文的 DSCP 优先级为 3。

```
[AP] traffic behavior behavior_mserver
[AP-behavior-behavior_mserver] remark dscp 3
[AP-behavior-behavior_mserver] quit
```

定义流行为 behavior_fserver，动作为重标记报文的 DSCP 优先级为 2。

```
[AP] traffic behavior behavior_fserver
[AP-behavior-behavior_fserver] remark dscp 2
[AP-behavior-behavior_fserver] quit
```

定义策略 policy_server，为类指定流行为。

```
[AP] qos policy policy_server
[AP-qospolicy-policy_server] classifier classifier_dbserver behavior behavior_dbserver
[AP-qospolicy-policy_server] classifier classifier_mserver behavior behavior_mserver
[AP-qospolicy-policy_server] classifier classifier_fserver behavior behavior_fserver
[AP-qospolicy-policy_server] quit
```

将策略 policy_server 应用到端口 GigabitEthernet1/0/1 上。

```
[AP] interface gigabitethernet 1/0/1
[AP-GigabitEthernet1/0/1] qos apply policy policy_server outbound
[AP-GigabitEthernet1/0/1] quit
```

4. 验证配置

数据库服务器收到的报文优先级高，邮件服务器收到的报文优先级次高，文件服务器收到的报文优先级低。

7 附录

7.1 附录 A 缩略语表

表7-1 附录 A 缩略语表

缩略语	英文全名	中文解释
AF	Assured Forwarding	确保转发
BE	Best Effort	尽力转发
BQ	Bandwidth Queuing	带宽队列
CAR	Committed Access Rate	承诺访问速率
CBQ	Class Based Queuing	基于类的队列
CBS	Committed Burst Size	承诺突发尺寸
CBWFQ	Class Based Weighted Fair Queuing	基于类的加权公平队列
CE	Customer Edge	用户边缘设备
CIR	Committed Information Rate	承诺信息速率
CQ	Custom Queuing	定制队列
DAR	Deeper Application Recognition	深度应用识别
DCBX	Data Center Bridging Exchange Protocol	数据中心桥能力交换协议
DiffServ	Differentiated Service	区分服务
DoS	Denial of Service	拒绝服务
DSCP	Differentiated Services Code Point	区分服务编码点
EACL	Enhanced ACL	增强型ACL
EBS	Excess Burst Size	超出突发尺寸
ECN	Explicit Congestion Notification	显示拥塞通知
EF	Expedited Forwarding	加速转发
FEC	Forwarding Equivalance Class	转发等价类
FIFO	First in First out	先入先出
FQ	Fair Queuing	公平队列
GMB	Guaranteed Minimum Bandwidth	最小带宽保证队列
GTS	Generic Traffic Shaping	通用流量整形
IntServ	Integrated Service	综合服务
ISP	Internet Service Provider	互联网服务提供商
LFI	Link Fragmentation and Interleaving	链路分片与交叉

缩略语	英文全名	中文解释
LLQ	Low Latency Queuing	低时延队列
LR	Line Rate	限速
LSP	Label Switched Path	标签交换路径
MPLS	Multiprotocol Label Switching	多协议标签交换
P2P	Peer-to-Peer	对等
PE	Provider Edge	服务提供商网络边缘
PHB	Per-hop Behavior	单中继段行为
PIR	Peak Information Rate	峰值信息速率
PQ	Priority Queuing	优先队列
PW	Pseudowire	伪线
QoS	Quality of Service	服务质量
QPPB	QoS Policy Propagation Through the Border Gateway Protocol	通过BGP传播QoS策略
RED	Random Early Detection	随机早期检测
RSVP	Resource Reservation Protocol	资源预留协议
RTP	Real-time Transport Protocol	实时传输协议
SLA	Service Level Agreement	服务水平协议
SP	Strict Priority	严格优先级队列
TE	Traffic Engineering	流量工程
ToS	Type of Service	服务类型
TP	Traffic Policing	流量监管
TS	Traffic Shaping	流量整形
VoIP	Voice over IP	在IP网络上传送语音
VPN	Virtual Private Network	虚拟专用网络
VSI	Virtual Station Interface	虚拟服务器接口
WFQ	Weighted Fair Queuing	加权公平队列
WRED	Weighted Random Early Detection	加权随机早期检测
WRR	Weighted Round Robin	加权轮询队列

7.2 附录 B 缺省优先级映射表

表7-2 dot1p-lp 缺省映射关系

映射输入索引	dot1p-lp 映射
dot1p	lp
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

表7-3 dot11e-lp 缺省映射关系

dot11e	lp
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

表7-4 dscp-lp 缺省映射关系

映射输入索引	dscp-lp 映射
dscp	lp
0～7	0
8～15	1
16～23	2
24～31	3
32～39	4
40～47	5
48～55	6

映射输入索引	dscp-lp 映射
56～63	7

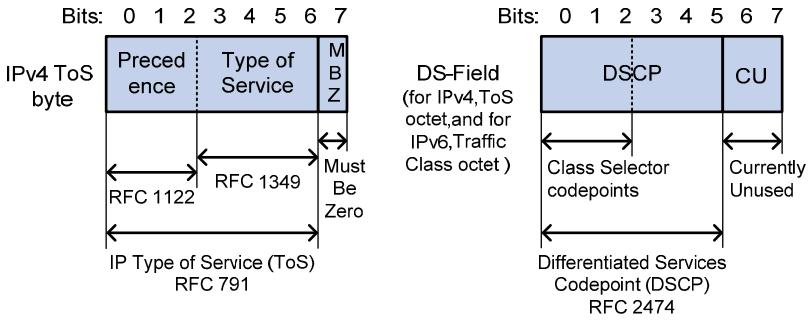
表7-5 lp-dot1p、lp-dot11e、lp-dscp 缺省映射关系

映射输入索引	lp-dot1p 映射	lp-dot11e 映射	lp-dscp 映射
lp	dot1p	dot11e	dscp
0	1	1	0
1	2	2	8
2	0	0	16
3	3	3	24
4	4	4	32
5	5	5	40
6	6	6	48
7	7	7	56

7.3 附录 C 各种优先级介绍

7.3.1 IP优先级和DSCP优先级

图7-1 ToS 和 DS 域



如 图 7-1 所示，IP报文头的ToS字段有 8 个bit，其中前 3 个bit表示的就是IP优先级，取值范围为 0～7。RFC 2474 中，重新定义了IP报文头部的ToS域，称之为DS（Differentiated Services，差分服务）域，其中DSCP优先级用该域的前 6 位（0～5 位）表示，取值范围为 0～63，后 2 位（6、7 位）是保留位。

表7-6 IP 优先级说明

IP 优先级（十进制）	IP 优先级（二进制）	关键字
0	000	routine
1	001	priority

IP 优先级（十进制）	IP 优先级（二进制）	关键字
2	010	immediate
3	011	flash
4	100	flash-override
5	101	critical
6	110	internet
7	111	network

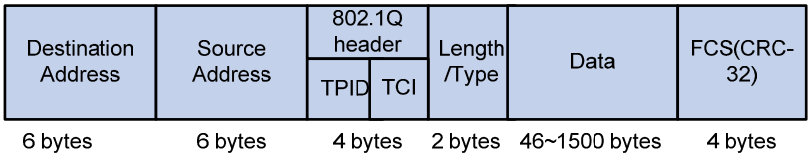
表7-7 DSCP 优先级说明

DSCP 优先级（十进制）	DSCP 优先级（二进制）	关键字
46	101110	ef
10	001010	af11
12	001100	af12
14	001110	af13
18	010010	af21
20	010100	af22
22	010110	af23
26	011010	af31
28	011100	af32
30	011110	af33
34	100010	af41
36	100100	af42
38	100110	af43
8	001000	cs1
16	010000	cs2
24	011000	cs3
32	100000	cs4
40	101000	cs5
48	110000	cs6
56	111000	cs7
0	000000	be（default）

7.3.2 802.1p优先级

802.1p 优先级位于二层报文头部，适用于不需要分析三层报头，而需要在二层环境下保证 QoS 的场合。

图7-2 带有 802.1Q 标签头的以太网帧



如 图 7-2 所示，4 个字节的 802.1Q标签头包含了 2 个字节的TPID（Tag Protocol Identifier，标签协议标识符）和 2 个字节的TCI（Tag Control Information，标签控制信息），TPID取值为 0x8100，图 7-3 显示了 802.1Q标签头的详细内容，Priority字段就是 802.1p优先级。之所以称此优先级为802.1p优先级，是因为有关这些优先级的应用是在 802.1p规范中被详细定义的。

图7-3 802.1Q 标签头

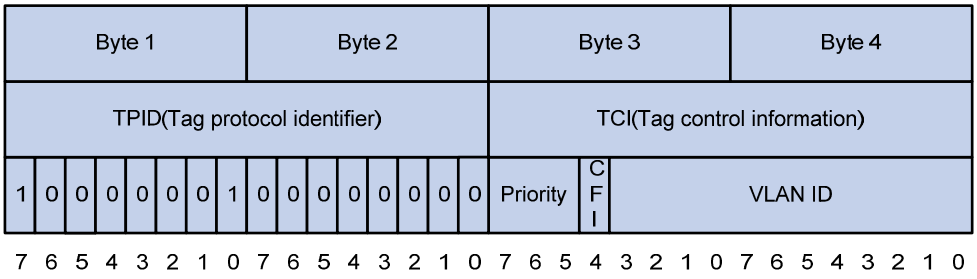


表7-8 802.1p 优先级说明

802.1p 优先级（十进制）	802.1p 优先级（二进制）	关键字
0	000	best-effort
1	001	background
2	010	spare
3	011	excellent-effort
4	100	controlled-load
5	101	video
6	110	voice
7	111	network-management

7.3.3 802.11e优先级

为了在无线网络中提供 QoS 服务，802.11e 标准被提出。802.11e 是 802.11 协议的 MAC 层增强协议，和 802.11 相比，在 802.11e 的 MAC 帧头中，增加了 2 个字节的 QoS Control 域，其中优先级位为 3bit。802.11e 优先级取值范围为 0～7。

图7-4 802.11e 的帧结构