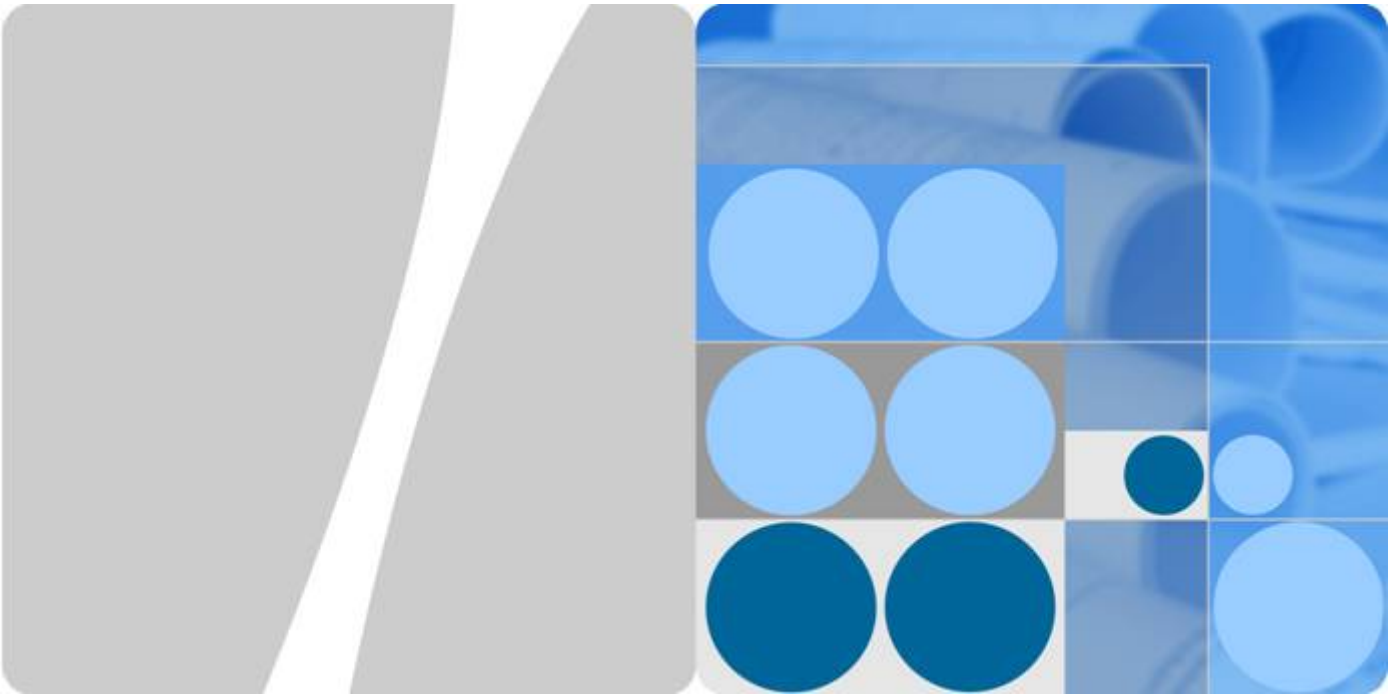


Huawei AR1200 系列企业路由器

V200R001C01

配置指南-WLAN

文档版本　03

发布日期　2012-01-06

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

前 言

读者对象

本文档介绍了 AR1200 中 WLAN 的基本概念、在不同应用场景中的配置过程和配置举例。

本文档提供了 WLAN 的配置方法。

本文档主要适用于以下工程师：

- 数据配置工程师
- 调测工程师
- 网络监控工程师
- 系统维护工程师

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
危险	以本标志开始的文本表示有高度潜在危险，如果不能避免，会导致人员死亡或严重伤害。
警告	以本标志开始的文本表示有中度或低度潜在危险，如果不能避免，可能导致人员轻微或中等伤害。
注意	以本标志开始的文本表示有潜在风险，如果忽视这些文本，可能导致设备损坏、数据丢失、设备性能降低或不可预知的结果。
窍门	以本标志开始的文本能帮助您解决某个问题或节省您的时间。
说明	以本标志开始的文本是正文的附加信息，是对正文的强调和补充。

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 | ... }	表示从两个或多个选项中选取一个。
[x | y | ...]	表示从两个或多个选项中选取一个或者不选。
{ x | y | ... }*	表示从两个或多个选项中选取多个，最少选取一个，最多选取所有选项。
[x | y | ...]*	表示从两个或多个选项中选取多个或者不选。
&<1-n>	表示符号&前面的参数可以重复 1 ～ n 次。
#	由“#”开始的行表示为注释行。

接口编号约定

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

修订记录

修改记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

文档版本 03 (2012-01-06)

相对于版本 02 (2011-11-27)的变化如下：

修改：

- **1.4.5 配置 WLAN 服务集**

文档版本 02 (2011-11-27)

相对于版本 01 (2011-08-15)的变化如下：

修改：

- **1.6.1 配置 WLAN 基本业务示例**

文档版本 01 (2011-08-15)

第一次正式发布。

目 录

1 WLAN 业务配置

关于本章

介绍胖 AP 组网模式下的 WLAN 业务配置过程。

1.1 WLAN 业务简介

1.2 AR1200 支持的 WLAN 特性
AR1200 支持的特性包括 WLAN 射频管理、WLAN 用户接入安全管理和 WLAN QoS 管理。

1.3 配置 WLAN 射频
WLAN 系统使用无线射频作为传输介质，且无线通讯通过抢占信道来传输数据。为了保证不同质量的无线接入服务，需要进行 WLAN 射频的相关配置。

1.4 配置 WLAN 业务
AP 正常工作后，AP 根据 VAP 的参数配置提供给用户不同的业务。

1.5 维护
介绍如何复位 AP。

1.6 配置举例

1.1 WLAN 业务简介

WLAN 概述

WLAN(Wireless Local Area Network)无线局域网是指应用无线通信技术将计算机设备互联起来，构成可以互相通信和实现资源共享的网络体系。它是一种利用无线技术实现快速接入以太网的技术。无线局域网本质的特点是不再使用通信电缆将计算机与网络连接起来，而是通过无线的方式连接，从而使网络的构建和终端的移动更加灵活。和传统的有线接入方式相比，无线局域网的启动和实施相对简单，维护的成本低廉，一般只要安放一个或多个接入点设备就可建立覆盖整个建筑或地区的局域网络。

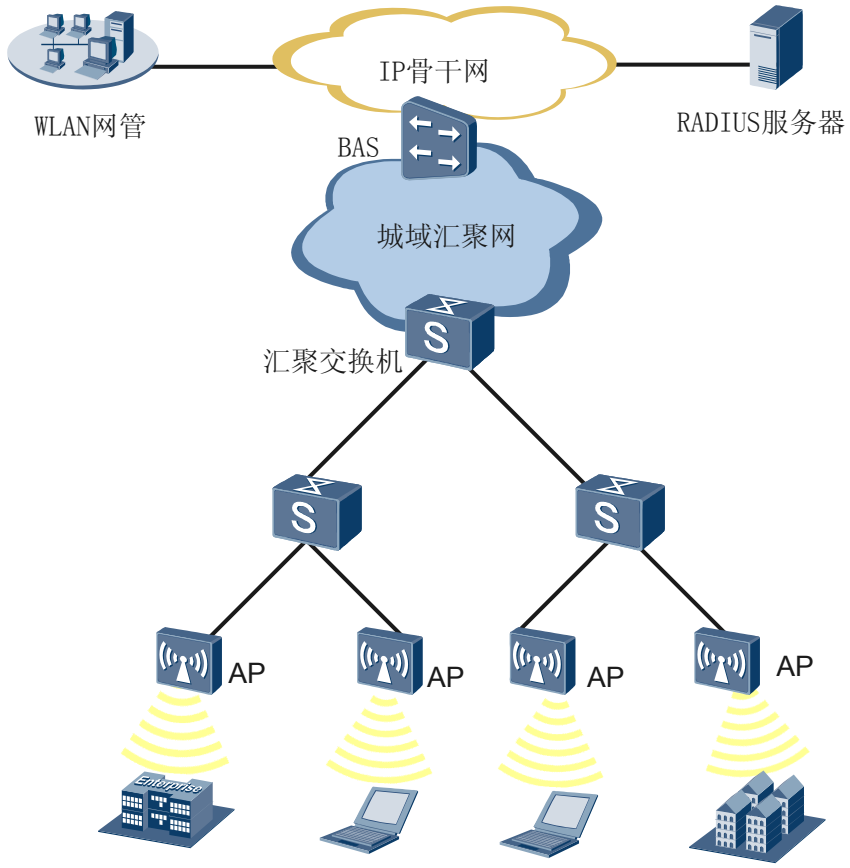
WLAN 以无线多址信道作为传输媒介，利用电磁波完成数据交互，实现传统有线局域网的功能。WLAN 技术现在已经广泛的应用在商务区，大学，机场，及其他公共区域。

WLAN 组网应用

WLAN 系统不是完全的无线系统，它的服务器和骨干网仍然安置在固定网络，只是用户可以通过无线方式接入网络。

WLAN(胖 AP)组网模式如图 1-1 所示。

图 1-1 胖 AP 组网模式



AP	无线信道管理、STA 接入安全控制由 AP 控制。AP 角色由 AR1200 承担。

WLAN 网管	采用华为统一网管通过 SNMP 或 TR069 远程管理控制 AP。
BAS	由 BAS 提供宽带用户接入认证鉴权、计费。

无线终端与 AP 之间的无线链路建立过程可以分为终端扫描 AP、终端在 AP 上认证和终端与 AP 进行关联三个步骤。

1. 无线局域网中多个 AP 定期发送 BEACON 帧，无线终端在每个信道上检测多个设备定期发送的 BEACON 帧后，选择一台 AP 作为 WLAN 接入设备。
2. 无线终端在通过 AP 的 802.11 链路认证后，发送关联请求给 AP，AP 决定是否允许此无线终端加入。
3. 无线终端开始拨号进行 802.1x 认证，与 AP 建立关联关系。

WLAN 基本概念

- STA（无线终端）

  带有无线网卡的 PC 或便携式笔记本电脑等终端。
- AP（Access Point，接入点）

  AP 提供无线终端到局域网的桥接功能，在无线终端与无线局域网之间进行无线到有线和有线到无线的帧转换。
- SSID

  SSID（Service Set Identifier，服务组合识别码），无线终端可以先扫描所有网络，然后选择特定的 SSID 接入某个指定无线网络。
- 无线介质

  无线介质是用于在无线用户间传输帧的介质。WLAN 系统使用无线射频作为传输介质。
- 服务集（Service-Set）

  服务集是 WLAN 业务参数的集合，用户可以预先配置多个服务集，然后将其绑定到 AP 的某个射频上，实现 WLAN 业务的快速配置和下发。
- VAP（virtual Access Point，虚拟接入点）

  VAP 是 AP 上的业务功能实体。用户可以在 AP 的每个射频上创建不同的 VAP，通过为 AP 的指定射频绑定服务集，就可以创建 VAP。

1.2 AR1200 支持的 WLAN 特性

AR1200 支持的特性包括 WLAN 射频管理、WLAN 用户接入安全管理和 WLAN QoS 管理。

WLAN 射频管理

成功部署 WLAN 网络后，由于无线环境的不断变化，移动障碍物的存在，或者其他射频信号的干扰都会对无线信号传播质量造成影响。

此时，AP 的信道、发射功率等射频资源必须能够动态调整以适应用户环境的变化。而人工完成这个调整过程成本太高，所以在 WLAN 系统中，AP 负责完成无线射频资源管理。

AR1200 支持通过射频模板进行 WLAN 射频管理。

WLAN 用户接入安全管理

无线局域网由于信道开放的特点，使得攻击者能够很容易的进行窃听，恶意修改并转发。为了更好的防止未授权用户接入网络，WLAN 提供了一些安全策略。根据安全级别的不同，可以选择不同的安全策略。

AR1200 支持通过安全模板进行用户接入安全管理，支持 WEP、WPA/WPA2、WAPI 四种安全策略。

WLAN QoS 管理

WLAN QoS 保证不同质量的无线接入服务之间的互通，满足实际应用的需求。

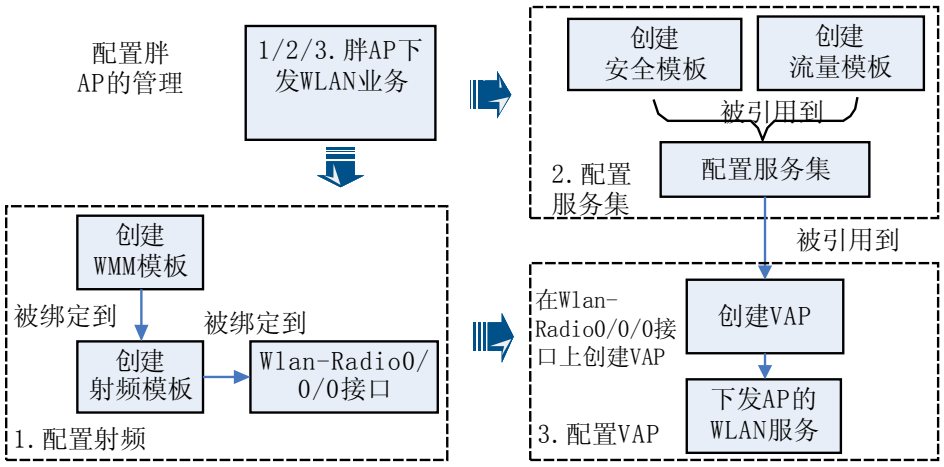
AR1200 支持通过创建 WMM 模板，流量模板进行 QoS 控制。

WLAN 业务配置流程

WLAN 业务的配置流程如图 1-2 所示，可以分为 3 个部分：

1. 配置 AP 的射频
2. 配置 AP 的服务集
3. 配置 VAP，下发 WLAN 服务

图 1-2 WLAN 业务的配置流程



1.3 配置 WLAN 射频

WLAN 系统使用无线射频作为传输介质，且无线通讯通过抢占信道来传输数据。为了保证不同质量的无线接入服务，需要进行 WLAN 射频的相关配置。

1.3.1 建立配置任务

在配置 WLAN 射频前了解 WLAN 射频的应用环境、前置任务和数据准备。

应用环境

WLAN 系统使用无线射频作为传输介质，且无线通讯通过抢占信道来传输数据。为了保证不同质量的无线接入服务，需要创建 WMM 模板并配置相应参数。另外，WLAN 系

统使用射频模板对射频参数进行配置。WMM 模板创建后需绑定到射频模板，随绑定的射频模板应用到射频中。

前置任务

在配置 WLAN 射频之前，需完成以下任务：

- WLAN 的基本功能已经配置完成，具体请参见 **1.4 配置 WLAN 业务**。

数据准备

在配置 WLAN 射频之前，需准备以下数据。

序号	数据
1	WMM 模板名称、（可选）WMM 模板 ID
2	（可选）WMM EDCA Client：AIFSN（空闲等待时长）、ECWmin 和 ECWmax（最小最大退避时间）、TXOPLimit（占用信道时长）
3	（可选）WMM EDCA AP：AIFSN（空闲等待时长）、ECWmin 和 ECWmax（最小最大退避时间）、TXOPLimit（占用信道时长）、ack-policy （ACK 策略）。
4	射频模板名称、（可选）射频模板 ID
5	AP ID、射频 ID、绑定的射频模板名称/或射频 ID
6	（可选）射频参数调优周期、调优的 AP 域 ID、定时调优时间

1.3.2 配置射频的 QoS 策略

配置射频的 QoS 策略，提供不同的信道抢占能力，实现不同的服务质量。

背景信息

配置射频 QoS 策略，需要创建 WMM 模板，然后将 WMM 模板绑定到射频模板。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 执行命令 **wmm-profile** { **id** *profile-id* | **name** *profile-name* } *，配置 WMM 模板。

WMM 模板创建成功后，模板内的参数均自动配置为缺省值。使用命令 **display wmm-profile** { **all** | **id** *profile-id* | **name** *profile-name* }，查看 WMM 模板配置的各项属性。

#创建 WMM 模板“wp”，所有配置均为缺省值。

```
[Huawei-wlan-view] display wmm-profile name wp
  Profile ID      : 2
```

```
Profile name    : wp
WMM switch      : enable
Client EDCA parameters:
-------------------------------------------------
       ECWmax  ECWmin  AIFSN  TXOPLimit
AC_VO  3       2       2      47
AC_VI  4       3       2      94
AC_BE  10      4       3      0
AC_BK  10      4       7      0
-------------------------------------------------
AP EDCA parameters:
-------------------------------------------------
       ECWmax  ECWmin  AIFSN  TXOPLimit  Ack-Policy
AC_VO  3       2       1      47         normal
AC_VI  4       3       1      94         normal
AC_BE  6       4       3      0          normal
AC_BK  10      4       7      0          normal
-------------------------------------------------
```

说明

终端和 AP 之间采用无线传输，通过占用信道来发送无线报文。为了实现不同报文获得不同级别的服务，我们将数据报文通过 4 个优先级队列发送，每个优先级队列占用信道的机会不一样。

四个优先级队列的名称和优先级顺序缺省为：AC_VO(语音) > AC_VI(视频) > AC_BE(尽力而为) > AC_BK(背景)。

四个优先级队列的优先级顺序并不是绝对的，可以通过参数修改来调整优先级顺序，这些参数称为 EDCA 参数(Enhanced Distributed Channel Access)。包括 AIFSN（arbitration inter Frame spacing number 仲裁帧间隙数）、ECWmin（exponetn form of CWmin 最小竞争窗口指数形式）、ECWmax (exponent form of CWmax 最大竞争窗口指数形式)、TXOPlimit（transmission opportunity limit 传输机会限制）以及 ack-policy （ACK 策略）。

- AIFSN：WMM 针对不同 AC 可以配置不同的空闲等待时长，AIFSN 数值越大，用户的空闲等待时间越长。
- ECWmin 和 ECWmax：这两个数值决定了平均退避时间值，数值越大，用户的平均退避时间越长。
- TXOPLimit：用户一次竞争成功后，可占用信道的最大时长，这个数值越大，用户一次能占用的信道时长越大，如果是 0，则每次占用信道后，只能发送一个报文。
- ack-policy：有 normal ack(应答)和 no ack(不应答)两种策略，缺省为 noraml ack。

占用信道发送报文的原理：终端在占用信道发送报文前，先监听信道，当信道空闲时间大于或等于空闲等待时间时，在竞争窗口范围内随即选择退避时间进行退避，最先结束退避的终端竞争到信道，开始发送报文。

步骤 4 （可选）执行命令 **wmm edca client** { **ac-vo** | **ac-vi** | **ac-be** | **ac-bk** } { **aifsn** *aifsn-value* | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* } *，配置终端上四个 WMM 队列的 EDCA 参数。

步骤 5 （可选）执行命令 **wmm edca ap** { **ac-vo** | **ac-vi** | **ac-be** | **ac-bk** } { **aifsn** *aifsn-value* | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* | **ack-policy** { **normal** | **noack** } } *，配置 AP 上四个 WMM 队列的 EDCA 参数。

----结束

1.3.3 配置射频模板

射频模板中可以配置射频类型、射频速率、射频功率模式、射频信道模式和绑定 WMM 模板，且只有绑定了 WMM 模板的射频模板才可以被射频绑定。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 执行命令 **radio-profile** { **id** *profile-id* | **name** *profile-name* } *，配置射频模板。

射频模板创建成功后，模板内的参数均自动配置为默认值。

执行命令 **display radio-profile** { **all** | **id** *profile-id* | **name** *profile-name* }，查看射频模板配置的各项属性。

```
[Huawei-wlan-radio-prof-radio-profile-1] display radio-profile name radio-profil
e-1
  ------------------------------------------------------------------------
  Profile ID                              :1
  Profile name                            :radio-profile-1
  Radio type                              :802.11b/g
  Rate mode                               :auto
  Rate(Mbps)                              :54
  Channel mode                            :auto
  Power mode                              :auto
  Calibrate interval(min)                 :720
  PER threshold(%)                        :30
  Conflict rate threshold(%)              :60
  RTS/CTS threshold(Byte)                 :2347
  Fragmentation threshold(Byte)           :2346
  Short retry number limit                :7
  Long retry number limit                 :4
  Support short preamble                  :support
  DTIM interval (Beacon interval numbers):3
  Beacon interval (time unit)             :1000
  WMM profile ID                          :-
  WMM profile name                        :-
  ------------------------------------------------------------------------
```

步骤 4 （可选）执行命令 **radio-type** { **80211gn** | **80211b** | **80211bg** | **80211bgn** | **80211g** | **80211n** }，配置射频模板的射频类型。

如果绑定了该模板的某个射频不支持新修改的射频类型，修改会失败。

步骤 5 （可选）执行命令 **rate auto max-rate rate-value** { **rate_1** | **rate_2** | **rate_5_5** | **rate_6** | **rate_9** | **rate_11** | **rate_12** | **rate_18** | **rate_22** | **rate_24** | **rate_33** | **rate_36** | **rate_48** | **rate_54** }，配置射频模板的速率参数。

步骤 6 （可选）执行命令 **power-mode** { **auto** | **fixed** }，配置射频模板的功率模式。

缺省情况下，功率模式为“auto”，即射频能够根据射频环境自动选择一个合适的值进行调整，无需用户指定。

步骤 7 （可选）执行命令 **channel-mode** { **auto** | **fixed** }，配置射频模板的信道模式。

缺省情况下，信道模式为“auto”，即射频能够根据射频环境自动选择一个合适的信道进行调整，无需用户指定。

步骤 8 执行命令 **wmm-profile** { **id** *profile-id* | **name** *profile-name* }，为射频模板绑定 WMM 模板。

说明

只有绑定了 WMM 模板的射频模板才可以被射频绑定。

----结束

1.3.4 在射频上绑定射频模板

为指定射频绑定射频模板，绑定成功后，射频模板参数会应用到该射频中。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface wlan-radio 0/0/0** ，进入射频视图。

步骤 3 执行命令 **radio-profile** { **id** *profile-id* | **name** *profile-name* }，为指定射频绑定射频模板。

----结束

1.3.5 （可选）配置 AP 射频资源管理

AP 的射频资源管理包括调整信道、传输功率和射频调优。

背景信息

当 WLAN 网络中的 AP 设备丢失，或者障碍物的阻挡会造成覆盖黑洞，AP 会周期性检测网络中是否有覆盖黑洞的存在并进行纠正。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 执行命令 **radio-profile** { **id** *profile-id* | **name** *profile-name* } *，配置射频模板。

射频模板创建成功后，模板内的参数均自动配置为缺省值。

步骤 4 执行命令 **channel-mode auto**，配置指定射频模板中的信道模式为自动模式，这样 AP 能够根据射频环境自动选择一个合适的信道进行调整，无需用户指定。

在 WLAN 网络运行期间，AP 会周期性测量网络环境，以判断是否调整 AP 信道以及如何调整 AP 信道。

步骤 5 执行命令 **power-mode auto**，配置指定射频模板中的功率模式为自动模式，这样 AP 能够根据射频环境自动选择一个合适的值进行调整，无需用户指定。

在 WLAN 网络运行期间，AP 会周期性采集邻居信息，判断是否需要调整 AP 的传输功率，以完整覆盖 WLAN 区域。

步骤 6 执行命令 **calibrate-interval** *calibrate-interval*，配置指定射频模板中的射频参数调优周期，启动 AP 域内局部调优。

调优的目的是为了使射频下用户之间发射功率不受干扰。配置调优周期后，将按调优周期定时检测周围信号环境，如果信号环境恶化则启动局部调优。

----结束

1.3.6 检查配置结果

WLAN 射频配置成功后，可查看 WLAN 射频的相关信息。

操作步骤

步骤 1 执行命令 **display wmm-profile** { **all** | **id** *profile-id* | **name** *profile-name* }，查看 WMM 模板信息。

步骤 2 执行命令 **display radio-profile** { **all** | **id** *profile-id* | **name** *profile-name* }，查看射频模板信息。

步骤 3 执行命令 **display binding radio-profile** { **id** *profile-id* | **name** *profile-name* }，查看指定射频模板的绑定关系。

步骤 4 执行命令 **display actual channel-power interface wlan-radio0/0/0**，查看当前实际的信道和功率值。

步骤 5 执行命令 **display radio config interface wlan-radio0/0/0**，查看射频的当前配置信息。

----结束

1.4 配置 WLAN 业务

AP 正常工作后，AP 根据 VAP 的参数配置提供给用户不同的业务。

1.4.1 建立配置任务

在配置 WLAN 业务前了解 WLAN 业务的应用环境、前置任务和数据准备。

应用环境

用户想通过无线方式接入以太网络时，需要配置 WLAN 业务。WLAN 业务的配置流程请参见 **1.2 AR1200 支持的 WLAN 特性**一节的“WLAN 业务配置流程”介绍。

前置任务

在配置 WLAN 业务之前，需完成以下任务：

- WLAN 射频已经配置完成，具体请参见 **1.3 配置 WLAN 射频**。

数据准备

在配置 WLAN 业务之前，需准备以下数据。

序号	数据
1	WLAN-BSS 接口编号、
2	安全模板名称、（可选）安全模板 ID。根据选择的安全策略，进行不同的数据准备： ● WEP 共享密钥认证：密钥值、密钥索引 ● WPA/WPA2 共享密钥认证：密钥值 ● WAPI 认证：AC 的证书文件、AC 证书颁布者的证书以及 ASU 的证书文件、ASU 服务器的 IP 地址、（可选）BK 更新间隔/生存期百分比、（可选）MSK 更新间隔、MSK 更新报文数和 MSK 密钥协商报文重传次数、（可选）证书认证鉴别报文的重传次数

序号	数据
3	流量模板名称、（可选）流量模板 ID、（可选）up-map-8021p 映射值、（可选）8021p-map-up 映射值、（可选）报文限速速率
4	服务集名称、（可选）服务集 ID，绑定的安全模板名称/ID、绑定的流量模板名称/ID
5	绑定的服务集名称/ID、（可选）WLAN 索引

1.4.2 配置 WLAN-BSS 接口

无线侧的 802.11 报文到达 AP 后，需要通过 WLAN-BSS 接口将报文送至 WLAN 业务处理模块。WLAN-BSS 接口下可以配置接口优先级、接口下的认证方式等参数。

背景信息

WLAN-BSS 是一种虚拟的二层接口，类似于 Access 类型的二层以太网接口，具有二层属性，并可配置多种二层协议。

创建 WLAN-BSS 接口后，需要在服务集下绑定该接口。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface wlan-bss** *wlan-bss-number*，创建 WLAN-BSS 接口。

步骤 3 执行命令**{ dot1x-authentication | mac-authentication } enable**，配置 WLAN-BSS 接口下接入用户的认证方式。

说明

- 如果接入安全策略采用 WPA/WPA2 dot1x 认证，必须在接口下执行 **dot1x-authentication enable** 。
- 如果接入安全策略采用 WPA/WPA2 PSK 认证，无需执行 **dot1x-authentication enable** 命令。
- **mac-authentication** 只能和 WPA/WPA2 PSK 结合起来用，即 WLAN 用户上线后，先进行 MAC 认证，再进行 WPA/WPA2 PSK 认证。

步骤 4 执行命令 **dot1x authentication-method** { **chap** | **pap** | **eap** }，配置 dot1x 的认证方式。

缺省情况下，使用 **chap** 认证方式。

说明

dot1x 的认证方式为 **chap** 或者 **pap** 时，不支持配置端口所在的 guest-vlan 和 restrict-vlan。

步骤 5 （可选）执行命令 **dot1x authentication domain** *domain-name*,用于在 WLAN-BSS 接口上绑定 AAA 域。

----结束

1.4.3 配置用户接入安全策略

配置用户接入 WLAN 网络使用的安全策略。

背景信息

WLAN 接入安全策略有 4 种，分别为 WEP 认证、WPA 认证、WPA2 认证和 WAPI 认证。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 执行命令 **security-profile** { **id** *profile-id* | **name** *profile-name* } *，配置用户的接入安全模板。

模板创建后，缺省配置如下：

- 对于 WEP：缺省配置为开放系统认证方式+空密钥。
- 对于 WPA1：缺省配置为 802.1x+PEAP 认证方式+TKIP 数据加密方式。
- 对于 WPA2：缺省配置为 802.1x+PEAP 认证方式+CCMP 数据加密方式。
- 对于 WAPI：缺省配置为 WAI 认证方式+WPI 数据加密方式。

步骤 4 配置各种安全策略：

- WEP 开放系统认证
  1. 执行命令 **security-policy wep**，配置安全策略为 **wep** 方式。
  2. 执行命令 **wep authentication-method open-system** [**data-encrypt**]，配置使用 WEP 开放系统认证。
- WEP 共享密钥认证
  1. 执行命令 **security-policy wep**，配置安全策略为 **wep** 方式。
  2. 执行命令 **wep authentication-method share-key**，配置使用 WEP 共享密钥认证。
  3. 执行命令 **wep key** { **wep-40** | **wep-104** } { **pass-phrase** | **hex** } *key-id key-value*，配置 WEP 的共享密钥。

     WEP-40 方式下：10 个十六进制或者 5 个 ASCII 字符；WEP-104 方式下：26 个十六进制或者 13 个 ASCII 字符。
  4. 执行命令 **wep default-key** *key-id*，配置 WEP 使用的密钥索引。

     WEP 的密钥可以配置 4 个，在认证或者加密时只使用一个，使用此命令来指定使用哪一个密钥。
- WPA/WPA2 认证
  1. 执行命令 **security-policy wpa**，配置安全策略为 **wpa** 方式。
  2. 执行命令**{ wpa | wpa2 } authentication-method dot1x** { **peap** | **tls** } **encryption-method** { **tkip** | **ccmp** }，配置 WPA/WPA2 使用 dot1x 认证方式和相应的加密方式。

     说明

     如果接入安全策略采用 WPA/WPA2 dot1x 认证，必须在 WLAN-BSS 接口下执行 **dot1x-authentication enable**。
  3. 执行命令**{ wpa | wpa2 } authentication-method psk** { **pass-phrase** | **hex** } *key* **encryption-method** { **tkip** | **ccmp** }，配置 WPA/WPA2 使用共享密钥认证方式和相应的加密方式。

- WAPI 认证
  1. 执行命令 **security-policy wapi**，配置安全策略为 **wapi** 方式。
  2. 执行命令 **wapi authentication-method** { **certificate** | **psk** { **pass-phrase** | **hex** } *key* }，配置 WAPI 使用的认证方式。

     WAPI 的认证方式支持基于证书和基于预共享密钥两种，当用户选择基于预共享密钥时，需要输入共享密钥。
  3. 执行命令 **wapi import certificate** { **ap** | **asu** | **issuer** } **file-name** *file_name*，导入 AP 的证书文件、AP 证书颁布者的证书以及 ASU 的证书文件。
  4. 执行命令 **wapi import private-key file-name** *file_name*，导入 AP 的私钥文件。
  5. 执行命令 **wapi asu ip** *ip-address*，配置 ASU 服务器的 IP 地址。
  6. （可选）执行如下命令修改 WAPI 的参数：
     - 执行命令 **wapi** { **bk-threshold** *bk-threshold* | **bk-update-interval** *bk-interval* }，配置 BK 更新间隔、生存期百分比。

       缺省情况下，BK 的更新间隔为 43200s，生存期百分比为 70%。
     - 执行命令 **wapi** { **msk-update-interval** *msk-interval* | **msk-update-packet** *msk-packet* | **msk-retrans-count** *msk-count* }，配置 MSK 更新间隔、MSK 更新报文数和 MSK 密钥协商报文重传次数。

       缺省情况下，MSK 更新间隔为 86400s，MSK 更新报文数为 10000，MSK 密钥协商报文重传次数为 3 次。
     - 执行命令 **wapi cert-retrans-count** *cert-count*，配置证书认证鉴别报文的重传次数。

       缺省情况下，重传次数为 3 次。
     - 执行命令 **wapi** { **usk** | **msk** } **key-update** { **disable** | **time-based** | **packet-based** | **timepacket-based** }，配置 WAPI 的 USK 和 MSK 的更新方式。

       缺省情况下，USK 和 MSK 都是基于时间更新。

----结束

1.4.4 配置流量模板

当需要为某个 VAP 定制特定的优先级映射、流量抑制等功能时，创建相应的流量模板并绑定到服务集中。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 执行命令 **traffic-profile** { **name** *profile-name* | **id** *profile-id* } *，配置流量模板。

流量模板创建成功后，模板内的参数均为缺省值。执行命令 **display traffic-profile** { **all** | **id** *profile-id* | **name** *profile-name* }，查看各项属性的缺省配置。

#查看 Traffic 模板“traffic-profile-1”的各项属性。

```
[Huawei-wlan-view] display traffic-profile name traffic-profile-1
  Profile ID         : 3
  Profile name       : traffic-profile-1
  Client Limit Rate  : 4294967295 Kbps(up)
                     : 4294967295 Kbps(down)
```

```
VAP Limit Rate     : 4294967295 Kbps(up)
                   : 4294967295 Kbps(down)
802.1p Mapping Mode: mapping
-----------------------------
User-priority  802.1p
0              0
1              1
2              2
3              3
4              4
5              5
6              6
7              7
-----------------------------
802.1p to User-priority Mapping List:
-----------------------------
802.1p  User-priority
0       0
1       1
2       2
3       3
4       4
5       5
6       6
7       7
-----------------------------
Tunnel priority(up) Mapping Mode:ToS(inner) to ToS(outer)
-----------------------------
ToS(inner)     ToS(outer)
0              0
1              1
2              2
3              3
4              4
5              5
6              6
7              7
-----------------------------
Tunnel priority(down) Mapping Mode:ToS(inner) to ToS(outer)
-----------------------------
ToS(inner)     ToS(outer)
0              0
1              1
2              2
3              3
4              4
5              5
6              6
7              7
-----------------------------
```

说明

STA 发出的 802.11 报文要通过 AP 进入以太网时，需要转换成 802.3 报文，这期间可以不进行优先级映射，也可以按照不同的 VAP 设置不同的优先级，或按照 UP（用户优先级）映射到优先级。

802.3 报文通过 AP 转发给 STA 时，被转换成 802.11 报文，其中的 UP 域可以根据 DSCP、CoS 映射而来，或者由流分类设置。

步骤 4 （可选）执行命令 **8021p** { **designate** *value* | **up-mapping** *value0 value1 value2 value3 value4 value5 value6 value7* }，配置 AP 的上行 802.3 报文的 802.1p 优先级值。

STA 发送 802.11 报文后，在 AP 上终结，同时构造 802.3 报文上行。为保证报文在 AP 转发时能够得到一定的服务质量，需要填充其优先级值以便调度。

步骤 5 （可选）执行命令 **8021p-map-up** *value0 value1 value2 value3 value4 value5 value6 value7*，配置下行时 802.1p 优先级值到用户优先级值的映射关系。

步骤 6 （可选）执行命令 **rate-limit** { **client** | **vap** } { **up** | **down** } *ratelimit-value*，限制单个终端或整个 VAP 内所有终端的无线侧上下行报文速率。

----结束

1.4.5 配置 WLAN 服务集

服务集（service-set）是业务层面的关键参数集，服务集应绑定安全模板和流量模板。

前提条件

安全模板和流量模板已经配置完成。

背景信息

服务集是一个业务参数集合。当它被绑定到指定 AP 的指定射频上时，即将它所有的业务参数应用到无线业务功能实体 VAP（Virtual Access Point）上。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 执行命令 **service-set** { **name** *service-set-name* | **id** *service-set-id* } *，配置服务集。

步骤 4 执行命令 **ssid** *ssid*，指定服务集中的 SSID。

步骤 5 （可选）执行命令 **ssid-hide**，配置 Beacon 帧中隐藏 SSID。

步骤 6 执行命令 **security-profile** { **name** *profile-name* | **id** *profile-id* } *，服务集下绑定安全模板。

步骤 7 执行命令 **traffic-profile** { **name** *profile-name* | **id** *profile-id* } *，服务集下绑定流量模板。

说明

服务集下绑定的安全模板和流量模板，对使用该服务集的所有用户起作用。

步骤 8 执行命令 **wlan-bss**，服务集下绑定 wlan-bss 接口。

----结束

1.4.6 配置 VAP

VAP 下发 AP 时，与 VAP 绑定的服务集参数作为 VAP 的参数一起下发到 AP，AP 根据 VAP 配置的参数提供给用户不同的业务。

前提条件

- 指定射频上已经绑定了射频模板，具体请参见 **1.3.4 在射频上绑定射频模板**。
- 服务集已经创建并配置好参数，具体请参见 **1.4.5 配置 WLAN 服务集**。

背景信息

VAP 是 AP 上的业务功能实体。用户可以在 AP 的射频口上创建不同的 VAP，通过为 AP 的射频口绑定服务集和射频模板，就可以创建 VAP。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **interface Wlan-Radio 0/0/0** ，进入射频视图。

步骤 3 执行命令 **service-set** { **name** *service-set-name* | **id** *service-set-id* } [**wlan** *wlan-id*]，绑定服务集。

----结束

1.4.7 检查配置结果

WLAN 业务配置完成后，可以查看 WLAN 业务相关的配置信息。

操作步骤

步骤 1 执行命令 **display vap** ，查看 VAP 信息。

步骤 2 执行命令 **display security-profile** { **all** | { **id** *profile-id* | **name** *profile-name* } [**detail**] }，查看安全模板信息。

步骤 3 执行命令 **display traffic-profile** { **all** | **id** *profile-id* | **name** *profile-name* }，查看流量模板信息。

步骤 4 执行命令 **display service-set** { **all** | **id** *service-set-id* | **name** *service-set-name* | **ssid** *ssid* }，查看服务集信息。

----结束

1.5 维护

介绍如何复位 AP。

1.5.1 复位 AP

当 AP 工作不正常时，可能需要对其复位。

背景信息

注意

AP 复位会中断业务，请谨慎使用。

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 执行命令 **ap-reset** ，进行 AP 复位。

----结束

1.6 配置举例

1.6.1 配置 WLAN 基本业务示例

组网需求

如图 1-3 所示，企业使用 WLAN 技术为用户提供方便的无线上网服务。其中，AR1200 作为 FAT AP，提供用户无线接入 Internet 功能，同时作为 DHCP Server 给用户分配 IP 地址。

图 1-3 配置 WLAN 基本业务示例图

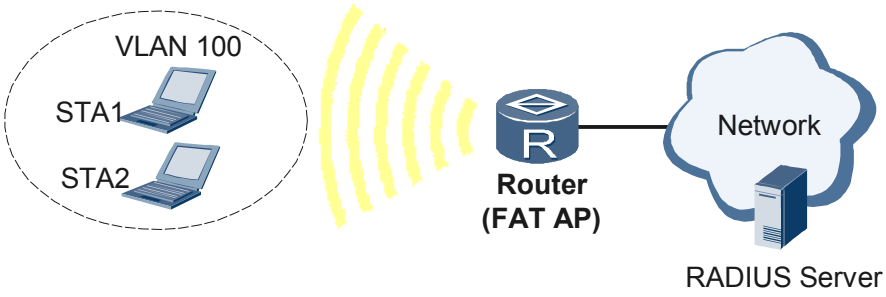


表 1-1 数据规划表

配置项	数据
WLAN 服务	WEP Open-System 认证，不加密。
服务集	● Name：Huawei-1 ● SSID：Huawei-1 ● WLAN 虚接口：WLAN-BSS 1
WLAN 用户 VLAN	VLAN：100
AR1200 的国家码	CN（中国）
DHCP 服务器	AR1200 作为 DHCP 服务器，为用户分配地址。 VLANIF100：192.168.0.1/24

配置思路

AR1200 作为 FAT AP，提供 WLAN 基本上网业务的配置思路如下：

1. 配置 AR1200 的基本功能，包括配置国家码、DHCP Server，实现为用户分配 IP 地址功能。

2. 配置 WLAN-BSS 接口，并在服务集下绑定该接口，实现无线侧报文到达 AR1200 后能够送至 WLAN 业务处理模块功能。
3. 配置 AR1200 对应的射频模板，并在射频口下绑定该模板，实现 STA 与 AR1200 之间的无线通信参数配置。
4. 配置 AR1200 对应的服务集，并在服务集下绑定安全模板、流量模板，实现 STA 接入网络安全策略及 QoS 控制。
5. 配置 VAP，实现 STA 访问 WLAN 网络功能。

操作步骤

步骤 1 配置 AR1200 的基本功能。

#配置 AR1200 的国家码，方便识别和管理。

```
<Huawei> system-view
[Huawei] wlan global country-code cn
```

#创建 VLANIF 接口，配置 IP 地址作为数据转发的三层接口，使能 DHCP 服务功能。接口 VLANIF100 为 STA 分配 IP 地址。

```
[Huawei] dhcp enable
[Huawei] vlan 100
[Huawei-vlan100] quit
[Huawei] interface vlanif100
[Huawei-Vlanif100] ip address 192.168.0.1 24
[Huawei-Vlanif100] dhcp select interface
[Huawei-Vlanif100] quit
```

步骤 2 配置 WLAN-BSS 虚接口。

```
[Huawei] interface wlan-bss 1
[Huawei-Wlan-Bss1] port hybrid tagged vlan 100
[Huawei-Wlan-Bss1] quit
```

步骤 3 配置 AR1200 对应的射频。

#创建名为“wmm-1”的 WMM 模板，参数采用缺省配置。

```
[Huawei] wlan
[Huawei-wlan-view] wmm-profile name wmm-1 id 1
[Huawei-wlan-wmm-prof-wmm-1] quit
```

#创建名为“radio-1”的射频模板，绑定 WMM 模板“wmm-1”。

```
[Huawei-wlan-view] radio-profile name radio-1
[Huawei-wlan-radio-prof-radio-1] wmm-profile name wmm-1
[Huawei-wlan-radio-prof-radio-1] quit
```

#将射频口绑定射频模板“radio-1”。

```
[Huawei] interface wlan-radio 0/0/0
[Huawei-Wlan-Radio0/0/0] radio-profile name radio-1
[Huawei-Wlan-Radio0/0/0] quit
```

步骤 4 配置 AP 对应的服务集。

#创建安全模板。

安全模板名为“security-1”，认证模式为 WEP 认证，开放认证，不加密。

```
[Huawei] wlan
[Huawei-wlan-view] security-profile name security-1 id 1
[Huawei-wlan-sec-prof-security-1] wep authentication-method open-system
[Huawei-wlan-sec-prof-security-1] security-policy wep
[Huawei-wlan-sec-prof-security-1] quit
```

#配置 QoS 策略，创建流量模板。

流量模板名为“traffic-1”，参数采用缺省配置。

```
[Huawei-wlan-view] traffic-profile name traffic-1
[Huawei-wlan-traffic-prof-traffic-1] quit
```

#创建服务集，并绑定流量模板及安全模板、WLAN-BSS 接口。

```
[Huawei-wlan-view] service-set name huawei-1
[Huawei-wlan-service-set-huawei-1] ssid huawei-1
[Huawei-wlan-service-set-huawei-1] traffic-profile name traffic-1
[Huawei-wlan-service-set-huawei-1] security-profile name security-1
[Huawei-wlan-service-set-huawei-1] wlan-bss 1
[Huawei-wlan-service-set-huawei-1] quit
```

步骤 5 配置 VAP。

#将射频口绑定服务集“Huawei-1”。

```
[Huawei] interface wlan-radio 0/0/0
[Huawei-Wlan-Radio0/0/0] service-set name huawei-1
[Huawei-Wlan-Radio0/0/0] quit
```

步骤 6 验证配置结果

无线接入用户可以搜索到 SSID 标识为 huawei-1 的 WLAN 网络，无需验证即可以正常使用 WLAN 上网服务。

----结束

配置文件

```
#
 sysname Huawei
#
 vlan 100
#
 dhcp enable
#
 wlan global country-code cn
#
interface Vlanif100
 ip address 192.168.0.1 255.255.255.0
 dhcp select interface
#
interface Wlan-Bss1
 port hybrid tagged vlan 100
#
wlan
 wmm-profile name wmm-1 id
1
 traffic-profile name traffic-1 id
1
 security-profile name security-1 id
1
 service-set name huawei-1 id 1
  wlan-bss 1
  ssid huawei-1
  traffic-profile id
1
 radio-profile name radio-1 id 1
  wmm-profile id 1
 #
interface Wlan-Radio0/0/0
 service-set name huawei-1
```

```
#
return
```

2 WLAN 安全配置

关于本章

介绍胖 AP 组网模式下 WLAN 安全特性的配置过程。

2.1 WLAN 安全简介

2.2 AR1200 支持的 WLAN 安全特性
AR1200 支持的 WLAN 安全特性包括接入安全策略管理、STA(Station)黑白名单管理及用户隔离管理。

2.3 配置用户接入安全策略
配置接入安全策略即根据网络情况配置用户接入 WLAN 设备采用的认证方式。

2.4 配置 STA 黑白名单
通过配置 STA 黑白名单功能，实现更简单、更灵活的控制某个 AP 下的 STA 接入 WLAN 网络。

2.5 配置示例

2.1 WLAN 安全简介

802.11 协议提供的无线安全性很好地抵御一般性网络攻击，但是仍有少数黑客能够入侵无线网络，从而无法充分保护包含敏感数据的网络。为了更好的防止未授权用户接入网络，需要实施性能高于 802.11 认证的高级安全机制。安全性高于 802.11 认证的 WLAN 安全机制有以下几种：链路认证方式、WLAN 服务的数据安全和用户接入认证。

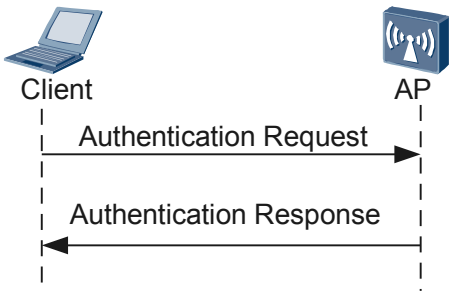
链路认证方式

- 开放系统认证（Open System Authentication）

  开放系统认证是缺省使用的认证机制，也是最简单的认证算法，即不认证。如果认证类型设置为开放系统认证，则所有请求认证的客户端都会通过认证。开放系统认证包括两个步骤：

  1. 无线客户端发起认证请求；
  2. AP 确定无线客户端可以通过无线链路认证，并向无线客户端回应认证结果为“成功”。

  图 2-1 开放系统认证过程

- 共享密钥认证（Shared key authentication）

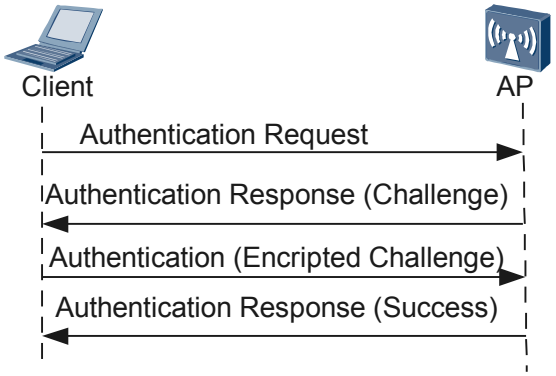
  共享密钥认证是除开放系统认证以外的另外一种认证机制。共享密钥认证需要无线客户端和无线设备端配置相同的共享密钥。

  共享密钥认证的认证过程为：

  1. 无线客户端先向无线设备端发送认证请求，无线设备端会随机产生一个 Challenge 包（即一个字符串）发送给客户端。
  2. 无线客户端会将接收到的字符串拷贝到新的消息中，用密钥加密后再发送给无线设备端。
  3. 无线设备端接收到该消息后，用密钥将该消息解密，然后对解密后的字符串和最初给客户端的字符串进行比较。

     如果相同，则说明客户端拥有无线设备端相同的共享密钥，即通过了 Shared Key 认证，否则 Shared Key 认证失败。

图 2-2 共享密钥认证过程



WLAN 服务的数据安全

相对于有线网络，WLAN 网络存在着与生俱来的数据安全问题。在一个区域内的所有的 WLAN 设备共享一个传输媒介，任何一个设备可以接收到其他所有设备的数据，这个特性直接威胁到 WLAN 接入数据的安全。

802.11 协议也在致力于解决 WLAN 的安全问题，主要的方法为对数据报文进行加密，保证只有特定的设备可以对接收到的报文成功解密。其他的设备虽然可以接收到数据报文，但是由于没有对应的密钥，无法对数据报文解密，从而实现了 WLAN 数据的安全性保护。

目前支持的加密方式有 RC4 加密、TKIP 加密和 CCMP 加密。

用户接入认证

- PSK 认证

  PSK 认证需要在无线客户端和设备端配置相同的预共享密钥，如果密钥相同，PSK 接入认证成功；如果密钥不同，PSK 接入认证失败。

- 802.1x 认证

  802.1x 协议是一种基于端口的网络接入控制协议。“基于端口的网络接入控制”是指在 WLAN 接入设备的端口这一级对所接入的用户设备进行认证和控制。连接在端口上的用户设备如果能通过认证，就可以访问 WLAN 中的资源；如果不能通过认证，则无法访问 WLAN 中的资源。

- MAC 接入认证

  MAC 地址认证是一种基于端口和 MAC 地址对用户的网络访问权限进行控制的认证方法，它不需要用户安装任何客户端软件。设备在首次检测到用户的 MAC 地址以后，即启动对该用户的认证操作。

2.2 AR1200 支持的 WLAN 安全特性

AR1200 支持的 WLAN 安全特性包括接入安全策略管理、STA(Station)黑白名单管理及用户隔离管理。

接入安全策略管理

接入安全策略管理即根据网络情况配置用户接入 WLAN 设备采用的认证方式。

AR1200 支持 WEP（Wired Equivalent Privacy）、WPA（Wi-Fi Protected Access）、WPA2 和 WAPI（WLAN Authentication and Privacy Infrastructure）四种接入安全策略。

STA 黑白名单

AR1200 通过将 STA 加入到黑白名单列表中，对 STA 的接入模式进行控制。

- 使能黑名单功能后，如果 STA 匹配黑名单列表，则该 STA 无法关联上 AP，从而无法访问无线网络。
- 使能白名单功能后，如果 STA 匹配白名单列表，则该 STA 可以关联上 AP，从而访问无线网络，而不在白名单内的 STA 将无法访问无线网络。

用户隔离

用户隔离功能是指关联到同一个 AP 上的所有无线用户之间的二层报文相互不能转发，从而使无线用户之间不能直接进行通讯。

AR1200 支持通过在服务集下配置用户隔离、及在 WLAN-BSS 口下配置端口隔离两种方式，实现关联到同一 AP 上的无线用户的二层隔离功能。

2.3 配置用户接入安全策略

配置接入安全策略即根据网络情况配置用户接入 WLAN 设备采用的认证方式。

应用环境

无线局域网由于信道开放的特点，使得攻击者能够很容易的进行窃听，用户信息被恶意的修改并转发。为了更好的防止未授权用户接入网络，WLAN 提供了一些安全策略。根据安全级别的不同，可以选择不同的安全策略。

- WEP 为早期的安全策略方案，存在一定的安全风险，可应用在安全要求不高的开放场合，如机场、车站等。
- WPA 和 WAPI 为安全性较高的安全策略，可为系统提供较高的安全保护。

数据准备

在配置用户接入安全策略之前，需准备以下数据。

序号	数据
1	安全模板名称、（可选）安全模板 ID
2	WEP 共享密钥、密钥索引
3	WPA/WPA2 共享密钥
4	●（采用共享密钥认证）WAPI 共享密钥 ●（采用证书认证）AP 的证书文件和私钥文件、AP 证书颁布者的证书以及 ASU 的证书文件名、ASU 服务器的 IP 地址。

序号	数据
5	（可选）BK（Base Key）更新间隔、生存期百分比；MSK 更新间隔、MSK 更新报文数和 MSK 密钥协商报文重传次数；证书认证鉴别报文的重传次数

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 执行命令 **security-profile** { **id** *profile-id* | **name** *profile-name* } *，配置用户的接入安全模板。

模板创建后，缺省配置如下：

- 对于 WEP：缺省配置为开放系统认证方式+空密钥。
- 对于 WPA1：缺省配置为 802.1x+PEAP 认证方式+TKIP 数据加密方式。
- 对于 WPA2：缺省配置为 802.1x+PEAP 认证方式+CCMP 数据加密方式。
- 对于 WAPI：缺省配置为 WAI 认证方式+WPI 数据加密方式。

步骤 4 配置各种安全策略：

- WEP 开放系统认证
  1. 执行命令 **security-policy wep**，配置安全策略为 **wep** 方式。
  2. 执行命令 **wep authentication-method open-system** [**data-encrypt**]，配置使用 WEP 开放系统认证。
- WEP 共享密钥认证
  1. 执行命令 **security-policy wep**，配置安全策略为 **wep** 方式。
  2. 执行命令 **wep authentication-method share-key**，配置使用 WEP 共享密钥认证。
  3. 执行命令 **wep key** { **wep-40** | **wep-104** } { **pass-phrase** | **hex** } *key-id key-value*，配置 WEP 的共享密钥。

     WEP-40 方式下：10 个十六进制或者 5 个 ASCII 字符；WEP-104 方式下：26 个十六进制或者 13 个 ASCII 字符。
  4. 执行命令 **wep default-key** *key-id*，配置 WEP 使用的密钥索引。

     WEP 的密钥可以配置 4 个，在认证或者加密时只使用一个，使用此命令来指定使用哪一个密钥。
- WPA/WPA2 认证
  1. 执行命令 **security-policy wpa**，配置安全策略为 **wpa** 方式。
  2. 执行命令**{ wpa | wpa2 } authentication-method dot1x** { **peap** | **tls** } **encryption-method** { **tkip** | **ccmp** }，配置 WPA/WPA2 使用 dot1x 认证方式和相应的加密方式。

说明

如果接入安全策略采用 WPA/WPA2 dot1x 认证，必须在 WLAN-BSS 接口下执行 **dot1x-authentication enable** 。

WPA 与 WPA2 认证的不同点主要表现在协议报文格式上，安全性上几乎没有差别。

3. 执行命令**{ wpa | wpa2 } authentication-method psk** { **pass-phrase** | **hex** } *key* **encryption-method** { **tkip** | **ccmp** }，配置 WPA/WPA2 使用共享密钥认证方式和相应的加密方式。

- WAPI 认证

1. 执行命令 **security-policy wapi** ，配置安全策略为 **wapi** 方式。
2. 执行命令 **wapi authentication-method** { **certificate** | **psk** { **pass-phrase** | **hex** } *key* }，配置 WAPI 使用的认证方式。

   WAPI 的认证方式支持基于证书和基于预共享密钥两种，当用户选择基于预共享密钥时，需要输入共享密钥。
3. 执行命令 **wapi import certificate** { **ap** | **asu** | **issuer** } **file-name** *file_name*，导入 AP 的证书文件、AP 证书颁布者的证书以及 ASU 的证书文件。
4. 执行命令 **wapi import private-key file-name** *file_name*，导入 AP 的私钥文件。
5. 执行命令 **wapi asu ip** *ip-address*，配置 ASU 服务器的 IP 地址。
6. （可选）执行如下命令修改 WAPI 的参数：
   - 执行命令 **wapi** { **bk-threshold** *bk-threshold* | **bk-update-interval** *bk-interval* }，配置 BK 更新间隔、生存期百分比。

     缺省情况下，BK 的更新间隔为 43200s，生存期百分比为 70%。
   - 执行命令 **wapi** { **msk-update-interval** *msk-interval* | **msk-update-packet** *msk-packet* | **msk-retrans-count** *msk-count* }，配置 MSK 更新间隔、MSK 更新报文数和 MSK 密钥协商报文重传次数。

     缺省情况下，MSK 更新间隔为 86400s，MSK 更新报文数为 10000，MSK 密钥协商报文重传次数为 3 次。
   - 执行命令 **wapi cert-retrans-count** *cert-count*，配置证书认证鉴别报文的重传次数。

     缺省情况下，重传次数为 3 次。
   - 执行命令 **wapi** { **usk** | **msk** } **key-update** { **disable** | **time-based** | **packet-based** | **timepacket-based** }，配置 WAPI 的 USK 和 MSK 的更新方式。

     缺省情况下，USK 和 MSK 都是基于时间更新。

----结束

检查配置结果

执行命令 **display security-profile** { **all** | { **id** *profile-id* | **name** *profile-name* } [**detail**] }，查看配置的安全模板信息。

查询单个模板的详细信息。

```
<Huawei> display security-profile id 0 detail
  ------------------------------------------------------------
  Profile name                    : lw
  Profile ID                      : 0
  Authentication                  : Share key
  Encryption                      : WEP-40
  ------------------------------------------------------------
  Service-set ID                  SSID
```

```
0                                   100129796_9300
1                                   100129796_93002
-------------------------------------------------------------
WEP's configuration
Authentication                      : Share key
Encryption                          : WEP-40
Key 0                               : *****
Key 1                               : Empty
Key 2                               : Empty
Key 3                               : Empty
Default key ID                      : 0
-------------------------------------------------------------
WPA's configuration
Authentication                      : WPA  802.1x + PEAP
Encryption                          : TKIP
-------------------------------------------------------------
WPA2's configuration
Authentication                      : WPA2 802.1x + PEAP
Encryption                          : CCMP
-------------------------------------------------------------
WAPI's configuration
CA certificate filename             : -
ASU certificate filename            : -
AC certificate filename             : -
AC private key filename             : -
Authentication server IP            : -
Authentication method               : WAPI PSK
WAI timeout(s)                      : 60
BK update interval(s)               : 43200
BK lifetime threshold(%)            : 70
USK update interval(s)              : 600
USK update packet(k)                : 10
MSK update interval(s)              : 86400
MSK update packet(k)                : 10
Cert auth retrans count             : 3
USK negotiate retrans count         : 3
MSK negotiate retrans count         : 3
USK update method                   : Time-based
MSK update method                   : Time-based
-------------------------------------------------------------
```

2.4 配置 STA 黑白名单

通过配置 STA 黑白名单功能，实现更简单、更灵活的控制某个 AP 下的 STA 接入 WLAN 网络。

应用环境

用户如果想让某些 STA 不能访问 WLAN 网络，可以将其加入 STA 黑名单列表中；如果仅想让某些 STA 访问 WLAN 网络，可以将其加入 STA 白名单列表中。

前置任务

在配置 STA 黑白名单之前，需完成以下任务：

- WLAN 的基本功能已经配置完成，具体请参见 **1.4 配置 WLAN 业务**。

数据准备

在配置 STA 黑白名单之前，需准备以下数据。

序号	数据
1	AP ID 号、STA 的 MAC 地址

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 配置黑白名单

- 配置黑名单
  1. 执行命令 **sta-access-mode** { **blacklist** | **whitelist** | **disable** }，配置 STA 接入控制模式为 **blacklist**。

     缺省情况下，STA 接入控制模式为 **disable**。
  2. 执行命令 **sta-blacklist** *mac-address*，配置 STA 黑名单。
- 配置白名单
  1. 执行命令 **sta-access-mode** { **blacklist** | **whitelist** | **disable** }，配置 STA 接入控制模式为 **whitelist**。

     缺省情况下，STA 接入控制模式为 **disable**。
  2. 执行命令 **sta-whitelist** *mac-address*，配置 STA 白名单。

----结束

检查配置结果

- 执行命令 **display sta-access-mode** ，查看 STA 接入控制模式。

  查询 STA 接入控制模式。

```
<Huawei> display sta-access-mode
  Station access control mode: disable
```

- 执行命令 **display sta-blacklist**，查看 STA 黑名单列表。

  查询黑名单信息。

```
<Huawei> display sta-blacklist
  Station mac global black list information:
  ------------------------------------------------------------------------------
  ID        MAC
  ------------------------------------------------------------------------------
  0         0026-0000-90a1
  1         0026-0000-909f
  ------------------------------------------------------------------------------
  Total number: 2
```

- 执行命令 **display sta-whitelist**，查看 STA 白名单列表。

  查询白名单信息。

```
<Huawei> display sta-whitelist
  Station mac global white list information:
  ------------------------------------------------------------------------------
  ID        MAC
  ------------------------------------------------------------------------------
  0         0025-9e26-b9bd
  1         001e-907a-b6a6
  2         0026-0000-90a1
```

```
-------------------------------------------------------------------------------
Total number: 3
```

2.5 配置示例

2.5.1 配置接入安全策略的业务示例

组网需求

如图 2-3 所示，AR1200 作为 FAT AP，为接入用户提供 WLAN 服务，用户可以搜索到 5 个无线网络，要求：

- SSID 为 huawei-1 的无线网络的 WLAN 服务采用开放式系统认证+不加密。
- SSID 为 huawei-2 的无线网络的 WLAN 服务采用共享密钥认证+WEP-40 加密。
- SSID 为 huawei-3 的无线网络采用 WPA1 认证+TKIP 加密。
- SSID 为 huawei-4 的无线网络采用 WPA2 认证+CCMP 加密。
- SSID 为 huawei-5 的无线网络采用 WAPI 认证。

图 2-3 配置 WLAN 用户接入安全策略示例图

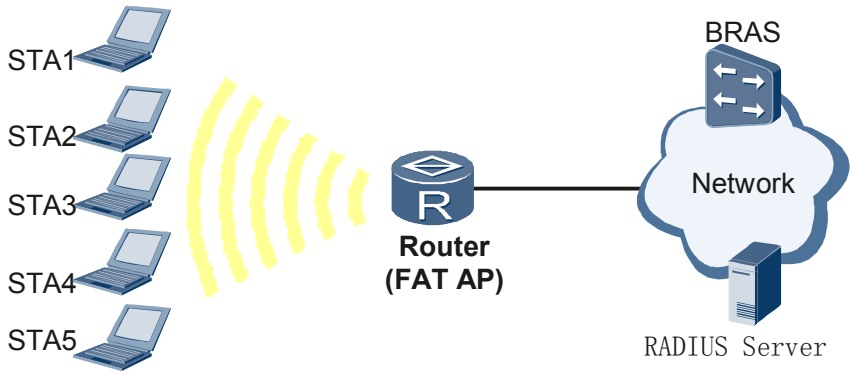


表 2-1 数据规划表

配置项	数据
WLAN 用户接入安全策略	● 安全模板:security-1 ● SSID：huawei-1 ● 认证模式：WEP 开放式系统认证+不加密
	● 安全模板:security-2 ● SSID：huawei-2 ● 认证模式：WEP 共享密钥认证 ● 加密方式：WEP-40 加密 密钥短语：12345

配置项	数据
	● 安全模板:security-3 ● SSID：huawei-3 ● 认证模式：WPA1 认证（802.1x+PEAP） ● 加密方式：TKIP
	● 安全模板:security-4 ● SSID：huawei-4 ● 认证模式：WPA2 认证（802.1x+PEAP） ● 加密方式：CCMP
	● 安全模板:security-5 ● SSID：huawei-5 ● 认证模式：WAPI 认证（证书认证） ● ASU 服务器 IP 地址：10.10.10.1

前提条件

- AP 证书、ASU 证书文件和 Issuer 认证证书已经保存到设备上，文件名为 huawei-ap.cer、huawei-asu.cer 和 huawei-issuer.cer。

配置思路

1. 全局启用 dot1x 和 AAA 配置。
2. 创建接入安全模板，并配置各种接入安全策略，实现各 SSID 网络下接入的 STA 采用不同的安全策略。
3. 创建服务集，并在服务集下绑定接入安全模板和 SSID，实现服务集和接入安全策略、SSID 的关联。
4. 创建 VAP，实现各 SSID 网络下接入的 STA，根据采用的不同安全策略均可正常访问 WLAN 网络。

操作步骤

步骤 1 全局启用 dot1x 和 AAA 配置。

- 全局启用 dot1x 的配置。

```
<Huawei> system-view
[Huawei] dot1x enable
```

- AAA 相关配置。

  #配置服务器信息，Radius 服务器地址为 10.137.146.163，共享密钥为 huawei。

```
[Huawei] radius-server template peap.radius.com
[Huawei-radius-peap.radius.com] radius-server authentication 10.137.146.163 1812
[Huawei-radius-peap.radius.com] radius-server accounting 10.137.146.163 1813
[Huawei-radius-peap.radius.com] radius-server shared-key simple huawei
[Huawei-radius-peap.radius.com] quit
```

  #配置 AAA 信息。

```
[Huawei] aaa
[Huawei-aaa] authentication-scheme radius
```

```
[Huawei-aaa-authen-radius] authentication-mode radius
[Huawei-aaa-authen-radius] quit
[Huawei-aaa] accounting-scheme radius
[Huawei-aaa-accounting-radius] accounting-mode radius
[Huawei-aaa-accounting-radius] quit
[Huawei-aaa] domain peap.radius.com
[Huawei-aaa-domain-peap.radius.com] radius-server peap.radius.com
[Huawei-aaa-domain-peap.radius.com] authentication-scheme radius
[Huawei-aaa-domain-peap.radius.com] accounting-scheme radius
[Huawei-aaa-domain-peap.radius.com] quit
[Huawei-aaa] quit
```

步骤 2 创建接入安全模板 security-1、security-2、security-3、security-4、security-5。

```
[Huawei] wlan
[Huawei-wlan-view] security-profile name security-1
[Huawei-wlan-sec-prof-security-1] quit
[Huawei-wlan-view] security-profile name security-2
[Huawei-wlan-sec-prof-security-2] quit
[Huawei-wlan-view] security-profile name security-3
[Huawei-wlan-sec-prof-security-3] quit
[Huawei-wlan-view] security-profile name security-4
[Huawei-wlan-sec-prof-security-4] quit
[Huawei-wlan-view] security-profile name security-5
[Huawei-wlan-sec-prof-security-5] quit
```

步骤 3 配置 WLAN 用户的接入安全模板。

- 配置接入安全模板 security-1 的安全策略。

  #安全模板采用 WEP 开放系统认证。

  ```
  [Huawei-wlan-view] security-profile name security-1
  [Huawei-wlan-sec-prof-security-1] wep authentication-method open-system
  [Huawei-wlan-sec-prof-security-1] security-policy wep
  [Huawei-wlan-sec-prof-security-1] quit
  ```

- 配置接入安全模板 security-2 的安全策略。

  #安全模板采用 WEP 共享密钥认证，WEP-40 方式，密钥短语为 12345。

  ```
  [Huawei-wlan-view] security-profile name security-2
  [Huawei-wlan-sec-prof-security-2] wep authentication-method share-key
  [Huawei-wlan-sec-prof-security-2] wep key wep-40 pass-phrase 0 12345
  [Huawei-wlan-sec-prof-security-2] wep default-key 0
  [Huawei-wlan-sec-prof-security-2] security-policy wep
  [Huawei-wlan-sec-prof-security-2] quit
  ```

- 配置接入安全模板 security-3 的安全策略。

  #安全模板的 WPA1 认证采用 802.1x+PEAP 方式，采用 TKIP 加密。

  ```
  [Huawei-wlan-view] security-profile name security-3
  [Huawei-wlan-sec-prof-security-3] wpa authentication-method dot1x peap encryption-method tkip
  [Huawei-wlan-sec-prof-security-3] security-policy wpa
  [Huawei-wlan-sec-prof-security-3] quit
  ```

- 配置接入安全模板 security-4 的安全策略。

  #安全模板的 WPA2 认证采用 802.1x+PEAP 方式，采用 CCMP 加密。

  ```
  [Huawei-wlan-view] security-profile name security-4
  [Huawei-wlan-sec-prof-security-4] wpa2 authentication-method dot1x peap encryption-method
  ccmp
  [Huawei-wlan-sec-prof-security-4] security-policy wpa2
  [Huawei-wlan-sec-prof-security-4] quit
  ```

- 配置接入安全模板 security-5 的安全策略。

  #安全模板的 WAPI 认证采用证书认证方式。

  ```
  [Huawei-wlan-view] security-profile name security-5
  [Huawei-wlan-sec-prof-security-5] wapi authentication-method certificate
  ```

#配置 ASU 服务器的 IP 地址为 10.10.10.1，AR1200 的认证证书为 huawei-ap.cer，ASU 认证证书为 huawei-asu.cer，Issuer 认证证书为 huawei-issuer.cer，私钥证书为 huawei-ap.cer。

```
[Huawei-wlan-sec-prof-security-5] wapi asu ip 10.10.10.1
[Huawei-wlan-sec-prof-security-5] wapi import certificate ap file-name flash:/huawei-ap.cer
[Huawei-wlan-sec-prof-security-5] wapi import certificate asu file-name flash:/huawei-asu.cer
[Huawei-wlan-sec-prof-security-5] wapi import certificate issuer file-name flash:/huawei-
issuer.cer
[Huawei-wlan-sec-prof-security-5] wapi import private-key file-name flash:/huawei-ap.cer
[Huawei-wlan-sec-prof-security-5] security-policy wapi
[Huawei-wlan-sec-prof-security-5] quit
```

步骤 4 创建服务集，并创建 VAP。

- #创建名为 SS-1 的 service-set，SSID 为 huawei-1，绑定 Traffic 模板 ctc，Security 模板 security-1 和 wlan-bss 接口 wlan-bss 0。应用 WLAN 服务到 AP 的射频 0 上。

```
[Huawei-wlan-view] traffic-profile name ctc
[Huawei-wlan-traffic-prof-ctc] quit
[Huawei-wlan-view] wmm-profile name wmm-1
[Huawei-wlan-wmm-prof-wmm-1] quit
[Huawei-wlan-view]quit
[Huawei]interface wlan-bss 0
[Huawei-Wlan-Bss0] port hybrid tagged vlan 1
[Huawei-Wlan-Bss0]quit
[Huawei]wlan
[Huawei-wlan-view] radio-profile name radio-1
[Huawei-wlan-radio-prof-radio-1] wmm-profile name wmm-1
[Huawei-wlan-radio-prof-radio-1] quit
[Huawei-wlan-view] service-set name ss-1
[Huawei-wlan-service-set-ss-1] ssid huawei-1
[Huawei-wlan-service-set-ss-1] traffic-profile name ctc
[Huawei-wlan-service-set-ss-1] security-profile name security-1
[Huawei-wlan-service-set-ss-1] wlan-bss 0
[Huawei-wlan-service-set-ss-1] quit
[Huawei-wlan-view] quit
[Huawei] interface wlan-radio 0/0/0
[Huawei-Wlan-Radio0/0/0] radio-profile name radio-1
[Huawei-Wlan-Radio0/0/0] service-set name ss-1
[Huawei-Wlan-Radio0/0/0] quit
```

- #创建名为 SS-2 的 service-set，SSID 为 huawei-2，绑定 Traffic 模板 ctc，Security 模板 security-2 和 wlan-bss 接口 wlan-bss 1。应用 WLAN 服务到 AP 的射频 0 上。

```
[Huawei]interface wlan-bss 1
[Huawei-Wlan-Bss1] port hybrid tagged vlan 2
[Huawei-Wlan-Bss1]quit
[Huawei] wlan
[Huawei-wlan-view] service-set name ss-2
[Huawei-wlan-service-set-ss-2] ssid huawei-2
[Huawei-wlan-service-set-ss-2] traffic-profile name ctc
[Huawei-wlan-service-set-ss-2] security-profile name security-2
[Huawei-wlan-service-set-ss-2] wlan-bss 1
[Huawei-wlan-service-set-ss-2] quit
[Huawei-wlan-view] quit
[Huawei] interface wlan-radio 0/0/0
[Huawei-Wlan-Radio0/0/0] service-set name ss-2
[Huawei-Wlan-Radio0/0/0] quit
```

- #创建名为 SS-3 的 service-set，SSID 为 huawei-3，绑定 Traffic 模板 ctc，Security 模板 security-3 和 wlan-bss 接口 wlan-bss 2。应用 WLAN 服务到 AP 的射频 0 上。

```
[Huawei]interface wlan-bss 2
[Huawei-Wlan-Bss2] port hybrid tagged vlan 3
[Huawei-Wlan-Bss2] dot1x-authentication enable
[Huawei-Wlan-Bss2] dot1x authentication-method eap
[Huawei-Wlan-Bss2]quit
[Huawei] wlan
[Huawei-wlan-view] service-set name ss-3
[Huawei-wlan-service-set-ss-3] ssid huawei-3
[Huawei-wlan-service-set-ss-3] traffic-profile name ctc
```

```
[Huawei-wlan-service-set-ss-3] security-profile name security-3
[Huawei-wlan-service-set-ss-3] wlan-bss 2
[Huawei-wlan-service-set-ss-3] quit
[Huawei-wlan-view] quit
[Huawei] interface wlan-radio 0/0/0
[Huawei-Wlan-Radio0/0/0] service-set name ss-3
[Huawei-Wlan-Radio0/0/0] quit
```

- #创建名为 SS-4 的 service-set，SSID 为 huawei-4，绑定 Traffic 模板 ctc，Security 模板 security-4 和 wlan-bss 接口 wlan-bss 3。应用 WLAN 服务到 AP 的射频 0 上。

```
[Huawei]interface wlan-bss 3
[Huawei-Wlan-Bss3] port hybrid tagged vlan 4
[Huawei-Wlan-Bss2] dot1x-authentication enable
[Huawei-Wlan-Bss2] dot1x authentication-method eap
[Huawei-Wlan-Bss3]quit
[Huawei] wlan
[Huawei-wlan-view] service-set name ss-4
[Huawei-wlan-service-set-ss-4] ssid huawei-4
[Huawei-wlan-service-set-ss-4] traffic-profile name ctc
[Huawei-wlan-service-set-ss-4] security-profile name security-4
[Huawei-wlan-service-set-ss-4] wlan-bss 3
[Huawei-wlan-service-set-ss-4] quit
[Huawei-wlan-view] quit
[Huawei] interface wlan-radio 0/0/0
[Huawei-Wlan-Radio0/0/0] service-set name ss-4
[Huawei-Wlan-Radio0/0/0] quit
```

- #创建名为 SS-5 的 service-set，SSID 为 huawei-5，绑定 Traffic 模板 ctc，Security 模板 security-5 和 wlan-bss 接口 wlan-bss 4。应用 WLAN 服务到 AP 的射频 0 上。

```
[Huawei]interface wlan-bss 4
[Huawei-Wlan-Bss4] port hybrid tagged vlan 5
[Huawei-Wlan-Bss4]quit
[Huawei] wlan
[Huawei-wlan-view] service-set name ss-5
[Huawei-wlan-service-set-ss-5] ssid huawei-5
[Huawei-wlan-service-set-ss-5] traffic-profile name ctc
[Huawei-wlan-service-set-ss-5] security-profile name security-5
[Huawei-wlan-service-set-ss-5] wlan-bss 4
[Huawei-wlan-service-set-ss-5] quit
[Huawei-wlan-view] quit
[Huawei] interface wlan-radio 0/0/0
[Huawei-Wlan-Radio0/0/0] service-set name ss-5
[Huawei-Wlan-Radio0/0/0] quit
```

步骤 5 验证配置结果

AR1200 下的接入用户可以搜索到 5 个无线网络，其网络标识分别为 huawei-1、huawei-2、huawei-3、huawei-4、huawei-5。

- 选择 SSID 为 huawei-1 的网络时，用户无需验证即可以正常使用 WLAN 服务。
- 选择 SSID 为 huawei-2 的网络时，用户需要有共享密钥才可以使用 WLAN 服务。
- 选择 SSID 为 huawei-3 和 huawei-4 的网络时，用户需要通过 802.1x 认证才可以使用 WLAN 服务。
- 选择 SSID 为 huawei-5 的网络时，用户需要有匹配的证书才可以使用 WLAN 服务。

----结束

配置文件

```
#
 dot1x enable
#
radius-server template peap.radius.com
 radius-server authentication 10.137.146.163 1812
```

```
 radius-server accounting 10.137.146.163 1813
#
interface Wlan-Bss0
 port hybrid tagged vlan 1
#
interface Wlan-Bss1
 port hybrid tagged vlan 2
#
interface Wlan-Bss2
 port hybrid tagged vlan 3
 dot1x-authentication enable
 dot1x authentication-method eap
#
interface Wlan-Bss3
 port hybrid tagged vlan 4
 dot1x-authentication enable
 dot1x authentication-method eap
#
interface Wlan-Bss4
 port hybrid tagged vlan 5
#
wlan
 wmm-profile name wmm-1 id 1
 traffic-profile name ctc id 1
 security-profile name security-1 id 1
 security-profile name security-2 id 2
  wep authentication-method share-key
  wep key wep-40 pass-phrase 0 12345
 security-profile name security-3 id 3
  security-policy wpa
 security-profile name security-4 id 4
  security-policy wpa2
 security-profile name security-5 id 5
  security-policy wapi
  wapi asu ip 10.10.10.1
  wapi import certificate ap file-name flash:/huawei-ac.cer
  wapi import certificate asu file-name flash:/huawei-asu.cer
  wapi import certificate issuer file-name flash:/huawei-
issuer.cer
 service-set name ss-1 id 0
  Wlan-Bss 0
  ssid huawei-1
  traffic-profile id 1
  security-profile id 1
 service-set name ss-2 id 1
  Wlan-Bss 1
  ssid huawei-2
  traffic-profile id 1
  security-profile id 2
 service-set name ss-3 id 2
  Wlan-Bss 2
  ssid huawei-3
  traffic-profile id 1
  security-profile id 3
 service-set name ss-4 id 3
  Wlan-Bss 3
  ssid huawei-4
  traffic-profile id 1
  security-profile id 4
 service-set name ss-5 id 4
  Wlan-Bss 4
  ssid huawei-5
  traffic-profile id 1
  security-profile id 5
 radio-profile name radio-1 id 0
  wmm-profile id 0
#
interface Wlan-Radio0/0/0
 radio-profile id
```

```
1
 service-set id 0 wlan 1
 service-set id 1 wlan 2
 service-set id 2 wlan 3
 service-set id 3 wlan 4
 service-set id 4 wlan 5
#
return
```

3 WLAN QoS 配置

关于本章

介绍胖 AP 组网模式下的 QoS 业务配置过程。

3.1 WLAN QoS 简介
WLAN QoS 保证不同质量的无线接入服务之间的互通，满足实际应用的需求。

3.2 AR1200 支持的 WLAN QoS 特性
AR1200 支持的 WLAN QoS 特性包括射频的 QoS 策略管理、VAP 的 QoS 策略管理。

3.3 配置射频的 QoS 策略
配置射频的 QoS 策略，提供不同的信道抢占能力，实现不同的服务质量。

3.4 配置 VAP 的 QoS 策略
当需要为某个 VAP 定制特定的优先级映射、流量抑制等功能时，创建相应的流量模板并绑定到服务集中。

3.5 配置示例

3.1 WLAN QoS 简介

WLAN QoS 保证不同质量的无线接入服务之间的互通，满足实际应用的需求。

802.11 网络提供了基于竞争的无线接入服务，但是不同的应用需求对于网络的要求是不同的，而原始的网络不能为不同的应用提供不同质量的接入服务，所以已经不能满足实际应用的需要。

IEEE 802.11e 为基于 802.11 协议的 WLAN 体系添加了 QoS 特性，这个协议的标准化时间很长， 在这个过程中，Wi-Fi 组织为了保证不同 WLAN 厂商提供 QoS 的设备之间可以互通，定义了 WMM（Wi-Fi Multimedia，Wi-Fi 多媒体）标准。WMM 标准使 WLAN 网络具备了提供 QoS 服务的能力。

WMM

WMM 是一种无线 QoS 协议，用于保证高优先级的报文有优先的发送权利，从而保证语音、视频等应用在无线网络中有更好的质量。

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。

AC

AC（Access Category，接入类），WMM 按照优先级从高到低的顺序分为 AC-VO（语音流）、AC-VI（视频流）、AC-BE（尽力而为流）、AC-BK（背景流）四个优先级队列，保证越高优先级队列中的报文，抢占信道的能力越高。

3.2 AR1200 支持的 WLAN QoS 特性

AR1200 支持的 WLAN QoS 特性包括射频的 QoS 策略管理、VAP 的 QoS 策略管理。

射频的 QoS 策略

在 802.11 协议中分布式协调功能 DCF(Distributed Coordination Function)规定了 AP 和客户端使用载波监听/冲突避免 CSMA/CA(Carrier Sense Multiple Access with Collision Avoidance)的接入方式。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。

WMM 协议将数据报文分为 4 个 AC 队列(AC_VO、AC_VI、AC_BE、AC_BK)，高优先级的 AC 占用信道的机会大于低优先级的 AC。每个 AC 队列定义了一套信道竞争 EDCA (Enhanced Distributed Channel Access)参数，该参数决定了队列占用信道的能力大小。

EDCA 参数包括：

- 仲裁帧间隙数 AIFSN(Arbitration Inter Frame Spacing Number)，AIFSN 数值越大，用户的空闲等待时间越长。

- 最小竞争窗口指数形式 ECWmin(Exponent form of CWmin)和最大竞争窗口指数形式 ECWmax(Exponent form of CWmax)，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。
- 传输机会限制 TXOPLimit(Transmission Opportunity Limit)，用户一次竞争成功后，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。
- ACK 策略：NORMAL ACK 是指对于每个发送的单播报文，接收者在成功接收到发送报文后，都要发送一个应答 ACK 进行确认。No ACK 指在通信质量很好、干扰很小的情况下，我们不进行应答 ACK，这样发送失败也不会重发，但是可以提高发送效率。

WLAN 特性中，将 EDCA 参数及其他的 WMM 参数集中在 WMM 模板中进行管理。WMM 模板创建后需绑定到射频模板中，随绑定的射频模板应用到射频中。

VAP 的 QoS 策略管理

报文上行时，AP 接收到无线客户端发送的 802.11 数据报文后，将其转换为 802.3 报文，然后向网络侧继续转发。在整个传送过程中依据 802.3 报文优先级进行调度。

报文下行时，AP 将网络侧接收到 802.3 报文，转换为 802.11 报文，并依据报文中的 UP 优先级选择不同的 AC 队列无线发送给用户终端。

VAP 的 QoS 策略管理通过 Traffic 模板进行管理。Traffic 模板参数说明如**表 3-1** 所示。

表 3-1 Traffic 模板参数说明

参数名	说明
Client/VAP 的无线上行限速	限制无线客户端或整个 VAP 上行的无线报文速率。
802.3 报文优先级配置	配置 AP 上行 802.3 报文内层的 802.1p 优先级：采用指定值或依据无线客户端发送的 802.11 报文 UP 优先级映射。
802.11 报文优先级配置	配置 AP 下行 802.11 报文的优先级。

Traffic 模板创建后需绑定到服务集 Sevice-Set 中，随着服务集应用到对应的 VAP 中。

3.3 配置射频的 QoS 策略

配置射频的 QoS 策略，提供不同的信道抢占能力，实现不同的服务质量。

应用环境

无线终端和 AP 之间采用无线传输，通过占用信道来发送无线报文。为了实现不同无线用户获得不同级别的服务，可通过配置 WMM 模板参数来实现。

前置任务

在配置射频的 QoS 策略之前，需完成以下任务：

- WLAN 的基本功能已经配置完成，具体请参见 **1.4 配置 WLAN 业务**。

数据准备

在配置射频的 QoS 策略之前，需准备以下数据。

序号	数据
1	WMM 模板名称、（可选）WMM 模板 ID
2	（可选）WMM EDCA Client：AIFSN（空闲等待时长）、ECWmin 和 ECWmax（最小最大退避时间）、TXOPLimit（占用信道时长）
3	（可选）WMM EDCA AP：AIFSN（空闲等待时长）、ECWmin 和 ECWmax（最小最大退避时间）、TXOPLimit（占用信道时长）

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 执行命令 **wmm-profile** { **id** *profile-id* | **name** *profile-name* } *，配置 WMM 模板。

WMM 模板创建成功后，模板内的参数均自动配置为缺省值。使用命令 **display wmm-profile** { **all** | **id** *profile-id* | **name** *profile-name* }，查看 WMM 模板配置的各项属性。

#创建 WMM 模板“wp”，所有配置均为缺省值。

```
[Huawei-wlan-view] display wmm-profile name wp
  Profile ID      : 2
  Profile name    : wp
  WMM switch      : enable
  Client EDCA parameters:
  ----------------------------------------------------
         ECWmax  ECWmin  AIFSN  TXOPLimit
  AC_VO  3       2       2      47
  AC_VI  4       3       2      94
  AC_BE  10      4       3      0
  AC_BK  10      4       7      0
  ----------------------------------------------------
  AP EDCA parameters:
  ----------------------------------------------------
         ECWmax  ECWmin  AIFSN  TXOPLimit  Ack-Policy
  AC_VO  3       2       1      47         normal
  AC_VI  4       3       1      94         normal
  AC_BE  6       4       3      0          normal
  AC_BK  10      4       7      0          normal
  ----------------------------------------------------
```

说明

终端和 AP 之间采用无线传输，通过占用信道来发送无线报文。为了实现不同报文获得不同级别的服务，我们将数据报文通过 4 个优先级队列发送，每个优先级队列占用信道的机会不一样。

四个优先级队列的名称和优先级顺序缺省为：AC_VO(语音) > AC_VI(视频) > AC_BE(尽力而为) > AC_BK(背景)。

四个优先级队列的优先级顺序并不是绝对的，可以通过参数修改来调整优先级顺序，这些参数称为 EDCA 参数(Enhanced Distributed Channel Access)。包括 AIFSN（arbitration inter Frame spacing number 仲裁帧间隙数）、ECWmin（exponetn form of CWmin 最小竞争窗口指数形式）、ECWmax (exponent form of CWmax 最大竞争窗口指数形式)、TXOPlimit（transmission opportunity limit 传输机会限制）以及 ack-policy（ACK 策略）。

- AIFSN：WMM 针对不同 AC 可以配置不同的空闲等待时长，AIFSN 数值越大，用户的空闲等待时间越长。
- ECWmin 和 ECWmax：这两个数值决定了平均退避时间值，数值越大，用户的平均退避时间越长。
- TXOPLimit：用户一次竞争成功后，可占用信道的最大时长，这个数值越大，用户一次能占用的信道时长越大，如果是 0，则每次占用信道后，只能发送一个报文。
- ack-policy：有 normal ack(应答)和 no ack(不应答)两种策略，缺省为 noraml ack。

占用信道发送报文的原理：终端在占用信道发送报文前，先监听信道，当信道空闲时间大于或等于空闲等待时间时，在竞争窗口范围内随即选择退避时间进行退避，最先结束退避的终端竞争到信道，开始发送报文。

步骤 4 （可选）执行命令 **wmm edca client** { **ac-vo** | **ac-vi** | **ac-be** | **ac-bk** } { **aifsn** *aifsn-value* | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* } *，配置终端上四个 WMM 队列的 EDCA 参数。

步骤 5 （可选）执行命令 **wmm edca ap** { **ac-vo** | **ac-vi** | **ac-be** | **ac-bk** } { **aifsn** *aifsn-value* | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* | **ack-policy** { **normal** | **noack** } } *，配置 AP 上四个 WMM 队列的 EDCA 参数。

----结束

检查配置结果

执行命令 **display wmm-profile** { **all** | **id** *profile-id* | **name** *profile-name* }，查看 WMM 模板配置的各项属性。

3.4 配置 VAP 的 QoS 策略

当需要为某个 VAP 定制特定的优先级映射、流量抑制等功能时，创建相应的流量模板并绑定到服务集中。

应用环境

STA 发出的 802.11 报文要通过 AP 进入以太网时，需要转换成 802.3 报文，这期间可以不进行优先级映射，也可以按照不同的 VAP 设置不同的优先级，从而提供不同的 QoS 服务质量。

前置任务

在配置 VAP 的 QoS 策略之前，需完成以下任务：

- WLAN 的基本功能已经配置完成，具体请参见 **1.4 配置 WLAN 业务**。

数据准备

在配置 VAP 的 QoS 策略之前，需准备以下数据。

序号	数据
1	流量模板名称、（可选）流量模板 ID
2	（可选）up-map-8021p 映射值、8021p-map-up 映射值
3	（可选）报文限速速率

操作步骤

步骤 1 执行命令 **system-view**，进入系统视图。

步骤 2 执行命令 **wlan**，进入 WLAN 视图。

步骤 3 执行命令 **traffic-profile** { **name** *profile-name* | **id** *profile-id* } *，配置流量模板。

流量模板创建成功后，模板内的参数均为缺省值。执行命令 **display traffic-profile** { **all** | **id** *profile-id* | **name** *profile-name* }，查看各项属性的缺省配置。

#查看 Traffic 模板“traffic-profile-1”的各项属性。

```
[Huawei-wlan-view] display traffic-profile name traffic-profile-1
  Profile ID         : 3
  Profile name       : traffic-profile-1
  Client Limit Rate  : 4294967295 Kbps(up)
                     : 4294967295 Kbps(down)
  VAP Limit Rate     : 4294967295 Kbps(up)
                     : 4294967295 Kbps(down)
  802.1p Mapping Mode: mapping
  ----------------------------
  User-priority  802.1p
  0              0
  1              1
  2              2
  3              3
  4              4
  5              5
  6              6
  7              7
  ----------------------------
  802.1p to User-priority Mapping List:
  ----------------------------
  802.1p  User-priority
  0       0
  1       1
  2       2
  3       3
  4       4
  5       5
  6       6
  7       7
  ----------------------------
  Tunnel priority(up) Mapping Mode:ToS(inner) to ToS(outer)
  ----------------------------
  ToS(inner)     ToS(outer)
  0              0
  1              1
  2              2
  3              3
```

```
4               4
5               5
6               6
7               7
----------------------------
Tunnel priority(down) Mapping Mode:ToS(inner) to ToS(outer)
----------------------------
ToS(inner)      ToS(outer)
0               0
1               1
2               2
3               3
4               4
5               5
6               6
7               7
----------------------------
```

说明

802.3 报文通过 AP 转发给 STA 时，被转换成 802.11 报文，其中的 UP 域可以根据 DSCP、CoS 映射而来，或者由流分类设置。

步骤 4 （可选）执行命令 **8021p** { **designate** *value* | **up-mapping** *value0 value1 value2 value3 value4 value5 value6 value7* }，配置 AP 的上行 802.3 报文的 802.1p 优先级值。

STA 发送 802.11 报文后，在 AP 上终结，同时构造 802.3 报文上行。为保证报文在 AP 转发时能够得到一定的服务质量，需要填充其优先级值以便调度。

步骤 5 （可选）执行命令 **8021p-map-up** *value0 value1 value2 value3 value4 value5 value6 value7*，配置下行时 802.1p 优先级值到用户优先级值的映射关系。

步骤 6 （可选）执行命令 **rate-limit** { **client** | **vap** } { **up** | **down** } *ratelimit-value*，限制单个终端或整个 VAP 内所有终端的无线侧上下行报文速率。

----结束

检查配置结果

执行命令 **display traffic-profile** { **all** | **id** *profile-id* | **name** *profile-name* }，查看流量模板配置的各项属性。

3.5 配置示例

3.5.1 配置 WLAN QoS 策略的业务示例

组网需求

如图 3-1 所示，STA1、STA2 通过 AR1200 连接到网络。AR1200 作为 FAT AP，其中 STA2 为 VIP 客户。要求：

- 优先满足接入用户的视频需求。
- 当网络带宽不足时，优先满足 VIP 客户的使用需求。

图 3-1 配置 WLAN QoS 策略示例图

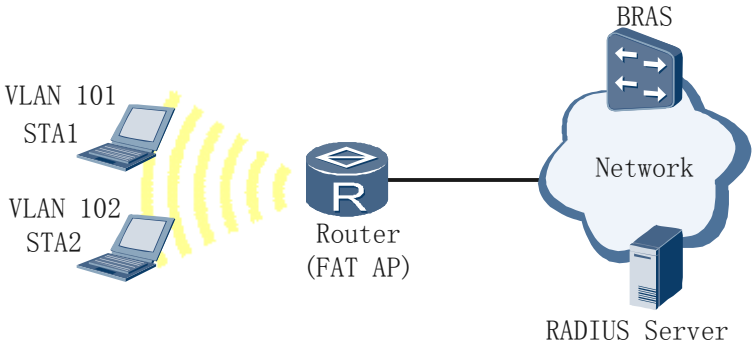


表 3-2 数据规划表

配置项	数据
WLAN 服务	● SSID：huawei-1 ● Traffic 模板：huawei ● Security 模板：huawei
	● SSID：huawei-2 ● Traffic 模板：huawei-vip ● Security 模板：huawei
AP 射频模板	射频模板:huawei-vi；WMM 模板：huawei-vi
业务 VLAN	VLAN 101、VLAN 102
国家码	CN

配置思路

AR1200 作为 FAT AP，配置 WLAN QoS 业务的基本思路如下：

1. 配置 AR1200 的基本功能，包括配置国家码、DHCP Server，实现为用户分配 IP 地址功能。
2. 配置 WLAN-BSS 接口，并在服务集下绑定该接口，实现无线侧报文到达 AR1200 后能够送至 WLAN 业务处理模块功能。
3. 创建 WMM 模板并配置模板属性，创建射频模板，并在射频模板下绑定 WMM 模板，实现优先满足用户视频通信的需求。
4. 创建流量模板并配置模板属性，实现当网络带宽不足时，优先满足 VIP 客户的通信需求。
5. 创建安全模板，实现 STA 接入网络的安全控制。
6. 创建服务集，并在服务集下绑定安全模板、流量模板。
7. 创建 VAP，实现不同 STA 使用 WLAN 网络的 QoS 控制。

操作步骤

步骤 1 配置 AP 的基本功能。

#配置 AP 的国家码，方便识别和管理。

```
<Huawei> system-view
[Huawei] wlan global country-code cn
```

#创建 VLANIF 接口，配置 IP 地址作为数据转发的三层接口，使能 DHCP 服务功能。接口 VLANIF101 为 STA1 分配 IP 地址。接口 VLANIF102 为 STA2 分配 IP 地址。

```
[Huawei] dhcp enable
[Huawei] vlan batch 101 102
[Huawei] interface vlanif101
[Huawei-Vlanif101] ip address 192.168.0.1 24
[Huawei-Vlanif101] dhcp select interface
[Huawei-Vlanif101] quit
[Huawei] interface vlanif102
[Huawei-Vlanif102] ip address 192.168.1.1 24
[Huawei-Vlanif102] dhcp select interface
[Huawei-Vlanif102] quit
```

步骤 2 配置 WLAN-BSS 虚接口。

```
[Huawei] interface Wlan-Bss 1
[Huawei-Wlan-Bss1] port hybrid tagged vlan 101
[Huawei-Wlan-Bss1] quit
[Huawei] interface Wlan-Bss 2
[Huawei-Wlan-Bss2] port hybrid tagged vlan 102
[Huawei-Wlan-Bss2] quit
```

步骤 3 配置 AP 的 WMM 模板和射频模板。

- 创建 WMM 模板

  #创建 WMM 模板“huawei-vi”，并修改队列优先级参数，使优先级队列顺序为：AC_VI(视频) >AC_VO(语音)。

  ```
  [Huawei] wlan
  [Huawei-wlan-view] wmm-profile name huawei-vi
  [Huawei-wlan-wmm-prof-huawei-vi] wmm edca ap ac-vi ecw ecwmin 1 ecwmax 1 aifsn 1 txoplimit 36 ack-policy normal
  [Huawei-wlan-wmm-prof-huawei-vi] wmm edca client ac-vi ecw ecwmin 1 ecwmax 3 aifsn 1 txoplimit 36
  [Huawei-wlan-wmm-prof-huawei-vi] quit
  ```

- #创建 Radio 模板，并绑定 WMM 模板。

  ```
  [Huawei-wlan-view] radio-profile name huawei-vi
  [Huawei-wlan-radio-prof-huawei-vi] wmm-profile name huawei-vi
  [Huawei-wlan-radio-prof-huawei-vi] quit
  ```

步骤 4 配置 AP 的安全模板。

#创建名为“huawei”的 Security 模板，采用缺省配置。

```
[Huawei-wlan-view] security-profile name huawei
[Huawei-wlan-sec-prof-huawei] quit
```

步骤 5 配置 AP 的流量模板。

#创建名为“huawei”的 Traffic 模板，设置 VAP 上行限速为 1024K，STA 上行限速为 512K。

```
[Huawei-wlan-view] traffic-profile name huawei
[Huawei-wlan-traffic-prof-huawei] rate-limit client up 512
[Huawei-wlan-traffic-prof-huawei] rate-limit vap up 1024
[Huawei-wlan-traffic-prof-huawei] quit
```

#创建名为“huawei-vip”的 Traffic 模板。设置 VAP 上行限速为 2048K，STA 上行限速为 1024K。

```
[Huawei-wlan-view] traffic-profile name huawei-vi
[Huawei-wlan-traffic-prof-huawei-vi] rate-limit client up 1024
[Huawei-wlan-traffic-prof-huawei-vi] rate-limit vap up 2048
[Huawei-wlan-traffic-prof-huawei-vi] quit
```

步骤 6 配置 AP 的服务集。

- #创建名为“huawei-1”的 service-set，SSID 为“huawei-1”，绑定 Traffic 模板“huawei”，Security 模板“huawei”，wlan-bss 接口“wlan-bss 1”。

```
[Huawei-wlan-view] service-set name huawei-1
[Huawei-wlan-service-set-huawei-1] ssid huawei-1
[Huawei-wlan-service-set-huawei-1] traffic-profile name Huawei
[Huawei-wlan-service-set-huawei-1] security-profile name Huawei
[Huawei-wlan-service-set-huawei-1] wlan-bss 1
[Huawei-wlan-service-set-huawei-1] quit
```

- #创建名为“huawei-2”的 service-set，SSID 为“huawei-2”，绑定 Traffic 模板“huawei-vip”，Security 模板“huawei”，wlan-bss 接口“wlan-bss 2”。

```
[Huawei-wlan-view] service-set name huawei-2
[Huawei-wlan-service-set-huawei-2] ssid huawei-2
[Huawei-wlan-service-set-huawei-2] traffic-profile name huawei-vi
[Huawei-wlan-service-set-huawei-2] security-profile name Huawei
[Huawei-wlan-service-set-huawei-2] wlan-bss 2
[Huawei-wlan-service-set-huawei-2] quit
```

步骤 7 配置 VAP。

#将 AP 的射频口绑定射频模板、服务集“huawei-1”和“huawei-2”，AR1200 上自动创建相应的 VAP 信息。

```
[Huawei] interface Wlan-Radio 0/0/0
[Huawei-Wlan-Radio0/0/0] radio-profile name huawei-vi
[Huawei-Wlan-Radio0/0/0] service-set name huawei-1
[Huawei-Wlan-Radio0/0/0] service-set name huawei-2
[Huawei-Wlan-Radio0/0/0] quit
```

步骤 8 验证配置结果

AR1200 下用户可以搜索到 2 个 WLAN 网络，其网络标识分别为 huawei-1 和 huawei-2。STA1、STA2 分别选择 huawi-1 和 huawei-2 的 WLAN 网络。

----结束

配置文件

```
#
 vlan batch 101 to 102
#
 dhcp enable
#
interface Vlanif101
 ip address 192.168.0.1 255.255.255.0
 dhcp select interface
#
interface Vlanif102
 ip address 192.168.1.1 255.255.255.0
 dhcp select interface
#
wlan
  wmm-profile name huawei-vi id 1
  wmm edca ap ac-vi aifsn 1 ecw ecwmin 1 ecwmax 1 txoplimit 36
  wmm edca client ac-vi aifsn 1 ecw ecwmin 1 ecwmax 3 txoplimit 36
  traffic-profile name huawei id 1
  rate-limit client up 512
  rate-limit vap up 1024
 traffic-profile name huawei-vi id 2
  rate-limit client up 1024
  rate-limit vap up 2048
```

```
 security-profile name huawei id 1
 service-set name huawei-1 id 0
  Wlan-Bss 1
  ssid huawei-1
  traffic-profile id 1
  security-profile id 1
 service-set name huawei-2 id 1
  Wlan-Bss 2
  ssid huawei-2
  traffic-profile id 2
  security-profile id 1
 radio-profile name huawei-vi id 1
  wmm-profile id 1
#
interface Wlan-Radio0/0/0
 radio-profile id 1
 service-set id 0 wlan 1
 service-set id 1 wlan 2
#
interface Wlan-Bss1
 port hybrid tagged vlan 101
#
interface Wlan-Bss2
 port hybrid tagged vlan 102
#
return
```