H3C 无线接入点

Web 网管配置指导

新华三技术有限公司
http://www.h3c.com

资料版本：6W107-20180112
产品版本：R1508P11

Copyright © 2014-2018 新华三技术有限公司及其许可者 版权所有，保留一切权利。
未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。

H3C、H3C、H3CS、H3CIE、H3CNE、Aolynk、Aolynk、H^{3}Care、H3care、IRF、NetPilot、Netflow、SecEngine、SecPath、SecCenter、SecBlade、Comware、ITCMM、HUASAN、华三均为新华三技术有限公司的商标。对于本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

由于产品版本升级或其他原因，本手册内容有可能变更。H3C 保留在没有任何通知或者提示的情况下对本手册的内容进行修改的权利。本手册仅作为使用指导，H3C 尽全力在本手册中提供准确的信息，但是 H3C 并不确保手册内容完全没有错误，本手册中的所有陈述、信息和建议也不构成任何明示或暗示的担保。

前 言

H3C 无线接入点 Web 网管配置指导介绍了 H3C 无线接入点 Web 网管页面的各种功能，如快速配置、Web 登录、无线服务相关配置、安全认证相关配置、QoS 相关配置和各种高级配置等。

说明

手册中设备的接口类型、显示信息与设备型号和配置信息相关，本手册致力于提供全面、准确的显示信息，但实际使用中还请以设备的实际情况为准。

前言部分包含如下内容：

- 读者对象
- 本书约定
- 资料获取方式
- 技术支持
- 资料意见反馈

1.1 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

1.2 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。

1.3 资料获取方式

您可以通过H3C网站（www.h3c.com）获取最新的产品资料：

- 获取安装类、配置类或维护类等产品资料
  http://www.h3c.com/cn/Technical_Documents
- 获取版本说明书等与软件版本配套的资料
  http://www.h3c.com/cn/Software_Download

1.4 技术支持

用户支持邮箱：service@h3c.com

技术支持热线电话：400-810-0504（手机、固话均可拨打）

技术支持知了社区：http://zhiliao.h3c.com（在线快速问题答复）

网址：http://www.h3c.com

1.5 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 Web概述 ····· 1-1
1.1 简介 ····· 1-1
1.2 登录Web网管 ····· 1-1
1.3 退出Web网管 ····· 1-2
1.4 Web网管页面布局介绍 ····· 1-2
1.5 Web网管用户级别 ····· 1-3
1.6 Web网管功能介绍 ····· 1-3
1.7 Web页面常用元素 ····· 1-10
1.7.1 常用按钮和图标 ····· 1-10
1.7.2 列表分页显示功能 ····· 1-10
1.7.3 列表查询显示功能 ····· 1-11
1.7.4 列表排序显示功能 ····· 1-13
1.8 Web网管使用限制 ····· 1-14
1.9 Web网管使用常见问题举例 ····· 1-15
1.9.1 无法通过Web网管正常访问设备 ····· 1-15

1 Web概述

说明

手册中设备的接口类型、显示信息与设备型号、支持射频情况和配置信息相关，实际使用中还请以设备的实际情况为准。

1.1 简介

为了方便网络管理员对网络设备进行操作和维护，设备提供了 Web 网管功能。管理员可以使用 Web 界面直观地管理和维护网络设备。

Web 网管的运行环境如下图所示。

图1-1 Web 网管运行环境



1.2 登录Web网管

设备出厂时已经默认启用了 HTTP 服务，并且设置有默认的 Web 登录信息，用户可以直接使用默认登录信息通过 HTTP 服务登录设备的 Web 界面。默认的 Web 登录信息包括：

- 用户名：admin
- 密码：h3capadmin
- 设备（Vlan-interface1）的 IP 地址：192.168.0.50

采用 Web 方式登录设备的步骤如下：

(1) 连接设备和 PC

用交叉以太网线将 PC 和设备上的以太网口（缺省情况下，所有端口均属于 VLAN 1）相连。

(2) 为 PC 配置 IP 地址，保证能与设备互通

修改 IP 地址为 192.168.0.0/24 网段内的任意地址（除 192.168.0.50），例如 192.168.0.2。

(3) 启动浏览器，输入登录信息

在 PC 上启动浏览器，在地址栏中输入“http://192.168.0.50”后回车，即可进入设备的 Web 登录页面，如下图所示。输入用户名“admin”、密码“h3capadmin”和验证码，选择 Web 网管的语言种类（目前支持中文和 English 两种），单击<登录>按钮即可登录。

图1-2 Web 网管登录界面



说明

- 这里的 PC 是进行设备基本配置时使用的 PC，不一定是 Web 网管终端。Web 网管终端是登录 Web 网管时使用的 PC，只需与设备路由可达即可。
- 在 Web 登录界面上单击显示的验证码图片，可以刷新得到新的验证码。
- 如果通过 **web captcha** 命令配置了固定的验证码，则除了使用 Web 登录界面上提示的验证码，使用指定的固定验证码也可以登录设备，具体配置请参见“基础配置指导”中的“登录设备”。
- 同时通过 Web 登录设备的最大用户数为 5
- 还可以通过 HTTPS 服务登录 Web 网管，但需要先在设备上启用 HTTPS 服务，并且用户在浏览器地址栏中输入的地址需以“https://”开头，具体配置请参见“服务管理”。需要注意的是，如果通过 **web https-authorization mode** 命令配置了采用 **auto** 认证模式对 HTTPS 登录用户进行认证，则在用户登录时，直接使用客户端的 PKI 证书自动进行认证，不需要用户输入用户名和密码，具体配置请参见“基础配置指导”中的“登录设备”。

1.3 退出Web网管

在Web网管页面上单击右上角的<退出>按钮（如 图 1-3 所示），即可退出Web网管。

退出 Web 网管时，系统不会自动保存当前配置。因此建议用户在退出 Web 网管前先设置保存当前配置。

注意

通过直接关闭浏览器的方式，已登录到设备上的用户不能自动退出登录。

1.4 Web网管页面布局介绍

Web 网管页面共分为：导航栏、配置区、辅助区三部分，如下图所示。

图1-3 Web 网管初始页面



(1) 导航栏	(2) 配置区	(3) 辅助区

- 导航栏：以导航树的形式组织设备的 Web 网管功能菜单。用户在导航栏中可以方便的选择功能菜单，选择结果显示在配置区中。
- 配置区：用户进行配置和查看的区域。
- 辅助区：辅助区的左侧用于显示当前配置区的页面在导航栏中的路径；右侧提供<保存>按钮可以快速保存当前配置，提供<帮助>按钮可以查看 Web 网管的版本和帮助信息，并提供<退出>按钮可以退出 Web 网管登录。

1.5 Web网管用户级别

Web 网管用户的级别由低到高分四级：Visitor、Monitor、Configure 和 Management。高级别用户具有低级别用户的所有操作权限。

- Visitor：处于该级别的用户可以进行 Ping 和 Trace Route 操作，但不能从设备读取任何数据，也不能对设备进行任何设置。
- Monitor：只能从设备读取数据，而不能对设备进行任何设置。
- Configure：可以从设备读取数据，并对设备进行配置，但是不能对设备进行软件升级、添加/删除/修改用户、备份/恢复配置文件等操作。
- Management：可以对设备进行任何操作。

1.6 Web网管功能介绍

Web 网管功能的具体说明如下表所示。

说明

下表中用户级别表示该级别或高于该级别的用户均可实现对应功能的操作。

表1-1 Web 网管功能说明

菜单/页签			功能说明	用户级别
快速配置			对设备进行快速配置	Configure
概览	设备概览		显示、刷新系统资源状态、设备信息、接口信息和近期发生的系统操作日志信息	Monitor
	无线服务		显示无线服务的查询信息，包括无线服务的详细信息、统计信息、连接历史	Monitor
	射频		显示射频信息的相关信息，包括与其相关的无线服务、Radio口统计信息	Monitor
	WDS		显示WDS的相关信息，包括WDS状态、邻居信息	Monitor
	客户端		显示客户端的详细信息、统计信息	Monitor
			清空客户端统计信息、断开连接。把客户端加入黑名单等	Configure
设备	基本信息	系统名称	显示、设置系统的名称	Configure
		Web闲置超时时间	显示、设置Web的闲置超时时间	Configure
	设备维护	软件升级	设置从本地主机上传升级文件，对系统软件进行升级	Management
		设备重启	设置重新启动设备	Management
		诊断信息	生成诊断信息文件，并将文件打开查看或保存到本地主机	Management
	时间设置	时间设置	显示和设置当前系统时间	Configure
		时区	显示和设置系统所在的时区	Configure
	日志管理	日志显示	显示、刷新日志信息	Monitor
			清空日志信息	Configure
		日志主机	显示、设置日志主机的信息	Configure
		参数设置	显示、设置缓冲区容量和日志显示的刷新周期的信息	Configure
	配置管理	配置备份	设置将配置文件备份到本地主机	Management
		配置恢复	设置从本地恢复配置文件到设备	Management
		保存配置	设置将当前的配置保存到配置文件中	Configure
		恢复出厂配置	设置将设备恢复到出厂时的配置	Management
	文件管理		对设备上的文件进行管理，包括显示、上传、下载、删除以及设置主用启动文件	Management
	接口管理		显示设备的接口信息，查看端口的统计信息	Monitor
			新建、修改、删除接口，清空端口的统计信息	Configure
	TR-069		显示TR-069配置信息	Monitor
			设置TR-069	Configure

菜单/页签			功能说明	用户级别
	用户管理	用户概览	显示Web、FTP和Telnet用户的概要信息	Monitor
		超级密码	设置用户从当前访问等级切换到管理级所使用的超级密码	Management
		创建用户	创建Web、FTP和Telnet用户	Management
		修改用户	修改Web、FTP和Telnet用户信息	Management
		删除用户	删除Web、FTP和Telnet用户	Management
		切换到管理级	切换用户当前的访问等级到管理级	Visitor
	SNMP		显示SNMP的配置信息	Monitor
			设置SNMP	Management
	环回测试		对以太网接口进行环回测试	Configure
网络	MAC地址	MAC	显示MAC地址信息	Monitor
			新建、删除MAC地址	Configure
		设置	显示、设置MAC地址老化时间	Configure
	VLAN	VLAN	显示设备上的所有VLAN及其端口信息	Monitor
			新建、修改、删除VLAN	Configure
		端口	显示设备上的端口所属VLAN的情况	Monitor
			修改端口所属的VLAN	Configure
	ARP管理	ARP表	显示ARP表的信息	Monitor
			新建、修改、删除ARP表项	Configure
		免费ARP	显示免费ARP功能的配置信息	Monitor
			设置免费ARP功能	Configure
	IGMP Snooping	基本配置	显示全局和VLAN内的IGMP Snooping配置信息，查看IGMP Snooping组播表项信息	Monitor
			在全局和VLAN内配置IGMP Snooping	Configure
		高级配置	显示端口上的IGMP Snooping配置信息	Monitor
			在端口上配置IGMP Snooping	Configure
	IPv4路由	显示	显示IPv4激活路由表信息	Monitor
		创建	创建IPv4静态路由	Configure
		删除	删除IPv4静态路由	Configure
	IPv6路由	显示	显示IPv6激活路由表信息	Monitor
		创建	创建IPv6静态路由	Configure
		删除	删除IPv6静态路由	Configure
	DHCP	DHCP服务器	显示DHCP服务的状态，显示DHCP地址池的信息，显示接口DHCP服务器状态、在用地址信息	Monitor

菜单/页签			功能说明	用户级别
			设置DHCP服务的使能状态，新建、修改、删除DHCP地址池，修改接口DHCP服务器状态	Configure
	DNS	静态域名解析	显示、新建、修改、删除静态域名解析	Configure
		动态域名解析	显示、设置动态域名解析的功能的相关参数，显示、添加、删除IP地址和域名后缀	Configure
	PPPoE	Client信息	显示PPPoE Client的信息	Monitor
			新建、修改、删除PPPoE Client	Configure
		会话信息	显示PPPoE会话的概要信息和统计信息	Monitor
	服务管理		显示各种服务的启动情况	Configure
			设置是否启用各种服务，并设置相关的参数	Management
	诊断工具	IPv4 Ping	执行对IPv4地址或主机名的Ping操作并显示执行结果	Visitor
		IPv6 Ping	执行对IPv6地址或主机名的Ping操作并显示执行结果	Visitor
		Trace Route	执行Trace Route操作并显示执行结果	Visitor
无线服务	接入服务		显示接入服务	Monitor
			新建、设置接入服务，添加MAC认证列表	Configure
	WDS	WDS设置	显示WDS服务	Monitor
			设置WDS服务	Configure
		WDS全局设置	显示WDS全局设置	Monitor
			对WDS全局参数进行设置	Configure
射频	射频设置		显示射频状态，包括射频模式、射频状态	Monitor
			设置射频参数，包括802.11n设置	Configure
	速率设置		显示速率设置	Monitor
			设置速率，包括MCS索引设置	Configure
	信道扫描		显示信道扫描，包括扫描模式、扫描类型、扫描间隔等；并且可以查看AP的工作模式（普通、监测、混合）	Monitor
			设置信道扫描，包括扫描模式、扫描类型等；并且可以对AP的工作模式（普通、监测、混合）进行设置	Configure
	功率信道优化	功率信道信息	显示或刷新AP的状态，包括AP所处的信道和功率大小	Monitor
		参数设置	显示射频的参数	Monitor
			对射频的参数进行设置	Configure
	信道环境检测		显示检测记录、历史记录	Monitor
			显示、刷新或刷新检测记录、历史记录	Configure
	天线切换		对AP的天线进行设置	Configure
认证	AAA	域设置	显示ISP域的配置信息	Monitor

菜单/页签			功能说明	用户级别
			新建、删除ISP域	Management
		认证	显示ISP域AAA认证方法的配置信息	Monitor
			设置ISP域的AAA认证方法	Management
		授权	显示ISP域AAA授权方法的配置信息	Monitor
			设置ISP域的AAA授权方法	Management
		计费	显示ISP域AAA计费方法的配置信息	Monitor
			设置ISP域的AAA计费方法	Management
	RADIUS		显示、新建、修改、删除RADIUS方案	Management
	HWTACACS	HWTACACS服务器配置	显示、修改HWTACACS服务器信息	Management
		HWTACACS参数设置	显示、修改HWTACACS参数信息	Management
	用户	本地用户	显示本地用户的配置信息	Monitor
			新建、修改、删除本地用户	Management
		用户组	显示用户组的配置信息	Monitor
			新建、修改、删除用户组	Management
		来宾用户	显示来宾用户的配置信息	Monitor
			新建、修改、删除来宾用户	Management
	证书管理	PKI实体	显示PKI实体的信息	Monitor
			新建、修改、删除PKI实体	Configure
		PKI域	显示PKI域的信息	Monitor
			新建、修改、删除PKI域	Configure
		证书	显示PKI域的证书信息，查看证书的详细内容	Monitor
			创建密钥、销毁密钥、获取证书、申请证书、删除证书	Configure
		CRL	查看CRL	Monitor
			获取CRL	Configure
安全	入侵检测	入侵检测设置	显示入侵检测的设置	Monitor
			设置入侵检测，包括泛洪攻击检测、spoof攻击检测和weak-iv攻击检测	Configure
		历史记录	显示入侵检测的历史记录	Monitor
			清空入侵检测的历史记录，把检测到的入侵设备加入黑名单	Configure
		统计信息	显示入侵检测的统计信息	Monitor
			清空入侵检测的统计信息	Configure

菜单/页签			功能说明	用户级别
	黑白名单	黑名单	显示动态黑名单、静态黑名单	Monitor
			清空动态黑名单、静态黑名单，使能动态黑名单，添加静态黑名单	Configure
		白名单	显示白名单	Monitor
			清空白名单，添加白名单	Configure
	用户隔离		开启或关闭用户隔离功能	Configure
QoS	时间段	显示	显示时间段的配置信息	Monitor
		新建	新建时间段	Configure
		删除	删除时间段	Configure
	ACL IPv4	显示	显示IPv4 ACL的配置信息	Monitor
		新建	新建IPv4 ACL	Configure
		基本配置	设置基本IPv4 ACL规则	Configure
		高级配置	设置高级IPv4 ACL规则	Configure
		链路层配置	设置链路层IPv4 ACL规则	Configure
		无线配置	设置WLAN-AP ACL规则	Configure
		删除	删除IPv4 ACL或其规则	Configure
	ACL IPv6	显示	显示IPv6 ACL的配置信息	Monitor
		新建	新建IPv6 ACL	Configure
		基本配置	设置基本IPv6 ACL规则	Configure
		高级配置	设置高级IPv6 ACL规则	Configure
		删除	删除IPv6 ACL或其规则	Configure
	无线服务质量	服务质量设置	显示无线服务质量，包括SVP报文映射、CAC策略、射频EDCA和用户EDCA	Monitor
			设置无线服务质量，包括SVP报文映射、CAC策略、射频EDCA和用户EDCA	Configure
		射频信息	显示射频信息，包括WMM状态和射频详细信息	Monitor
			显示射频信息，包括WMM状态和射频详细信息，清空射频信息	Configure
		客户端信息	显示客户端信息，包括WMM状态和客户端详细信息	Monitor
			显示客户端信息，包括WMM状态和客户端详细信息，清空客户端信息	Configure
		用户限速	显示已配置的用户限速信息	Monitor
			新建、修改用户限速模式、方向及速率	Configure
		智能带宽保障	显示智能带宽保障功能的配置情况、查看带宽信息	Monitor

菜单/页签			功能说明	用户级别
			配置智能带宽保障功能	Configure
	信任模式		显示端口优先级信任模式的配置信息	Management
			设置端口优先级信任模式	Management
	类	显示	显示类的配置信息	Monitor
		新建	新建类	Configure
		设置	设置类的分类规则	Configure
		删除	删除类或其分类规则	Configure
	流行为	显示	显示流行为的配置信息	Monitor
		新建	新建流行为	Configure
		设置	设置流行为的动作	Configure
		删除	删除流行为	Configure
	QoS Policy	显示	显示QoS策略的配置信息	Monitor
		新建	新建QoS策略	Configure
		设置	设置QoS策略中类和流行为的对应关系	Configure
		删除	删除策略或其中的类和流行为对应关系	Configure
	端口策略	显示	显示端口上应用QoS策略的配置信息	Monitor
		设置	设置在端口上应用QoS策略	Configure
		删除	删除端口上的QoS策略应用	Configure
	服务策略		显示在无线接口上应用QoS策略的配置信息	Monitor
			设置在无线接口上应用QoS策略	Configure
高级设置	区域码		显示区域码	Monitor
			修改区域码	Configure
	形态切换		显示AP形态切换	Monitor
			可以对AP形态进行切换	Configure
	常发模式		显示AP的常发模式	Monitor
			可以对AP的常发模式进行切换	Configure
	上行链路检测		显示上行链路接口	Monitor
			可以对上行链路接口进行设置	Configure
	信道利用率		显示信道利用率结果	Monitor
			对信道利用率进行评估，输出的信道利用率结果	Configure
	频谱导航		显示频谱导航的设置情况	Monitor
			设置频谱导航功能的参数	Configure

菜单/页签		功能说明	用户级别
	组播优化	设置组播优化功能的参数	Configure

1.7 Web页面常用元素

1.7.1 常用按钮和图标

表1-2 Web 页面常用按钮和图标

按钮和图标	功能
确定、应用	用于使当前页面的配置内容生效
取消	用于取消当前页面的配置内容，使页面跳转回相应的列表显示页面
刷新	用于刷新当前页面的显示信息
清空	用于删除列表中的所有项或清除所有统计信息
新建	用于进入新建表项的页面
删除、删除选中	用于删除列表中被选中的表项
全部选中	用于选中列表框中的所有选项或设备面板上的所有端口
全部取消	用于将列表框中的所有选项或设备面板上的所有端口置为非选中状态
恢复缺省	用于将当前配置页面中的所有配置项的取值恢复到缺省情况
下一步	一般出现在配置向导的页面中，用于将当前步骤的配置缓存起来（不生效），并进入下一个配置步骤的页面
上一步	一般出现在配置向导的页面中，用于将当前步骤的配置缓存起来（不生效），并返回到上一个配置步骤的页面
完成	一般出现在配置向导的页面中，用于使所有配置步骤的配置生效
	一般出现在显示页面列表的“操作”列中，用于进入相应表项的修改页面，以便对该表项的详细配置进行查看或修改
	一般出现在显示页面列表的“操作”列中，用于删除相应的表项

1.7.2 列表分页显示功能

对于某些列表显示页面，Web 界面提供了列表分页显示功能，如下图所示的列表的下方。当列表中包含较多表项时，用户可以根据需要设置每页显示多少条信息，可以选择查看首页、上一页、下一页、尾页的内容，或者直接跳转到要查看的页。

图1-4 分页显示功能



1.7.3 列表查询显示功能

对于某些列表显示页面，Web 界面提供了简单查询和高级查询的功能。当列表中包含较多表项时，用户可以通过查询功能使列表中只显示符合指定查询条件的表项，方便用户的查看。

1. 简单查询

在如 图 1-4 所示的列表上方的文本框中输入查询关键字，选择要查询的标题项，单击<查询>按钮即可。如下图所示的例子为查询MAC地址中包含“00e0”的表项。

图1-5 简单查询功能举例



2. 高级查询

在如 图 1-4 所示的列表上方单击“高级查询”，弹出“高级查询”的页面，如下图所示。设置高级查询的条件后，单击<确定>按钮，页面即可按照指定的查询条件来显示。

图1-6 高级查询



举例说明高级查询功能的使用：ARP表显示页面如 图 1-4 所示，要查看MAC地址以“000f”开头，且IP地址范围为 192.168.1.50～192.168.1.59 的ARP表项。进行如下操作：

(1) 单击“高级查询”。

(2) 进行如下图所示的设置。

图1-7 高级查询功能举例（一）



(3) 单击<确定>按钮。此时，页面显示 MAC 地址以“000f”开头的 ARP 表项信息。

(4) 再次单击“高级查询”。

(5) 进行如下图所示的设置。

图1-8 高级查询功能举例（二）



(6) 单击<确定>按钮。此时，页面显示 MAC 地址以“000f”开头，且 IP 地址范围为 192.168.1.50～192.168.1.59 的 ARP 表项信息，如下图所示。

图1-9 高级查询功能（三）



1.7.4 列表排序显示功能

对于某些列表显示页面，Web 界面提供了简单排序和高级排序的功能。当列表中包含较多表项时，用户可以通过排序显示功能使列表中的表项按照一定的顺序显示，方便用户的查看。

1. 简单排序

在列表中单击字体颜色为浅蓝色的标题项，可使列表按照该标题项中的内容的升序顺序排序显示。再次单击该标题项，可使列表按照该标题项中的内容的降序顺序排序显示。依此类推。

排序显示时的页面如下图所示，当前排序标题项的右边会出现一个箭头，箭头向上表示升序排序，箭头向下表示降序排序。

图1-10 简单排序显示功能举例（按 IP 地址降序显示）



1.8 Web网管使用限制

- Web 网管支持的操作系统包括：Windows XP、Windows 2000、Windows Server 2003 企业版、Windows Server 2003 标准版、Windows Vista、Windows 7、Windows 8、Linux 和 MAC OS。
- Web 网管支持的浏览器包括：Microsoft Internet Explorer 6.0 SP2 及以上版本、Mozilla Firefox 3.0 及以上版本、Google Chrome 2.0.174.0 及以上版本。
- Web 网管不支持浏览器自带的后退、前进、刷新等按钮。使用这些按钮可能会导致 Web 页面显示不正常。
- 由于 Windows 操作系统自带的防火墙会对 TCP 连接数进行限制，使用 Web 网管时偶尔会出现无法打开 Web 网管页面的情况。为了避免这种情况，建议关闭 Windows 自带的防火墙。
- 设备的软件版本变化后，在通过 Web 网管登录设备时，建议先清除浏览器的缓存数据，否则 Web 网管的内容可能无法正确显示。
- Web 网管中，支持分页显示功能的列表最多只能显示 2 万条表项。

1.9 Web网管使用常见问题举例

1.9.1 无法通过Web网管正常访问设备

1. 问题现象

用户可以 Ping 通设备，可以通过 Telnet 登录到设备上，HTTP 服务已经启用，并且使用的操作系统和浏览器版本都符合 Web 网管的要求。但是，无法正常访问设备的 Web 网管。

2. 问题分析

- 使用 Microsoft Internet Explorer 浏览器时，以下功能必须都处于启用状态，才能正常访问 Web 网管：对标记为可安全执行脚本的 ActiveX 控件执行脚本、运行 ActiveX 控件和插件、活动脚本。
- 使用 Mozilla Firefox 浏览器时，必须启用 JavaScript，才能正常访问 Web 网管。

3. Internet Explorer浏览器处理过程

(1) 启动 Internet Explorer 浏览器，选择“工具 > Internet 选项”菜单项。

(2) 单击“安全”页签，选中要访问的站点所在的区域，如下图所示。

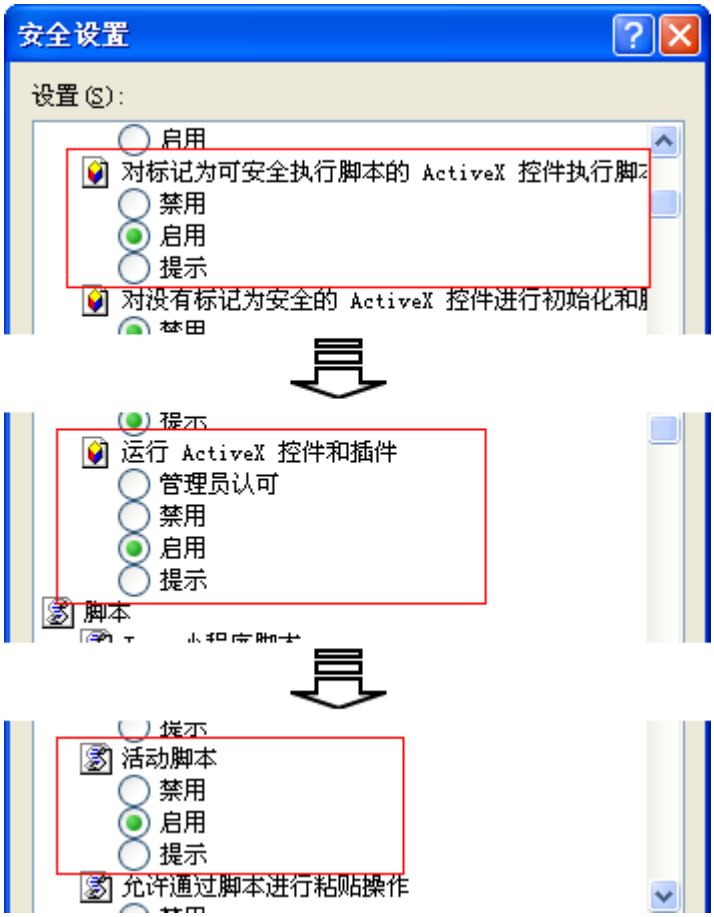
图1-11 Internet Explorer 浏览器设置（一）



(3) 单击<自定义级别>按钮，弹出“安全设置”对话框。

(4) 如下图所示，设置启用以下功能：对标记为可安全执行脚本的 ActiveX 控件执行脚本、运行 ActiveX 控件和插件、活动脚本。

图1-12 Internet Explorer 浏览器设置（二）



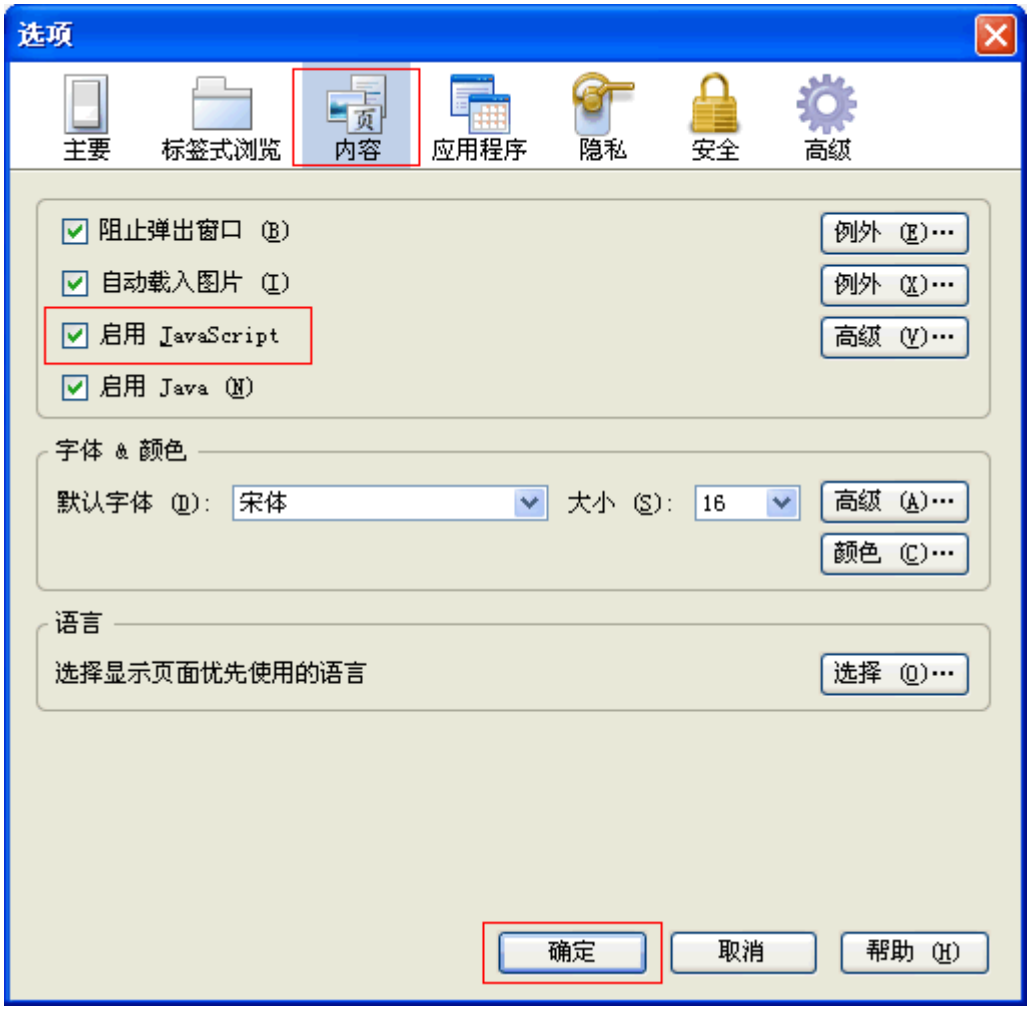
(5) 在“安全设置”对话框中单击<确定>按钮完成操作。

4. Firefox浏览器处理过程

(1) 启动 Firefox 浏览器，选择“工具 > 选项”菜单项。

(2) 如下图所示，单击“内容”页签，选中“启用 JavaScript”前的复选框，单击<确定>按钮完成操作。

图1-13 Firefox 浏览器设置



目 录

1 快速配置 ····· 1-1
1.1 概述 ····· 1-1
1.2 快速配置 ····· 1-1
1.2.1 快速配置首页面 ····· 1-1
1.2.2 基本设置 ····· 1-2
1.2.3 Admin设置 ····· 1-3
1.2.4 IP设置 ····· 1-4
1.2.5 无线设置 ····· 1-5
1.2.6 RADIUS设置 ····· 1-6
1.2.7 加密设置 ····· 1-8
1.2.8 Radio设置 ····· 1-9
1.2.9 配置汇总 ····· 1-11
1.3 快速配置举例 ····· 1-11
1.3.1 明文无线接入快速配置举例 ····· 1-11
1.3.2 WEP（Open-System）加密无线接入快速配置举例 ····· 1-13

1 快速配置

说明

手册中设备的接口类型、显示信息与设备型号、支持射频情况和配置信息相关，实际使用中还请以设备的实际情况为准。

1.1 概述

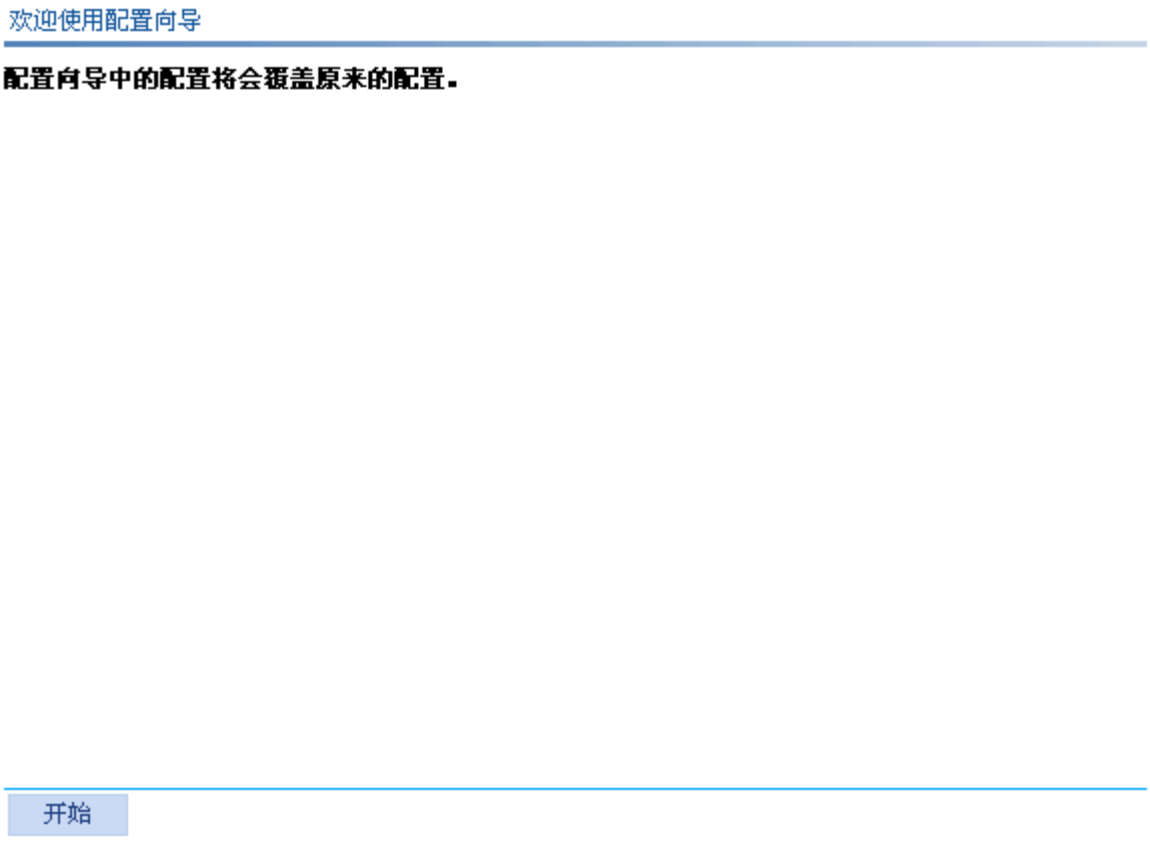
快速配置功能给用户提供向导，执行该功能后，系统会通过提示信息指导用户逐项输入设备的基本参数（比如基本设置、Admin 设置、IP 设置等），以便迅速将设备配置到可以运行的状态，用户不再需要通过多个页面来分别配置这些参数，从而简化了用户的配置。

1.2 快速配置

1.2.1 快速配置首页面

在导航栏中选择“快速配置”，进入快速配置向导首页面，如下图所示。

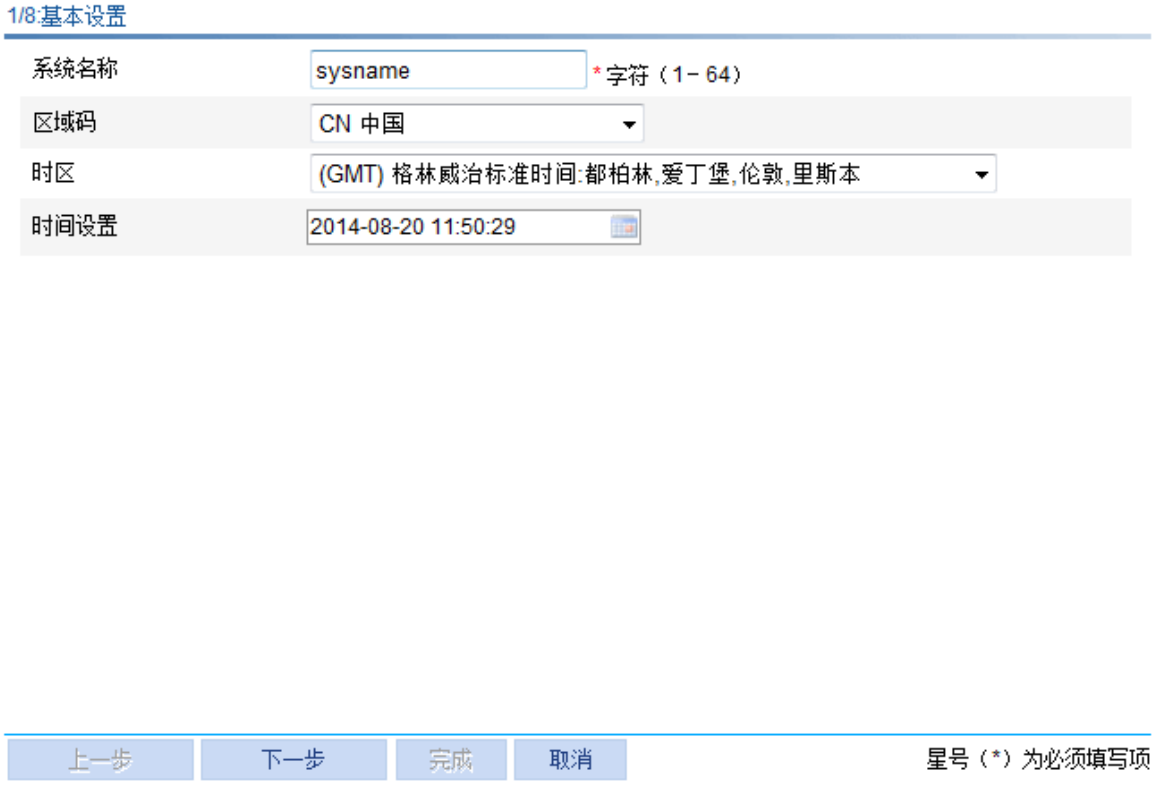
图1-1 快速配置向导首页面



1.2.2 基本设置

在快速配置向导首页面单击<开始>按钮，进入基本设置页面，如下图所示。

图1-2 基本设置页面



基本设置页面的参数说明如下表所示。

表1-1 基本设置页面的参数说明

配置项	说明
系统名称	当前设备的名称 缺省情况下，设备名称为设备型号
区域码	区域码用来标识使用射频所在的国家，它规定了射频特性，如功率和可用于帧传输的信道总数。在配置设备之前，必须配置有效的区域码
时区	系统时区设置
时间设置	当前时间和日期

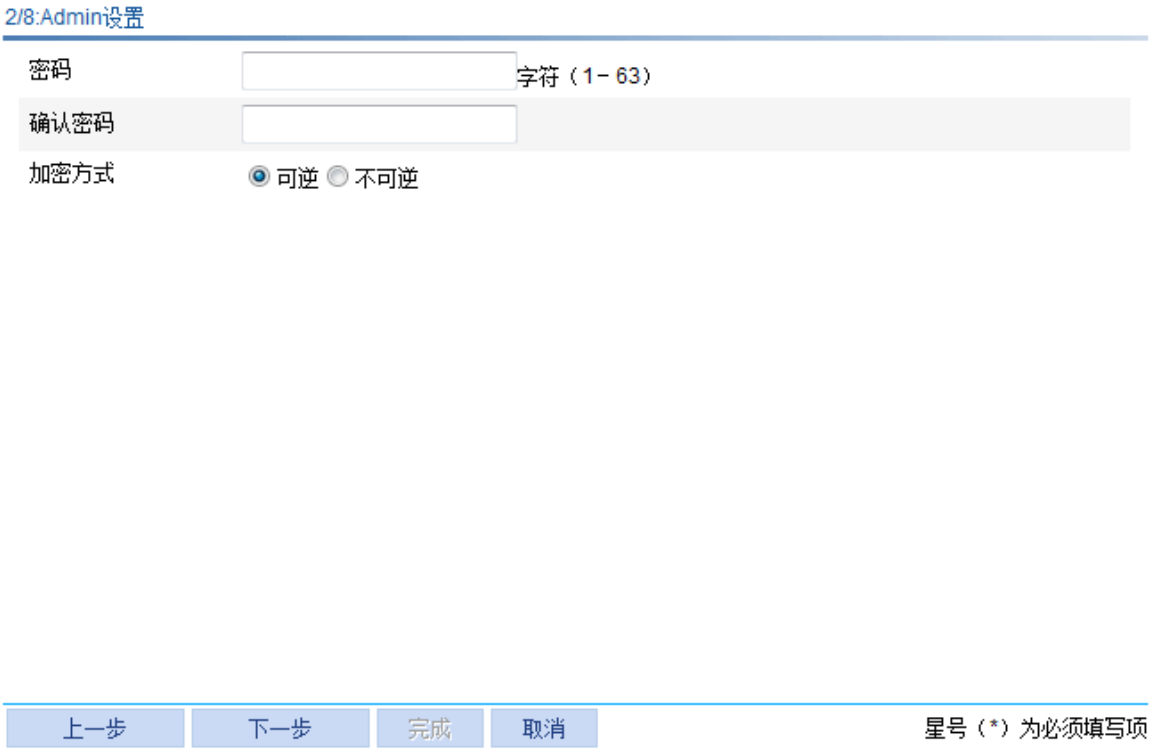
说明

如果区域码设置选框显灰，则表示该区域码已经被锁定，在这种情况下，用户不能更改此项设置。

1.2.3 Admin设置

在基本设置页面中单击<下一步>按钮，进入 Admin 设置页面，如下图所示。

图1-3 Admin 设置页面



Admin 设置页面的参数说明如下表所示。

表1-2 Admin 设置页面的参数说明

配置项	说明
密码	配置用户“Admin”登录设备时的密码
确认密码	确认密码，必须与指定的用户“Admin”的密码一致
加密方式	• 可逆：表示设备以可逆的加密算法对用户密码加密后保存 • 不可逆：表示设备以不可逆的加密算法对用户密码加密后保存

1.2.4 IP设置

在 Admin 设置页面中单击<下一步>按钮，进入 IP 设置页面，如下图所示。

图1-4 IP 设置页面



IP 设置页面的参数说明如下表所示。

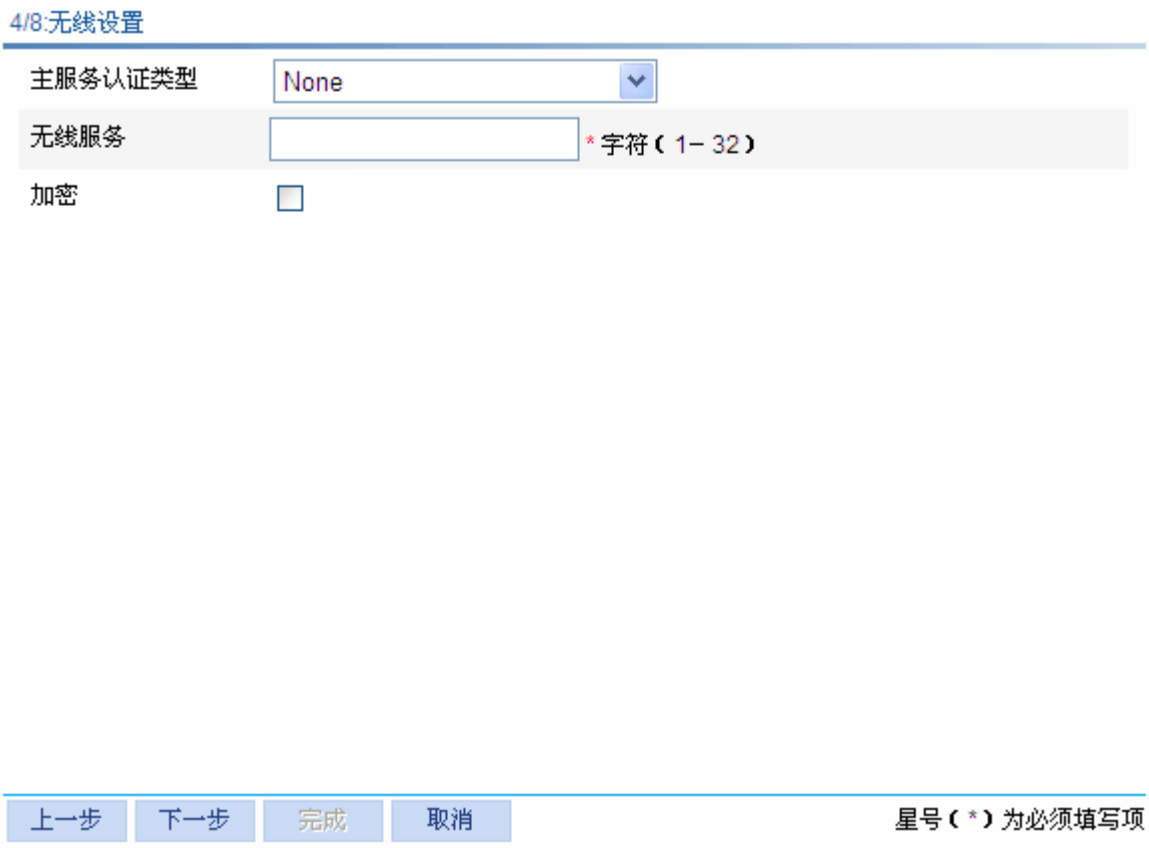
表1-3 IP 设置页面的参数说明

配置项	说明
IP地址	Vlan-interface1的IP地址，可通过该IP地址登录设备 IP地址的缺省情况为192.168.0.50
掩码	Vlan-interface1的IP地址的子网掩码 缺省情况下，掩码为24位
默认网关	当前无线设备连接到网络中的默认网关 缺省情况下，没有配置默认网关

1.2.5 无线设置

在 IP 设置页面中单击<下一步>按钮，进入无线设置页面，如下图所示。

图1-5 无线设置页面



无线设置页面的参数说明如下表所示。

表1-4 无线设置页面的参数说明

配置项	说明
主服务认证类型	无线服务的认证类型，包括以下两种： • None：不认证 • User authentication (802.1X)：使用 802.1X 认证 缺省情况下，采用None方式，如果选择None方式，即不使用“主服务认证”，那么会省略快速配置中“5/8 :RADIUS设置”步骤
无线服务	表示SSID（Service Set Identifier，服务集标识符）
加密	选中加密前面的复选框，才会进入“6/8:加密设置”步骤 缺省情况下，不对无线服务进行加密，如果不选择此项，那么会省略快速配置中“6/8:加密设置”步骤

1.2.6 RADIUS设置

当在无线设置页面中选择主服务认证类型为 User authentication (802.1X)，单击<下一步>按钮将进入 RADIUS 设置页面，如下图所示。

图1-6 RADIUS 设置页面



RADIUS 设置页面的参数说明如下表所示。

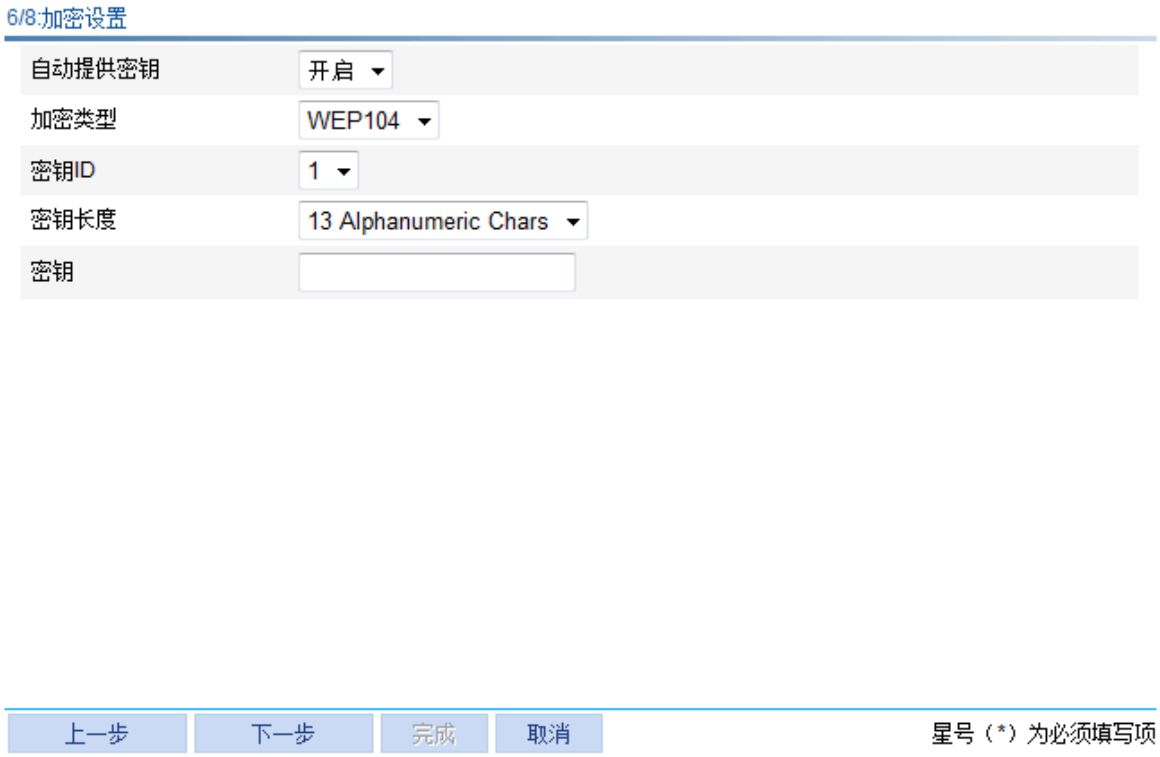
表1-5 RADIUS 设置页面的参数说明

配置项	说明
服务器类型	设置支持何种类型的RADIUS服务器 • extended：指定 extended 的 RADIUS 服务器（一般为 CAMS/iMC），即要求 RADIUS 客户端（设备系统）和 RADIUS 服务器按照私有 RADIUS 协议的规程和报文格式进行交互 • standard：指定 standard 类型的 RADIUS 服务器，即要求 RADIUS 客户端（设备系统）和 RADIUS 服务器按照标准 RADIUS 协议（RFC 2138/2139 或更新）的规程和报文格式进行交互
认证服务器IP地址	RADIUS认证服务器的IP地址
认证服务器UDP端口	RADIUS认证服务器的端口号
认证服务器共享密钥	RADIUS认证服务器的共享密钥
计费服务器IP地址	RADIUS计费服务器的IP地址
计费服务器UDP端口	RADIUS计费服务器的端口号
计费服务器共享密钥	RADIUS计费服务器的共享密钥

1.2.7 加密设置

如果在无线设置页面中选中“加密”前面的复选框，会进入加密设置页面，如下图所示。

图1-7 加密设置页面



选择 WEP 加密类型时，页面的参数说明如下表所示。

表1-6 加密设置页面的参数说明

配置项	说明
自动提供密钥	使用自动提供WEP密钥方式 • 开启：使用自动提供 WEP 密钥方式 • 关闭：使用静态 WEP 密钥方式 缺省情况下，使用静态WEP密钥方式 选择自动提供WEP密钥方式后，“密钥类型”选项会自动使用WEP 104加密方式 提示 自动提供 WEP 密钥必须和 802.1x 认证方式一起使用，因此只有选择无线设置页面中的“User authentication (802.1X)”后，此选项才可配置
密钥类型	WEP加密机制的密钥类型，包括WEP40、WEP104和WEP 128三种密钥长度

配置项	说明
密钥ID	• 1：选择密钥索引为 1 • 2：选择密钥索引为 2 • 3：选择密钥索引为 3 • 4：选择密钥索引为 4 WEP中的密钥索引号（WEP中有四个静态的密钥），其密钥索引分别是1、2、3和4。指定的密钥索引所对应的密钥将被用来进行帧的加密和解密 提示 如果开启“自动提供密钥”，密钥 ID 只能在 1～3 中选择
密钥长度	密钥的长度： • 当密钥类型选择 WEP40 时，可选的密钥长度 5 个字符（5 Alphanumeric Chars）或者 10 位 16 进制数（10 Hexadecimal Chars） • 当密钥类型选择 WEP104 时，可选的密钥长度 13 个字符（13 Alphanumeric Chars）或者 26 位 16 进制数（26 Hexadecimal Chars） • 当密钥类型选择 WEP128 时，可选的密钥长度 16 个字符（16 Alphanumeric Chars）或者 32 位 16 进制数（32 Hexadecimal Chars）
密钥	配置WEP密钥

选择 TKIP 或 AES-CCMP 加密类型时，设置页面的参数说明如下表所示。

表1-7 TKIP 或 AES-CCMP 加密设置页面的参数说明

配置项	说明
加密类型	• TKIP：采用 TKIP 加密方式 • AES-CCMP：采用 AES-CCMP 加密方式
安全IE	配置无线报文中携带的安全IE，安全IE用来通告AP具有的安全机制： • WPA：在 802.11i 协议之前，Wi-Fi Protected Access 定义的安全机制 • WPA2：802.11i 定义的安全机制，也就是 RSN（Robust Security Network，健壮安全网络）安全机制，提供比 WEP 和 WPA 更强的安全性
端口模式	目前只支持PSK（Pre-Shared Key，预共享密钥）方式
预共享密钥类型	• pass-phrase：以字符串方式输入预共享密钥 • raw-key：以十六进制数方式输入预共享密钥
预共享密钥	配置预共享密钥

1.2.8 Radio设置

进入如下图所示 Radio 设置页面。

图1-8 Radio 设置页面



Radio 设置页面的参数说明如下表所示。

表1-8 Radio 设置页面参数说明

配置项	说明
射频单元	显示AP的射频单元。
射频模式	显示AP的射频模式
信道	指定射频的工作信道。信道列表由国家码和射频模式决定。 Auto：自动选择信道模式。选择此模式后，AP会评估无线网络中的信道质量，自动选择质量最优的信道作为工作信道 更改工作信道设置后，功率列表会自动刷新
功率	选择发射功率大小 射频的最大功率和国家码、信道、AP型号、射频模式和天线类型相关，如果采用802.11n射频模式，那么射频的最大功率和带宽模式也相关
选中射频单元前面的复选框，将“1.2.5 无线设置”中设置的无线服务和指定射频进行绑定 说明 用户可以根据实际组网需求，在射频模式、信道和功率下列框中选择需要的参数。需要注意的是，只有选中射频单元前面的复选框，将无线服务和指定的 Radio 绑定后，这些参数配置才能生效	

1.2.9 配置汇总

在 Radio 设置页面中单击<下一步>按钮，进入配置汇总页面。配置汇总页面显示了快速配置页面中的配置信息，单击<完成>按钮完成快速配置。

1.3 快速配置举例

说明

目前通过快速配置页面能够完成的无线接入方式有：明文方式、WEP（Open-System）加密方式、WPA-PSK 和 WPA2-PSK 认证方式，如果需要采取其它的无线接入方式（如 MAC 地址认证、远程 802.1x 认证等），可以进入“无线服务 > 接入服务”页面进行配置，相关配置请参见“无线服务”中的配置举例。

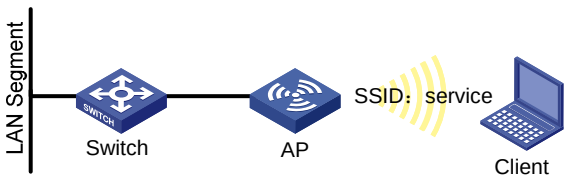
1.3.1 明文无线接入快速配置举例

1. 组网需求

某部门为了保证工作人员可以随时随地访问部门内部的网络资源，需要通过部署 AP 实现移动办公。设备管理员可以通过快速配置页面完成明文无线接入配置，具体要求如下：

- AP 提供 SSID 为“service”的明文方式的无线接入服务。
- 为了满足高带宽要求，并兼容现有的 802.11g 无线网络，采用 802.11n（2.4GHz）射频模式。

图1-9 明文无线接入组网图



2. 配置AP

(1) 配置基本业务

在导航栏中选择“快速配置”，根据实际需求在 1～3 步完成时间参数、登录设备时的密码、登录设备的 IP 地址等基本设置。

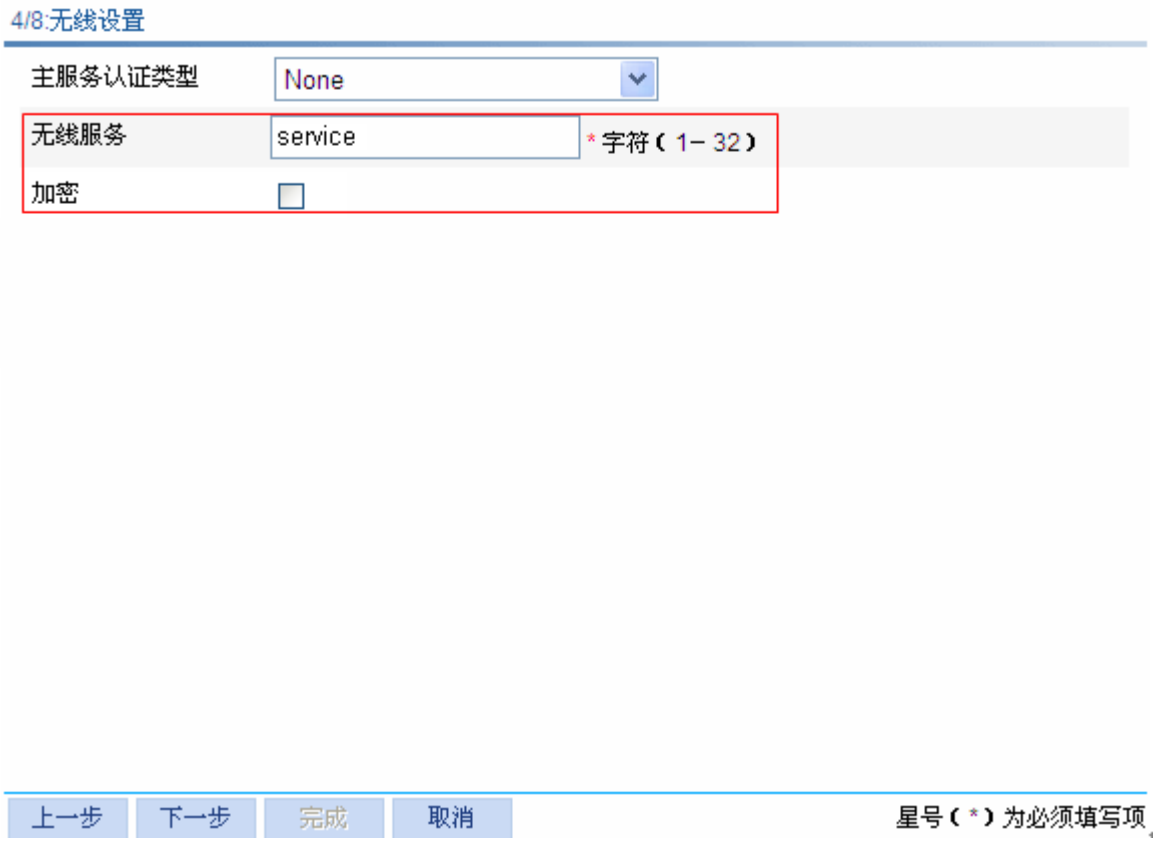
(2) 配置无线服务

步骤 1：在 IP 设置页面中单击<下一步>按钮，进入无线设置页面。

步骤 2：进行如下配置，如下图所示。

- 主服务认证类型保持缺省设置。
- 设置无线服务名称为“service”。
- 加密类型保持缺省设置，即不加密。

图1-10 无线设置页面



步骤 3：单击<下一步>按钮，进入如下图所示 Radio 设置页面。

步骤 4：选中 802.11n（2.4GHz）前面的复选框，将无线服务“service”和 802.11n（2.4GHz）射频进行绑定。其它参数保持缺省设置。

步骤 5：单击<下一步>按钮。

图1-11 Radio 设置页面



(3) 确认配置，执行操作

单击<下一步>按钮，进入配置汇总页面。确认设置的数据是否正确，如果需要修改，则单击<上一步>按钮，可以返回到前面的页面对配置进行修改；如果确认设置的数据正确，则单击<完成>按钮，即可执行已完成的设置。

3. 验证配置结果

- 打开无线客户端，刷新网络列表，在“选择无线网络”列表里找到配置的网络服务（此例中为 service），单击<连接>。客户端成功关联 AP 后，可以访问无线网络。
- 在导航栏中选择“概览 > 客户端”，可以查看成功上线的客户端。

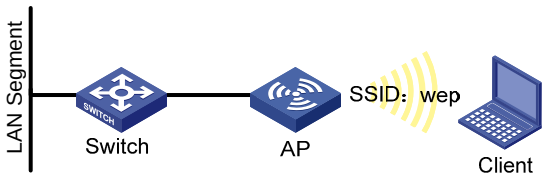
1.3.2 WEP（Open-System）加密无线接入快速配置举例

1. 组网需求

在一个小型办公室中，设备管理员可以通过快速配置页面完成 WEP（Open-System）加密配置，具体要求如下：

- AP 提供 SSID 为“wep”的 WEP（Open-System）加密无线接入服务。
- 为了满足高带宽要求，并兼容现有的 802.11g 无线网络，采用 802.11n（2.4GHz）射频模式。

图1-12 WEP（Open-System）加密无线接入组网图



2. 配置AP

(1) 配置基本业务

在导航栏中选择“快速配置”，根据实际需求在 1～3 步完成时间参数、登录设备时的密码、登录设备的 IP 地址等基本设置。

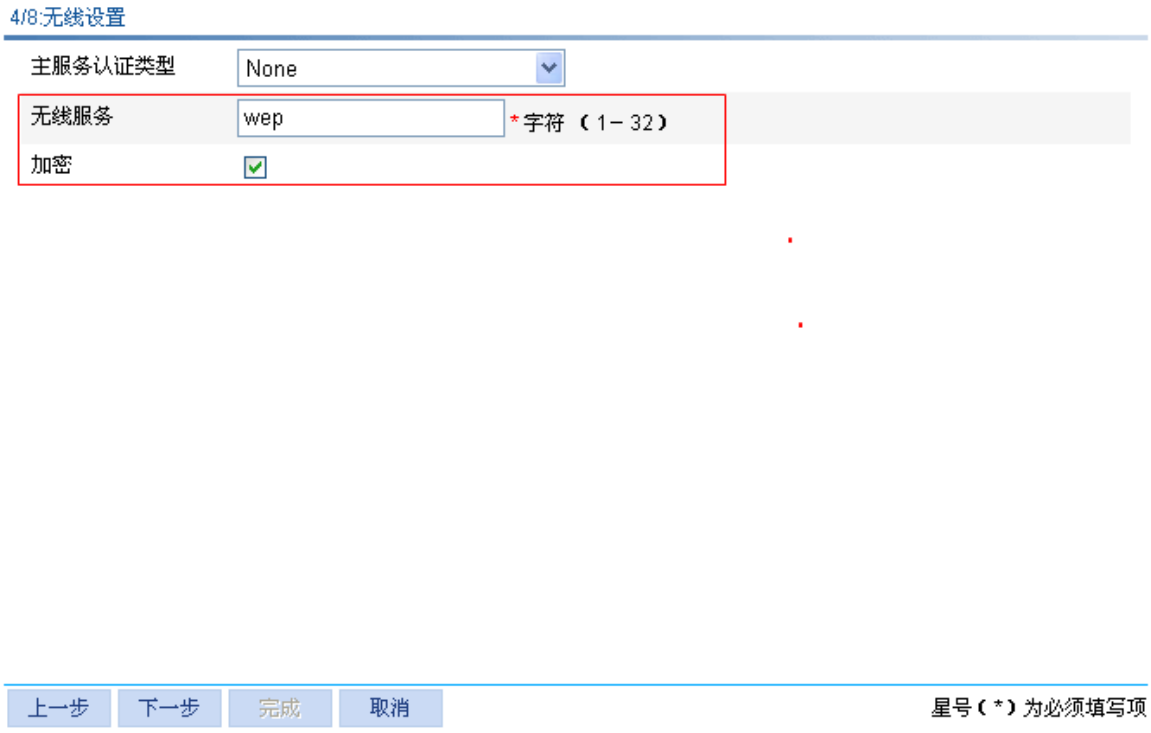
(2) 配置无线服务

步骤 1：在 IP 设置页面中单击<下一步>按钮，进入如下图所示无线设置页面。

步骤 2：进行如下配置，如下图所示。

- 主服务认证类型保持缺省设置。
- 设置无线服务名称为“wep”。
- 选中加密选项前的复选框。

图1-13 无线设置页面

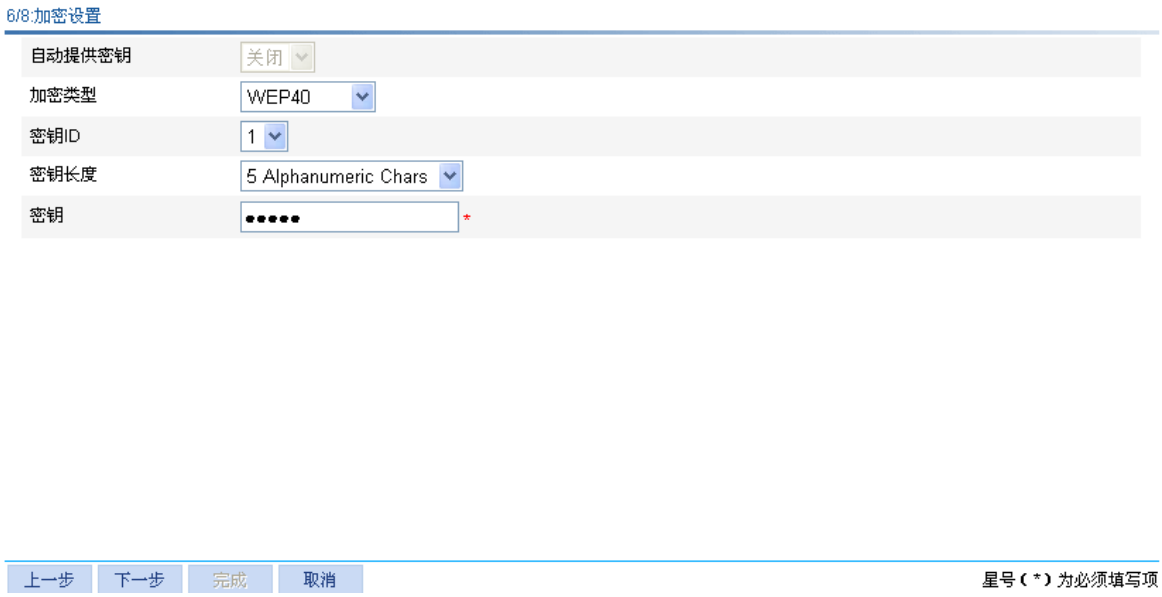


步骤 3：单击<下一步>按钮，进入如下图所示加密设置页面。

- 在“加密类型”下拉框中选择“WEP40”。
- 在“密钥 ID”下拉框中选择密钥索引为“1”。

- 在“密钥长度”下拉框中选择“5 Alphanumeric Chars”。
- 在密钥输入栏中设置 WEP 密钥为“12345”。

图1-14 加密设置页面

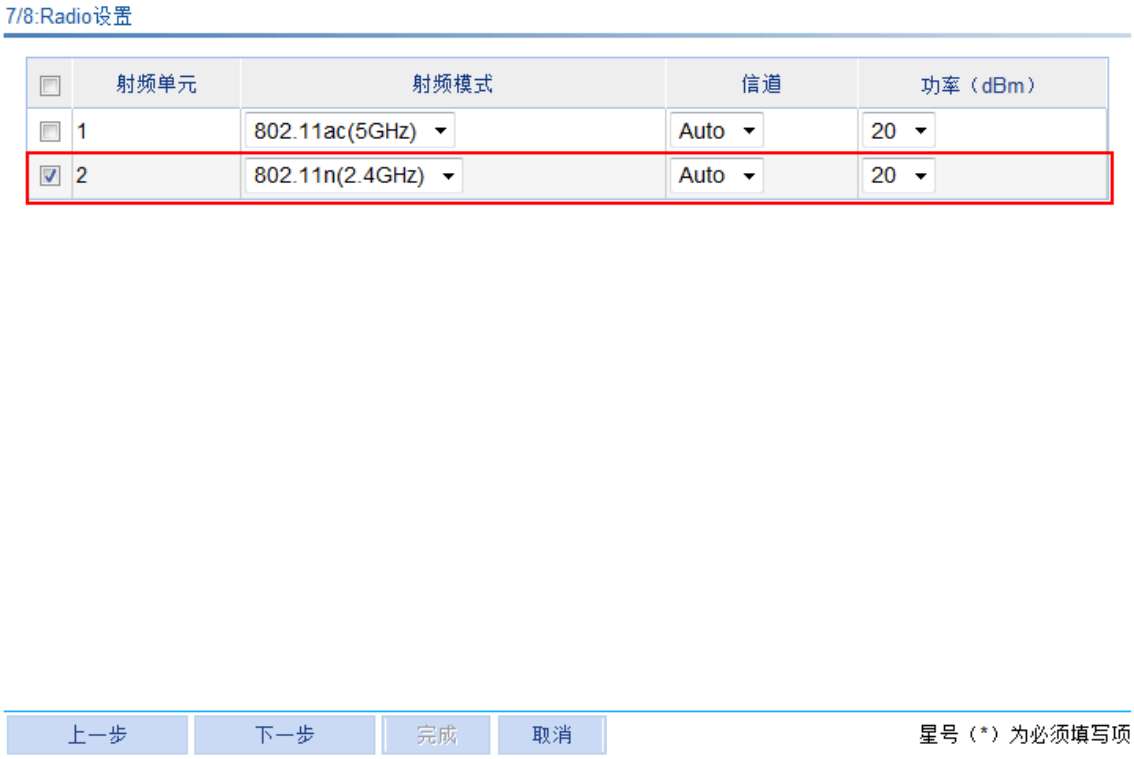


步骤 4：单击<下一步>按钮，进入如下图所示 Radio 设置页面。

步骤 5：选中 802.11n（2.4GHz）前面的复选框，将无线服务“wep”和 802.11n（2.4GHz）射频进行绑定。其它参数保持缺省设置。

步骤 6：单击<下一步>按钮。

图1-15 Radio 设置页面



(3) 确认配置，执行操作

单击<下一步>按钮，进入配置汇总页面。确认设置的数据是否正确，如果需要修改，则单击<上一步>按钮，可以返回到前面的页面对配置进行修改；如果确认设置的数据正确，则单击<完成>按钮，即可执行已完成的设置。

3. 验证配置结果

- 打开无线客户端，刷新网络列表，在“选择无线网络”列表里找到配置的网络服务（此例中为 WEP），单击<连接>，在弹出的对话框里输入 WEP 密钥为“12345”（即客户端中输入的 WEP 密钥必须和设备上设置的 WEP 密钥保持一致）。客户端成功关联 AP 后，可以访问无线网络。
- 在导航栏中选择“概览 > 客户端”，可以查看成功上线的客户端。

目 录

1 概览 ····· 1-1
1.1 设备概览 ····· 1-1
1.1.2 设备信息 ····· 1-2
1.1.3 系统资源状态 ····· 1-2
1.1.4 设备接口信息 ····· 1-2
1.1.5 近期发生的系统日志 ····· 1-3
1.2 查看无线服务 ····· 1-3
1.2.1 查看无线服务的详细信息 ····· 1-3
1.2.2 查看无线服务的统计信息 ····· 1-6
1.2.3 查看无线服务的连接历史信息 ····· 1-7
1.3 查看射频 ····· 1-8
1.3.1 查看与射频绑定的无线服务 ····· 1-8
1.3.2 查看射频的详细信息 ····· 1-8
1.4 查看WDS ····· 1-9
1.5 查看客户端 ····· 1-10
1.5.1 查看客户端详细信息 ····· 1-10
1.5.2 查看客户端统计信息 ····· 1-13
1.5.3 对客户端进行RFPing操作 ····· 1-14
1.5.4 查看从客户端接收到的信标测量报告 ····· 1-15

1 概览

说明

手册中设备的接口类型、显示信息与设备型号、支持射频情况和配置信息相关，实际使用中还请以设备的实际情况为准。

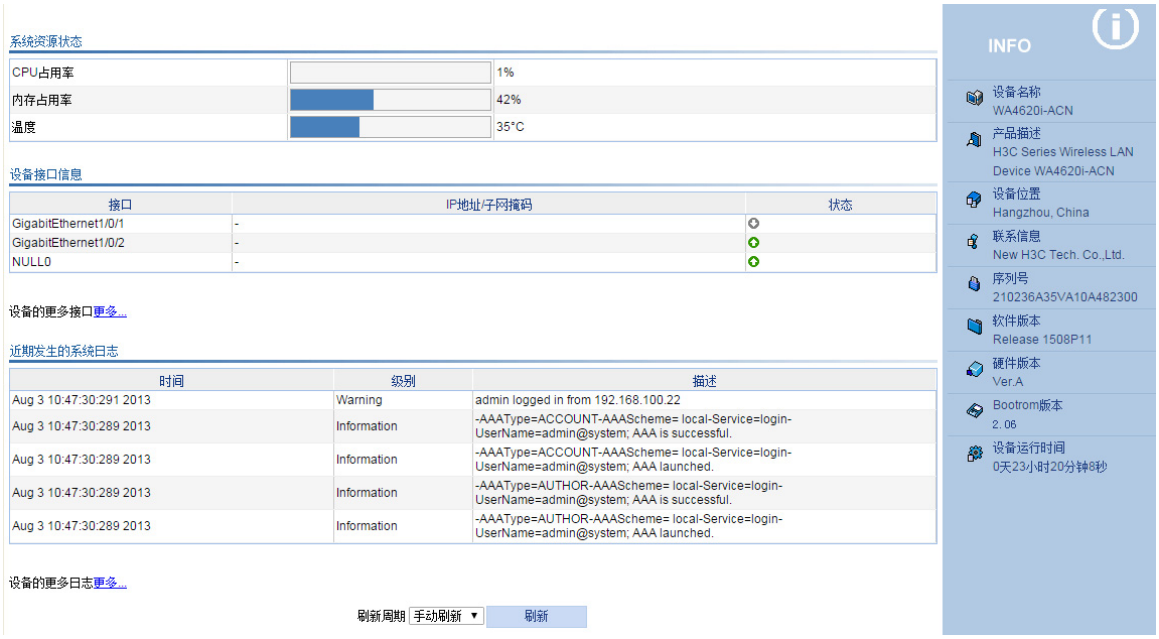
1.1 设备概览

设备概览模块可以帮助用户了解设备的状态和概要信息，具体包括以下几方面内容：

- 查看设备信息
- 查看系统资源状态
- 查看设备接口信息
- 查看近期发生的系统日志（显示最近发生的 5 条系统日志）

用户登录到 Web 后，默认进入“概览 > 设备概览”菜单的页面，如下图所示。

图1-1 设备概览



说明

设备概览的页面显示信息与设备的型号有关，请以设备的实际情况为准。

在页面下方“刷新周期”后面的下拉框中进行选择：

- 如果选择具体的刷新周期时间（如：1 分钟），则系统会根据所选的刷新周期周期性地对设备概览页面进行自动刷新。
- 如果选择“手动刷新”，则需要用户手动单击<刷新>按钮，设备概览页面内容才会刷新。

1.1.2 设备信息

对设备信息的详细说明如下表所示。

表1-1 设备信息详细说明

标题项	说明
设备名称	显示设备的型号
产品描述	显示设备产品描述信息
设备位置	显示设备的位置信息 设备位置信息可以在“设备 > SNMP”中配置，详细配置请参见“SNMP”
联系信息	显示设备维护者的联系信息 联系信息可以在“设备 > SNMP”中配置，详细配置请参见“SNMP”
序列号	显示设备的序列号
软件版本	显示设备的软件版本
硬件版本	显示设备的硬件版本
Bootrom版本	显示设备的Bootrom版本
设备运行时间	显示设备最近一次启动后连续运行的时长

1.1.3 系统资源状态

对系统资源状态的详细说明如下表所示。

表1-2 系统资源状态详细说明

标题项	说明
CPU占用率	显示CPU的实时占用率
内存占用率	显示内存的实时占用率，以及内存的总量 提示 内存总量的支持情况与设备的具体型号有关，请以设备的实际情况为准
温度	显示设备的温度

1.1.4 设备接口信息

对设备接口信息的详细说明如下表所示。

表1-3 设备接口信息详细说明

标题项	说明
接口	显示接口的名称和编号
IP地址/子网掩码	显示接口的IP地址和子网掩码
状态	显示接口的协议状态 • ：表示接口当前状态为开启，且已连接 • ：表示接口当前状态为开启，且未连接 • ：表示接口当前状态为关闭

说明

如果想了解更多的设备接口信息，可以单击“设备接口信息”列表下方的“更多...”超链接，进入“设备 > 接口管理”的页面进行查看和操作，详细内容请参见“接口管理”。

1.1.5 近期发生的系统日志

对近期发生的系统日志的详细说明如下表所示。

表1-4 近期发生的系统日志详细说明

标题项	说明
时间	显示系统日志产生的时间
级别	显示系统日志的严重程度
描述	显示系统日志的具体内容

说明

如果想了解更多的系统日志信息，可以单击“近期发生的系统日志”列表下方的“更多...”超链接，进入“设备 > 日志管理”中“日志显示”页签的页面进行查看，详细内容请参见“日志管理”。

1.2 查看无线服务

在界面左侧的导航栏中选择“概览 > 无线服务”，点击指定的无线服务后，可以查看相关的详细信息、统计信息、连接历史。

1.2.1 查看无线服务的详细信息

clear 类型无线服务的详细信息如下图所示，详细信息中的各字段解释请参见下表。

图1-2 查看 clear 类型的无线服务的详细信息



表1-5 clear 类型无线服务显示信息描述表

配置项	说明
Service Template Number	服务模板的序号
SSID	Service Set Identifier，表示设置的服务集标识符
Description	服务模板的描述字符串，Not Configured表示没有配置服务模板的描述字符串
Service Template Type	服务模板类型
Authentication Method	使用的认证类型，clear类型的无线服务只能使用Open System（开放系统认证）方式
Beacon-measurement	Enable：信标测量功能处于开启状态
Beacon-measurement Interval	信标测量请求的发送间隔，单位为秒
Beacon-measurement Type	信标测量模式： • Passive：被动模式 • Active：主动模式 • Beacon-table：信标表模式
SSID-hide	• Disable：启用 SSID 通告 • Enable：禁用 SSID 通告。SSID 隐藏后，AP 发送的信标帧里面不包含 SSID 信息
Service Template Status	服务模板状态： • Enable：无线服务处于使能状态 • Disable：无线服务处于关闭状态
Maximum clients per BSS	一个BSS中能够连接的最大客户端数

crypto 类型无线服务的详细信息如下图所示，详细信息中的各字段解释请参见下表。

图1-3 查看 crypto 类型的无线服务的详细信息

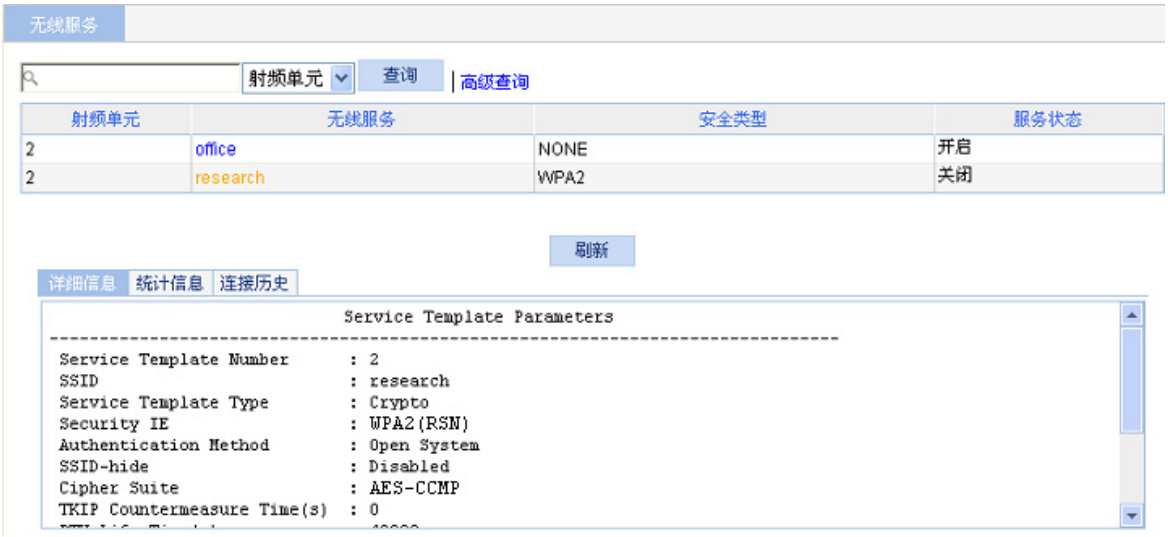


表1-6 crypto 类型无线服务显示信息描述表

配置项	说明
Service Template Number	服务模板的序号
SSID	AP提供的SSID
Description	服务模板的描述字符串，Not Configured表示没有配置服务模板的描述字符串
Service Template Type	服务模板类型
Security IE	安全IE：WPA或WPA2(RSN)
Authentication Method	使用的认证类型：Open System（开放系统认证）或者Shared Key（共享密钥认证）；
Beacon-measurement	Enable：信标测量功能处于开启状态
Beacon-measurement Interval	信标测量请求的发送间隔，单位为秒
Beacon-measurement Type	信标测量模式： • Passive：被动模式 • Active：主动模式 • Beacon-table：信标表模式
SSID-hide	• Disable：启用 SSID 通告 • Enable：禁用 SSID 通告。SSID 隐藏后，AP 发送的信标帧里面不包含 SSID 信息
WEP Key Index	加密或解密帧的密钥索引

配置项	说明
WEP Key Mode	WEP密钥模式： • HEX：WEP 密钥为 16 进制数的形式 • ASCII：WEP 密钥为字符串的形式
WEP Key	WEP密钥
Cipher Suite	加密套件：AES-CCMP、TKIP、WEP40、WEP104或WEP128
TKIP Countermeasure Time(s)	TKIP反制策略时间，单位为秒
PTK Life Time(s)	PTK生存时间，单位为秒
GTK Rekey	GTK密钥更新配置
GTK Rekey Method	GTK密钥更新方法：基于包或基于时间
GTK Rekey Time(s)	当选择基于时间的GTK密钥更新方法时，显示GTK密钥更新时间，单位为秒 当选择基于包的GTK密钥更新方法时，显示数据包的数目
PMF Status	保护管理帧功能的状态： • Disable：保护管理帧功能处于关闭状态 • Optional：保护管理帧功能处于开启状态，支持或不支持保护管理帧功能的客户端均可接入 • Mandatory：保护管理帧功能处于开启状态，且强制要求只有支持保护管理帧功能的客户端可以接入
Service Template Status	服务模板状态： • Enable：无线服务处于使能状态 • Disable：无线服务处于关闭状态
Maximum clients per BSS	一个BSS中能够连接的最大客户端数

1.2.2 查看无线服务的统计信息

无线服务的统计信息如下图所示。

图1-4 查看无线服务的统计信息



1.2.3 查看无线服务的连接历史信息

无线服务的连接历史信息如下图所示。

图1-5 查看无线服务的连接历史信息



1.3 查看射频

1.3.1 查看与射频绑定的无线服务

在界面左侧的导航栏中选择“概览 > 射频”，点击指定的射频单元后，选择“无线服务”，可以查看与射频绑定的无线服务。

图1-6 查看与射频绑定的无线服务



说明

- 表格中的“背景噪声”表示无线通信过程中遇到的各种随机的电磁波。对于背景噪声较强的环境，可以通过“增加信号功率”或“降低背景噪声”来改善 SNR（Signal-to-Noise Ratio，信噪比）。
- 资源利用率表示该射频因为收发报文占用信道的时间率，例如在 10 秒钟内，某射频收发报文占用信道的时间为 5 秒，那么该射频的资源利用率为 50%。

1.3.2 查看射频的详细信息

在界面左侧的导航栏中选择“概览 > 射频”，点击指定的射频单元后，选择“详细信息”，可以查看射频相关的详细信息。

图1-7 查看射频的详细信息



1.4 查看WDS

在导航栏中选择“概览 > WDS”，进入如下图所示 WDS 显示页面。

图1-8 WDS 显示页面



说明

AP 有两种工作模式：

- 桥接模式：AP 作为二层设备在网络中运行。
- 路由模式：AP 作为三层设备在网络中运行。

目前 AP 只支持工作在桥接模式。

表1-7 WDS 邻居信息描述表

字段	描述
邻居MAC地址	邻居Radio口的MAC地址
本地MAC地址	本端Radio口的MAC地址
邻居状态	• UP：表示连接已经建立 • DOWN：表示连接中断 • PROCESSING：表示正在连接
链路UP时间	当前WDS链路UP的时间
信号质量	：只显示最下方1个信号格，表示0<RSSI<=20 ：显示2个信号格，表示20<RSSI<=30 ：显示3个信号格，表示30<RSSI<=35 ：显示4个信号格，表示35<RSSI<=40 ：显示5个信号格，表示40<RSSI

1.5 查看客户端

1.5.1 查看客户端详细信息

在界面左侧的导航栏中选择“概览 > 客户端”，进入页面后，选择“详细信息”页签，点击指定的客户端后，可以查看相关的详细信息。

客户端详细信息如下图所示，客户端详细信息中的各字段解释，请参见下表。

图1-9 查看客户端详细信息



表1-8 客户端详细信息显示信息描述表

字段	描述
MAC address	客户端的MAC地址

字段	描述
User Name	客户端的认证用户名 如果客户端采用明文方式或无用户名的加密方式接入，该字段显示为-NA- 需要注意的是，该字段的显示情况和客户端是否采用Portal认证无关。也就是说，如果客户端采用Portal认证方式，User Name字段不会显示客户端的Portal用户名
IP Address	客户端的IP地址
AID	客户端的关联ID
Radio Interface	客户端关联的Radio接口
Service Template Number	客户端关联的服务模板
SSID	客户端关联的SSID
BSSID	基本服务集标识
Port	与客户端关联的WLAN-BSS接口
VLAN	客户端所在的VLAN
State	客户端的状态，例如：Running（运行）
Power Save Mode	客户端节电模式的状态： • Active 模式（激活） • Sleep 模式（睡眠）
Wireless Mode	无线模式：802.11a，802.11b，802.11g，802.11an，802.11gn，802.11ac
Channel Band-width	带宽模式： • 20MHz：工作带宽为 20MHz • 40MHz：工作带宽为 40MHz • 80MHz：工作带宽为 80MHz
SM Power Save Enable	SM Power Save可以使客户端上只有一个天线处于工作状态，其余天线均处于休眠状态，从而达到节省电源的目的 • Enabled：支持 SM Power Save • Disabled：不支持 SM Power Save
Short GI for 20MHz	客户端工作带宽为20MHz时，对于Short GI的支持情况： • Not Supported：客户端不支持 Short GI • Supported：客户端支持 Short GI
Short GI for 40MHz	客户端工作带宽为40MHz时，对于Short GI的支持情况： • Not Supported：客户端不支持 Short GI • Supported：客户端支持 Short GI
Short GI for 80MHz	客户端工作带宽为80MHz时，对于Short GI的支持情况： • Not Supported：客户端不支持 Short GI • Supported：客户端支持 Short GI

字段	描述
Short GI for 160/80+80MHz	客户端工作带宽为160/80+80MHz时，对于Short GI的支持情况： • Not Supported：客户端不支持 Short GI • Supported：客户端支持 Short GI
LDPC	• Not Supported：无线客户端不支持 LDPC Supported：无线客户端支持LDPC
STBC Tx Capability	• Not Supported：不支持 STBC 发送能力 • Supported：支持 STBC 发送能力 对于STBC发送能力的支持情况，AP和Client会进行协商。只有客户端和AP都支持STBC发送能力，才能协商成功
STBC Rx Capability	• Not Supported：不支持 STBC 接收能力 • Supported： 支持 STBC 接收能力 对于STBC接收能力的支持情况，AP和Client会进行协商。只有客户端和AP都支持STBC接收能力，才能协商成功
Support MCS Set	客户端支持的MCS集
Support VHT-MCS and Nss Set	客户端支持的VHT-MCS和NSS集
BLOCK ACK-TID	按照QoS优先级ID值协商BLOCK ACK： • OUT：下行方向 • IN：上行方向 • BOTH：上行方向和下行方向
QoS Mode	AP是否支持WMM标志
Listen Interval (Beacon Interval)	处于Sleep模式的客户端定期醒来接收缓存在AP中的数据帧的时间间隔，单位为Beacon interval（信标发送时间间隔）
RSSI	接收信号强度指示，该值表明了AP检测到Client的信号强度
Rx/Tx Rate	客户端发送/接收报文的速率（包括数据、管理和控制报文）
Client Type	客户端类型，例如：RSN、WPA或Pre-RSN
Authentication Method	认证方式，例如：开放系统认证或共享密钥认证
AKM Method	AKM套件，如Dot1X，PSK
Key Derivation	密钥衍生类型： • SHA1：采用 HMAC-SHA1 散列算法 • SHA256：采用 HMAC-SHA256 散列算法 • -NA-：表示客户端使用的认证类型不涉及密钥衍生算法
4-Way Handshake State	四次握手状态： • IDLE：初始化状态 • PTKSTART：四次握手初始化完毕 • PTKNEGOTIATING：发送了第三个有效消息 • PTKINITDONE：四次握手成功

字段	描述
Group Key State	组密钥状态，包括以下几种： • IDLE：初始化状态 • REKEYNEGOTIATE：向用户发送初始化消息 • REKEYESTABLISHE：密钥更新成功
Encryption Cipher	加密密码：明文或者密文加密的类型
PMF Status	保护管理帧功能状态： • Active：支持保护管理帧功能 • Inactive：不支持保护管理帧功能 • -NA-：表示客户端使用的认证类型不涉及保护管理帧功能
Roam Status	漫游状态： Normal：普通漫游
Roam Count	无线客户端的漫游次数
Up Time	客户端和AP关联的时间

该页面的控件含义如下：

- <刷新>按钮

单击<刷新>按钮，刷新当前页面的显示信息。

- <黑名单>按钮

单击<黑名单>按钮，可以把选定的客户端加入到静态黑名单中，静态黑名单可以选择通过“安全 > 黑白名单”进行查看。

- <清空统计>按钮

单击<清空统计>按钮，可以清除选定的客户端的统计信息。

- <断开连接>按钮

单击<断开连接>按钮，可以使选定的客户端下线。

1.5.2 查看客户端统计信息

在界面左侧的导航栏中选择“概览 > 客户端”，进入页面后，选择“统计信息”页签，点击指定的客户端后，可以查看如下图所示的客户端统计信息。客户端统计信息中的各字段解释，请参见下表。

图1-10 查看客户端详细信息



表1-9 客户端统计信息显示信息描述表

字段	描述
AP Name	接入点名称
Radio Id	客户端关联的Radio口的编号
SSID	客户端关联的SSID
BSSID	基本服务集标识
MAC Address	客户端的MAC地址
RSSI	接收信号强度指示，该值表明了AP检测到Client的信号强度
Transmitted Frames	发送的帧的数目
Back Ground(Frames/Bytes)	以帧或字节为单位对背景流优先级队列进行统计
Best Effort(Frames/Bytes)	以帧或字节为单位对尽力而为流优先级队列进行统计
Video(Frames/Bytes)	以帧或字节为单位对视频流优先级队列进行统计
Voice(Frames/Bytes)	以帧或字节为单位对语音流优先级队列进行统计
Received Frames	收到的帧的数目
Discarded Frames	丢弃的帧的数目

1.5.3 对客户端进行RFPing操作

RFPing（Radio Frequency Ping）是一种针对无线链路的 Ping 功能，通过该检测可以获取 AP 和与之关联的客户端之间的无线链路的连接信息，如信号强度、报文重传次数、RTT（Round-trip Time，往返时间）等。

在界面左侧的导航栏中选择“概览 > 客户端”，进入页面后，选择“链路测试结果”页签。单击客户端对应的图标，显示如下图所示链路测试结果。链路测试结果中的各字段解释，请参见下表。

图1-11 查看客户链路测试结果



表1-10 链路测试结果

字段	描述
No./MCS	• 对非 802.11n 客户端进行 RFPing 操作后，链路测试结果中会显示 No.字段，表示非 802.11n 客户端的速率编号 • 对 802.11n 客户端进行 RFPing 操作后，链路测试结果中会显示 MCS 字段，表示 802.11n 客户端的 MCS 索引值
Rate(Mbps)	Radio接口发送无线Ping包的速率
TxCnt	Radio接口发送无线Ping包的个数
RxCnt	Radio接口收到客户端回应无线Ping包的个数
RSSI	接收信号强度指示，该值表明了AP检测到客户端的信号强度
Retries	Radio接口发送无线Ping包失败时的重传总次数
RTT(ms)	从Radio接口发出无线Ping包到收到客户端回应的平均往返时间

1.5.4 查看从客户端接收到的信标测量报告

在界面左侧的导航栏中选择“概览 > 客户端”，进入页面后，选择“信标测量报告”页签，点击指定的客户端后，可以查看相关的详细信息。

信标测量报告如下图所示，报告中的各字段解释，请参见下表。

图1-12 查看从客户端接收到的信标测量报告



表1-11 信标测量报告显示信息描述表

字段	描述
MAC Address	回复信标测量报告的客户端MAC地址
Total Number of Reports	信标测量报告的数量
Channel	信道号
BSSID	基本服务集标识
Regulatory Class	调整集，取值为12或5。关于该值的详细含义请参见802.11k协议
Antenna ID	天线ID
SSID	服务集标识符

目 录

1 基本信息 ····· 1-1

1.1 概述 ····· 1-1

1.2 配置系统名称 ····· 1-1

1.3 配置Web闲置超时时间 ····· 1-1

2 设备维护 ····· 2-1

2.1 软件升级 ····· 2-1

2.2 设备重启 ····· 2-2

2.3 诊断信息 ····· 2-2

3 时间设置 ····· 3-1

3.1 概述 ····· 3-1

3.2 查看当前系统时间 ····· 3-1

3.3 配置系统时间 ····· 3-1

3.4 配置系统时区和夏令时 ····· 3-2

4 日志管理 ····· 4-1

4.1 概述 ····· 4-1

4.2 查看系统日志 ····· 4-1

4.3 配置日志主机 ····· 4-2

4.4 配置缓冲区容量和刷新周期 ····· 4-3

5 配置管理 ····· 5-1

5.1 配置备份 ····· 5-1

5.2 配置恢复 ····· 5-1

5.3 保存配置 ····· 5-2

5.4 恢复出厂配置 ····· 5-3

6 文件管理 ····· 6-1

6.1 概述 ····· 6-1

6.2 查看文件列表 ····· 6-1

6.3 下载文件 ····· 6-2

6.4 上传文件 ····· 6-2

6.5 删除文件 ····· 6-2

6.6 设置主用启动文件 ····· 6-2

7 接口管理 ····· 7-1

7.1 概述 ····· 7-1

7.2 查看接口信息和接口统计信息 7-1
7.3 新建接口 7-3
7.4 修改二层接口 7-5
7.5 修改三层接口 7-8
7.6 接口管理典型配置举例 7-10
8 TR-069 8-1
8.1 概述 8-1
8.2 配置TR-069 8-2
8.3 注意事项 8-3
9 用户管理 9-1
9.1 概述 9-1
9.2 创建用户 9-1
9.3 设置超级密码 9-2
9.4 切换用户访问等级到管理级 9-3
10 SNMP 10-1
10.1 概述 10-1
10.2 配置SNMP Agent 10-1
10.3 SNMPv1/v2c典型配置举例 10-3
10.4 SNMPv3 典型配置举例 10-4
11 环回测试 11-1
11.1 概述 11-1
11.2 环回测试操作 11-1
11.3 注意事项 11-2

1 基本信息

1.1 概述

基本信息模块提供如下功能：

- 设置设备的系统名称。设置的系统名称显示在导航栏的最上方。
- 设置用户通过 Web 登录到设备的闲置超时时间，即用户登录到 Web 网管界面后，如果在指定的时间内未进行任何操作，系统将会强制该用户退出登录，以保证设备的安全性。

1.2 配置系统名称

(1) 在导航栏中选择“设备 > 基本信息”，默认进入“系统名称”页签的页面，如下图所示。

(2) 配置设备的系统名称。

(3) 单击<确定>按钮完成操作。

图1-1 系统名称



1.3 配置Web闲置超时时间

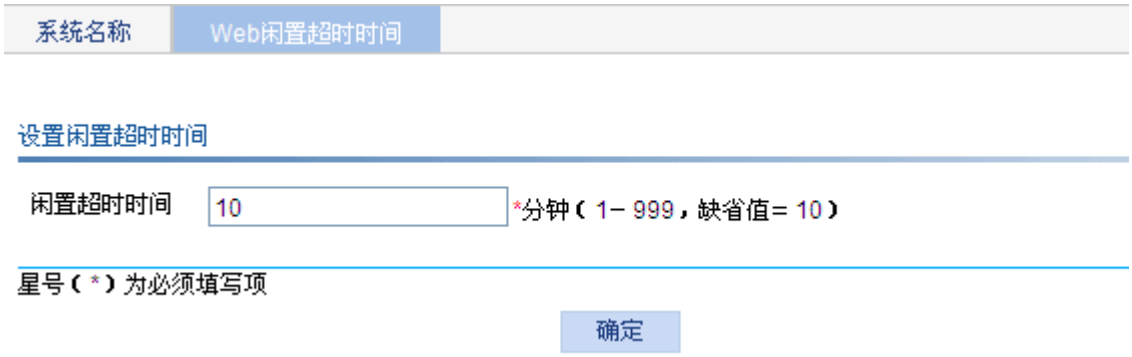
(1) 在导航栏中选择“设备 > 基本信息”。

(2) 单击“Web 闲置超时时间”，进入如下图所示的页面。

(3) 配置用户通过 Web 登录到设备的闲置超时时间。

(4) 单击<确定>按钮完成操作。

图1-2 Web 闲置超时时间



2 设备维护

2.1 软件升级

启动文件是用于引导、启动设备的应用程序文件，又称为系统软件或者设备软件。

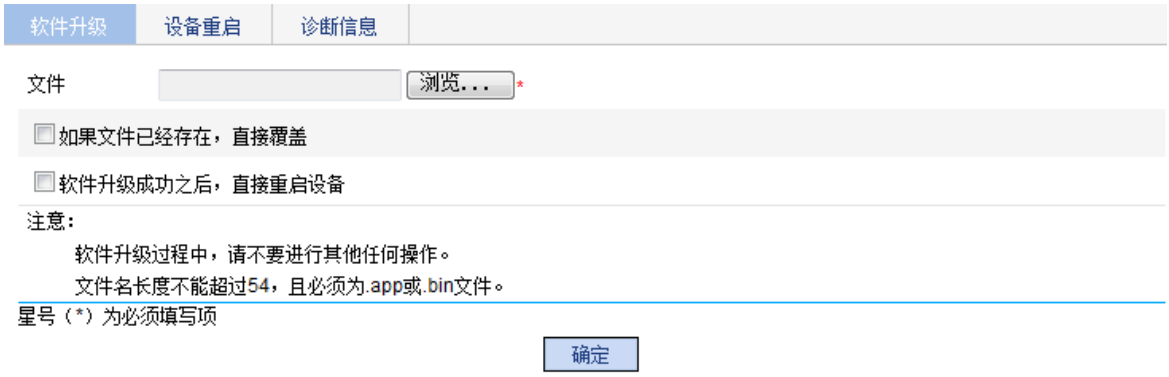
软件升级模块提供了从本地主机上获取目标应用程序文件，并将该文件设置为设备下次启动时使用的启动文件的功能。同时，还可以选择在完成上述操作后，是否直接重启设备使更新后的软件生效。

注意

- 软件升级需要一定的时间。在软件升级的过程中，请不要在 Web 上进行任何操作，否则可能会导致软件升级中断。
- 从本地主机上获取到目标应用程序文件后，保留文件的原名称。

(1) 在导航栏中选择“设备 > 设备维护”，默认进入“软件升级”页签的页面，如下图所示。

图2-1 软件升级



(2) 配置软件升级的参数，详细配置如下表所示。

(3) 单击<确定>按钮开始进行软件升级。

表2-1 软件升级的详细配置

配置项	说明
文件	设置保存在本地的应用程序文件的路径 其中，文件名必须带扩展名，且扩展名必须为.app或.bin
如果文件已经存在，直接覆盖	设置如果设备上存在重名文件时，是否直接覆盖 如果不选中此项，则当设备上有重名的文件存在时，将提示“文件已存在”，无法进行升级
软件升级成功之后，直接重启设备	设置当文件上传成功后，是否直接重启设备使更新后的软件生效

2.2 设备重启

注意

- 设备重启前请保存配置，否则重启后，未保存的配置将会全部丢失。
- 设备重启后，用户需重新登录设备。

(1) 在导航栏中选择“设备 > 设备维护”。

(2) 单击“设备重启”页签，进入如下图所示的页面。

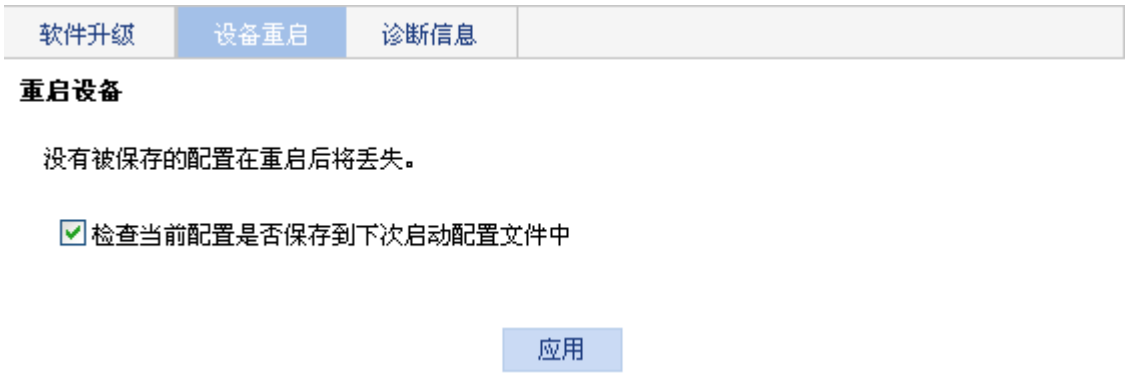
(3) 配置重启前是否对设备当前配置的保存情况进行检查。

(4) 单击<应用>按钮，弹出是否确认重启的对话框。

(5) 单击对话框中的<确定>按钮，此时：

- 如果已在页面上选中“检查当前配置是否保存到下次启动配置文件中”前的复选框，则系统会先进行检查。若检查通过，则直接重启设备；若检查不通过，则会弹出提示框提示当前配置和系统保存的配置不一致，且不会重启设备。
- 如果未在页面上选中“检查当前配置是否保存到下次启动配置文件中”前的复选框，则系统会直接重启设备。

图2-2 设备重启



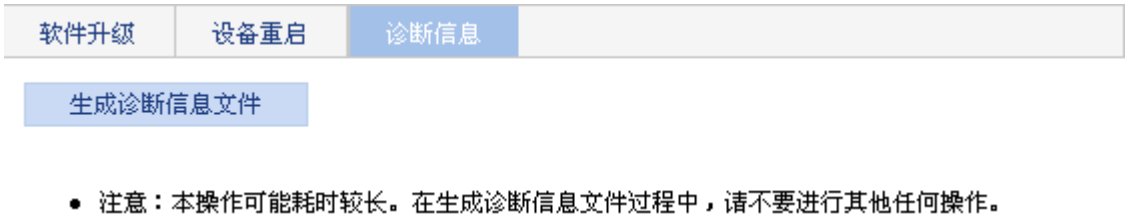
2.3 诊断信息

因为各个功能模块都有其对应的运行信息，所以一般情况下，用户需要逐个模块查看显示信息。为了在日常维护或系统出现故障时能够一次性收集更多信息，设备支持诊断信息模块。用户执行生成诊断信息文件的操作时，系统会将当前多个功能模块运行的统计信息保存在一个名为“default.diag”的文件中，用户可以通过查看该文件来更快的定位问题。

(1) 在导航栏中选择“设备 > 设备维护”。

(2) 单击“诊断信息”页签，进入如下图所示的页面。

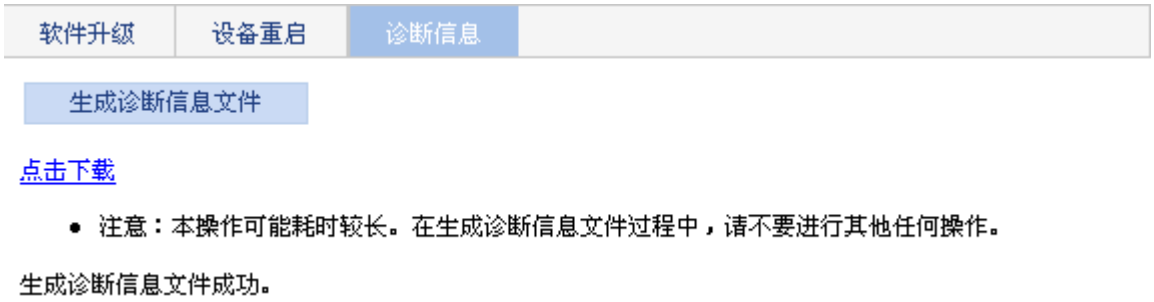
图2-3 诊断信息



(3) 单击<生成诊断信息文件>按钮，系统开始生成诊断信息文件。

(4) 文件生成后，页面如下图所示，单击“点击下载”，弹出“文件下载”对话框，可以选择直接将文件打开进行查看，或将文件保存到本地主机。

图2-4 生成诊断信息文件成功



说明

- 诊断信息文件的生成需要一定的时间。在诊断信息文件生成的过程中，建议用户不要在 Web 上进行任何操作。
- 生成诊断信息文件成功后，还可以在“设备 > 文件管理”中查看文件，或将文件下载到本地主机保存，详细说明请参见“文件管理”。

3 时间设置

3.1 概述

为了保证本设备与其它设备协调工作，用户需要将系统时间配置准确。时间设置模块用于配置和查看系统时间，以及设置系统时区和夏令时。

设备支持设置手动配置系统时间和通过自动同步 NTP（Network Time Protocol，网络时间协议）服务器的时间。

对于网络中的多台设备来说，依靠管理员手动配置每台设备的系统时间是不可能的，不但工作量巨大，而且也不能保证时间的精确性。

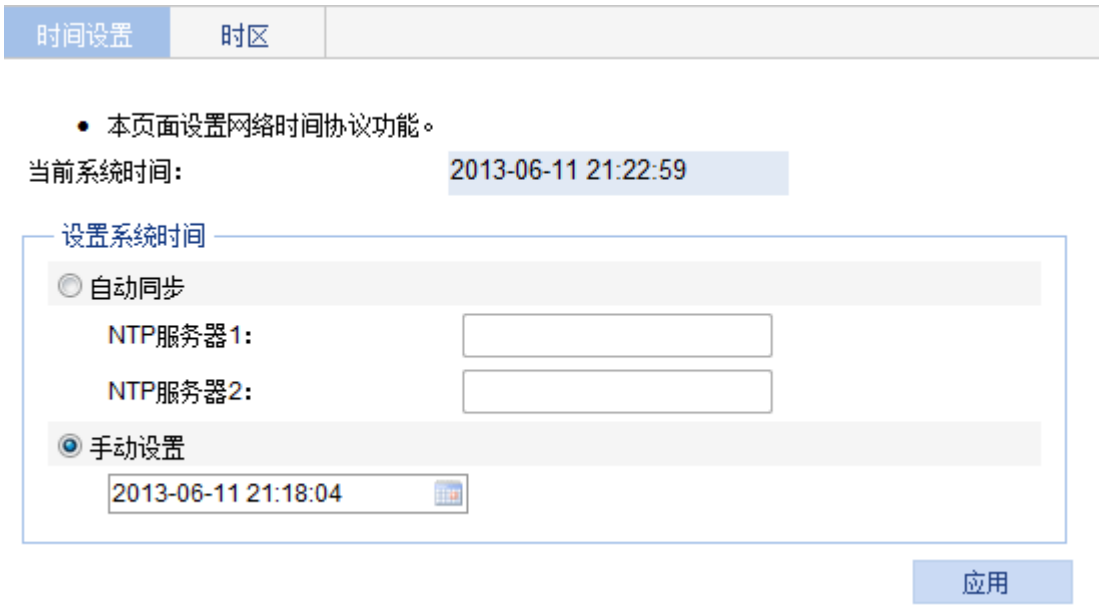
NTP 是由 RFC 1305 定义的时间同步协议，用来在分布式时间服务器和客户端之间进行时间同步。使用 NTP 可以使网络内所有设备的时钟保持一致，同时也能保证很高的精度，从而使设备能够提供基于统一时间的多种应用。

3.2 查看当前系统时间

(1) 在导航栏中选择“设备 > 时间设置”，默认进入“时间设置”页签的页面，如下图所示。

(2) 在页面上方查看实时显示的当前系统时间。

图3-1 时间设置



3.3 配置系统时间

(1) 在导航栏中选择“设备 > 时间设置”，默认进入“时间设置”页签的页面，如上图所示。

(2) 配置系统时间，详细配置如下表所示。

(3) 单击<确定>按钮完成操作。

表3-1 系统时间的详细配置

配置项		说明
自动同步	NTP服务器1	设置选择自动同步NTP服务器的时间，并输入主用NTP服务器（即NTP服务器1）的IP地址和备用NTP服务器（即NTP服务器2）的IP地址 提示 • 选择自动同步时，设备会周期性地向 NTP 服务器进行时钟同步。当同步失败时，系统时间为手动设置的时间；在同步成功后，再切换回自动同步的时间 • NTP 服务器 IP 地址是一个主机地址，不能为广播地址、组播地址或本地时钟的 IP 地址 • 如果 NTP 服务器的系统时间比设备当前系统时间晚较多，超过了设备上指定的 Web 闲置超时时间，则 NTP 时钟同步成功后，所有在线 Web 用户会超时退出登录
	NTP服务器2	
手动设置		设置选择手动设置的系统时间，并制定指定具体的日期和时间 可以直接在文本框中修改系统时间，也可以通过日历操作界面来修改系统时间。单击此文本框，展开日历操作界面，如图3-2所示，可以进行的操作如下： • 单击<今天>按钮，将日历上当前的日期设置为本地主机的当前系统日期，时间参数保持之前的值不变 • 设置年、月、日和具体时间，单击<确定>按钮完成日期和时间参数的设置

图3-2 日历操作界面

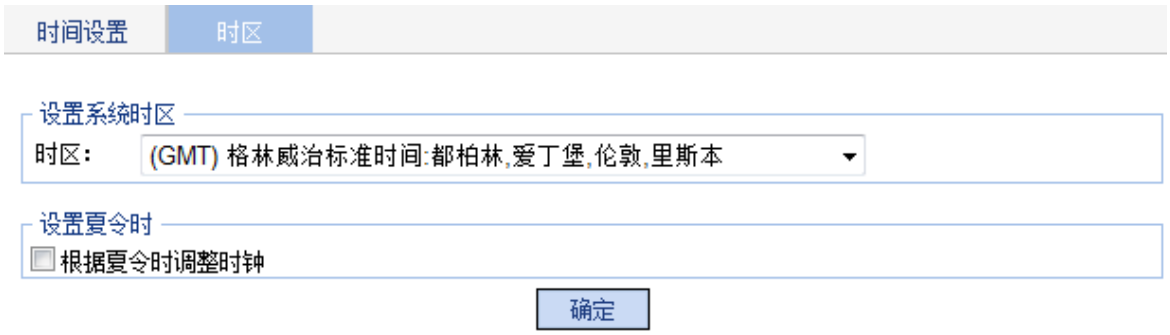


3.4 配置系统时区和夏令时

(1) 在导航栏中选择“设备 > 时间设置”。

(2) 单击“时区”页签，进入如下图所示的页面。

图3-3 时区



(3) 配置系统时区和夏令时，详细配置如下表所示。

(4) 单击<确定>按钮完成操作。

表3-2 系统时区和夏令时的详细配置

配置项	说明
时区	设置系统所在的时区
根据夏令时调整时钟	设置根据夏令时制调整系统时钟，即在指定时间段内将系统的当前时间增加1小时 单击“根据夏令时调整时钟”前的复选框，展开夏令时生效时间段的配置内容，如图3-4所示。夏令时生效时间段的有两种配置方式： • 从某一个年份开始，以 1 年为周期，每年从一个绝对的起始日期和时间到一个绝对的结束日期和时间的时间段内采用夏令时，该时间段必须大于 1 天且小于 1 年，如：从 2006 年开始每年 8 月 1 日 06:00:00 开始到 9 月 1 日 06:00:00 结束采用夏令时 • 以 1 年为周期，每年从一个相对的起始日期和时间到一个相对的结束日期和时间的时间段内采用夏令时，该时间段必须大于 1 天且小于 1 年，如：每年从 8 月的第一周的周一 06:00:00 开始到 9 月的最后一周的周日 06:00:00 结束采用夏令时

图3-4 设置夏令时



4 日志管理

4.1 概述

系统日志包含了网络和设备的大量信息，包括运行状态、配置变化等，是网络管理员监控网络和设备运行情况的重要途径。系统日志提供的信息可以帮助网络管理员发现网络问题或安全隐患，以便采取针对性的措施。

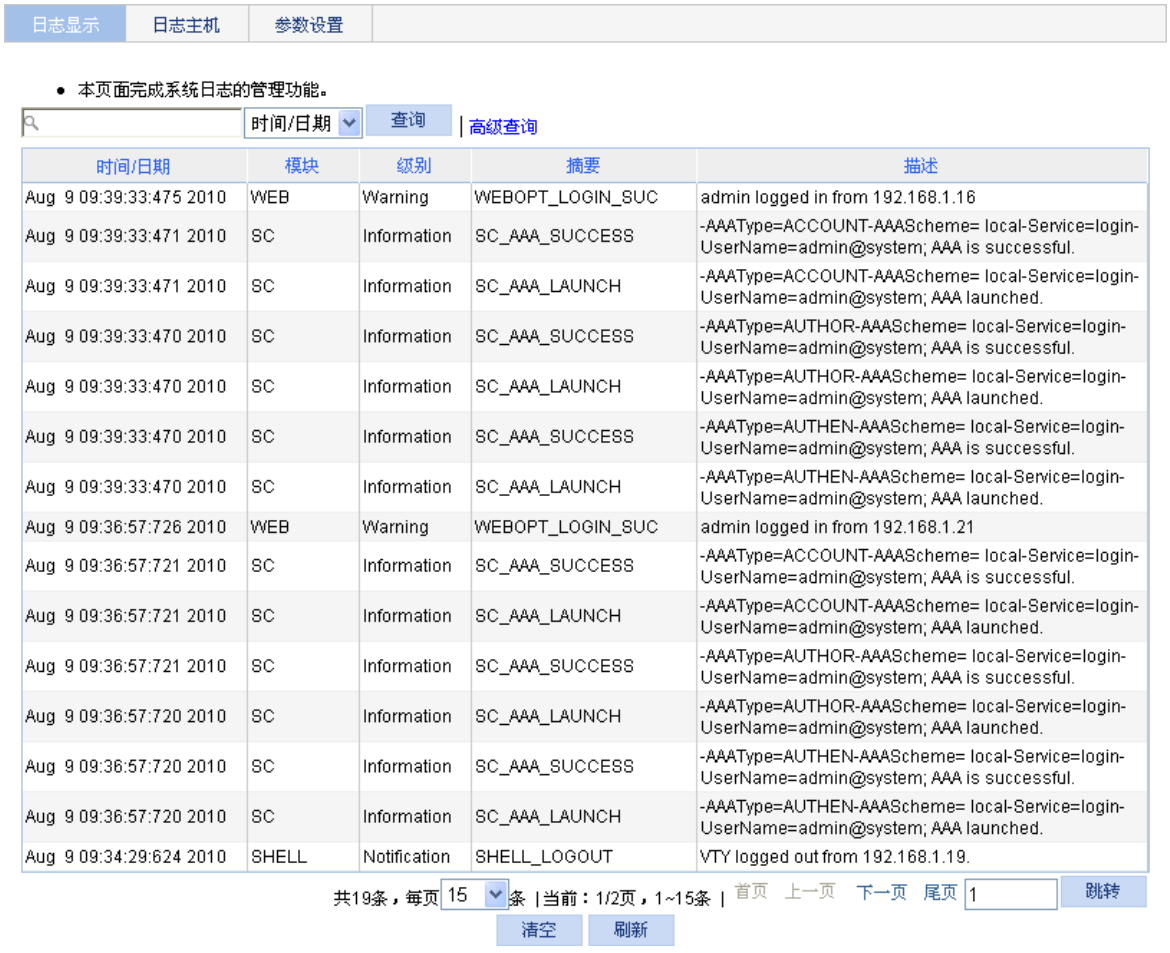
系统可以向以下五个方向发送系统日志：控制台、监视终端（即以 AUX、VTY、TTY 类型用户界面登录的用户终端）、日志缓冲区、日志主机和 Web 页面。

4.2 查看系统日志

Web 页面提供了丰富的搜索和排序功能，用户可以通过 Web 页面方便快捷地查看设备的系统日志。

(1) 在导航栏中选择“设备 > 日志管理”，默认进入“日志显示”页签的页面，如下图所示。

图4-1 日志显示



窍门

- 可以通过单击<清空>按钮将 Web 页面日志缓冲区中保存的所有系统日志清空。
- 可以通过单击<刷新>按钮手动刷新当前页面显示的系统日志信息；也可以通过在“参数设置”页签的页面设置刷新周期，使系统日志显示页面自动刷新，详细配置请参见“4.4 配置缓冲区容量和刷新周期”。

(2) 查看系统日志的信息，详细说明如下表所示。

表4-1 系统日志的详细说明

标题项	说明
时间/日期	系统日志产生的时间和日期
模块	产生系统日志的模块名
级别	系统日志的级别。系统日志按严重性划分为八个级别，严重性由高到低的顺序依次为： • Emergency：系统不可用信息 • Alert：需要立刻做出反应的信息 • Critical：严重信息 • Error：错误信息 • Warning：警告信息 • Notification：正常出现但是重要的信息 • Information：需要记录的通知信息 • Debug：调试过程产生的信息
摘要	系统日志的摘要内容
描述	系统日志的详细内容

4.3 配置日志主机

通过 Web 页面可以配置日志主机的信息，以便将系统日志发送到指定日志主机。最多可以指定 4 台不同的日志主机。

(1) 在导航栏中选择“设备 > 日志管理”。

(2) 单击“日志主机”页签，进入日志主机设置页面，如下图所示。

图4-2 日志主机



(3) 配置日志主机的信息，详细配置如下表所示。

(4) 单击<应用>按钮完成操作。

表4-2 日志主机的详细配置

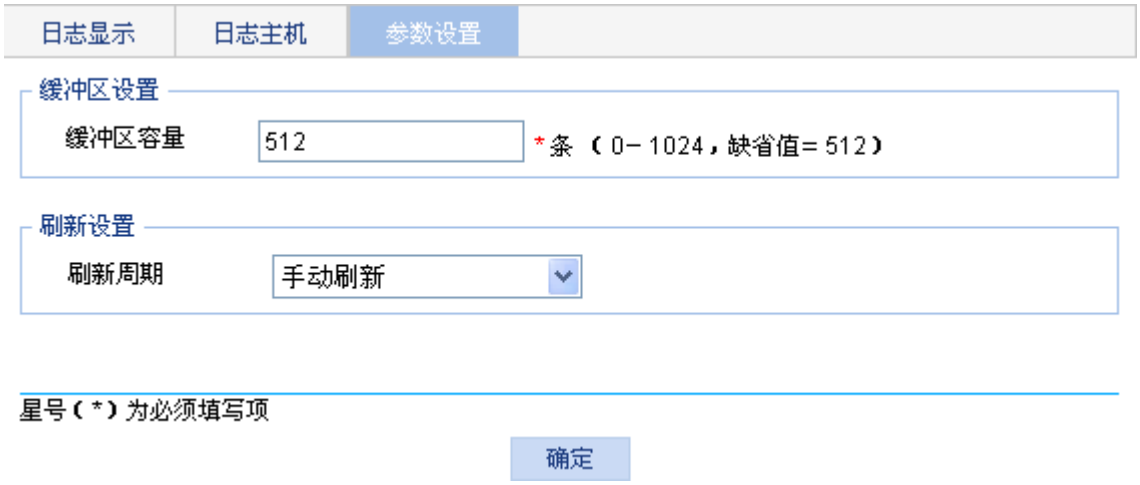
配置项	说明
IPv4/域名	设置日志主机的IPv4地址、域名或IPv6地址 最多可以指定4台不同的日志主机
主机IP地址/域名	

4.4 配置缓冲区容量和刷新周期

(1) 在导航栏中选择“设备 > 日志管理”。

(2) 单击“参数设置”页签，进入如下图所示的页面。

图4-3 系统设置



(3) 配置系统日志相关的参数，详细配置如下表所示。

(4) 单击<应用>按钮完成操作。

表4-3 系统日志相关参数的详细配置

配置项	说明
缓冲区容量	设置Web页面日志缓冲区可存储的日志条数
刷新周期	设置日志显示Web页面的刷新间隔，分为手动刷新和自动刷新两种方式 • 手动刷新：只能在日志显示页面单击<刷新>按钮手动刷新页面 • 自动刷新：系统将根据选择的周期，每隔 1、5 或 10 分钟自动刷新日志显示页面

5 配置管理

5.1 配置备份

注意

在执行配置文件备份的操作时，请同步备份“.xml”结尾的配置文件，否则在某些情况下（如配置不小心被删除的情况）可能会导致部分配置信息无法恢复。

配置备份模块提供如下功能：

- 打开下次启动的配置文件（包括.cfg 文件和.xml 文件）进行查看。
- 将下次启动的配置文件（包括.cfg 文件和.xml 文件）备份到当前用户的主机上保存。

(1) 在导航栏中选择“设备 > 配置管理”，默认进入“配置备份”页签的页面，如下图所示。

图5-1 配置备份



(2) 单击“备份以”.cfg”结尾的配置文件”后面的<备份>按钮，弹出“文件下载”对话框，可以选择将下次启动的.cfg 配置文件打开进行查看或者保存到本地。

(3) 单击“备份以”.xml”结尾的配置文件”后面的<备份>按钮，弹出“文件下载”对话框，可以选择将下次启动的.xml 配置文件打开进行查看或者保存到本地。

5.2 配置恢复

注意

恢复的配置文件在设备下次启动后才会生效。

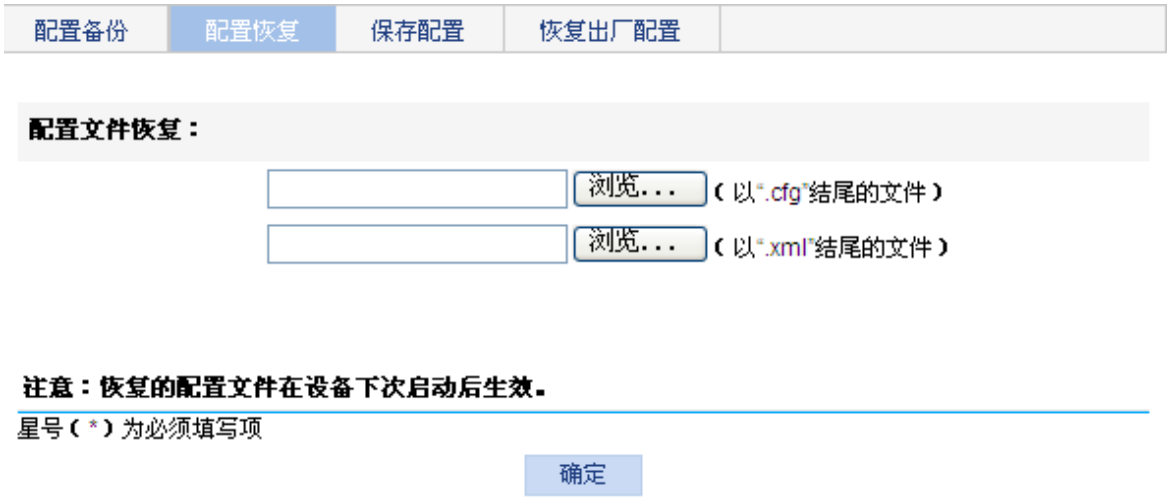
配置恢复模块提供如下功能：

- 将保存在当前用户主机上的.cfg 文件上传到设备作为下次启动的.cfg 配置文件。
- 将保存在当前用户主机上的.xml 文件上传到设备作为下次启动的.xml 配置文件，并删除之前的下次启动.xml 配置文件。

(1) 在导航栏中选择“设备 > 配置管理”。

(2) 单击“配置恢复”页签，进入如下图所示的页面。

图5-2 配置恢复



(3) 单击“（以".cfg"结尾的文件）”前的<浏览>按钮，在弹出的对话框中选择要上传到设备的.cfg配置文件。

(4) 单击“（以".xml"结尾的文件）”前的<浏览>按钮，在弹出的对话框中选择要上传到设备的.xml配置文件。

(5) 单击<确定>按钮开始进行配置恢复。

5.3 保存配置

注意

- 保存配置需要一定时间，请耐心等待。
- 系统不支持两个或两个以上用户同时执行保存配置的操作，系统将提示后操作的用户稍后再试。

保存配置模块提供将用户当前的配置保存到下次启动配置文件（包括.cfg 文件和.xml 文件）的功能。Web 网管提供了快捷和常规两种保存配置的方法。

1. 快捷方法

如下图中红框处所示，直接单击页面辅助区右侧的<保存>按钮，即可将当前的配置保存到配置文件。

图5-3 保存配置



注意：保存当前配置信息。

2. 常规方法

(1) 在导航栏中选择“设备 > 配置管理”。

(2) 单击“保存配置”页签，进入如上图所示的页面。

(3) 单击<保存当前配置>按钮将当前的配置保存到配置文件。

5.4 恢复出厂配置

恢复出厂配置模块提供将设备中的所有配置恢复到出厂时的缺省配置，删除当前的配置文件，并重新启动设备的功能。

(1) 在导航栏中选择“设备 > 配置管理”。

(2) 单击“恢复出厂配置”页签，进入如下图所示的页面。

(3) 单击<恢复出厂配置>按钮开始恢复出厂配置。

图5-4 恢复出厂配置



注意：删除当前配置文件，把设备恢复到出厂时的配置，并重启设备。

6 文件管理

6.1 概述

设备运行过程中所需要的文件（如：主机软件、配置文件等）保存在设备的存储设备中，为了方便用户对这些文件进行有效的管理，系统提供了文件管理功能。文件管理具体可以提供的功能如下：

- 查看文件列表
- 从设备下载文件
- 上传文件到设备
- 删除文件
- 设置主用启动文件

6.2 查看文件列表

(1) 在导航栏中选择“设备 > 文件管理”，进入如下图所示的页面。

图6-1 文件管理



说明

该页面显示的文件信息与设备的型号有关，请以设备的实际情况为准。

(2) 在页面上方选择要查看的磁盘。

(3) 在下拉框后面查看该磁盘的已用空间、可用空间和总容量。

(4) 在页面下方的列表中查看该磁盘中存储的所有文件（以“路径+文件名”的格式显示）、文件的大小，如果某文件是应用程序文件（扩展名为.bin 或.app），还可以查看该文件是否是设备下次启动时的主用或备用启动文件。

6.3 下载文件

(1) 在导航栏中选择“设备 > 文件管理”，进入如 图 6-1 所示的页面。

(2) 在文件列表中选中一个要下载的文件。需要注意的是，一次只能选择一个要下载的文件。

(3) 单击<下载文件>按钮，弹出“文件下载”对话框，可以选择将该文件打开进行查看或者保存到指定路径。

6.4 上传文件

说明

上传文件需要一定的时间。在文件上传过程中，建议用户不要在 Web 上进行任何操作。

(1) 在导航栏中选择“设备 > 文件管理”，进入如 图 6-1 所示的页面。

(2) 在“上传文件”框中选择保存文件的磁盘。

(3) 通过<浏览>按钮设置要上传文件的路径和名称。

(4) 单击<确定>按钮将该文件上传到设备。

6.5 删除文件

(1) 在导航栏中选择“设备 > 文件管理”，进入如 图 6-1 所示的页面。

(2) 在文件列表中选中一个或多个要删除的文件。

(3) 单击<删除文件>按钮将选中的文件删除。

说明

也可以在文件列表中直接单击某文件对应的 图标将其删除，此处不再赘述。

6.6 设置主用启动文件

(1) 在导航栏中选择“设备 > 文件管理”，进入如 图 6-1 所示的页面。

(2) 选中某个应用程序文件（扩展名为.bin 或.app）前的复选框。需要注意的是，一次只能设置一个文件。

(3) 单击<设置为主用启动文件>按钮将该文件设置为设备下次启动时的主用启动文件。

7 接口管理

7.1 概述

接口是设备与设备之间交换数据并相互作用的部分，其功能就是完成设备之间的数据交换。物理接口是真实存在、有对应器件支持的接口，如以太网接口。逻辑接口是指能够实现数据交换功能但物理上不存在、需要通过配置建立的接口，如 VLAN 接口等。

接口管理特性用于在 Web 网管上管理设备的以下几种接口：

- 二层以太网接口：设备上的一种物理接口，工作在数据链路层，处理二层协议，实现二层快速转发。
- WLAN-Radio：设备上的一种物理接口，提供无线接入服务，可以和 WLAN-BSS 接口、WLAN-Ethernet 接口绑定。
- Loopback 接口（环回接口）：一种纯软件性质的虚拟接口。Loopback 接口创建后除非手工关闭该接口，否则 Loopback 接口物理层状态和链路层协议永远处于 UP 状态；Loopback 接口下可以使能路由协议，可以收发路由协议报文；当 Loopback 接口配置 IPv4 地址时，子网掩码必须是 32 位的。
- NULL 接口：一种纯软件性质的逻辑接口。NULL 接口永远处于 Up 状态，不能转发数据包，也不能配置 IP 地址和链路层协议。如果在静态路由中指定到达某一网段的下一跳为 Null 接口，则任何送到该网段的网络数据报文都会被丢弃，因此设备通过 Null 接口提供了一种过滤报文的简单方法——将不需要的网络流量发送到 Null 接口，从而免去配置 ACL（Access Control List，访问控制列表）的复杂工作。
- VLAN 接口：一种三层模式下的虚拟接口，主要用于实现 VLAN 间的三层互通。每个 VLAN 对应一个 VLAN 接口，在为 VLAN 接口配置了 IP 地址后，该接口即可作为本 VLAN 内网络设备的网关，对需要跨网段的报文进行基于 IP 地址的三层转发。
- 二层聚合（Bridge-aggregation，BAGG）接口：将多个二层以太网接口捆绑在一起形成一个二层聚合组，其对应的聚合接口称为二层聚合接口。
- Dialer 接口：为了实现拨号服务而设置的逻辑接口，物理接口（如 Serial、BRI、Async 等）可以通过绑定到 Dialer 接口而继承配置信息。Dialer 接口的波特率恒定为 64000bps。
- Cellular-Ethernet 接口：设备上的一种物理 3G/4G Modem 接口，可以使用该接口作为 LTE 上行接口。

接口管理功能是指用户查看设备接口信息、创建和删除逻辑接口、更改接口状态以及重新设置接口的参数。

7.2 查看接口信息和接口统计信息

(1) 在导航栏中选择“设备 > 接口管理”，进入如下图所示的页面，可以查看接口的名称、IP 地址/掩码和状态信息。

图7-1 接口管理

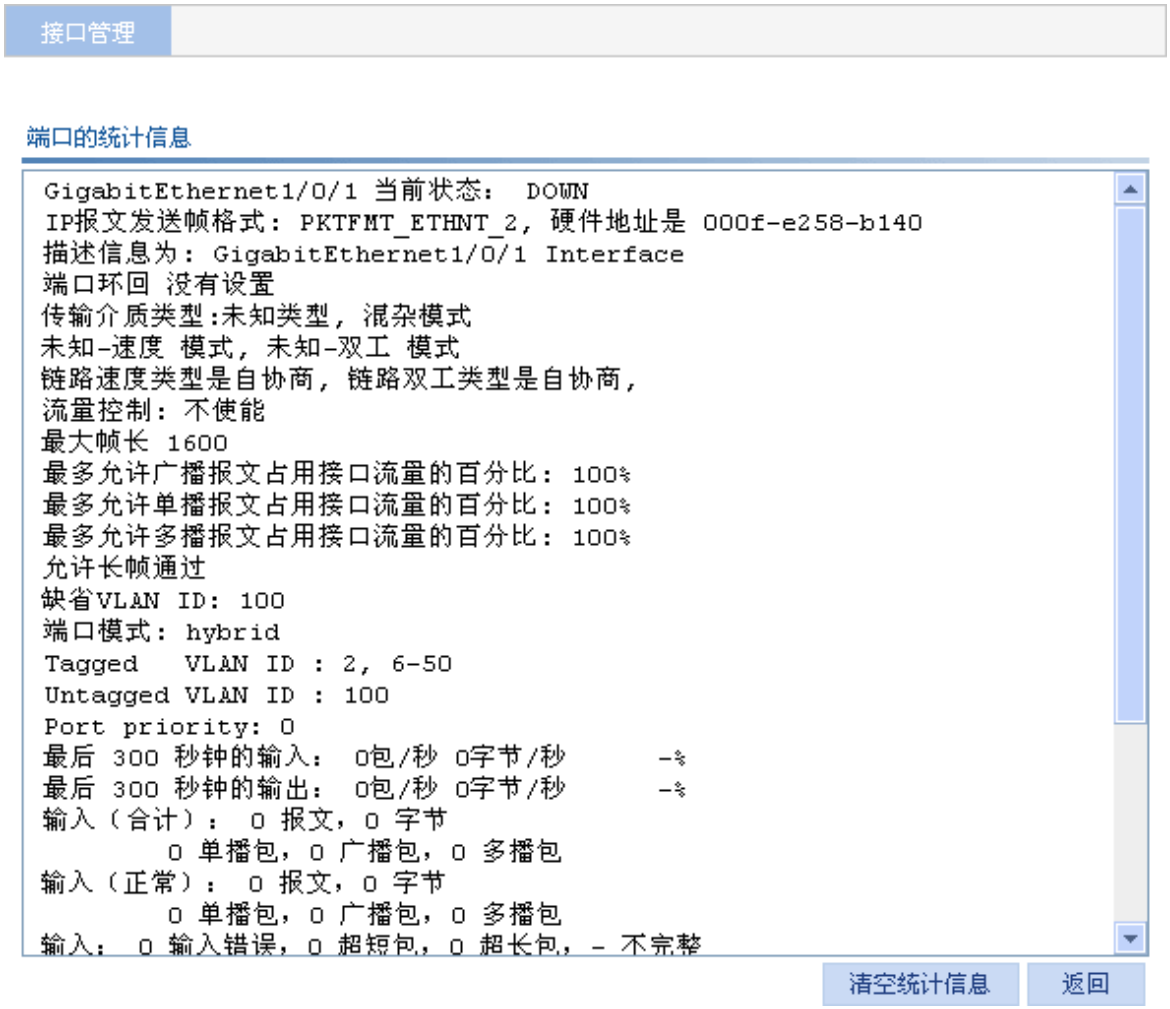


说明

该页面显示的接口信息与设备的型号有关，请以设备的实际情况为准。

(2) 单击接口名称的链接，进入如下图所示的页面，可以查看端口的统计信息。

图7-2 端口的统计信息

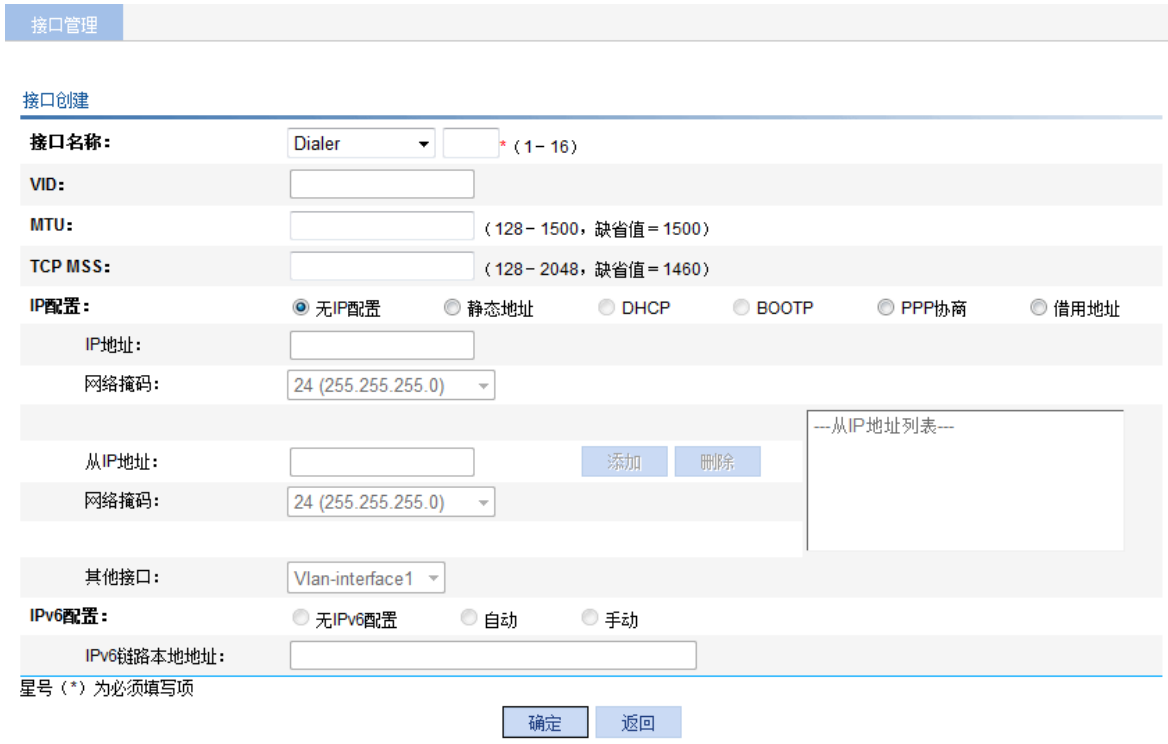


7.3 新建接口

(1) 在导航栏中选择“设备 > 接口管理”，进入接口的显示页面，如 图 7-1 所示。

(2) 单击<新建>按钮，进入新建接口的配置页面，如下图所示。

图7-3 新建接口



(3) 配置接口的信息，详细配置如下表所示。

(4) 单击<确定>按钮完成操作。

表7-1 新建接口的详细配置

配置项	说明
接口名称	设置逻辑接口类型和接口编号
VID	设置三层以太网子接口相关联的VLAN 该参数只在“接口名称”为三层以太网子接口时可配 提示 由于设备不支持三层以太网子接口，所以此配置项不可配
MTU	设置接口允许通过的最大传输单元
TCP MSS	设置接口的TCP最大报文段长度

配置项	说明
IP配置	设置接口获取IP地址的方式，包括： • 无 IP 配置：表示不配置接口的 IP 地址 • 静态地址：表示手动设置接口的 IP 地址，选择此项时需要为接口设置“IP 地址/网络掩码”配置项 • DHCP：表示接口通过 DHCP 协议自动获取 IP 地址 • BOOTP：表示接口通过 BOOTP 协议自动获取 IP 地址 • PPP 协商：表示接口通过 PPP 协商获得 IP 地址 • 借用地址：表示接口借用同一设备其他接口的 IP 地址，选择此项时需要为接口设置其他接口配置项 提示 获取方式的支持情况与选择的接口类型有关，请以实际情况为准
IP地址/网络掩码 从IP地址/网络掩码	当接口获取IP地址的方式选择“静态地址”时，设置接口的主IP地址/网络掩码和从IP地址和网络掩码 提示 • 主 IP 地址和从 IP 地址均不能为 0.0.0.0 • Loopback 接口的网络掩码固定为 32 位不可配置 • FAT AP 仅支持一个从 IP 地址
其他接口	当接口获取IP地址的方式选择“借用地址”时，设置被借用IP地址的接口
IPv6配置	设置接口获取IPv6链路本地地址的方式，包括： • 无 IPv6 配置：表示不配置接口的 IPv6 链路本地地址 • 自动：表示自动生成接口的 IPv6 链路本地地址 • 手动：表示手动设置接口的 IPv6 链路本地地址选择此项时需要为接口设置“IPv6 链路本地地址”配置项
IPv6链路本地地址	当接口获取IPv6链路本地地址的方式选择“手动”时，设置接口的IPv6链路本地地址

7.4 修改二层接口

(1) 在导航栏中选择“设备 > 接口管理”，进入接口的显示页面，如 图 7-1 所示。

(2) 单击二层接口对应的图标，进入如下图所示的页面。

图7-4 修改二层物理接口



(3) 修改二层物理接口的信息，详细配置如下表所示。

(4) 单击<确定>按钮完成操作。

表7-2 修改二层物理接口的详细配置

配置项	说明
端口状态	设置开启或关闭该端口 在某些特殊情况下，如修改接口的工作参数时，改动不能立即生效，需要关闭和重启接口后，才能生效
速率	设置端口的速率 • 10：10Mbps • 100：100Mbps • 1000：1000Mbps • Auto：自动协商端口速率 • Auto 10：端口自协商速率为 10Mbps • Auto 100：端口自协商速率为 100Mbps • Auto 1000：端口自协商速率为 1000Mbps • Auto 10 100：端口自协商速率为 10Mbps 或 100Mbps • Auto 10 1000：端口自协商速率为 10Mbps 或 1000Mbps • Auto 100 1000：端口自协商速率为 100Mbps 或 1000Mbps • Auto 10 100 1000：端口自协商速率为 10Mbps、100Mbps 或 1000Mbps
双工状态	设置端口的双工模式 • Auto：自动协商双工模式 • Full：全双工状态 • Half：半双工状态

配置项	说明
连接类型	设置端口的链路类型，包括Access、Hybrid和Trunk Access、Hybrid和Trunk的详细说明如表7-3所示 提示 Trunk 端口和 Hybrid 端口之间不能直接切换，只能把端口先设为 Access 端口，然后再设置为其它类型端口。例如：Trunk 端口必须先设为 Access 端口，然后才能设置为 Hybrid 端口
PVID	设置Hybrid或Trunk端口的缺省VLAN ID 提示 建议本端设备端口的缺省 VLAN ID 和相连的对端设备端口的缺省 VLAN ID 保持一致
网线类型	设置端口的MDI（Medium Dependent Interface，介质相关接口）模式 用于连接以太网设备的双绞线有两种：直通线缆和交叉线缆。为了使以太网接口支持使用这两种线缆，设备实现了三种MDI模式：Across、Normal和Auto 物理以太网接口由8个引脚组成，缺省情况下，每个引脚都有专门的作用，比如，使用引脚1和2发送信号，引脚3和6接收信号。通过设置MDI模式，可以改变引脚在通信中的角色 • Across：不改变引脚的角色，即使用引脚 1 和 2 发送信号，使用引脚 3 和 6 接收信号 • Auto：通过协商来决定物理引脚的角色 • Normal：改变引脚的角色，使用引脚 1 和 2 接收信号，使用引脚 3 和 6 发送信号 只有将设备的发送引脚连接到对端的接收引脚后才能正常通信，所以MDI模式需要和两种线缆配合使用： • 通常情况下，建议用户使用 Auto 模式，只有当设备不能获取网线类型参数时，才需要将模式手工指定为 Across 或 Normal • 当使用直通线缆时，两端设备的 MDI 模式配置不能相同 • 当使用交叉线缆时，两端设备的 MDI 模式配置必须相同或者至少有一端设置为 Auto 模式
流量控制	设置使能或禁止端口流量控制功能 当本端和对端设备都使能了流量控制功能后，如果本端设备发生拥塞，就向对端设备发送消息，通知对端设备暂时停止发送报文；对端设备在接收到该消息后将暂时停止向本端发送报文；反之亦然。从而避免了报文丢失现象的发生 提示 只有本端和对端端口都开启了流量控制功能，才能实现流量控制
最大MAC数	设置端口能学习的MAC地址的最大数量 • User Defined：用户自定义，选择此项时需要手动输入最大 MAC 数 • No Limited：不限制最大 MAC 数
广播风暴抑制比	设置抑制广播风暴的方式和参数值 • ratio：允许通过的最大广播流量占该端口传输能力的百分比，选择此项时需要输入具体的百分数 • pps：端口每秒允许转发的最大广播包数，选择此项时需要输入具体的包数

配置项	说明
多播风暴抑制比	设置抑制多播风暴的方式和参数值 • ratio：允许通过的最大多播流量占该端口传输能力的百分比，选择此项时需要输入具体的百分数 • pps：端口每秒允许转发的最大多播包数，选择此项时需要输入具体的包数
未知单播风暴抑制比	设置抑制未知单播风暴的方式和参数值 • ratio：允许通过的最大未知单播流量占该端口传输能力的百分比，选择此项时需要输入具体的百分数 • pps：端口每秒允许转发的最大未知单播包数，选择此项时需要输入具体的包数

表7-3 链路类型说明

链路类型	说明
Access	端口只能属于1个VLAN 一般用于连接用户设备
Hybrid	端口可以允许多个VLAN通过，可以接收和发送多个VLAN的报文，且允许多个VLAN的报文发送时不带Tag标签 可以用于网络设备之间的连接，也可以用于连接用户设备
Trunk	端口可以允许多个VLAN通过，可以接收和发送多个VLAN的报文，但只允许缺省VLAN的报文发送时不带Tag标签 一般用于网络设备之间的连接

7.5 修改三层接口

(1) 在导航栏中选择“设备 > 接口管理”，进入接口的显示页面，如 图 7-1 所示。

(2) 单击三层接口对应的图标，进入如下图所示的页面。

图7-5 修改三层接口



(3) 修改三层接口的信息，详细配置与新建接口的配置类似，这里只介绍修改三层接口特有的参数，如下表所示。

(4) 单击<确定>按钮完成操作。

表7-4 修改三层接口的详细配置

配置项	说明
接口类型	设置接口的类型，包括光口、电口、不设置

配置项	说明
接口状态	显示和设置接口的状态 • 当显示为“已连接”时，表示接口当前状态为开启且已连接，可以单击后面的<关闭>按钮，将接口强制关闭 • 当显示为“未连接”时，表示接口当前状态为开启但未连接，可以单击后面的<关闭>按钮，将接口强制关闭 • 当显示为“强制关闭”时，表示接口当前状态为强制关闭，可以单击后面的<开启>按钮，将接口开启 单击按钮修改接口状态后，页面会跳转到接口的显示页面 提示 对于不支持修改接口状态的接口，此配置项后没有对应的按钮，请以实际情况为准
工作模式	显示接口的工作模式为三层

7.6 接口管理典型配置举例

1. 组网需求

创建 Vlan-interface100，并配置其 IP 地址为 10.1.1.2。

2. 配置步骤

(1) 创建 VLAN 100。

步骤 1：在导航栏中选择“网络 > VLAN”，默认进入“VLAN”页签的页面。

步骤 2：单击<新建>按钮。

步骤 3：如下图所示，输入 VLAN ID 为“100”。

步骤 4：单击<确定>按钮完成操作。

图7-6 创建 VLAN 100



(2) 创建 Vlan-interface100，并配置其 IP 地址。

步骤 1：在导航栏中选择“设备 > 接口管理”。

步骤 2：单击<新建>按钮。

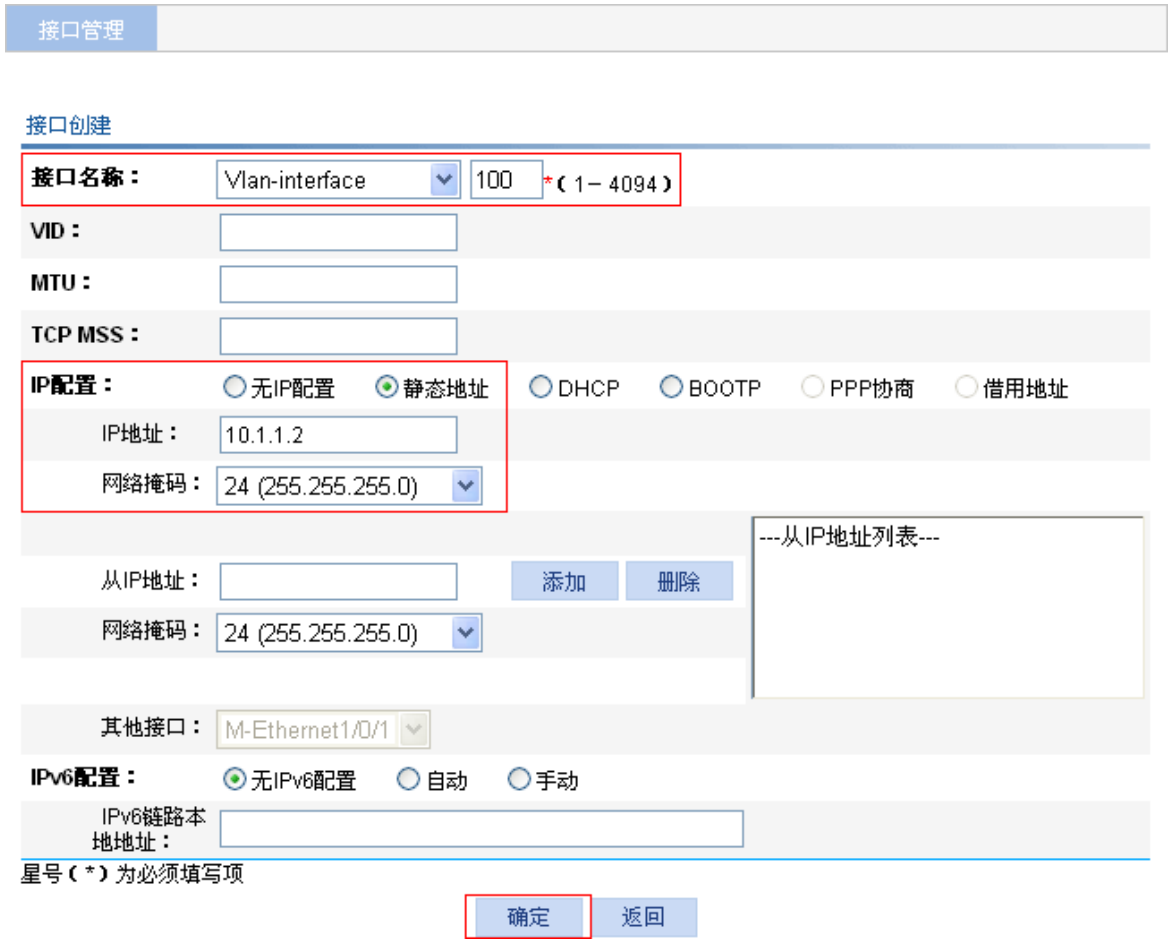
步骤 3：进行如下配置，如下图所示。

- 在接口名称中选择接口类型为“Vlan-interface”，输入接口编号为“100”。
- 选择 IP 配置为“静态地址”。

- 输入 IP 地址为“10.1.1.2”。
- 选择网络掩码为“24 (255.255.255.0)”。

步骤 4：单击<确定>按钮完成操作。

图7-7 创建 Vlan-interface100



8 TR-069

设备各款型对于本节所描述的特性支持情况有所不同，详细差异信息如下：

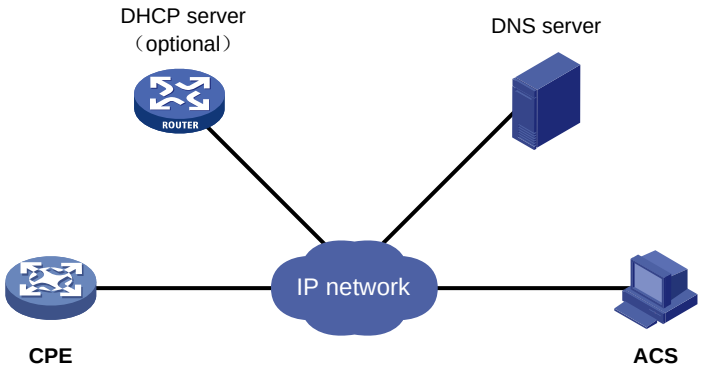
产品系列	型号	特性	描述
WA2600系列	WA2610H	TR-069	支持
WA4600系列	WA4620i-ACN/WA4620E-ACN		不支持
WA4300系列	WA4320H-ACN		支持
	WA4320i-ACN/WA4320i-X		支持
	WA4320-TS/WA4320-TQ/WA4320-TQ-V		支持
	WA4320X		支持
	WA4320-ACN/WA4320/WA4320-ACN-SI/WA4320-ACN-C/WA4320-ACN-D/WA4320-ACN-E/WA4320-ACN-PI		支持
	WA4330-ACN		不支持
LA4300系列	LA4310/LA4310V/LA4320/LA4320V/LA4320X		支持
小贝系列	WAP722/WAP722E/WAP722S		支持
	WAP712/WAP712C		支持

8.1 概述

TR-069 协议是由 DSL（Digital Subscriber's Line，数字用户线路）论坛所开发的技术规范之一，它提供了对下一代网络中家庭网络设备进行管理配置的通用框架、消息规范、管理方法和数据模型。

TR-069 主要应用于 DSL 接入网络环境。在 DSL 接入网络中，由于用户设备数量繁多、部署分散，通常位于用户侧，不易进行设备的管理和维护。TR-069 提出通过 ACS（Auto-Configuration Server，自动配置服务器）对 CPE（Customer Premise Equipment，用户侧设备）进行远程集中管理，解决 CPE 设备的管理困难，节约维护成本，提高问题解决效率。

图8-1 TR-069 网络的基本框架示意图



TR-069 网络的基本框架如上图所示，其网络元素主要有：

- ACS：自动配置服务器，网络中的管理设备。
- CPE：用户端设备，网络中的被管理设备。
- DNS server：域名服务器。TR-069 协议规定 ACS 和 CPE 使用 URL 地址来互相识别和访问，DNS 用于帮助解析 URL 参数。
- DHCP server：动态主机配置协议服务器，给 ACS 和 CPE 分配 IP 地址，使用 DHCP 报文中的 option 字段给 CPE 配置参数。

H3C 设备属于 CPE，使用 TR-069 协议与 ACS 进行消息交互。

说明

关于 TR-069 的详细介绍请参见“网络管理与监控配置指导”中的“CWMP（TR-069）”。

8.2 配置TR-069

说明

CPE 的 TR-069 参数可以通过 ACS 远程管理自动配置，也可以通过 Web 手动配置，这里只介绍通过 Web 手动配置的方法。

(1) 在导航栏中选择“设备 > TR-069”，进入如下图所示的页面。

图8-2 设置



(2) 配置 TR-069 参数，详细配置如下表所示。

(3) 单击<应用>按钮完成操作。

表8-1 TR-069 参数的详细配置

配置项		说明
TR-069		设置开启或关闭TR-069功能 开启TR-069功能后，其它的配置才有效
ACS	URL	设置向ACS发起连接所使用的URL
	用户名	设置向ACS发起连接所使用的用户名
	密码	设置向ACS发起连接所使用的密码 可以只用用户名验证，但ACS和CPE上的配置必须一致
CPE	用户名	设置CPE对从ACS发来的连接进行认证所使用的用户名
	密码	设置CPE对从ACS发来的连接进行认证所使用的密码 可以只用用户名验证，但ACS和CPE上的配置必须一致
	发送Inform报文	设置开启或关闭CPE周期发送Inform报文功能
	发送周期	设置CPE发送Inform报文的周期
	电信维护帐号	设置开启或关闭通知ACS修改电信维护帐号“TelecomAdmin”的密码的功能
	CPE连接接口	设置CPE连接接口，CPE将在Inform报文中携带此接口的IP地址，希望ACS通过此IP地址和自己建立连接

8.3 注意事项

配置 TR-069 时需要注意如下事项：

(1) 通过 ACS 自动配置比通过 Web 手动配置的优先级高，且低优先级的配置方式不能修改高优先级配置方式配置的参数。

(2) 配置 TR-069 时，如果要取消某项参数的配置，必须选中该参数前的复选框，并将指定的参数值清空，然后单击<应用>按钮提交配置。

9 用户管理

9.1 概述

用户管理模块提供如下功能：

- 配置本地用户及其登录密码、访问等级和服务类型。
- 配置切换当前 Web 用户的访问等级到管理级所使用的超级密码。
- 切换当前 Web 用户的访问等级到管理级。

9.2 创建用户

(1) 在导航栏中选择“设备 > 用户管理”。

(2) 单击“创建用户”页签，进入如下图所示的页面。

图9-1 创建用户



(3) 配置用户的信息，详细配置如下表所示。

(4) 单击<应用>按钮完成操作。

表9-1 创建用户的详细配置

配置项	说明
用户名	设置用户的用户名

配置项	说明
访问等级	设置用户的访问等级，以对不同用户能够进行的操作进行分类 用户访问等级由低到高分四级： • Visitor（访问级）：处于该级别的用户可以进行 Ping 和 Trace Route 操作，但不能从设备读取任何数据，也不能对设备进行任何设置 • Monitor（监控级）：只能从设备读取数据，而不能对设备进行任何设置 • Configure（系统级）：可以从设备读取数据，并对设备进行配置，但是不能对设备进行软件升级、添加/删除/修改用户、备份/恢复配置文件等操作 • Management（管理级）：可以对设备进行任何操作
密码	设置用户登录时的密码
确认密码	输入的确认密码必须与密码一致。如果不一致，在提交设置时，系统会弹出提示框，提示两次输入的密码不匹配
加密方式	• 可逆：表示设备以可逆的加密算法对用户密码加密后保存 • 不可逆：表示设备以不可逆的加密算法对用户密码加密后保存
服务类型	设置用户可以使用的服务类型，包括Web服务、FTP服务、Telnet服务和Terminal服务，必须至少选择一种服务

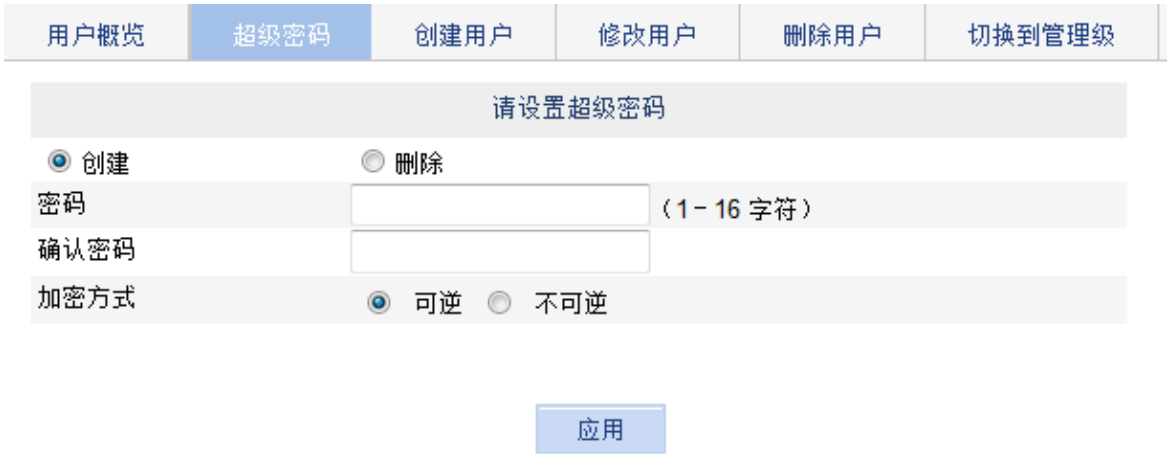
9.3 设置超级密码

本功能用来设置用户从当前访问权限向管理级权限切换时使用的密码。切换密码只能由管理级权限的用户设置，给低于管理级权限的用户使用。如果没有设置切换密码，则切换操作失败。

(1) 在导航栏中选择“设备 > 用户管理”。

(2) 单击“超级密码”页签，进入如下图所示的页面。

图9-2 超级密码



注意：使用超级密码可以使用户的访问等级从当前切换到管理级。

(3) 配置超级密码，详细配置如下表所示。

(4) 单击<应用>按钮完成操作。

表9-2 超级密码的详细配置

配置项	说明
创建/删除	设置要进行操作的类型 • 创建：表示要设置或修改超级密码 • 删除：表示要删除当前的超级密码设置
密码	设置用户切换到管理级权限时的密码
确认密码	输入的确认密码必须与密码一致。如果不一致，在提交设置时，系统会弹出提示框，提示管理员两次输入的密码不匹配
加密方式	• 可逆：表示设备以可逆的加密算法对用户密码加密后保存 • 不可逆：表示设备以不可逆的加密算法对用户密码加密后保存

9.4 切换用户访问等级到管理级

本功能用来使用户从当前级别的访问权限切换到管理级访问权限。进行切换操作时需要注意以下事项：

- 切换前必须有管理级用户设置好的超级密码，如果没有设置超级密码，则不能进行切换。
- 切换操作只对用户当次登录有效，而不改变实际对用户访问等级的配置，用户退出后再次登录时，访问权等级仍为原有级别。

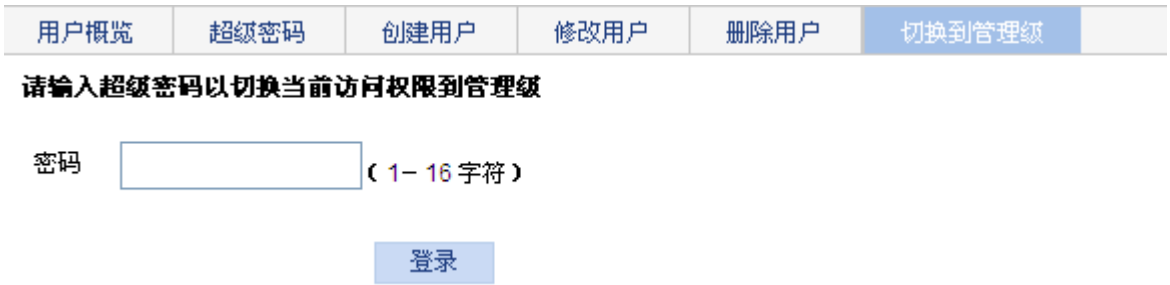
(1) 在导航栏中选择“设备 > 用户管理”。

(2) 单击“切换到管理级”页签，进入如下图所示的页面。

(3) 输入超级密码后。

(4) 单击<登录>按钮切换为管理级用户登录到 Web 页面。

图9-3 切换到管理级



10 SNMP

10.1 概述

SNMP（Simple Network Management Protocol，简单网络管理协议）是因特网中的一种网络管理标准协议，被广泛用于实现管理设备对被管理设备的访问和管理。通过 SNMP 能够对网络设备进行智能化的管理，并且可以屏蔽不同设备物理特性上的差异，实现对不同厂商设备的管理。

SNMP 网络包含 NMS（Network Management System，网络管理系统）和 Agent 两种元素。NMS 是 SNMP 网络的管理者，Agent 是 SNMP 网络的被管理者。NMS 和 Agent 之间通过 SNMP 协议来交互管理信息。

Agent 和 NMS 使用的 SNMP 版本必须相同，才能成功建立连接。目前，Agent 支持 SNMPv1、SNMPv2c 和 SNMPv3 三种版本。

- SNMPv1 采用口令（即团体名，Community Name）认证机制。口令用来限制 NMS 和 Agent 之间的通信。如果 NMS 设置的口令和被管理设备上设置的口令不同，则 NMS 和 Agent 不能建立 SNMP 连接，从而导致 NMS 无法访问 Agent，Agent 发送的告警信息也会被 NMS 丢弃。
- SNMPv2c 也采用口令认证机制。SNMPv2c 对 SNMPv1 的功能进行了扩展：提供了更多的操作类型；支持更多的数据类型；提供了更丰富的错误代码，能够更细致地区分错误。
- SNMPv3 采用 USM（User-Based Security Model，基于用户的安全模型）认证机制。网络管理员可以设置认证和加密功能，认证用于验证报文发送方的合法性，避免非法用户的访问；加密则是对 NMS 和 Agent 之间的传输报文进行加密，以免被窃听。采用认证和加密功能，可以为 NMS 和 Agent 之间的通信提供更高的安全性。



说明

关于 SNMP 协议的详细介绍请参见“网络管理和监控配置指导”中的“SNMP”。

10.2 配置SNMP Agent

(1) 在导航栏中选择“设备 > SNMP”，进入如下图所示的页面。

图10-1 SNMP



(2) 配置 SNMP Agent 的信息，详细配置如下表所示。

(3) 单击<确定>按钮完成操作。

表10-1 SNMP Agent 的详细配置

配置项	说明
SNMP	设置开启或关闭SNMP Agent功能 提示 当 SNMP Agent 关闭时，所有 SNMP Agent 的配置将不会被保存
SNMP版本	设置系统启用的SNMP版本号（选项中的v2即指SNMPv2c版本） Agent上必须设置与NMS上相同的SNMP版本
联系信息	设置描述系统维护联系信息的字符串 如果设备发生故障，维护人员可以利用系统维护联系信息，及时与设备生产厂商取得联系
系统名称	设置设备的系统名称 设置的系统名称显示在导航栏的最上方
设备位置	设置描述设备物理位置的字符串
安全用户名	当SNMP版本选择“SNMP v3”时，设置SNMP安全用户名 Agent上必须设置与NMS上相同的SNMP安全用户名
认证密码	当SNMP版本选择“SNMP v3”时，设置安全用户的认证密码 Agent上必须设置与NMS上相同的认证密码 Agent采用的认证算法为MD5，NMS上也必须设置相同的认证算法

配置项	说明
加密密码	当SNMP版本选择“SNMP v3”时，设置安全用户的加密密码 Agent上必须设置与NMS上相同的加密密码 Agent采用的认证算法为DES56，NMS上也必须设置相同的加密算法
SNMP只读口令	当SNMP版本选择“SNMP v1 & v2”时，设置NMS对Agent进行只读访问时使用的口令 Agent上必须设置与NMS上相同的只读口令，NMS通过该口令只能对Agent进行读操作
SNMP读写口令	当SNMP版本选择“SNMP v1 & v2”时，设置NMS对Agent进行读写访问时使用的口令 Agent上必须设置与NMS上相同的读写口令，NMS通过该口令可以对Agent进行读写操作
Trap口令	• 当 SNMP 版本选择“SNMP v1 & v2”时，设置 Agent 向 NMS 发送 Trap 消息的认证口令。Agent 上必须设置与 NMS 上相同的 Trap 口令，通常将 Trap 口令设置为与只读口令或读写口令相同 • 当 SNMP 版本选择“SNMP v3”时，Trap 口令默认为安全用户名，不可以配置
SNMP信任主机	设置Agent信任的IP地址，以实现仅允许指定源IP地址的NMS对Agent的访问 如果不设置此项，则不对NMS的IP地址进行限制
Trap接收主机地址/域名	设置SNMP Trap消息的目标主机的IP地址或主机名

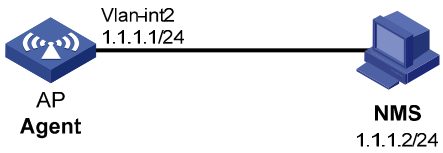
10.3 SNMPv1/v2c典型配置举例

1. 组网需求

如下图所示，NMS（IP 地址为 1.1.1.2/24）与 AP（IP 地址为 1.1.1.2/24）相连。现要实现如下需求：

- NMS 通过 SNMPv1 或者 SNMPv2c 对 AP 进行监控管理。
- AP 在出现故障时能主动向 NMS 发送 Trap 报文。

图10-2 SNMPv1/v2c 配置组网图



2. 配置步骤

(1) 配置 AP 作为 SNMP Agent。

步骤 1：在导航栏中选择“设备 > SNMP”。

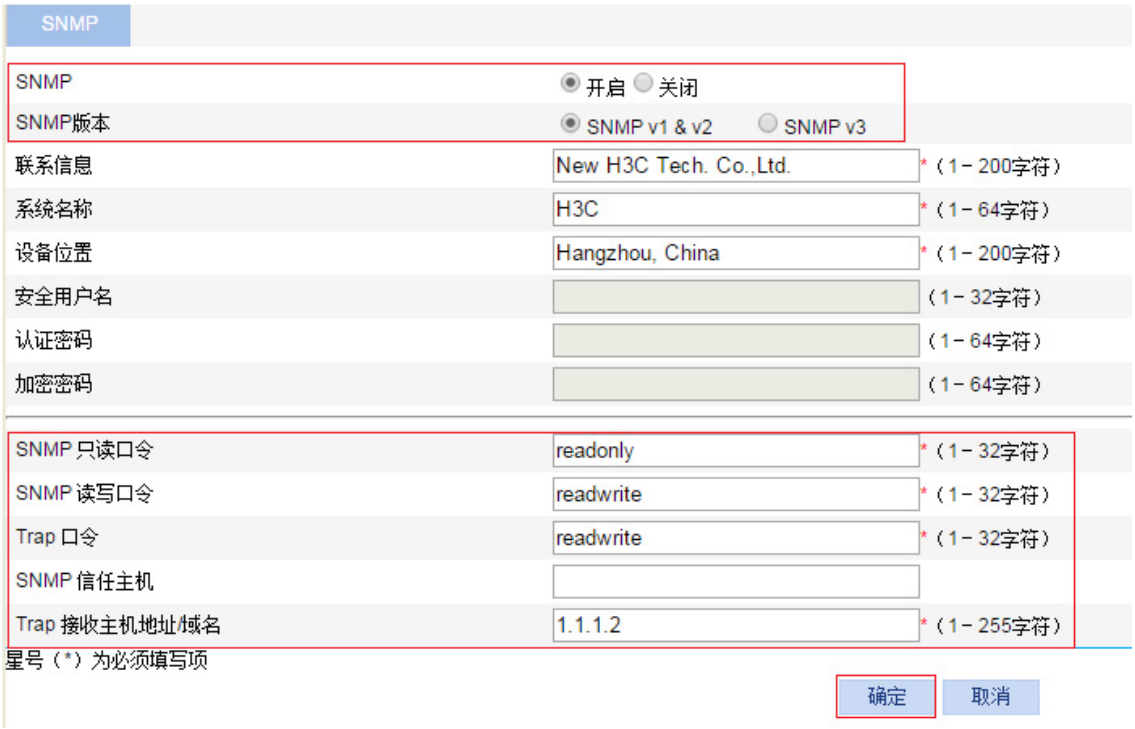
步骤 2：进行如下配置，如下图所示。

- 选中 SNMP“开启”前的单选按钮。
- 选择 SNMP 版本为“SNMP v1 & v2”。
- 输入 SNMP 只读口令为“readonly”。
- 输入 SNMP 读写口令为“readwrite”。

- 输入 Trap 口令为“readwrite”。
- 输入 Trap 接收主机地址为“1.1.1.2”。

步骤 3：单击<确定>按钮完成操作。

图10-3 配置 Agent



(2) 配置 NMS。

说明

NMS 侧的配置必须和 Agent 侧保持一致，否则无法进行相应操作。

设置 NMS 使用的 SNMP 版本为 SNMPv1/v2c，只读口令为 readonly，读写口令为 readwrite。具体配置请参考 NMS 的相关手册。

3. 配置结果验证

- 通过以上配置，NMS 可以和 AP 建立 SNMP 连接，能够通过 MIB 节点查询、设置 AP 上某些参数的值。
- 对 AP 上某个空闲的接口执行关闭/开启操作，NMS 上将看到相应的 Trap 信息。

10.4 SNMPv3典型配置举例

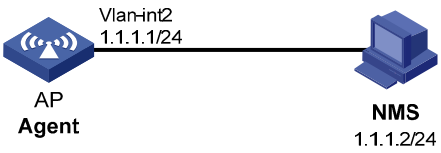
1. 组网需求

如下图所示，NMS（IP 地址为 1.1.1.2/24）与 AP（IP 地址为 1.1.1.1/24）相连。现要实现如下需求：

- NMS 通过 SNMPv3 实现对 AP 的监控管理，并且 AP 只接受 NMS 的管理。

- AP 在出现故障时能主动向 NMS 发送 Trap 报文。
- NMS 与 Agent 建立 SNMP 连接时需要认证，认证密码为 authkey；NMS 与 Agent 之间传输的 SNMP 报文需要加密，加密密码为 prikey。

图10-4 SNMPv3 配置组网图



2. 配置步骤

(1) 配置 AP 作为 SNMP Agent。

步骤 1：在导航栏中选择“设备 > SNMP”。

步骤 2：进行如下配置，如下图所示。

- 选中 SNMP“开启”前的单选按钮。
- 选择 SNMP 版本为“SNMP v3”。
- 输入安全用户名为“user1”。
- 输入认证密码为“authkey”。
- 输入加密密码为“prikey”。
- 输入 SNMP 信任主机为“1.1.1.2”。
- 输入 Trap 接收主机地址为“1.1.1.2”。

步骤 3：单击<确定>按钮完成操作。

图10-5 配置 Agent



(2) 配置 NMS。

说明

NMS 侧的配置必须和 Agent 侧保持一致，否则无法进行相应操作。

设置 NMS 使用的 SNMP 版本为 SNMPv3，用户名为 user1，启用认证和加密功能，认证算法为 MD5，认证密码为 authkey，加密算法为 DES56，加密密码为 prikey。具体配置请参考 NMS 的相关手册。

3. 配置结果验证

- 通过以上配置，NMS 可以和 AP 建立 SNMP 连接，能够通过 MIB 节点查询、设置 AP 上某些参数的值。
- 对 AP 上某个空闲的接口执行关闭/开启操作，NMS 上将看到相应的 Trap 信息。

11 环回测试

11.1 概述

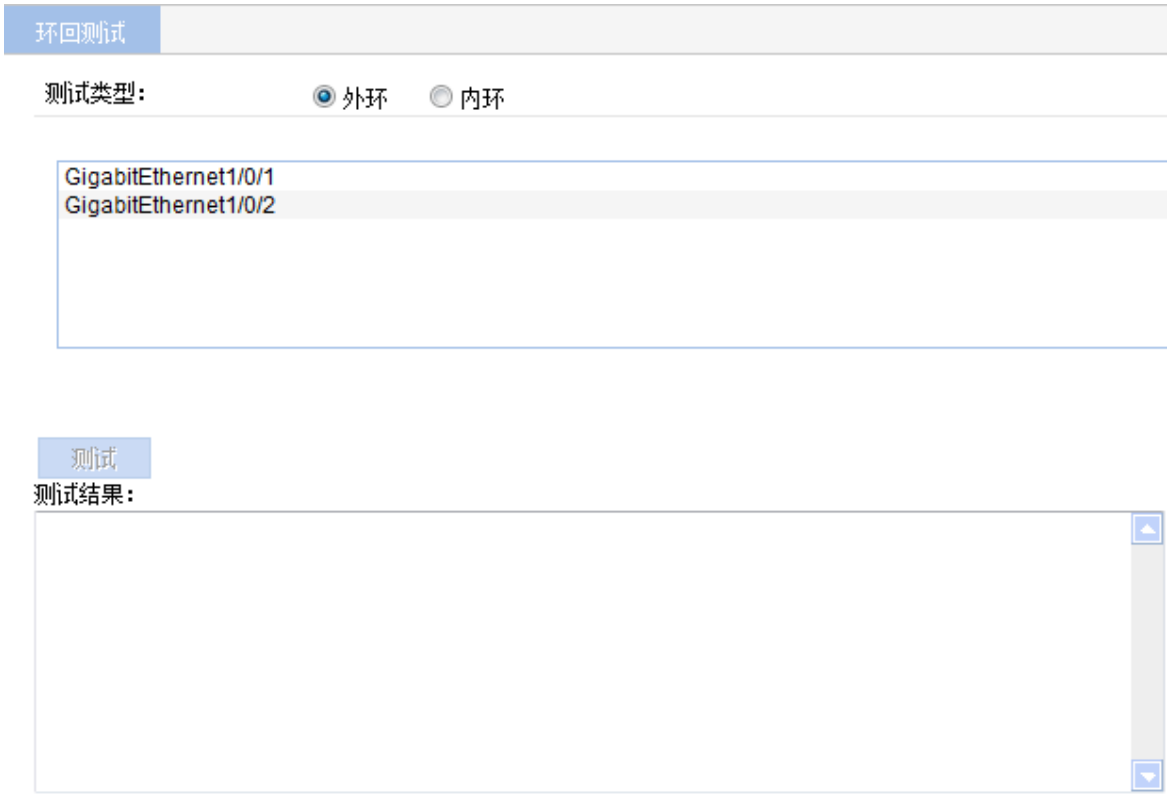
通过使用以太网接口环回测试工具，用户可以检验以太网接口能否正常工作。测试时接口将不能正常转发数据包。以太网接口环回测试功能包括内部环回测试和外部环回测试。

- 内部环回测试是在交换芯片内部建立自环，用以定位芯片内与该端口相关的功能是否出现故障。
- 外部环回测试是在以太网接口上接一个自环头，从接口发出的报文通过自环头又环回到该接口，并被该接口接收。用以定位该端口的硬件功能是否出现故障。

11.2 环回测试操作

(1) 在导航栏中选择“设备 > 环回测试”，进入如下图所示的页面。

图11-1 环回测试



说明

该页面显示的接口信息与设备的型号有关，请以设备的实际情况为准。

(2) 配置环回测试的参数，详细配置如下表所示。

表11-1 环回测试的详细配置

配置项		说明
测试类型	外环	设置对以太网接口进行环回测试的具体测试类型 在“外环”和“内环”前的单选按钮中进行选择： 测试类型的支持情况与设备的型号有关，请以设备的实际情况为准
	内环	
接口		设置要进行环回测试的以太网接口

(3) 单击<测试>按钮开始执行环回测试。

(4) 环回测试结束后，在“测试结果”框中查看环回测试的结果，如下图所示。

图11-2 环回测试结果（以内环测试为例）



说明

该页面显示的接口信息与设备的型号有关，请以设备的实际情况为准。

11.3 注意事项

进行环回测试时需要注意如下事项：

(1) 端口物理关闭状态下可以进行内部环回测试，但不能进行外部环回测试。手工关闭时，则不能进行内部和外部环回测试。

(2) 在进行环回测试时系统将禁止在接口上进行“速率”、“双工状态”、“网线类型”和“端口状态”配置项的配置。

(3) 以太网接口在进行环回测试时将工作在全双工状态；环回测试关闭后恢复原有配置。

目 录

1 MAC地址 ····· 1-1
1.1 概述 ····· 1-1
1.2 配置MAC地址表项 ····· 1-2
1.3 配置MAC地址表项的老化时间 ····· 1-3
1.4 MAC地址典型配置举例 ····· 1-4
2 VLAN ····· 2-1
2.1 概述 ····· 2-1
2.2 VLAN配置任务简介 ····· 2-1
2.3 新建VLAN ····· 2-2
2.4 配置VLAN中的端口 ····· 2-3
2.5 配置端口所属的VLAN ····· 2-4
2.6 VLAN典型配置举例 ····· 2-5
2.7 注意事项 ····· 2-7
3 ARP管理 ····· 3-1
3.1 概述 ····· 3-1
3.1.1 ARP简介 ····· 3-1
3.1.2 免费ARP简介 ····· 3-1
3.2 查看ARP表项 ····· 3-2
3.3 配置静态ARP表项 ····· 3-2
3.4 删除ARP表项 ····· 3-3
3.5 配置免费ARP功能 ····· 3-3
3.6 静态ARP典型配置举例 ····· 3-4
4 IGMP Snooping ····· 4-1
4.1 概述 ····· 4-1
4.2 IGMP Snooping配置任务简介 ····· 4-2
4.3 全局启用IGMP Snooping ····· 4-2
4.4 在VLAN内配置IGMP Snooping ····· 4-3
4.5 在端口上配置IGMP Snooping ····· 4-4
4.6 查看IGMP Snooping组播表项信息 ····· 4-6
4.7 IGMP Snooping典型配置举例 ····· 4-7
5 IPv4 和IPv6 路由 ····· 5-1
5.1 概述 ····· 5-1
5.2 查看IPv4 激活路由表 ····· 5-1

5.3 新建IPv4 静态路由 ····· 5-2
5.4 查看IPv6 激活路由表 ····· 5-4
5.5 新建IPv6 静态路由 ····· 5-4
5.6 IPv4 静态路由典型配置举例 ····· 5-6
5.7 IPv6 静态路由典型配置举例 ····· 5-8
5.8 注意事项 ····· 5-10
6 DHCP ····· 6-1
6.1 概述 ····· 6-1
6.1.1 DHCP简介 ····· 6-1
6.2 配置DHCP服务器 ····· 6-2
6.2.1 DHCP服务器配置任务简介 ····· 6-2
6.2.2 启动DHCP服务 ····· 6-2
6.2.3 配置DHCP服务器的静态地址池 ····· 6-3
6.2.4 配置DHCP服务器的动态地址池 ····· 6-5
6.2.5 配置接口工作在DHCP服务器模式 ····· 6-6
6.2.6 查看地址池中已被分配的地址信息 ····· 6-6
6.3 DHCP服务器典型配置举例 ····· 6-7
7 DNS ····· 7-1
7.1 概述 ····· 7-1
7.2 DNS配置任务简介 ····· 7-1
7.3 配置静态域名解析表 ····· 7-2
7.4 启动动态域名解析 ····· 7-3
7.5 配置DNS服务器的IP地址 ····· 7-3
7.6 配置域名后缀 ····· 7-4
7.7 清空动态域名缓存区 ····· 7-4
7.8 DNS典型配置举例 ····· 7-4
8 PPPoE ····· 8-1
8.1 概述 ····· 8-1
8.2 配置PPPoE Client ····· 8-1
8.3 查看PPPoE Client会话统计信息 ····· 8-3
8.4 查看PPPoE Client会话概要信息 ····· 8-4
8.5 PPPoE Client典型配置举例 ····· 8-5
8.6 注意事项 ····· 8-7
9 服务管理 ····· 9-1
9.1 概述 ····· 9-1
9.2 配置服务管理 ····· 9-1

10 诊断工具 ····· 10-1
10.1 概述 ····· 10-1
10.1.1 Ping ····· 10-1
10.1.2 Trace Route ····· 10-1
10.2 Ping操作 ····· 10-1
10.2.1 IPv4 Ping ····· 10-1
10.2.2 IPv6 Ping ····· 10-3
10.3 Trace Route操作 ····· 10-5

1 MAC地址

说明

- MAC 地址模块中对于接口的相关配置，目前只能在二层以太网接口上进行。
- 本章节内容只涉及静态和动态地址表项的管理，不涉及组播 MAC 地址表项管理的内容。

1.1 概述

为了转发报文，设备需要维护 MAC 地址表。MAC 地址表的表项包含了与该设备相连的设备的 MAC 地址、与此设备相连的设备的接口号以及所属的 VLAN ID。MAC 地址表中的表项包括静态表项和动态表项，其中静态表项是由用户配置的；动态表项包括用户配置的以及设备学习得来的。静态表项不会被老化掉，而动态表项会被老化掉。

设备学习 MAC 地址的方法如下：如果从某接口（假设为接口 A）收到一个数据帧，设备就会分析该数据帧的源 MAC 地址（假设为 MAC-SOURCE）并认为目的 MAC 地址为 MAC-SOURCE 的报文可以由接口 A 转发；如果 MAC 地址表中已经包含 MAC-SOURCE，设备将对该表项进行更新；如果 MAC 地址表中尚未包含 MAC-SOURCE，设备则将这个新 MAC 地址以及该 MAC 地址对应的接口 A 作为一个新的表项加入到 MAC 地址表中。

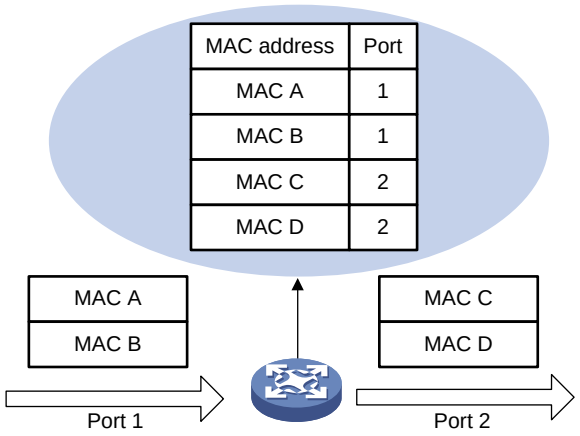
说明

在设备学习 MAC 地址时，用户手工配置的静态 MAC 地址表项不能被学习中获得的动态 MAC 地址覆盖，而动态 MAC 地址表项可以被静态 MAC 地址覆盖。

设备在转发报文时，根据 MAC 地址表项信息，会采取以下两种转发方式：

- 单播方式：当 MAC 地址表中包含与报文目的 MAC 地址对应的表项时，设备直接将报文从该表项中的转发出接口发送。
- 广播方式：当设备收到目的地址为全 F 的报文，或 MAC 地址表中没有包含对应报文目的 MAC 地址的表项时，设备将采取广播方式将报文向除接收接口外的所有接口进行转发。

图1-1 设备的 MAC 地址表项



1.2 配置MAC地址表项

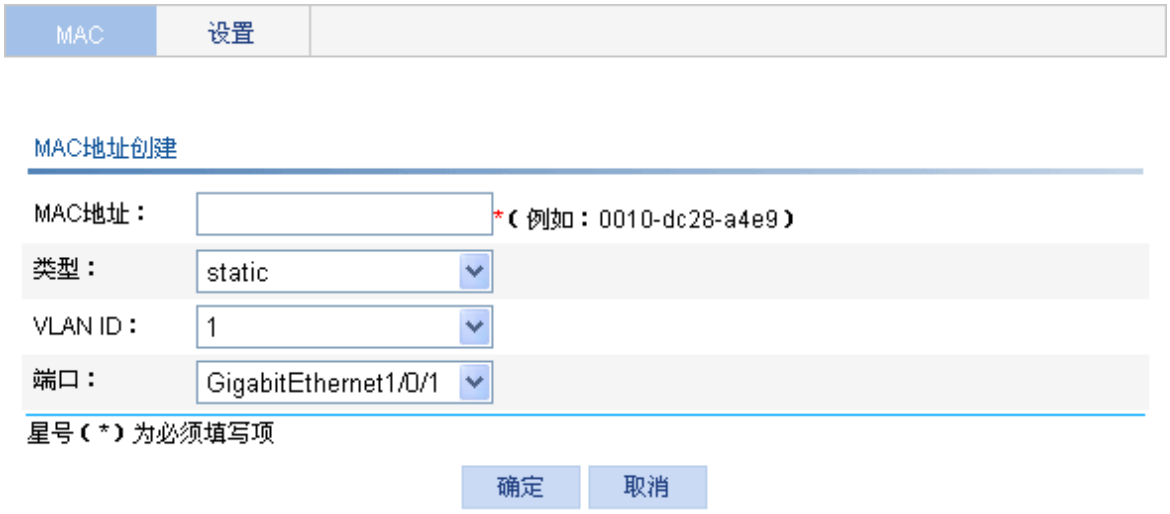
(1) 在导航栏中选择“网络 > MAC 地址”，默认进入“MAC”页签的页面，页面显示所有的 MAC 地址表项，如下图所示。

图1-2 MAC



(2) 单击<新建>按钮，进入新建 MAC 地址表项的配置页面，如下图所示。

图1-3 MAC 地址创建



(3) 配置 MAC 地址表项的信息，详细配置如下表所示。

(4) 单击<确定>按钮完成操作。

表1-1 新建 MAC 地址表项的详细配置

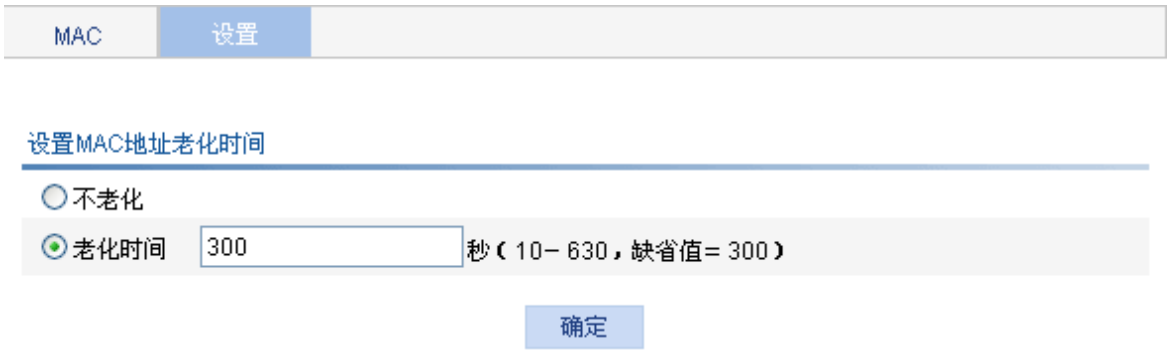
配置项	说明
MAC地址	设置待添加的MAC地址
类型	设置该MAC地址表项的类型，包括： • static：表示该表项是静态 MAC 地址表项，没有老化时间 • dynamic：表示该表项是动态 MAC 地址表项，有老化时间 • blackhole：表示该表项是黑洞 MAC 地址表项，没有老化时间 提示 在 MAC 地址表项显示页面的列表中共有如下几种类型： • Config static：表示该表项是用户手工配置的静态表项 • Config dynamic：表示该表项是用户手工配置的动态表项 • Blackhole：表示该表项是黑洞表项 • Learned：表示该表项是设备学习得来的动态表项 • Other：表示该表项为除上述状态外的其他类型
VLAN ID	设置该MAC地址表项所属的VLAN
端口	设置该MAC地址表项所属的端口，黑洞表项不需要设置所属端口

1.3 配置MAC地址表项的老化时间

(1) 在导航栏中选择“网络 > MAC 地址”。

(2) 单击“设置”页签，进入 MAC 地址表项老化时间的配置页面，如下图所示。

图1-4 设置



(3) 配置 MAC 地址表项老化时间，详细配置如下表所示。

(4) 单击<确定>按钮完成操作。

表1-2 MAC 地址老化时间的详细配置

配置项	说明
不老化	设置MAC地址表项不会老化
老化时间	设置MAC地址表项的老化，并指定老化时间

1.4 MAC地址典型配置举例

1. 组网需求

用户通过 Web 网管设置 MAC 地址表功能。要求在 VLAN1 中的 GigabitEthernet1/0/1 端口下添加一个静态 MAC 地址表项 00e0-fc35-dc71。

2. 配置步骤

配置静态 MAC 地址表项。

步骤 1：在导航栏中选择“网络 > MAC 地址”，默认进入“MAC”页签的页面。

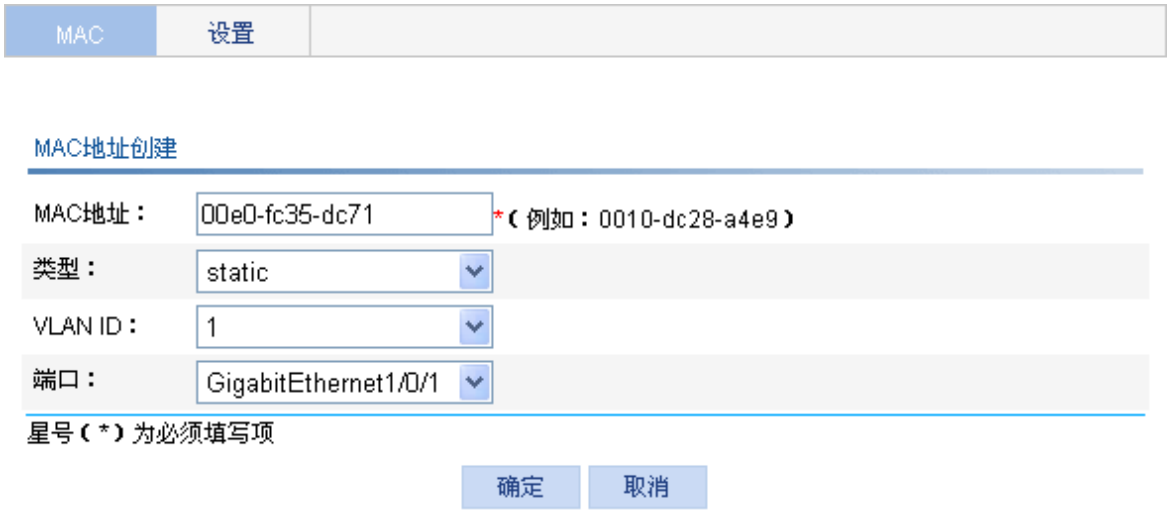
步骤 2：单击<新建>按钮。

步骤 3：进行如下配置，如下图所示。

- 输入 MAC 地址为“00e0-fc35-dc71”。
- 选择类型为“static”。
- 选择 VLAN ID 为“1”。
- 选择端口为“GigabitEthernet1/0/1”。

步骤 4：单击<确定>按钮完成操作。

图1-5 新建静态 MAC 地址表项

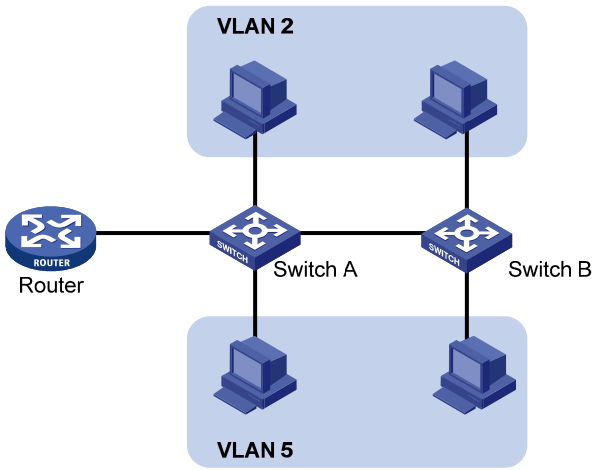


2 VLAN

2.1 概述

以太网是一种基于 CSMA/CD（Carrier Sense Multiple Access/Collision Detect，带冲突检测的载波侦听多路访问）的共享通讯介质的数据网络通讯技术，当主机数目较多时会导致冲突严重、广播泛滥、性能显著下降，甚至网络不可用等问题。通过交换机实现 LAN 互联虽然可以解决冲突（Collision）严重的问题，但仍然不能隔离广播报文。在这种情况下出现了 VLAN（Virtual Local Area Network，虚拟局域网）技术，这种技术可以把一个 LAN 划分成多个虚拟的 LAN——VLAN，每个 VLAN 是一个广播域，VLAN 内的主机间通信就和在一个 LAN 内一样，而 VLAN 间则不能直接互通。这样，广播报文被限制在一个 VLAN 内，如下图所示。

图2-1 VLAN 示意图



VLAN 根据划分方式不同可以分为不同类型，Web 界面目前只支持对基于端口的 VLAN 的配置。基于端口划分 VLAN 是 VLAN 最简单、最有效的划分方式。他按照设备端口来定义 VLAN 成员，将指定端口加入到指定 VLAN 中之后，端口就可以转发指定 VLAN 的报文。

说明

关于 VLAN 的详细介绍请参见“二层技术配置指导”中的“VLAN”。

2.2 VLAN配置任务简介

表2-1 VLAN 配置步骤

步骤	配置任务	说明
1	2.3 新建VLAN	必选 新建一个或多个VLAN

步骤	配置任务	说明
2	2.4 配置VLAN中的端口	二者至少选择其一 配置VLAN的Untagged、Tagged成员，或从VLAN中删除成员
3	2.5 配置端口所属的VLAN	

2.3 新建VLAN

(1) 在导航栏中选择“网络 > VLAN”，默认进入“VLAN”页签的页面，如下图所示。

图2-2 VLAN



窍门

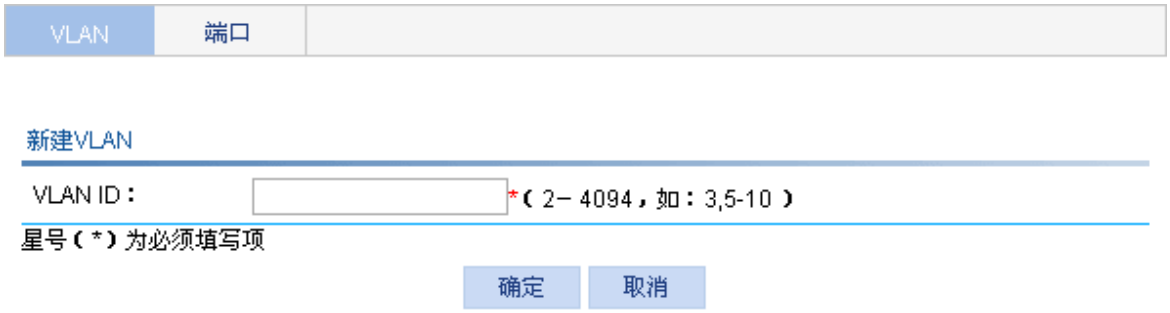
当存在大量 VLAN 时，在上图所示页面的“VLAN 范围”文本框中输入一个 VLAN 范围，单击<选择>按钮，页面的 VLAN 列表中将只显示该范围内的 VLAN 信息，并且对 VLAN 的查询也将在此范围内进行，这样可以方便用户的操作；而单击<删除>按钮，则会将该范围内的 VLAN 全部删除。

(2) 单击<新建>按钮，进入新建 VLAN 的配置页面，如下图所示。

(3) 在“VLAN ID”文本框中输入要创建的 VLAN ID。

(4) 单击<确定>按钮完成操作。

图2-3 新建 VLAN

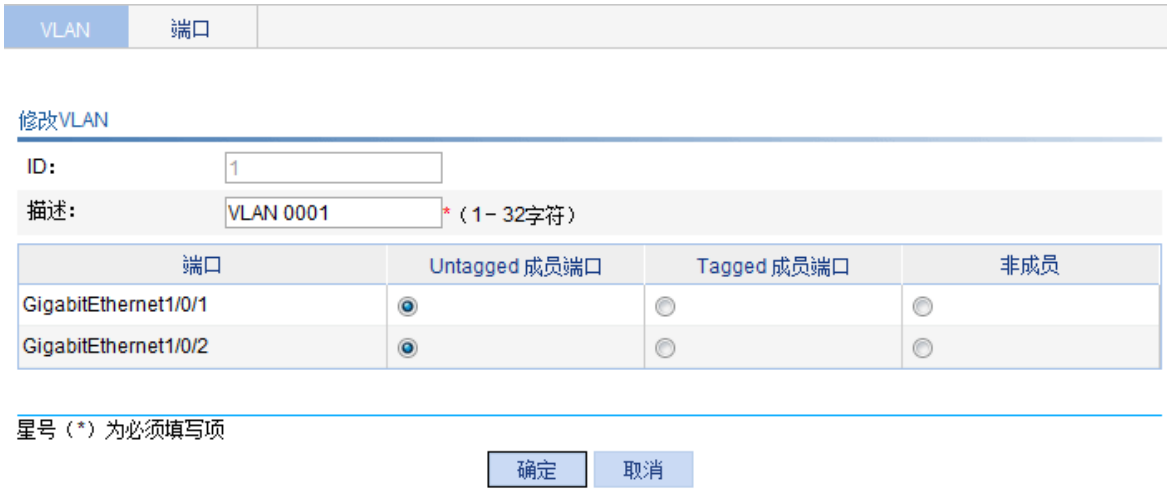


2.4 配置VLAN中的端口

(1) 在导航栏中选择“网络 > VLAN”，默认进入“VLAN”页签的页面，如 图 2-2 所示。

(2) 在 VLAN 列表中单击某 VLAN 对应的 图标，进入修改该 VLAN 的配置页面，如下图所示。

图2-4 修改 VLAN



(3) 配置 VLAN 的描述，以及 VLAN 中的端口成员，详细配置如下表所示。

(4) 单击<确定>按钮完成操作。

表2-2 VLAN 中端口的详细配置

配置项		说明
ID		显示要修改的VLAN的ID
描述		设置VLAN的描述字符串 缺省情况下，VLAN的描述字符串为该VLAN的VLAN ID，如“VLAN 0001”
端口	Untagged成员端口	在端口列表中找到要加入或删除的端口，在端口对应的“Untagged成员端口”、“Tagged成员端口”和“非成员”列的单选按钮中进行选择： • Untagged：表示端口成员发送该 VLAN 报文时不带 Tag 标签
	Tagged成员端口	

配置项		说明
	非成员	• Tagged：表示端口成员发送该 VLAN 报文时带 Tag 标签 • 非成员：表示从该 VLAN 中删除端口成员 提示 将 Access 端口配置为某 VLAN 时，该端口会被修改为 Hybrid 端口

2.5 配置端口所属的VLAN

(1) 在导航栏中选择“网络 > VLAN”。

(2) 单击“端口”页签，进入端口显示页面，如下图所示。

图2-5 端口



(3) 在端口列表中单击某端口对应的图标，进入修改该端口的配置页面，如下图所示。

图2-6 修改端口



(4) 配置端口所属的 VLAN，详细配置如下表所示。

(5) 单击<确定>按钮完成操作。

表2-3 端口所属 VLAN 的详细配置

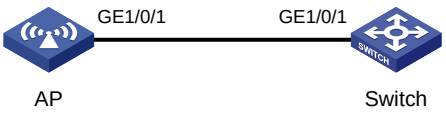
配置项		说明
端口		显示要修改所属VLAN的端口
Untagged成员VLAN		显示该端口目前是哪个或哪些VLAN的Untagged成员
Tagged成员VLAN		显示该端口目前是哪个或哪些VLAN的Tagged成员
成员类型	Untagged	在“Untagged”、“Tagged”和“非成员”前的单选按钮中进行选择 • Untagged：表示端口成员发送该 VLAN 报文时不带 Tag 标签 • Tagged：表示端口成员发送该 VLAN 报文时带 Tag 标签 • 非成员：表示从该 VLAN 中删除端口成员 提示 • 将 Access 端口配置为某 VLAN 的 Untagged 成员时，该 VLAN 必须已经存在 • 将 Access 端口配置为某 VLAN 的 Tagged 成员或将 Trunk 端口一次配置为多个 VLAN 的 Untagged 成员时，该端口会被修改为 Hybrid 端口 • 将 Hybrid 端口配置为某 VLAN 的 Untagged 或 Tagged 成员时，该 VLAN 必须是已经存在的静态 VLAN
	Tagged	
	非成员	
VLAN ID		设置要修改端口成员的目的VLAN

2.6 VLAN典型配置举例

1. 组网需求

- AP 与 Switch 使用 GigabitEthernet1/0/1 相连。
- GigabitEthernet1/0/1 为 Hybrid 端口，缺省 VLAN ID 为 1。
- 配置 GigabitEthernet1/0/1，使该端口允许 VLAN 1、VLAN 2、VLAN 6 到 VLAN 50、VLAN 100 的报文通过，且允许 VLAN 1 和 VLAN 100 的报文发送时不带 Tag 标签。

图2-7 VLAN 配置组网图



2. 配置AP

注意

- 缺省情况下，GigabitEthernet1/0/1 为 Access 端口，缺省 VLAN ID 为 1。
- 执行下述的配置步骤时，如果颠倒配置端口 GigabitEthernet1/0/1 的 Tagged 成员和 Untagged 成员的先后顺序，则在配置 Untagged 成员时输入的 VLAN ID 必须为“1,100”，否则端口的缺省 VLAN ID 将变为 100。

(1) 创建 VLAN 2、VLAN 6 到 VLAN 50、VLAN 100。

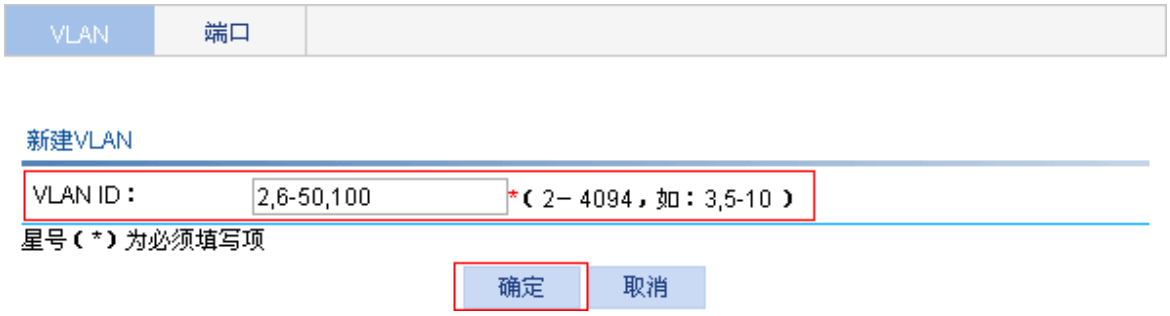
步骤 1：在导航栏中选择“网络 > VLAN”，默认进入“VLAN”页签的页面。

步骤 2：单击<新建>按钮。

步骤 3：如下图所示，输入 VLAN ID 为“2,6-50,100”。

步骤 4：单击<确定>按钮完成操作。

图2-8 新建 VLAN



(2)　配置 GigabitEthernet1/0/1 为 VLAN 2、VLAN 6 到 VLAN 50 的 Tagged 成员。

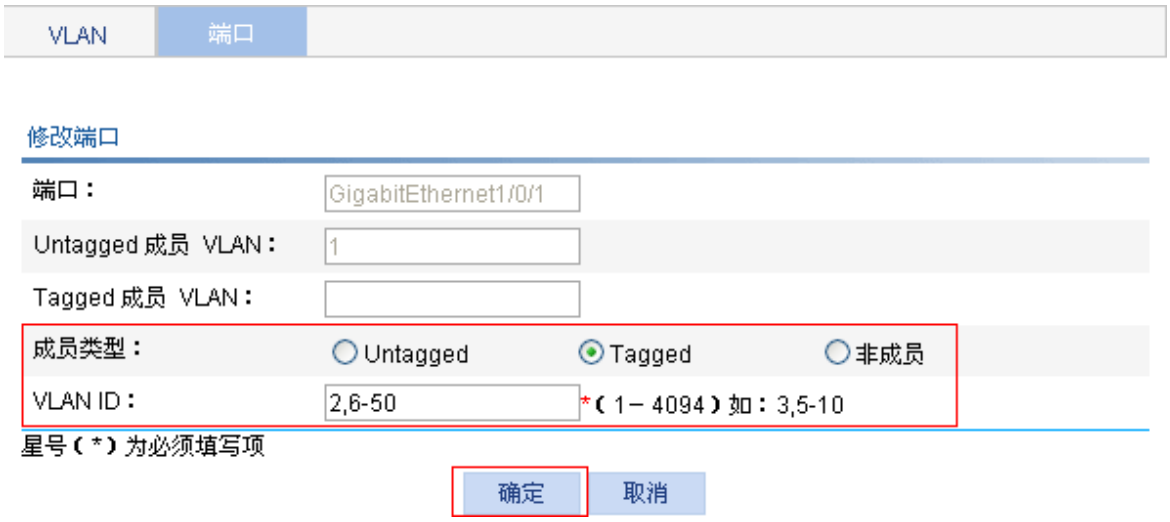
步骤 1：单击“端口”页签。

步骤 2：在端口列表中单击 GigabitEthernet1/0/1 对应的图标。

步骤 3：进行如下配置，如下图所示。

- 选择成员类型为“Tagged”。
- 输入 VLAN ID 为“2,6-50”。

图2-9 配置 GigabitEthernet1/0/1 的 Tagged 成员



步骤 4：单击<确定>按钮，弹出如下图所示的对话框。

步骤 5：在对话框中单击<确定>完成操作。

图2-10 确认配置对话框



(3) 配置 GigabitEthernet1/0/1 为 VLAN 100 的 Untagged 成员。

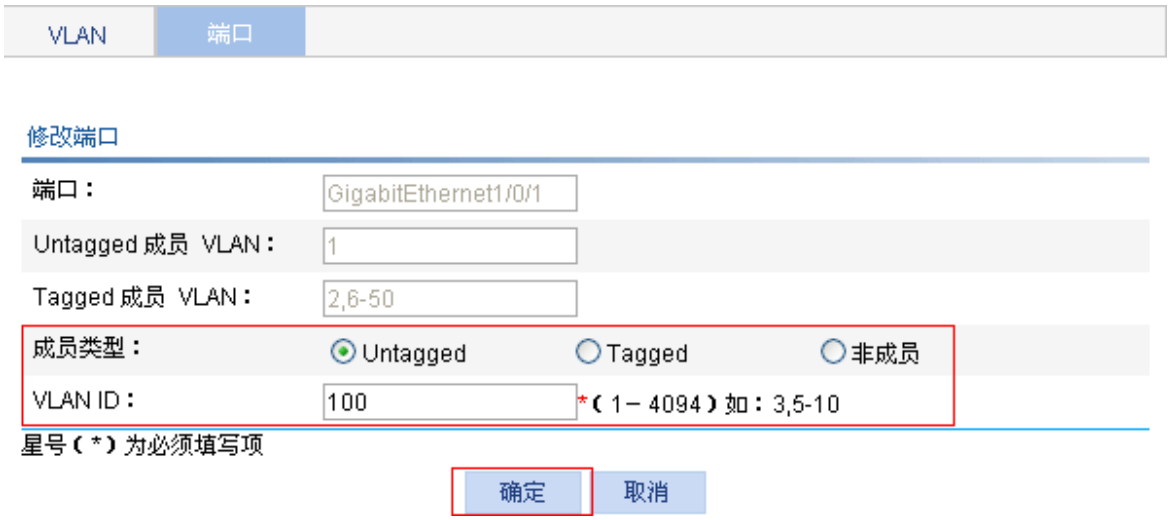
步骤 1：再次在端口列表中单击 GigabitEthernet1/0/1 对应的 图标。

步骤 2：进行如下配置，如下图所示。

- 选择成员类型为“Untagged”。
- 输入 VLAN ID 为“100”。

步骤 3：单击<确定>按钮完成操作。

图2-11 配置 GigabitEthernet1/0/1 的 Untagged 成员



3. 配置Switch

与 AP 上的配置步骤相似，不再赘述。

2.7 注意事项

配置 VLAN 时需要注意如下事项：

(1) VLAN1 为系统缺省 VLAN，用户不能手工创建和删除。

(2) 保留 VLAN 是系统为实现特定功能预留的 VLAN，用户不能手工创建和删除。

(3) 用户不能手工删除设备上动态学习到的 VLAN。

3 ARP管理

3.1 概述

3.1.1 ARP简介

ARP（Address Resolution Protocol，地址解析协议）是将 IP 地址解析为以太网 MAC 地址（或称物理地址）的协议。

在局域网中，当主机或其它网络设备有数据要发送给另一个主机或设备时，它必须知道对方的网络层地址（即 IP 地址）。但是仅仅有 IP 地址是不够的，因为 IP 数据报文必须封装成帧才能通过物理网络发送，因此发送站还必须有接收站的物理地址，所以需要一个从 IP 地址到物理地址的映射。APR 就是实现这个功能的协议。



说明

关于 ARP 协议的详细介绍请参见“三层技术配置指导”中的“ARP”。

3.1.2 免费ARP简介

1. 免费ARP报文

免费 ARP 报文是一种特殊的 ARP 报文，该报文中携带的发送者 IP 地址和目标 IP 地址都是本机 IP 地址，报文源 MAC 地址是本机 MAC 地址，报文的目的 MAC 地址是广播地址。

设备通过对外发送免费 ARP 报文来实现以下功能：

- 确定其它设备的 IP 地址是否与本机 IP 地址冲突。当其它设备收到免费 ARP 报文后，如果发现报文中的IP地址和自己的IP地址相同，则给发送免费ARP报文的设备返回一个ARP应答，告知该设备 IP 地址冲突。
- 设备改变了硬件地址，通过发送免费 ARP 报文通知其他设备更新 ARP 表项。

2. 免费ARP报文学习功能

使能了免费 ARP 报文学习功能后，设备会根据收到的免费 ARP 报文中携带的信息（源 IP 地址、源 MAC 地址）对自身维护的 ARP 表进行修改。设备先判断 ARP 表中是否存在与此免费 ARP 报文源 IP 地址对应的 ARP 表项：

- 如果没有对应的 ARP 表项，设备会根据该免费 ARP 报文中携带的信息新建 ARP 表项。
- 如果存在对应的ARP表项，设备会根据该免费ARP报文中携带的信息更新对应的ARP表项。

关闭免费 ARP 报文学习功能后，设备不会根据收到的免费 ARP 报文来新建 ARP 表项，但是会更新已存在的对应 ARP 表项。如果用户不希望通过免费 ARP 报文来新建 ARP 表项，可以关闭免费 ARP 报文学习功能，以节省 ARP 表项资源。

3.2 查看ARP表项

在导航栏中选择“网络 > ARP 管理”，默认进入“ARP 表”页签的页面，如下图所示。页面显示所有 ARP 表项的信息。

图3-1 ARP 表

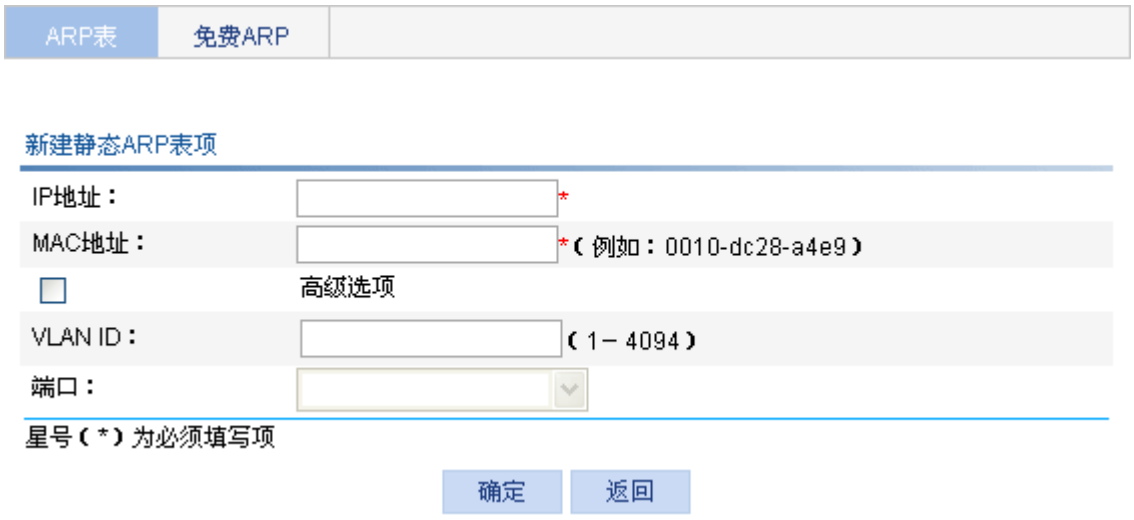


3.3 配置静态ARP表项

(1) 在导航栏中选择“网络 > ARP管理”，默认进入“ARP表”页签的页面，如 图 3-1 所示。

(2) 单击<新建>按钮，进入新建静态 ARP 表项的配置页面，如下图所示。

图3-2 新建静态 ARP



(3) 配置静态 ARP 表项的信息，详细配置如下表所示。

(4) 单击<确定>按钮完成操作。

表3-1 静态 ARP 表项的详细配置

配置项	说明
IP地址	设置静态ARP表项的IP地址

配置项		说明
MAC地址		设置静态ARP表项的MAC地址
高级选项	VLAN ID	设置静态ARP表项所属的VLAN和端口 提示 指定的 VLAN ID 必须是已经创建好的 VLAN 的 ID，且指定的端口必须属于这个 VLAN；指定的 VLAN ID 对应的 VLAN 虚接口必须已经创建
	端口	

3.4 删除ARP表项

(1) 在导航栏中选择“网络 > ARP管理”，默认进入“ARP表”页签的页面，如 图 3-1 所示。

(2) 删除 ARP 表项，详细配置如下表所示。

表3-2 删除 ARP 表项的详细配置

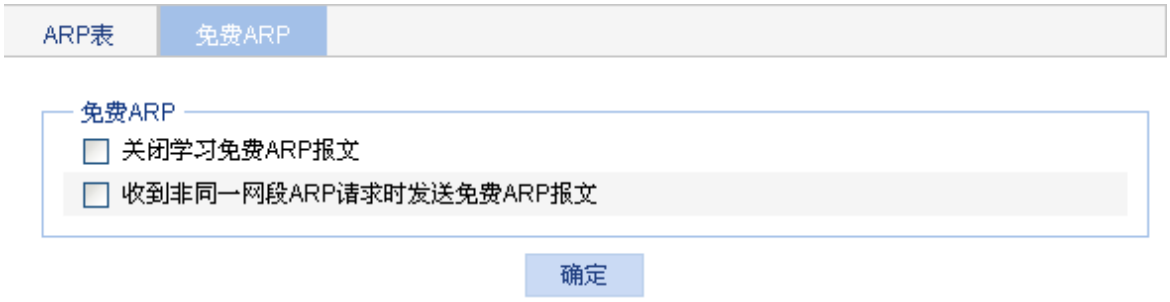
功能	配置方法
删除指定的ARP表项	在列表中选中指定ARP表项前的复选框，单击<删除选中>按钮
删除所有静态和动态ARP表项	单击<删除所有静态和动态表项>按钮
删除所有静态ARP表项	单击<删除所有静态表项>按钮
删除所有动态ARP表项	单击<删除所有动态表项>按钮

3.5 配置免费ARP功能

(1) 在导航栏中选择“网络 > ARP 管理”。

(2) 单击“免费 ARP”页签，进入如下图所示的页面。

图3-3 免费 ARP



(3) 配置免费 ARP 功能，详细配置如下表所示。

(4) 单击<确定>按钮完成操作。

表3-3 免费 ARP 功能的详细配置

配置项	说明
关闭学习免费ARP报文	设置是否关闭免费ARP报文学习功能 缺省情况下，免费ARP报文学习功能处于开启状态
收到非同一网段ARP请求时发送免费ARP报文	设置开启收到非同一网段ARP请求时发送免费ARP报文功能 缺省情况下，收到非同一网段ARP请求时不发送免费ARP报文

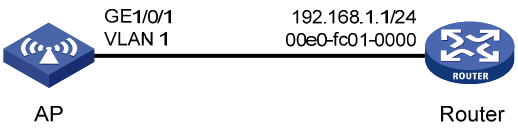
3.6 静态ARP典型配置举例

1. 组网需求

- AP 通过接口 GigabitEthernet1/0/1 连接 Router。接口 GigabitEthernet1/0/1 属于 VLAN 1。
- Router 的 IP 地址为 192.168.1.1/24，MAC 地址为 00e0-fc01-0000。

为了增加 AP 和 Router 通信的安全性，可以在 AP 上配置静态 ARP 表项。

图3-4 静态 ARP 配置组网图



2. 配置步骤

说明

进行下面的配置前，假设接口 Vlan-interface1 已存在，管理员通过 Vlan-interface1 登录 AP 的 Web 页面进行配置。

(1) 配置静态 ARP 表项。

步骤 1：在导航栏中选择“网络 > ARP 管理”，默认进入“ARP 表”页签的页面。

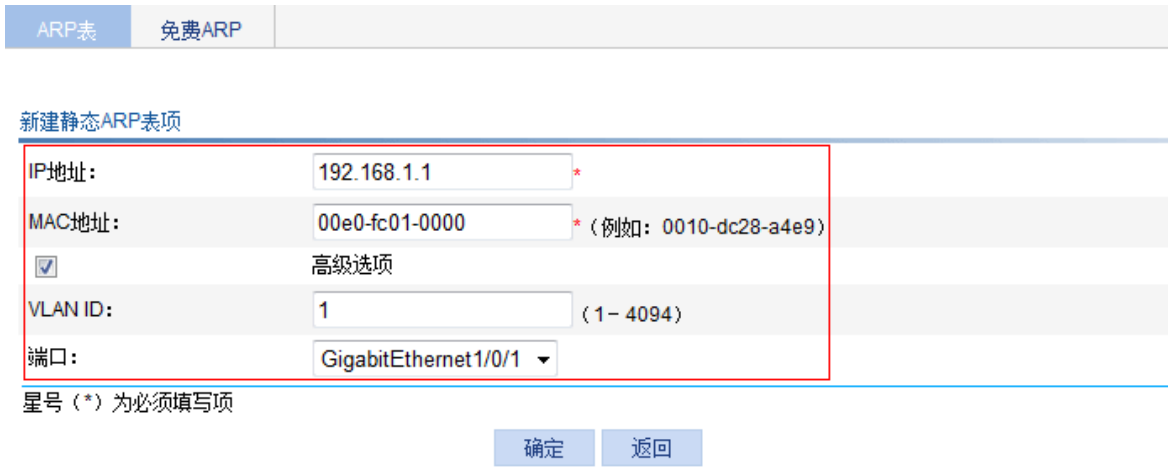
步骤 2：单击<新建>按钮。

步骤 3：进行如下配置，如下图所示。

- 输入 IP 地址为“192.168.1.1”。
- 输入 MAC 地址为“00e0-fc01-0000”。
- 选中“高级选项”前的复选框。
- 输入 VLAN ID 为“1”。
- 选择端口为“GigabitEthernet1/0/1”。

步骤 4：单击<确定>按钮完成操作。

图3-5 新建静态 ARP 表项



4 IGMP Snooping

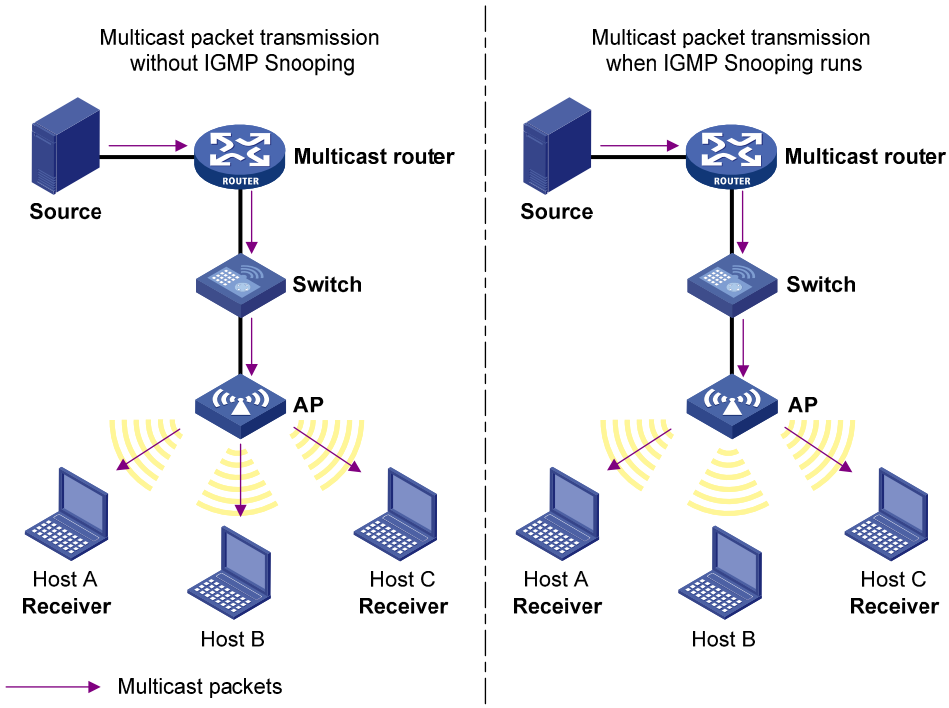
4.1 概述

IGMP Snooping 是 Internet Group Management Protocol Snooping（互联网组管理协议窥探）的简称，它是运行在二层设备上的组播约束机制，用于管理和控制组播组。

运行 IGMP Snooping 的二层设备通过对收到的 IGMP 报文进行分析，为端口和 MAC 组播地址建立起映射关系，并根据这样的映射关系转发组播数据。

如下图所示，当二层设备没有运行 IGMP Snooping 时，组播数据在二层被广播；当二层设备运行了 IGMP Snooping 后，已知组播组的组播数据不会在二层被广播，而在二层被组播给指定的接收者。

图4-1 二层设备运行 IGMP Snooping 前后的对比



IGMP Snooping 通过二层组播将信息只转发给有需要的接收者，可以带来以下好处：

- 减少二层网络中的广播报文，节约网络带宽。
- 增强组播信息的安全性。
- 为实现对每台主机的单独计费带来方便。

说明

关于 IGMP Snooping 的详细介绍请参见“IP 组播配置指导”中的“IGMP Snooping”。

4.2 IGMP Snooping配置任务简介

表4-1 IGMP Snooping 配置步骤

步骤	配置任务	说明
1	4.3 全局启用IGMP Snooping	必选 缺省情况下，全局IGMP Snooping处于关闭状态
2	4.4 在VLAN内配置IGMP Snooping	必选 在VLAN内启用IGMP Snooping，配置IGMP Snooping版本、查询器等功能 缺省情况下，VLAN内的IGMP Snooping处于关闭状态 提示 • 在 VLAN 内配置 IGMP Snooping 之前，必须先在全局启用 IGMP Snooping • 在 VLAN 内启用 IGMP Snooping 之后，不允许在该 VLAN 所对应的 VLAN 接口上再启用 IGMP 和 PIM，反之亦然 • 在 VLAN 内启用了 IGMP Snooping 之后，该功能只在属于该 VLAN 的端口上生效
3	4.5 在端口上配置IGMP Snooping	可选 在指定VLAN内容配置端口的最大组播组数和端口快速离开功能 提示 • 在端口上配置 IGMP Snooping 之前，必须先全局启用组播路由或 IGMP Snooping • 在 VLAN 内启用 IGMP Snooping 或者 VLAN 接口上启用 IGMP 的情况下，端口上的 IGMP Snooping 配置才生效
4	4.6 查看IGMP Snooping组播表项信息	可选

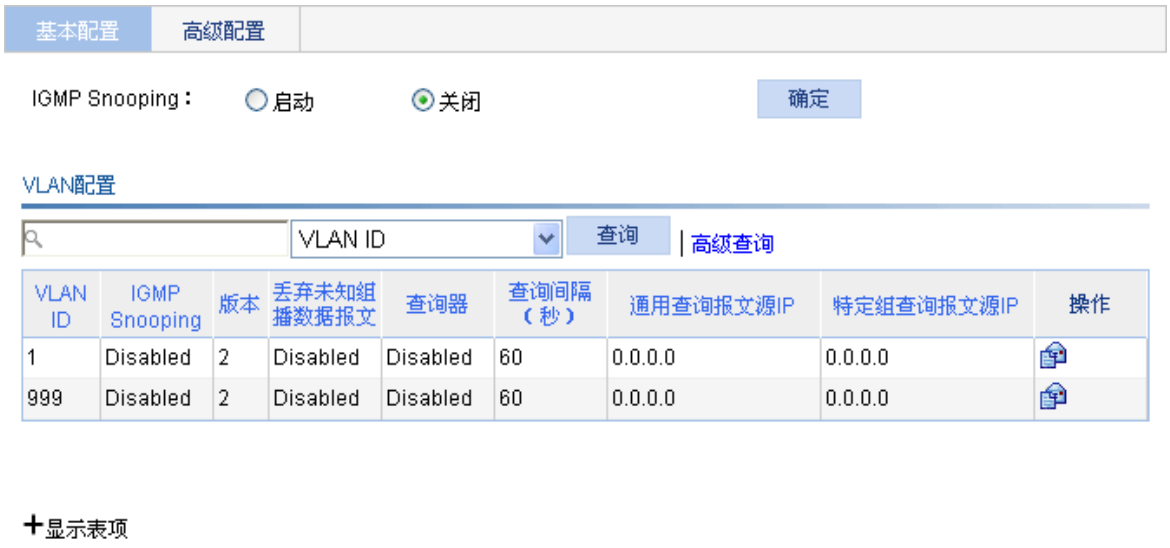
4.3 全局启用IGMP Snooping

(1) 在导航栏中选择“网络 > IGMP Snooping”，默认进入“基本配置”页签的页面，如下图所示。

(2) 选中 IGMP Snooping“启动”前的单选按钮。

(3) 单击<确定>按钮完成操作。

图4-2 基本配置

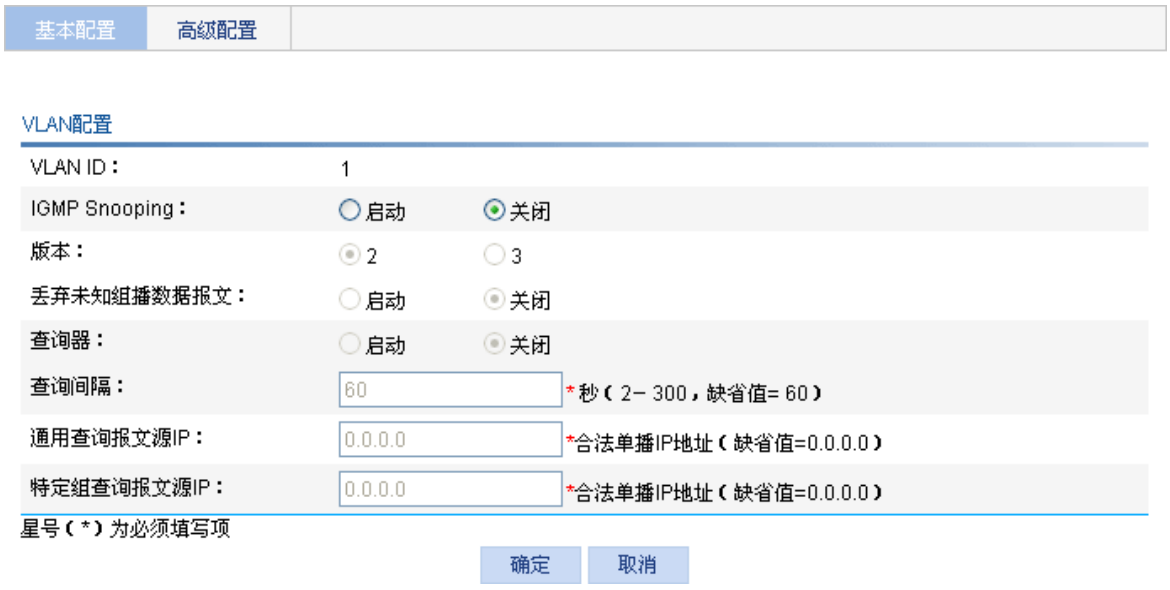


4.4 在VLAN内配置IGMP Snooping

(1) 在导航栏中选择“网络 > IGMP Snooping”，默认进入“基本配置”页签的页面，如上图所示。

(2) 在“VLAN 配置”中单击要配置的 VLAN 对应的图标，进入该 VLAN 的 IGMP Snooping 配置页面，如下图所示。

图4-3 VLAN 配置



(3) 在 VLAN 内配置 IGMP Snooping，详细配置如下表所示。

(4) 单击<确定>按钮完成操作。

表4-2 VLAN 内 IGMP Snooping 的详细配置

配置项	说明
VLAN ID	显示当前要配置的VLAN的ID
IGMP Snooping	设置在该VLAN内启用或关闭IGMP Snooping 只有在此项选择“启动”时，才能进行后面配置项的设置
版本	设置IGMP Snooping的版本，即设置IGMP Snooping可以处理的IGMP报文的版本 • 当 IGMP Snooping 的版本为 2 时，IGMP Snooping 能够对 IGMPv1 和 IGMPv2 的报文进行处理，对 IGMPv3 的报文则不进行处理，而是在 VLAN 内将其广播 • 当 IGMP Snooping 的版本为 3 时，IGMP Snooping 能够对 IGMPv1、IGMPv2 和 IGMPv3 的报文进行处理 提示 当 IGMP Snooping 的版本由版本 3 切换到版本 2 时，系统将清除所有通过动态加入的 IGMP Snooping 转发表项
丢弃未知组播数据报文	设置启用或关闭丢弃未知组播数据报文功能 未知组播数据报文是指在IGMP Snooping转发表中不存在对应转发表项的那些组播数据报文： • 当启用丢弃未知组播数据报文功能时，设备将丢弃所有收到的未知组播数据报文 • 当关闭丢弃未知组播数据报文功能时，设备将在未知组播数据报文所属的 VLAN 内广播该报文
查询器	设置启用或关闭IGMP Snooping查询器功能 在运行了IGMP的组播网络中，会有一台三层组播设备充当IGMP查询器，负责发送IGMP查询报文，使三层组播设备能够在网络层建立并维护组播转发表项，从而在网络层正常转发组播数据。但是，在一个没有三层组播设备的网络中，由于二层设备并不支持IGMP，因此无法实现IGMP查询器的相关功能。为了解决这个问题，可以在二层设备上启用IGMP Snooping查询器，使二层设备能够在数据链路层建立并维护组播转发表项，从而在数据链路层正常转发组播数据
查询间隔	设置发送IGMP普遍组查询报文的时间间隔
通用查询报文源IP	设置IGMP普遍组查询报文的源IP地址
特定组查询报文源IP	设置IGMP特定组查询报文的源IP地址

4.5 在端口上配置IGMP Snooping

(1) 在导航栏中选择“网络 > IGMP Snooping”。

(2) 单击“高级配置”页签，进入如下图所示的页面。

图4-4 高级配置



(3) 在端口上配置 IGMP Snooping，详细配置如下表所示。

(4) 单击<确定>按钮完成操作。

表4-3 IGMP Snooping 高级参数的详细配置

配置项	说明
端口名称	设置要进行IGMP Snooping高级配置的端口 选择一个端口后，页面下方的列表中显示该端口的高级配置信息
VLAN ID	设置在指定VLAN内配置端口快速离开功能或配置允许端口加入的组播组最大数量
最大组播组数	设置允许端口加入的组播组最大数量 通过配置允许端口加入的组播组最大数量，可以限制用户点播组播节目的数量，从而控制了端口上的数据流量 提示 在对允许端口加入的组播组最大数量进行配置时，如果当前端口上的组播组数量已经超过了配置值，系统将把该端口相关的所有转发表项从 IGMP Snooping 转发表中删除，该端口上的主机需要重新加入组播组
端口快速离开	设置在指定端口上启用或关闭快速离开功能 端口快速离开是指当设备从某端口收到主机发送的离开某组播组的IGMP离开组报文时，直接把该端口从对应转发表项的出端口列表中删除。此后，当设备收到对该组播组的IGMP特定组查询报文时，设备将不再向该端口转发 在设备上，在只连接有一个接收者的端口上，可以通过启用端口快速离开功能来节约带宽和资源；而在连接有多个接收者的端口上，如果交换机或该端口所在的VLAN已使能了丢弃未知组播数据报文功能，则不要再启用端口快速离开功能，否则，一个接收者的离开将导致该端口下属于同一组播组的其它接收者无法收到组播数据

4.6 查看IGMP Snooping组播表项信息

(1) 在导航栏中选择“网络 > IGMP Snooping”，默认进入“基本配置”页签的页面，如 图 4-2 所示。

(2) 单击“显示表项”前的扩展按钮，展开如下图所示的内容，可以查看IGMP Snooping组播表项的概要信息，详细说明如 表 4-4 所示。

图4-5 显示表项



(3) 单击要查看的表项对应的图标，进入该IGMP Snooping组播表项详细信息的显示页面，如下图所示，详细说明如 表 4-4 所示。

图4-6 表项详细信息

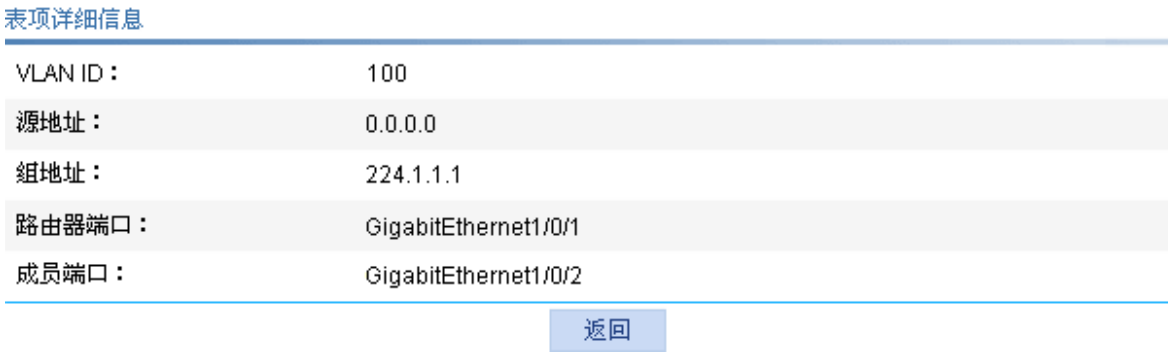


表4-4 IGMP Snooping 组播表项信息的详细说明

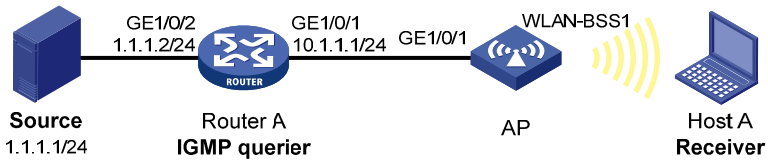
标题项	说明
VLAN ID	组播表项所属VLAN的ID
源地址	组播源地址，0.0.0.0表示所有组播源
组地址	组播组地址
路由器端口	所有路由器端口
成员端口	所有成员端口

4.7 IGMP Snooping典型配置举例

1. 组网需求

- 如下图所示，Router A 通过 GigabitEthernet1/0/2 接口连接组播源（Source），通过 GigabitEthernet1/0/1 接口连接 AP；Router A 上运行 IGMPv2，AP 上运行版本 2 的 IGMP Snooping，并由 Router A 充当 IGMP 查询器。
- 通过配置，使 Host A 能接收发往组播组 224.1.1.1 的组播数据；同时，使 AP 将收到的未知组播数据直接丢弃，避免在其所属的 VLAN 内广播。

图4-7 IGMP Snooping 配置组网图



2. 配置Router A

在 Router A 上启用 IP 组播路由，在各接口上启用 PIM-DM，并在接口 GigabitEthernet1/0/1 上启用 IGMP。具体配置过程略。

3. 配置AP

(1) 全局启用 IGMP Snooping。

步骤 1：在 AP 的导航栏中选择“网络 > IGMP Snooping”，默认进入“基本配置”页签的页面。

步骤 2：如下图所示，选中 IGMP Snooping“启动”前的单选按钮。

步骤 3：单击<确定>按钮完成操作。

图4-8 全局启用 IGMP Snooping



(2) 在 VLAN 1（端口 GigabitEthernet1/0/1 和 WLAN-BSS1 默认属于 VLAN 1）内启用 IGMP Snooping 和丢弃未知组播数据报文功能。

步骤 1：单击 VLAN 1 对应的图标。

步骤 2：进行如下配置，如下图所示。

- 选中 IGMP Snooping“启动”前的单选按钮。
- 选中版本“2”前的单选按钮。
- 选中丢弃未知组播数据报文“启动”前的单选按钮。

步骤 3：单击<确定>按钮完成操作。

图4-9 VLAN 配置



4. 配置结果验证

在 AP 上查看 IGMP Snooping 组播表项的信息。

步骤 1：在 AP 的导航栏中选择“网络 > IGMP Snooping”，默认进入“基本配置”的页面。

步骤 2：单击“显示表项”前的扩展按钮。

步骤 3：查看 IGMP Snooping 组播表项概要信息，如下图所示。

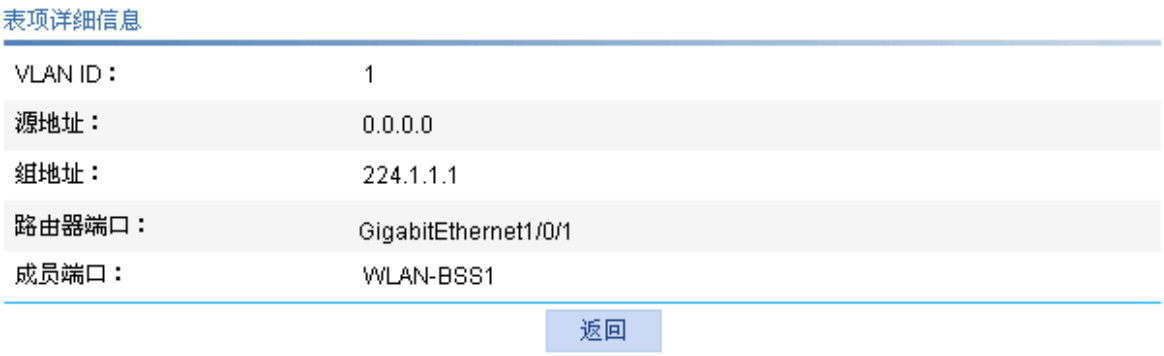
图4-10 配置结果（IGMP Snooping 组播表项概要信息）



步骤 4：单击 VLAN 1 的 IGMP Snooping 组播表项（0.0.0.0，224.1.1.1）对应的图标。

步骤 5：查看该 IGMP Snooping 组播表项的详细信息，如下图所示。

图4-11 配置结果（IGMP Snooping 组播表项详细信息）



由此可见，AP 上的端口 WLAN-BSS1 已经加入了组播组 224.1.1.1。

5 IPv4 和IPv6 路由

说明

本章所指的路由器代表了一般意义下的路由器，以及运行了路由协议的三层交换机。

5.1 概述

在网络中路由器根据所收到的报文的目的地址选择一条合适的路径，并将报文转发到下一个路由器。路径中最后的路由器负责将报文转发给目的主机。路由就是报文在转发过程中的路径信息，用来指导报文转发。

路由表中保存了各种路由协议发现的路由。路由器通过路由表选择路由，把优选路由下发到 FIB（Forwarding Information Base，转发信息库）表中，通过 FIB 指导报文转发。每个路由器中都至少保存着一张路由表和一张 FIB 表。

静态路由是一种特殊的路由，由管理员手工配置。配置静态路由后，去往指定目的地的数据报文将按照管理员指定的路径进行转发。静态路由配置方便，对系统要求低，适用于拓扑结构简单并且稳定的小型网络。其缺点是每当网络拓扑结构发生变化，都需要手工重新配置，不能自动适应。

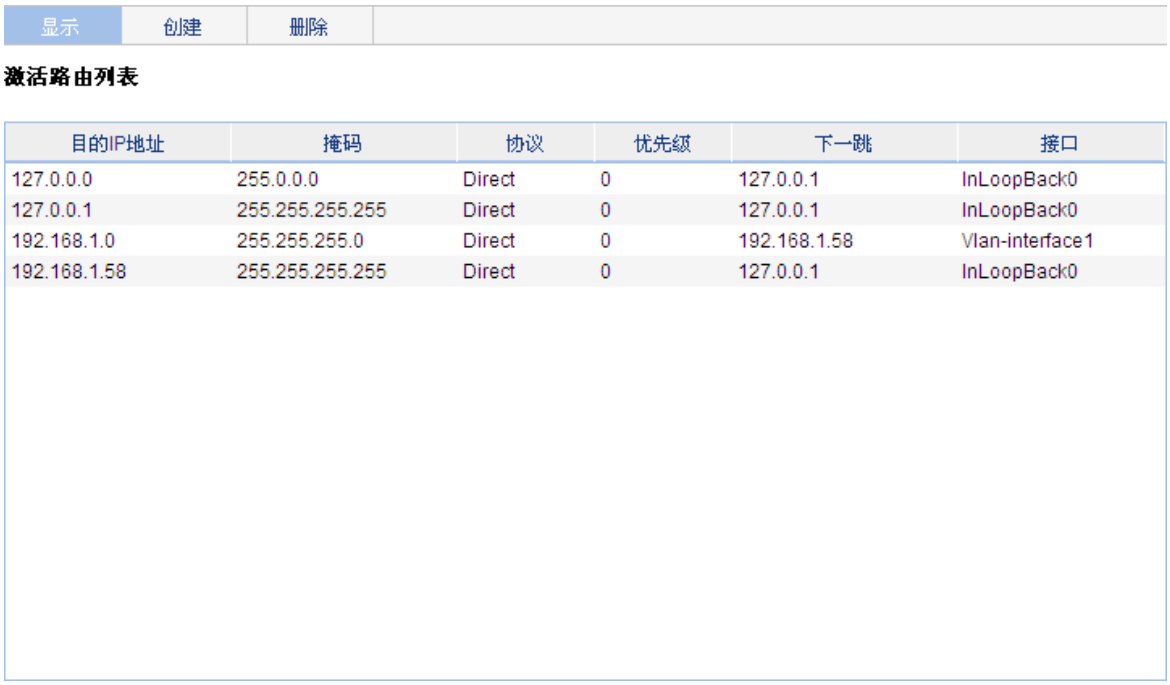
说明

关于路由表和静态路由的详细介绍请参见“三层技术配置指导”中的“IP 路由基础”和“静态路由”。

5.2 查看IPv4激活路由表

(1) 在导航栏中选择“网络 > IPv4 路由”，默认进入“显示”页签的页面，如下图所示。

图5-1 IPv4 路由显示



(2) 查看 IPv4 激活路由表的信息，详细说明如下表所示。

表5-1 IPv4 激活路由表的详细说明

标题项	说明
目的IP地址	IPv4路由的目的IP地址和子网掩码
掩码	
协议	发现该IPv4路由的路由协议
优先级	该IPv4路由的优先级 数值越小，优先级越高
下一跳	该IPv4路由下一跳IP地址
接口	该IPv4路由的出接口，即到该目的网段的数据包将从此接口发出

5.3 新建IPv4静态路由

(1) 在导航栏中选择“网络 > IPv4 路由”。

(2) 单击“创建”页签，进入 IPv4 静态路由配置页面，如下图所示。

图5-2 IPv4 静态路由创建



(3) 配置 IPv4 静态路由的信息，详细配置如下表所示。

(4) 单击<确定>按钮完成操作。

表5-2 IPv4 静态路由的详细配置

配置项	说明
目的IP地址	设置IPv4数据报文的目的主机或目的网段，格式要求为点分十进制
掩码	设置目的主机或目的网段的掩码 可以输入掩码长度或者点分十进制格式的掩码
优先级	设置本条静态路由的优先级，数值越小优先级越高 配置到达相同目的地的多条路由，如果指定相同优先级，则可实现负载分担；如果指定不同优先级，则可实现路由备份
下一跳	设置IPv4数据报文要经过的下一个设备的IP地址，格式要求为点分十进制
接口	设置IPv4数据报文从设备的哪个接口向外转发 可以选择当前设备中的所有三层接口，包括各种虚接口。如果选择NULL0，表示目的IP地址不可达

5.4 查看IPv6激活路由表

(1) 在导航栏中选择“网络 > IPv6 路由”，默认进入“显示”页签的页面，如下图所示。

图5-3 IPv6 路由显示



(2) 查看 IPv6 激活路由表的信息，详细说明如下表所示。

表5-3 IPv6 激活路由表的详细说明

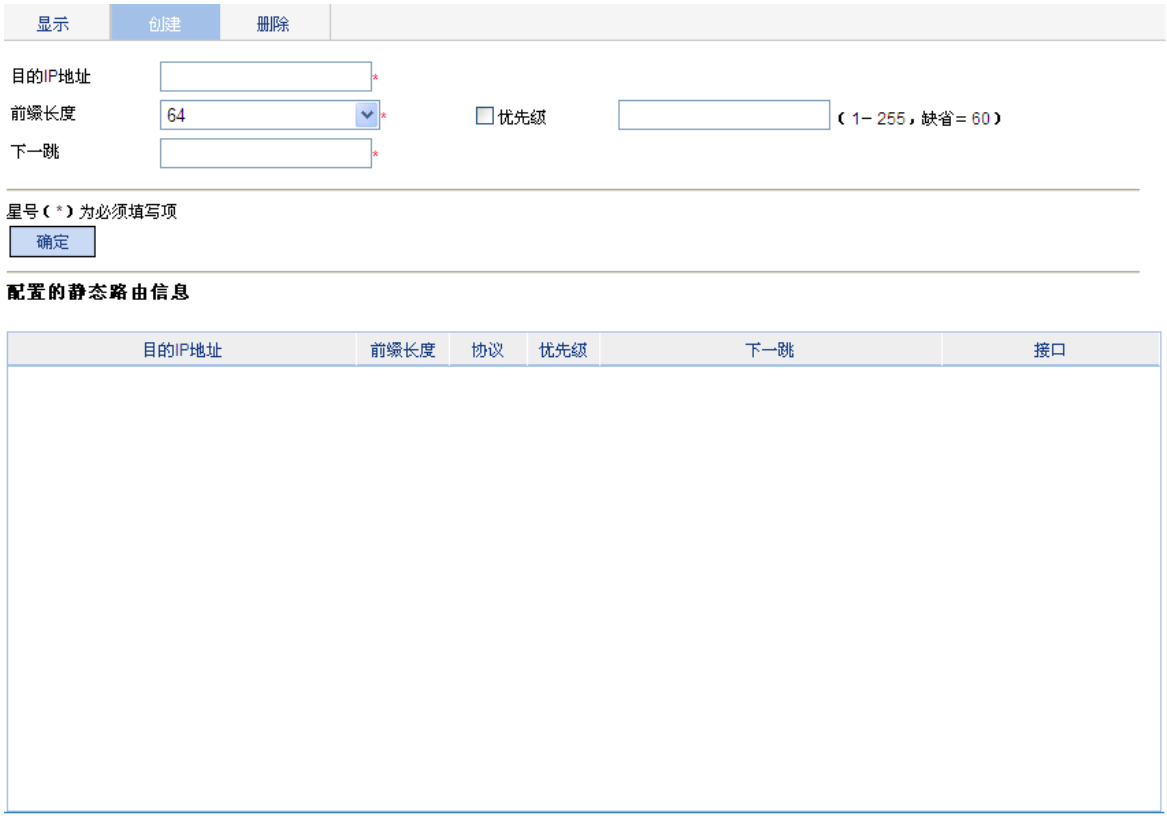
标题项	说明
目的IP地址	IPv6路由的目的IP地址和前缀长度
前缀长度	
协议	发现该IPv6路由的路由协议
优先级	该IPv6路由的优先级 数值越小，优先级越高
下一跳	该IPv6路由下一跳IP地址
接口	该IPv6路由的出接口，即到该目的网段的数据包将从此接口发出

5.5 新建IPv6静态路由

(1) 在导航栏中选择“网络 > IPv6 路由”。

(2) 单击“创建”页签，进入 IPv6 静态路由配置页面，如下图所示。

图5-4 IPv6 静态路由创建



(3) 配置 IPv6 静态路由的信息，详细配置如下表所示。

(4) 单击<确定>按钮完成操作。

表5-4 IPv6 静态路由的详细配置

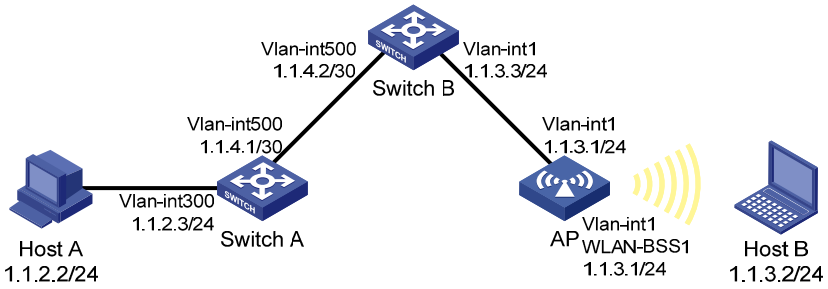
配置项	说明
目的IP地址	设置IPv6数据报文的目的主机或目的网段，格式类似于X:X::X:X 目的IP地址共128bit，每16bit为一段，段之间用“:”分隔，每段都可以用4位十六进制数表示
前缀长度	设置目的主机或目的网段的前缀长度
优先级	设置本条静态路由的优先级，数值越小优先级越高 配置到达相同目的地的多条路由，如果指定相同优先级，则可实现负载分担；如果指定不同优先级，则可实现路由备份
下一跳	设置IPv6数据报文要经过的下一个设备的IP地址，格式要求和目的IP地址相同
接口	设置IPv6数据报文从设备的哪个接口向外转发 可以选择当前设备中的所有三层接口，包括各种虚接口。如果选择NULL0，表示目的IP地址不可达

5.6 IPv4静态路由典型配置举例

1. 组网需求

Switch A、Switch B 和 AP 各接口及主机的 IP 地址和掩码如下图所示。要求 Switch A、Switch B 和 AP 之间配置 IPv4 静态路由后，Host A 和 Host B 之间能够互通。

图5-5 IPv4 静态路由配置组网图



2. 配置思路

采用如下的思路配置 IPv4 静态路由：

(1) 在 Switch A 上配置一条到 Switch B 的缺省路由。

(2) 在 Switch B 上配置一条到 Switch A 的静态路由。

(3) 在 AP 上配置一条到 Switch B 的缺省路由。

3. 配置步骤

(1) 配置 Host A 的网关地址为 1.1.2.3，配置 Host B 的网关地址为 1.1.3.3。

(2) 在 Switch A 上配置一条下一跳为“1.1.4.2”的缺省路由。

(3) 在 Switch B 上配置一条目的地址为“1.1.2.0/24”、下一跳为“1.1.4.1”的静态路由。

(4) 在 AP 上配置缺省路由。

步骤 1：在 AP 的导航栏中选择“网络 > IPv4 路由”。

步骤 2：单击“创建”页签，进入 IPv4 静态路由配置页面。

步骤 3：进行如下配置，如下图所示。

- 输入目的 IP 地址为“0.0.0.0”。
- 输入掩码为“0”。
- 输入下一跳为“1.1.3.3”。

步骤 4：单击<确定>按钮完成操作。

图5-6 配置缺省路由



4. 配置结果验证

(1) 查看激活路由列表。

分别进入 Switch A、Switch B 和 AP 的 IPv4 路由显示页面。查看到页面上的激活路由列表中有新配置的静态路由。

(2) 在 Host A 上使用 **ping** 命令验证 Host B 是否可达(假定主机安装的操作系统为 Windows XP)。

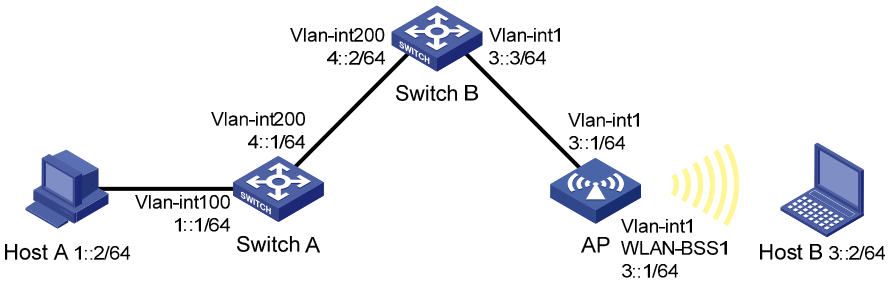
```
C:\Documents and Settings\Administrator>ping 1.1.3.2

Pinging 1.1.3.2 with 32 bytes of data:

Reply from 1.1.3.2: bytes=32 time=1ms TTL=128
Reply from 1.1.3.2: bytes=32 time=1ms TTL=128
Reply from 1.1.3.2: bytes=32 time=1ms TTL=128
Reply from 1.1.3.2: bytes=32 time=1ms TTL=128

Ping statistics for 1.1.3.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

5.7 IPv6静态路由典型配置举例

1. 组网需求

Switch A、Switch B 和 AP 各接口及主机的 IP 地址和掩码如下图所示。要求 Switch A、Switch B 和 AP 之间配置 IPv6 静态路由协议后，Host A 和 Host B 之间能够互通。

图5-7 IPv6 静态路由配置组网图



2. 配置思路

采用如下的思路配置 IPv6 静态路由：

(1) 在 Switch A 上配置一条到 Switch B 的缺省路由。

(2) 在 Switch B 上配置一条到 Switch A 的静态路由。

(3) 在 AP 上配置一条到 Switch B 的缺省路由。

3. 配置步骤

(1) 配置 Host A 的网关地址为 1::1，配置 Host B 的网关地址为 3::1。

(2) 在 Switch A 上配置一条下一跳为“4::2”的缺省路由。

(3) 在 Switch B 上配置一条目的地址为“1::/64”、下一跳为“4::1”的静态路由。

(4) 在 AP 上配置缺省路由。

步骤 1：在 AP 的导航栏中选择“网络 > IPv6 路由”。

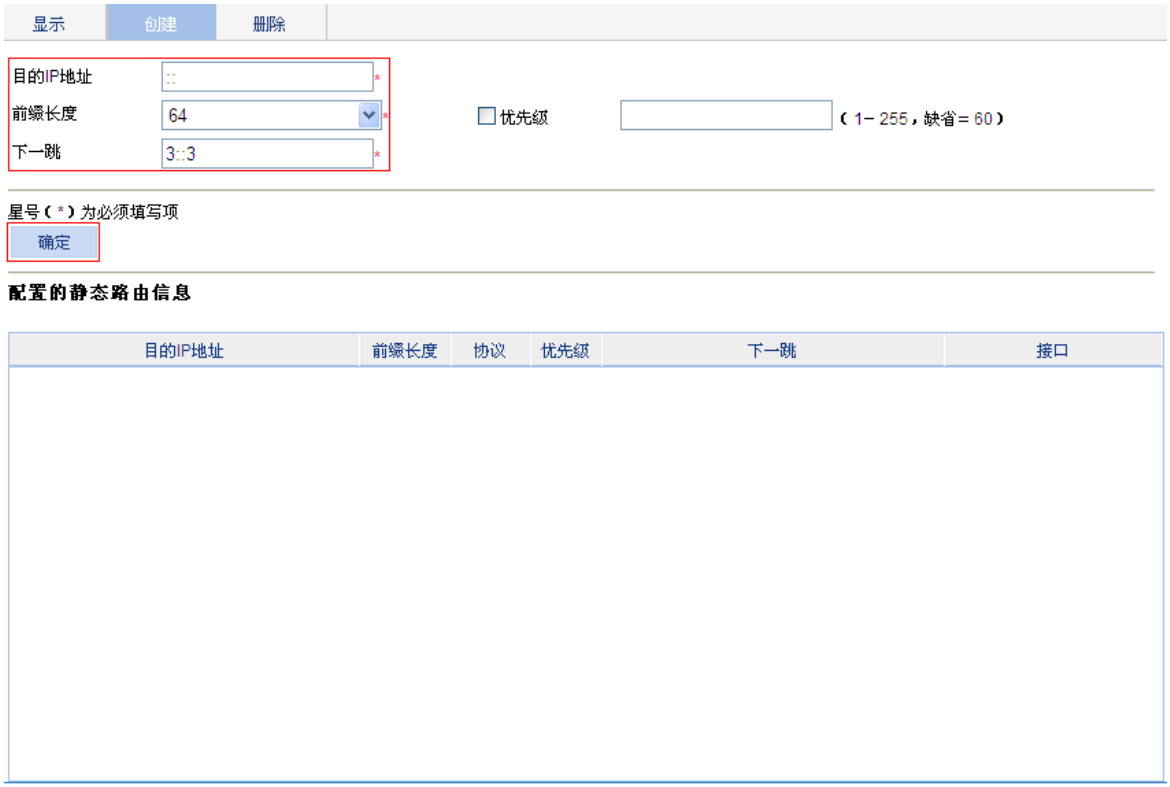
步骤 2：单击“创建”页签，进入 IPv6 静态路由配置页面。

步骤 3：进行如下配置，如下图所示。

- 输入目的 IP 地址为“::”。
- 选择前缀长度为“0”。
- 输入下一跳为“3::3”。

步骤 4：单击<确定>按钮完成操作。

图5-8 配置缺省路由



4. 配置结果验证

(1) 查看激活路由列表。

分别进入 Switch A、Switch B 和 AP 的 IPv6 路由显示页面。查看到页面上的激活路由列表中有新配置的静态路由。

(2) 在 Switch A 上使用 **ping** 命令验证 Host B 是否可达。

```
<SwitchA> system-view
[SwitchA] ping ipv6 3::2
  PING 3::2 : 56  data bytes, press CTRL_C to break
    Reply from 3::2
    bytes=56 Sequence=1 hop limit=254  time = 63 ms
    Reply from 3::2
    bytes=56 Sequence=2 hop limit=254  time = 62 ms
    Reply from 3::2
    bytes=56 Sequence=3 hop limit=254  time = 62 ms
    Reply from 3::2
    bytes=56 Sequence=4 hop limit=254  time = 63 ms
    Reply from 3::2
    bytes=56 Sequence=5 hop limit=254  time = 63 ms

  --- 3::2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
```

```
round-trip min/avg/max = 62/62/63 ms
```

5.8 注意事项

配置静态路由时需要注意如下事项：

(1) 如果在配置静态路由时没有指定优先级，就会使用缺省优先级。重新设置缺省优先级后，新设置的缺省优先级仅对新增的静态路由有效。Web 界面目前不支持对缺省优先级的配置。

(2) 在配置静态路由时，如果先指定下一跳，然后再将该下一跳的地址配置为本地接口（如以太网接口、VLAN 接口等）的 IP 地址，则该条静态路由不会生效。

(3) 在指定出接口时要注意：

- 对于 NULL0 和 Loopback 接口，配置了出接口就不再配置下一跳。
- 对于点到点接口，即使不知道对端地址，也可以在路由器配置时指定出接口。这样，即使对端地址发生了改变也无须改变该路由器的配置。如封装 PPP 协议的接口，通过 PPP 协商获取对端的 IP 地址，这时可以不指定下一跳，只需指定出接口即可。

6 DHCP

说明

- 指定设备的接口作为 DHCP 客户端后，可以使用 DHCP 协议从 DHCP 服务器动态获得 IP 地址等参数，方便用户配置，也便于集中管理。配置 DHCP 客户端即配置接口通过 DHCP 协议自动获取 IP 地址，详细配置请参见“设备”模块中的“接口管理”，本章不对 DHCP 客户端的配置进行介绍。
- 关于 DHCP 协议的详细介绍请参见“三层技术配置指导”中的“DHCP”。

6.1 概述

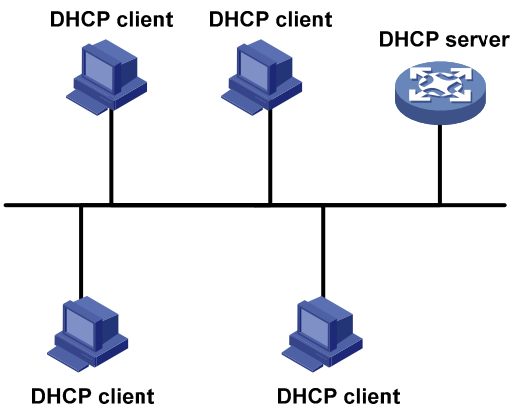
6.1.1 DHCP简介

DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）用来为网络设备动态地分配 IP 地址等网络配置参数。

DHCP 采用客户端/服务器通信模式，由客户端向服务器提出配置申请，服务器返回为客户端分配的 IP 地址等相应的配置信息，以实现 IP 地址等信息的动态配置。

在 DHCP 的典型应用中，一般包含一台 DHCP 服务器和多台客户端（如 PC 和便携机），如下图所示。

图6-1 DHCP 典型应用



6.2 配置DHCP服务器

6.2.1 DHCP服务器配置任务简介

表6-1 DHCP 服务器配置步骤

步骤	配置任务	说明
1	6.2.2 启动DHCP服务	必选 启动全局DHCP服务 缺省情况下，全局DHCP服务处于关闭状态
2	6.2.3 配置DHCP服务器的静态地址池 6.2.4 配置DHCP服务器的动态地址池	二者至少选其一 提示 DHCP 服务器和客户端在同一个子网内，直接进行 DHCP 报文交互时，DHCP 服务器上配置的地址池需要与 DHCP 服务器接口 IP 地址的网段一致，否则会导致 DHCP 客户端无法获得正确的 IP 地址
3	6.2.5 配置接口工作在DHCP服务器模式	可选 配置接口工作在DHCP服务器模式后，当接口收到DHCP客户端发来的DHCP报文时，将从DHCP服务器的地址池中分配地址 缺省情况下，接口工作在DHCP服务器模式 提示 DHCP 服务器只在 IP 地址为手工配置的接口上起作用
4	6.2.6 查看地址池中已被分配的地址信息	可选

6.2.2 启动DHCP服务

(1) 在导航栏中选择“网络 > DHCP”，默认进入“DHCP 服务器”页签的页面，如下图所示。

(2) 在页面最上方选中 DHCP 服务“启动”前的单选按钮，即可启动全局 DHCP 服务。

图6-2 DHCP 服务器



6.2.3 配置DHCP服务器的静态地址池

(1) 在导航栏中选择“网络 > DHCP”，默认进入“DHCP服务器”页签的页面，如 图 6-2 所示。

(2) 在“地址池”中选中“静态”前的单选按钮，显示的是所有静态地址池。

(3) 单击<新建>按钮，进入新建静态地址池的配置页面，如下图所示。

图6-3 静态地址池创建



(4) 配置静态地址池的信息，详细配置如下表所示。

(5) 单击<确定>按钮完成操作。

表6-2 静态地址池的详细配置

配置项	说明
地址池名称	设置静态地址池的名称
IP地址	设置静态绑定的IP地址和子网掩码 静态绑定的IP地址不能是DHCP服务器的接口IP地址，否则会导致IP地址冲突，被绑定的客户端将无法正常获取到IP地址 输入的掩码可以是掩码长度或点分十进制格式的掩码
掩码	
客户端MAC地址	设置地址池中静态绑定的客户端MAC地址或客户端ID，二选一 提示 静态绑定的客户端ID要与待绑定客户端的ID一致，否则客户端无法成功获取IP地址
客户端ID	
客户端域名	设置DHCP地址池为DHCP客户端分配的域名后缀 为地址池指定客户端使用的域名后，在给客户端分配IP地址的同时，也将域名发送给客户端
网关地址	设置DHCP地址池为DHCP客户端分配的网关IP地址 DHCP客户端访问本网段以外的服务器或主机时，数据必须通过网关进行转发。为地址池指定网关地址后，在给客户端分配IP地址的同时，也将网关地址发送给客户端 最多可以配置8个网关地址，多个地址间用“,”隔开
DNS服务器地址	设置DHCP地址池为DHCP客户端分配的DNS服务器IP地址 为了使DHCP客户端能够通过域名访问Internet上的主机，DHCP服务器应在为客户端分配IP地址的同时指定DNS服务器地址 最多可以配置8个DNS服务器地址，多个地址间用“,”隔开

配置项	说明
WINS服务器地址	设置DHCP地址池为DHCP客户端分配的WINS服务器IP地址 为DHCP客户端分配的WINS服务器地址，如果选择节点类型是b类节点，则WINS服务器地址可以不配 最多可以配置8个WINS服务器地址，多个地址间用“,”隔开
NetBIOS节点类型	设置DHCP地址池为DHCP客户端分配的NetBIOS节点类型

6.2.4 配置DHCP服务器的动态地址池

(1) 在导航栏中选择“网络 > DHCP”，默认进入“DHCP服务器”页签的页面，如 图 6-2 所示。

(2) 在“地址池”中选中“动态”前的单选按钮，显示的是所有动态地址池。

(3) 单击<新建>按钮，进入新建动态地址池的配置页面，如下图所示。

图6-4 动态地址池创建



(4) 配置动态地址池的信息，详细配置如下表所示。

(5) 单击<确定>按钮完成操作。

表6-3 动态地址池的详细配置

配置项		说明
地址池名称		设置动态地址池的名称
IP地址		设置动态分配的IP地址范围，为一个IP网段
掩码		DHCP服务器在分配地址时，需要排除已经被占用的IP地址（如网关、FTP服务器等）。否则，同一地址分配给两个客户端会造成IP地址冲突 输入的掩码可以是掩码长度或点分十进制格式的掩码
租用	不限制	设置DHCP地址池中动态分配的IP地址的租用有效期限

配置项		说明
期限	天/小时/分/秒	选择“不限制”，表示不限制IP地址的租用期限
客户端域名		设置DHCP地址池为DHCP客户端分配的域名后缀 为地址池指定客户端使用的域名后，在给客户端分配IP地址的同时，也将域名发送给客户端
网关地址		设置DHCP地址池为DHCP客户端分配的网关IP地址 DHCP客户端访问本网段以外的服务器或主机时，数据必须通过网关进行转发。为地址池指定网关地址后，在给客户端分配IP地址的同时，也将网关地址发送给客户端 最多可以配置8个网关地址，多个地址间用“,”隔开
DNS服务器地址		设置DHCP地址池为DHCP客户端分配的DNS服务器IP地址 为了使DHCP客户端能够通过域名访问Internet上的主机，DHCP服务器应在为客户端分配IP地址的同时指定DNS服务器地址 最多可以配置8个DNS服务器地址，多个地址间用“,”隔开
WINS服务器地址		设置DHCP地址池为DHCP客户端分配的WINS服务器IP地址 为DHCP客户端分配的WINS服务器地址，如果选择节点类型是b类节点，则可以不配置WINS服务器地址 最多可以配置8个WINS服务器地址，多个地址间用“,”隔开
NetBIOS节点类型		设置DHCP地址池为DHCP客户端分配的NetBIOS节点类型

6.2.5 配置接口工作在DHCP服务器模式

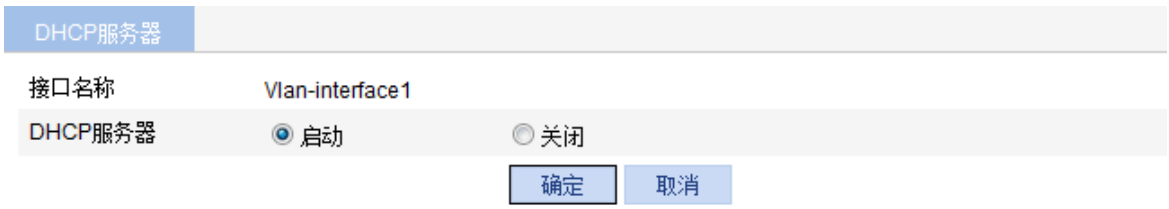
(1) 在导航栏中选择“网络 > DHCP”，默认进入“DHCP服务器”页签的页面，如 图 6-2 所示。

(2) 在“接口设置”中单击某接口对应的 图标，进入该接口 DHCP 服务器功能的配置页面，如下图所示。

(3) 选中 DHCP 服务器“启动”前的单选按钮。

(4) 单击<确定>按钮完成操作。

图6-5 DHCP 服务器接口设置



6.2.6 查看地址池中已被分配的地址信息

(1) 在导航栏中选择“网络 > DHCP”，默认进入“DHCP服务器”页签的页面，如 图 6-2 所示。

(2) 在“在用地址”中查看地址池中已被分配的 IP 地址信息，详细说明如下表所示。

表6-4 已被分配的地址信息的详细说明

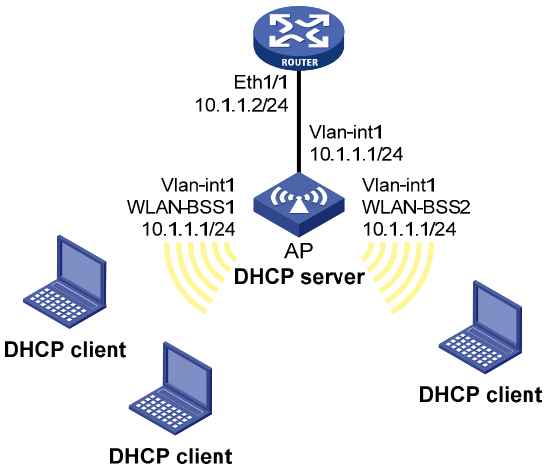
标题项	说明
IP地址	已被分配的IP地址
客户端MAC地址/客户端ID	该IP地址绑定的DHCP客户端MAC地址或客户端ID
地址池名称	分配该IP地址的DHCP地址池名称
租约到期时间	该IP地址的租约到期时间

6.3 DHCP服务器典型配置举例

1. 组网需求

- 配置 AP 作为 DHCP 服务器为网段 10.1.1.0/24 中的客户端动态分配 IP 地址，AP 上 Vlan-interface1 的 IP 地址为 10.1.1.1/24。
- 10.1.1.0/24 网段内的地址租用期限为 10 天 12 小时，网关的地址为 10.1.1.2。

图6-6 DHCP 服务器配置组网图



2. 配置步骤

(1) 启动 DHCP 服务。

步骤 1：在导航栏中选择“网络 > DHCP”，默认进入“DHCP 服务器”页签的页面。

步骤 2：如下图所示，选中 DHCP 服务“启动”前的单选按钮完成操作。

图6-7 启动 DHCP 服务



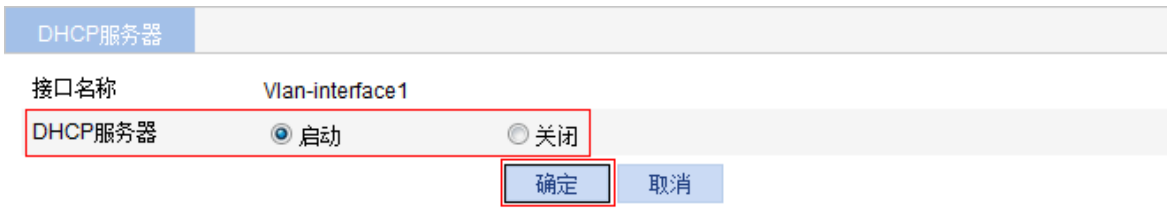
(2) 配置 Vlan-interface1 工作在 DHCP 服务器模式。（缺省情况下接口工作在 DHCP 服务器模式，此步骤可以省略）

步骤 1：在“接口设置”中单击 Vlan-interface1 对应的 图标。

步骤 2：如下图所示，选中 DHCP 服务器“启动”前的单选按钮。

步骤 3：单击<确定>按钮完成操作。

图6-8 配置 Vlan-interface1 工作在 DHCP 服务器模式



(3) 配置 DHCP 服务器的动态地址池。

步骤 1：在“地址池”中默认选中的是“动态”前的单选按钮，单击<新建>按钮。

步骤 2：进行如下配置，如下图所示。

- 输入地址池名称为“test”。
- 输入 IP 地址为“10.1.1.0”。
- 输入掩码为“255.255.255.0”。
- 输入租用期限为“10”天“12”小时“0”分“0”秒。
- 输入网关地址为“10.1.1.2”。

步骤 3：单击<确定>按钮完成操作。

图6-9 置 DHCP 服务器的动态地址池



7 DNS

7.1 概述

域名系统（DNS，Domain Name System）是一种用于 TCP/IP 应用程序的分布式数据库，提供域名与 IP 地址之间的转换。通过域名系统，用户进行某些应用时，可以直接使用便于记忆的、有意义的域名，而由网络中的域名解析服务器将域名解析为正确的 IP 地址。

域名解析分为静态域名解析和动态域名解析，二者可以配合使用。在解析域名时，首先采用静态域名解析（查找静态域名解析表），如果静态域名解析不成功，再采用动态域名解析。由于动态域名解析可能会花费一定的时间，且需要域名服务器的配合，因而可以将一些常用的域名放入静态域名解析表中，这样可以大大提高域名解析效率。

1. 静态域名解析

静态域名解析就是手工建立域名和 IP 地址之间的对应关系。当用户使用域名进行某些应用（如 Telnet 应用）时，系统查找静态域名解析表，从中获取指定域名对应的 IP 地址。

2. 动态域名解析

动态域名解析是通过域名服务器进行动态域名解析。



说明

关于 DNS 的详细介绍请参见“三层技术配置指导”中的“域名解析”。

7.2 DNS配置任务简介

1. 配置静态域名解析表

表7-1 静态域名解析表的配置步骤

步骤	配置任务	说明
1	7.3 配置静态域名解析表	必选 缺省情况下，静态域名解析表中没有主机名及其IP地址的对应关系

2. 配置动态域名解析

表7-2 动态域名解析配置步骤

步骤	配置任务	说明
1	7.4 启动动态域名解析	必选 缺省情况下，动态域名解析功能处于关闭状态
2	7.5 配置DNS服务器的IP地址	必选 缺省情况下，没有配置DNS服务器的IP地址

步骤	配置任务	说明
3	7.6 配置域名后缀	可选 缺省情况下，没有配置域名后缀
4	7.7 清空动态域名缓存区	可选

7.3 配置静态域名解析表

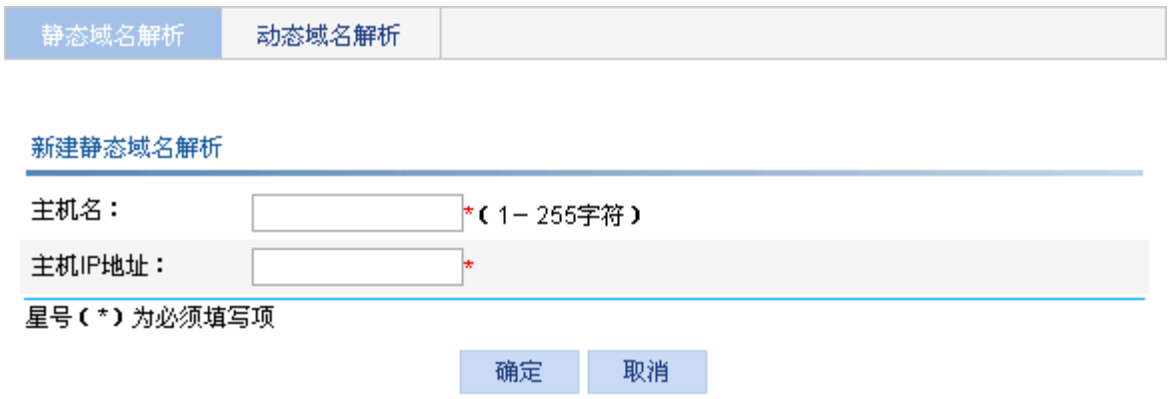
(1) 在导航栏中选择“网络> DNS”，默认进入“静态域名解析”页签的页面，如下图所示。

图7-1 静态域名解析



(2) 单击<新建>按钮，进入新建静态域名解析表项的配置页面，如下图所示。

图7-2 新建静态域名解析



(3) 配置静态域名解析表的信息，详细配置如下表所示。

(4) 单击<确定>按钮完成操作。

表7-3 静态域名解析表的详细配置信息

配置项	说明
主机名	设置静态域名解析表中主机名和主机IP地址的对应关系 每个主机名只能对应一个IP地址，当对同一主机名进行多次配置时，最后配置的IP地址有效
主机IP地址	

7.4 启动动态域名解析

(1) 在导航栏中选择“网络 > DNS”。

(2) 单击“动态域名解析”页签，进入如下图所示的页面。

(3) 选中动态域名解析“启动”前的单选按钮。

(4) 单击<确定>按钮完成操作。

图7-3 动态域名解析



7.5 配置DNS服务器的IP地址

(1) 在导航栏中选择“网络 > DNS”。

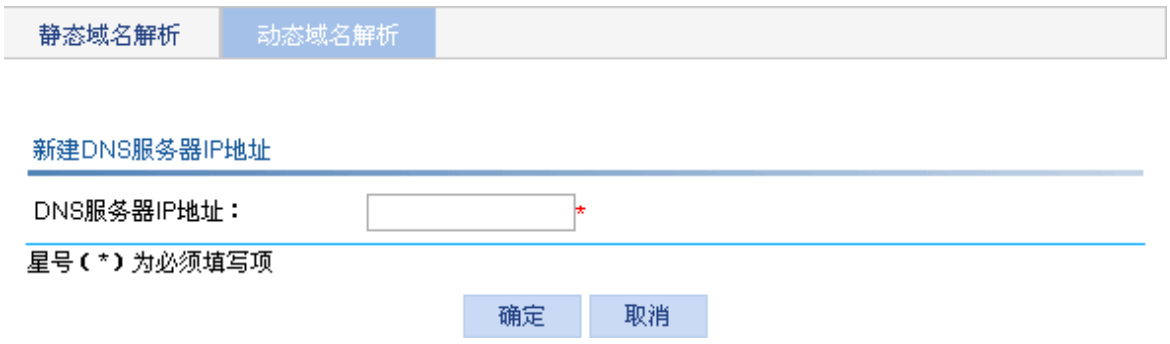
(2) 单击“动态域名解析”页签，进入如 图 7-3 所示的页面。

(3) 单击<添加 IP 地址>按钮，进入新建 DNS 服务器 IP 地址的页面，如下图所示。

(4) 在文本框中输入 DNS 服务器的 IP 地址。

(5) 单击<确定>按钮完成操作。

图7-4 新建 DNS 服务器 IP 地址



7.6 配置域名后缀

(1) 在导航栏中选择“网络 > DNS”。

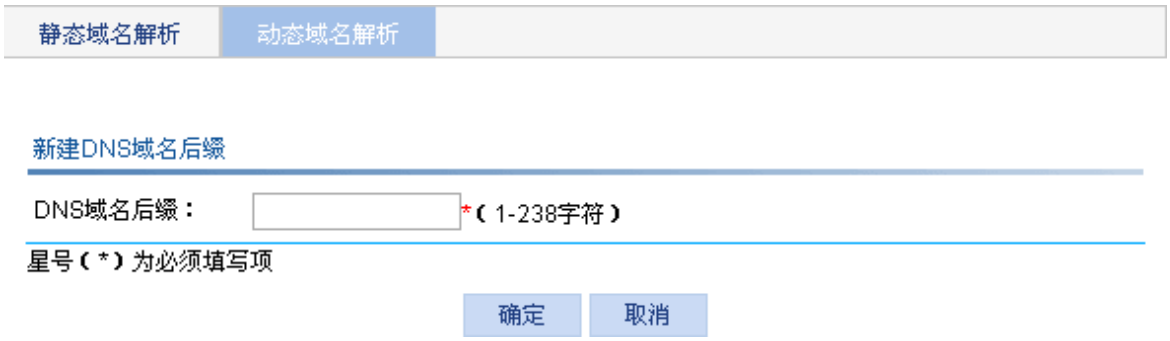
(2) 单击“动态域名解析”页签，进入如 图 7-3 所示的页面。

(3) 单击<添加域名后缀>按钮，进入新建 DNS 域名后缀的页面，如下图所示。

(4) 在文本框中输入 DNS 域名后缀。

(5) 单击<确定>按钮完成操作。

图7-5 新建 DNS 域名后缀



7.7 清空动态域名缓存区

(1) 在导航栏中选择“网络 > DNS”。

(2) 单击“动态域名解析”页签，进入如 图 7-3 所示的页面。

(3) 选中“清空动态域名缓存区”前的复选框。

(4) 单击<确定>按钮完成操作。

7.8 DNS典型配置举例

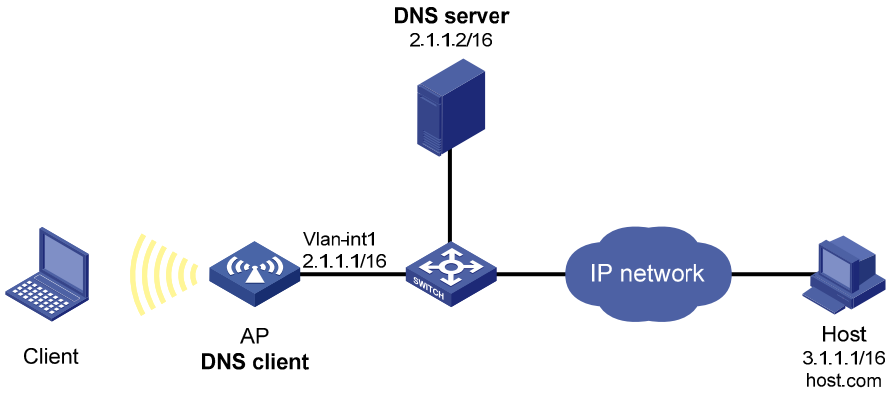
1. 组网需求

为了避免记忆复杂的 IP 地址，AP 希望通过便于记忆的域名访问某一主机。如果网络中存在 DNS 服务器，则可以利用动态域名解析功能，实现通过域名访问主机。

在本例中：

- DNS 服务器的 IP 地址是 2.1.1.2/16，DNS 服务器上存在 com 域，且 com 域中包含域名“host”和 IP 地址 3.1.1.1/16 的对应关系。
- AP 作为 DNS 客户端，使用动态域名解析功能，将域名解析为 IP 地址。
- AP 上配置域名后缀 com，以便简化访问主机时输入的域名，例如通过输入 host 即可访问域名为 host.com、IP 地址为 3.1.1.1/16 的主机 Host。

图7-6 DNS 配置组网图



说明

- 在开始下面的配置之前，假设 AP 与 Host 之间的路由可达，AP 和 Host 都已经配置完毕，接口 IP 地址如上图所示。
- 不同 DNS 服务器的配置方法不同，下面仅以 Windows Server 2000 为例，说明 DNS 服务器的配置方法。

2. 配置DNS服务器

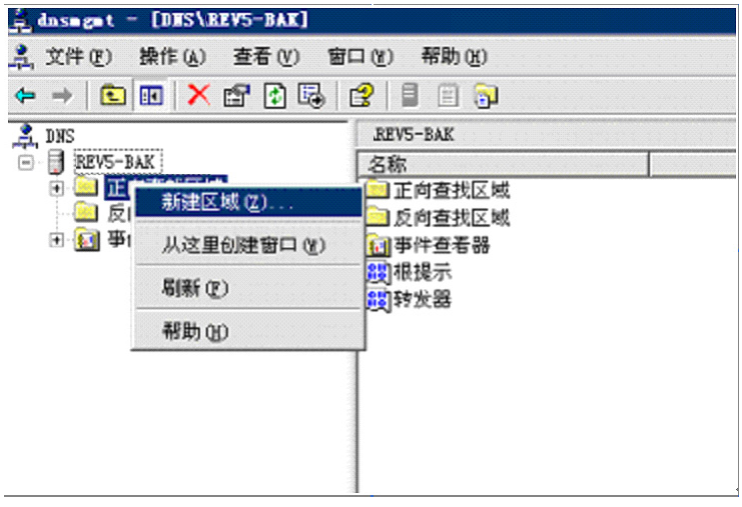
(1) 创建区域 com。

步骤 1：在开始菜单中，选择“程序 > 管理工具 > DNS”，进入域名服务器配置界面。

步骤 2：如下图所示，右键点击“正向查找区域”，选择“新建区域”。

步骤 3：按照提示创建新的区域 com。

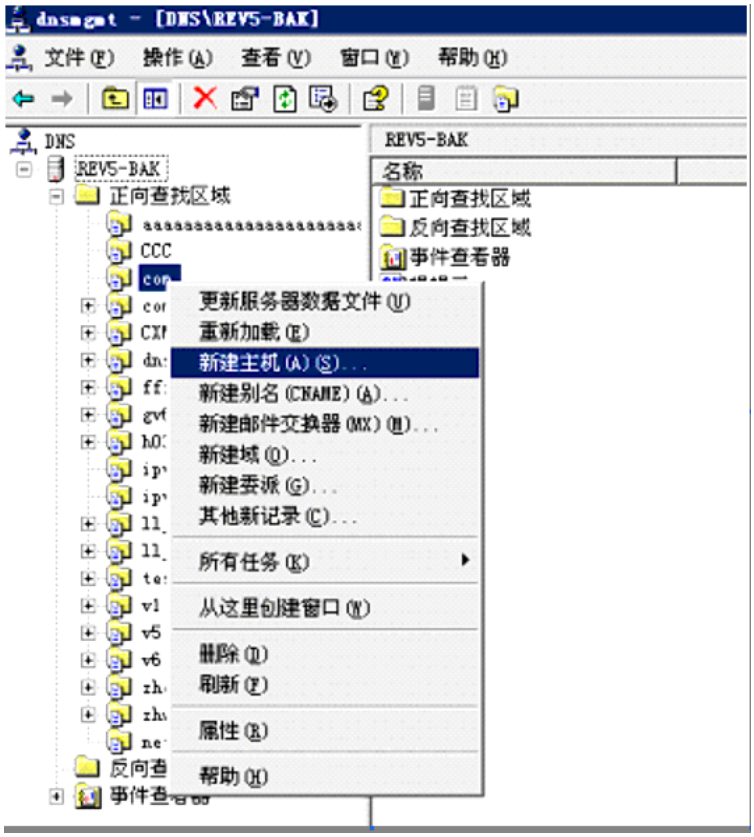
图7-7 创建区域



(2) 添加域名和 IP 地址的映射。

步骤 1：如下图所示，右键点击区域 com，选择“新建主机”，弹出新建主机的对话框。

图7-8 新建主机



步骤 2：如下图所示，在新建主机的对话框中输入名称 host 和 IP 地址 3.1.1.1。

步骤 3：单击<添加主机>按钮完成操作。

图7-9 添加域名和 IP 地址的映射



3. 配置AP

(1)　启动动态域名解析功能。

步骤 1：在导航栏中选择“网络 > DNS”。

步骤 2：单击“动态域名解析”页签。

步骤 3：如下图所示，选中动态域名解析“启动”前的单选按钮。

步骤 4：单击<确定>按钮完成操作。

图7-10 使能动态域名解析功能



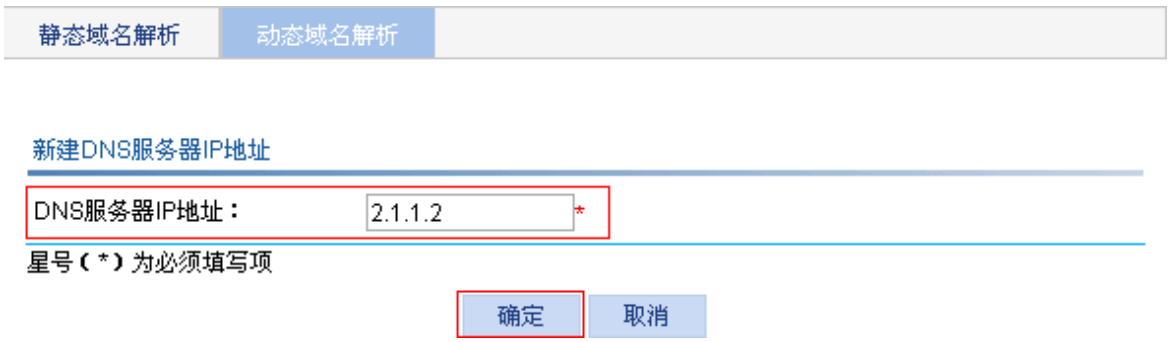
(2)　配置 DNS 服务器 IP 地址。

步骤 1：单击<添加 IP 地址>按钮，进入新建 DNS 服务器 IP 地址的页面。

步骤 2：如下图所示，输入 DNS 服务器 IP 地址为“2.1.1.2”。

步骤 3：单击<确定>按钮完成操作。

图7-11 新建 DNS 服务器 IP 地址



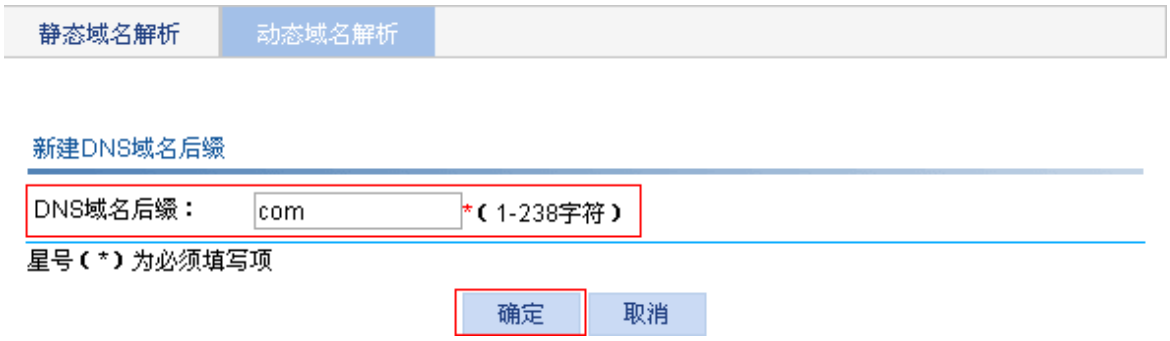
(3)　配置域名后缀。

步骤 1：单击<添加域名后缀>按钮，进入新建 DNS 域名后缀的页面。

步骤 2：如下图所示，输入 DNS 域名后缀为“com”。

步骤 3：单击<确定>按钮完成操作。

图7-12 新建 DNS 域名后缀



4. 配置结果验证

在 AP 上执行 Ping 主机名 host 的操作，可以 ping 通，且对应的目的地址为 3.1.1.1。

步骤 1：在导航栏中选择“网络 > 诊断工具”，进入“IPv4 Ping”页签的页面。

步骤 2：输入目的主机名为“host”。

步骤 3：单击<开始>按钮执行 Ping 操作。

步骤 4：查看到如下图所示的 Ping 操作结果。

图7-13 Ping 操作结果



8 PPPoE

8.1 概述

PPPoE 是 Point-to-Point Protocol over Ethernet 的简称。PPPoE 协议采用 Client/Server 方式，它将 PPP 报文封装在以太网帧之内，在以太网上提供点对点的连接。

AP 设备上运行了 PPPoE Client 功能后，可以通过一个远端接入设备连入因特网，并可以实现对接入的每个 AP 设备进行控制、计费等。

PPPoE 有两个阶段：Discovery 阶段和 PPP Session 阶段，具体如下：

- Discovery 阶段

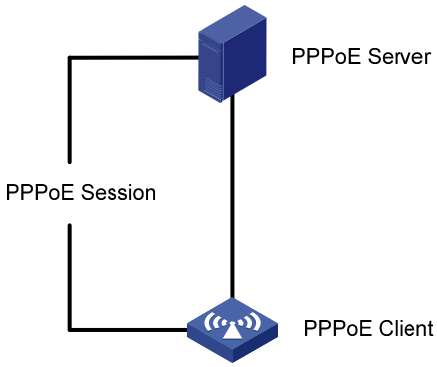
当一个客户端想开始 PPPoE 进程的时候，它必须先识别接入端的以太网 MAC 地址，建立 PPPoE 的 SESSION ID。这就是 Discovery 阶段的目的。

- PPP Session 阶段

当 PPPoE 进入 Session 阶段后 PPP 报文就可以作为 PPPoE 帧的净荷封装在以太网帧发到对端，SESSION ID 必须是 Discovery 阶段确定的 ID，MAC 地址必须是对端的 MAC 地址，PPP 报文从 Protocol ID 开始。在 Session 阶段，客户端或服务器任何一方都可发 PADT（PPPoE Active Discovery Terminate，PPPoE 活动发现终止）报文通知对方结束本 Session。

关于 PPPoE 的详细介绍，可以参考 RFC2516。

图8-1 PPPoE 组网图



8.2 配置PPPoE Client

(1) 在导航栏中选择“网络 > PPPoE”，默认进入“Client 信息”页签的页面，如下图所示。

图8-2 Client 信息



(2) 单击<新建>按钮，进入新建 PPPoE Client 页面，如下图所示。

图8-3 新建 PPPoE Client



(3) 配置 PPPoE Client 的信息，详细配置如下表所示。

(4) 单击<确定>按钮完成操作。

表8-1 新建 PPPoE Client 的详细配置

配置项	说明
Dialer接口	设置Dialer接口号
用户名	设置PPPoE Client认证使用的用户名和密码 用户名和密码必须同时配置或者同时不配置
密码	
IP配置	设置接口配置或获取IP地址的方式 • 无 IP 配置：不配置 IP 地址 • 静态地址：静态配置接口的 IP 地址和掩码 • PPP 协商：通过 PPP 协商获得 IP 地址 • 借用地址：借用同一设备上其他接口的 IP 地址

配置项	说明
IP地址	设置接口的IP地址和掩码 当IP配置选择“静态地址”时，需配置此两项
网络掩码	
其他接口	设置被借用IP地址的接口 当IP配置选择“借用地址”时，需配置此项
绑定接口	设置PPPoE Client绑定的接口
连接方式	设置PPPoE Client的连接方式为永久在线方式或非永久在线方式 • 永久在线方式是指，当物理线路 up 后，设备会立即发起 PPPoE 呼叫，建立 PPPoE 会话。除非用户删除 PPPoE 会话，否则此 PPPoE 会话将一直存在 • 非永久在线方式是指，当物理线路 up 后，设备不立即发起 PPPoE 呼叫，只有当有数据需要传送时，设备才会发起 PPPoE 呼叫，建立 PPPoE 会话。如果 PPPoE 链路的空闲时间超过用户指定的超时时间，设备会自动中止此 PPPoE 会话。选择此方式时需配置超时时间
超时时间	设置PPPoE链路的空闲超时时间 当连接方式选择“非永久在线”时，需配置此项

8.3 查看PPPoE Client会话统计信息

(1) 在导航栏中选择“网络 > PPPoE”。

(2) 单击“会话信息”页签。

(3) 选择会话信息查看类型为“统计信息”，页面如下图所示。

(4) 查看 PPPoE Client 会话统计信息，详细说明如下表所示。

图8-4 会话统计信息



表8-2 PPPoE Client 会话统计信息的详细说明

标题项	说明
接口	PPPoE会话所属的以太网接口 PPPoE Client绑定的是VLAN接口时，此处显示空
会话编号	Session ID，PPPoE会话的编号
接收报文数	PPPoE Client会话的接收报文数
接收字节数	PPPoE Client会话的接收字节数
丢弃报文数（接收）	PPPoE Client会话的丢弃报文数（接收方向）
发送报文数	PPPoE Client会话的发送报文数
发送字节数	PPPoE Client会话的发送字节数
丢弃报文数（发送）	PPPoE Client会话的丢弃报文数（发送方向）

8.4 查看PPPoE Client会话概要信息

(1) 在导航栏中选择“网络 > PPPoE”。

(2) 单击“会话信息”页签，进入会话信息查看页面。

(3) 选择会话信息查看类型为“概要信息”。

(4) 查看 PPPoE Client 会话概要信息，详细说明如下表所示。

图8-5 会话概要信息



表8-3 PPPoE Client 会话概要信息的详细说明

标题项	说明
会话编号	Session ID，PPPoE会话的编号
Dialer接口号	PPPoE会话所对应的Dialer接口号
接口	PPPoE会话所属的以太网接口 PPPoE Client绑定的是VLAN接口时，此处显示空

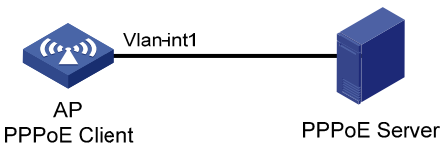
标题项	说明
Client-MAC	PPPoE Client的MAC地址
Server-MAC	PPPoE Server的MAC地址
状态	PPPoE会话所处的状态 • IDLE：没有进行 PPPoE Client 协商 • PADI：发送 PADI 报文，等待 PADO 应答 • PADR：发送 PADR 报文，等待 PADS 应答 • PPPNEG：开始进行 PPP 协商 • PPPUP：PPP 协商完成

8.5 PPPoE Client典型配置举例

1. 组网需求

如下图所示，配置 AP 实现 PPPoE Client 的功能，能够与 PPPoE Server 建立 PPPoE 互通。

图8-6 PPPoE Client 配置组网图



2. 配置步骤

(1) 配置 PPPoE Client。

步骤 1：在 AP 的导航栏中选择“网络 > PPPoE”，默认进入“Client 信息”页签的页面。

步骤 2：单击<新建>按钮。

步骤 3：进行如下配置，如下图所示。

- 输入 Dialer 接口为“1”。
- 输入用户名为“user1”。
- 输入密码为“hello”。
- 选择 IP 配置为“PPP 协商”。
- 选择绑定接口为“Vlan-interface1”。
- 选择连接方式为“永久在线”。

步骤 4：单击<确定>按钮完成操作。

图8-7 新建 PPPoE Client



(2) 配置 PPPoE Server。

PPPoE Server 上需要启用 PPPoE 协议、配置与 Client 上的配置相同的 PPPoE 用户和密码、为 PPP 对端分配的 IP 地址等，详细配置略。

3. 配置结果验证

在 AP 上查看 PPPoE Client 会话的概要信息。

步骤 1：在 AP 的导航栏中选择“网络 > PPPoE”，单击“会话信息”页签。

步骤 2：选择会话信息查看类型为“概要信息”。

步骤 3：查看到 PPP 协商已完成，如下图所示。

图8-8 查看 PPPoE Client 会话的概要信息



8.6 注意事项

配置 PPPoE Client 时需要注意，在“设备 > 接口管理”中创建的 Dialer 接口也可以在 PPPoE Client 的显示页面中显示出来，并且可以修改和删除，但是无法建立 PPPoE Client 会话。

9 服务管理

9.1 概述

服务管理模块提供了 Telnet、SSH、SFTP、HTTP 和 HTTPS 服务的使能管理功能，可以使用户只在需要使用相应的服务时使能服务，否则关闭服务。这样，可以提高系统的性能和设备的安全性，实现对设备的安全管理。

服务管理模块还提供了修改 HTTP、HTTPS 服务端口号的功能，以及设置将 HTTP、HTTPS 服务与 ACL（Access Control List，访问控制列表）关联，只允许通过 ACL 过滤的客户端访问设备的功能，以减少非法用户对这些服务的攻击。

1. Telnet服务

Telnet 协议在 TCP/IP 协议族中属于应用层协议，用于在网络中提供远程登录和虚拟终端的功能。

2. SSH服务

SSH 是 Secure Shell（安全外壳）的简称。用户通过一个不能保证安全的网络环境远程登录到设备时，SSH 可以利用加密和强大的认证功能提供安全保障，保护设备不受诸如 IP 地址欺诈、明文密码截取等攻击。

3. SFTP服务

SFTP 是 Secure FTP 的简称，是 SSH 2.0 中新增的功能。SFTP 建立在 SSH 连接的基础之上，它使得远程用户可以安全地登录设备，进行文件管理和文件传送等操作，为数据传输提供了更高的安全保障。

4. HTTP服务

HTTP 是 Hypertext Transfer Protocol（超文本传输协议）的简称。它用来在 Internet 上传递 Web 页面信息。HTTP 位于 TCP/IP 协议栈的应用层。

在设备上使能 HTTP 服务后，用户就可以通过 HTTP 协议登录设备，利用 Web 功能访问并控制设备。

5. HTTPS服务

HTTPS（Hypertext Transfer Protocol Secure，超文本传输协议的安全版本）是支持 SSL（Secure Sockets Layer，安全套接字层）协议的 HTTP 协议。

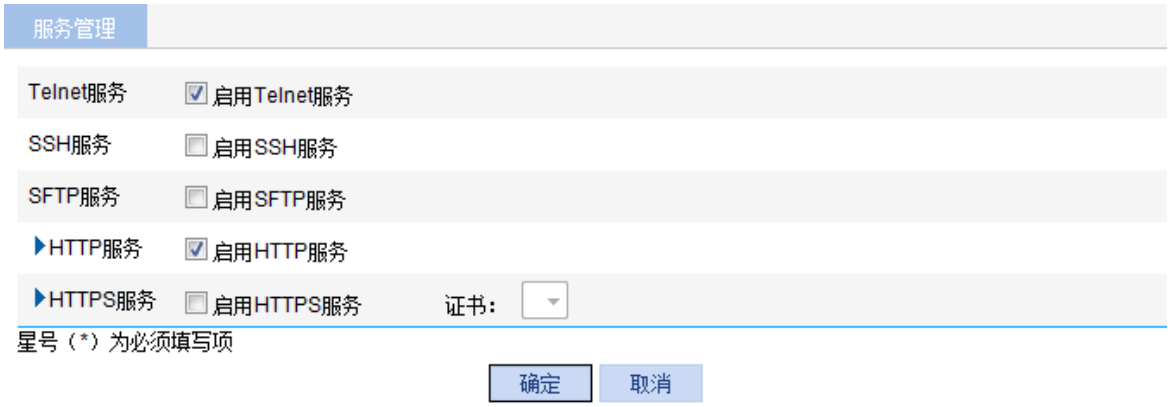
HTTPS 通过 SSL 协议，从以下几方面提高了设备的安全性：

- 通过 SSL 协议保证合法客户端可以安全地访问设备，禁止非法的客户端访问设备；
- 客户端与设备之间交互的数据需要经过加密，保证了数据传输的安全性和完整性，从而实现了对设备的安全管理；
- 为设备制定基于证书属性的访问控制策略，对客户端的访问权限进行控制，进一步避免了非法客户对设备进行攻击。

9.2 配置服务管理

(1) 在导航栏中选择“网络 > 服务管理”，进入服务管理的配置页面，如下图所示。

图9-1 服务管理



(2) 配置各种服务的启用状态及相关参数，详细配置如下表所示。

(3) 单击<确定>按钮完成操作。

表9-1 服务管理的详细配置

配置项		说明
Telnet服务	启用Telnet服务	设置是否在设备上启用Telnet服务 缺省情况下，Telnet服务处于关闭状态
SSH服务	启用SSH服务	设置是否在设备上启用SSH服务 缺省情况下，SSH服务处于关闭状态
SFTP服务	启用SFTP服务	设置是否在设备上启用SFTP服务 缺省情况下，SFTP服务处于关闭状态 提示 启用 SFTP 服务的同时必须启用 SSH 服务
HTTP服务	启用HTTP服务	设置是否在设备上启用HTTP服务 缺省情况下，HTTP服务处于启用状态
	端口号	设置HTTP服务的端口号 单击“HTTP服务”前的扩展按钮可以显示此配置项 提示 修改端口时必须保证该端口没有被其他服务使用
	ACL	设置将HTTP服务与ACL关联，只允许通过ACL过滤的客户端使用HTTP服务 单击“HTTP服务”前的扩展按钮可以显示此配置项
HTTPS服务	启用HTTPS服务	设置是否在设备上启用HTTPS服务 缺省情况下，HTTPS服务处于关闭状态

配置项		说明
	证书	设置HTTPS服务所使用的本地证书，下拉框中显示的为证书的主题 可选的证书在“认证 > 证书管理”中配置，详细配置请参见“认证”模块中的“证书管理”  提示 不指定证书时，HTTPS 服务将自己生成证书
	端口号	设置HTTPS服务的端口号 单击“HTTPS服务”前的扩展按钮可以显示此配置项  提示 修改端口时必须保证该端口没有被其他服务使用
	ACL	设置将HTTPS服务与ACL关联，只允许通过ACL过滤的客户端使用HTTPS服务 单击“HTTPS服务”前的扩展按钮可以显示此配置项

10 诊断工具

10.1 概述

10.1.1 Ping

通过使用 Ping 工具，用户可以检查指定 IP 地址的设备是否可达，测试网络连接是否出现故障。

Ping 的成功执行过程为：

(1) 源设备向目的设备发送 ICMP 回显请求（ECHO-REQUEST）报文。

(2) 目的设备在接收到该请求报文后，向源设备发送 ICMP 回显应答（ECHO-REPLY）报文。

(3) 源设备在收到该应答报文后，显示相关的统计信息。

Ping 的输出信息分为以下几种情况：

- Ping 的执行对象可以是目的设备的 IP 地址或者主机名，如果该目的设备的主机名不可识别，则源设备上输出提示信息。
- 如果在超时时间内源设备没有收到目的设备回的 ICMP 回显应答报文，则输出提示信息和 Ping 过程报文的统计信息；如果在超时时间内源设备收到响应报文，则输出响应报文的字节数、报文序号、TTL（Time to Live，生存时间）、响应时间和 Ping 过程报文的统计信息。

Ping 过程报文的统计信息包括发送报文个数、接收到响应报文个数、未响应报文数百分比、响应时间的最小值、平均值和最大值。

10.1.2 Trace Route

通过使用 Trace Route 工具，用户可以查看报文从源设备传送到目的设备所经过的三层设备。当网络出现故障时，用户可以使用该命令分析出现故障的网络节点。

Trace Route 的执行过程为：

(1) 源设备发送一个 TTL 为 1 的报文给目的设备。

(2) 第一跳（即该报文所到达的第一个三层设备）回应一个 TTL 超时的 ICMP 报文（该报文中含有第一跳的 IP 地址），这样源设备就得到了第一个三层设备的地址。

(3) 源设备重新发送一个 TTL 为 2 的报文给目的设备。

(4) 第二跳回应一个 TTL 超时的 ICMP 报文，这样源设备就得到了第二个三层设备的地址。

(5) 以上过程不断进行，直到最终到达目的设备，源设备就得到了从它到目的设备所经过的所有三层设备的地址。

Trace Route 的执行对象可以是目的设备的 IP 地址或者主机名，如果该目的设备的主机名不可识别，则源设备上输出提示信息。

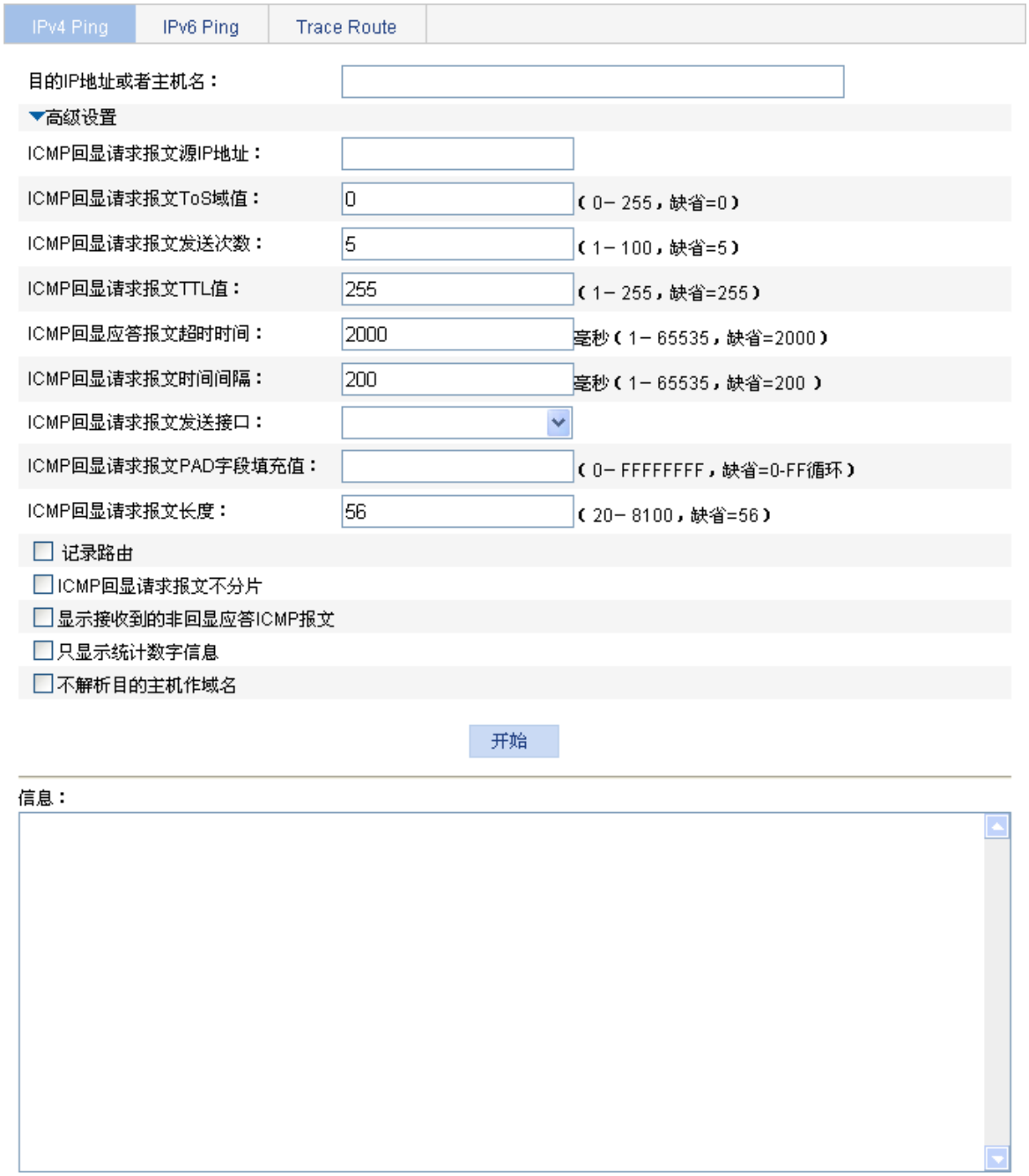
10.2 Ping操作

10.2.1 IPv4 Ping

(1) 在导航栏中选择“网络 > 诊断工具”，默认进入“IPv4 Ping”页签的页面。

(2) 单击“高级设置”前的扩展按钮，可以展开 IPv4 Ping 操作高级参数的配置内容，如下图所示。

图10-1 IPv4 Ping



(3) 在“目的 IP 地址或者主机名”文本框中输入目标设备的 IPv4 地址或者主机名。

(4) 根据具体需要设置 IPv4 Ping 操作的高级参数。

(5) 单击<开始>按钮开始执行 Ping 操作。

(6) 在“信息”框中查看 Ping 操作的输出结果，如下图所示。

图10-2 IPv4 Ping 操作结果

信息：

```
PING 192.168.1.16：56 字节
  来自 192.168.1.16 的回复：字节=56 序号=1 TTL=128 时间=1 毫秒
  来自 192.168.1.16 的回复：字节=56 序号=2 TTL=128 时间=1 毫秒
  来自 192.168.1.16 的回复：字节=56 序号=3 TTL=128 时间=1 毫秒
  来自 192.168.1.16 的回复：字节=56 序号=4 TTL=128 时间=1 毫秒
  来自 192.168.1.16 的回复：字节=56 序号=5 TTL=128 时间=1 毫秒

--- 192.168.1.16 ping 统计 ---
   传输包数：5
   接收包数：5
   0.00% 包丢失
  往返 最少/平均/最大 = 1/1/1 毫秒
```

10.2.2 IPv6 Ping

(1) 在导航栏中选择“网络 > 诊断工具”。

(2) 单击“IPv6 Ping”页签。

(3) 单击“高级设置”前的扩展按钮，可以展开 IPv6 Ping 操作高级参数的配置内容，如下图所示。

图10-3 IPv6 Ping



(4) 在“目的 IPv6 地址或主机名”文本框中输入目标设备的 IPv6 地址或者主机名。

(5) 根据具体需要设置 IPv6 Ping 操作的高级参数。

(6) 单击<开始>按钮开始执行 Ping 操作。

(7) 在“信息”框中查看 Ping 操作的输出结果，如下图所示。

图10-4 IPv6 Ping 操作结果

信息：

```
PING 3::2: 56  数据字节
  请求超时.
  请求超时.
  请求超时.
  请求超时.
  请求超时.

--- 3::2 ping 统计 ---
  5 包被传输
  0 包被接收
  100.00% 包丢失
  来回旅程 min/avg/max = 0/0/0 ms
```

10.3 Trace Route操作

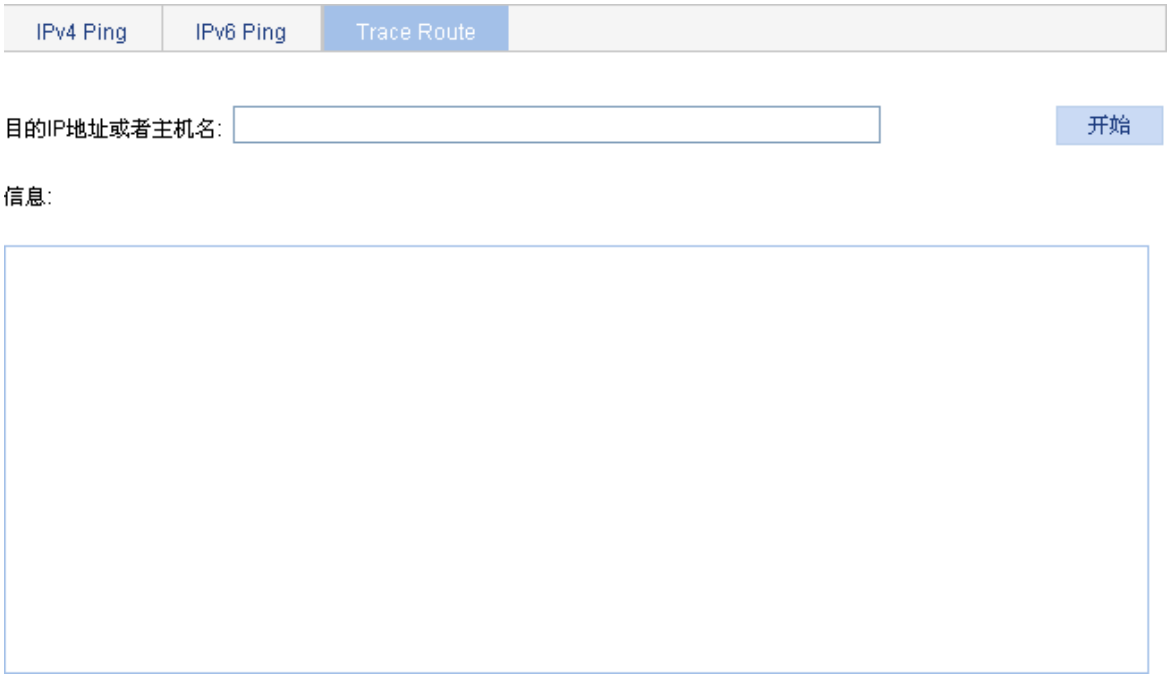
说明

- Web 目前不支持对 IPv6 地址进行 Trace Route 操作。
- 进行 Trace Route 操作前，需要先在中间设备上执行 **ip ttl-expires enable** 命令开启 ICMP 超时报文的发送功能，并且在目的设备上执行 **ip unreachables enable** 命令开启 ICMP 目的不可达报文发送功能。

(1) 在导航栏中选择“网络 > 诊断工具”。

(2) 单击“Trace Route”页签，进入如下图所示的页面。

图10-5 Trace Route

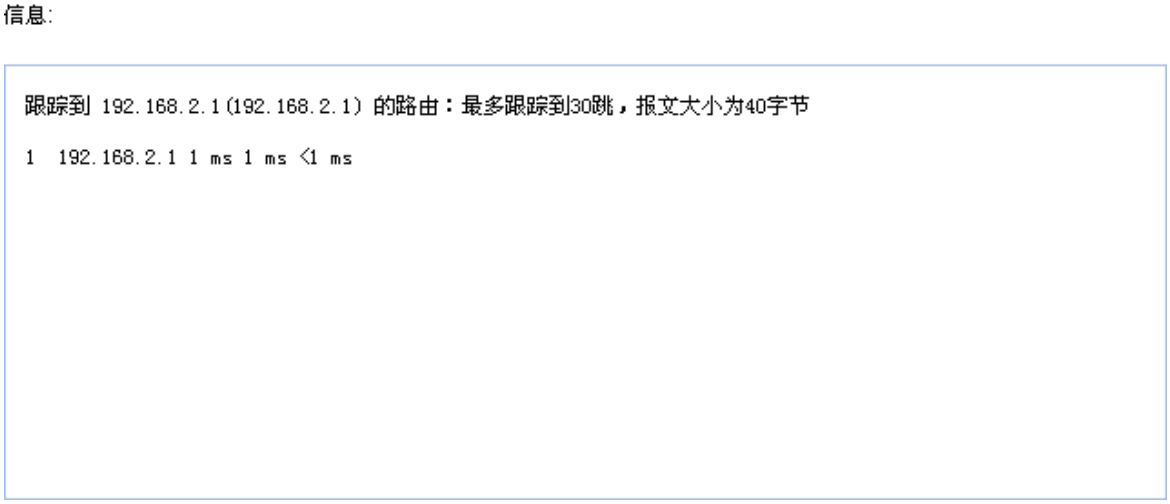


(3) 在文本框中输入 Trace Route 操作的目的 IP 地址或者主机名。

(4) 单击<开始>按钮开始执行 Trace Route 操作。

(5) 在“信息”框中查看 Trace Route 操作的输出结果，如下图所示。

图10-6 Trace Route 操作结果



目 录

1 无线服务 ····· 1-1
1.1 接入服务 ····· 1-1
1.1.1 常用术语 ····· 1-1
1.1.2 无线用户接入过程 ····· 1-1
1.1.3 WLAN服务的数据安全 ····· 1-4
1.1.4 用户接入认证 ····· 1-6
1.2 WDS简介 ····· 1-7
1.2.1 WDS的优势 ····· 1-8
1.2.2 WDS的网络拓扑 ····· 1-8
1.3 Repeater模式简介 ····· 1-9
2 配置无线服务 ····· 2-1
2.1 配置接入服务 ····· 2-1
2.1.1 新建无线服务 ····· 2-1
2.1.2 配置clear类型无线服务 ····· 2-2
2.1.3 配置crypto类型无线服务 ····· 2-12
2.1.4 绑定AP的射频 ····· 2-22
2.1.5 开启无线服务 ····· 2-22
2.1.6 开启射频 ····· 2-23
2.2 配置WDS服务 ····· 2-23
2.2.1 配置WDS服务 ····· 2-23
2.2.2 配置邻居MAC地址 ····· 2-24
2.2.3 配置WDS高级设置 ····· 2-25
2.2.4 WDS全局设置 ····· 2-27
2.2.5 配置信道 ····· 2-27
2.2.6 开启WDS服务 ····· 2-28
2.3 配置Repeater服务 ····· 2-28
2.4 无线接入配置举例 ····· 2-29
2.4.1 无线服务典型配置举例 ····· 2-29
2.4.2 基于接入服务的VLAN配置举例 ····· 2-32
2.4.3 WPA-PSK认证典型配置举例 ····· 2-36
2.4.4 MAC地址本地认证配置举例 ····· 2-39
2.4.5 远程MAC地址认证配置举例 ····· 2-43
2.4.6 远程 802.1X认证配置举例 ····· 2-52

2.4.7 自动提供WEP密钥-802.1x认证配置举例 ····· 2-67
2.4.8 802.11n典型配置举例 ····· 2-75
2.5 WDS配置举例 ····· 2-78
2.5.1 WDS典型配置举例 ····· 2-78
2.5.2 WDS点到多点典型配置举例 ····· 2-81
2.6 Repeater模式配置举例 ····· 2-82

1 无线服务

WLAN（Wireless Local Area Network，无线局域网）技术是当今通信领域的热点之一，和有线相比，无线局域网的启动和实施相对简单，成本相对低廉，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。然而，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有线网络，只是用户可以通过无线方式接入网络。

使用 WLAN 解决方案，网络运营商和企业能够为用户提供方便的无线接入服务，主要包括：

- 通过无线网络，用户可以方便的接入到网络，并访问已有网络或因特网；
- 安全问题是无线网络最大的挑战，当前无线网络可以使用不同认证和加密方式，提供安全的无线网络接入服务；
- 在无线网络内，用户可以在网络覆盖区域内自由移动，彻底摆脱有线束缚。

1.1 接入服务

1.1.1 常用术语

(1) 无线客户端

带有无线网卡的 PC、笔记本电脑以及支持 WiFi 功能的各种终端。

(2) FAT AP

一种控制和管理无线客户端的无线设备。帧在客户端和 LAN 之间传输需要经过无线到有线以及有线到无线的转换，而 FAT AP 在这个过程中起到了桥梁的作用。

(3) SSID

SSID（Service Set Identifier，服务集标识符），客户端可以先进行无线扫描，然后选择特定的 SSID 接入某个指定无线网络。

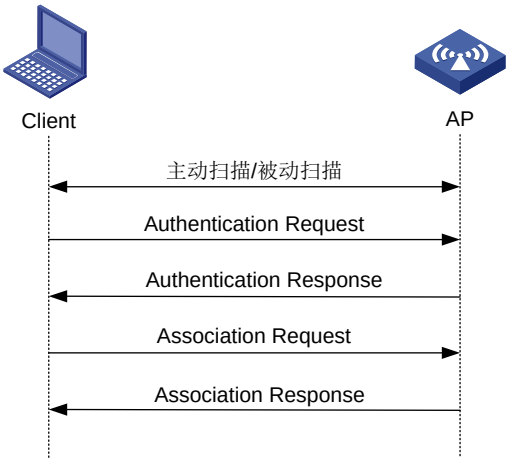
(4) 无线介质

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。

1.1.2 无线用户接入过程

无线用户首先需要通过主动/被动扫描发现周围的无线服务，再通过认证和关联两个过程后，才能和 AP 建立连接，最终接入无线局域网。整个过程如下图所示。

图1-1 建立无线连接过程



1. 无线扫描

无线客户端有两种方式可以获取到周围的无线网络信息：一种是被动扫描，无线客户端只是通过监听周围 AP 发送的 Beacon（信标帧）获取无线网络信息；另外一种为主动扫描，无线客户端在扫描的时候，同时主动发送一个探测请求帧（Probe Request 帧），通过收到探查响应帧（Probe Response）获取网络信息。

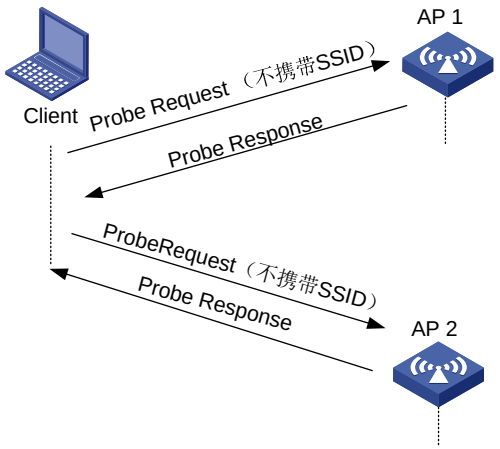
无线客户端在实际工作过程中，通常同时使用被动扫描和主动扫描获取周围的无线网络信息。

(1) 主动扫描

无线客户端在工作过程中，会定期地搜索周围的无线网络，也就是主动扫描周围的无线网络。根据 Probe Request 帧（探测请求帧）是否携带 SSID，可以将主动扫描分为两种：

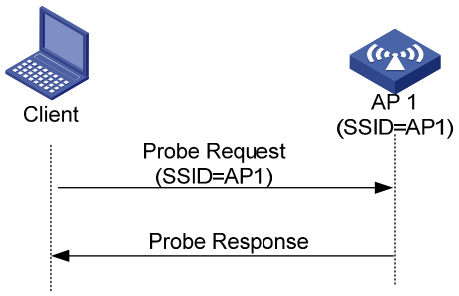
- 客户端发送 Probe Request 帧（SSID 为空，也就是 SSID IE 的长度为 0）：客户端会定期地在其支持的信道列表中，发送探查请求帧（Probe Request）扫描无线网络。当 AP 收到探查请求帧后，会回应探查响应帧（Probe Response）通告可以提供的无线网络信息。无线客户端通过主动扫描，可以主动获知可使用的无线服务，之后无线客户端可以根据需要选择适当的无线网络接入。无线客户端主动扫描方式的过程如下图所示。

图1-2 主动扫描过程（Probe Request 中 SSID 为空，也就是不携带任何 SSID 信息）



- 客户端发送 Probe Request（Probe Request 携带指定的 SSID）：当无线客户端配置希望连接的无线网络或者已经成功连接到一个无线网络情况下，客户端也会定期发送探查请求帧（Probe Request）(该报文携带已经配置或者已经连接的无线网络的 SSID)，当能够提供指定 SSID 无线服务的 AP 接收到探测请求后回复探查响应。通过这种方法，无线客户端可以主动扫描指定的无线网络。这种无线客户端主动扫描方式的过程如下图所示。

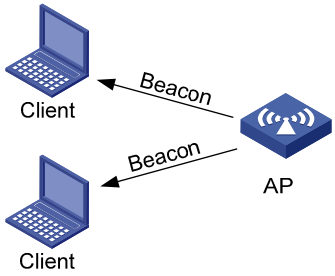
图1-3 主动扫描过程（Probe Request 携带指定的 SSID 为“AP 1”）



(2) 被动扫描

被动扫描是指客户端通过侦听 AP 定期发送的 Beacon 帧发现周围的无线网络。提供无线网络服务的 AP 设备都会周期性发送 Beacon 帧，所以无线客户端可以定期在支持的信道列表监听信标帧获取周围的无线网络信息。当用户需要节省电量时，可以使用被动扫描。一般 VoIP 语音终端通常使用被动扫描方式。被动扫描的过程如下图所示。

图1-4 被动扫描过程



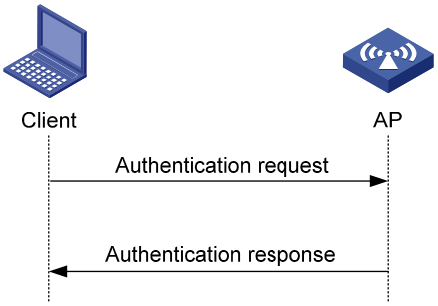
2. 认证过程

为了保证无线链路的安全，AP 需要完成对客户端的认证，只有通过认证后才能进入后续的关联阶段。802.11 链路定义了两种认证机制：开放系统认证和共享密钥认证。

- 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：第一步是无线客户端发起认证请求，第二步 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1-5 开放系统认证过程

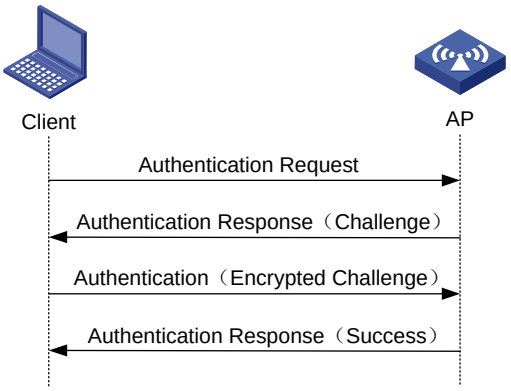


- 共享密钥认证

共享密钥认证是除开放系统认证以外的另外一种链路认证机制。共享密钥认证需要客户端和设备端配置相同的共享密钥。

共享密钥认证的认证过程为：客户端先向 AP 发送认证请求，AP 端会随机产生一个 Challenge（即一个字符串）发送给客户端；客户端会将接收到的 Challenge 加密后再发送给 AP；AP 接收到该消息后，对该消息解密，然后对解密后的字符串和原始字符串进行比较。如果相同，则说明客户端通过了 Shared Key 链路认证；否则 Shared Key 链路认证失败。

图1-6 共享密钥认证过程



3. 关联过程

如果用户想接入无线网络，必须同特定的 AP 关联。当用户通过指定 SSID 选择无线网络，并通过 AP 链路认证后，就会立即向 AP 发送关联请求。AP 会对关联请求帧携带的能力信息进行检测，最终确定该无线终端支持的能力，并回复关联响应通知链路是否关联成功。通常，无线终端同时只可以和一个 AP 建立链路，而且关联总是由无线终端发起。

1.1.3 WLAN服务的数据安全

相对于有线网络，WLAN 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。目前支持四种安全服务。

(1) 明文数据

该种服务本质上为无安全保护的 WLAN 服务，所有的数据报文都没有通过加密处理。

(2) WEP 加密

WEP（Wired Equivalent Privacy，有线等效加密）用来保护无线局域网中的授权用户所交换的数据的机密性，防止这些数据被随机窃听。WEP 使用 RC4 加密算法实现数据报文的加密保护。根据 WEP 密钥的生成方式，WEP 加密分为静态 WEP 加密和动态 WEP 加密。

- 静态 WEP 加密：

静态 WEP 加密要求手工指定 WEP 密钥，接入同一 SSID 下的所有客户端使用相同的 WEP 密钥。如果 WEP 密钥被破解或泄漏，攻击者就能获取所有密文。因此静态 WEP 加密存在比较大的安全隐患。并且手工定期更新 WEP 密钥会给网络管理员带来很大的设备管理负担。

- 动态 WEP 加密（自动提供 WEP 密钥）：

动态 WEP 加密的自动密钥管理机制对原有的静态 WEP 加密进行了较大的改善。在动态 WEP 加密机制中，用来加密单播数据帧的 WEP 密钥并不是手工指定的，而是由客户端和服务器通过 802.1x 协议协商产生，这样每个客户端协商出来的 WEP 单播密钥都是不同的，提高了单播数据帧传输的安全性。

虽然 WEP 加密在一定程度上提供了安全性和保密性，增加了网络侦听、会话截获等的攻击难度，但是受到 RC4 加密算法、过短的初始向量等限制，WEP 加密还是存在比较大的安全隐患。

(3) TKIP 加密

虽然 TKIP 加密机制和 WEP 加密机制都是使用 RC4 算法，但是相比 WEP 加密机制，TKIP 加密机制可以为 WLAN 提供更加安全的保护。

首先，TKIP 通过增长了算法的 IV（初始化向量）长度提高了加密的安全性。相比 WEP 算法，TKIP 直接使用 128 位密钥的 RC4 加密算法，而且将初始化向量的长度由 24 位加长到 48 位；

其次，虽然 TKIP 采用的还是和 WEP 一样的 RC4 加密算法，但其动态密钥的特性很难被攻破，并且 TKIP 支持密钥更新机制，能够及时提供新的加密密钥，防止由于密钥重用带来的安全隐患；

另外，TKIP 还支持了 MIC 认证（Message Integrity Check，信息完整性校验）和 Countermeasure 功能。当 TKIP 报文发生 MIC 错误时，数据可能已经被篡改，也就是无线网络很可能正在受到攻击。当在一段时间内连续接收到两个 MIC 错误的报文，AP 将会启动 Countermeasure 功能，此时，AP 将通过静默一段时间不提供服务，实现对无线网络的攻击防御。

(4) AES-CCMP 加密

CCMP（Counter mode with CBC-MAC Protocol，[计数器模式]搭配[区块密码锁链－信息真实性检查码]协议）加密机制是基于 AES（Advanced Encryption Standard，高级加密标准）加密算法的 CCM（Counter-Mode/CBC-MAC，区块密码锁链－信息真实性检查码）方法。CCM 结合 CTR（Counter mode，计数器模式）进行机密性校验，同时结合 CBC-MAC（区块密码锁链－信息真实性检查码）进行认证和完整性校验。CCMP 中的 AES 块加密算法使用 128 位的密钥和 128 位的块大小。同样 CCMP 包含了一套动态密钥协商和管理方法，每一个无线用户都会动态的协商一套密钥，而且密钥可以定时进行更新，进一步提供了 CCMP 加密机制的安全性。在加密处理过程中，CCMP 也会使用 48 位的 PN（Packet Number）机制，保证每一个加密报文都会是用不同的 PN，在一定程度上提高安全性。

1.1.4 用户接入认证

当无线终端成功和 AP 建立无线链路，可以认为无线终端成功接入到无线网络，但是为了无线网络的安全和管理，无线接入用户只有通过后面的接入认证后才可能真正访问网络资源。其中 PSK（Preshared Key 预共享密钥）认证和 802.1x 认证伴随着无线链路的动态密钥协商和管理，所以和无线链路协商关系比较密切，而且它的认证和无线链路本身没有直接关系。

(1) PSK 认证

WPA 和 WPA2 无线接入都支持 PSK 认证，无线客户端接入无线网络前，需要配置和 AP 设备相同的预共享密钥。

四次握手（4-Way Handshake）密钥协商通过 802.1x 的 4 个密钥报文交互为无线链路在无线终端和 AP 侧动态协商出私有密钥，而预共享密钥将作为密钥协商的种子密钥使用。在协商过程中，种子密钥将被双方进行验证，只有密钥设置相同，密钥协商才可以成功，也就是无线用户成功通过 PSK 接入认证；否则无线用户 PSK 接入认证失败，无线用户链路将被断开。

(2) 802.1x 认证

802.1x 协议是一种基于端口的网络接入控制协议（Port Based Network Access Control Protocol）。“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。

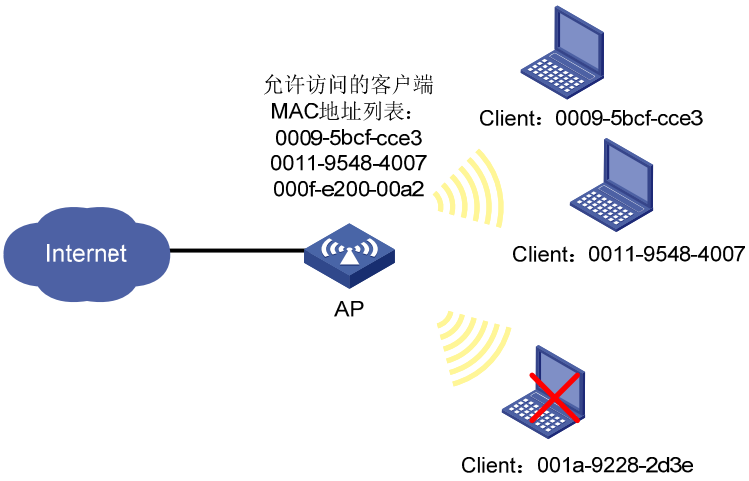
(3) MAC 地址认证

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。认证过程中，也不需要用户手动输入用户名或者密码。在 WLAN 网络应用中，MAC 认证需要预先获知可以访问无线网络的终端设备 MAC 地址，所以一般适用于用户比较固定的、小型的无线网络，例如家庭、小型办公室等环境。

MAC 地址认证分为以下两种方式：

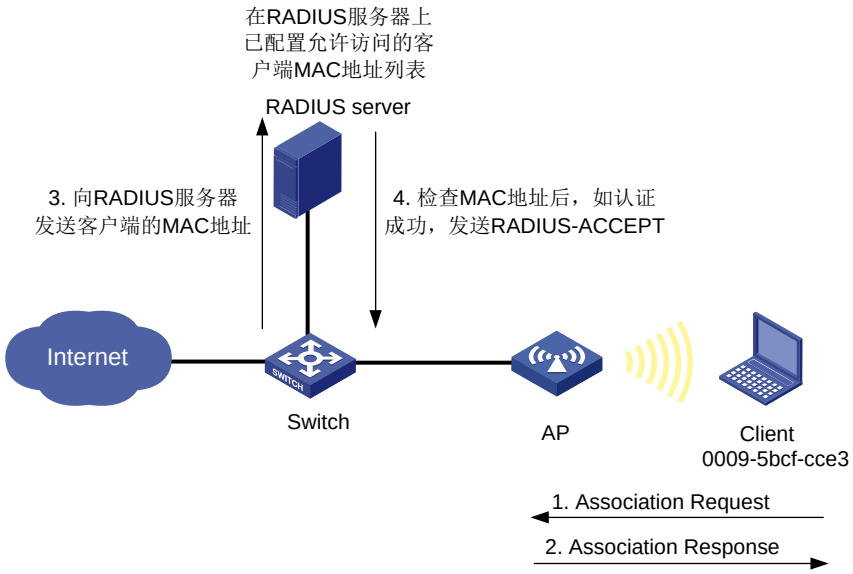
- 本地 MAC 地址认证：当选用本地认证方式进行 MAC 地址认证时，直接在设备上完成对用户的认证，此时需要在设备上配置本地用户名和密码。通常情况下，可以采用 MAC 地址作为用户名，需要事先获知无线接入用户的 MAC 地址，并将客户端的 MAC 配置为本地用户名。无线用户接入网络时，只有存在用户的 MAC 地址可以认证通过，其它用户将被拒绝接入。

图1-7 本地 MAC 地址认证



-
- 远程 MAC 地址认证，即通过 RADIUS 服务器进行 MAC 地址认证。当选用 RADIUS 服务器认证方式进行 MAC 地址认证时，设备作为 RADIUS 客户端，与 RADIUS 服务器配合完成 MAC 地址认证操作。当 MAC 接入认证发现当前接入的客户端为未知客户端，AP 设备作为 RADIUS 客户端，会与 RADIUS 服务器完成 MAC 地址认证。在 RADIUS 服务器完成对该用户的认证后，认证通过的用户可以访问无线网络，而且 RADIUS 服务器可以下发相应的授权信息。

图1-8 远程 MAC 地址认证



采用 RADIUS 服务器进行 MAC 地址认证时，可以通过在各无线服务下分别指定各自的 domain 域，将不同 SSID 的 MAC 地址认证用户信息发送到不同的远端 RADIUS 服务器。

1.2 WDS简介

WDS（Wireless Distribution System，无线分布式系统），通过无线链路连接两个或者多个独立的有线局域网或者无线局域网，组建一个互通的网络实现数据访问。

1.2.1 WDS的优势

802.11 的无线技术已经在家庭、SOHO、企业等得到广泛地应用，用户已经能通过这些无线局域网方便地访问 Internet 网络。但是在这种网络应用中，AP 必须链接到已有的有线网络，才可能提供无线用户的网络访问服务。采用传统的方式，AP 需要和有线网络连接，会导致最终部署成本较高，并且在大面积无线覆盖时需要大量的时间，而使用 WDS 技术可以在一些复杂的环境中方便快捷建设无线局域网。WDS 网络的优点包括：

- 通过无线网桥连接两个独立的局域网段，并且在他们之间提供数据传输。
- 低成本，高性能。
- 扩展性好，并且无需铺设新的有线连接和部署更多的 AP。
- 适用于公司，大型仓储，制造，码头等领域。

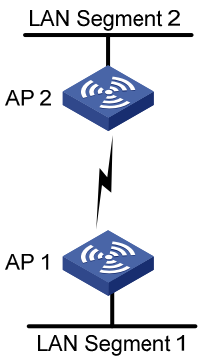
1.2.2 WDS的网络拓扑

根据实际应用需求，WDS网络可以提供了以下三种拓扑。通过在每个AP的射频模式下配置邻居AP的MAC地址来实现，详细配置请参见“2.2.2 配置邻居MAC地址”。

1. 点到点的桥接

该网络中，WDS 通过两台设备实现了两个网络无线桥接，最终实现两个网络的互通。实际应用中，每一台设备可以通过配置的对端设备的 MAC 地址，确定需要建立的桥接链路。如下图所示，AP 1 和 AP 2 之间建立 WDS 桥接链路，可以将 LAN Segment 1 和 LAN Segment 2 链接成一个统一的局域网。局域网 1 中的用户需要访问局域网 2 中的资源的时候，所有的报文都会被 AP1 转换成无线报文通过无线桥接链路发送到 AP2，最终在由 AP2 将报文还原发送到目的地；反之亦然。

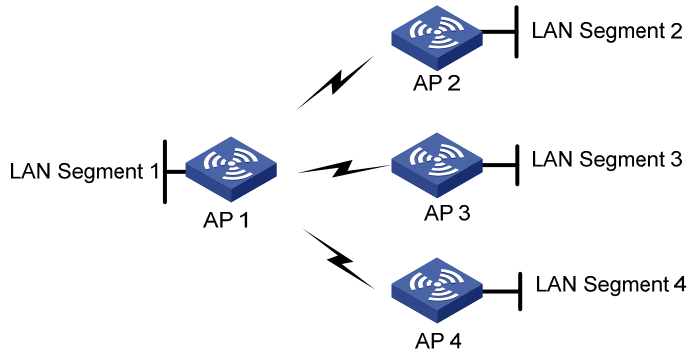
图1-9 点到点的桥接



2. 点到多点的桥接

在点到多点的组网环境中，一台设备作为中心设备，其他所有的设备都只和中心设备建立无线桥接，实现多个网络的互联。该组网可以方便地解决多个网络孤岛需要连接到已有网络的要求，但是多个分支网络的互通都要通过中心桥接设备进行数据转发。

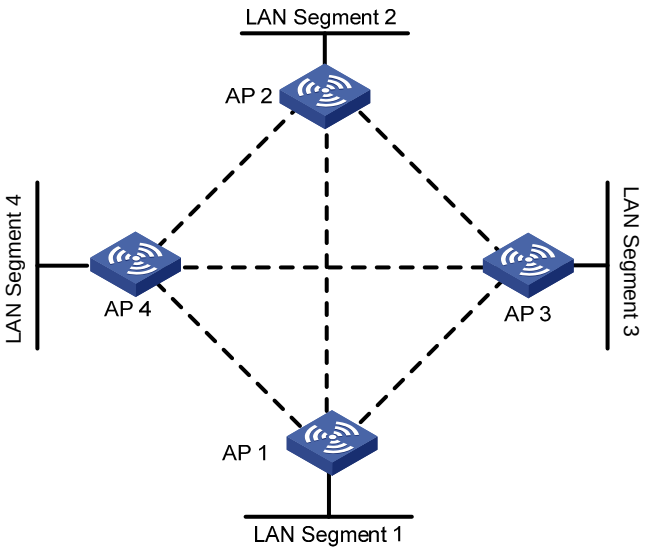
图1-10 点到多点的桥接



3. 网状桥接

多台桥接设备可以采用手动配置或者自动检测方式，互相建立网状无线桥接，将多个局域网连接成一个网络。网状桥接网络，在一条 WDS 链路故障时可以提供链路备份的功能，但是应用中需要结合 STP 解决网络的环路问题。

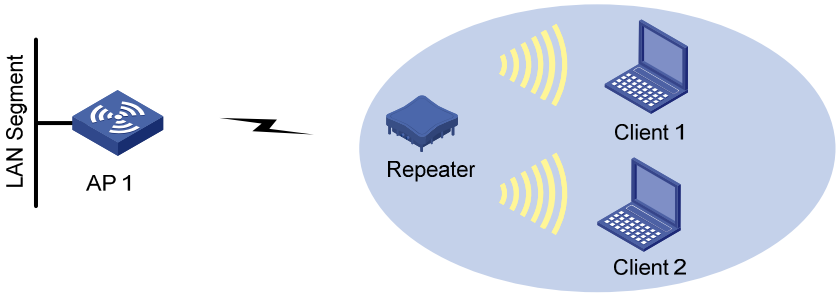
图1-11 自拓扑检测与桥接



1.3 Repeater模式简介

Repeater 即 AP 中继模式，是指作为 Repeater 的 AP 不但通过 WDS 链路与另一台 AP 建立桥接，而且同时提供无线接入服务，也就是 Repeater 不但创建无线网络而且通过 WDS 桥接将无线网络接入到已有网络中。以下图为例，Repeater 虽然不直接接入有线网络，但是可以为 Client 1 和 Client 2 提供访问有线网络的服务。从应用的角度来看，通过网络中部署了 Repeater AP，延长了无线通信的距离和扩大了无线网络的覆盖范围。

图1-12 Repeater 模式



2 配置无线服务

说明

手册中设备的接口类型、显示信息与设备型号、支持射频情况和配置信息相关，实际使用中还请以设备的实际情况为准。

2.1 配置接入服务

接入服务配置的推荐步骤如下表所示。

表2-1 接入服务配置步骤

步骤	配置任务	说明
1	新建无线服务	必选
2	配置clear类型的无线服务	两者必选其一 按实际需求完成接入服务页面的安全设置部分
3	配置crypto类型的无线服务	
4	绑定AP的射频	必选
5	开启无线服务	必选
6	开启射频	可选

2.1.1 新建无线服务

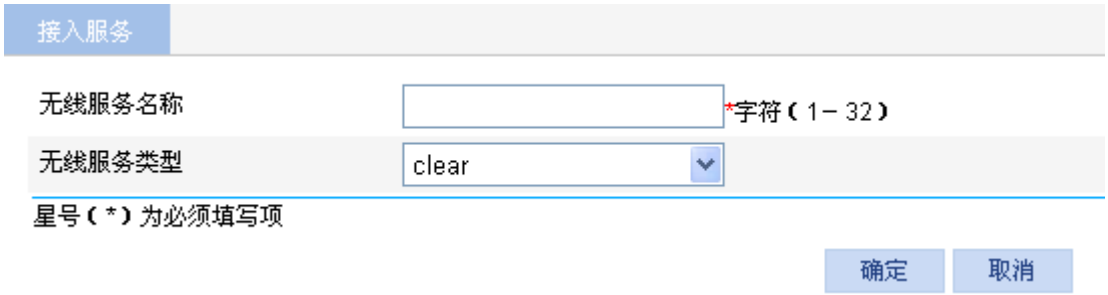
(1) 在界面左侧的导航栏中选择“无线服务 > 接入服务”，进入如下图所示接入服务配置页面。

图2-1 接入服务配置页面



(2) 单击<新建>按钮，进入如下图所示无线服务新建页面。

图2-2 接入服务新建页面



(3) 配置无线服务，详细配置如下表所示。

(4) 单击<确定>按钮完成操作。

表2-2 新建无线服务的详细配置

配置项	说明
无线服务名称	设置SSID SSID的名称应该尽量具有唯一性。从安全方面考虑不应该体现公司名称，也不推荐使用长随机数序列作为SSID，因为长随机数序列只是增加了Beacon报文长度和使用难度，对无线安全没有改进
无线服务类型	选择无线服务类型： • clear：使用明文发送数据 • crypto：使用密文发送数据

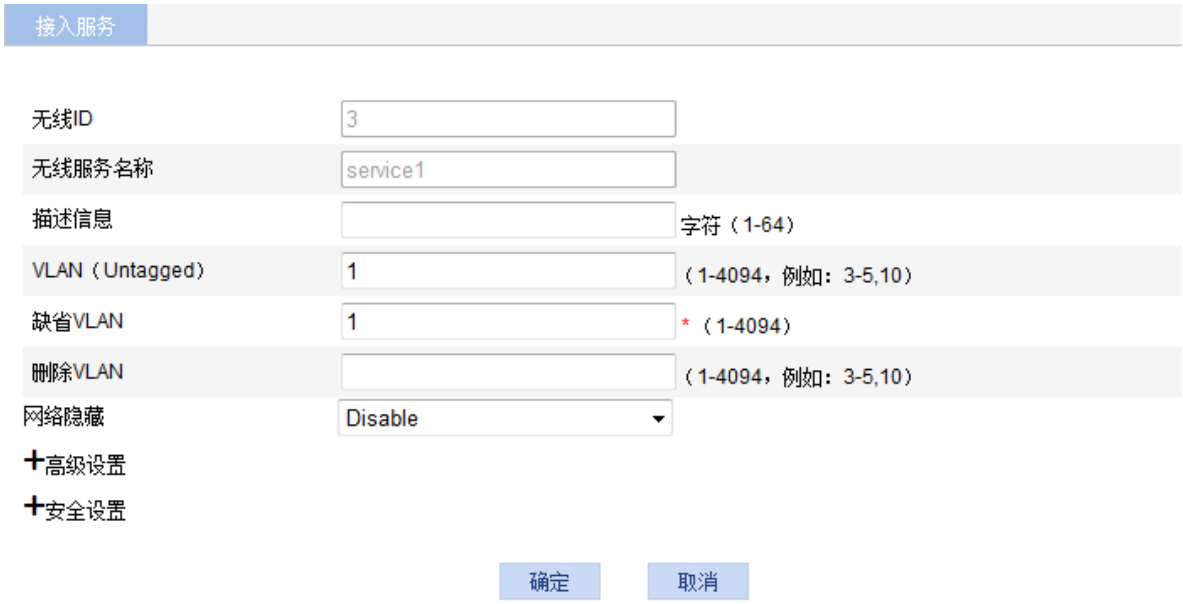
2.1.2 配置clear类型无线服务

1. clear类型无线服务基本配置

(1) 在界面左侧的导航栏中选择“无线服务 > 接入服务”。

(2) 在列表中找到要进行配置的 clear 类型无线服务，单击对应的图标，进入如下图所示的配置页面。

图2-3 clear 类型无线服务基本配置页面



(3) 配置 clear 类型无线服务基本信息，详细配置如下表所示。

(4) 单击<确定>按钮完成操作。

表2-3 clear 类型无线服务基本配置的详细配置

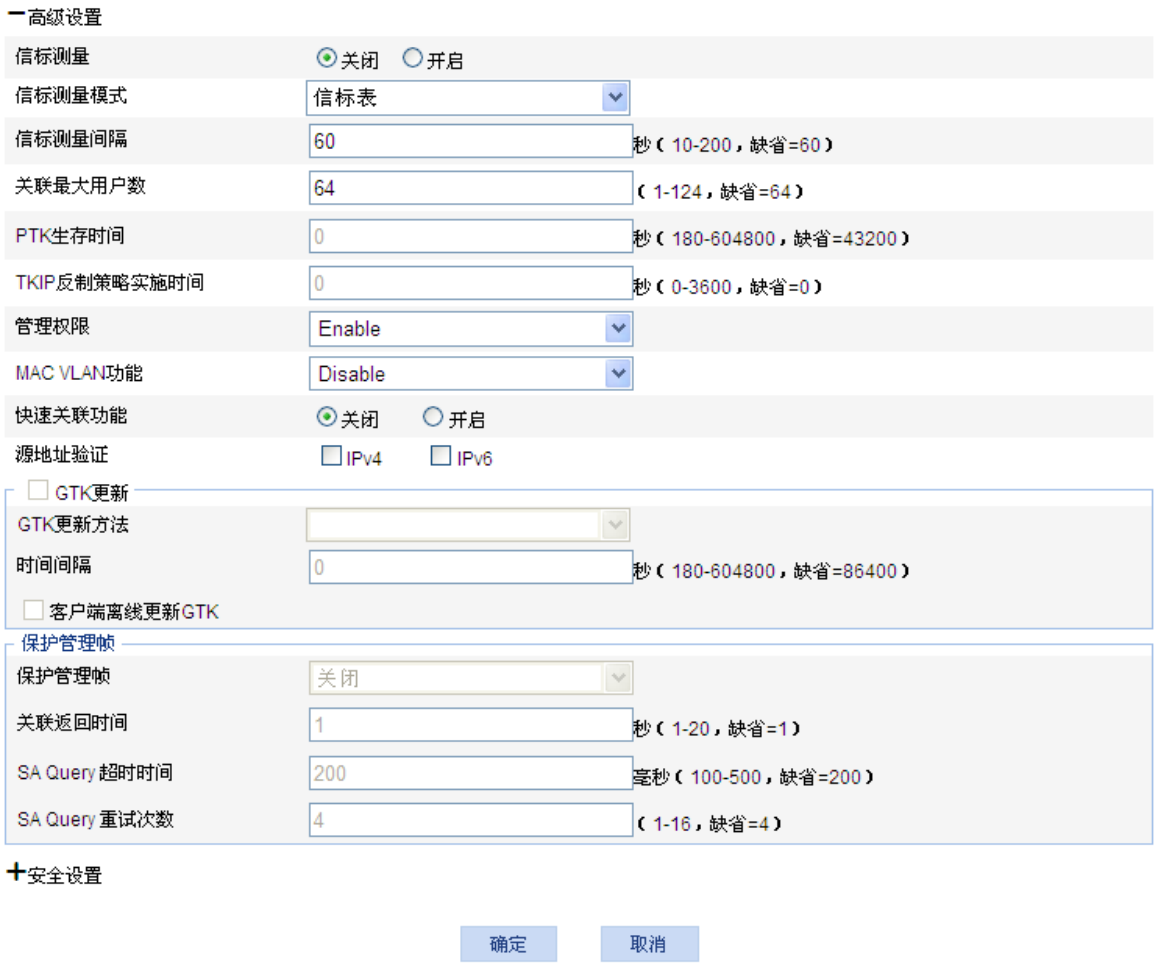
配置项	说明
无线ID	显示无线服务的ID信息
无线服务名称	显示选择的SSID
VLAN（Untagged）	添加Untagged的VLAN ID，VLAN（Untagged）表示端口成员发送该VLAN报文时不带Tag标签
缺省VLAN	设置端口的缺省VLAN 在缺省情况下，所有端口的缺省VLAN均为VLAN 1，设置新的缺省VLAN后，VLAN 1为Untagged的VLAN ID
删除VLAN	删除已有Tagged和Untagged的VLAN ID
网络隐藏	配置是否在信标帧中通告SSID，缺省情况下，信标帧通告SSID • Enable：禁止在信标帧中通告 SSID • Disable：在信标帧中通告 SSID 提示 • SSID 隐藏后，AP 发送的信标帧里面不包含 SSID 信息，接入客户端必须在无线网卡上手动配置该 SSID 标识才能接入 AP • 隐藏 SSID 对无线安全意义不大。允许广播 SSID 可以使客户端更容易发现 AP

2. clear类型无线服务高级配置

(1) 在界面左侧的导航栏中选择“无线服务 > 接入服务”。

(2) 在列表中找到要进行配置的 clear 类型无线服务，单击对应的图标，进入如下图所示 clear 类型无线服务高级配置页面。

图2-4 clear 类型无线服务高级配置页面



(3) 配置 clear 类型无线服务高级信息，详细配置如下表所示。

(4) 单击<确定>按钮完成操作。

表2-4 clear 类型无线服务高级配置的详细配置

配置项	说明
信标测量	• 开启：开启信标测量功能 • 关闭：关闭信标测量功能 缺省情况下，信标测量功能处于关闭状态 信标测量是802.11k协议定义的一套用于无线设备向其他无线设备查询无线环境信息的标准方法之一。开启信标测量功能后，AP会周期性地向客户端发送信标测量请求，客户端收到信标测量请求后，会回复信标测量报告。AP通过信标测量报告获取客户端收集到的信标测量信息

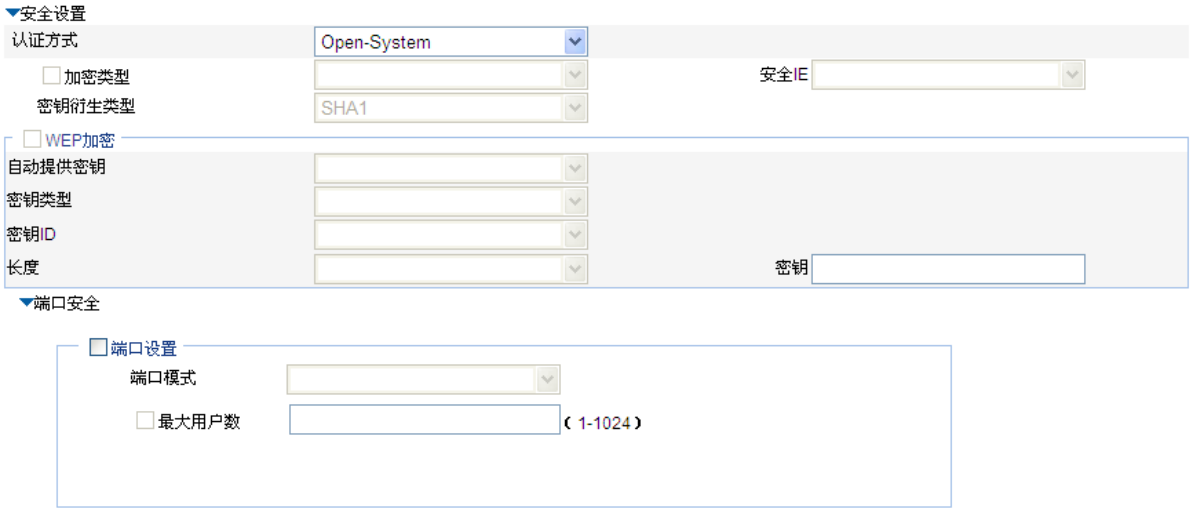
配置项	说明
信标测量模式	信标测量的三种模式： • 主动模式：AP 向客户端发送信标测量请求，客户端收到信标测量请求后，会在其支持的所有信道上广播发送 Probe Request 帧，然后设置一个测量持续时长，在测量结束后，处理收到的所有 Beacon 帧和 Probe Response 帧，并编制信标测量报告回复给 AP • 信标表模式：AP 向客户端发送信标测量请求，客户端收到信标测量请求后，不执行额外的测量，直接向 AP 回复信标测量报告，该报告中包含客户端当前存储的所有信标测量信息 • 被动模式：AP 向客户端发送信标测量请求，客户端收到信标测量请求后，会设置一个测量持续时长，在测量结束后，处理收到的所有 Beacon 帧和 Probe Response 帧，并编制信标测量报告回复给 AP
信标测量间隔	配置信标测量请求的发送间隔
关联最大用户数	在一个射频下，某个SSID下关联客户端的最大个数 提示 当某个 SSID 下关联的客户端达到最大个数时，该 SSID 会自动隐藏
MAC VLAN功能	• Enable：表示在指定无线服务下开启 mac-vlan 功能 • Disable：表示在指定无线服务下禁止 mac-vlan 功能
快速关联功能	• 开启：开启快速关联功能 • 关闭：关闭快速关联功能 缺省情况下，快速关联功能处于关闭状态 开启此功能后，设备不会对关联到此无线服务的客户端进行频谱导航计算

3. clear类型无线服务安全配置

(1) 在界面左侧的导航栏中选择“无线服务 > 接入服务”。

(2) 在列表中找到要进行配置的 clear 类型无线服务，单击对应的图标，进入 clear 类型无线服务安全配置页面。

图2-5 clear 类型无线服务安全配置页面



(3) 配置 clear 类型无线服务安全信息，详细配置如下表所示。

(4) 单击<确定>按钮完成操作。

表2-5 clear 类型无线服务安全配置的详细配置

配置项	说明
认证方式	clear类型只能选择Open-System方式

配置项	说明
端口安全	• mac-authentication：对接入用户采用 MAC 地址认证 • mac-else-userlogin-secure：端口同时处于 mac-authentication 模式和 userlogin-secure 模式，但 MAC 地址认证优先级大于 802.1x 认证；对于非 802.1x 报文直接进行 MAC 地址认证。对于 802.1x 报文先进行 MAC 地址认证，如果 MAC 地址认证失败进行 802.1x 认证 • mac-else-userlogin-secure-ext：与 mac-else-userlogin-secure 类似，但允许端口下有多个 802.1x 和 MAC 地址认证用户 • userlogin-secure：对接入用户采用基于端口的 802.1X 认证，此模式下，端口允许多个 802.1X 认证用户接入，但只有一个用户在线 • userlogin-secure-or-mac：端口同时处于 userlogin-secure 模式和 mac-authentication 模式，但 802.1x 认证优先级大于 MAC 地址认证；在用户接入方式为无线的情况下，报文首先进行 802.1x 认证，如果 802.1x 认证失败再进行 MAC 地址认证 • userlogin-secure-or-mac-ext：与 userlogin-secure-or-mac 类似，但允许端口下有多个 802.1x 和 MAC 地址认证用户 • userlogin-secure-ext：对接入用户采用基于 MAC 的 802.1x 认证，且允许端口下有多个 802.1x 用户 窍门 由于安全模式种类较多，为便于记忆，部分端口安全模式名称的构成可按如下规则理解： • “userLogin”表示基于端口的 802.1X 认证 • “mac”表示 MAC 地址认证 • “Else”之前的认证方式先被采用，失败后根据请求认证的报文协议类型决定是否转为“Else”之后的认证方式 • “Or”连接的两种认证方式无固定生效顺序，设备根据请求认证的报文协议类型决定认证方式，但无线接入的用户先采用 802.1X 认证方式 • 携带“Secure”的 userLogin 表示基于 MAC 地址的 802.1X 认证 • 携带“Ext”表示可允许多个 802.1X 用户认证成功，不携带则表示仅允许一个 802.1X 用户认证成功
最大用户数	控制能够通过某端口接入网络的最大用户数

当选择 mac-authentication 时，需要配置如下选项。

图2-6 mac-authentication 端口安全配置页面



表2-6 mac-authentication 端口安全配置的详细配置

配置项	说明
端口模式	mac-authentication：对接入用户采用MAC地址认证 在导航栏中选择“无线服务 > 接入服务”，单击<MAC认证列表>按钮，输入客户端的MAC地址
最大用户数	控制能够通过某端口接入网络的最大用户数
MAC认证	选中“MAC认证”前的复选框
域名	在下拉框中选择已存在的域 设备的缺省域为“system”。在界面左侧的导航栏中选择“认证 > AAA”，选择“域设置”页签，在域名下拉输入框中可以新建域 需要注意的是： • 在该选项中选择的域名仅对此无线服务生效，并且从该无线服务接入的客户端将被强制使用该认证域来进行认证、授权和计费 • 请不要删除使用中的域名，否则会导致正在使用此无线服务的客户端下线

当选择 userlogin-secure/userlogin-secure-ext 时，需要配置如下选项。

图2-7 userlogin-secure/userlogin-secure-ext 端口安全配置页面（以 userlogin-secure 为例）



表2-7 userlogin-secure/userlogin-secure-ext 端口安全配置的详细配置

配置项	说明
端口模式	• userlogin-secure：对接入用户采用基于端口的 802.1X 认证，此模式下，端口允许多个 802.1X 认证用户接入，但只有一个用户在线 • userlogin-secure-ext：对接入用户采用基于 MAC 的 802.1x 认证，且允许端口下有多个 802.1x 用户
最大用户数	控制能够通过某端口接入网络的最大用户数
域名	在下拉框中选择已存在的域 设备的缺省域为“system”。在界面左侧的导航栏中选择“认证 > AAA”，选择“域设置”页签，在域名下拉输入框中可以新建域 需要注意的是： • 在该选项中选择的域名仅对此无线服务生效，并且从该无线服务接入的客户端将被强制使用该认证域来进行认证、授权和计费 • 请不要删除使用中的域名，否则会导致正在使用此无线服务的客户端下线
认证方法	• EAP：采用 EAP 认证方式。采用 EAP 认证方式意味着设备直接把 802.1X 用户的认证信息以 EAP 报文直接封装到 RADIUS 报文的属性字段中，发送给 RADIUS 服务器完成认证，而无须将 EAP 报文转换成标准的 RADIUS 报文后再发给 RADIUS 服务器来完成认证 • CHAP：采用 CHAP 认证方式。缺省情况下，采用 CHAP 认证方式。表示在网络上以明文方式传输用户名，以密文方式传输口令。相比之下，CHAP 认证保密性较好，更为安全可靠 • PAP：采用 PAP 认证方式。PAP 采用明文方式传送口令
用户握手	• Enable：开启在线用户握手功能，通过设备端定期向客户端发送握手报文来探测用户是否在线。缺省情况下，在线用户握手功能处于开启状态 • Disable：关闭在线用户握手功能

配置项	说明
多播触发	• Enable：开启 802.1X 的组播触发功能，即周期性地向客户端发送组播触发报文。缺省情况下，802.1X 的组播触发功能处于开启状态 • Disable：关闭 802.1X 的组播触发功能 提示 对于无线局域网来说，可以由客户端主动发起认证，或由无线模块发现用户并触发认证，而不必端口定期发送 802.1X 的组播报文来触发。同时，组播触发报文会占用无线的通信带宽，因此建议无线局域网中的接入设备关闭该功能

当选择其他四种端口安全时，需要配置如下选项。

图2-8 四种端口安全配置页面（以 mac-else-userlogin-secure 为例）

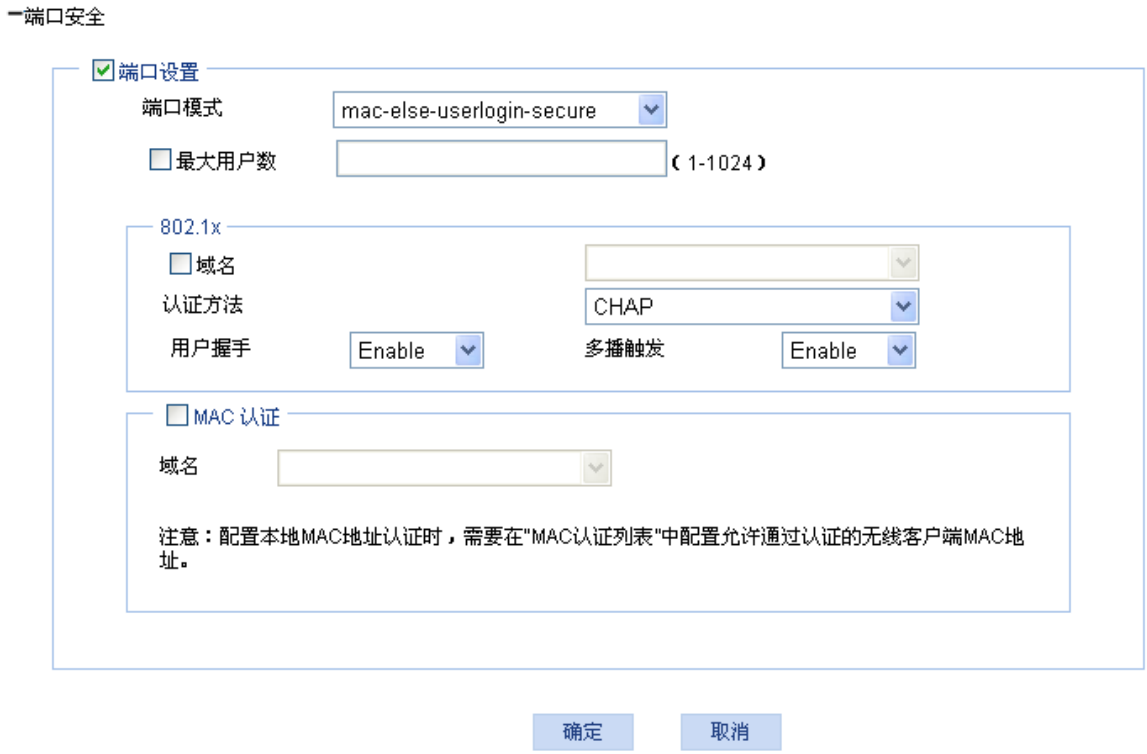


表2-8 其他四种端口安全配置的详细配置

配置项	说明
端口模式	• mac-else-userlogin-secure：端口同时处于 mac-authentication 模式和 userlogin-secure 模式，但 MAC 地址认证优先级大于 802.1x 认证；对于非 802.1x 报文直接进行 MAC 地址认证。对于 802.1x 报文先进行 MAC 地址认证，如果 MAC 地址认证失败进行 802.1x 认证 • mac-else-userlogin-secure-ext：与 mac-else-userlogin-secure 类似，但允许端口下有多个 802.1x 和 MAC 地址认证用户 • userlogin-secure-or-mac：端口同时处于 userlogin-secure 模式和 mac-authentication 模式，但 802.1x 认证优先级大于 MAC 地址认证；在用户接入方式为无线的情况下，报文首先进行 802.1x 认证，如果 802.1x 认证失败再进行 MAC 地址认证 • userlogin-secure-or-mac-ext：与 userlogin-secure-or-mac 类似，但允许端口下有多个 802.1x 和 MAC 地址认证用户 在导航栏中选择“无线服务 > 接入服务”，单击<MAC认证列表>按钮，输入客户端的MAC地址
最大用户数	控制能够通过某端口接入网络的最大用户数
域名	在下拉框中选择已存在的域，配置了强制认证域后，所有从该端口接入的802.1X用户将被强制使用该认证域来进行认证、授权和计费 设备的缺省域为“system”。在界面左侧的导航栏中选择“认证 > AAA”，选择“域设置”页签，在域名下拉输入框中可以新建域
认证方法	• EAP：采用 EAP 认证方式。采用 EAP 认证方式意味着设备直接把 802.1X 用户的认证信息以 EAP 报文直接封装到 RADIUS 报文的属性字段中，发送给 RADIUS 服务器完成认证，而无须将 EAP 报文转换成标准的 RADIUS 报文后再发给 RADIUS 服务器来完成认证 • CHAP：采用 CHAP 认证方式。缺省情况下，采用 CHAP 认证方式。表示在网络上以明文方式传输用户名，以密文方式传输口令。相比之下，CHAP 认证保密性较好，更为安全可靠 • PAP：采用 PAP 认证方式。PAP 采用明文方式传送口令
用户握手	• Enable：开启在线用户握手功能，通过设备端定期向客户端发送握手报文来探测用户是否在线。缺省情况下，在线用户握手功能处于开启状态 • Disable：关闭在线用户握手功能
多播触发	• Enable：开启 802.1X 的组播触发功能，即周期性地向客户端发送组播触发报文。缺省情况下，802.1X 的组播触发功能处于开启状态 • Disable：关闭 802.1X 的组播触发功能 提示 对于无线局域网来说，可以由客户端主动发起认证，或由无线模块发现用户并触发认证，而不必端口定期发送 802.1X 的组播报文来触发。同时，组播触发报文会占用无线的通信带宽，因此建议无线局域网中的接入设备关闭该功能
MAC认证	选中“MAC认证”前的复选框

配置项	说明
域名	在下拉框中选择已存在的域 设备的缺省域为“system”。在界面左侧的导航栏中选择“认证 > AAA”，选择“域设置”页签，在域名下拉输入框中可以新建域 需要注意的是： • 在该选项中选择的域名仅对此无线服务生效，并且从该无线服务接入的客户端将被强制使用该认证域来进行认证、授权和计费 • 请不要删除使用中的域名，否则会导致正在使用此无线服务的客户端下线

2.1.3 配置crypto类型无线服务

1. crypto类型无线服务基本配置

(1) 在界面左侧的导航栏中选择“无线服务 > 接入服务”。

(2) 在列表中找到要进行配置的 crypto 类型无线服务，单击对应的 图标，进入如下图所示页面。

图2-9 crypto 类型无线服务基本配置页面



(3) 配置crypto类型无线服务基本信息，详细配置请参见 表 2-3。

(4) 单击<确定>按钮完成操作。

2. crypto类型无线服务高级配置

(1) 在界面左侧的导航栏中选择“无线服务 > 接入服务”。

(2) 在列表中找到要进行配置的 crypto 类型无线服务，单击对应的 图标，进入如下图所示页面。

图2-10 crypto 类型无线服务高级配置页面



(3) 配置 crypto 类型无线服务高级信息，详细配置如下表所示。

(4) 单击<确定>按钮完成操作。

说明

开启服务模板后，服务模板的设置无法修改。

表2-9 crypto 类型无线服务高级配置的详细配置

配置项	说明
信标测量	• 开启：开启信标测量功能 • 关闭：关闭信标测量功能 缺省情况下，信标测量功能处于关闭状态 信标测量是802.11k协议定义的一套用于无线设备向其他无线设备查询无线环境信息的标准方法之一。开启信标测量功能后，AP会周期性地向客户端发送信标测量请求，客户端收到信标测量请求后，会回复信标测量报告。AP通过标测量报告获取客户端收集到的信标测量信息

配置项	说明
信标测量模式	信标测量的三种模式： • 主动模式：AP 向客户端发送信标测量请求，客户端收到信标测量请求后，会在其支持的所有信道上广播发送 Probe Request 帧，然后设置一个测量持续时长，在测量结束后，处理收到的所有 Beacon 帧和 Probe Response 帧，并编制信标测量报告回复给 AP • 信标表模式：AP 向客户端发送信标测量请求，客户端收到信标测量请求后，不执行额外的测量，直接向 AP 回复信标测量报告，该报告中包含客户端当前存储的所有信标测量信息 • 被动模式：AP 向客户端发送信标测量请求，客户端收到信标测量请求后，会设置一个测量持续时长，在测量结束后，处理收到的所有 Beacon 帧和 Probe Response 帧，并编制信标测量报告回复给 AP
信标测量间隔	配置信标测量请求的发送间隔
关联最大用户数	在一个射频下，某个SSID下的关联客户端的最大个数 提示 当某个 SSID 下关联的客户端达到最大个数时，该 SSID 会自动隐藏
PTK生存时间	设置PTK的生存时间，PTK通过四次握手方式生成
TKIP反制策略实施时间	设置反制策略实施时间 缺省情况下，TKIP反制策略实施的时间为0秒，即不启动反制策略；如果时间设置为其他值则启动反制策略 MIC（Message Integrity Check，信息完整性校验）是为了防止黑客的篡改而定制的，它采用Michael算法，具有很高的安全特性。当MIC发生错误的时候，数据很可能已经被篡改，系统很可能正在受到攻击。启动反制策略后，如果在一定时间内发生了两次MIC错误，则会解除所有关联到该无线服务的客户端，并且只有在TKIP反制策略实施的时间后，才允许客户端重新建立关联
管理权限	上线的客户端对设备WEB界面的管理权限 • Disable：表示上线的客户端对设备 WEB 界面没有管理权限 • Enable： 表示上线的客户端对设备 WEB 界面有管理权限
MAC VLAN功能	• Enable：表示在指定无线服务下开启 mac-vlan 功能 • Disable：表示在指定无线服务下禁止 mac-vlan 功能
快速关联功能	• 开启：开启快速关联功能 • 关闭：关闭快速关联功能 缺省情况下，快速关联功能处于关闭状态 开启此功能后，设备不会对关联到此无线服务的客户端进行频谱导航计算
源地址验证	• IPv4 地址 • IPv6 地址 缺省情况下，没有配置源地址验证

配置项	说明
GTK更新方法	GTK由AP生成，在AP和客户端认证处理的过程中通过组密钥握手和4次握手的方式发送到客户端。客户端使用GTK来解密组播和广播报文 • 选用基于时间更新的方法，需要指定 GTK 密钥更新的周期时间间隔 • 选用基于数据包更新的方法，需要指定传输的数据包的数目，在传送指定数目的数据包后更新 GTK 缺省情况下，GTK密钥更新采用基于时间的方法，缺省的时间间隔是86400秒
客户端离线更新GTK	启动当客户端离线时更新GTK的功能 缺省情况下，客户端离线更新GTK的功能处于关闭状态

3. crypto类型无线服务的保护管理帧功能

保护管理帧功能通过保护无线网络中的管理帧来完善无线网络的安全性。保护管理帧的标准是建立在 802.11i 的框架上的。802.11w 保护的管理帧包括解除认证帧，解除关联帧和部分强壮 Action 帧。

对于单播管理帧，保护管理帧功能仍旧使用数据帧的成对临时密钥对单播管理帧进行加密，保证单播管理帧的机密性、完整性以及重放保护。

对广播/组播管理帧，保护管理帧功能使用 BIP（Broadcast Integrity Protocol，广播完整性协议）保证广播/组播管理帧的完整性以及重放保护，实现防止客户端受到仿冒 AP 的攻击。但保护管理帧功能不能为广播/组播管理帧的传输提供机密性。BIP 通过在广播/组播管理帧的帧主体后增加 MME（Management MIC IE，管理 MIC IE）字段来实现保护广播/组播管理帧。

- 完整性：AP 和客户端通过四次握手或者组播握手产生 IGTK（Integrity Group Temporal Key，完整性组临时密钥），IGTK 与广播/组播管理帧的帧主体进行运算生成 MIC（Message Integrity Check，消息完整性校验），将生成的 MIC 放入 MME 字段中。客户端通过四次握手消息 3 或组播握手消息 1 收到的 IGTK，也产生 MIC，客户端将此 MIC 与从 AP 接收到的 MIC 进行比较，相同即表示广播/组播管理帧是完整的。
- 重放保护：AP 为每个 IGTK 维护一个 IPN（IGTK Packet Number，IGTK 报文序列号），通过四次握手消息 3 或者组播握手消息 1 将 IPN 初始值发送给客户端。AP 后续发送保护的广播/组播帧时，将 IPN 存放于 MME 中发送给客户端，客户端会将收到的 IPN 与本地保存的 IPN 进行比较，如果收到的 IPN 比本地保存的 IPN 增加 1，则表示客户端没有受到重放攻击。

AP 与客户端协商结果为使用保护管理帧功能后，无线设备将使用 SA Query 机制增强客户端的安全连接。SA Query 包括主动 SA Query 和被动 SA Query。

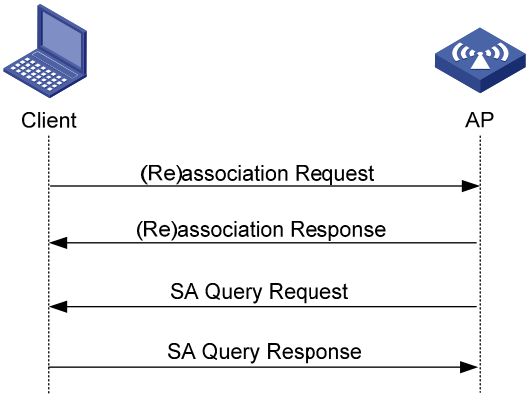
(1) 主动 SA Query

在 AP 收到仿冒的关联/重关联报文的情况下，主动 SA Query 机制可以防止 AP 对客户端作出错误的响应。

当 AP 收到客户端的关联/重关联请求，AP 将发送关联/重关联响应帧，响应状态值为“关联/重关联临时被拒绝，稍后重连”，并携带关联返回时间，随后 AP 会触发 SA Query 过程。

AP 向客户端发送 SA Query 请求帧，若 AP 在 SA Query 超时时间内收到客户端发送的 SA Query 响应帧，则 AP 认为该客户端在线。若 AP 在 SA Query 超时时间内未收到客户端的 SA Query 响应帧，AP 将再次发送 SA Query 请求帧。若 AP 在 SA Query 重试次数内收到 SA Query 响应帧，则认为客户端在线，并且在关联返回时间内，AP 将不再响应关联/重关联请求。若 AP 在 SA Query 重试次数内未收到 SA Query 响应帧，AP 将认为客户端已经掉线，允许其重新接入。

图2-11 主动 SA Query 过程

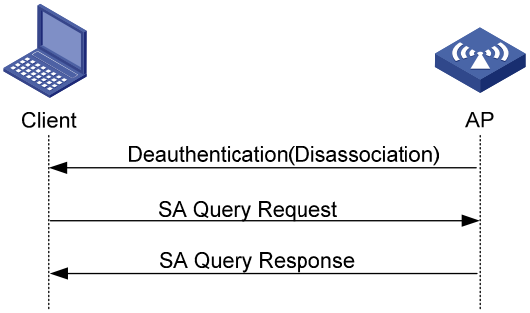


(2) 被动 SA Query

在客户端收到未加密的解除关联/解除认证报文（失败码为 6 或 7）的情况下，被动 SA Query 机制可以防止客户端异常下线。

当客户端收到一个未保护的解除关联帧或者解除认证帧，客户端会触发 SA Query 过程。客户端向 AP 发送 SA Query 请求帧，AP 回复 SA Query 响应帧。客户端收到 SA Query 响应帧，判定 AP 在线，AP 和客户端之间的连接处于正常状态，客户端不会下线。

图2-12 被动 SA Query 过程

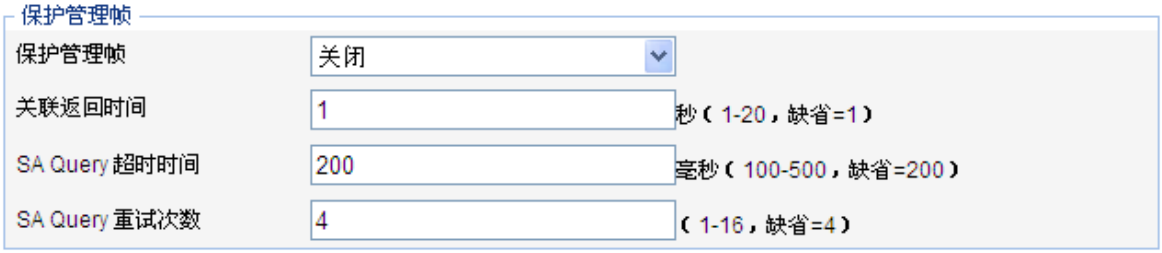


配置保护管理帧功能的步骤如下：

(3) 在界面左侧的导航栏中选择“无线服务 > 接入服务”。

(4) 在列表中找到要进行配置的 crypto 类型无线服务，单击对应的 图标，进入如下图所示页面。

图2-13 crypto 类型无线服务保护管理帧配置页面



(5) 配置 crypto 类型无线服务的保护管理帧功能，详细配置如下表所示。

(6) 单击<确定>按钮完成操作。

表2-10 crypto 类型无线服务保护管理帧的详细配置

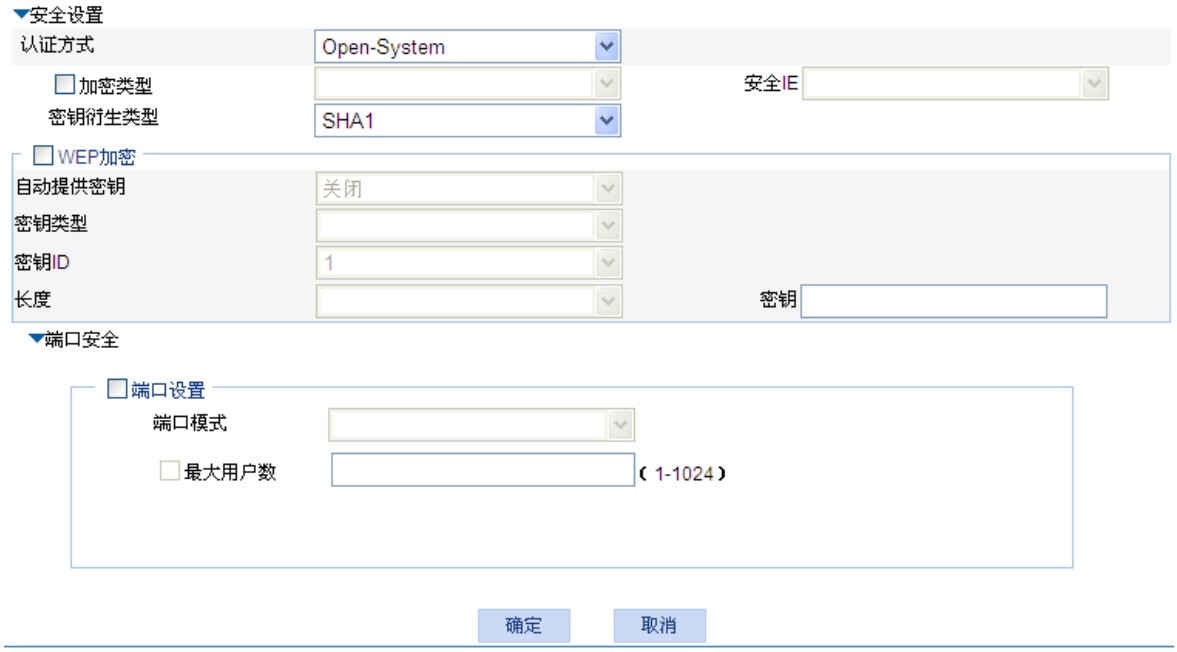
配置项	说明
保护管理帧	• 强制：开启保护管理帧功能，支持保护管理帧功能的客户端可上线，同时对通信过程中的管理帧进行保护，不支持保护管理帧功能的客户端无法上线 • 可选：开启保护管理帧功能，支持或不支持保护管理帧功能的客户端均可接入，但仅对支持保护管理帧功能的上线客户端提供保护管理帧功能，对通信过程中的的管理帧进行保护 • 关闭：关闭保护管理帧功能。支持或不支持保护管理帧功能的客户端均可上线，但不对通信过程中的的管理帧进行保护 缺省情况下，保护管理帧功能处于关闭状态 提示 使用认证类型为 PSK 或 802.1X，并且加密类型和安全 IE 为 AES、WPA2 的接入服务上才能设置保护管理帧功能
关联返回时间	• 关联返回时间，在该时间超时前，AP 不会处理客户端发送的关联/重关联请求
SA Query超时时间	SA Query超时时间，若AP在SA Query超时时间内未收到客户端的SA Query响应帧，AP将再次发送SA Query请求帧
SA Query重试次数	• AP 发送 SA Query 请求帧的重传次数

4. crypto类型无线服务安全配置

(1) 在界面左侧的导航栏中选择“无线服务 > 接入服务”。

(2) 在列表中找到要进行配置的 crypto 类型无线服务，单击对应的图标，进入如下图所示页面。

图2-14 crypto 类型无线服务安全配置页面



(3) 配置 crypto 类型无线服务安全信息，详细配置如下表所示。

(4) 单击<确定>按钮完成操作。

表2-11 crypto 类型无线服务安全配置的详细配置

配置项	说明
认证方式	链路认证方式，可选择以下几种： • Open-System：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 • Shared-Key：共享密钥认证需要客户端和设备端配置相同的共享密钥；只有在使用 WEP 加密时才可选用 shared-key 认证机制 • Open-System and Shared-Key：可以同时选择使用 Open-System 和 Shared-Key 认证 提示 WEP 加密方式可以分别和 Open system、Shared key 链路认证方式使用 • 采用 Open system authentication 方式：此时 WEP 密钥只做加密，即使密钥配置不一致，用户也可以成功建立无线链路，但所有的数据都会因为密钥不一致被接收端丢弃 • 采用 Shared key authentication 方式：此时 WEP 密钥同时作为认证密钥和加密密钥，如果密钥配置不一致，客户端就不能通过链路认证，也就无法接入无线网络
加密类型	无线服务支持加密机制： • AES：AES 加密算法 • TKIP：一种基于 RC4 算法和动态密钥管理的加密机制 • AES and TKIP：可以同时选择使用 AES 和 TKIP 加密
安全IE	无线服务类型（Beacon或者Probe response报文中携带对应的IE信息） • WPA：在 802.11i 协议之前，Wi-Fi Protected Access 定义的安全机制 • WPA2：802.11i 定义的安全机制，也就是 RSN（Robust Security Network，健壮安全网络）安全机制，提供比 WEP 和 WPA 更强的安全性 • WPA and WPA2：同时选择使用 WPA 和 WPA2
密钥衍生类型	指定由PMK（Pairwise Master Key，成对主密钥）产生PTK/GTK所使用的散列算法。目前使用的散列算法有两种，分别是SHA1和SHA256。SHA1使用HMAC-SHA1散列算法进行迭代计算产生密钥，SHA256使用HMAC-SHA256散列算法进行迭代计算产生密钥 配置密钥衍生类型： • SHA1：采用 HMAC-SHA1 散列算法 • SHA1 and SHA256：采用 HMAC-SHA1 或 HMAC-SHA256 散列算法 • SHA256：采用 HMAC-SHA256 散列算法 缺省情况下，密钥衍生类型是SHA1 提示 当认证类型为 PSK 或 802.1X 时，配置的密钥衍生类型才能生效
WEP加密	

配置项	说明
自动提供密钥	使用自动提供WEP密钥方式： • 开启：使用自动提供 WEP 密钥方式 • 关闭：使用静态 WEP 密钥方式 缺省情况下，使用静态WEP密钥方式 选择自动提供WEP密钥方式后，“密钥类型”选项会自动使用WEP 104加密方式 提示 • 自动提供 WEP 密钥方式必须和 802.1x 认证方式一起使用 • 配置动态 WEP 加密后，用来加密单播数据帧的 WEP 密钥由客户端和服务器协商产生。如果配置动态 WEP 加密的同时配置了 WEP 密钥，则该 WEP 密钥作为组播密钥，用来加密组播数据帧。如果不配置 WEP 密钥，则由设备随机生成组播密钥
密钥类型	• WEP 40：选择 WEP 40 进行加密 • WEP 104：选择 WEP 104 进行加密 • WEP 128：选择 WEP 128 进行加密
密钥ID	密钥ID用来配置密钥索引号，可选以下几种： 1：选择密钥索引为1 2：选择密钥索引为2 3：选择密钥索引为3 4：选择密钥索引为4 在WEP中有四个静态的密钥。其密钥索引分别是1、2、3和4。指定的密钥索引所对应的密钥将被用来进行帧的加密和解密
长度	选择WEP密钥长度： • 当密钥类型选择 WEP 40 时，可选的密钥长度 5 个字符（5 Alphanumeric Chars）或者 10 位 16 进制数（10 Hexadecimal Chars） • 当密钥类型选择 WEP 104 时，可选的密钥长度 13 个字符（13 Alphanumeric Chars）或者 26 位 16 进制数（26 Hexadecimal Chars） • 当密钥类型选择 WEP 128 时，可选的密钥长度 16 个字符（16 Alphanumeric Chars）或者 32 位 16 进制数（32 Hexadecimal Chars）
密钥	配置WEP密钥
端口安全	请参见表2-5 “认证方式”、“加密类型”等参数直接决定了端口模式的可选范围，具体请参见表2-14 在选则“加密类型”后，增加以下三种端口安全模式： • mac and psk：接入用户必须先进行 MAC 地址认证，通过认证后使用预先配置的预共享密钥与设备协商，协商成功后可访问端口 • psk：接入用户必须使用设备上预先配置的静态密钥，即 PSK（Pre-Shared Key，预共享密钥）与设备进行协商，协商成功后可访问端口 • userlogin-secure-ext：对接入用户采用基于 MAC 的 802.1x 认证，且允许端口下有多个 802.1x 用户

当选择 mac and psk 时，需要配置如下选项。

图2-15 mac and psk 端口安全配置页面



表2-12 mac and psk 端口安全配置的详细配置

配置项	说明
端口模式	mac and psk：接入用户必须先进行MAC地址认证，通过认证后使用预先配置的预共享密钥与设备协商，协商成功后可访问端口 在导航栏中选择“无线服务 > 接入服务”，单击<MAC认证列表>按钮，输入客户端的MAC地址
最大用户数	控制能够通过某端口接入网络的最大用户数
MAC认证	选中“MAC认证”前的复选框
域名	在下拉框中选择已存在的域 设备的缺省域为“system”。在界面左侧的导航栏中选择“认证 > AAA”，选择“域设置”页签，在域名下拉输入框中可以新建域 需要注意的是： • 在该选项中选择的域名仅对此无线服务生效，并且从该无线服务接入的客户端将被强制使用该认证域来进行认证、授权和计费 • 请不要删除使用中的域名，否则会导致正在使用此无线服务的客户端下线
预共享密钥	• pass-phrase：以字符串方式输入预共享密钥 • raw-key：以十六进制数方式输入预共享密钥

当选择 psk 时，需要配置如下选项。

图2-16 psk 端口安全配置页面

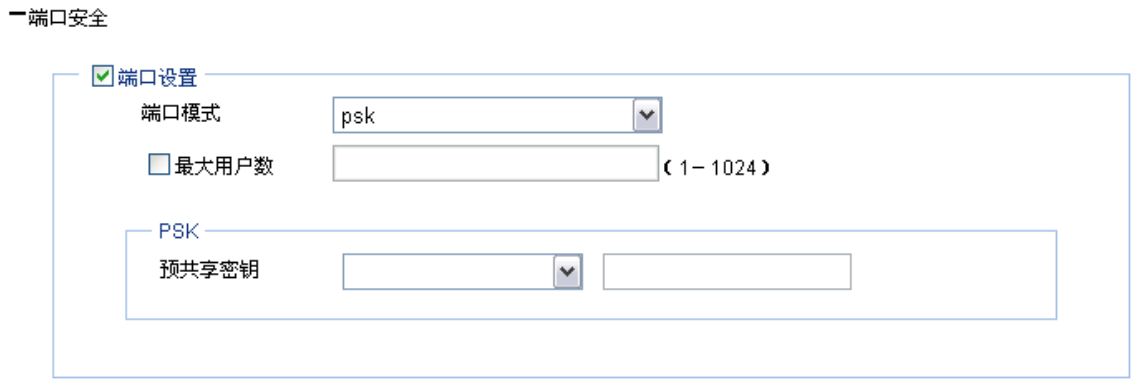


表2-13 psk 端口安全配置的详细配置

配置项	说明
端口模式	psk：接入用户必须使用设备上预先配置的静态密钥，即PSK（Pre-Shared Key，预共享密钥）与设备进行协商，协商成功后可访问端口
最大用户数	控制能够通过某端口接入网络的最大用户数
预共享密钥	• pass-phrase：以字符串方式输入预共享密钥 • raw-key：以十六进制数方式输入预共享密钥

当选择userlogin-secure-ext时，需要配置的选项如 表 2-7 所示。

5. 安全参数关系表

clear 类型和 crypto 类型无线服务类型下，各参数之间的关系如下表所示。

表2-14 安全参数关系表

服务类型	认证方式	加密类型	安全 IE	WEP 加密/密钥 ID	端口模式
clear	Open-System	不可选	不可选	不可选	mac-authentication mac-else-userlogin-secure mac-else-userlogin-secure-ext userlogin-secure userlogin-secure-ext userlogin-secure-or-mac userlogin-secure-or-mac-ext
crypto	Open-System	选择	必选	WEP加密可选/密钥ID可选1234	mac and psk psk userlogin-secure-ext
		不选择	不可选	WEP加密必选/密钥ID可选1234	mac-authentication userlogin-secure userlogin-secure-ext

服务类型	认证方式	加密类型	安全 IE	WEP 加密/密钥 ID	端口模式
	Shared-Key	不可选	不可选	WEP加密必选/密钥ID可选1234	mac-authentication
	Open-System and Shared-Key	选择	必选	WEP加密必选/密钥ID可选1234	mac and psk psk userlogin-secure-ext
		不选择	不可选	WEP加密必选/密钥ID可选1234	mac-authentication userlogin-secure userlogin-secure-ext

2.1.4 绑定AP的射频

(1) 在导航栏中选择“无线服务 > 接入服务”。

(2) 在列表里查找到需要绑定射频的无线服务，单击对应的图标，进入下图所示页面。

图2-17 绑定 AP 的射频



(3) 选中需要绑定的射频前的复选框。

(4) 单击<绑定>按钮完成操作。

2.1.5 开启无线服务

(1) 在导航栏中选择“无线服务 > 接入服务”，进入如下图所示页面。

图2-18 开启无线服务



(2) 选中需要开启的无线服务前的复选框。

(3) 单击<开启>按钮完成操作。

2.1.6 开启射频

在导航栏中选择“射频 > 射频设置”，进入射频设置页面，确认射频处于开启状态。

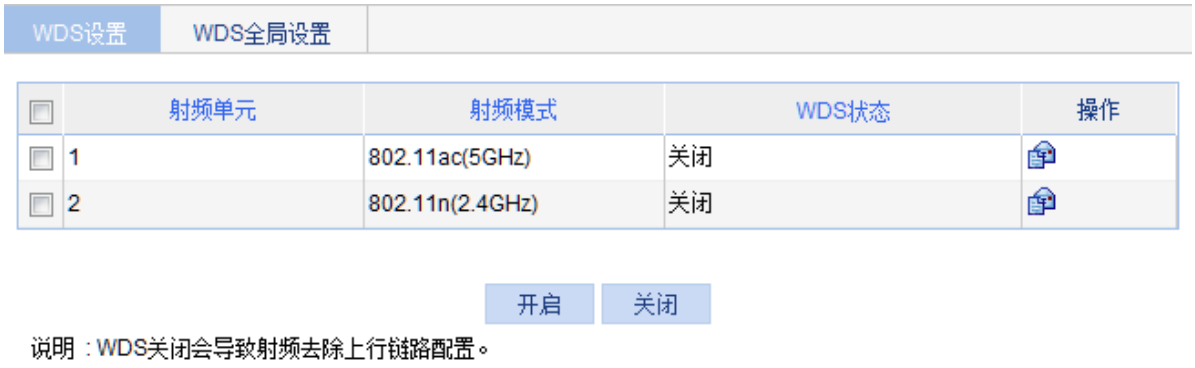
2.2 配置WDS服务

2.2.1 配置WDS服务

(1) 在界面左侧的导航栏中选择“无线服务 > WDS”。

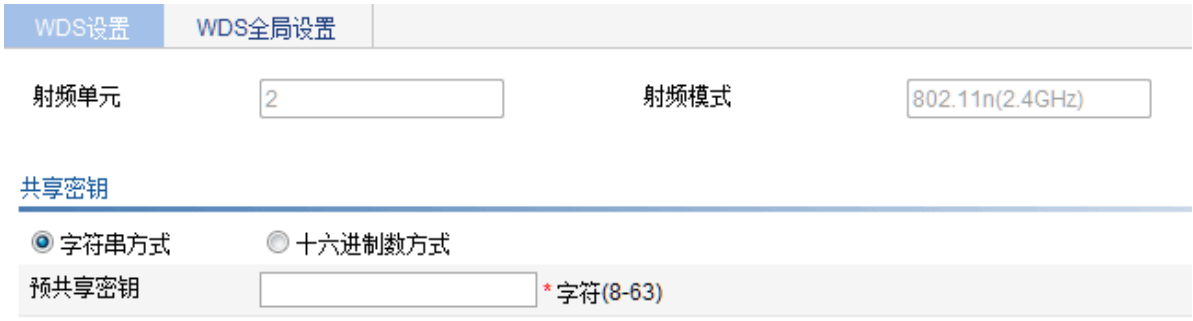
(2) 单击“WDS 设置”页签，进入如下图所示 WDS 设置页面。

图2-19 WDS 设置页面



(3) 在列表中找到要进行配置的射频模式，单击对应的图标，进入如下图所示 WDS 设置页面。

图2-20 WDS 设置页面



(4) 配置 WDS 的信息，详细配置如下表所示。

(5) 单击<确定>按钮完成操作。

表2-15 WDS 设置的详细配置

配置项	说明
射频单元	AP支持的射频号，取值为1或2。
射频模式	实际的取值与射频单元有关
字符串方式	以字符串方式输入预共享密钥
十六进制数方式	以十六进制数方式输入预共享密钥
预共享密钥	预共享密钥 • 若类型为字符串，则为 8～63 个字符的可显示字符串 • 若类型为十六进制数，则为长度是 64 位的合法十六进制数

2.2.2 配置邻居MAC地址

说明

如果不配置任何的邻居 MAC 地址，则表示该 AP 可以和任何其它 AP 建立 WDS 链路。如果设置了邻居 MAC 地址，那么该 AP 只能和这些指定的邻居 AP 建立 WDS 链路。

(1) 在导航栏中选择“无线服务 > WDS”。

(2) 在列表中找到要进行配置的射频模式，单击对应的图标，进入如下图所示配置邻居 MAC 地址。

图2-21 配置邻居 MAC 地址



(3) 在邻居 MAC 地址表项里输入 MAC 地址，单击<新建>按钮完成操作。

(4) 单击<确定>按钮完成操作。

2.2.3 配置WDS高级设置

(1) 在界面左侧的导航栏中选择“无线服务 > WDS”。

(2) 单击“WDS 设置”页签。

(3) 在列表中找到要进行配置的射频模式，单击对应的图标，进入如下图所示的 WDS 高级设置配置页面。

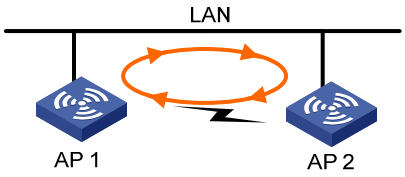
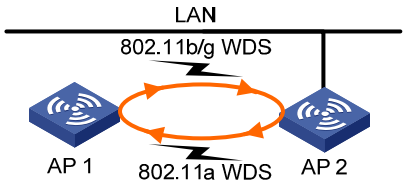
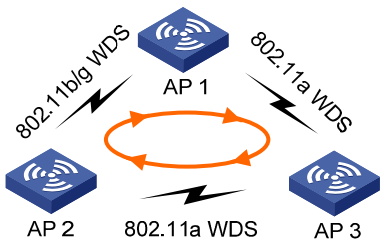
图2-22 WDS 高级设置页面



(4) 配置 WDS 高级设置选项，详细配置如下表所示。

(5) 单击<确定>按钮完成操作。

表2-16 WDS 高级设置的详细配置

配置项	说明
网桥链路标识	设置网桥链路标识，设备的缺省标识由射频模式决定
保活时间间隔	配置链路保活报文发送时间间隔
链路回程速率	配置链路回程速率
STP	WDS网络中可能存在以下环路类型：    当网络中存在环路时，可以结合STP选择性地阻塞冗余链路来消除环路，并且在WDS链路故障时还可以提供备链路备份的功能 WDS环路检测算法： • 开启：开启 WDS 环路检测 • 关闭：关闭 WDS 环路检测 缺省情况下，WDS环路检测功能处于开启状态 该配置只对当前WLAN-Mesh接口生效，全局STP（请参见“2.2.4 WDS全局设置”）对所有接口生效
最大WDS链路数	设置允许建立的最大WDS链路数 提示 在建立 WDS 时，如果在 AP 上建立的 WDS 链路大于 2 时，需要根据实际链路数进行设置

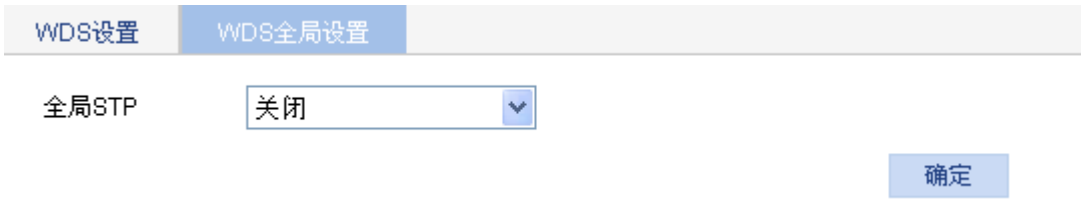
配置项	说明
链路保持RSSI	设置链路保持RSSI 用于建立和保持一条链路的最小RSSI值。一条链路的RSSI值必须不小于这个值，才能被建立和保持。因此这个值必须要保证，否则错误率会很高，链路性能会变差
速率选择方式	• 固定方式：采用的速率为固定值，其值为当前 Radio 接口速率集的最大值 • 实时更新方式：采用的速率会根据链路质量（RSSI）实时变化，即速率值随 Radio 接口下的信号强度（RSSI）而变化 缺省情况下，采用固定方式
VLAN（Tagged）	添加Tagged的VLAN ID，VLAN（Tagged）表示端口成员发送该VLAN报文时带Tag标签
VLAN（Untagged）	添加Untagged的VLAN ID，VLAN（Untagged）表示端口成员发送该VLAN报文时不带Tag标签
缺省VLAN	设置端口的缺省VLAN 在缺省情况下，所有端口的缺省VLAN均为VLAN 1，设置新的缺省VLAN后，VLAN 1为Untagged的VLAN ID
排除下列VLAN	删除已有Tagged和Untagged的VLAN ID

2.2.4 WDS全局设置

(1) 在界面左侧的导航栏中选择“无线服务 > WDS”。

(2) 单击“WDS 全局设置”页签，进入如下图所示 WDS 全局设置页面。

图2-23 WDS 基本设置页面



(3) 配置 WDS 全局设置，详细配置如下表所示。

(4) 单击<确定>按钮完成操作。

表2-17 WDS 全局设置的详细配置

配置项	说明
全局STP	• 开启：全局 STP 处于开启状态 • 关闭：全局 STP 处于关闭状态 缺省情况下，全局STP处于关闭状态

2.2.5 配置信道

可以通过以下两种方式完成 WDS 的信道配置：

- 手工指定信道：需要为 AP 之间的 WDS 链路手工指定射频的工作信道，并且在两个 AP 上配置的工作信道必须保持一致。
- 自动信道选择：AP 上配置信道为 auto 方式，AP 间的射频建立 WDS 链接时，自动协商工作信道。

说明

- 无论是手工指定信道或是使用自动信道选择方式配置 WDS 的工作信道，只要有 AP 在工作信道上检测到雷达信号，该 AP 和与其建立 WDS 链路的其它所有 AP 都会将工作信道切换到其它可用信道上。
- 部分国家 802.11a 频段的可用信道大部分为雷达信道，因此如果要在 802.11a 频段上建立 WDS 链路，建议为 AP 配置使用自动信道选择方式建立 WDS 网络。
- 选择自动信道选择方式时，在没有建立 WDS 链接时，会自动选择一个临时工作信道。临时工作信道的有效时间为 10～20 秒。临时工作信道超时后，射频切换回 auto 信道，再重新选择新的临时工作信道。射频在 auto 信道和临时工作信道间的切换信息会保存在射频的信道切换记录中。

2.2.6 开启WDS服务

(1) 在界面左侧的导航栏中选择“无线服务 > WDS”。

(2) 单击“WDS 设置”页签，进入如下图所示 WDS 设置配置页面。

图2-24 开启 WDS 服务



(3) 选中需要开启 WDS 的射频前的复选框。

(4) 单击<开启>按钮完成操作。

2.3 配置Repeater服务

说明

使用 Repeater 服务，需要在 AP 的一个射频上同时配置 WDS 和无线接入服务，且必须将该射频配置为使用固定信道。

配置 Repeater 服务需要在 AP 的一个射频上同时配置 WDS 和无线接入服务：

- 为Repeater配置接入服务的相关配置请参见“2.1 配置接入服务”。
- 为Repeater配置WDS的相关配置请参见“2.2 配置WDS服务”。

配置成功后，在界面左侧的导航栏中选择“概览 > 射频”，在如下图所示页面中的“服务类型”中可以看到 Repeater 上的 802.11n 射频模式会显示该射频同时提供“接入”和“WDS”。

图2-25 Repeater 模式



说明

使用 Repeater 服务，需要在 AP 的一个射频上同时配置 WDS 和无线接入服务，且必须将该射频配置为使用固定信道。

2.4 无线接入配置举例

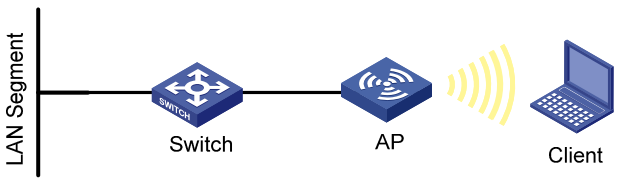
2.4.1 无线服务典型配置举例

1. 组网需求

某部门为了保证工作人员可以随时随地访问部门内部的网络资源，需要通过部署 AP 实现移动办公。具体要求如下：

- AP 提供 SSID 为 service1 的明文方式的无线接入服务。
- 采用目前较为常用的 802.11n 射频模式。

图2-26 无线服务组网图



2. 配置AP

(1) 配置 FAT AP 的接口 IP 地址

在 FAT AP 上创建 VLAN（在导航栏中选择“网络 > VLAN”，进入页面后可以创建 VLAN），并配置 IP 地址（在导航栏中选择 “设备 > 接口管理”，进入页面后可以配置 VLAN 的 IP 地址）。

(2) 配置无线服务

步骤 1：在导航栏中选择“无线服务 > 接入服务”。

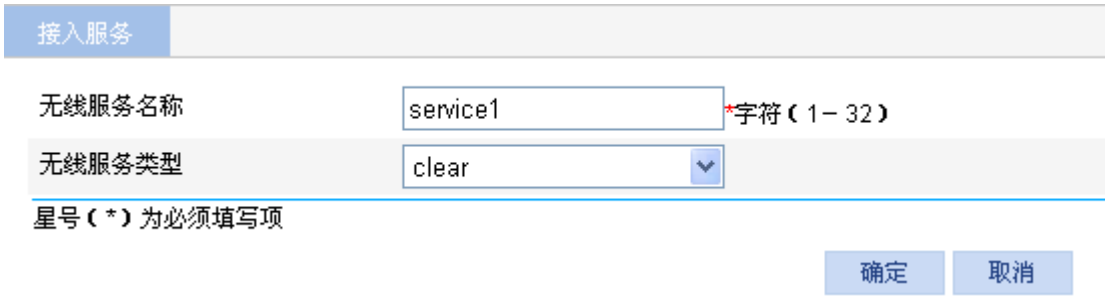
步骤 2：单击<新建>按钮，进入无线服务新建页面。

步骤 3：进行如下配置，如下图所示。

- 设置无线服务名称为“service1”。
- 选择无线服务类型为“clear”。

步骤 4：单击<确定>按钮完成操作。

图2-27 创建无线服务



(3) 绑定 AP 的射频

步骤 1：在导航栏中选择“无线服务 > 接入服务”。

步骤 2：单击无线服务“service1”对应的图标，进入如下图所示页面。

步骤 3：选中“802.11n”前的复选框

步骤 4：单击<绑定>按钮完成操作。

图2-28 绑定 AP 的射频



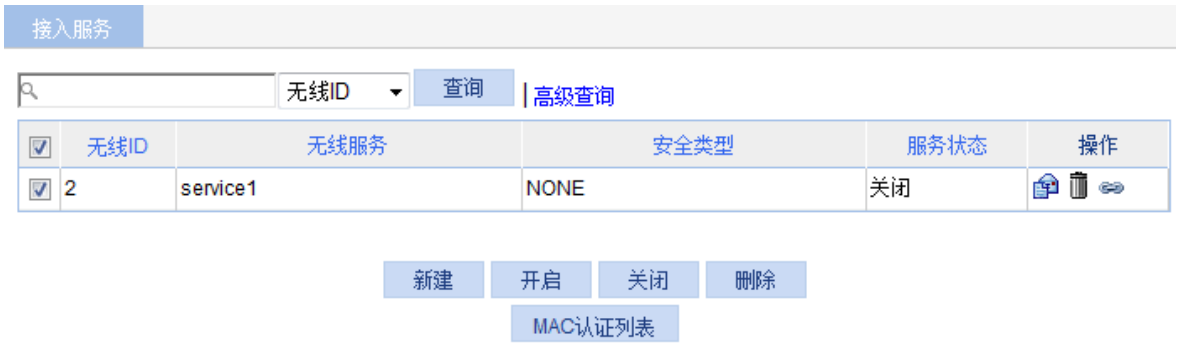
(4) 开启无线服务

步骤 1：在导航栏中选择“无线服务 > 接入服务”，进入如下图所示页面。

步骤 2：选中“service1”前的复选框。

步骤 3：单击<开启>按钮完成操作。

图2-29 开启无线服务



(5) 开启 802.11n 射频（缺省情况下，802.11n 处于开启状态，此步骤可选）

在导航栏中选择“射频 > 射频设置”，进入下图所示射频设置页面，确认 802.11n 处于开启状态。

图2-30 开启 802.11n 射频



3. 验证配置结果

(1) 客户端可以成功关联 AP，并且可以访问无线网络。

(2) 在导航栏中选择“概览 > 客户端”，进入如下图所示页面，可以查看到成功上线的客户端。

图2-31 查看成功上线的客户端



4. 配置注意事项

配置无线服务需注意如下事项：

- 选择正确的区域码。
- 确认射频单元处于开启状态。

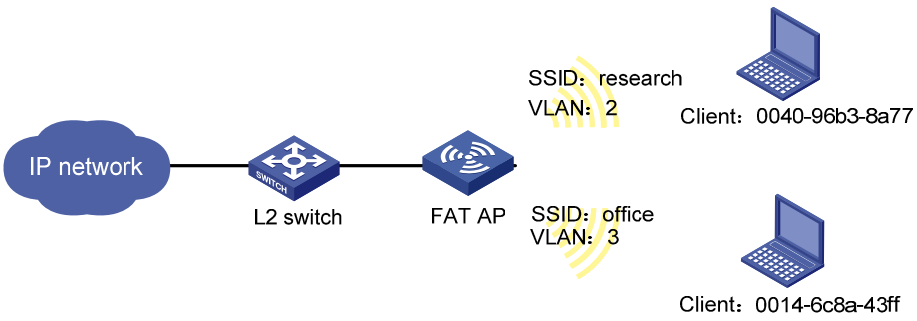
2.4.2 基于接入服务的VLAN配置举例

1. 组网需求

AP 可以同时支持多个无线接入服务，不但无线接入服务可以采用不同的无线安全策略，而且可以把将无线接入服务绑定到不同 VLAN 中，实现无线接入用户的隔离。本例要求如下：

- 建立一个名为“research”的无线接入服务，使用 PSK 认证方式，所有接入该无线网络的客户端都在 VLAN 2 中。
- 建立一个名为“office”的无线接入服务，使用明文接入方式，所有接入该无线网络的客户端都在 VLAN 3 中。

图2-32 基于接入服务的 VLAN 拓扑图



2. 配置AP

(1) 配置 FAT AP 的接口

- 配置 FAT AP 的接口 IP 地址：在 FAT AP 上创建 VLAN（在导航栏中选择“网络 > VLAN”，进入页面后可以创建 VLAN），并配置 IP 地址（在导航栏中选择 “设备 > 接口管理”，进入页面后可以配置 VLAN 的 IP 地址）。
- 配置 FAT AP 的以太网接口链路类型配置为 Trunk，并允许 VLAN 2 和 VLAN 3 的报文通过。（具体的配置步骤请参见“网络”模块中的“VLAN”。）

(2) 配置名为 research 的无线服务

步骤 1：在导航栏中选择“无线服务 > 接入服务”。

步骤 2：单击<新建>按钮，进入无线服务新建页面。

步骤 3：进行如下配置，如下图所示。

- 设置无线服务名称为“research”。
- 选择无线服务类型为“crypto”。

步骤 4：单击<确定>按钮完成操作。

步骤 5：创建无线服务后，直接进入配置无线服务界面，进行 VLAN 设置（请先通过“网络 > VLAN”，新建 VLAN 2）。

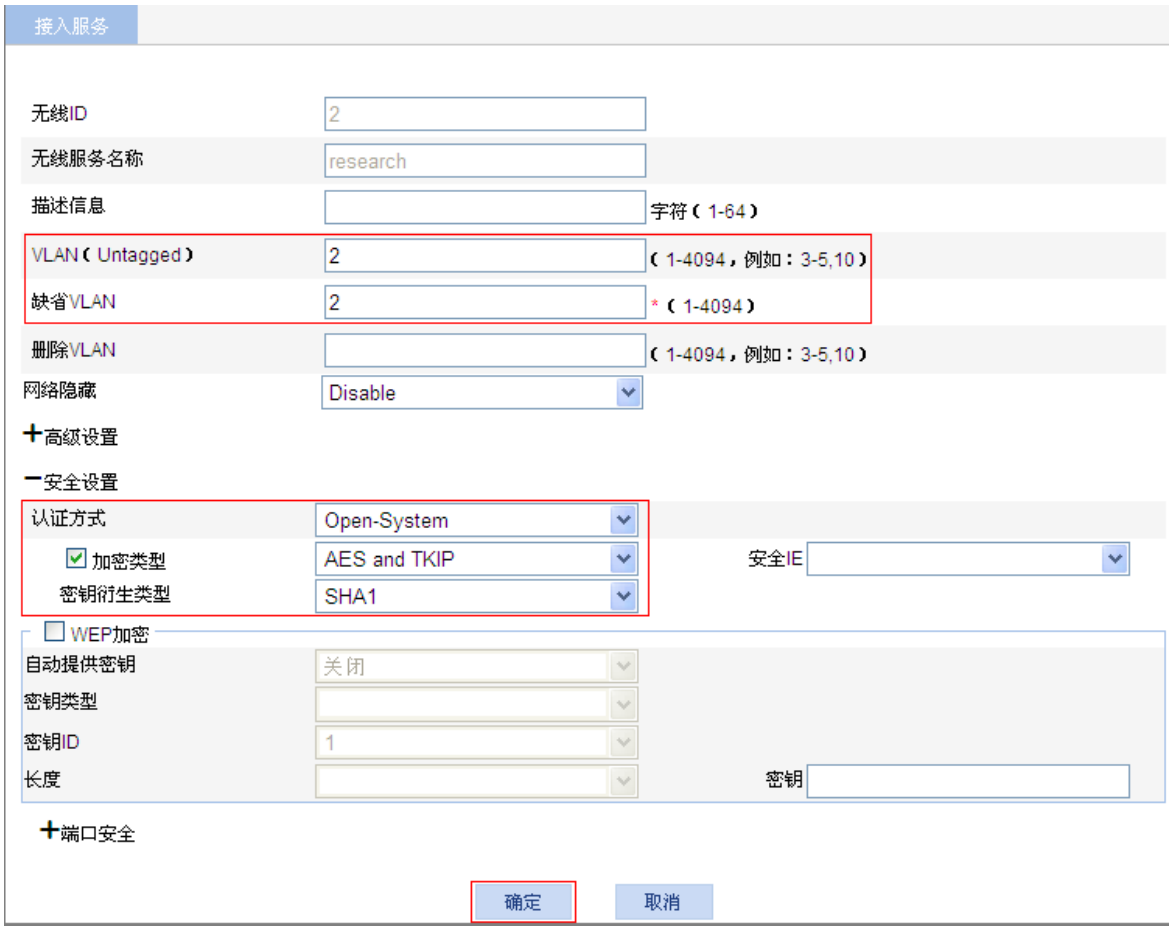
步骤 6：进行如下配置，如下图所示。

- 设置 VLAN（Untagged）为“2”。
- 设置缺省 VLAN 为“2”。
- 设置删除 VLAN 为“1”。

步骤 7：进入安全设置，勾选“加密类型”，选择“AES and TKIP”。

步骤 8：单击<确定>按钮完成操作。

图2-33 设置 VLAN



说明

PSK认证的相关配置请参见“2.4.3 WPA-PSK认证典型配置举例”，可以完全参照相关举例完成配置。

(3) 配置名为 office 的无线服务

步骤 1：在导航栏中选择“无线服务 > 接入服务”。

步骤 2：单击<新建>按钮，进入无线服务新建页面。

步骤 3：进行如下配置，如下图所示。

- 设置无线服务名称为“office”。
- 选择无线服务类型为“clear”。

步骤 4：单击<确定>按钮完成操作。

步骤 5：创建无线服务后，直接进入配置无线服务界面，配置 VLAN（请先通过“网络 > VLAN”，新建 VLAN 3）。

步骤 6：进行如下配置，如下图所示。

- 设置 VLAN（Untagged）为“3”。

- 设置缺省 VLAN 为“3”。
- 设置删除 VLAN 为“1”。

步骤 7：单击<确定>按钮完成操作。

图2-34 设置 VLAN



说明

无线接入的相关配置请参见“2.2 无线服务典型配置举例”，可以完全参照相关举例完成配置。

3. 验证配置结果

(1) 客户端可以成功关联 AP，并且可以访问无线网络。

(2) 在导航栏中选择“概览 > 客户端”，进入如下图所示页面，可以查看到成功上线的客户端。

图2-35 查看成功上线的客户端



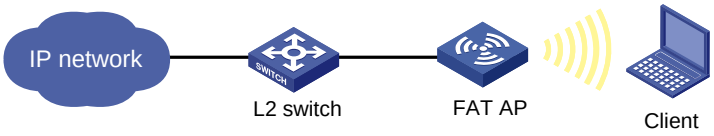
通过该页面可知，接入 SSID 为 office 的客户端 984b-4ad4-3f24 加入 VLAN 3，接入 SSID 为 research 的客户端 984b-4ad4-3fd4 加入 VLAN 2，两个客户端不在同一 VLAN，相互不能访问。

2.4.3 WPA-PSK认证典型配置举例

1. 组网需求

要求客户端使用WPA-PSK方式接入无线网络，客户端的PSK密钥配置与AP端相同，为12345678。

图2-36 WPA-PSK认证配置组网图



2. 配置AP

(1) 配置FAT AP的接口IP地址

在FAT AP上创建VLAN（在导航栏中选择“网络 > VLAN”，进入页面后可以创建VLAN），并配置IP地址（在导航栏中选择 “设备 > 接口管理”，进入页面后可以配置VLAN的IP地址）。

(2) 配置无线服务

步骤1：在导航栏中选择“无线服务 > 接入服务”。

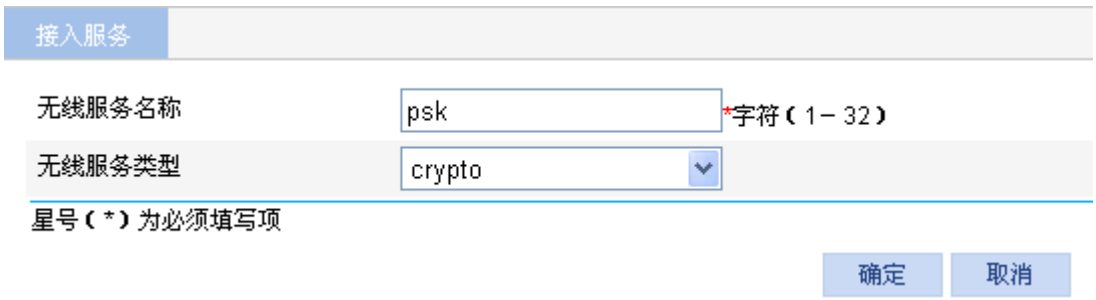
步骤2：单击<新建>按钮，进入无线服务新建页面。

步骤3：进行如下配置，如下图所示。

- 设置无线服务名称为“psk”。
- 选择无线服务类型为“crypto”。

步骤4：单击<确定>按钮完成操作。

图2-37 创建无线服务



(3) 配置PSK认证

创建无线服务后，直接进入配置无线服务界面。

步骤1：PSK认证需要对“安全设置”部分进行如下配置，如下图所示。

- 在“认证方式”下拉框中选择“Open-System”。
- 选中“加密类型”前的复选框，选择“TKIP”加密类型（请根据实际情况，选择需要的加密类型），选择“WPA”安全IE。
- 选中“端口设置”前的复选框，在端口模式的下拉框中选择“psk”方式。
- 在PSK预共享密钥下拉框里选择“pass-phrase”，输入密钥“12345678”。

步骤 2：单击<确定>按钮完成操作。

图2-38 安全设置



(4) 绑定 AP 的射频

步骤 1：在导航栏中选择“无线服务 > 接入服务”。

步骤 2：单击无线服务“psk”对应的图标，进入如下图所示页面。

步骤 3：选中“802.11n”前的复选框。

步骤 4：单击<绑定>按钮完成操作。

图2-39 绑定 AP 的射频



(5) 开启无线服务

步骤 1：在导航栏中选择“无线服务 > 接入服务”，进入如下图所示页面。

步骤 2：选中“psk”前的复选框。

步骤 3：单击<开启>按钮完成操作。

图2-40 开启无线服务



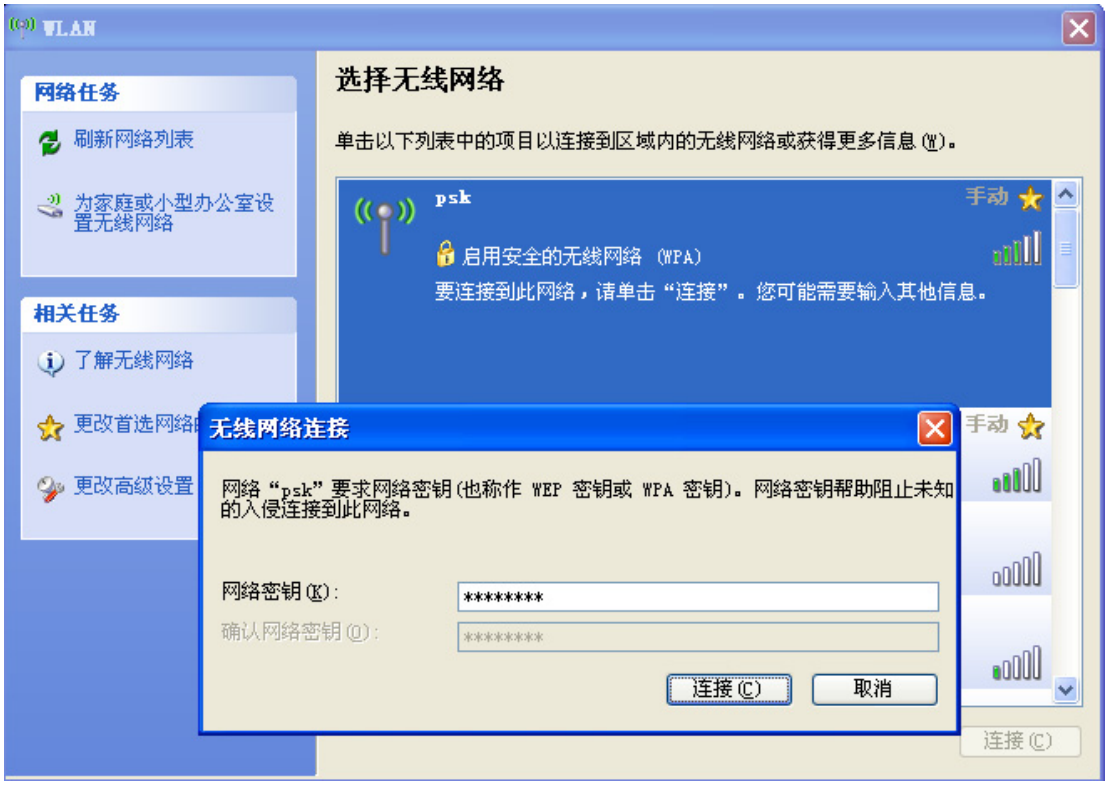
(6) 开启 802.11n 射频（缺省情况下，802.11n 处于开启状态，此步骤可选）

在导航栏中选择“射频 > 射频设置”，进入射频设置页面，确认 802.11n 处于开启状态。

3. 配置无线客户端

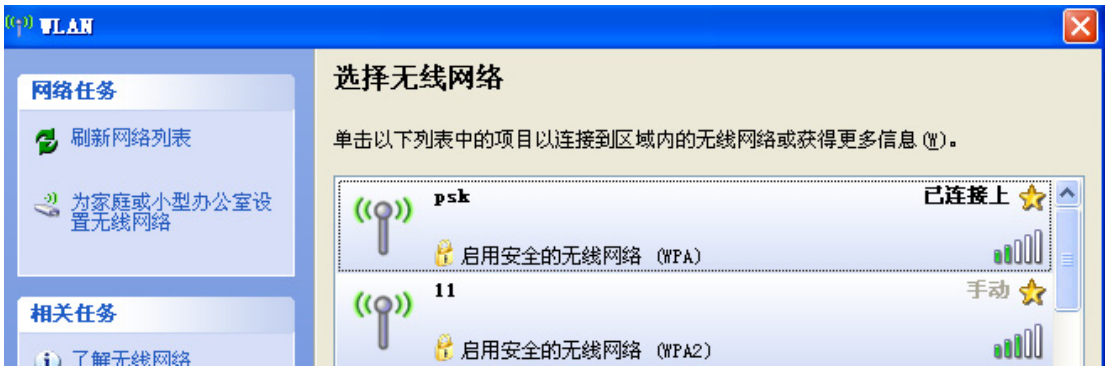
打开无线客户端，刷新网络列表，在“选择无线网络”列表里找到配置的网络服务（此例中为 psk），单击<连接>，在弹出的对话框里输入网络密钥（此例中为 12345678），整个过程如下图所示。

图2-41 配置无线客户端



客户端配置相同的 PSK 预共享密钥，客户端可以成功关联 AP。

图2-42 客户端成功关联 AP



4. 验证配置结果

(1) 客户端可以成功关联 AP，并且可以访问无线网络。

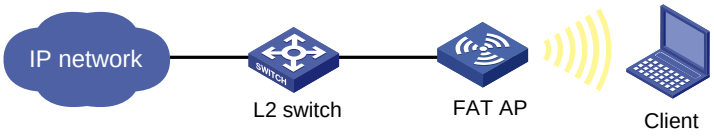
(2) 在导航栏中选择“概览 > 客户端”，可以查看到成功上线的客户端。

2.4.4 MAC地址本地认证配置举例

1. 组网需求

要求使用客户端使用 MAC 地址本地认证方式接入无线网络。

图2-43 MAC 地址本地认证配置组网图



2. 配置AP

(1) 配置 FAT AP 的接口 IP 地址

在 FAT AP 上创建 VLAN（在导航栏中选择“网络 > VLAN”，进入页面后可以创建 VLAN），并配置 IP 地址（在导航栏中选择 “设备 > 接口管理”，进入页面后可以配置 VLAN 的 IP 地址）。

(2) 配置无线服务

步骤 1：在导航栏中选择“无线服务 > 接入服务”。

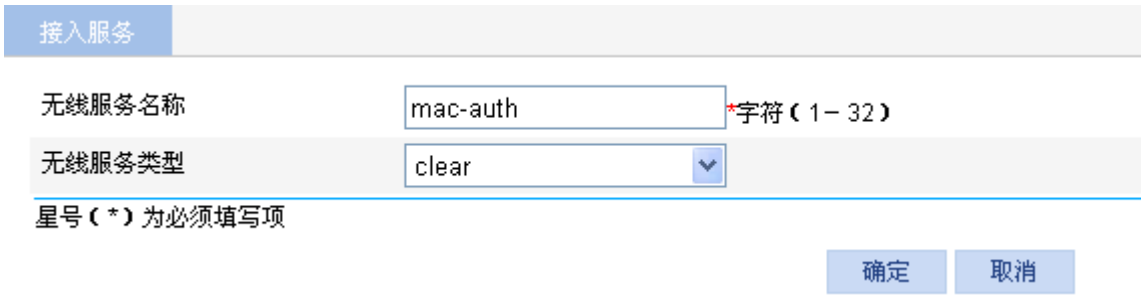
步骤 2：单击<新建>按钮，进入无线服务新建页面。

步骤 3：进行如下配置，如下图所示。

- 设置无线服务名称为“mac-auth”。
- 选择无线服务类型为“clear”。

步骤 4：单击<确定>按钮完成操作。

图2-44 创建无线服务



(3) 配置 MAC 地址本地认证

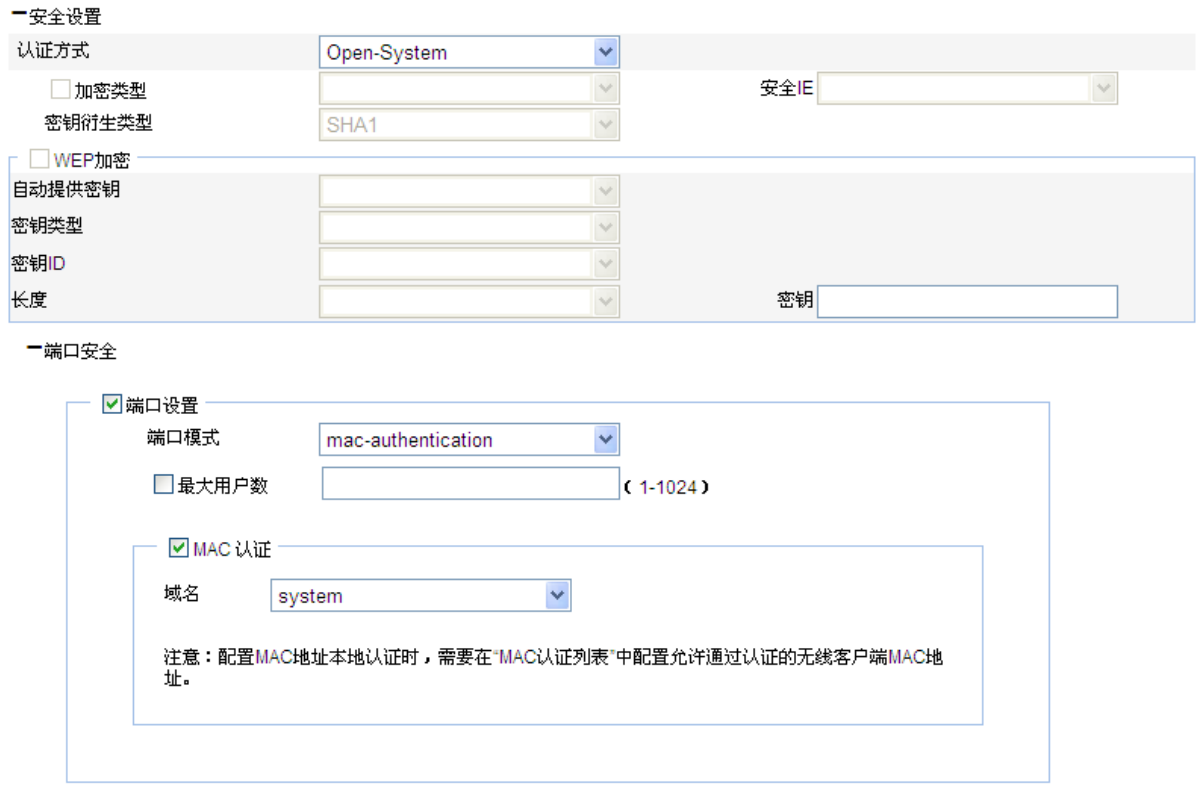
创建无线服务后，直接进入配置无线服务界面。

步骤 1：MAC 地址本地认证需要在“安全设置”部分进行如下配置，如下图所示。

- 在“认证方式”下拉框中选择“Open-System”。
- 选中“端口设置”前的复选框，在端口模式的下拉框中选择“mac-authentication”方式。
- 选中“MAC 认证”前的复选框，在域名下拉框中选择“system”（在界面左侧的导航栏中选择“认证 > AAA”，选择“域设置”页签，在域名下拉输入框中可以创建新的域）。

步骤 2：单击<确定>按钮完成操作。

图2-45 安全设置



(4) 绑定 AP 的射频

步骤 1：在导航栏中选择“无线服务 > 接入服务”。

步骤 2：单击无线服务“mac-auth”对应的图标，进入如下图所示页面。

步骤 3：选中“802.11n”前的复选框。

步骤 4：单击<绑定>按钮完成操作。

图2-46 绑定 AP 的射频



(5) 开启无线服务

步骤 1：在导航栏中选择“无线服务 > 接入服务”，进入如下图所示页面。

步骤 2：选中“mac-auth”前的复选框。

步骤 3：单击<开启>按钮完成操作。

图2-47 开启无线服务



(6) 配置 MAC 认证列表

步骤 1：在导航栏中选择“无线服务 > 接入服务”。

步骤 2：单击<MAC 认证列表>按钮。

步骤 3：进入如下图所示页面，在 MAC 地址栏里添加本地接入用户，本例中为“00-14-6c-8a-43-ff”。

步骤 4：单击<新建>按钮完成操作。

图2-48 添加 MAC 认证列表



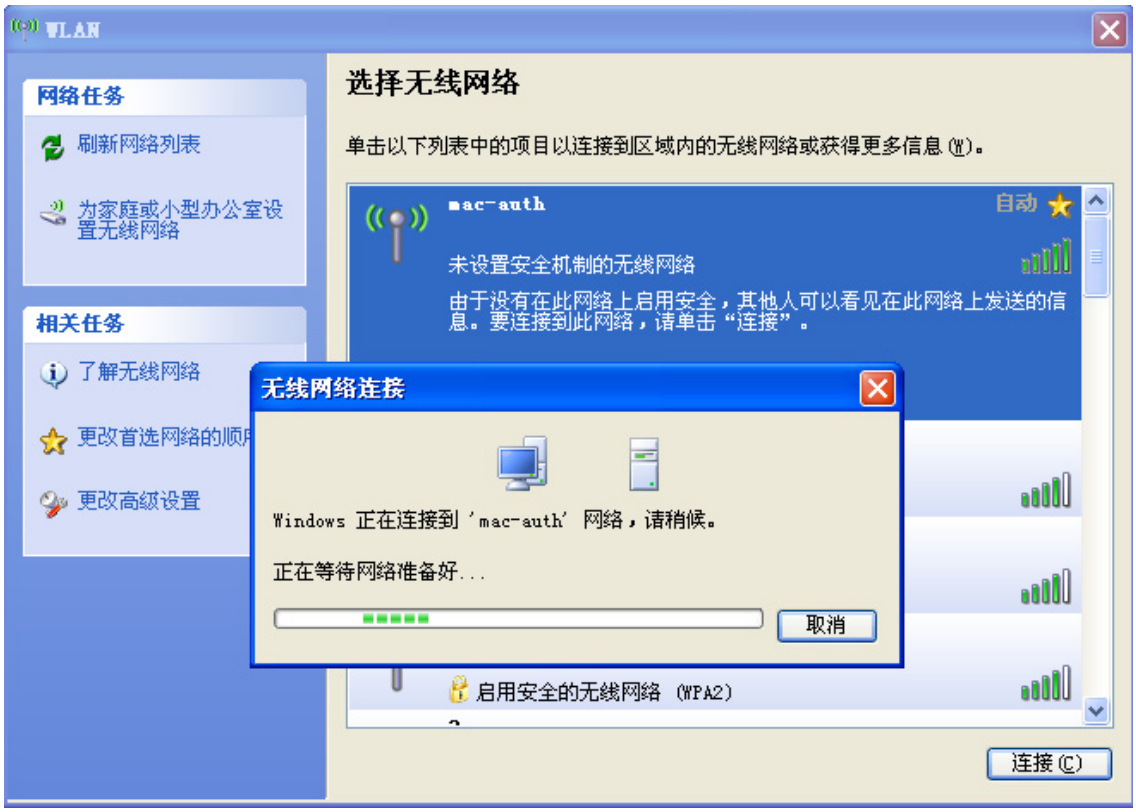
(7) 开启 802.11n 射频（缺省情况下，802.11n 处于开启状态，此步骤可选）

在导航栏中选择“射频 > 射频设置”，进入射频设置页面，确认 802.11n 处于开启状态。

3. 配置无线客户端

打开无线客户端，刷新网络列表，在“选择无线网络”列表里找到配置的网络服务（此例中为 mac-auth），单击<连接>按钮。

图2-49 配置无线客户端



4. 验证配置结果

(1) 客户端可以成功关联 AP，并且可以访问无线网络。

(2) 在导航栏中选择“概览 > 客户端”，可以查看到成功上线的客户端。

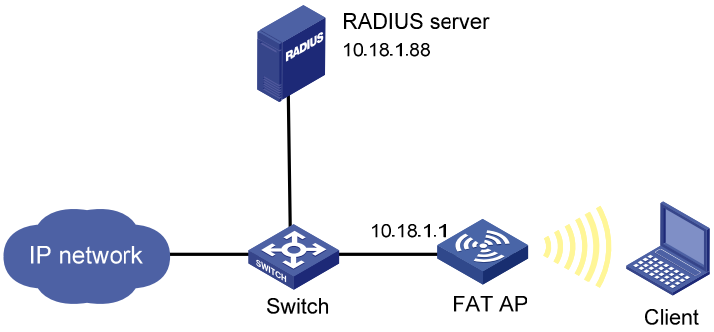
2.4.5 远程MAC地址认证配置举例

1. 组网需求

要求使用无线客户端使用远程 MAC 地址认证方式接入无线网络。

- 一台 RADIUS 服务器（使用 CAMS/iMC 服务器，担当认证、授权、计费服务器的职责）。在 RADIUS 服务器上已经添加了 Client 的用户名和密码(用户名和密码为 Client 的 MAC 地址)，同时设置了与 AP 交互报文时的共享密钥为“expert”，RADIUS 服务器 IP 地址为 10.18.1.88。
- AP 的 IP 地址为 10.18.1.1。AP 与认证、授权、计费 RADIUS 服务器交互报文时的共享密钥均为 expert，发送给 RADIUS 服务器的用户名中不带域名。

图2-50 远程 MAC 地址认证配置组网图



2. 配置AP

(1) 配置 FAT AP 的接口 IP 地址

在 FAT AP 上创建 VLAN（在导航栏中选择“网络 > VLAN”，进入页面后可以创建 VLAN），并配置 IP 地址（在导航栏中选择 “设备 > 接口管理”，进入页面后可以配置 VLAN 的 IP 地址）。

(2) 配置 RADIUS 方案

步骤 1：在导航栏中选择“认证 > RADIUS”。

步骤 2：单击<新建>按钮，进入 RADIUS 方案配置页面。

步骤 3：进行如下配置，如下图所示。

- 在RADIUS服务器配置中增加如 图 2-51 所示的两个服务器，其中密钥为“expert”。
- 输入方案名称为“mac-auth”。
- 选择服务类型为“Extended”。
- 选择用户名格式为“不带域名”。

步骤 4：单击<确定>按钮完成操作。

图2-51 配置 RADIUS



(3) 配置 AAA

步骤 1：创建 ISP 域。在导航栏中选择“认证 > AAA”，默认进入“域设置”页签的页面，本例使用缺省的 system 域（如果需要定制 ISP 域，可以创建新的 ISP 域）。

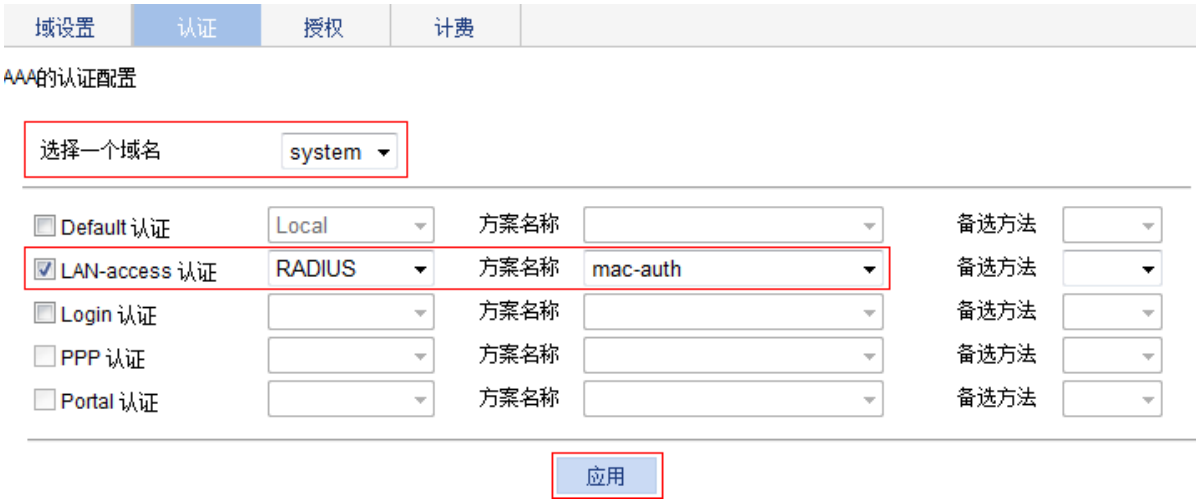
步骤 2：配置 ISP 域的 AAA 认证方案。单击“认证”页签。

步骤 3：进行如下配置，如下图所示。

- 选择域名为“system”。
- 选中“LAN-access 认证”前的复选框，选择认证方式为“RADIUS”。
- 选择认证方案名称为“mac-auth”。

步骤 4：单击<应用>按钮完成操作。

图2-52 配置 ISP 域的 AAA 认证方案



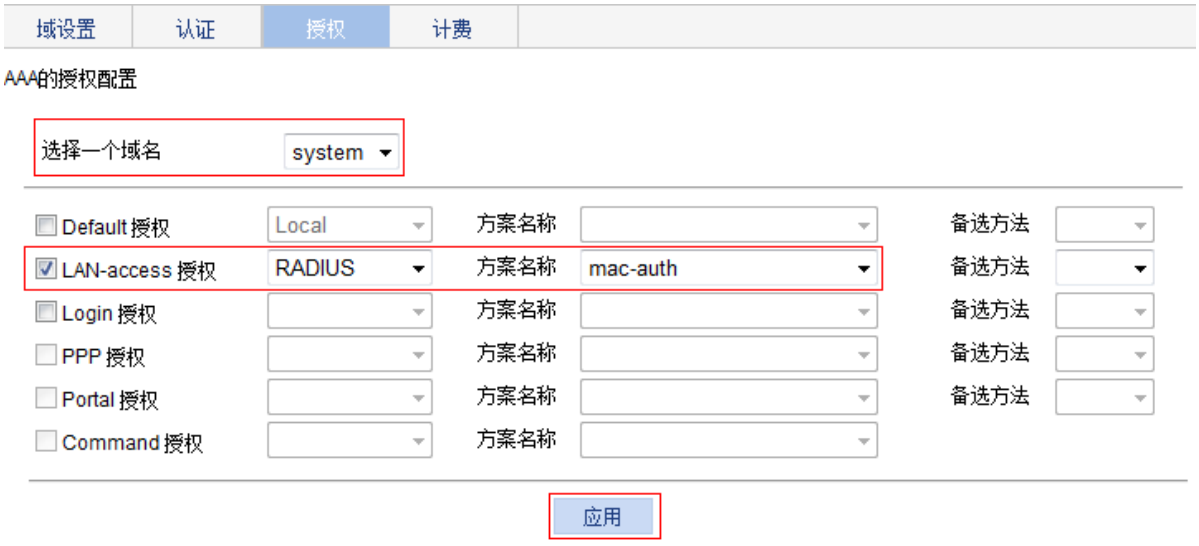
步骤 5：配置 ISP 域的 AAA 授权方案。单击“授权”页签，

步骤 6：进行如下配置，如下图所示。

- 选择域名为“system”。
- 选中“LAN-access 授权”前的复选框，选择授权方式为“RADIUS”。
- 选择授权方案名称为“mac-auth”。

步骤 7：单击<应用>按钮完成操作。

图2-53 配置 ISP 域的 AAA 授权方案



步骤 8：配置 ISP 域的 AAA 计费方案。单击“计费”页签。

步骤 9：进行如下配置，如下图所示。

- 选择域名为“system”。
- 选中“计费可选开关”前的复选框，选择“Enable”。
- 选中“LAN-access 计费”前的复选框，选择计费方式为“RADIUS”。

- 选择计费方案名称为“mac-auth”。

步骤 10：单击<应用>按钮完成操作。

图2-54 配置 ISP 域的 AAA 计费方案



(4) 配置无线服务

步骤 1：在导航栏中选择“无线服务 > 接入服务”。

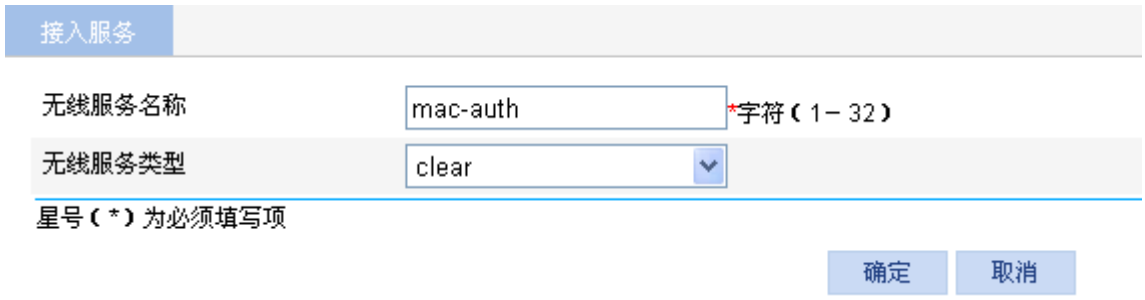
步骤 2：单击<新建>按钮，进入无线服务新建页面。

步骤 3：进行如下配置，如下图所示。

- 设置无线服务名称为“mac-auth”。
- 选择无线服务类型为“clear”。

步骤 4：单击<确定>按钮完成操作。

图2-55 创建无线服务



(5) 配置 MAC 地址认证

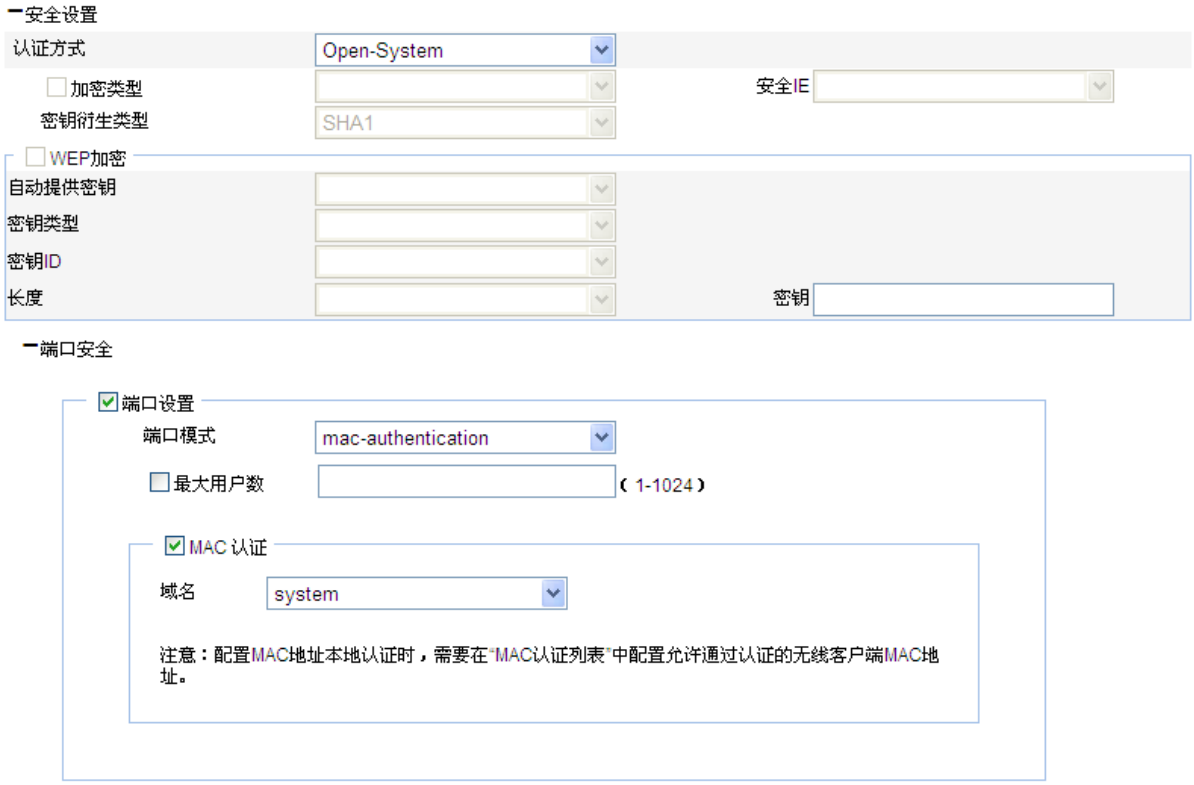
创建无线服务后，直接进入配置无线服务界面。

步骤 1：配置 MAC 地址本地认证需要在“安全设置”部分进行如下配置，如下图所示。

- 在“认证方式”下拉框中选择“Open-System”。
- 选中“端口设置”前的复选框，在端口模式的下拉框中选择“mac-authentication”方式。
- 选中“MAC 认证”前的复选框，在域名下拉框中选择“system”。

步骤 2：单击<确定>按钮完成操作。

图2-56 安全设置



(6) 绑定 AP 的射频

步骤 1：在导航栏中选择“无线服务 > 接入服务”。

步骤 2：单击无线服务“mac-auth”对应的图标，进入如下图所示页面。

步骤 3：选中“802.11n”前的复选框

步骤 4：单击<绑定>按钮完成操作。

图2-57 绑定 AP 的射频



(7) 开启无线服务

步骤 1：在导航栏中选择“无线服务 > 接入服务”，进入如下图所示页面。

步骤 2：选中“mac-auth”前的复选框。

步骤 3：单击<开启>按钮完成操作。

图2-58 开启无线服务



(8) 开启 802.11n 射频（缺省情况下，802.11n 处于开启状态，此步骤可选）

在导航栏中选择“射频 > 射频设置”，进入射频设置页面，确认 802.11n 处于开启状态。

3. 配置RADIUS server（iMC V3）

说明

下面以 iMC 为例（使用 iMC 版本为：iMC PLAT 3.20-R2602、iMC UAM 3.60-E6102），说明 RADIUS server 的基本配置。

(1) 增加接入设备

步骤 1：在 iMC 管理平台选择“业务”页签。

步骤 2：单击导航树中的“接入业务 > 接入设备配置”菜单项，进入接入设备配置页面。

步骤 3：在接入设备页面中单击<增加>按钮，进入增加接入设备页面。

步骤 4：进行如下配置，如下图所示。

- 设置认证、计费共享密钥为 expert；
- 设置认证及计费的端口号分别为 1812 和 1813；
- 选择协议类型为 LAN 接入业务；
- 选择接入设备类型为 H3C；
- 选择或手工增加接入设备，添加 IP 地址为 10.18.1.1 的接入设备。

步骤 5：单击<确定>按钮完成操作。

图2-59 增加接入设备



(2) 增加服务配置

步骤 1：选择“业务”页签。

步骤 2：单击导航树中的“接入业务 > 服务配置管理”菜单项，进入增加服务配置页面。

步骤 3：在服务配置页面中单击<增加>按钮，进入增加接入设备页面。

步骤 4：设置服务名为 mac，其他保持缺省配置。

步骤 5：单击<确定>按钮完成操作。

图2-60 增加服务配置页面



(3) 增加接入用户

步骤 1：选择“用户”页签。

步骤 2：单击导航树中的“接入用户视图 > 所有接入用户”菜单项，进入用户页面。

步骤 3：在该页面中单击<增加>按钮，进入增加接入用户页面。

步骤 4：进行如下配置，如下图所示。

- 添加用户名 00146c8a43ff；
- 添加帐号名和密码为 00146c8a43ff；
- 选中刚才配置的服务 mac。

步骤 5：单击<确定>按钮完成操作。

图2-61 增加接入用户



4. 配置RADIUS server（iMC V5）

说明

下面以 iMC 为例（使用 iMC 版本为：iMC PLAT 5.0、iMC UAM 5.0），说明 RADIUS server 的基本配置。

(1) 增加接入设备

步骤 1：在 iMC 管理平台选择“业务”页签。

步骤 2：单击导航树中的“接入业务 > 接入设备配置”菜单项，进入接入设备配置页面。

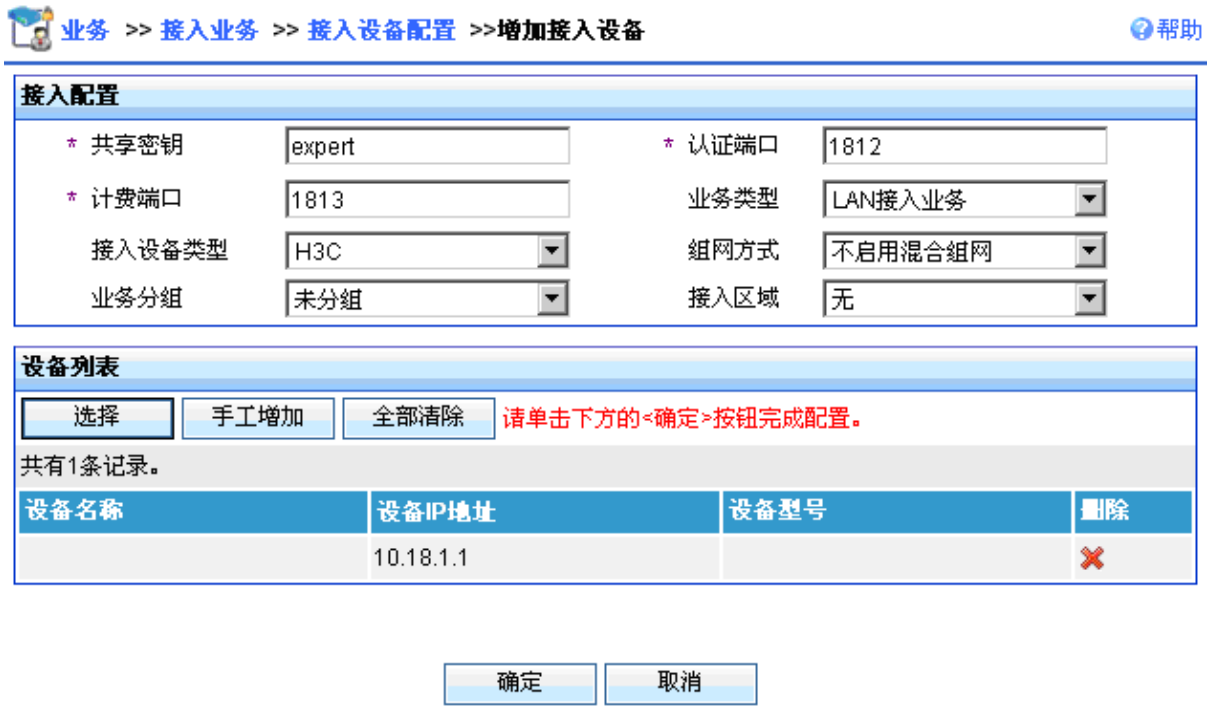
步骤 3：在接入设备页面中单击<增加>按钮，进入增加接入设备页面。

步骤 4：进行如下配置，如下图所示。

- 设置认证、计费共享密钥为 expert，其它保持缺省配置；
- 选择或手工增加接入设备，添加 IP 地址为 10.18.1.1 的接入设备。

步骤 5：单击<确定>按钮完成操作。

图2-62 增加接入设备



(2) 增加服务配置

步骤 1：选择“业务”页签。

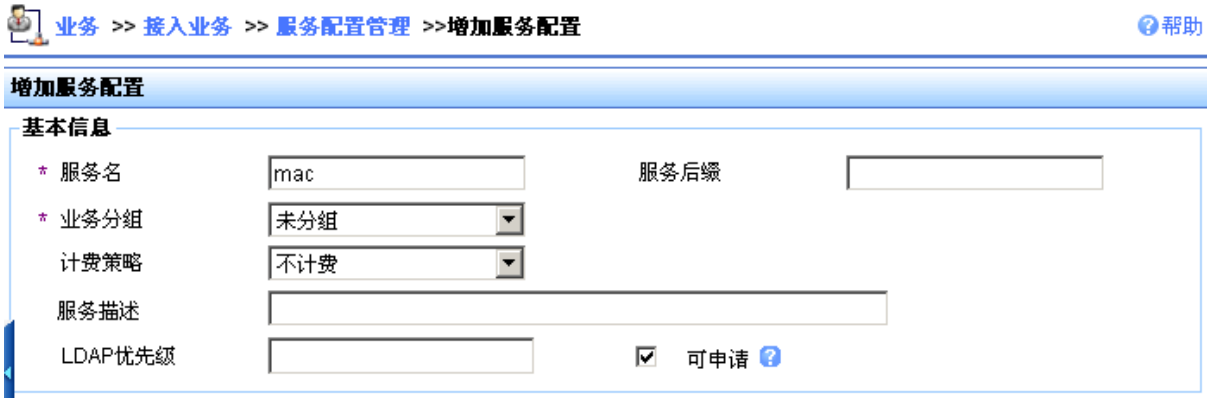
步骤 2：单击导航树中的“接入业务 > 服务配置管理”菜单项，进入增加服务配置页面。

步骤 3：在服务配置页面中单击<增加>按钮，进入增加接入设备页面。

步骤 4：设置服务名为 mac，其它保持缺省配置。

步骤 5：单击<确定>按钮完成操作。

图2-63 增加服务配置页面



(3) 增加接入用户

步骤 1：选择“用户”页签。

步骤 2：单击导航树中的“接入用户视图 > 所有接入用户”菜单项，进入用户页面。

步骤 3：在该页面中单击<增加>按钮，进入增加接入用户页面。

步骤 4：进行如下配置，如下图所示。

- 添加用户 00146c8a43ff；
- 添加帐号名和密码为 00146c8a43ff；
- 选中刚才配置的服务 mac。

步骤 5：单击<确定>按钮完成操作。

图2-64 增加接入用户



5. 验证结果

(1) 客户端不需要用户手动输入用户名或者密码。该客户端通过 MAC 地址认证后，可以通过访问无线网络。

(2) 在导航栏中选择“概览 > 客户端”，可以查看到成功上线的客户端。

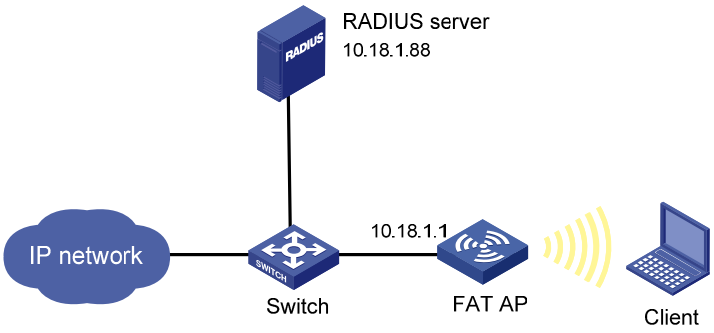
2.4.6 远程 802.1X认证配置举例

1. 组网需求

要求无线客户端使用远程 802.1X 认证方式接入无线网络。

- 一台 RADIUS 服务器（使用 CAMS/iMC 服务器，担当认证、授权、计费服务器的职责）。在 RADIUS 服务器上已经添加了 Client 的用户名和密码（用户名为 user，密码为 dot1x），同时设置了与 AP 交互报文时的共享密钥为“expert”，RADIUS 服务器 IP 地址为 10.18.1.88。
- AP 的 IP 地址为 10.18.1.1。AP 与认证、授权、计费 RADIUS 服务器交互报文时的共享密钥均为 expert，发送给 RADIUS 服务器的用户名中不带域名。

图2-65 远程 802.1x 认证配置组网图



2. 配置AP

(1) 配置 FAT AP 的接口 IP 地址

在 FAT AP 上创建 VLAN（在导航栏中选择“网络 > VLAN”，进入页面后可以创建 VLAN），并配置 IP 地址（在导航栏中选择 “设备 > 接口管理”，进入页面后可以配置 VLAN 的 IP 地址）。

(2) 配置 RADIUS 方案

步骤 1：在导航栏中选择“认证 > RADIUS”。

步骤 2：单击<新建>按钮，进入 RADIUS 方案配置页面。

步骤 3：进行如下配置，如下图所示。

- 在RADIUS服务器配置中增加如 图 2-66 所示的两个服务器，其中密钥为“expert”。
- 输入方案名称为“802.1x”。
- 选择服务类型为“Extended”。
- 选择用户名格式为“不带域名”。

步骤 4：单击<确定>按钮完成操作。

图2-66 配置 RADIUS



(3) 配置 AAA

步骤 1：创建 ISP 域。在导航栏中选择“认证 > AAA”，默认进入“域设置”页签的页面，本例使用缺省的 system 域（如果需要定制 ISP 域，可以创建新的 ISP 域）。

步骤 2：配置 ISP 域的 AAA 认证方案。单击“认证”页签。

步骤 3：进行如下配置，如下图所示。

- 选择域名为“system”。
- 选中“LAN-access 认证”前的复选框，选择认证方式为“RADIUS”。
- 选择认证方案名称为“802.1x”。

步骤 4：单击<应用>按钮完成操作。

图2-67 配置 ISP 域的 AAA 认证方案



步骤 5：配置 ISP 域的 AAA 授权方案。单击“授权”页签。

步骤 6：进行如下配置，如下图所示。

- 选择域名为“system”。
- 选中“LAN-access 授权”前的复选框，选择授权方式为“RADIUS”。
- 选择授权方案名称为“802.1x”。

步骤 7：单击<应用>按钮完成操作。

图2-68 配置 ISP 域的 AAA 授权方案



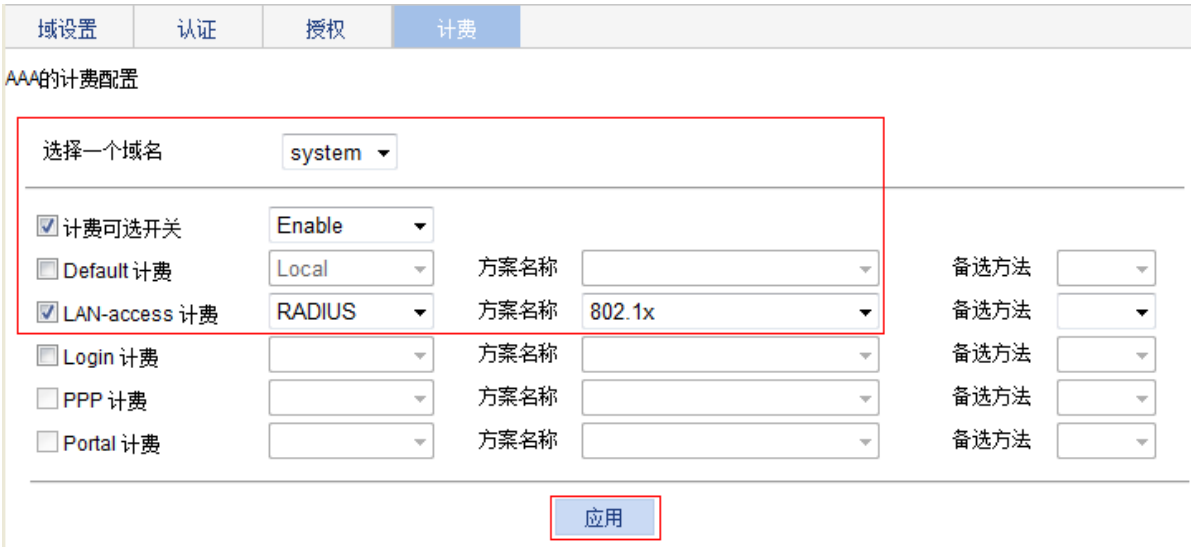
步骤 8：配置 ISP 域的 AAA 计费方案。单击“计费”页签。

步骤 9：进行如下配置，如下图所示。

- 选择域名为“system”。
- 选中“计费可选开关”前的复选框，选择“Enable”。
- 选中“LAN-access 计费”前的复选框，选择计费方式为“RADIUS”。
- 选择计费方案名称为“802.1x”。

步骤 10：单击<应用>按钮完成操作。

图2-69 配置 ISP 域的 AAA 计费方案



(4) 配置无线服务

步骤 1：在导航栏中选择“无线服务 > 接入服务”。

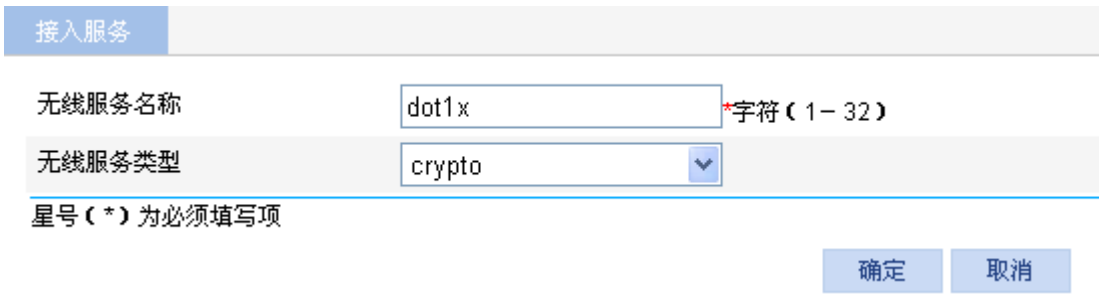
步骤 2：单击<新建>按钮，进入无线服务新建页面。

步骤 3：进行如下配置，如下图所示。

- 设置无线服务名称为“dot1x”。
- 选择无线服务类型为“crypto”。

步骤 4：单击<确定>按钮完成操作。

图2-70 创建无线服务



(5) 配置 802.1x 认证

创建无线服务后，直接进入配置无线服务界面。

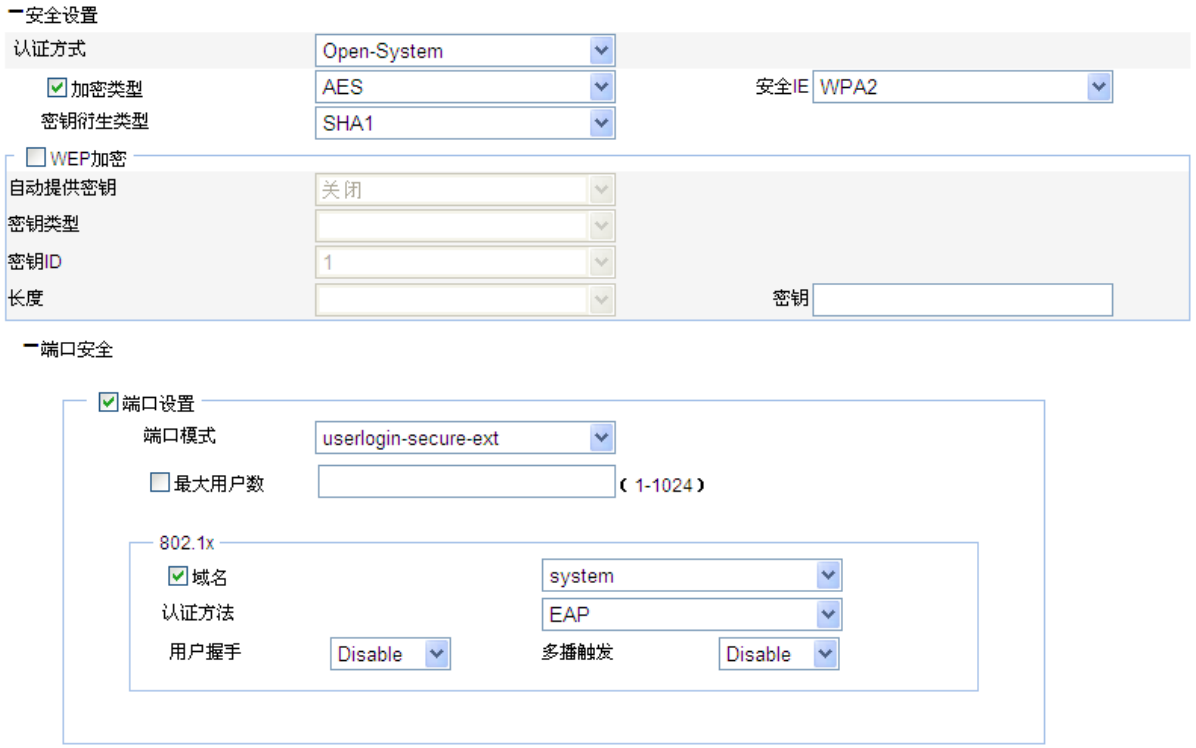
步骤 1：802.1x 认证需要在“安全设置”部分进行如下配置，如下图所示。

- 在“认证方式”下拉框中选择“Open-System”。
- 选中“加密类型”前的复选框，在加密类型下拉框中选择“AES”，在安全 IE 下拉框中选择“WPA2”。

- 选中“端口设置”前的复选框，在端口模式的下拉框中选择“userlogin-secure-ext”方式。
- 选中“域名”前的复选框，在域名下拉框中选择“system”。
- 在认证方法下拉框中选择“EAP”。
- 建议关闭用户握手和多播触发。

步骤 2：单击<确定>按钮完成操作。

图2-71 安全设置



(6) 绑定 AP 的射频

步骤 1：在导航栏中选择“无线服务 > 接入服务”。

步骤 2：单击无线服务“dot1x”对应的图标，进入如下图所示页面。

步骤 3：选中“802.11n”前的复选框。

步骤 4：单击<绑定>按钮完成操作。

图2-72 绑定 AP 的射频



(7) 开启无线服务

步骤 1：在导航栏中选择“无线服务 > 接入服务”，进入如下图所示页面。

步骤 2：选中“dot1x”前的复选框。

步骤 3：单击<开启>按钮完成操作。

图2-73 开启无线服务



(8) 开启 802.11n 射频（缺省情况下，802.11n 处于开启状态，此步骤可选）

在导航栏中选择“射频 > 射频设置”，进入射频设置页面，确认 802.11n 处于开启状态。

3. 配置RADIUS server（iMC V3）

说明

- 下面以 iMC 为例（使用 iMC 版本为：iMC PLAT 3.20-R2602、iMC UAM 3.60-E6102），说明 RADIUS server 的基本配置。
- 在服务器上已经完成证书安装。

(1) 增加接入设备

步骤 1：在 iMC 管理平台选择“业务”页签。

步骤 2：单击导航树中的“接入业务 > 接入设备配置”菜单项，进入接入设备配置页面。

步骤 3：在接入设备页面中单击<增加>按钮，进入增加接入设备页面。

步骤 4：进行如下配置，如下图所示。

- 设置认证、计费共享密钥为 expert；
- 设置认证及计费的端口号分别为 1812 和 1813；
- 选择协议类型为 LAN 接入业务；
- 选择接入设备类型为 H3C；
- 选择或手工增加接入设备，添加 IP 地址为 10.18.1.1 的接入设备。

步骤 5：单击<确定>按钮完成操作。

图2-74 增加接入设备



(2) 增加服务配置

步骤 1：选择“业务”页签。

步骤 2：单击导航树中的“接入业务 > 服务配置管理”菜单项，进入增加服务配置页面。

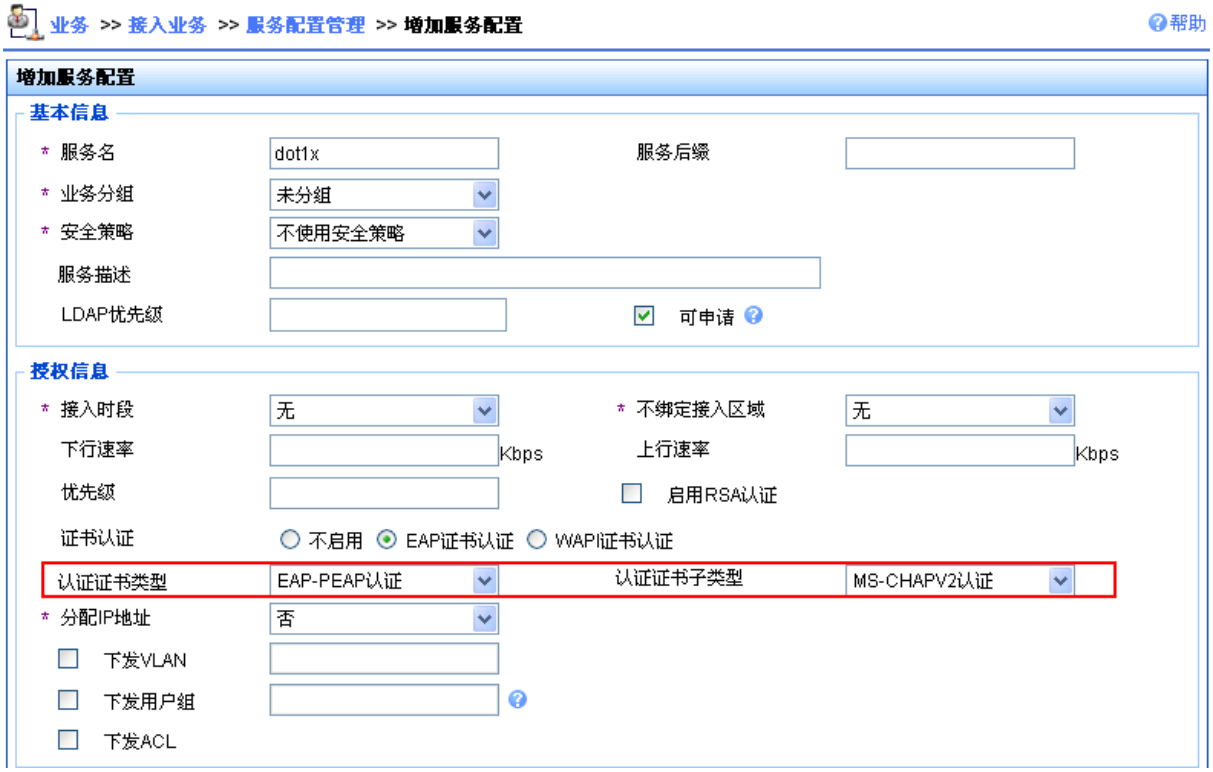
步骤 3：在服务配置页面中单击<增加>按钮，进入增加接入设备页面。

步骤 4：进行如下配置，如下图所示。

- 设置服务名为 dot1x；
- 选择认证证书类型为 EAP-PEAP 认证，认证证书子类型为 MS-CHAPV2 认证。

步骤 5：单击<确定>按钮完成操作。

图2-75 增加服务配置页面



(3) 增加接入用户

步骤 1：选择“用户”页签。

步骤 2：单击导航树中的“接入用户视图 > 所有接入用户”菜单项，进入用户页面。

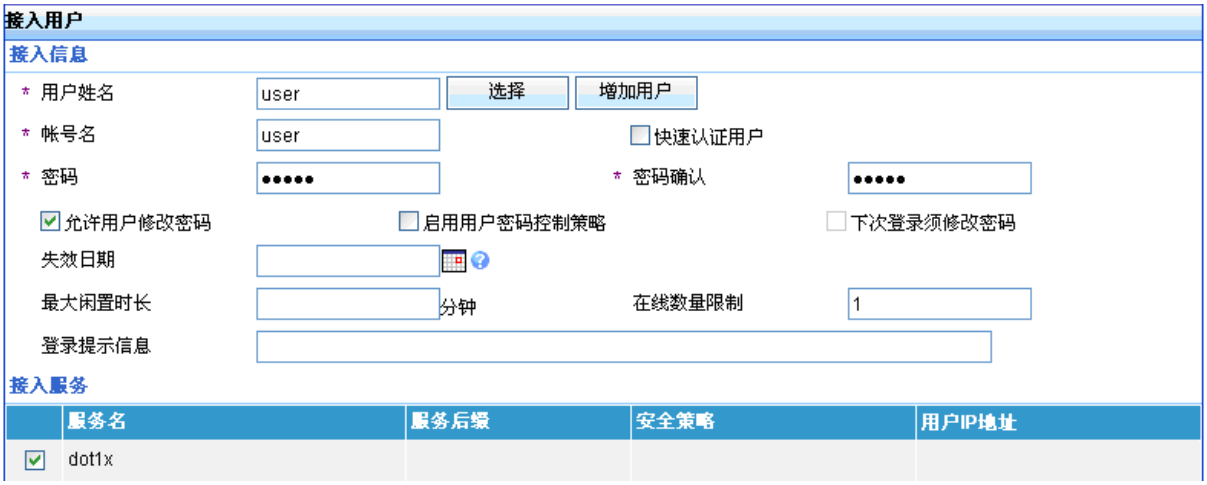
步骤 3：在该页面中单击<增加>按钮，进入增加接入用户页面。

步骤 4：进行如下配置，如下图所示。

- 添加用户名 user；
- 添加帐号名为 user，密码为 dot1x；
- 选中刚才配置的服务 dot1x。

步骤 5：单击<确定>按钮完成操作。

图2-76 增加接入用户



4. 配置RADIUS server（iMC V5）

说明

- 下面以 iMC 为例（使用 iMC 版本为：iMC PLAT 5.0、iMC UAM 5.0），说明 RADIUS server 的基本配置。
- 在服务器上已经完成证书安装。

(1) 增加接入设备

步骤 1：在进入 iMC 管理平台选择“业务”页签。

步骤 2：单击导航树中的“接入业务 > 接入设备配置”菜单项，进入接入设备配置页面。

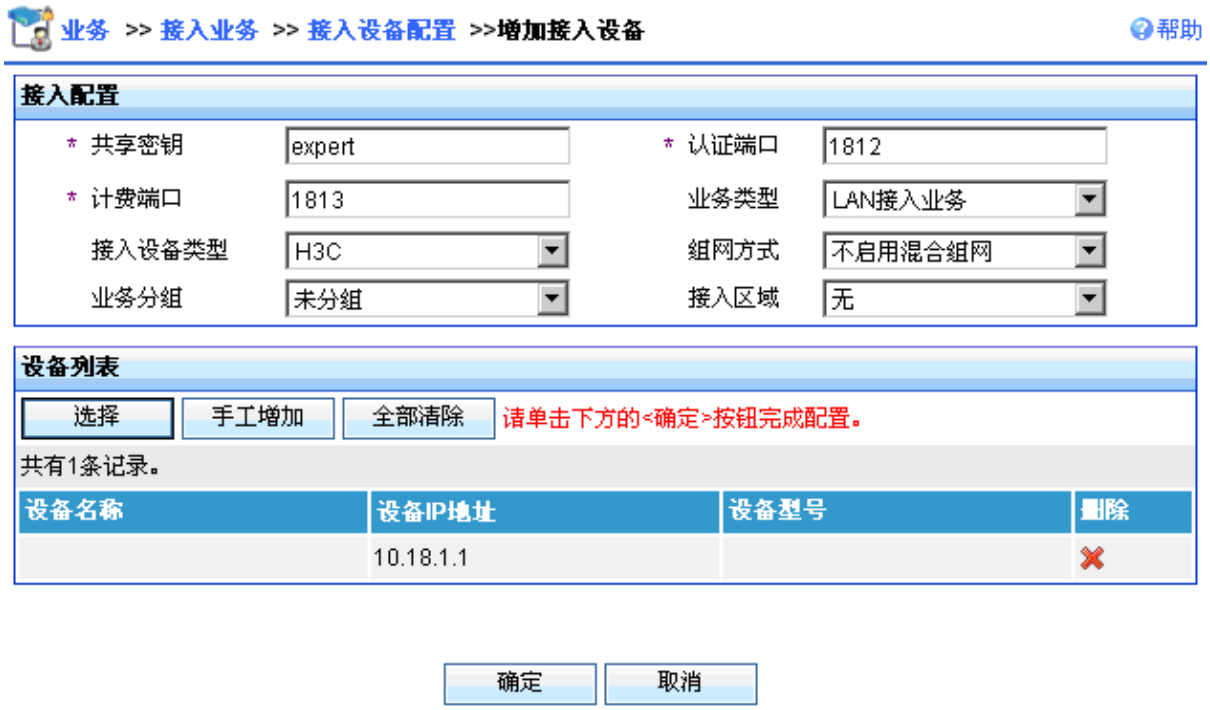
步骤 3：在接入设备页面中单击<增加>按钮，进入增加接入设备页面。

步骤 4：进行如下配置，如下图所示。

- 设置认证、计费共享密钥为 expert，其它保持缺省配置；
- 选择或手工增加接入设备，添加 IP 地址为 10.18.1.1 的接入设备。

步骤 5：单击<确定>按钮完成操作。

图2-77 增加接入设备



(2) 增加服务配置

步骤 1：选择“业务”页签。

步骤 2：单击导航树中的“接入业务 > 服务配置管理”菜单项，进入增加服务配置页面。

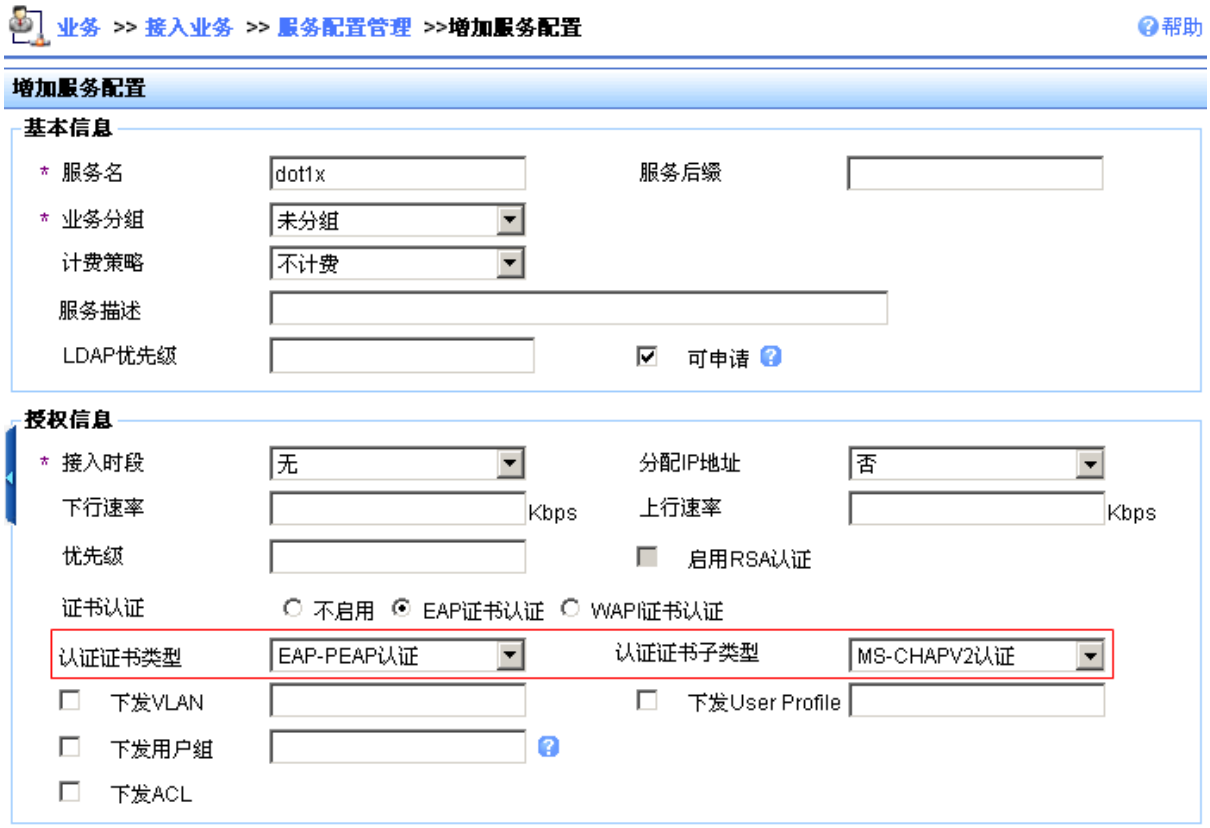
步骤 3：在服务配置页面中单击“增加”按钮，进入增加接入设备页面。

步骤 4：进行如下配置，如下图所示。

- 设置服务名为 dot1x；
- 选择认证证书类型为 EAP-PEAP 认证，认证证书子类型为 MS-CHAPV2 认证。

步骤 5：单击<确定>按钮完成操作。

图2-78 增加服务配置页面



(3) 增加接入用户

步骤 1：选择“用户”页签。

步骤 2：单击导航树中的“接入用户视图 > 所有接入用户”菜单项，进入用户页面。

步骤 3：在该页面中单击<增加>按钮，进入增加接入用户页面。

步骤 4：进行如下配置，如下图所示。

- 添加用户 user；
- 添加帐号名为 user，密码为 dot1x；
- 选中刚才配置的服务 dot1x。

步骤 5：单击<确定>按钮完成操作。

图2-79 增加接入用户



5. 配置无线网卡

选择无线网卡，在验证对话框中，选择 EAP 类型为 PEAP，点击“属性”，去掉验证服务器证书选项（此处不验证服务器证书），点击“配置”，去掉自动使用 windows 登录名和密码选项。单击“确定”按钮完成操作。整个过程如下图所示。

图2-80 无线网卡配置过程



图2-81 无线网卡配置过程

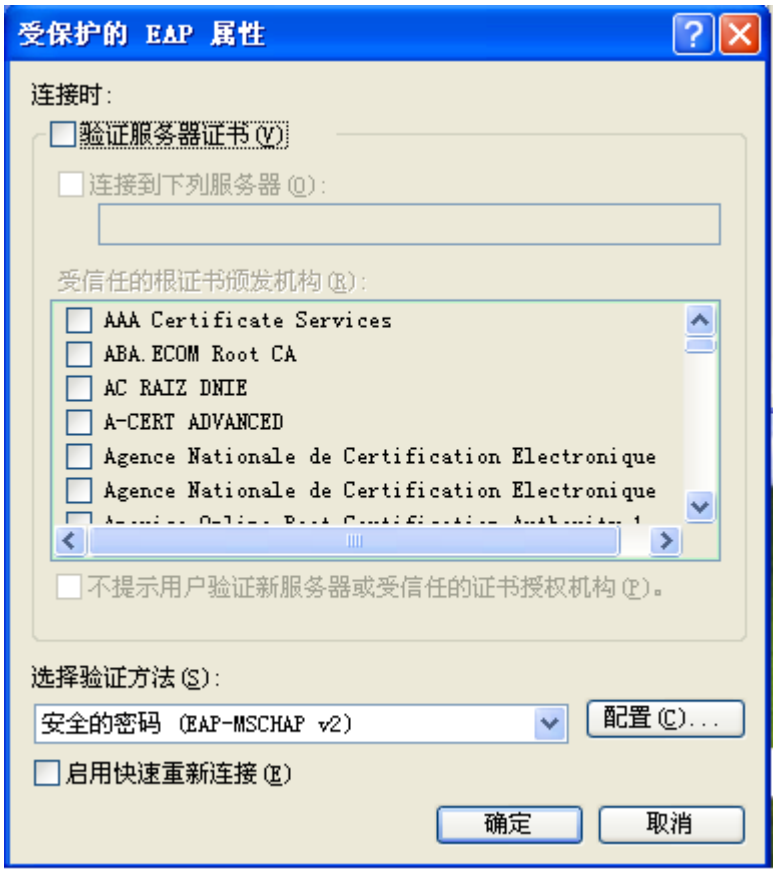
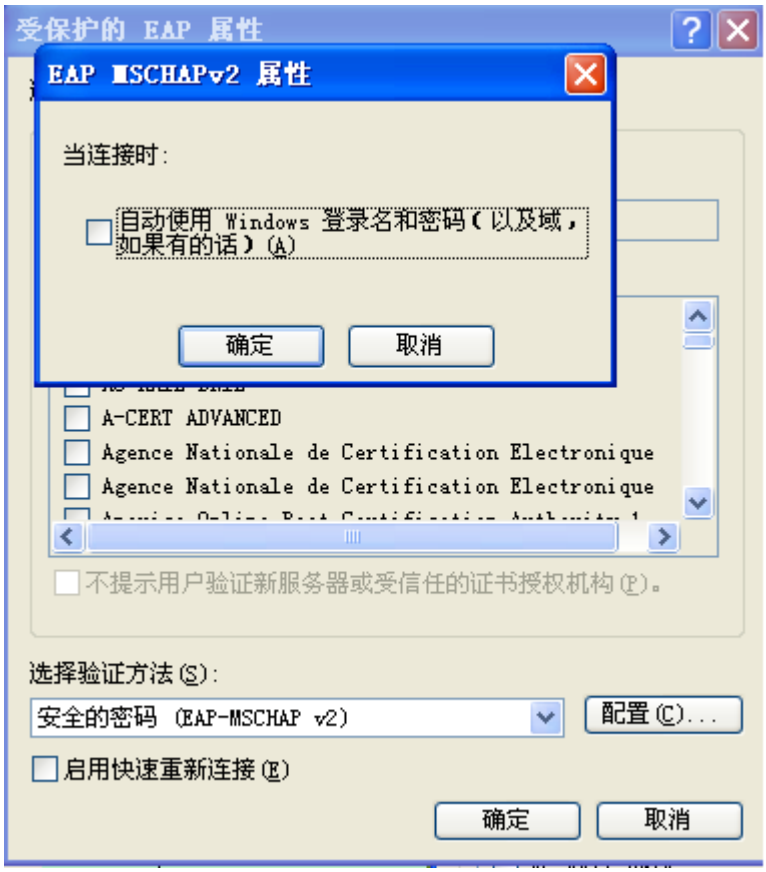


图2-82 无线网卡配置过程



6. 验证结果

(1) 在客户端弹出的对话框中输入用户名 user 和密码 dot1x。客户端可以成功关联 AP，并且可以访问无线网络。

(2) 在导航栏中选择“概览 > 客户端”，可以查看到成功上线的客户端。

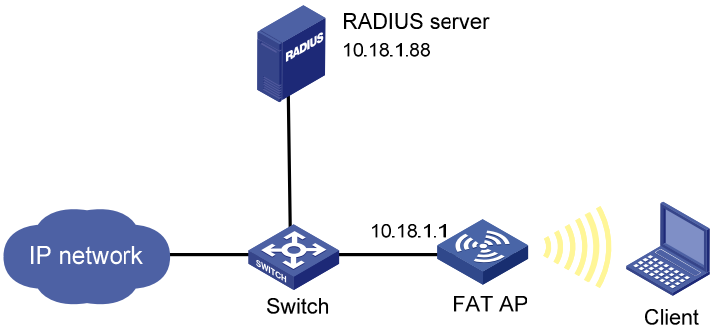
2.4.7 自动提供WEP密钥-802.1x认证配置举例

1. 组网需求

要求使用客户端使用远程自动提供 WEP 密钥-802.1x 认证方式接入无线网络。

- 一台 RADIUS 服务器（使用 CAMS/iMC 服务器，担当认证、授权、计费服务器的职责）。在 RADIUS 服务器上添加 Client 的用户名和密码（用户名为 user，密码为 dot1x），同时设置共享密钥为“expert”，RADIUS 服务器 IP 地址为 10.18.1.88。
- AP 的 IP 地址为 10.18.1.1。在 AP 上设置共享密钥为 expert，发送给 RADIUS 服务器的用户名中不带域名。

图2-83 自动提供 WEP 密钥-802.1x 配置组网图



2. 配置AP

(1) 配置 FAT AP 的接口 IP 地址

在 FAT AP 上创建 VLAN（在导航栏中选择“网络 > VLAN”，进入页面后可以创建 VLAN），并配置 IP 地址（在导航栏中选择 “设备 > 接口管理”，进入页面后可以配置 VLAN 的 IP 地址）。

(2) 配置 RADIUS 方案

请参考“2.4.6_2. (2)配置RADIUS方案”部分。

(3) 配置 AAA

请参考“2.4.6_2. (3)配置AAA”部分。

(4) 配置无线服务

步骤 1：在导航栏中选择“无线服务 > 接入服务”。

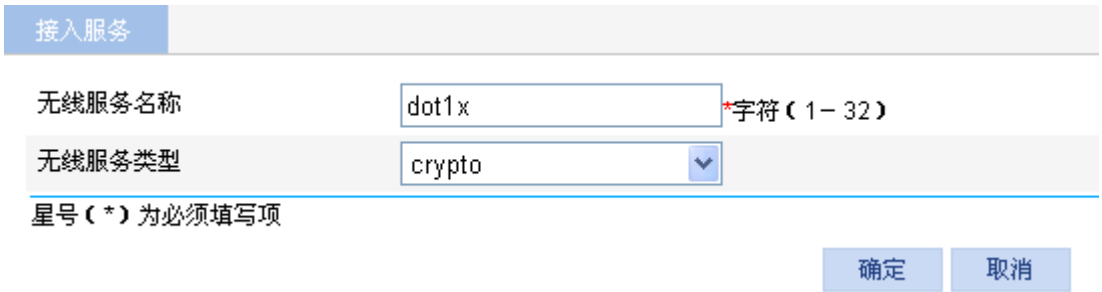
步骤 2：单击<新建>按钮，进入无线服务新建页面。

步骤 3：进行如下配置，如下图所示。

- 设置无线服务名称为“dot1x”。
- 选择无线服务类型为“crypto”。

步骤 4：单击<确定>按钮完成操作。

图2-84 创建无线服务



(5) 配置 802.1x 认证

创建无线服务后，直接进入配置无线服务界面。

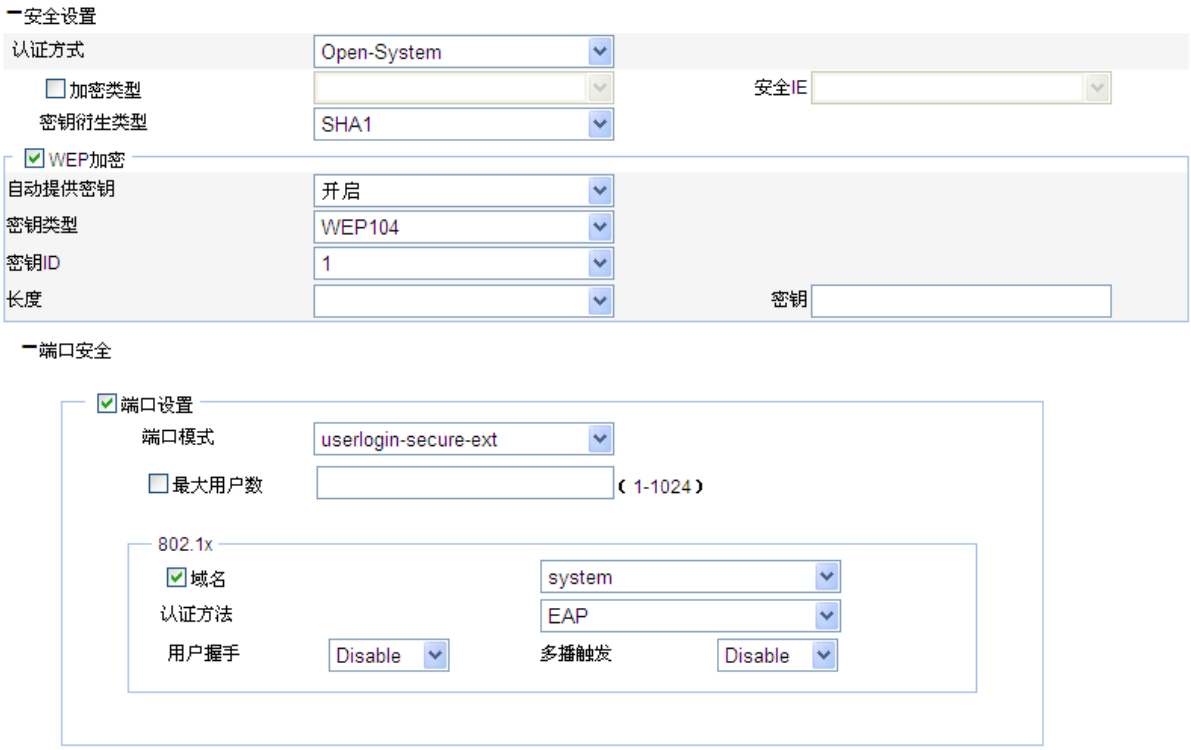
步骤 1：802.1x 认证需要在“安全设置”部分进行如下设置，如下图所示。

- 在“认证方式”下拉框中选择“Open-System”。
- 选中“WEP 加密”前的复选框，在自动提供密钥下拉框中选择“开启”。

- 选中“端口设置”前的复选框，在端口模式的下拉框中选择“userlogin-secure-ext”方式。
- 选中“域名”前的复选框，在域名下拉框中选择“system”。
- 在认证方法下拉框中选择“EAP”。
- 建议关闭用户握手和多播触发。

步骤 2：单击<确定>按钮完成操作。

图2-85 安全设置



(6) 绑定 AP 的射频

步骤 1：在导航栏中选择“无线服务 > 接入服务”。

步骤 2：单击无线服务“dot1x”对应的图标，进入如下图所示页面。

步骤 3：选中“802.11n”前的复选框。

步骤 4：单击<绑定>按钮完成操作。

图2-86 绑定 AP 的射频



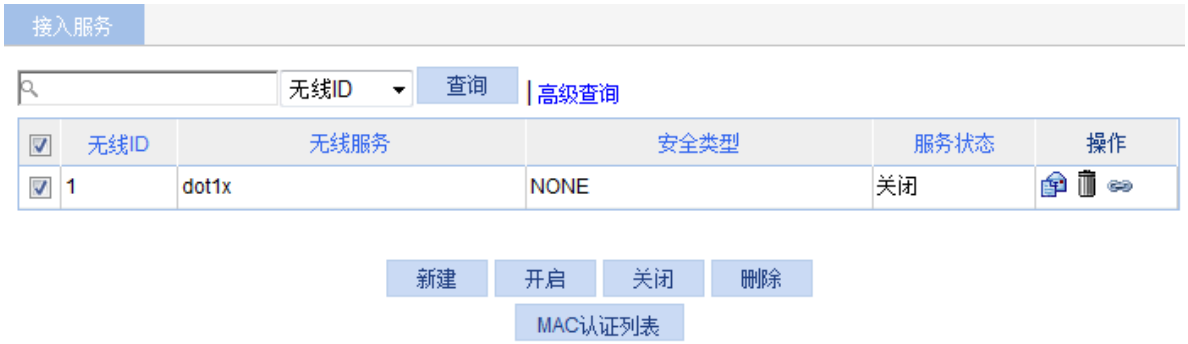
(7) 开启无线服务

步骤 1：在导航栏中选择“无线服务 > 接入服务”，进入如下图所示页面。

步骤 2：选中“dot1x”前的复选框。

步骤 3：单击<开启>按钮完成操作。

图2-87 开启无线服务



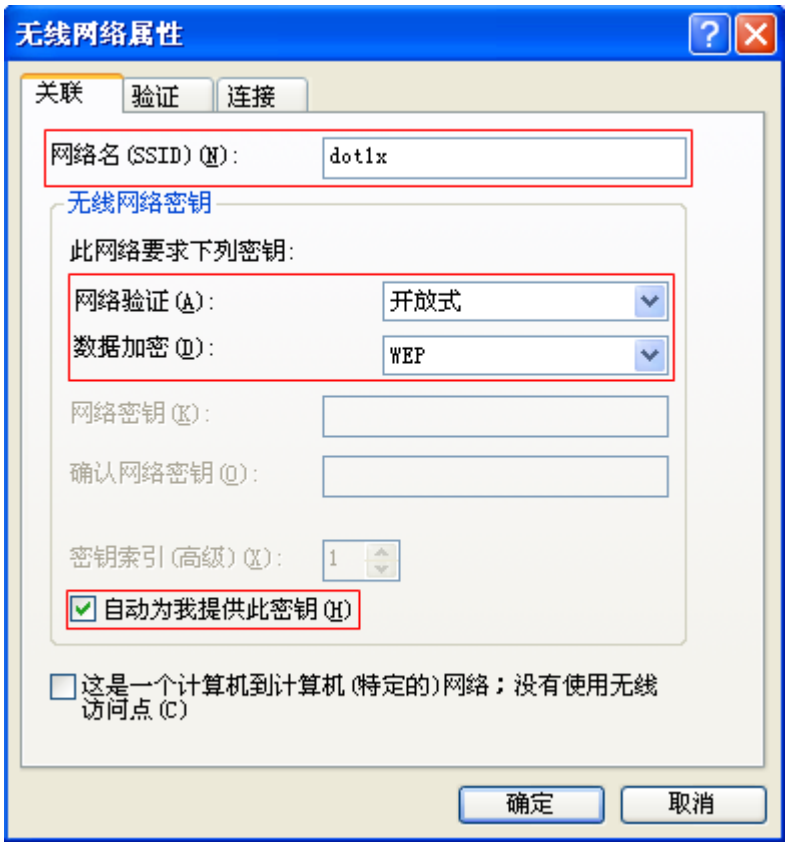
(8) 开启 802.11n 射频（缺省情况下，802.11n 处于开启状态，此步骤可选）

在导航栏中选择“射频 > 射频设置”，进入射频设置页面，确认 802.11n 处于开启状态。

3. 配置无线网卡

双击桌面右下角的图标，在弹出“无线网络连接状态”窗口上点击“属性”，在弹出的属性页面中单击<添加>按钮，选择关联页签，添加名为“dot1x”的 SSID，并确保选择了“自动为我提供此密钥(H)”。最后单击<确定>按钮完成操作。

图2-88 无线网卡配置过程（关联对话框）



在验证页签中，选择 EAP 类型为“受保护的 EAP（PEAP）”，点击“属性”，取消“验证服务器证书（V）”（此处不验证服务器证书），点击“配置”，取消“自动使用 windows 登录名和密码（以及域，如果有的话）（A）”。然后单击<确定>按钮完成客户端操作。

图2-89 无线网卡配置过程（关联对话框）

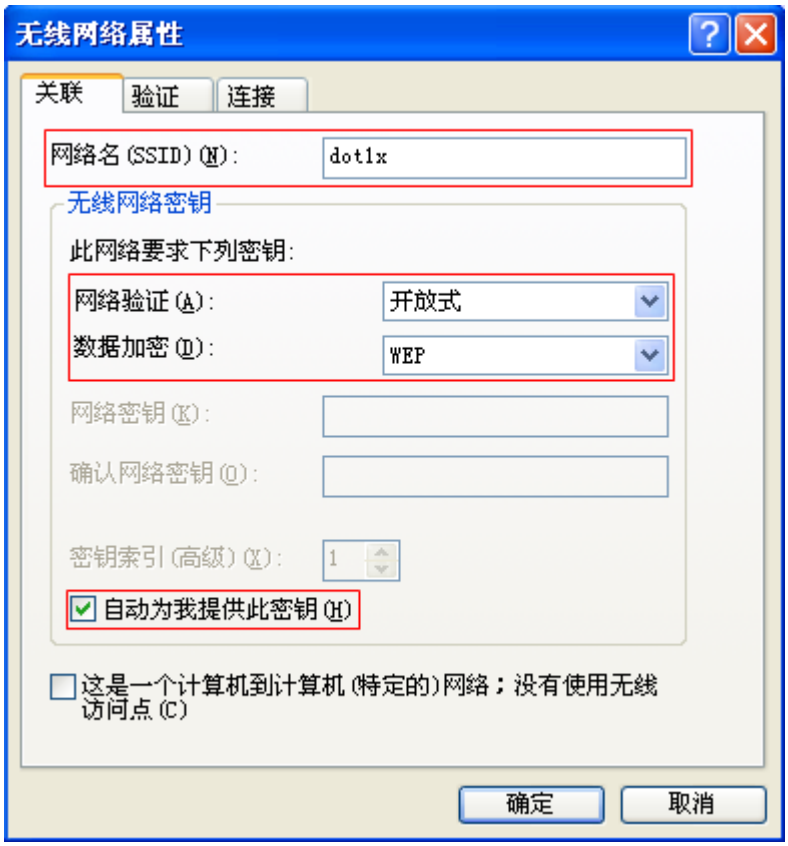


图2-90 无线网卡配置过程（验证对话框）

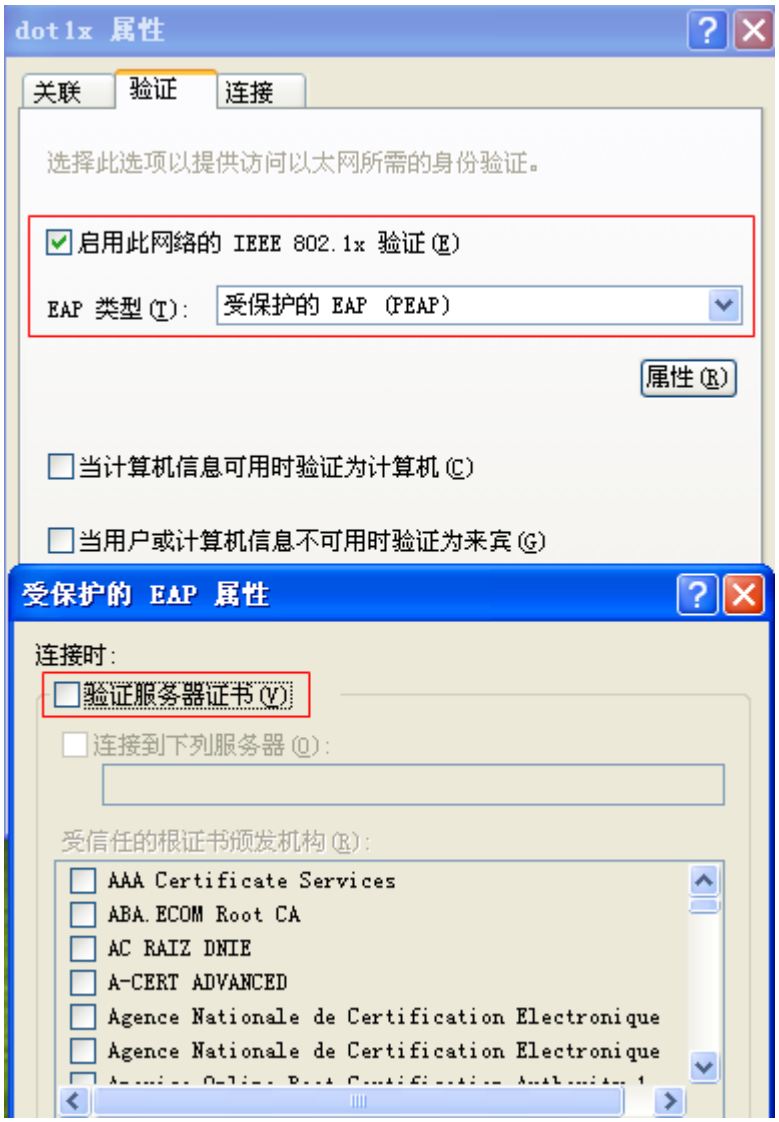


图2-91 无线网卡配置过程

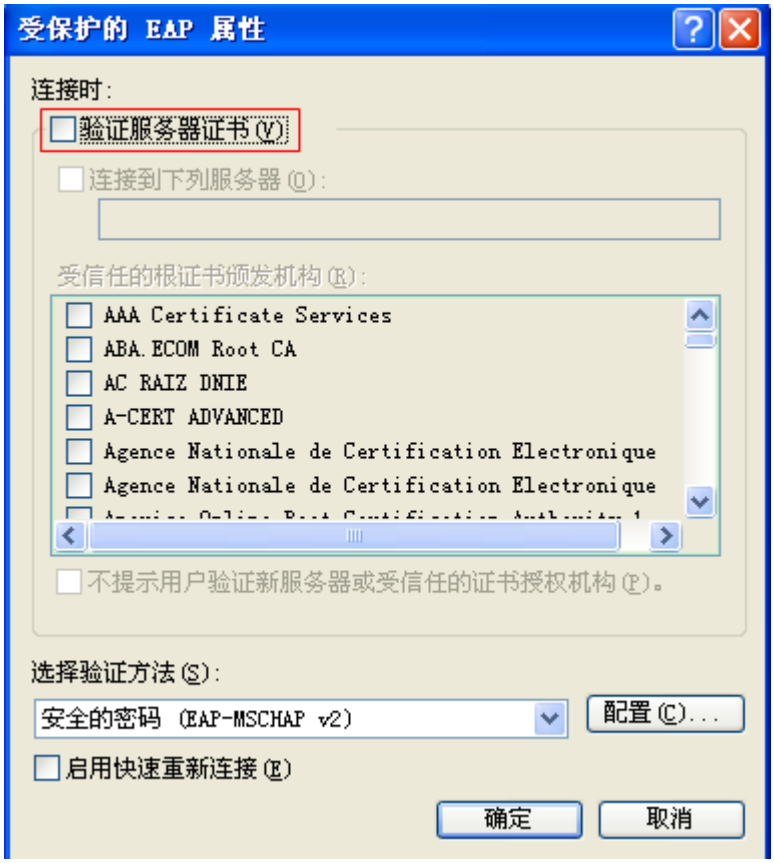
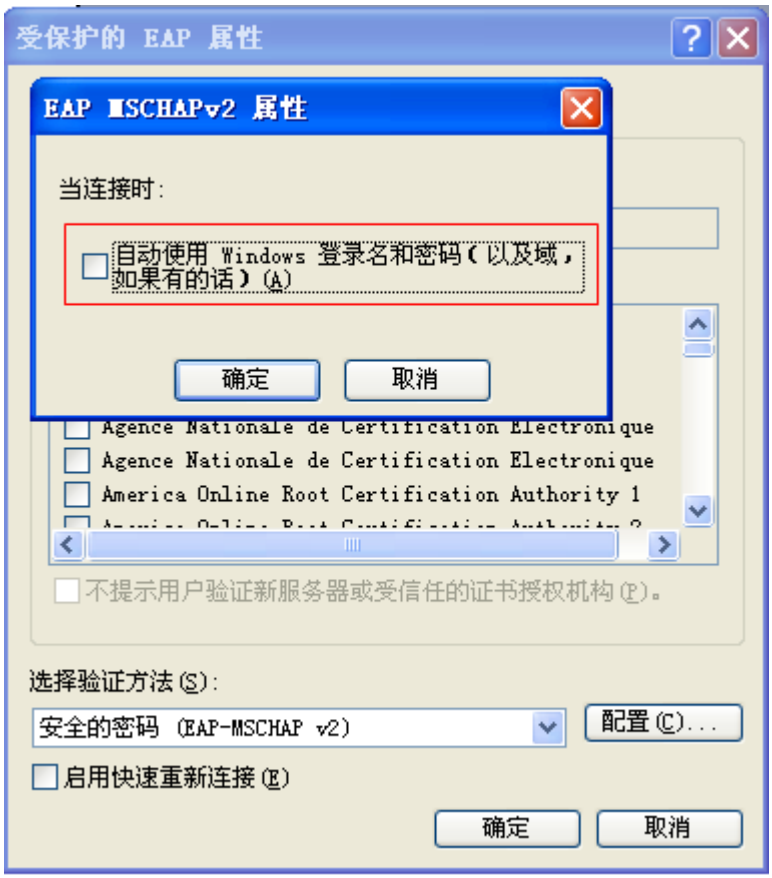


图2-92 无线网卡配置过程



4. 验证结果

(1) 在客户端弹出的对话框中输入用户名 user 和密码 dot1x。客户端可以成功关联 AP，并且可以访问无线网络。

(2) 在导航栏中选择“概览 > 客户端”，可以查看到成功上线的客户端。

2.4.8 802.11n典型配置举例

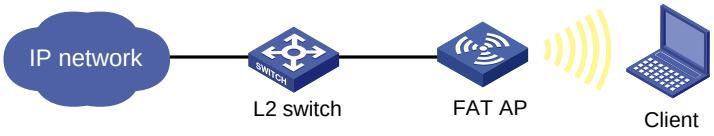
1. 组网需求

某公司为了满足多媒体应用的高带宽要求，需要部署高速接入的 802.11n 无线网络。

具体要求如下：

- AP 提供 SSID 为 11nservice 的明文方式的无线接入服务。
- 为了保护现有投资，兼容现有的 802.11g 无线网络，采用 802.11n（2.4GHz）射频模式。

图2-93 802.11n 无线服务组网图



2. 配置AP

(1) 配置 FAT AP 的接口 IP 地址

在 FAT AP 上创建 VLAN（在导航栏中选择“网络 > VLAN”，进入页面后可以创建 VLAN），并配置 IP 地址（在导航栏中选择 “设备 > 接口管理”，进入页面后可以配置 VLAN 的 IP 地址）。

(2) 配置无线服务

步骤 1：在导航栏中选择“无线服务 > 接入服务”。

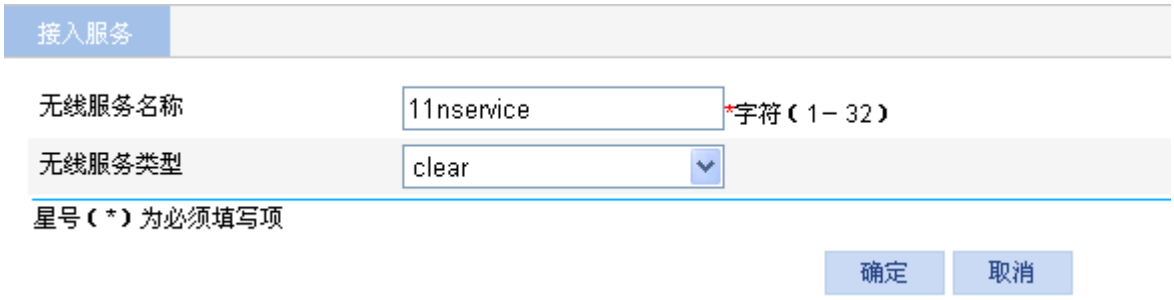
步骤 2：单击<新建>按钮，进入无线服务新建页面。

步骤 3：进行如下配置，如下图所示。

- 设置无线服务名称为“11nservice”。
- 选择无线服务类型为“clear”。

步骤 4：单击<确定>按钮完成操作。

图2-94 创建无线服务



(3) 绑定 AP 的射频

步骤 1：在导航栏中选择“无线服务 > 接入服务”。

步骤 2：单击无线服务“11nservice”对应的图标，进入如下图所示页面。

步骤 3：选中“802.11n(2.4GHz)”前的复选框。

步骤 4：单击<绑定>按钮完成操作。

图2-95 绑定 AP 的射频



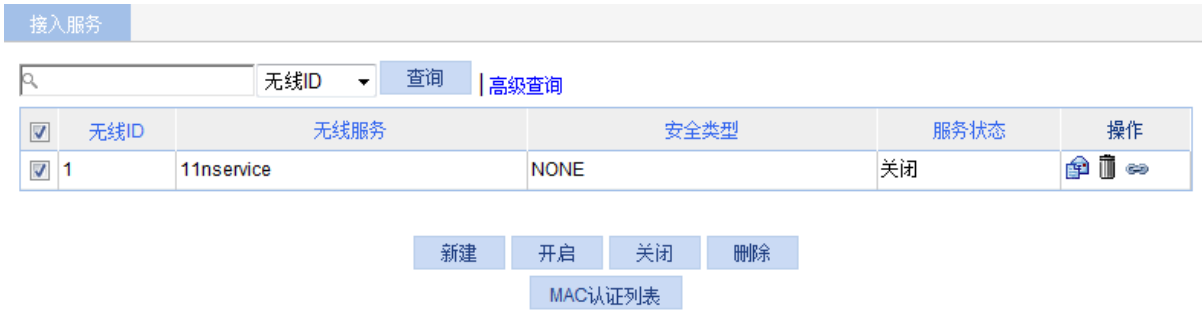
(4) 开启无线服务

步骤 1：在导航栏中选择“无线服务 > 接入服务”，进入如下图所示页面。

步骤 2：选中“11nservice”前的复选框。

步骤 3：单击<开启>按钮完成操作。

图2-96 开启无线服务



(5) 开启 802.11n(2.4GHz)射频（缺省情况下，802.11n(2.4GHz)处于开启状态，此步骤可选）

在导航栏中选择“射频 > 射频设置”，进入如下图所示射频设置页面，确认 802.11n(2.4GHz)处于开启状态。

图2-97 开启 802.11n(2.4GHz)射频



3. 验证配置结果

(1) 客户端可以成功关联 AP，并且可以访问无线网络。

(2) 在导航栏中选择“概览 > 客户端”，可以查看到成功上线的客户端。

图2-98 查看成功上线的客户端



从上图中可以看到，984b-4ad4-3f24 是 802.11g 用户，984b-4ad4-3fd4 是 802.11n 用户，因为本例中没有对用户类型进行限制，所以 802.11g、802.11n 用户都可以接入无线网络。如果开启了“只允许 11n 用户接入”，那么只有 984b-4ad4-3fd4 用户才能接入无线网络。

4. 配置注意事项

配置 802.11n 需注意如下事项：

- 在导航栏中选择“射频 > 射频设置”，选择需要配置的 AP 的射频单元，单击图标进入射频配置页面可以修改关于 802.11n 的相关参数，包括带宽模式、A-MPDU、A-MSDU、short GI 和允许 11n 用户接入情况。
- 确认 802.11n(2.4GHz)处于开启状态。
- 在导航栏中选择“射频 > 速率设置”，可以修改 802.11n 的速率。

2.5 WDS配置举例

2.5.1 WDS典型配置举例

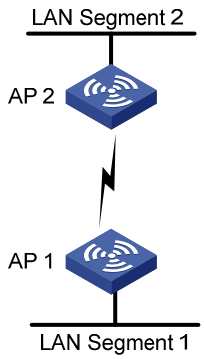
1. 组网需求

在如下图所示的室外环境中存在两个独立的局域网，如果采用有线方式连接这两个局域网，需要使用挖沟开渠等方式铺设线缆，这样做工期长、开销大。在这种部署有线网络不方便的情况下，可以采用 WDS 链路连接这两个局域网，实现两个局域网之间的互通。

具体部署方式如下：

- AP 1 和 AP 2 分别连接不同的局域网。
- 手工指定固定信道 153，通过 802.11ac 射频模式使 AP 1 和 AP 2 之间形成 WDS 链路。
- 为了保证 WDS 链路的安全性，设置预共享密钥为“12345678”。

图2-99 WDS 配置组网图



2. 配置AP 1

(1) 配置 AP 1 的接口 IP 地址

创建 VLAN（在导航栏中选择“网络 > VLAN”，进入页面后可以创建 VLAN），并配置 IP 地址（在导航栏中选择 “设备 > 接口管理”，进入页面后可以配置 VLAN 的 IP 地址）。

(2) 配置 WDS

步骤 1：在导航栏中选择“无线服务 > WDS”，进入如下图所示 WDS 设置页面。

图2-100 WDS 设置



步骤 2：在列表中找到要进行配置的射频模式，单击对应的图标，进入 WDS 设置页面。

步骤 3：进行如下配置，如下图所示。

- 选择字符串方式，设置预共享密钥为“12345678”。
- 不对邻居列表进行操作，即 AP 可以和任何其它 AP 建立 WDS 链路。

步骤 4：单击<确定>按钮完成操作。

图2-101 WDS 设置页面



(3) 手工指定信道

步骤 1：在界面左侧的导航栏中选择“射频 > 射频设置”。

步骤 2：在列表中选择需要配置的射频单元，单击对应的图标，进入射频设置页面。

步骤 3：在信道下拉框中选择使用的信道。

步骤 4：单击<确定>按钮完成操作。

图2-102 手工配置相同的信道



(4) 开启 802.11ac 射频（缺省情况下，802.11ac 处于开启状态，此步骤可选）

在导航栏中选择“射频 > 射频设置”，进入射频设置页面，确认 802.11ac 处于开启状态。

(5) 开启 WDS

步骤 1：在导航栏中选择“无线服务 > WDS”，进入 WDS 设置页面。

步骤 2：选中“802.11ac”前的复选框。

步骤 3：单击<开启>按钮完成操作。

图2-103 WDS 设置



3. 配置AP 2

AP 2 的配置步骤和 AP 1 相同，此处不再重复。

4. 验证配置结果

在导航栏中选择“概览 > WDS”，进入 WDS 显示页面。

图2-104 WDS 显示页面



在上图中可以看到 WDS 链路已经成功建立。

5. 配置注意事项

在一个 WDS 链路中，显示的信息包括：邻居 MAC 地址、本地 MAC 地址、邻居状态、链路 UP 时间、信号质量。

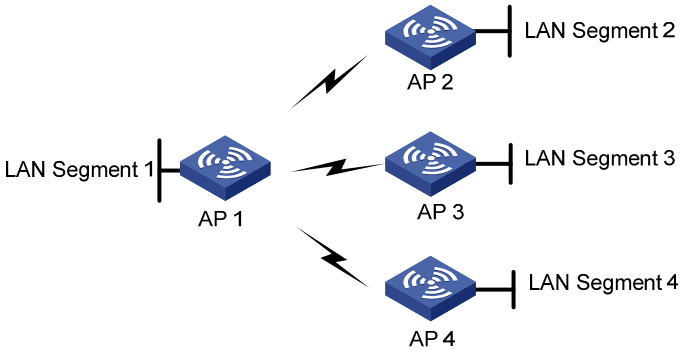
当信号质量显示为绿色（五格）时，表明信号质量最好；如果显示为黄色，则表明当前信号质量比较差，此时需要关注：当前采用的天线是否和 Radio 匹配、天线连接是否正确、当前射频的最大功率是否过小等。

2.5.2 WDS点到多点典型配置举例

1. 组网需求

要求在 AP 1 分别和 AP 2，AP 3，AP 4 建立 WDS 链路。

图2-105 WDS 配置组网图



2. 配置思路

WDS 点到多点配置和普通无线 WDS 配置基本相同，但需要注意以下几点：

- 在每个 AP 的射频模式下配置邻居 AP 的 MAC 地址（否则 AP2、AP3、AP4 之间也可能建立 WDS 链路）。
- 设置允许建立的最大 WDS 链路数（缺省值为 2，需要根据实际链路数进行设置，此例中在 AP 1 上该值应设为 3）。

3. 配置步骤

WDS点到多点配置和普通无线WDS配置相同，具体配置步骤请参见“2.5.1 2. 配置AP 1”。

4. 验证配置结果

查看 WDS 链路状态：

(1) 在 AP 1 上的 WDS 链路状态页面（在导航栏中选择“概览 > WDS”）可以看到 AP 1 与 AP 2、AP 3、AP 4 建立的三条 WDS 链路。

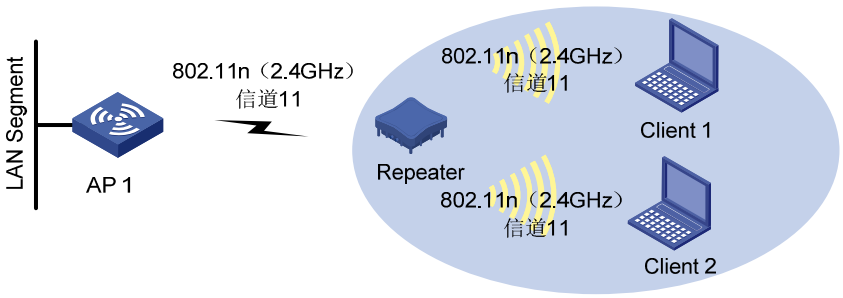
(2) 在 AP 2、AP 3 和 AP 4 上的 WDS 链路状态页面（在导航栏中选择“概览 > WDS”）可以看到它们各自与 AP 1 建立的一条 WDS 链路。

2.6 Repeater模式配置举例

1. 组网需求

- AP 1 接入有线局域网，作为 Repeater 的 AP 通过 WDS 链路与 AP 1 建立连接，同时该 Repeater 也能为 Client 提供无线接入服务。
- 通过 802.11n 射频模式使 AP 1 和 Repeater 建立 WDS 链路。
- 通过 802.11n 射频模式使 Client 接入 Repeater。
- 接入服务使用的信道和 WDS 链路使用的信道应该保持一致，本例中选用 802.11n 射频模式下的信道 11 作为工作信道。

图2-106 Repeater 模式配置组网图



2. 配置思路

- 配置AP 1：在AP 1 上配置WDS，具体配置步骤请参见“2.5.1 2. 配置AP 1”。
- 配置 Repeater：在 Repeater 上配置 WDS 和接入服务。

3. 配置Repeater

(1) 配置 WDS

步骤 1：在导航栏中选择“无线服务 > WDS”，进入如下图所示 WDS 设置页面。

图2-107 WDS 设置



步骤 2：在列表中找到要进行配置的 802.11n 射频模式，单击对应的图标，进入 WDS 设置页面。

步骤 3：选择字符串方式，设置预共享密钥为“12345678”。

步骤 4：单击<确定>按钮完成操作。

图2-108 WDS 设置页面



(2) 手工配置信道

步骤 1：在界面左侧的导航栏中选择“射频 > 射频设置”。

步骤 2：在列表中选择需要配置的射频单元，单击对应的图标，进入射频设置页面。

步骤 3：在信道下拉框中选择使用的信道 11。

步骤 4：单击<确定>按钮完成操作。

图2-109 手工配置相同的信道



(3) 开启 802.11n 射频（缺省情况下，802.11n 处于开启状态，此步骤可选）。

在导航栏中选择“射频 > 射频设置”，进入射频设置页面，确认 802.11n 处于开启状态。

(4) 开启 WDS

步骤 1：在导航栏中选择“无线服务 > WDS”，进入 WDS 设置页面。

步骤 2：选中“802.11n”前的复选框。

步骤 3：单击<开启>按钮完成操作。

图2-110 WDS 设置

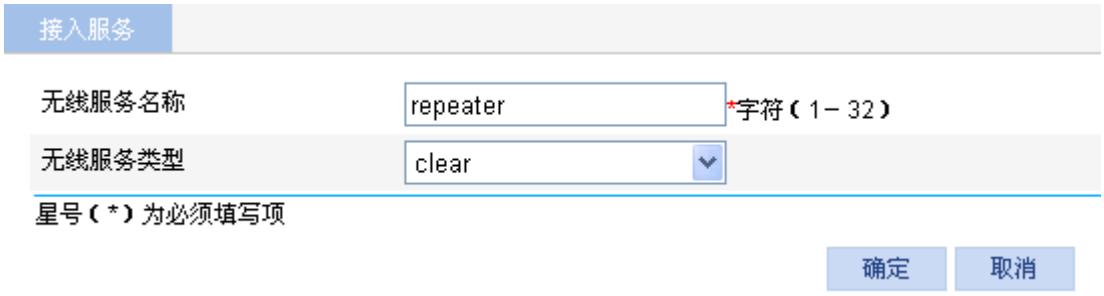


(5) 配置接入服务

说明

为 Repeater 配置接入服务的相关配置请参见“无线接入配置举例”，可以完全参照相关举例完成配置。

图2-111 配置接入服务



说明

在 Repeater 上配置接入服务时，应保证以下两点：

- 接入服务使用的射频模式和 WDS 链路使用的射频模式应该保持一致，本例中 WDS 和接入服务都使用 802.11n 射频模式。
- 接入服务使用的信道和 WDS 链路使用的信道应该保持一致，本例中选用 802.11n 射频模式下的信道 11 作为工作信道。

4. 验证配置结果

(1) 验证 Repeater 模式中 WDS 链接已经建立

在导航栏中选择“概览 > WDS”，进入 WDS 显示页面。单击射频单元 2，可以查看到邻居信息。

图2-112 显示 WDS



(2) 已经成功建立 Repeater 模式

在界面左侧的导航栏中选择“概览 > 射频”，在服务类型中可以看到 Repeater 上的 802.11n 射频模式同时提供“接入”和“WDS”服务，并且有一个客户端通过 repeater 接入无线网络。

图2-113 显示射频


射频
射频单元
状态
射频模式
信道
功率(dBm)
服务类型
资源利用率(%)
背景噪声(dBm)
1
Up
802.11ac(5GHz)
149
19
接入
0
-95
2
Up
802.11n(2.4GHz)
11
20
接入，WDS
0
-91
清空统计
刷新
无线服务
详细信息
无线服务
服务状态
连接用户数
repeater
开启
1

目 录

1 射频配置 ····· 1-1
1.1 配置射频设置 ····· 1-1
1.2 配置射频速率 ····· 1-7
1.2.1 配置 802.11a/802.11b/802.11g射频速率 ····· 1-7
1.2.2 配置 802.11n MCS ····· 1-9
1.2.3 配置 802.11ac射频速率 ····· 1-12
1.3 配置功率信道优化 ····· 1-15
1.3.1 功率信道信息 ····· 1-15
1.3.2 参数设置 ····· 1-15
1.4 配置信道扫描 ····· 1-17
1.4.1 设置信道扫描参数 ····· 1-17
1.4.2 设置AP工作模式 ····· 1-19
1.5 信道环境检测 ····· 1-21
1.5.1 查看检测记录 ····· 1-21
1.5.2 设置检测记录老化时间 ····· 1-22
1.5.3 查看历史记录 ····· 1-22
1.6 天线切换 ····· 1-23

1 射频配置

说明

手册中设备的接口类型、显示信息与设备型号、支持射频情况和配置信息相关，实际使用中还请以设备的实际情况为准。

设备各款型对于本节所描述的特性支持情况有所不同，详细差异信息如下：

产品系列	型号	特性	描述
WA2600系列	WA2610H	5G射频接口	不支持
WA4600系列	WA4620i-ACN/WA4620E-ACN		支持
WA4300系列	WA4320H-ACN		支持
	WA4320i-ACN/WA4320i-X		支持
	WA4320-TS/WA4320-TQ/WA4320-TQ-V		支持
	WA4320X		支持
	WA4320-ACN/WA4320/WA4320-ACN-SI/ WA4320-ACN-C/WA4320-ACN-D/WA4320 -ACN-E/WA4320-ACN-PI		支持
	WA4330-ACN		支持
LA4300系列	LA4310/LA4310V/LA4320/LA4320V/ LA4320X		LA4320/LA4320V/LA4320X支持，LA4310/LA4310V不支持，所有在5G射频配置的选项均不支持
小贝系列	WAP722/WAP722E/WAP722S		支持
	WAP712/WAP712C		支持

射频（Radio Frequency）表示具有远距离传输能力、可以辐射到空间的电磁频率。在 IEEE 802.11 无线局域网协议中的 802.11b/g 工作于 2.4GHz 射频段、802.11a/ac 工作于 5GHz 射频段、802.11n 可以同时工作于 2.4GHz 和 5GHz 射频段。按照不同的工作频率可以将射频划分为信道（表示以无线信号作为传输媒体的传送通道），每个信道对应一个频率范围。

1.1 配置射频设置

说明

只有射频处于关闭状态时才能配置射频。

(1) 在导航栏中选择“射频 > 射频设置”。

(2) 在列表中选择需要配置的射频单元，单击对应的图标，进入射频的配置页面，如下图所示。

图1-1 射频设置



(3) 配置射频，详细配置如下表所示。

表1-1 射频设置的详细配置

配置项	说明
射频单元	显示选择AP的射频单元
射频模式	显示选择射频单元的射频模式 如果改变AP的射频模式，功率和信道会恢复到对应模式下的缺省情况
发送功率	射频的最大传输功率 射频的最大功率和国家码、信道、AP型号、射频模式和天线类型相关，如果采用802.11n射频模式，那么射频的最大功率和带宽 模式也相关
信道	指定射频的工作信道。信道列表由国家码和射频模式决定 auto：自动选择信道模式。选择此模式后，AP会评估无线网络中的信道质量，自动选择质量最优的信道作为工作信道 更改工作信道设置后，功率列表会自动刷新
天线增益	配置第三方天线的增益值
802.11n	提示 只有支持 802.11n 的 AP 且选择的射频模式为 802.11n 时，下列 802.11n 的选项才可见
802.11ac	提示 只有支持 802.11ac 的 AP 且选择的射频模式为 802.11ac 时，下列 802.11ac 的选项才可见

配置项	说明
带宽模式	802.11n通过将两个20MHz的带宽绑定在一起组成一个40MHz通讯带宽，在实际工作时可以作为两个20MHz的带宽使用（一个为主信道，一个为辅信道），这样可将速率提高一倍，提高无线网络的吞吐量 • 20MHz：工作带宽为 20MHz • 40MHz：工作带宽为 40MHz 缺省情况下，802.11n(5GHz)的带宽为40MHz，802.11n(2.4GHz)的带宽为20MHz 802.11ac通过采用由四个20MHz的带宽绑定成一个80MHz带宽的方式增加了通信带宽，提高了吞吐量。同时，802.11ac也继承了802.11n中的提高信道利用率的方式确保设备的吞吐量。目前，802.11ac仅支持5GHz频段 • 80MHz：工作带宽为 80MHz 缺省情况下，802.11ac的带宽为80MHz 提示 • 在指定带宽为 40MHz 情况下，如果找到两条可以绑定到一起的信道，那么使用 40MHz 带宽，如果找不到可以绑定的信道，那么实际只能使用 20MHz 带宽，关于此部分的协议规范可参见“IEEE 802.11n-2009” • 在指定带宽为 80MHz 情况下，如果找到相应的中心频率，那么使用 80MHz 带宽；如果找不到相应的中心频率，则尝试采用 40MHz 带宽；若采用 40MHz 能够找到可用的可以绑定的信道，那么将 40MHz 带宽作为工作带宽，如果找不到可以绑定的信道，则实际只能使用 20MHz 带宽作为工作带宽。关于此部分的协议规范可参见“IEEE P802.11ac™/D5.0” • 更改带宽模式设置后，功率会自动刷新
MIMO	用来配置射频的MIMO模式 • 缺省：表示不配置射频的 MIMO 模式 • 1x1：表示配置射频采用一条流发送和接收 • 2x2：表示配置射频采用两条流发送和接收 • 3x3：表示配置射频采用三条流发送和接收 提示 只有至少支持 2 条流的 802.11n 或 802.11ac 射频才支持此功能 **说明** 仅 WA4620i-ACN/WA4620E-ACN 支持 3x3 MIMO 模式
允许带宽自动切换	选中“允许带宽自动切换”前的复选框，表示允许射频带宽自动切换。当802.11gn射频工作在40MHz带宽下，默认不开启带宽自动切换功能 **说明** 仅射频模式为 802.11gn 时支持

配置项	说明
接入类型	用来配置射频允许接入AP的客户端类型 • 全部类型：表示当前射频允许 802.11a/an/ac 类型客户端接入 AP • 802.11n 及 802.11ac：表示只有 802.11n 和 802.11ac 的客户端才能接入 AP • 802.11ac：表示只有 802.11ac 的客户端才能接入 AP 缺省情况下，允许802.11a/11an/ac类型客户端接入 **说明** 仅射频模式为 802.11ac 时支持 如果用户需要采用“802.11n及 802.11ac”或“802.11ac”，则必须配置NSS，NSS的配置请参见“1.2.3 配置 802.11ac射频速率”
绿色自动节能	选中“绿色自动节能”前的复选框，表示开启绿色自动节能。默认不开启绿色自动节能功能 **说明** 仅射频模式为 802.11n 和 802.11ac 时支持
只允许11n用户接入	选中“只允许11n用户接入”前的复选框，表示只有802.11n的客户端才能接入AP。如果需要接入802.11n客户端的同时，还要兼容802.11a/b/g客户端，则不要选中该选项 **说明** 如果用户需要采用“只允许 11n用户接入”，则必须配置基本MCS，基本MCS的配置请参见“1.2.2 配置 802.11n MCS”
A-MSDU	选中“A-MSDU”前的复选框，表示开启A-MSDU功能 802.11n和802.11ac协议定义了一个新的MAC特性A-MSDU，该特性实现了将多个MSDU组合成一个MSDU发送，通过聚合，A-MSDU减少了传输每个MSDU的MAC头的附加信息，提高了MAC层的传输效率
A-MPDU	选中“A-MPDU”前的复选框，表示开启A-MPDU功能 802.11n和802.11ac标准中采用A-MPDU聚合帧格式，即将多个MPDU聚合为一个A-MPDU，只保留一个PHY头，删除其余MPDU的PHY头，减少了传输每个MPDU的PHY头的附加信息，同时也减少了ACK帧的数目，从而降低了协议的负荷，有效的提高网络吞吐量
short GI	选中“short GI”前的复选框，表示开启short GI功能 802.11a/g的GI时长为800ns，802.11n和802.11ac可以配置使用Short GI，Short GI时长为400ns。在使用Short GI的情况下，可提高10%的无线吞吐量

(4) 展开射频的高级配置部分，如下图所示。

图1-2 射频设置（高级设置）



(5) 配置射频，详细配置如下表所示。

(6) 单击<确定>按钮完成操作。

表1-2 射频设置的详细配置

配置项	说明
前导码	前导码是位于数据包起始处的一组bit位，接收者可以据此同步并准备接收实际的数据。 • 短：短前导码。选择短前导码能使网络同步性能更好，一般选择短前导码 • 长：长前导码。在网络中需要兼容一些比较老的客户端网卡时，可以选择长前导码进行兼容 802.11a/802.11n(5GHz)/802.11ac(5GHz)不支持此项配置
发射距离	射频可覆盖的最大距离

配置项	说明
分片门限	指定帧的分片门限值。分片的基本原理是将一个大的帧分成小的分片，每个分片独立地传输和确认。当数据包的实际大小超过指定的分片门限值时，该数据包被分片传输 在误码率较高的无线环境下，可以把分片门限适当降低，这样在传输失败的情况下，只有未成功发送的部分需要重新发送，从而提高帧传输的吞吐量 在无干扰环境下，适当提高分片门限，可以减少确认帧的次数，也可以提高帧传输的吞吐量 **说明** 配置分片门限时，WMM 功能必须处于关闭状态
Beacon间隔	发送信标帧的时间间隔。信标帧按规定的时间间隔周期性发送，以允许移动用户接入网络。与其它接入点设备或其它网络控制设备进行联络
RTS（CTS）方式	在配置冲突避免机制时，支持用户配置RTS/CTS和CTS to self两种方式： • RTS/CTS 方式：当 AP 向某个客户端发送数据的时候，AP 会向客户端发送一个 RTS 报文，这样所有在 AP 覆盖范围内设备在收到 RTS 后都会在指定的时间内不发送数据。该客户端收到 RTS 后，会再发送一个 CTS 报文，这样保证在该客户端覆盖范围内的所有的设备都会在指定的时间内不发送数据。使用 RTS/CTS 方式实现冲突避免需要发送两个报文，报文开销较大 • CTS to self 方式：当 AP 需要向客户端发送报文的时候，会使用自己的地址发送一个 CTS 通告 AP 要发送报文，这样所有在 AP 覆盖范围内的设备都会在指定的时间内不发送数据。使用 CTS to self 方式只需发送一个控制报文就可以满足冲突避免的大部分应用环境，但是如果有另一个设备在客户端的覆盖范围，但是不在 AP 的覆盖范围内，仍然可能会产生冲突 和RTS/CTS相比，CTS-To-Self机制减少了控制报文的数量。但在某些情况下可能会出现因为隐藏节点收不到AP发送的CTS报文而仍然产生冲突的情况。因此，RTS-CTS机制比CTS-To-Self机制的保护范围要大
RTS（CTS）门限	启用冲突避免机制所要求的帧的长度门限值。当帧的实际长度大于设定的门限值时，会启用冲突避免机制 冲突避免用于在无线局域网中避免数据发送冲突。RTS（CTS）包的发送频率需要合理设置，设置RTS（CTS）门限时需要进行权衡：如果将门限值设得较小，则会增加RTS（CTS）包的发送频率，消耗更多的带宽。但RTS（CTS）包发送得越频繁，无线网络从冲突中恢复得就越快 在高密度无线网络环境可以降低此门限值，以减少冲突发生的概率 **提示** 使用冲突避免机制会占用一定的网络带宽，所以只在传输高于 RTS（CTS）门限的数据帧时才使用，对于小于 RTS（CTS）门限的数据帧不启动该机制
DTIM周期	设置信标帧的DTIM（Delivery Traffic Indication Message，数据待传指示信息）周期 当DTIM计数达到0时，AP才会发送缓存中的多播帧或广播帧
长帧重传门限	设置帧长超过RTS（CTS）门限值的单播帧的最大重传次数
短帧重传门限	设置帧长不大于RTS（CTS）门限值的单播帧的最大重传次数
接收帧缓存时间	AP接收到的帧可以在缓存区保存的最大时间

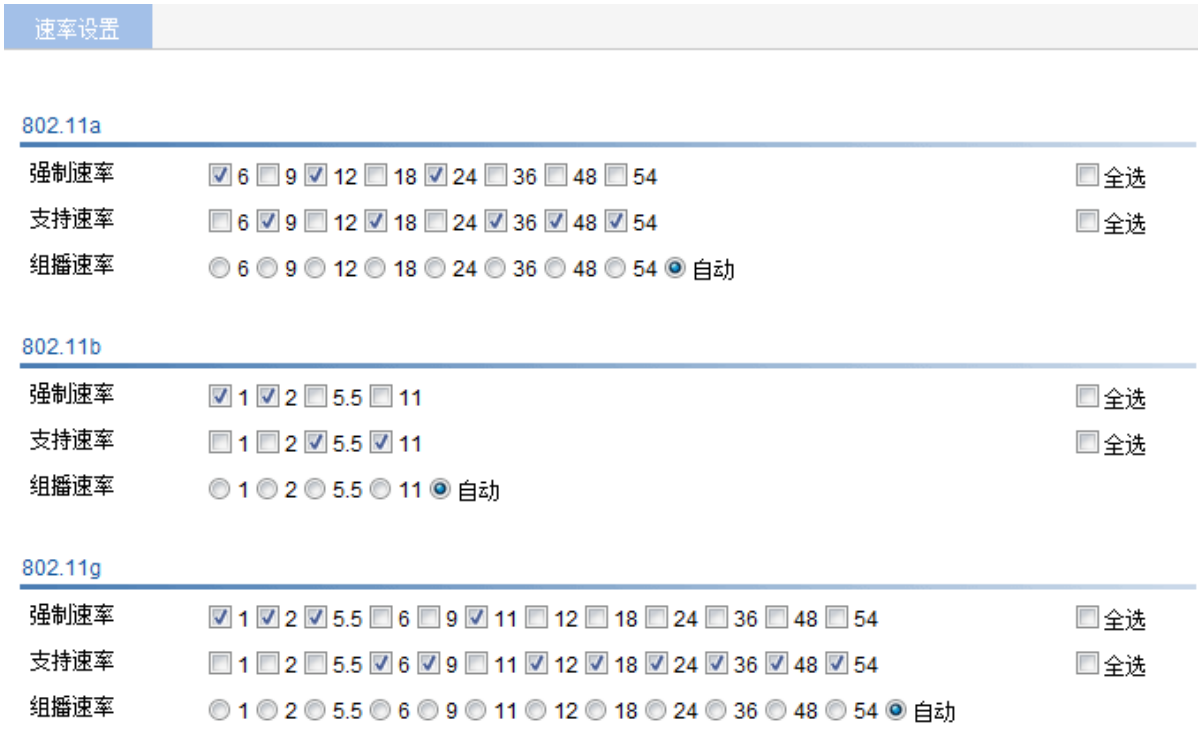
配置项	说明
STBC	• 开启：开启 STBC • 关闭：关闭 STBC 缺省情况下，STBC处于开启状态 开启STBC后，可以提高接收端的SNR，增强数据传输的可靠性 STBC可用于无线接入、WDS链路。用于WDS链路时，为使性能达到最佳，建议在发送设备和接收设备上同时开启STBC 当AP上存在的天线 > Radio使用速率对应的空间流时，STBC才能生效
LDPC	• 开启：开启 LDPC • 关闭：关闭 LDPC 缺省情况下，LDPC（Low Density Parity Check Code）处于关闭状态
智能天线	• 开启：开启智能天线 • 关闭：关闭智能天线 使用智能天线，可以有以下作用： • 保证覆盖范围内的客户端具有较高和稳定的带宽 • 在高密度的无线网络环境中，减少 AP 和客户端之间形成的干扰，避开非无线设备形成的干扰 缺省情况下，智能天线处于开启状态 只有为射频配置使用内置天线的情况下，智能天线才会起作用。在导航栏中选择“射频 > 天线切换”页面可以选择内置天线 不支持智能天线的设备该选项为不可选状态
智能天线策略	• 自动：使用自适应策略，对语音视频等报文使用高可靠性策略，对其它报文使用高吞吐量策略 • 可靠性：使用高可靠性策略 • 高吞吐量：使用高吞吐量策略 缺省情况下，智能天线使用自适应策略

1.2 配置射频速率

1.2.1 配置 802.11a/802.11b/802.11g射频速率

(1) 在导航栏中选择“射频管理 > 速率设置”，进入射频速率的配置页面，如下图所示。

图1-3 速率设置



(2) 配置 802.11a/802.11b/802.11g 射频速率，详细配置如下表所示。

(3) 单击<确定>按钮完成操作。

表1-3 802.11a/802.11b/802.11g 射频速率的详细配置

配置项	说明
802.11a	802.11a速率设置 缺省情况下： • 强制速率：6，12，24； • 支持速率：9，18，36，48，54； • 组播速率：自动从强制速率集中选取，在所有客户端都支持的强制速率中选取发送速率，作为 BSS 中的多播报文的发送速率
802.11b	802.11b速率设置 缺省情况下： • 强制速率：1，2； • 支持速率：5.5，11； • 组播速率：自动从强制速率集中选取，在所有客户端都支持的强制速率中选取发送速率，作为 BSS 中的多播报文的发送速率

配置项	说明
802.11g	802.11g速率设置 缺省情况下： • 强制速率：1，2，5.5，11； • 支持速率：6，9，12，18，24，36，48，54； • 组播速率：自动从强制速率集中选取，在所有客户端都支持的强制速率中选取发送速率，作为 BSS 中的多播报文的发送速率

1.2.2 配置 802.11n MCS

1. MCS简介

802.11n 射频速率的配置通过 MCS（Modulation and Coding Scheme，调制与编码策略）索引值实现。MCS 调制编码表是 802.11n 协议为表征 WLAN 的通讯速率而提出的一种表示形式。MCS 将所关注的影响通讯速率的因素作为表的列，将 MCS 索引作为行，形成一张速率表。所以，每一个 MCS 索引其实对应了一组参数下的物理传输速率，下面分别列举了带宽为 20MHz 和带宽为 40MHz 的 MCS 速率表（全部速率的描述可参见“IEEE P802.11n D2.00”）。

从表中可以得到结论：当 MSC 索引取值为 0～7 时，空间流数量为 1，当 MCS＝7 时，速率值最大。当 MSC 索引取值为 8～15 时，空间流数量为 2，当 MCS＝15 时，速率值最大。当 MSC 索引取值为 16～23 时，空间流数量为 3，当 MCS＝23 时，速率值最大。

说明

完整的 MCS 对应速率表可参见“IEEE 802.11n-2009”。

表1-4 MCS 对应速率表（20MHz）

MCS 索引	空间流数量	调制方式	速率(Mb/s)	
			800ns GI	400ns GI
0	1	BPSK	6.5	7.2
1	1	QPSK	13.0	14.4
2	1	QPSK	19.5	21.7
3	1	16-QAM	26.0	28.9
4	1	16-QAM	39.0	43.3
5	1	64-QAM	52.0	57.8
6	1	64-QAM	58.5	65.0
7	1	64-QAM	65.0	72.2
8	2	BPSK	13.0	14.4
9	2	QPSK	26.0	28.9
10	2	QPSK	39.0	43.3

MCS 索引	空间流数量	调制方式	速率(Mb/s)	
			800ns GI	400ns GI
11	2	16-QAM	52.0	57.8
12	2	16-QAM	78.0	86.7
13	2	64-QAM	104.0	115.6
14	2	64-QAM	117.0	130.0
15	2	64-QAM	130.0	144.4
16	3	BPSK	19.5	21.7
17	3	QPSK	39.0	43.3
18	3	QPSK	58.5	65.0
19	3	16-QAM	78.0	86.7
20	3	16-QAM	117.0	130.0
21	3	64-QAM	156.0	173.3
22	3	64-QAM	175.5	195.0
23	3	64-QAM	195.0	216.7

表1-5 MCS 对应速率表（40MHz）

MCS 索引	空间流数量	调制方式	速率(Mb/s)	
			800ns GI	400ns GI
0	1	BPSK	13.5	15.0
1	1	QPSK	27.0	30.0
2	1	QPSK	40.5	45.0
3	1	16-QAM	54.0	60.0
4	1	16-QAM	81.0	90.0
5	1	64-QAM	108.0	120.0
6	1	64-QAM	121.5	135.0
7	1	64-QAM	135.0	150.0
8	2	BPSK	27.0	30.0
9	2	QPSK	54.0	60.0
10	2	QPSK	81.0	90.0
11	2	16-QAM	108.0	120.0
12	2	16-QAM	162.0	180.0
13	2	64-QAM	216.0	240.0
14	2	64-QAM	243.0	270.0
15	2	64-QAM	270.0	300.0

MCS 索引	空间流数量	调制方式	速率(Mb/s)	
			800ns GI	400ns GI
16	3	BPSK	40.5	45
17	3	QPSK	81.0	90.0
18	3	QPSK	121.5	135.0
19	3	16-QAM	162.0	180.0
20	3	16-QAM	243.0	270.0
21	3	64-QAM	324.0	360.0
22	3	64-QAM	364.5	405.0
23	3	64-QAM	405.0	450.0

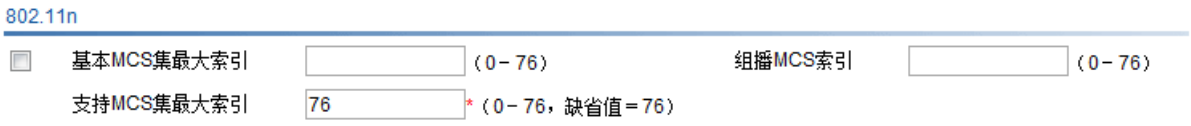
用户对 MCS 的配置分为三类，配置基本 MCS、支持 MCS 和组播 MCS。配置输入的 MCS 索引是一个范围，即指 0～配置值，如输入 5，即指定了所要输入的 MCS 范围为 0～5。

- 基本 MCS：基本 MCS 是指 AP 正常工作所必须支持的 MCS 速率集，客户端必须满足 AP 所配置的基本 MCS 速率才能够与 AP 以 802.11n 模式进行连接。
- 支持 MCS：支持 MCS 速率集是在 AP 的基本 MCS 速率集基础上 AP 所能够支持的更高的速率集合，用户可以配置支持 MCS 速率集让客户端在满足基本 MCS 的前提下选择更高的速率与 AP 进行连接。
- 组播 MCS：802.11n 的组播 MCS 索引。

2. 配置 802.11n射频速率

(1) 在导航栏中选择“射频 > 速率设置”，进入射频速率的配置页面，如 图 1-3 所示。在页面 802.11n 部分进行射频速率的配置，如下图所示。

图1-4 配置 802.11n 射频速率



(2) 配置 802.11n 速率，详细配置如下表所示。

(3) 单击<确定>按钮完成操作。

表1-6 802.11n 射频速率的详细配置

配置项	说明
基本MCS集最大MCS索引	选中“基本MCS集最大MCS索引”前的复选框，设置802.11n的基本MCS集的最大MCS索引号

配置项	说明
组播MCS索引	设置802.11n的组播MCS索引 对于802.11n模式，当所有的客户端都使用802.11n射频时，才使用组播MCS索引，如果存在非802.11n客户端，则使用基础模式的组播速率 提示 • 在设置组播 MCS 索引时，如果设置的值超过了射频支持的最大值，则实际采用的组播 MCS 索引值为射频支持的最大值 • 组播 MCS 起作用时，无论是 20M 模式还是 40M 模式，统一采用 20M 模式没有开启 SGI 功能时对应的速率进行发送
支持MCS集最大MCS索引	设置802.11n的支持MCS集的最大MCS索引号 需要注意的是，支持MCS集最大MCS索引不能小于基本MCS集最大MCS索引

说明

- 关于 MCS 的详细介绍请参见“WLAN 配置指导”中的“WLAN RRM”。
- 在 WDS 使用 802.11n 射频的情况下，请确保在各 AP 上关于 MCS 索引的配置保持一致。

1.2.3 配置 802.11ac射频速率

1. 802.11ac射频速率简介

802.11ac射频速率的配置通过NSS（Number of Spatial Streams，空间流数）值实现。802.11ac协议表示WLAN的通讯速率的方式与 802.11n协议有很大的不同。在 802.11ac协议中，提出了与MCS类似的VHT-MCS（Very High Throughput Modulation and Coding Scheme，超高吞吐量调制与编码策略）概念来表征WLAN的通讯速率。VHT-MCS将所关注的影响通讯速率的因素作为表的列，将VHT-MCS索引作为行，形成一张速率表。但在 802.11ac协议中，VHT-MCS速率表与空间流数共同决定VHT-MCS索引对应的一组参数下的物理传输速率，表 1-7、表 1-8 和 表 1-9 分别列举了带宽为20MHz、带宽为 40MHz和带宽为 80MHz针对于NSS = 1 情况的VHT-MCS速率表。

根据协议：空间流数取值范围为 1～8；在每个空间流数中，VHT-MSC 索引取值范围为 0～9。

说明

完整的 VHT-MCS 对应速率表可参见“IEEE Draft P802.11ac_D5.0”。

表1-7 VHT-MCS 对应速率表（20MHz Nss = 1）

VHT-MCS 索引	调制方式	速率(Mb/s)	
		800ns GI	400ns GI
0	BPSK	6.5	7.2
1	QPSK	13.0	14.4
2	QPSK	19.5	21.7

VHT-MCS 索引	调制方式	速率(Mb/s)	
		800ns GI	400ns GI
3	16-QAM	26.0	28.9
4	16-QAM	39.0	43.3
5	64-QAM	52.0	57.8
6	64-QAM	58.5	65.0
7	64-QAM	65.0	72.2
8	256-QAM	78.0	86.7
9	not valid		

表1-8 VHT-MCS 对应速率表（40MHz Nss = 1）

MCS 索引	调制方式	速率(Mb/s)	
		800ns GI	400ns GI
0	BPSK	13.5	15.0
1	QPSK	27.0	30.0
2	QPSK	40.5	45.0
3	16-QAM	54.0	60.0
4	16-QAM	81.0	90.0
5	64-QAM	108.0	120.0
6	64-QAM	121.5	135.0
7	64-QAM	135.0	150.0
8	256-QAM	162.0	180.0
9	256-QAM	180.0	200.0

表1-9 VHT-MCS 对应速率表（80MHz Nss = 1）

MCS 索引	调制方式	速率(Mb/s)	
		800ns GI	400ns GI
0	BPSK	29.3	32.5
1	QPSK	58.5	65.0
2	QPSK	87.8	97.5
3	16-QAM	117.0	130.0
4	16-QAM	175.5	195.0
5	64-QAM	234.0	260.0
6	64-QAM	263.3	292.5
7	64-QAM	292.5	325.0

MCS 索引	调制方式	速率(Mb/s)	
		800ns GI	400ns GI
8	256-QAM	351.0	390.0
9	256-QAM	390.0	433.3

NSS 分为三类：基本 NSS、支持 NSS 和组播 NSS。

- 基本 NSS：基本 NSS 是指 AP 正常工作所必须支持的 NSS，客户端必须满足 AP 所配置的基本 NSS 才能够与 AP 以 802.11ac 模式进行连接。
- 支持 NSS：支持 NSS 是在 AP 的基本 NSS 基础上 AP 所能够支持的更高的速率集合，用户可以配置支持 NSS 速率集让客户端在满足基本 NSS 的前提下选择更高的速率与 AP 进行连接。
- 组播 NSS：在基本 NSS 的基础上，AP 所能够支持的更高的组播 NSS 集合，组播 NSS 使设备能够以配置的组播 NSS 发送组播数据。

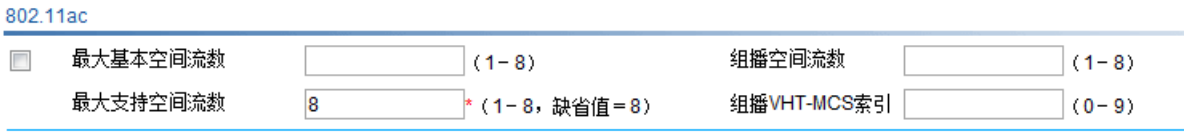
需要注意的是：

- 配置 NSS 值时，输入的 NSS 值表示的是一个范围，即指 0～配置值，例如输入 5，则表示指定了所设置的 NSS 值为 0～5。
- 针对 802.11ac 类型射频配置组播速率，不仅需要指定组播 NSS，同时需要指定具体的组播 VHT-MCS。

2. 配置 802.11ac射频速率

(1) 在导航栏中选择“射频 > 速率设置”，进入射频速率的配置页面，如 图 1-3 所示。在页面802.11ac部分进行射频速率的配置，如下图所示。

图1-5 配置 802.11ac 射频速率



(2) 配置 802.11ac 速率，详细配置如下表所示。

(3) 单击<确定>按钮完成操作。

表1-10 802.11ac 射频速率的详细配置

配置项	说明
最大基本空间流数	802.11ac的基本最大空间流数
组播空间流数	802.11ac的组播空间流数
最大支持空间流数	802.11ac的支持速率集的最大空间流数
组播VHT-MCS索引	802.11ac的组播VHT-MCS索引

1.3 配置功率信道优化

1.3.1 功率信道信息

(1) 在导航栏中选择“射频> 功率信道优化”，默认进入“功率信道信息”页签的页面。

(2) 点击射频单元，可以查看信道切换记录，如下图所示。信道切换记录的各字段说明如下表所示。

图1-6 功率信道信息



表1-11 信道切换记录描述表

字段	描述
NO	显示信道切换记录的顺序号
Chl(After/Before)	显示信道变化情况（变更后 / 变更前）
Date(yyyy-mm-dd)	显示发生信道切换的日期（年-月-日）
Time(hh:mm:ss)	显示发生信道切换的时间（时：分：秒）

1.3.2 参数设置

(1) 在导航栏中选择“射频> 功率信道优化”。

(2) 选择“参数设置”页签，进入功率信道优化参数的配置页面，如下图所示。

图1-7 参数设置



(3) 配置功率信道优化的参数，详细配置如下表所示。

(4) 单击<确定>按钮完成操作。

表1-12 参数设置的详细配置

字段	说明
802.11g保护功能	当网络中同时接入了802.11b和802.11g的用户，由于调制方式不同，这两种用户很容易产生冲突，导致网络速率严重下降。为了保证802.11b用户和802.11g用户能够同时正常工作，可启动802.11g保护机制，使运行802.11g的设备发送RTS/CTS或CTS-to-self来避免和802.11b设备发生冲突，确保802.11b和802.11g用户可以同时工作 • 开启：开启 802.11g 保护功能 • 关闭：关闭 802.11g 保护功能 以下两种情况会使运行802.11g的AP启动802.11g保护功能： 情况一：802.11b的客户端和运行802.11g的AP相关联； 情况二：运行802.11g的AP探测到周边同一信道内的运行802.11b的AP或无线客户端 提示 • 需要注意的是，开启 802.11g 保护功能会降低网络性能 • 这里的开启“802.11g 保护功能”，仅是针对“情况二”。对于“情况一”，802.11g 保护功能始终是启用的，不受用户界面配置所控制
802.11g保护方式	• RTS/CTS：使用 RTS/CTS 方式实现 802.11g 保护方式。当 AP 向某个客户端发送数据的时候，AP 会向客户端发送一个 RTS 报文，这样所有在 AP 覆盖范围内设备在收到 RTS 后都会在指定的时间内不发送数据。该客户端收到 RTS 后，会再发送一个 CTS 报文，这样保证在该客户端覆盖范围内的所有的设备都会在指定的时间内不发送数据 • CTS-to-Self：使用 CTS-to-Self 方式实现 802.11g 保护方式。当 AP 需要向客户端发送报文的时候，会使用自己的地址发送一个 CTS 通告 AP 要发送报文，这样所有在 AP 覆盖范围内设备都会在指定的时间内不发送数据

字段	说明
802.11n保护方式	802.11n保护方式可以采用RTS/CTS或CTS-to-self方式，两种方式的实现机制与802.11g保护方式相同，此处不再重复
802.11n保护功能	• 开启：开启 802.11n 保护功能。当周围环境中如果存在非 802.11n 设备或非 802.11n 客户端时，需要开启 802.11n 保护机制 • 关闭：关闭 802.11n 保护功能
频谱管理	• 开启：开启 802.11a 频段的频谱管理 • 关闭：关闭 802.11a 频段的频谱管理 缺省情况下，频谱管理处于关闭状态 开启频谱管理功能后，AP会通告其功率能力和对客户端的功率限制
功率限制	将设置的限制功率值通知给802.11a客户端。例如，配置功率限制值为5，设备会通知802.11a客户端将其最大发送功率降低5dBm 缺省情况下，不对802.11a客户端发送的功率进行限制 提示 在配置功率限制前，需要先开启频谱管理，否则该配置无效

1.4 配置信道扫描

1.4.1 设置信道扫描参数

(1) 在导航栏中选择“射频 > 信道扫描”，默认进入“信道扫描”页签的页面，如下图所示。

图1-8 信道扫描



(2) 配置信道扫描，详细配置如下表所示。

(3) 单击<确定>按钮完成操作。

表1-13 信道扫描的详细配置

配置项	说明
扫描802.11h信道	802.11h信道即雷达信道，使用了部分和802.11a重叠的频段，一旦设备选择了和802.11h相同的信道作为工作信道，可能会影响无线网络的服务质量。排除802.11h信道，设备在选择信道时，只扫描属于配置区域码的非802.11h信道，避免和802.11h信道产生冲突 • 包含：表示初始信道选择时，扫描的信道中包括 802.11h 信道 • 排除：表示初始信道选择时，扫描的信道中不包括 802.11h 信道 缺省情况下，选择信道没有限制，即扫描包括802.11h的所有属于国家码的合法信道
扫描类型	设置扫描类型： • 主动：主动扫描类型。主动扫描模下，AP 主动发送 Probe Request 报文，这种方式使 AP 更容易地发现周围设备。 • 被动：被动扫描类型。当 AP 需要节省电量时，可以使用被动扫描。一般语音终端通常使用被动扫描方式 缺省情况下，扫描类型为被动扫描 当AP具有检测功能时，扫描类型的含义如下： • 主动：在扫描过程中会模拟客户端发送 Probe Request 报文 • 被动：在扫描过程中不会发送 Probe Request 报文 当AP具有检测功能时，将扫描模式设置为主动扫描类型，可以增加检测到周围设备的概率
扫描报告间隔	设置扫描报告间隔为指定值 • 如果将扫描报告间隔设置的偏长，则每次扫描报告中检测到的设备会较多，有利于扫描检测的正确性 • 如果将扫描报告间隔设置的偏短，则扫描报告上送的频率会较快 当AP具有检测功能时，扫描报告间隔会影响扫描结果能否及时被处理和消息交互的频繁程度，请权衡网络中的实际情况进行设置
5GHz/2.4GHz信道排除列表	为了避免设备在自动选择信道时使用某些不合适的信道，用户可以通过配置信道排除列表使部分信道不参与信道选择。配置信道排除列表之后，设备在进行信道选择前会过滤指定的信道，被排除的信道将不会参与自动选择信道（无线接入服务）、自动信道调整。WIDS攻击检测等不会受此配置影响 选中信道前的复选框，将信道加入到5GHz/2.4GHz信道排除列表中 缺省情况下，信道排除列表中不存在任何信道 提示 • 信道排除列表的选择范围不受国家码限制，即不在当前国家码范围内的信道也可被添加到信道排除列表中。修改国家码不会影响已经配置的信道排除列表。设备会在没有被排除的信道及国家码支持信道的交集内选择信道，因此在配置此功能时，请不要将当前国家码下的所有信道都添加到信道排除列表中 • 本功能只对自动选择信道、自动信道调整功能生效 • 如果用户将设备自动选择出来的信道加入到信道排除列表，那么设备会先自动关闭射频，再开启射频，然后会在没有被排除的信道及国家码支持信道的交集内重新选择一个可用信道 • 自动选择出来的主信道加入到信道排除列表，设备会重新选择一个可用的主信道；在设备自动选择主信道的情况下，如果将辅信道加入到信道排除列表，设备也会重新选择辅信道，如果设备找不到可用的辅信道，无线接入服务将没有可用信道

1.4.2 设置AP工作模式

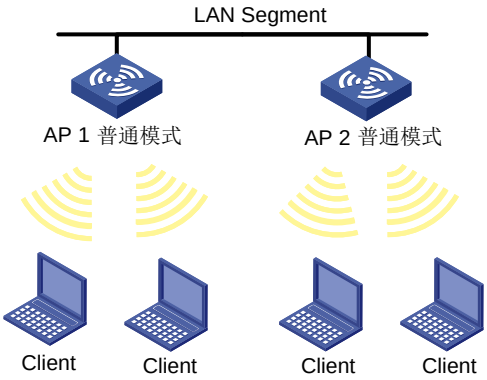
1. AP工作模式简介

FAT AP 支持以下三种工作模式：

- 普通工作模式

当 AP 工作在普通模式时，如下图所示，AP 1 和 AP 2 作为无线接入点，为无线客户端提供接入服务。

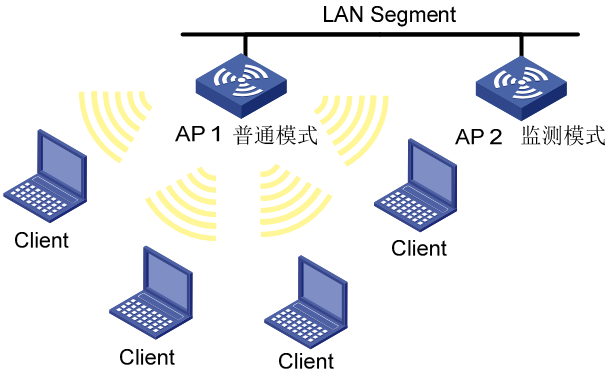
图1-9 普通工作模式



- 监测工作模式

当AP工作在监测模式时，AP需要扫描无线环境中的设备，记录检测记录，此时AP仅做监测AP，不做接入AP。如下图所示，将AP 2 设置为监测模式，AP 2 将监听所有的 802.11 帧，检测记录请参见“1.5.1 查看检测记录”。

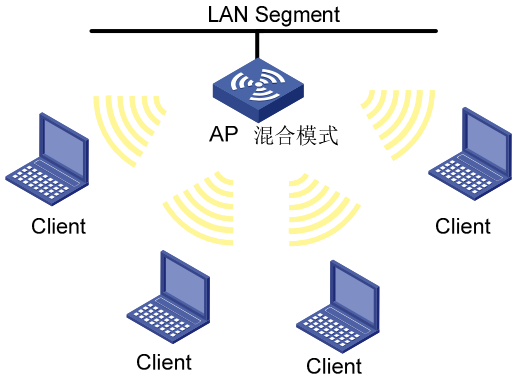
图1-10 监测工作模式



- 混合工作模式

当 AP 工作在混合模式时，如下图所示，AP 可以在做监测 AP 的同时也可以作为无线接入点。

图1-11 混合工作模式



说明

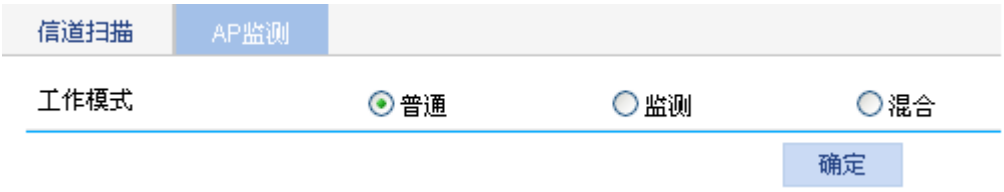
当 AP 工作在监测工作模式或混合工作模式时，可以对周围的无线环境进行检测。网络管理员通过查看检测记录，可以监控无线环境的质量，以便在干扰较强时，能够对网络环境及时进行调整。

2. 设置AP工作模式

(1) 在导航栏中选择“射频 > 信道扫描”。

(2) 选择“AP 监测”页签，进入 AP 工作模式的配置页面，如下图所示。

图1-12 设置 AP 监测的工作模式



(3) 配置 AP 工作模式，详细配置如下表所示。

(4) 单击<确定>按钮完成操作。

表1-14 AP 工作模式的详细配置

配置项	说明
工作模式	设置工作模式： • 普通：AP 仅传输 WLAN 用户的数据，不进行任何监测 • 监测：在这种模式下，AP 需要扫描无线环境中的设备，此时 AP 仅做监测 AP，不做接入 AP。当 AP 工作在监测模式时，该 AP 提供的所有 WLAN 服务都将关闭。处于监测模式的 AP，监听所有 802.11 帧 • 混合：在这种模式下，AP 可以在做监测 AP 的同时也传输 WLAN 数据 提示 • 当 AP 从普通或混合模式切换到监测模式时，不再提供接入服务，会使已经上线的客户端下线 • 当 AP 从监测模式切换到普通或混合模式时，AP 会重启

说明

- 如果 AP 工作模式为“混合”，需要对无线服务进行配置，这样 AP 在监测的同时可以提供无线服务。
- 如果 AP 工作模式为“监测”，那么 AP 不需要提供无线服务，不必配置无线服务。

1.5 信道环境检测

1.5.1 查看检测记录

在导航栏中选择“射频 > 信道环境检测”，默认进入“检测记录”页签的页面，如下图所示。

图1-13 查看检测记录



说明

目前支持检测 AP、Wireless bridge、Client 和 Adhoc 四种设备类型。

1.5.2 设置检测记录老化时间

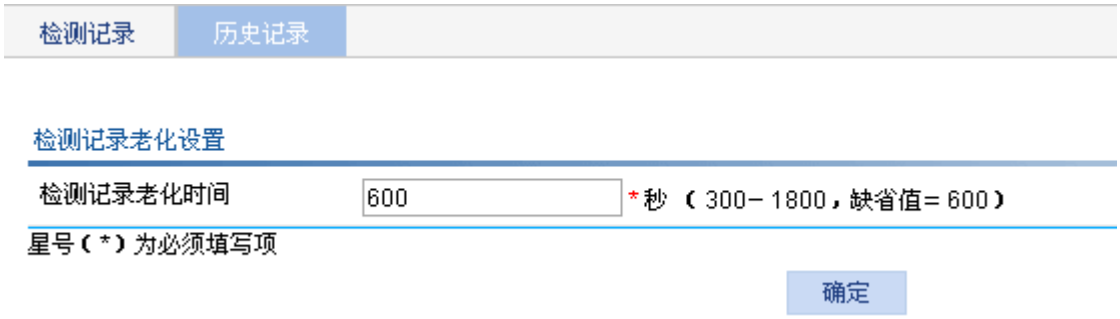
(1) 在导航栏中选择“射频 > 信道环境检测”。

(2) 选择“历史记录”页签，进入历史记录页面。

(3) 在页面上部配置检测记录老化时间，如下图所示。

(4) 单击<确定>按钮完成操作。

图1-14 设置检测记录老化时间



1.5.3 查看历史记录

(1) 在导航栏中选择“射频 > 信道环境检测”。

(2) 选择“历史记录”页签，进入历史记录页面。

(3) 在页面下部的列表中查看信道环境监测的历史记录，如下图所示。

图1-15 查看历史记录



说明

如果在老化时间内，“检测记录”的表项没有再被检测到，那么该表项会从检测记录中删除并被添加到历史记录中。

1.6 天线切换

在导航栏中选择“射频> 天线切换”，如下图所示，可以给相应的射频模式选择适当的天线。

图1-16 配置天线切换



目 录

1 AAA ····· 1-1
1.1 概述 ····· 1-1
1.2 AAA配置任务简介 ····· 1-1
1.3 配置ISP域 ····· 1-2
1.4 配置ISP域的AAA认证方法 ····· 1-3
1.5 配置ISP域的AAA授权方法 ····· 1-5
1.6 配置ISP域的AAA计费方法 ····· 1-6
1.7 AAA典型配置举例 ····· 1-7
2 RADIUS ····· 2-1
2.1 概述 ····· 2-1
2.2 配置RADIUS方案 ····· 2-1
2.3 RADIUS典型配置举例 ····· 2-6
2.4 注意事项 ····· 2-14
3 HWTACACS ····· 3-1
3.1 概述 ····· 3-1
3.2 HWTACACS方案配置任务简介 ····· 3-1
3.3 创建HWTACACS方案system ····· 3-2
3.4 配置HWTACACS服务器信息 ····· 3-2
3.5 配置HWTACACS参数 ····· 3-3
3.6 HWTACACS典型配置举例 ····· 3-5
3.7 注意事项 ····· 3-9
4 用户 ····· 4-1
4.1 概述 ····· 4-1
4.2 配置本地用户 ····· 4-1
4.3 配置用户组 ····· 4-4
4.4 配置来宾用户 ····· 4-5
4.4.1 Management级别的普通用户配置来宾用户 ····· 4-5
4.4.2 来宾管理员配置来宾用户 ····· 4-7
5 证书管理 ····· 5-1
5.1 概述 ····· 5-1
5.2 PKI配置任务简介 ····· 5-1
5.3 新建PKI实体 ····· 5-4
5.4 新建PKI域 ····· 5-6

5.5 生成RSA密钥对 ····· 5-8
5.6 销毁RSA密钥对 ····· 5-9
5.7 获取和查看证书 ····· 5-9
5.8 申请本地证书 ····· 5-11
5.9 获取和查看CRL ····· 5-13
5.10 PKI典型配置举例 ····· 5-14
5.11 注意事项 ····· 5-18

1 AAA

1.1 概述

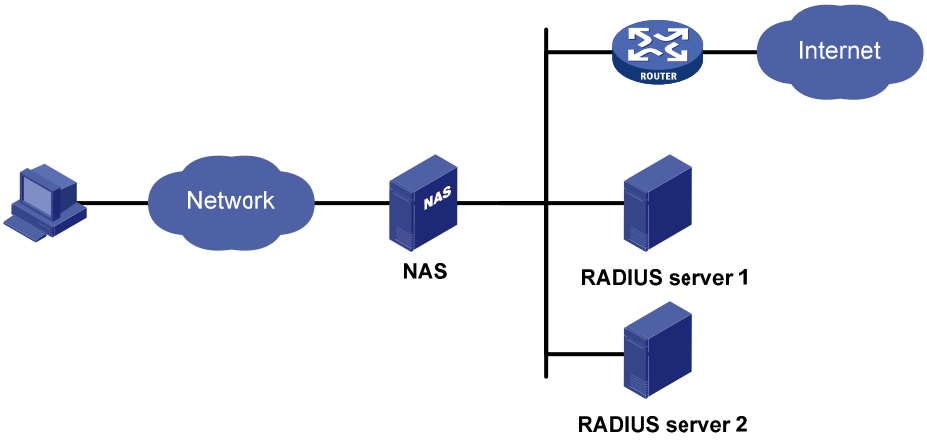
AAA 是 Authentication、Authorization、Accounting（认证、授权、计费）的简称，是网络安全的一种管理机制，提供了认证、授权、计费三种安全功能。

- 认证：确认远端访问用户的身份，判断访问者是否为合法的网络用户。
- 授权：对不同用户赋予不同的权限，限制用户可以使用的服务。例如用户成功登录服务器后，管理员可以授权用户对服务器中的文件进行访问和打印操作。
- 计费：记录用户使用网络服务中的所有操作，包括使用的服务类型、起始时间、数据流量等，它不仅是一种计费手段，也对网络安全起到了监视作用。

AAA 可以通过多种协议来实现，目前设备支持基于 RADIUS 协议、HWTACACS 协议来实现 AAA。在实际应用中，最常使用 RADIUS 协议。

AAA 一般采用客户端/服务器结构，客户端运行于 NAS（Network Access Server，网络接入服务器）上，服务器上则集中管理用户信息。NAS 对于用户来讲是服务器端，对于服务器来说是客户端。AAA 的基本组网结构如下图所示。

图1-1 AAA 基本组网结构示意图



说明

关于 AAA 的详细介绍请参见“安全配置指导”中的“AAA”。

1.2 AAA配置任务简介

进行 AAA 配置前要做如下准备：

- 要进行本地认证，需要配置本地用户，具体配置请参见“用户”。
- 要进行RADIUS认证，需要先配置RADIUS方案，具体配置请参见“RADIUS”。

- 要进行HWTACACS认证，需要先配置HWTACACS方案，具体配置请参见“HWTACACS”。

表1-1 AAA 配置步骤

步骤	配置任务	说明
1	1.3 配置ISP域	可选 配置ISP域，并指定其中一个为缺省ISP域 缺省情况下，系统存在名为system的缺省ISP域
2	1.4 配置ISP域的AAA认证方法	可选 配置对ISP域中不同类型的用户所使用的认证方法 缺省情况下，所有类型的用户采用Local认证方法
3	1.5 配置ISP域的AAA授权方法	可选 配置对ISP域中不同类型的用户所使用的授权方法 缺省情况下，所有类型的用户采用Local授权方法
4	1.6 配置ISP域的AAA计费方法	必选 配置对ISP域中不同类型的用户所使用的计费方法 缺省情况下，所有类型的用户采用Local计费方法

1.3 配置ISP域

(1) 在导航栏中选择“认证 > AAA”，默认进入“域设置”页签的页面，如下图所示。

图1-2 域设置



(2) 配置 ISP 域的信息，详细配置如下表所示。

(3) 单击<应用>按钮完成操作。

表1-2 ISP 域的详细配置

配置项	说明
域名	设置ISP域的名称，用于标识域 可以输入新的域名来创建域，也可以选择已有域来配置其是否为缺省域
缺省域	设置该ISP域是否为缺省域 • Enable：设置为缺省域 • Disable：设置为非缺省域 同时只能存在一个缺省域，当某个域被设置为缺省域时，原来的缺省域自动被设置为非缺省域

1.4 配置ISP域的AAA认证方法

(1) 在导航栏中选择“认证 > AAA”。

(2) 单击“认证”页签，进入如下图所示的页面。

图1-3 认证



(3) 配置 ISP 域中不同类型用户所使用的认证方法，详细配置如下表所示。

(4) 单击<应用>按钮，弹出配置进度对话框。

(5) 看到配置成功的提示后，在对话框中单击<关闭>按钮完成操作。

表1-3 ISP 域 AAA 认证方法的详细配置

配置项	说明
选择一个域名	设置要配置的ISP域
Default认证 方案名称 备选方法	设置所有类型用户的缺省认证方法和备选方法 • HWTACACS：HWTACACS 认证，此时需要设置具体选用的 HWTACACS 方案 • Local：本地认证 • None：不认证，即对用户非常信任，不进行合法性检查，一般情况下不采用此方法 • RADIUS：RADIUS 认证，此时需要设置具体选用的 RADIUS 方案 • Not Set：不设置 Default 认证，即恢复缺省情况（本地认证）
LAN-access认证 方案名称 备选方法	设置LAN-access用户的认证方法和备选方法 • Local：本地认证 • None：不认证，即对用户非常信任，不进行合法性检查，一般情况下不采用此方法 • RADIUS：RADIUS 认证，此时需要设置具体选用的 RADIUS 方案 • Not Set：不设置 LAN-access 认证，此时缺省使用 Default 认证的配置
Login认证 方案名称 备选方法	设置Login用户的认证方法和备选方法 • HWTACACS：HWTACACS 认证，此时需要设置具体选用的 HWTACACS 方案 • Local：本地认证 • None：不认证，即对用户非常信任，不进行合法性检查，一般情况下不采用此方法 • RADIUS：RADIUS 认证，此时需要设置具体选用的 RADIUS 方案 • Not Set：不设置 Login 认证，此时缺省使用 Default 认证的配置
PPP认证	设备不支持PPP认证的配置

配置项	说明
方案名称	
备选方法	
Portal认证	设备不支持Portal认证的配置
方案名称	

1.5 配置ISP域的AAA授权方法

(1) 在导航栏中选择“认证 > AAA”。

(2) 单击“授权”页签，进入如下图所示的页面。

图1-4 授权



(3) 配置 ISP 域中不同类型用户所使用的授权方法，详细配置如下表所示。

(4) 单击<应用>按钮，弹出配置进度对话框。

(5) 看到配置成功的提示后，在对话框中单击<关闭>按钮完成操作。

表1-4 ISP 域 AAA 授权方法的详细配置

配置项	说明
选择一个域名	设置要配置的ISP域
Default授权	设置所有类型用户的缺省授权方法和备选方法 • HWTACACS：HWTACACS 授权，此时需要设置具体选用的 HWTACACS 方案 • Local：本地授权 • None：直接授权，即对用户非常信任，直接授权通过，此时用户权限为系统默认权限 • RADIUS：RADIUS 授权，此时需要设置具体选用的 RADIUS 方案 • Not Set：不设置 Default 授权，即恢复缺省情况（本地授权）
方案名称	
备选方法	
LAN-access授权	设置LAN-access用户的授权方法和备选方法

配置项	说明
方案名称	• Local：本地授权 • None：直接授权，即对用户非常信任，直接授权通过，此时用户权限为系统默认权限 • RADIUS：RADIUS 授权，此时需要设置具体选用的 RADIUS 方案 • Not Set：不设置 LAN-access 授权，此时缺省使用 Default 授权的配置
备选方法	
Login授权	设置Login用户的授权方法和备选方法
方案名称	• HWTACACS：HWTACACS 授权，此时需要设置具体选用的 HWTACACS 方案 • Local：本地授权 • None：直接授权，即对用户非常信任，直接授权通过，此时用户权限为系统默认权限 • RADIUS：RADIUS 授权，此时需要设置具体选用的 RADIUS 方案 • Not Set：不设置 Login 授权，此时缺省使用 Default 授权的配置
备选方法	
PPP授权	设备不支持PPP授权的配置
方案名称	
备选方法	
Portal授权	设备不支持Portal授权的配置
方案名称	
Command授权	设备不支持Command授权的配置
方案名称	

1.6 配置ISP域的AAA计费方法

(1) 在导航栏中选择“认证 > AAA”。

(2) 单击“计费”页签，进入如下图所示的页面。

图1-5 计费



(3) 配置 ISP 域中不同类型用户所使用的计费方法，详细配置如下表所示。

(4) 单击<应用>按钮，弹出配置进度对话框。

(5) 看到配置成功的提示后，在对话框中单击<关闭>按钮完成操作。

表1-5 ISP 域 AAA 计费方法的详细配置

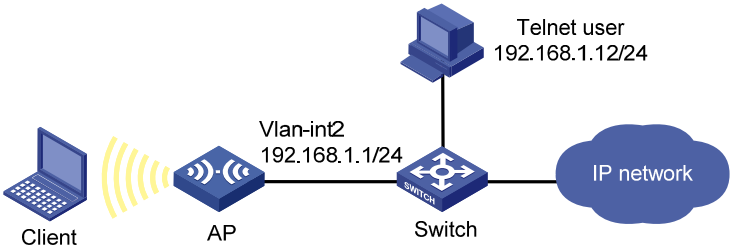
配置项	说明
选择一个域名	设置要配置的ISP域
计费可选开关	设置是否开启计费可选功能 • 对上线用户计费时，如果发现没有可用的计费服务器或与计费服务器通信失败时，若开启计费可选功能，则用户可以继续使用网络资源，否则用户连接将被切断 • 对于计费过程失败但因计费可选功能上线的用户，系统不再对其发送实时计费更新报文
Default计费 方案名称 备选方法	设置所有类型用户的缺省计费方法和备选方法 • HWTACACS：HWTACACS 计费，此时需要设置具体选用的 HWTACACS 方案 • Local：本地计费 • None：不计费 • RADIUS：RADIUS 计费，此时需要设置具体选用的 RADIUS 方案 • Not Set：不设置 Default 计费，即恢复缺省情况（本地计费）
LAN-access计费 方案名称 备选方法	设置LAN-access用户的计费方法和备选方法 • Local：本地计费 • None：不计费 • RADIUS：RADIUS 计费，此时需要设置具体选用的 RADIUS 方案 • Not Set：不设置 LAN-access 计费，此时缺省使用 Default 计费的配置
Login计费 方案名称 备选方法	设置Login用户的计费方法和备选方法 • HWTACACS：HWTACACS 计费，此时需要设置具体选用的 HWTACACS 方案 • Local：本地计费 • None：不计费 • RADIUS：RADIUS 计费，此时需要设置具体选用的 RADIUS 方案 • Not Set：不设置 Login 计费，此时缺省使用 Default 计费的配置
PPP计费 方案名称 备选方法	设备不支持PPP计费的配置
Portal计费 方案名称	设备不支持Portal计费的配置

1.7 AAA典型配置举例

1. 组网需求

如下图所示，配置 AP，实现对登录 AP 的 Telnet 用户进行本地认证和授权。

图1-6 AAA 配置组网图



2. 配置步骤

(1) 配置本地用户。

步骤 1：在导航栏中选择“认证 > 用户”，默认进入“本地用户”页签的页面。

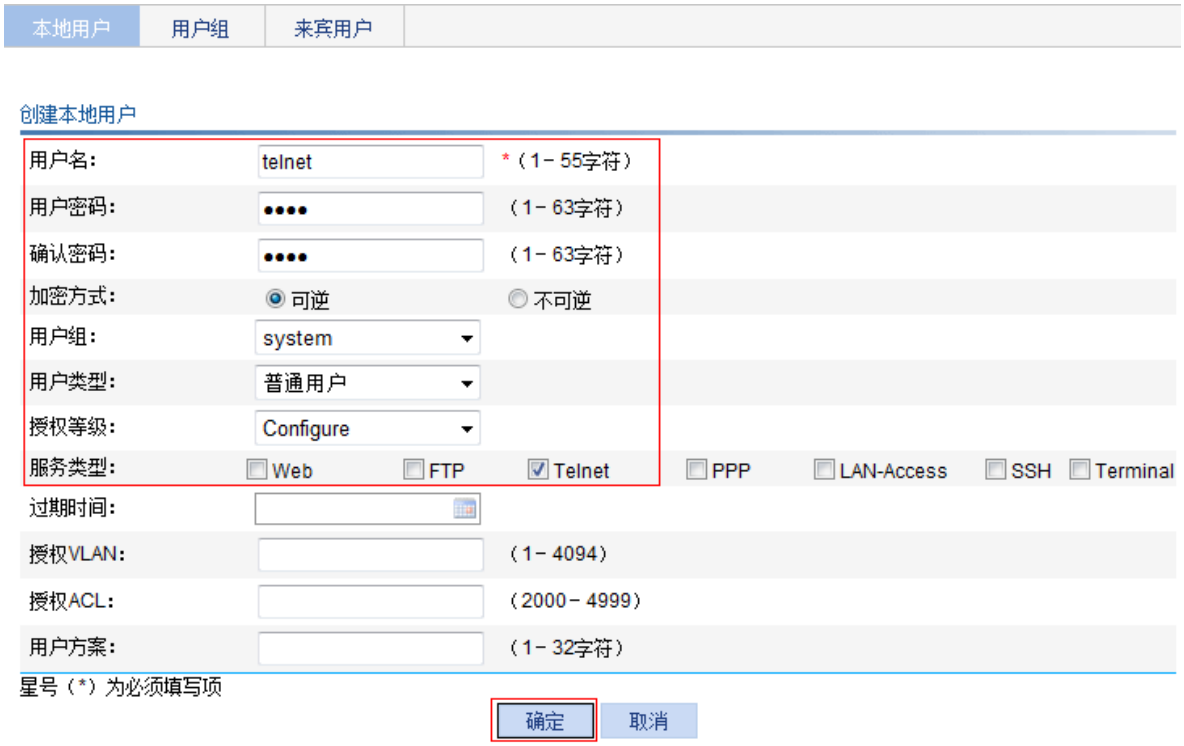
步骤 2：单击<新建>按钮。

步骤 3：进行如下配置，如下图所示。

- 输入用户名为“telnet”。
- 输入用户密码为“abcd”。
- 输入确认密码为“abcd”。
- 加密方式为“可逆”。
- 选中用户类型为“普通用户”。
- 选中授权等级为“Configure”。
- 选择服务类型为“Telnet”。

步骤 4：单击<确定>按钮完成操作。

图1-7 创建本地用户



(2) 配置 ISP 域 system 中 Login 用户的 AAA 认证方法为本地认证。

步骤 1：在导航栏中选择“认证 > AAA”。

步骤 2：单击“认证”页签。

步骤 3：进行如下配置，如下图所示。

- 选择域名为“system”。
- 选中“Login 认证”前的复选框，选择认证方法为“Local”。

步骤 4：单击<应用>按钮，弹出配置进度对话框。

步骤 5：看到配置成功的提示后，在对话框中单击<关闭>按钮完成操作。

图1-8 配置 ISP 域 test 中 Login 用户的 AAA 认证方法为本地认证



(3) 配置 ISP 域 test 中 Login 用户的 AAA 授权方法为本地授权。

步骤 1：在导航栏中选择“认证 > AAA”。

步骤 2：单击“授权”页签。

步骤 3：进行如下配置，如下图所示。

- 选择域名为“system”。
- 选中“Login 授权”前的复选框，选择授权方法为“Local”。

步骤 4：单击<应用>按钮，弹出配置进度对话框。

步骤 5：看到配置成功的提示后，在对话框中单击<关闭>按钮完成操作。

图1-9 配置 ISP 域 test 中 Login 用户的 AAA 授权方法为本地授权



(4) 通过命令行开启 Telnet 服务器功能，并配置 Telnet 用户登录采用 AAA 认证方式。

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

```
[AP] telnet server enable
[AP] user-interface vty 0 4
[AP-ui-vty0-4] authentication-mode scheme
[AP-ui-vty0-4] quit
```

使用 Telnet 登录时输入用户名为 telnet@system（密码为 abcd），以使用 system 域进行认证。

2 RADIUS

2.1 概述

RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）是实现 AAA（Authentication, Authorization and Accounting，认证、授权和计费）的一种最常用的协议，是分布式的、客户端/服务器结构的信息交互协议，能保护网络不受未授权访问的干扰，常应用在既要求较高安全性、又允许远程用户访问的各种网络环境中。该协议定义了 RADIUS 的报文格式及其消息传输机制，并规定使用 UDP 作为封装 RADIUS 报文的传输层协议（UDP 端口 1812、1813 分别作为认证、计费端口）。

RADIUS 最初仅是针对拨号用户的 AAA 协议，后来随着用户接入方式的多样化发展，RADIUS 也适应多种用户接入方式，如以太网接入、ADSL 接入。它通过认证授权来提供接入服务，通过计费来收集、记录用户对网络资源的使用。

说明

关于 RADIUS 和 AAA 协议的详细介绍请参见“安全配置指导”中的“AAA”。

2.2 配置RADIUS方案

RADIUS 方案中定义了设备和 RADIUS 服务器之间进行信息交互所必须的一些参数。当创建一个新的 RADIUS 方案之后，需要对属于此方案的 RADIUS 服务器的 IP 地址、UDP 端口号和报文共享密钥进行设置，这些服务器包括认证和计费服务器，而每种服务器又有主服务器和备份服务器的区别。每个 RADIUS 方案的属性包括：主服务器的 IP 地址、备份服务器的 IP 地址、共享密钥以及 RADIUS 服务器类型等。缺省情况下，不存在任何 RADIUS 方案。

(1) 在导航栏中选择“认证 > RADIUS”，进入如下图所示的页面。

图2-1 RADIUS



(2) 单击<新建>按钮，进入新建 RADIUS 方案的配置页面，如下图所示。

图2-2 新建 RADIUS 方案



(3) 配置 RADIUS 方案的名称。

(4) 配置 RADIUS 方案的通用参数，详细配置如下表所示。

表2-1 通用参数的详细配置

配置项	说明
服务类型	设置设备支持的RADIUS服务器类型： • Standard：指定 Standard 类型的 RADIUS 服务器，即要求 RADIUS 客户端和 RADIUS 服务器按照标准 RADIUS 协议（RFC 2865/2866 或更新）的规程和报文格式进行交互 • Extended：指定 Extended 类型的 RADIUS 服务器（一般为 CAMS/iMC），即要求 RADIUS 客户端和 RADIUS 服务器按照私有 RADIUS 协议的规程和报文格式进行交互
用户名格式	设置发送给RADIUS服务器的用户名格式 接入用户通常以“userid@isp-name”的格式命名，“@”后面的部分为域名，如果RADIUS服务器不接受带域名的用户名时，可以配置将用户名的域名去除后再传送给RADIUS服务器 • 保持用户原始输入：表示发送给 RADIUS 服务器的用户名保持用户原始的输入，不做任何修改 • 带域名：表示发送给 RADIUS 服务器的用户名带域名 • 不带域名：表示发送给 RADIUS 服务器的用户名不带域名

(5) 单击“高级”前的扩展按钮，展开通用参数中的高级配置，如下图所示。

图2-3 通用配置



(6) 配置高级通用参数，详细配置如下表所示。

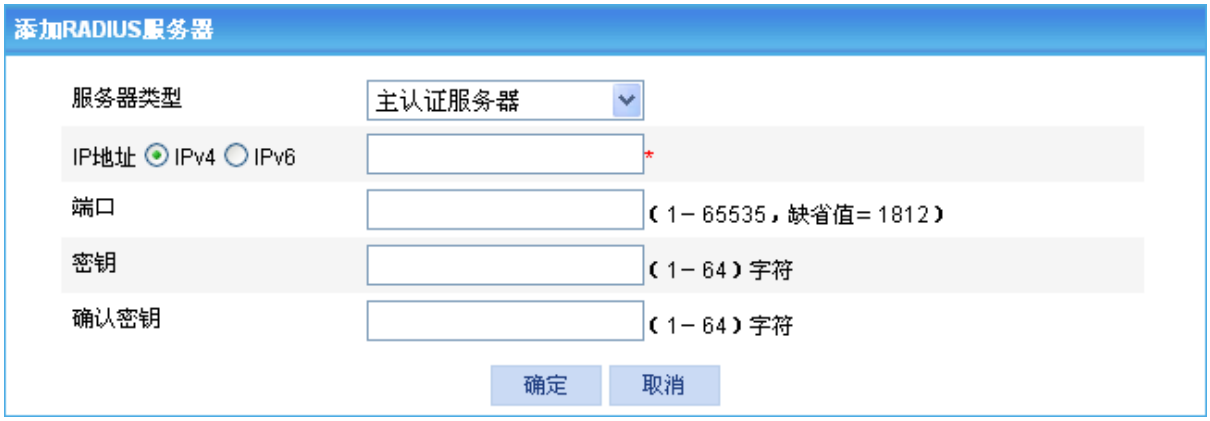
表2-2 高级通用参数的详细配置

配置项	说明
认证服务器共享密钥 确认认证服务器共享密钥 计费服务器共享密钥 确认计费服务器共享密钥	设置RADIUS认证报文的共享密钥和RADIUS计费报文的共享密钥 RADIUS客户端与RADIUS服务器使用MD5算法来加密RADIUS报文，双方通过设置共享密钥来验证报文的合法性。只有在密钥一致的情况下，彼此才能接收对方发来的报文并作出响应 提示 • 必须保证设备上设置的共享密钥与 RADIUS 服务器上的完全一致 • 设备优先采用“RADIUS 服务器配置”中指定的共享密钥，此处指定的共享密钥仅在“RADIUS 服务器配置”中未指定相应共享密钥的情况下使用
静默时间间隔	设置RADIUS服务器恢复激活状态的时间 当静默时间间隔设置为0时，若当前用户使用的认证或计费服务器不可达，则设备并不会切换它的状态，而是保持其为active，并且将使用该服务器的用户认证或计费的报文发送给下一个状态为active的服务器，而后续其它用户的认证请求报文仍然可以发送给该服务器进行处理 若判断主服务器不可达是网络端口短暂中断或者服务器忙碌造成的，则可以结合网络的实际运行状况，将静默时间间隔设置为0，使得用户尽可能的集中在主服务器上进行认证和计费
服务器应答超时时间 RADIUS报文最大尝试发送次数	设置RADIUS服务器应答超时时间，以及发送RADIUS报文的最大尝试次数 由于RADIUS协议采用UDP报文来承载数据，因此其通信过程是不可靠的。如果在指定的服务器应答超时时间内没有收到服务器的响应，则设备有必要向RADIUS服务器重传RADIUS请求报文。如果发送RADIUS请求报文的累计次数超过指定的RADIUS报文最大尝试发送次数而RADIUS服务器仍旧没有响应，则设备将尝试与其它服务器通信。如果不存在状态为active的服务器，则认为本次认证或计费失败 提示 服务器应答超时时间和 RADIUS 报文最大尝试发送次数的乘积不能超过 75 秒
实时计费间隔	设置实时计费的时间间隔，取值必须为3的整数倍 为了对用户实施实时计费，有必要设置实时计费的时间间隔。设置了该属性以后，每隔设定的时间，设备会向RADIUS服务器发送一次在线用户的计费信息 实时计费间隔的取值对NAS和RADIUS服务器的性能有一定的相关性要求，取值越小，对NAS和RADIUS服务器的性能要求越高。建议当用户量比较大（≥1000）时，尽量把该间隔的值设置得大一些 实时计费间隔与用户量之间的推荐比例关系请参见“2.4 注意事项”
实时计费报文最大发送次数	设置允许实时计费请求无响应的最大次数
流量数据的单位	设置发送到RADIUS服务器的流量数据的单位 • Byte：表示流量数据的单位为字节 • Kilo-byte：表示流量数据的单位为千字节 • Mega-byte：表示流量数据的单位为兆字节 • Giga-byte：表示流量数据的单位为千兆字节 提示 设备上配置的发送到RADIUS 服务器的数据流单位及数据包单位应与 RADUIS 服务器上的

配置项	说明	
数据包的单位	设置发送到RADIUS服务器的数据包的单位 • One-packet：表示数据包的单位为包 • Kilo-packet：表示数据包的单位为千包 • Mega-packet：表示数据包的单位为兆包 • Giga-packet：表示数据包的单位为千兆包	流量统计单位保持一致，否则无法正确计费
安全策略服务器IP地址	设置安全策略服务器的IP地址	
RADIUS报文源IP地址	设备向RADIUS服务器发送RADIUS报文时使用的源IP地址 RADIUS服务器上通过IP地址来标识接入设备，并根据收到的RADIUS报文的源IP地址是否与服务器所管理的接入设备的IP地址匹配，来决定是否处理来自该接入设备的认证或计费请求。因此，为保证认证和计费报文可被服务器正常接收并处理，接入设备上发送RADIUS报文使用的源地址必须与RADIUS服务器上指定的接入设备的IP地址保持一致 通常，该地址为接入设备上与RADIUS服务器路由可达的接口IP地址，但在一些特殊的组网环境中，例如接入设备与RADIUS服务器之间存在NAT设备时，需要将该地址指定为转换后的公网IP地址；在接入设备使用VRRP进行双机热备应用时，可以将该地址指定为VRRP上行链路所在备份组的虚拟IP地址 如果不指定此地址，则以发送报文的接口地址作为源IP地址 提示 RADIUS 报文源 IP 地址与 RADIUS 方案中设置的 RADIUS 服务器 IP 地址的协议版本必须保持一致，否则配置能成功但不能生效	
缓存未得到响应的停止计费报文	设置是否在设备上缓存没有得到响应的停止计费请求报文	
停止计费报文最大发送次数	设置当出现没有得到响应的停止计费请求时，将该报文存入设备缓存后，允许停止计费请求无响应的最大次数	
启用accounting-on报文发送功能	设置是否启用accounting-on报文发送功能 在启用accounting-on报文发送功能的情况下，设备重启后，会发送accounting-on报文通知RADIUS服务器该设备已经重启，要求RADIUS服务器强制该设备的用户下线 提示 设备启动后，如果当前系统中没有启用 accounting-on 报文发送功能的 RADIUS 方案，则启用此功能后，必须保存配置，这样设备重启后此功能才能生效。但是，如果当前系统中已经有 RADIUS 方案启用了 accounting-on 报文发送功能，则对未启用此功能的 RADIUS 方案启用此功能后，功能会立即生效	
accounting-on发送间隔	当启用accounting-on报文发送功能时，设置accounting-on报文重发时间间隔	
accounting-on发送次数	当启用accounting-on报文发送功能时，设置accounting-on报文的最大发送次数	
属性 属性值类型	设置开启RADIUS Attribute 25的CAR参数解析功能	

(7) 在“RADIUS 服务器配置”中单击<添加>按钮，弹出如下图所示的页面。

图2-4 添加 RADIUS 服务器



(8) 配置 RADIUS 服务器的信息，详细配置如下表所示。

(9) 单击<确定>按钮向 RADIUS 方案中添加一个 RADIUS 服务器。

(10) 重复步骤(7)～(9)向 RADIUS 方案中添加多个 RADIUS 服务器。

(11) 在新建 RADIUS 方案页面单击<确定>按钮完成操作。

表2-3 RADIUS 服务器的详细配置

配置项	说明
服务器类型	设置要添加的RADIUS服务器类型，包括：主认证服务器、主计费服务器、备份认证服务器、备份计费服务器
IP地址	设置RADIUS服务器的IP地址，可以配置IPv4地址或IPv6地址 提示 • 主认证服务器和备份认证服务器的 IP 地址不能相同，主计费服务器和备份计费服务器的 IP 地址不能相同 • 同一 RADIUS 方案中所有 RADIUS 服务器的 IP 地址协议版本必须一致
端口	设置RADIUS服务器的UDP端口号
密钥	设置RADIUS服务器的共享密钥
确认密钥	当RADIUS服务器中未指定共享密钥时，使用RADIUS方案的通用配置中指定的共享密钥

2.3 RADIUS典型配置举例

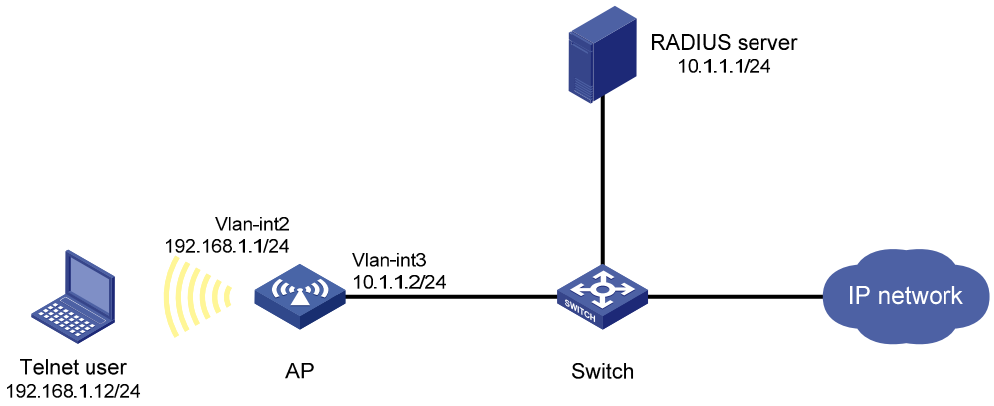
1. 组网需求

如下图所示，AP 通过 Switch 与一台 RADIUS 服务器相连，需要实现 RADIUS 服务器对登录 AP 的 Telnet 用户进行认证、授权和计费（Telnet 用户在线时长统计）。

- 由一台 iMC 服务器（IP 地址为 10.1.1.1/24）担当认证/授权、计费 RADIUS 服务器的职责。
- AP 与认证/授权、计费 RADIUS 服务器交互报文时的共享密钥均为 expert，认证/授权、计费的端口号分别为 1812 和 1813。
- AP 向 RADIUS 服务器发送的用户名携带域名。

- Telnet 用户登录 AP 时使用 RADIUS 服务器上配置的用户名 hello@system 以及密码 abc 进行认证，认证通过后的用户级别为 3。

图2-5 RADIUS 服务器配置组网图



2. 配置RADIUS服务器（iMC）

说明

下面以 iMC 为例说明 RADIUS 服务器的基本配置，使用的 iMC 版本为：iMC PLAT 7.0-E0202、iMC UAM 7.0-E0202。

(1) 增加接入设备。

步骤 1：在 iMC 管理平台选择“用户”页签。

步骤 2：单击导航树中的[接入策略管理/接入设备管理/接入设备配置]菜单项。

步骤 3：在接入设备配置页面中单击<增加>按钮。

步骤 4：进行如下配置，如下图所示。

- 输入与 AP 交互报文时的认证、计费共享密钥为“expert”。
- 选择业务类型为“设备管理业务”。
- 单击<选择>或<手工增加>按钮，添加 IP 地址为“10.1.1.2”的接入设备。
- 其它参数采用缺省值。

说明

添加的接入设备 IP 地址要与 AP 发送 RADIUS 报文的源地址保持一致。缺省情况下，设备发送 RADIUS 报文的源地址是发送 RADIUS 报文的接口 IP 地址。

步骤 5：单击<确定>按钮完成操作。

图2-6 增加接入设备



(2) 增加设备管理用户。

步骤 1：选择“用户”页签。

步骤 2：单击导航树中的[接入用户管理/设备管理用户]菜单项。

步骤 3：在设备管理用户列表页面中单击<增加>按钮。

步骤 4：进行如下配置，如下图所示。

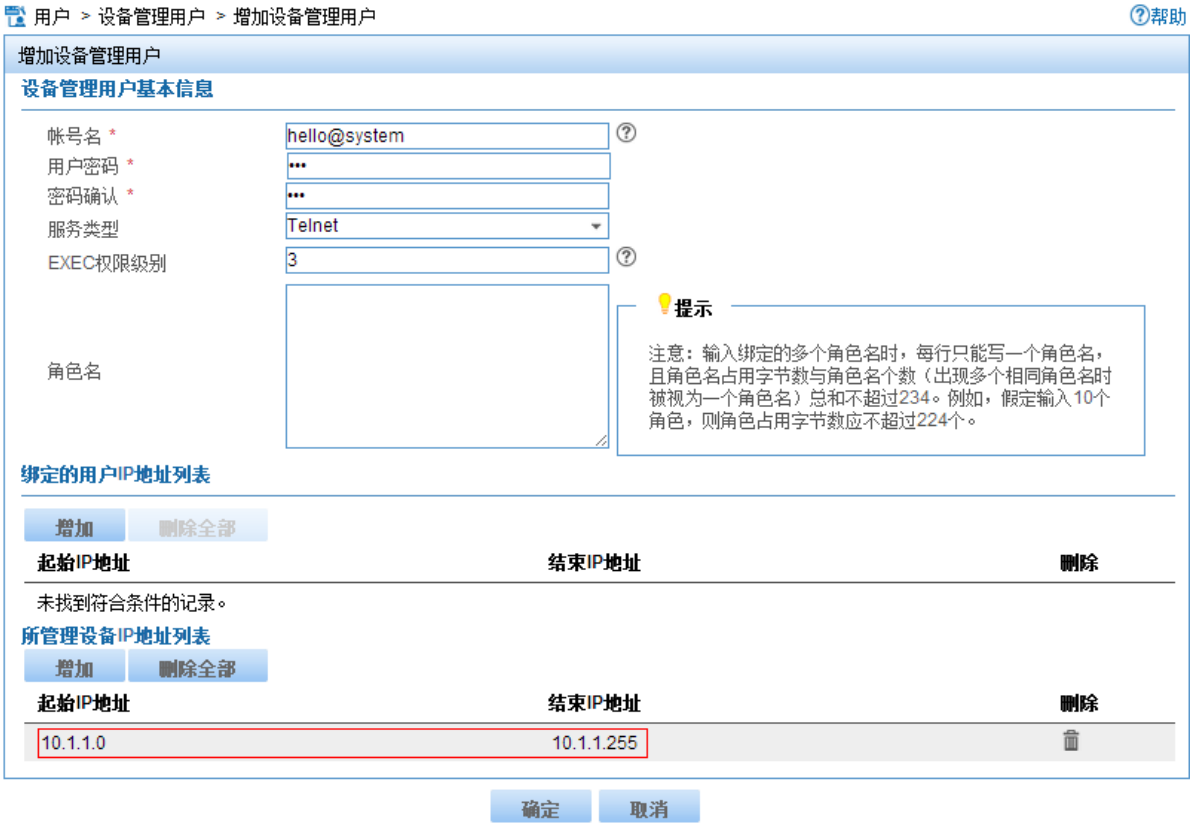
- 输入帐号名为“hello@system”。
- 输入用户密码和密码确认为“abc”。
- 选择服务类型为“Telnet”。
- 输入 EXEC 权限级别为“3”（该值为 Telnet 用户登录系统后的用户级别，缺省为 0）。
- 在所管理设备 IP 地址列表中单击<增加>按钮，设置 IP 地址范围为“10.1.1.0～10.1.1.255”。

说明

添加的所管理设备的 IP 地址范围要包含添加的接入设备的 IP 地址。

步骤 5：单击<确定>按钮完成操作。

图2-7 增加设备管理用户



3. 配置AP

(1) 配置 RADIUS 方案 system。

步骤 1：在导航栏中选择“认证 > RADIUS”。

步骤 2：单击<新建>按钮。

步骤 3：进行如下配置。

- 输入方案名称为“system”。
- 选择服务类型为“Extended”。
- 选择用户名格式为“带域名”。

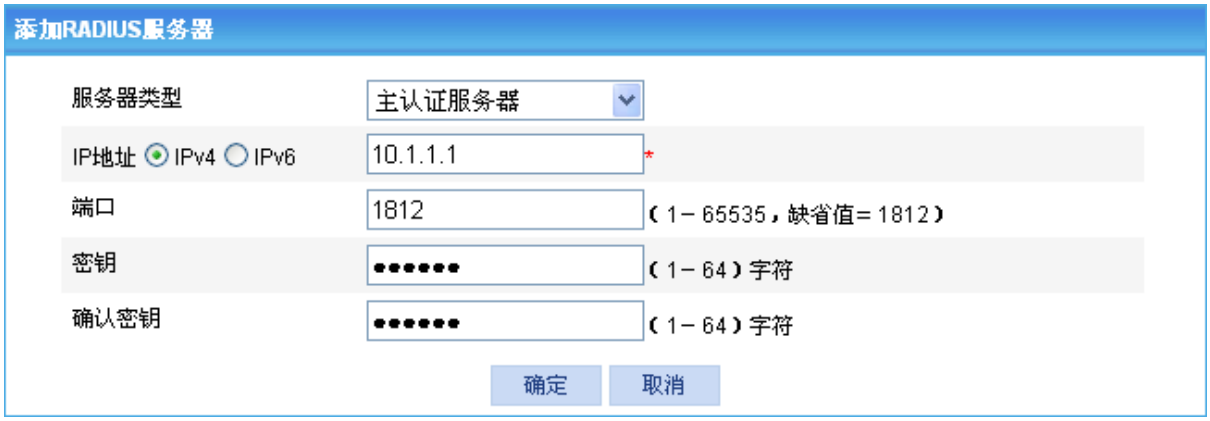
步骤 4：在 RADIUS 服务器配置中单击<添加>按钮。

步骤 5：在弹出的页面上进行如下配置，如下图所示。

- 选择服务器类型为“主认证服务器”。
- 输入 IP 地址为“10.1.1.1”。
- 输入端口为“1812”。
- 输入密钥为“expert”。
- 输入确认密钥为“expert”。

步骤 6：单击<确定>按钮向 system 方案中添加一个主认证服务器。

图2-8 配置 RADIUS 认证服务器



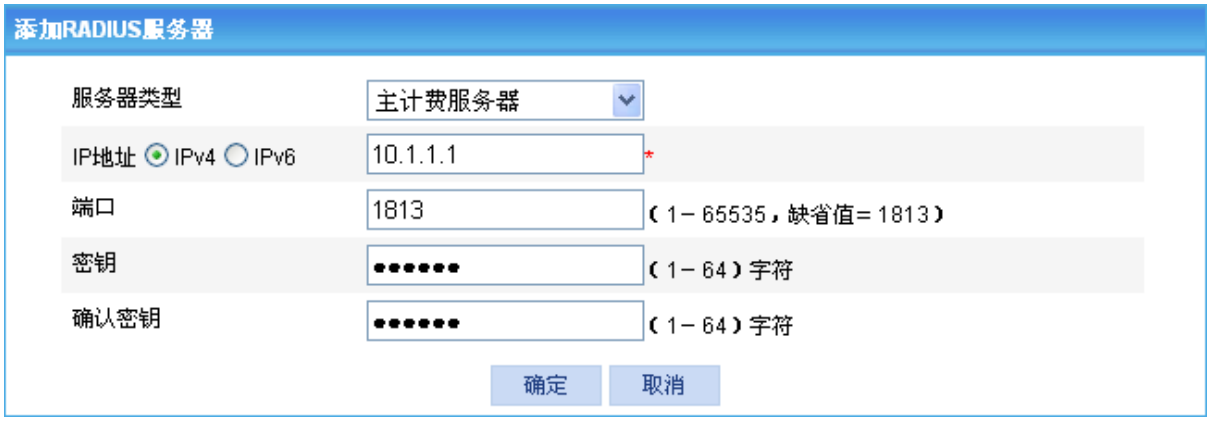
步骤 7：再次在 RADIUS 服务器配置中单击<添加>按钮。

步骤 8：在弹出的页面上进行如下配置，如下图所示。

- 选择服务器类型为“主计费服务器”。
- 输入 IP 地址为“10.1.1.1”。
- 输入端口为“1813”。
- 输入密钥为“expert”。
- 输入确认密钥为“expert”。

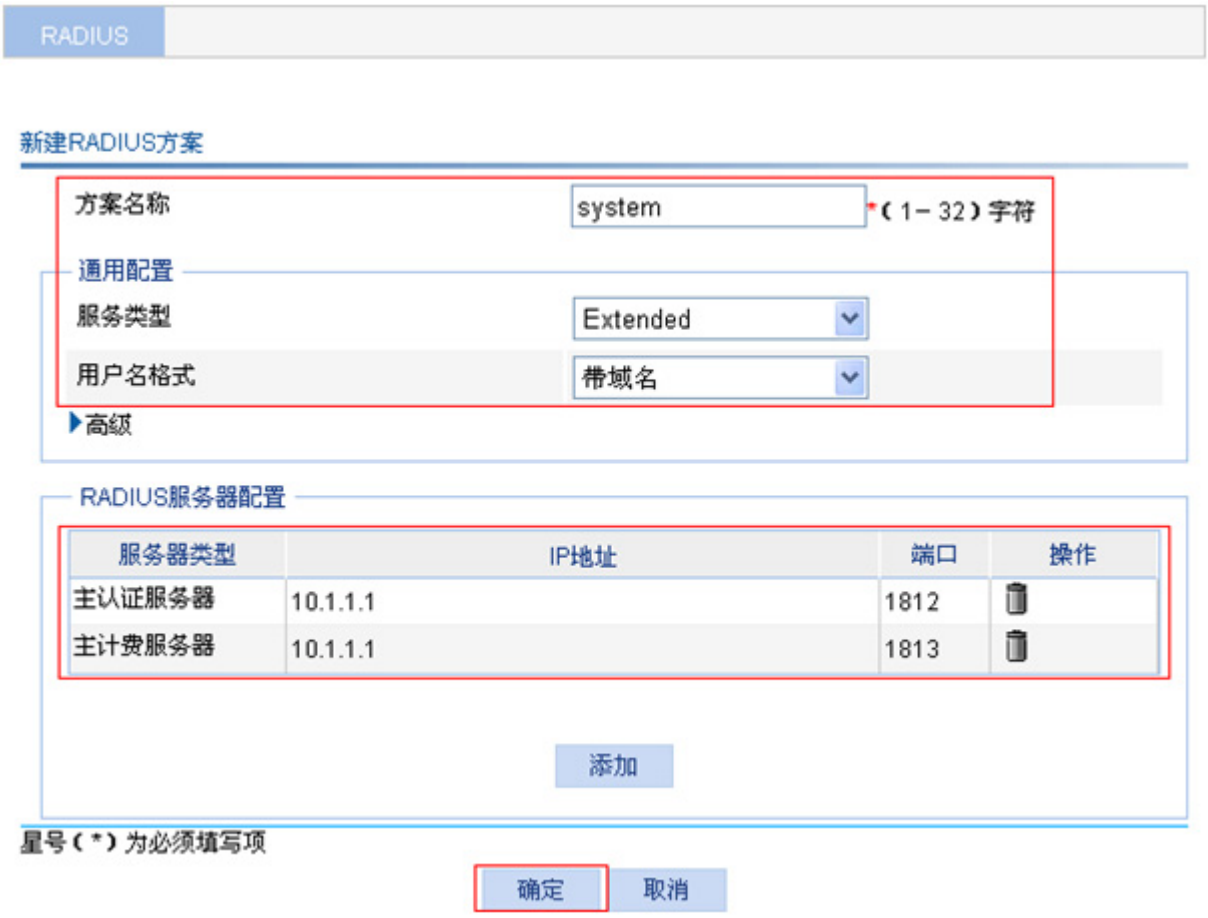
步骤 9：单击<确定>按钮向 system 方案中添加一个主计费服务器。

图2-9 配置 RADIUS 计费服务器



步骤 10：完成上述配置后的新建 RADIUS 方案的页面如下图所示，单击<确定>按钮完成操作。

图2-10 新建 RADIUS 方案 system



(2) 配置 ISP 域的 AAA 认证方案。

步骤 1：单击“认证”页签。

步骤 2：进行如下配置，如下图所示。

- 选择域名为“system”。
- 选中“Default 认证”前的复选框，选择认证方式为“RADIUS”。
- 选择认证方案名称为“system”。

步骤 3：单击<应用>按钮，弹出配置进度对话框。

步骤 4：看到配置成功的提示后，在对话框中单击<关闭>按钮完成操作。

图2-11 配置 ISP 域的 AAA 认证方案



(3) 配置 ISP 域的 AAA 授权方案。

步骤 1：单击“授权”页签。

步骤 2：进行如下配置，如下图所示。

- 选择域名为“system”。
- 选中“Default 授权”前的复选框，选择授权方式为“RADIUS”。
- 选择授权方案名称为“system”。

步骤 3：单击<应用>按钮，弹出配置进度对话框。

步骤 4：看到配置成功的提示后，在对话框中单击<关闭>按钮完成操作。

图2-12 配置 ISP 域的 AAA 授权方案



(4) 配置 ISP 域的 AAA 计费方案，并配置用户计费可选。

步骤 1：单击“计费”页签。

步骤 2：进行如下配置，如下图所示。

- 选择域名为“system”。

- 选中“计费可选开关”前的复选框，选择“Enable”。
- 选中“Default 计费”前的复选框，选择计费方式为“RADIUS”。
- 选择计费方案名称为“system”。

步骤 3：单击<应用>按钮，弹出配置进度对话框。

步骤 4：看到配置成功的提示后，在对话框中单击<关闭>按钮完成操作。

图2-13 配置 ISP 域的 AAA 计费方案



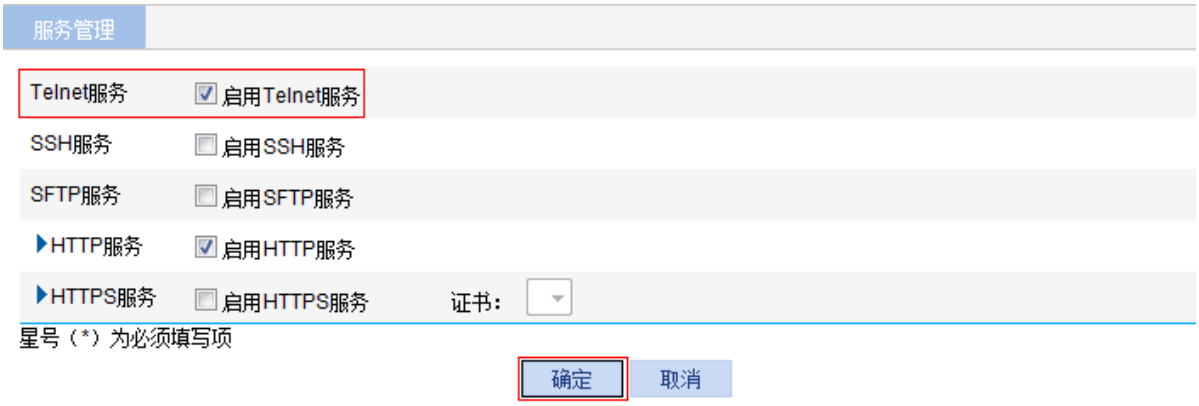
(5) 开启 AP 的 Telnet 服务器功能。

步骤 1：在导航栏中选择“网络 > 服务管理”。

步骤 2：如下图所示，选中“启用 Telnet 服务”前的复选框。

步骤 3：单击<确定>按钮完成操作。

图2-14 启用 Telnet 服务



(6) 通过命令行配置 Telnet 用户登录采用 AAA 认证方式。

```
<AP> system-view
[AP] user-interface vty 0 4
[AP-ui-vty0-4] authentication-mode scheme
```

```
[AP-ui-vty0-4] quit
```

4. 配置结果验证

在 Telnet 客户端按照提示输入用户名 hello@bbb 及密码 abc，即可进入 AP 的用户界面，并可以使用级别为 0、1、2、3 的命令。

2.4 注意事项

配置 RADIUS 客户端时，需要注意如下事项：

(1) 目前 RADIUS 不支持对 FTP 用户进行计费。

(2) 如果在线用户正在使用的计费服务器被删除，则设备将无法发送用户的实时计费请求和停止计费请求，且停止计费报文不会被缓存到本地。

(3) RADIUS 方案中各服务器的状态（active、block）决定了设备向哪个服务器发送请求报文，以及设备在与当前服务器通信中断的情况下，如何转而与另外一个服务器进行交互。在实际组网环境中，可指定一个主 RADIUS 服务器和多个备份 RADIUS 服务器，由备份服务器作为主服务器的备份。通常情况下，设备上主/备份服务器的切换遵从以下原则：

- 当主服务器状态为 active 时，设备首先尝试与主服务器通信，若主服务器不可达，设备更改主服务器的状态为 block，并启动该服务器的静默定时器，然后按照备份服务器的配置先后顺序依次查找状态为 active 的备份服务器进行认证或者计费。如果状态为 active 的备份服务器也不可达，则将该备份服务器的状态置为 block，同时启动该服务器的静默定时器，并继续查找状态为 active 的备份服务器。当服务器的静默定时器超时，或者设备收到该服务器的认证/计费应答报文时，该服务器将恢复为 active 状态。在一次认证或计费过程中，如果设备在尝试与备份服务器通信时，主服务器状态由 block 恢复为 active，则设备并不会立即恢复与主服务器的通信，而是继续查找备份服务器。如果所有已配置的服务器都不可达，则认为本次认证或计费失败。
- 一个用户的计费流程开始之后，设备就不会再与其它的计费服务器通信，即该用户的实时计费报文和停止计费报文只会发往当前使用的计费服务器。如果当前使用的计费服务器被删除，则实时计费和停止计费报文都将无法发送。
- 如果在认证或计费过程中删除了服务器，则设备在与当前服务器通信超时后，将会重新从主服务器开始依次查找状态为 active 的服务器进行通信。
- 当主/备份服务器的状态均为 block 时，设备仅与主服务器通信，若主服务器可达，则主服务器状态变为 active，否则保持不变。
- 只要存在状态为 active 的服务器，设备就仅与状态为 active 的服务器通信，即使该服务器不可达，设备也不会尝试与状态为 block 的服务器通信。
- 设备收到服务器的认证或计费应答报文后会将与报文源 IP 地址相同且状态为 block 的认证或计费服务器的状态更改为 active。

(4) 实时计费间隔与用户量之间的推荐比例关系如下表所示。

表2-4 实时计费间隔与用户量之间的推荐比例关系

用户数	实时计费间隔（分钟）
1～99	3
100～499	6

用户数	实时计费间隔（分钟）
500～999	12
≥1000	≥15

3 HWTACACS

3.1 概述

HWTACACS（HW Terminal Access Controller Access Control System，HW 终端访问控制器控制系统协议）是在 TACACS（RFC1492）基础上进行了功能增强的安全协议。该协议与 RADIUS 协议类似，用于实现 AAA 的协议，且采用客户端/服务器模式实现 NAS 与 HWTACACS 服务器之间的通信。

HWTACACS 协议主要用于 PPP（Point-to-Point Protocol，点到点协议）和 VPDN（Virtual Private Dial-up Network，虚拟专用拨号网络）接入用户及终端用户的认证、授权和计费。其典型应用是对需要登录到设备上进行操作的终端用户进行认证、授权以及对终端用户执行的操作进行记录。设备作为 HWTACACS 的客户端，将用户名和密码发给 HWTACACS 服务器进行验证，用户验证通过并得到授权之后可以登录到设备上进行操作，HWTACACS 服务器上会记录用户对设备执行过的命令。



说明

关于 HWTACACS 的详细介绍请参见“安全配置指导”中的“AAA”。

3.2 HWTACACS方案配置任务简介



说明

通过 Web 配置的 HWTACACS 的方案名为 system。

表3-1 HWTACACS 配置步骤

步骤	配置任务	说明
1	3.3 创建HWTACACS方案system	必选 创建名为“system”的HWTACACS方案 缺省情况下，不存在任何HWTACACS方案
2	3.4 配置HWTACACS服务器信息	认证和授权服务器为必选项，计费服务器为可选项 配置HWTACACS方案system的认证、授权、计费服务器信息 缺省情况下，未配置各服务器 提示 建议在不需要备份的情况下，只配置主服务器即可
3	3.5 配置HWTACACS参数	可选 配置设备和HWTACACS服务器之间进行信息交互所需的参数

3.3 创建HWTACACS方案system

(1) 当系统中不存在“system”方案时，在导航栏中选择“认证 > HWTACACS”，可以进入如下图所示的页面。

(2) 在页面上单击<新建>按钮即可完成“system”方案的创建。

图3-1 创建 system 方案



3.4 配置HWTACACS服务器信息

(1) 当已经创建了“system”方案时，在导航栏中选择“认证 > HWTACACS”，默认进入“HWTACACS 服务器配置”页签的页面，如下图所示。

图3-2 HWTACACS 服务器配置



(2) 配置 HWTACACS 服务器的信息，详细配置如下表所示。

(3) 单击<确定>按钮完成操作。

表3-2 HWTACACS 服务器的详细配置

配置项	说明
服务类型	选择待配置的HWTACACS服务器的类型，包括：认证服务器、授权服务器、计费服务器

配置项	说明
主服务器IP地址	设置主服务器的IP地址 未配置主服务器时，主IP地址和TCP端口均显示空 输入空时，表示删除配置的主服务器 主服务器与备份服务器的IP地址不能相同
主服务器TCP端口	设置主服务器的TCP端口号 不同的服务类型需要根据实际情况设置不同的端口号
备份服务器IP地址	设置备份服务器的IP地址 未配置备份服务器时，备份IP地址和TCP端口均显示空 输入空时，表示删除配置的备份服务器 主服务器与备份服务器的IP地址不能相同
备份服务器TCP端口	设置备份服务器的TCP端口号 不同的服务类型需要根据实际情况设置不同的端口号
共享密钥	设置服务器的共享密钥，并再次输入以确认
确认共享密钥	HWTACACS客户端（即设备系统）与HWTACACS服务器使用MD5算法来加密交互的HWTACACS报文，双方通过设置共享密钥来验证报文的合法性。只有在密钥一致的情况下，双方才能彼此接收对方发来的报文并作出响应。因此，必须保证设备上设置的共享密钥与HWTACACS服务器上的完全一样

3.5 配置HWTACACS参数

(1) 当已经创建了“system”方案时，在导航栏中选择“认证 > HWTACACS”。

(2) 单击“HWTACACS 参数设置”页签，进入 HWTACACS 参数设置页面，如下图所示。

图3-3 HWTACACS 参数设置



(3) 配置 HWTACACS 参数，详细设置如下表所示。

(4) 单击<确定>按钮完成操作。

表3-3 设置 HWTACACS 参数详细信息

配置项	说明
NAS-IP	设备向HWTACACS服务器发送HWTACACS报文时使用的源IP 为了避免物理接口故障时从服务器返回的报文不可达，推荐使用Loopback接口地址
实时计费间隔	设置实时计费的时间间隔，取值必须为3的整数倍 为了对用户实施实时计费，有必要设置实时计费的时间间隔。在设置了该属性以后，每隔设定的时间，设备会向HWTACACS服务器发送一次在线用户的计费信息。按照协议，如果服务器对实时计费报文没有正常响应，设备也不会强制切断在线用户 输入空时，恢复实时计费的时间间隔为缺省值 提示 实时计费间隔的取值对设备和HWTACACS服务器的性能有一定的相关性要求，取值越小，对设备和HWTACACS服务器的性能要求越高。建议当用户量比较大（≥1000）时，尽量把该间隔的值设置得大一些。实时计费间隔与用户量之间的推荐比例关系请参见“3.7 注意事项”
停止计费缓存	设置使能或禁止在设备上缓存没有得到响应的停止计费请求报文 由于停止计费请求报文涉及到话单结算、并最终影响收费多少，对用户和ISP都有比较重要的影响，因此设备应该尽最大努力把它发送给HWTACACS计费服务器。所以，如果HWTACACS计费服务器对设备发出的停止计费请求报文没有响应，设备应将其缓存在本机上，然后发送直到HWTACACS计费服务器产生响应，或者在发送的次数达到指定的次数限制后将其丢弃
停止计费报文重发次数	设置当出现没有得到响应的停止计费请求时，停止计费报文的重发次数 当停止计费缓存为Disable状态时，该值无效 输入空时，恢复停止计费报文传送次数为缺省值
应答超时时间	设置HWTACACS服务器应答超时时间 服务器应答超时可能导致与HWTACACS服务器的连接断开 输入空时，恢复应答超时时间为缺省值 提示 由于 HWTACACS 是基于 TCP 实现的，因此，服务器应答超时或 TCP 超时都可能导致与 HWTACACS 服务器的连接断开
Quiet时间间隔	设置主服务器恢复激活状态的时间 输入空时，恢复Quiet时间间隔为缺省值
用户名格式	设置发送给HWTACACS服务器的用户名格式 接入用户通常以“userid@isp-name”的格式命名，“@”后面的部分为域名，如果HWTACACS服务器不接受带域名的用户名时，可以配置将用户名的域名去除后再传送给HWTACACS服务器 • without-domain：表示发送给 HWTACACS 服务器的用户名不带域名 • with-domain：表示发送给 HWTACACS 服务器的用户名带域名

配置项	说明
流量数据的单位	设置发送到HWTACACS服务器的流量数据的单位，用于流量计费 • byte：表示流量数据的单位为字节 • kilo-byte：表示流量数据的单位为千字节 • mega-byte：表示流量数据的单位为兆字节 • giga-byte：表示流量数据的单位为千兆字节 • 选择空时，恢复发送到 HWTACACS 服务器的流量数据的单位为缺省值
数据包的单位	设置发送到HWTACACS服务器的数据包的单位，用于流量计费 • one-packet：表示数据包的单位为包 • kilo-packet：表示数据包的单位为千包 • mega-packet：表示数据包的单位为兆包 • giga-packet：表示数据包的单位为千兆包 • 选择空时，恢复发送到 HWTACACS 服务器的数据包的单位为缺省值

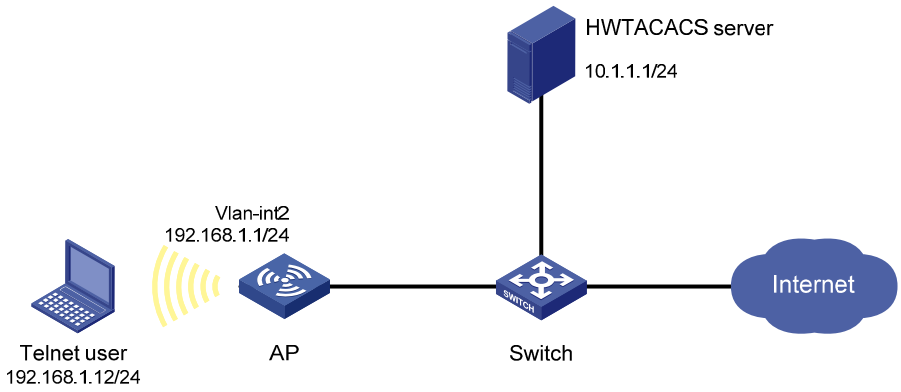
3.6 HWTACACS典型配置举例

1. 组网需求

通过配置 AP 实现 HWTACACS 服务器对 Telnet 登录 AP 的用户进行认证、授权、计费。

- 由一台 HWTACACS 服务器担当认证、授权、计费服务器的职责，服务器 IP 地址为 10.1.1.1/24。
- AP 与认证、授权、计费 HWTACACS 服务器交互报文时的共享密钥均为 expert，向 HWTACACS 服务器发送的用户名中不带域名。

图3-4 HWTACACS 配置组网图



2. 配置HWTACACS服务器

在 HWTACACS 服务器设置其与 AP 交互报文时的共享密钥为 expert，添加 Telnet 用户名及密码。

3. 配置AP

(1) 创建 HWTACACS 方案 system。

步骤 1：在导航栏中选择“认证 > HWTACACS”，进入“HWTACACS 服务器配置”页签的页面。

步骤 2：如下图所示，单击<新建>按钮完成操作。

图3-5 创建 HWTACACS 方案 system



(2) 配置 HWTACACS 认证服务器信息。

步骤 1：完成上述配置后自动进入 HWTACACS 服务器配置页面，进行如下配置，如下图所示。

- 选择服务类型为“认证服务器”。
- 输入主服务器 IP 地址为“10.1.1.1”。
- 输入主服务器 TCP 端口为“49”。
- 选中“共享密钥”前的复选框，输入共享密钥和确认共享密钥为“expert”。

步骤 2：单击<确定>按钮完成操作。

图3-6 配置 HWTACACS 认证服务器信息



(3) 配置 HWTACACS 授权服务器信息。

步骤 1：进行如下配置，参见 图 3-6。

- 选择服务类型为“授权服务器”。
- 输入主服务器 IP 地址为“10.1.1.1”。
- 输入主服务器 TCP 端口为“49”。
- 选中“共享密钥”前的复选框，输入共享密钥和确认共享密钥为“expert”。

步骤 2：单击<确定>按钮完成操作。

(4) 配置 HWTACACS 计费服务器信息。

步骤 1：进行如下配置，参见 图 3-6。

- 选择服务类型为“计费服务器”。
- 输入主服务器 IP 地址为“10.1.1.1”。
- 输入主服务器 TCP 端口为“49”。
- 选中“共享密钥”前的复选框，输入共享密钥和确认共享密钥为“expert”。

步骤 2：单击<确定>按钮完成操作。

(5) 配置 AP 与服务器交互的方案。

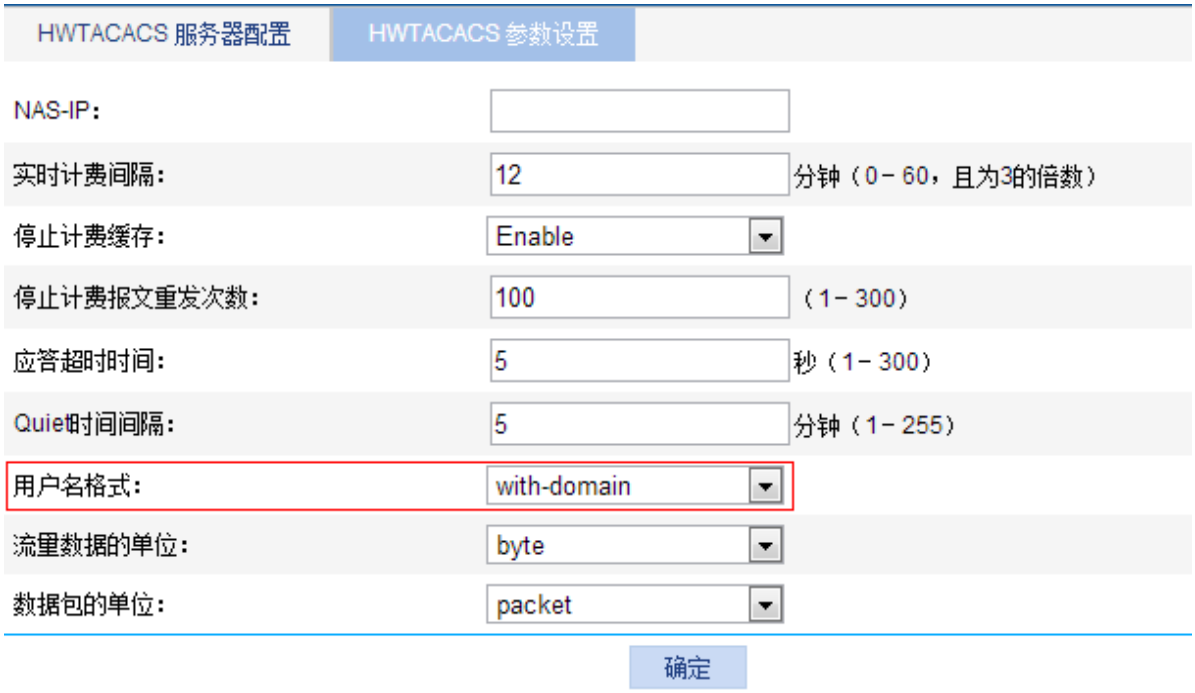
步骤 1：在导航栏中选择“认证 > HWTACACS”。

步骤 2：单击“HWTACACS 参数设置”页签。

步骤 3：如下图所示，选择用户名格式为“without-domain”。

步骤 4：单击<确定>按钮完成操作。

图3-7 配置 Device 与服务器交互的方案



(6) 配置 ISP 域的 AAA 认证方案。

步骤 1：单击“认证”页签。

步骤 2：进行如下配置，如下图所示。

- 选择域名为“system”。
- 选中“Default 认证”前的复选框，选择认证方式为“HWTACACS”。
- 选择 HWTACACS 认证方案名称为“system”。

步骤 3：单击<应用>按钮，弹出配置进度对话框。

步骤 4：看到配置成功的提示后，在对话框中单击<关闭>按钮完成操作。

图3-8 配置 ISP 域的 AAA 认证方案



(7) 配置 ISP 域的 AAA 授权方案。

步骤 1：单击“授权”页签。

步骤 2：进行如下配置，如下图所示。

- 选择域名为“system”。
- 选中“Default 授权”前的复选框，选择授权方式为“HWTACACS”。
- 选择 HWTACACS 授权方案名称为“system”。

步骤 3：单击<应用>按钮，弹出配置进度对话框。

步骤 4：看到配置成功的提示后，在对话框中单击<关闭>按钮完成操作。

图3-9 配置 ISP 域的 AAA 授权方案



(8) 配置 ISP 域的 AAA 计费方案，并配置用户计费可选。

步骤 1：单击“计费”页签。

步骤 2：进行如下配置，如下图所示。

- 选择域名为“system”。
- 选中“计费可选开关”前的复选框，选择“Enable”。
- 选中“Default 计费”前的复选框，选择计费方式为“HWTACACS”。
- 选择 HWTACACS 计费方案名称为“system”。

步骤 3：单击<应用>按钮，弹出配置进度对话框。

步骤 4：看到配置成功的提示后，在对话框中单击<关闭>按钮完成操作。

图3-10 配置 ISP 域的 AAA 计费方案



(9) 通过命令行开启 AP 的 Telnet 服务器功能，并配置 Telnet 用户登录采用 AAA 认证方式。

```
<AP> system-view
[AP] telnet server enable
[AP] user-interface vty 0 4
[AP-ui-vty0-4] authentication-mode scheme
[AP-ui-vty0-4] quit
```

4. 配置结果验证

在 Telnet 客户端输入正确的用户名（格式为 *userid*@test）和密码，即可进入 AP 的用户界面。

3.7 注意事项

配置 HWTACACS 客户端时需要注意如下事项：

(1) 有用户在线时，不能删除 HWTACACS 方案，并且不能修改 HWTACACS 服务器 IP 地址。

(2) 对于 HWTACACS，只有在删除 HWTACACS 方案和修改 HWTACACS 服务器 IP 地址时，才会检查当前是否有用户在线，其他配置修改均不会进行检查。

(3) 对于所有类型的用户，如果只配置了 HWTACACS 认证，但没有配置 HWTACACS 授权，则用户无法登录设备。

(4) 只有当没有活跃的用于发送认证/授权/计费报文的 TCP 连接使用该认证/授权/计费服务器时，才允许删除该服务器。

(5) 目前 HWTACACS 不支持对 FTP 用户进行计费。

(6) 实时计费间隔与用户量之间的推荐比例关系如下表所示。

表3-4 实时计费间隔与用户量之间的推荐比例关系

用户数	实时计费间隔（分钟）
1～99	3
100～499	6
500～999	12
≥1000	≥15

4 用户

4.1 概述

用户模块提供了本地用户、用户组、来宾用户和用户方案的配置功能。

1. 本地用户

本地用户是本地设备上设置的一组用户属性的集合。该集合以用户名为用户的唯一标识，可配置多种属性，比如用户密码、用户类型、服务类型、授权属性等。为使某个请求网络服务的用户可以通过本地认证，需要在设备上的本地用户数据库中添加相应的表项。本地认证的详细介绍请参见“AAA”。

2. 用户组

用户组是一个本地用户属性的集合，某些需要集中管理的授权属性可在用户组中统一配置和管理，用户组内的所有本地用户都可以继承这些属性。

每个新增的本地用户都默认属于一个系统自动创建的用户组 system，且继承该组的所有属性，但本地用户的属性比用户组的属性优先级高。

3. 来宾用户

来宾用户是一种有特殊应用环境的本地用户。在有 Portal 或 LAN-Access 用户临时需要接入网络的情况下，设备管理员或来宾管理员可以为用户建立临时使用的来宾用户帐户，并置对来宾用户帐户进行生效时间的控制。

4.2 配置本地用户

(1) 在导航栏中选择“认证 > 用户”，默认进入“本地用户”页签的页面，如下图所示，页面显示的是所有本地用户的信息，包括：普通用户、安全日志管理员、来宾管理员和来宾用户。

说明

在“本地用户”页签的页面中可以修改用户类型为来宾用户的本地用户，但是修改后的用户类型不能再为来宾用户。

图4-1 本地用户



(2) 单击<新建>按钮，进入新建本地用户的配置页面，如下图所示，可以新建除来宾用户外其他类型的本地用户。

图4-2 创建本地用户



(3) 配置本地用户的信息，详细配置如下表所示。

(4) 单击<确定>按钮完成操作。

表4-1 本地用户的详细配置

配置项	说明
用户名	设置本地用户的名称
用户密码	设置本地用户的密码和确认密码 用户密码和确认密码必须一致
确认密码	提示 输入的密码如果以空格开头，则开头的空格将被忽略
加密方式	• 可逆：表示设备以可逆的加密算法对用户密码加密后保存 • 不可逆：表示设备以不可逆的加密算法对用户密码加密后保存
用户组	设置本地用户所属的用户组 用户组的配置请参见“4.3 配置用户组”

配置项	说明
用户类型	设置本地用户的类型，包括： • 普通用户 • 安全日志管理员：该类型的用户仅能通过 Web 对安全日志文件进行管理，并且只有安全日志管理员可以对安全日志文件进行管理 • 来宾管理员：该类型的用户仅能通过 Web 对来宾用户的账户进行管理，访问“认证 > 用户 [来宾用户]”的页面，新建、修改、删除来宾用户 提示 目前，设备暂不支持安全日志管理员的配置
授权等级	设置本地用户的授权等级，由低到高依次为Visitor、Monitor、Configure、Management，高级别用户具有低级别用户的所有操作权限 • Visitor：处于该级别的用户可以进行 Ping 和 Trace Route 操作，但不能从设备读取任何数据，也不能对设备进行任何设置 • Monitor：只能从设备读取数据，而不能对设备进行任何设置 • Configure：可以从设备读取数据，并对设备进行配置，但是不能对设备进行软件升级、添加/删除/修改用户、备份/恢复配置文件等操作 • Management：可以对设备进行任何操作 提示 授权等级只对服务类型为 Web、FTP、Telnet 和 SSH 的普通用户有效
服务类型	设置本地用户可以使用的服务类型，包括Web、FTP、Telnet、PPP、Portal、LAN-Access（主要指以太网接入用户，比如802.1x用户）和SSH 提示 • 服务类型是本地认证的检测项，如果没有用户可以使用的服务类型，则该用户无法正常认证通过 • 来宾管理员和安全日志管理员的服务类型为 Web • 来宾用户的服务类型为 Portal 和 LAN-Access
过期时间	设置本地用户的有效截止时间 当指定了过期时间的用户进行本地认证时，接入设备检查当前系统时间是否在用户的过期时间内，若在过期时间内则允许用户登录，否则拒绝用户登录
授权VLAN	设置本地用户的授权VLAN ID 提示 授权 VLAN 只对服务类型为 Portal 和 LAN-Access 的普通用户有效
授权ACL	设置本地用户的授权ACL序号 提示 授权 ACL 只对服务类型为 PPP、Portal 和 LAN-Access 的普通用户有效
用户方案	设置本地用户的授权用户方案名称 提示 授权用户方案只对服务类型为 PPP、Portal 和 LAN-Access 的普通用户有效 设备不支持用户方案的配置

4.3 配置用户组

(1) 在导航栏中选择“认证 > 用户”。

(2) 单击“用户组”页签，进入用户组的显示页面，如下图所示。

图4-3 用户组



(3) 单击<新建>按钮，进入新建用户组的配置页面，如下图所示。

图4-4 新建用户组



(4) 配置用户组的信息，详细配置如下表所示。

(5) 单击<确定>按钮完成操作。

表4-2 用户组的详细配置

配置项	说明
用户组名称	设置用户组的名称
访问等级	设置用户组的访问等级，由低到高依次为Visitor、Monitor、Configure、Management
授权VLAN	设置用户组的授权VLAN ID

配置项	说明
授权ACL	设置用户组的授权ACL序号
用户方案	设置用户组的授权用户方案名称 目前，设备不支持用户方案的配置
来宾用户可选	设置是否允许来宾用户加入该用户组 提示 用户组 system 默认为来宾用户可选组，不可修改

4.4 配置来宾用户

有两种用户可以配置来宾用户：Management 级别的普通用户和来宾管理员。

说明

关于用户类型和授权等级的详细介绍请参见 表 4-1。

4.4.1 Management级别的普通用户配置来宾用户

(1) 在导航栏中选择“认证 > 用户”。

(2) 单击“来宾用户”页签，进入来宾用户的显示页面，如下图所示。

图4-5 来宾用户



(3) 单击<新建>按钮，进入新建来宾用户的配置页面，如下图所示。

图4-6 新建来宾用户



(4) 配置来宾用户的信息，详细配置如下表所示。

(5) 单击<确定>按钮完成操作。

表4-3 来宾用户的详细配置

配置项	说明
批量创建用户	设置是否批量创建来宾用户
用户名	当非批量创建用户时，设置来宾用户的名称
用户名前缀	当批量创建用户时，设置要批量创建的来宾用户的用户名前缀和数量 例如：设置用户名前缀为abc，用户数量为50，则会创建50个来宾用户，用户名分别为abc0~abc49
用户数量	
用户密码	设置来宾用户的密码
和用户名一致	• 当选中“和用户名一致”前的复选框时，不需要再输入具体的用户密码和确认密码，来宾用户的密码将与其用户名一致 • 当未选中“和用户名一致”前的复选框时，需要输入具体的用户密码和确认密码，且二者必须一致
确认密码	提示 输入的密码如果以空格开头，则开头的空格将被忽略
加密方式	• 可逆：表示设备以可逆的加密算法对用户密码加密后保存 • 不可逆：表示设备以不可逆的加密算法对用户密码加密后保存
所属用户组	设置来宾用户所属的用户组
生效时间	设置来宾用户的生效时间段，包括起始时间和终止时间 当指定了生效时间的来宾用户进行本地认证时，接入设备检查当前系统时间是否在用户的生效时间内，若在生效时间内则允许用户登录，否则拒绝用户登录

4.4.2 来宾管理员配置来宾用户

来宾管理员仅能通过 Web 对来宾用户的账户进行管理。

(1) 来宾管理员登录设备后，在导航栏中选择“认证 > 用户”，进入如下图所示的页面。

图4-7 来宾用户



(2) 单击<新建>按钮，进入新建来宾用户的配置页面，如下图所示。

图4-8 新建来宾用户



(3) 配置来宾用户的信息，详细配置如 表 4-3 所示。

(4) 单击<确定>按钮完成操作。

5 证书管理

5.1 概述

PKI（Public Key Infrastructure，公钥基础设施）是一个利用公共密钥理论和技术来实现并提供信息安全服务的具有通用性的安全基础设置。我司的 PKI 可为 SSL（Secure Sockets Layer，安全套接字层）提供证书管理机制。

公共密钥体制也称为非对称密钥体制，是目前应用最广泛的一种加密体制。这一体制使用一个非对称的密钥对，分别是一个公开的加密密钥（公钥）和一个保密的解密密钥（私钥），用公钥加密的信息只能用私钥解密，反之亦然。由于公钥是公开的，需要在网上传送，故公钥的管理问题就是公共密钥体制所需要解决的关键问题。

目前，PKI 系统中引出的数字证书机制就是一个很好的解决方案。基于公共密钥技术的数字证书是一个用户的身份和他所持有的公钥的结合，是使用 PKI 系统的用户建立安全通信的信任基础。

基于数字证书的 PKI 系统，能够为网络通信和网络交易，特别是电子政务和电子商务业务，透明地提供一整套安全服务，主要包括身份认证、保密、数据完整性和不可否认性。

PKI 技术的广泛应用能满足人们对网络交易安全保障的需求。作为一种基础设施，PKI 的应用范围非常广泛，并且在不断发展之中，下面给出几个应用实例。

- VPN：VPN（Virtual Private Network，虚拟专用网络）是一种构建在公用通信基础设施上的专用数据通信网络，利用网络层安全协议（如 IPsec）和建立在 PKI 上的加密与数字签名技术来获得机密性保护。
- 安全电子邮件：电子邮件的安全也要求机密、完整、认证和不可否认，而这些都可以利用 PKI 技术来实现。目前发展很快的安全电子邮件协议 S/MIME(Secure/Multipurpose Internet Mail Extensions，安全/多用途 Internet 邮件扩充协议)，是一个允许发送加密和有签名邮件的协议。该协议的实现需要依赖于 PKI 技术。
- Web 安全：为了透明地解决 Web 的安全问题，在两个实体进行通信之前，先要建立 SSL 连接，以此实现对应用层透明的安全通信。利用 PKI 技术，SSL 协议允许在浏览器和服务器之间进行加密通信。此外，服务器端和浏览器端通信时双方可以通过数字证书确认对方的身份。



说明

关于 PKI 的详细介绍请参见“安全配置指导”中的“PKI”。

5.2 PKI配置任务简介

PKI 证书的申请方式有两种：

- 手动申请证书方式：需要手工完成获取 CA（Certificate Authority，证书颁发机构）证书、生成密钥对、申请本地证书的工作。
- 自动申请证书方式：在没有本地证书时实体自动通过 SCEP（Simple Certification Enrollment Protocol，简单证书注册协议，专门用于与认证机构进行通信）协议进行申请，而且在证书即将过期时自动申请新的证书并获取至本地。

证书申请的方式可在 PKI 域中进行配置。根据证书申请方式的不同，PKI 的配置步骤也不同。

1. 手动申请证书方式

手动申请证书方式下 PKI 配置的推荐步骤如下表所示。

表5-1 PKI 配置步骤（手动申请证书方式）

步骤	配置任务	说明
1	3.4 配置HWTACACS服务器信息	必选 新建实体并配置实体的身份信息参数 一份证书是一个公开密钥与一个身份的绑定，而身份必须与一个特定的PKI实体相关联。实体DN（Distinguished Name，识别名）的参数是实体的身份信息，CA根据实体提供的身份信息来唯一标识证书申请者 实体DN的配置必须与CA证书颁发策略相匹配，以确认实体DN的配置任务，如哪些实体参数为必选配置，哪些为可选配置。申请者的身份信息必须符合CA证书颁发策略，否则证书申请可能会失败
2	5.4 新建PKI域	必选 新建PKI域，配置证书申请方式为“Manual” 实体在进行PKI证书申请操作之前需要配置一些注册信息来配合完成申请的过程，这些信息的集合就是一个实体的PKI域 PKI域是一个本地概念，因此创建PKI域的目的是便于其它应用引用PKI的配置，比如IKE、SSL等，一个设备上配置的PKI域对CA和其它设备是不可见的，每一个PKI域有单独的域参数配置信息
3	5.5 生成RSA密钥对	必选 配置生成本地RSA密钥对 缺省情况下，本地没有RSA密钥对 密钥对的产生是证书申请过程中重要的一步。申请过程使用了一对主机密钥：私钥和公钥。私钥由用户保留，公钥和其他信息则交由CA中心进行签名，从而产生证书 提示 若本地证书已存在，为保证密钥对与现存证书的一致性，必须在删除本地证书后，再生成新的密钥对
4	获取CA证书	必选 将CA证书获取至本地，详细配置请参见“5.7 获取和查看证书” 获取证书的目的是： • 将 CA 签发的与实体所在安全域有关的证书存放到本地，以提高证书的查询效率，减少向 PKI 证书存储库查询的次数 • 为证书的验证做好准备 提示 如果本地已有 CA 证书存在，则不允许再执行获取 CA 证书的操作，避免因相关配置的修改使得证书与注册信息不匹配。请先删除存储于本地的 CA 证书与本地证书后，再重新获取

步骤	配置任务	说明
5	5.8 申请本地证书	必选 证书申请就是实体向CA自我介绍的过程，实体向CA提供身份信息和相应的公钥，这些信息将成为颁发给该实体证书的主要组成部分 申请本地证书有在线和离线两种方式： • 在线申请成功后，会自动将本地证书获取至本地 • 离线申请成功后，需要用户通过离线方式将本地证书获取至本地 提示 如果本地已有本地证书存在，则不允许再执行申请本地证书的操作，避免因相关配置的修改使得证书与注册信息不匹配。请先删除存储于本地的 CA 证书与本地证书，再重新申请
6	5.6 销毁RSA密钥对	可选 如果要获取的证书中含有RSA密钥对，则必须先将设备上已有的密钥对销毁，否则无法成功获取证书。销毁RSA密钥对的同时，也会销毁对应的本地证书
7	5.7 获取和查看证书	当采用离线方式申请证书时必选 将已存在的证书获取至本地，获取后可以查看证书的详细信息 提示 • 在线获取本地证书之前必须完成 LDAP 服务器的配置 • 当采用离线方式申请证书时，必须通过离线方式将下载到的 CA 证书和本地证书获取至本地
8	5.9 获取和查看CRL	可选 获取CRL至本地，获取后可以查看CRL的内容

2. 自动申请证书方式

自动申请证书方式下 PKI 配置的推荐步骤如下表所示。

表5-2 PKI 配置步骤（自动申请证书方式）

步骤	配置任务	说明
1	3.4 配置HWTACACS服务器信息	必选 新建实体并配置实体的身份信息参数 一份证书是一个公开密钥与一个身份的绑定，而身份必须与一个特定的PKI实体相关联，实体DN（Distinguished Name，识别名）的参数是实体的身份信息，CA根据实体提供的身份信息来唯一标识证书申请者 实体DN的配置必须与CA证书颁发策略相匹配，以确认实体DN的配置任务，如哪些实体参数为必选配置，哪些为可选配置。申请者的身份信息必须符合CA证书颁发策略，否则证书申请可能会失败

步骤	配置任务	说明
2	5.4 新建PKI域	必选 新建PKI域，配置证书申请方式为“Auto” 实体在进行PKI证书申请操作之前需要配置一些注册信息来配合完成申请的过程，这些信息的集合就是一个实体的PKI域 PKI域是一个本地概念，因此创建PKI域的目的是便于其它应用引用PKI的配置，比如IKE、SSL等，一个设备上配置的PKI域对CA和其它设备是不可见的，每一个PKI域有单独的域参数配置信息
3	5.6 销毁RSA密钥对	可选 如果要获取的证书中含有RSA密钥对，则必须先将设备上已有的密钥对销毁，否则无法成功获取证书。销毁RSA密钥对的同时，也会销毁对应的本地证书
4	5.7 获取和查看证书	可选 将已存在的证书获取至本地，获取后可以查看证书的详细信息 提示 • 在线获取本地证书之前必须完成 LDAP 服务器的配置 • 如果本地已有 CA 证书存在，则不允许再执行获取 CA 证书的操作，避免因相关配置的修改使得证书与注册信息不匹配。请先删除存储于本地的 CA 证书与本地证书后，再重新获取
5	5.9 获取和查看CRL	可选 获取CRL至本地，获取后可以查看CRL的内容

5.3 新建PKI实体

(1) 在导航栏中选择“认证 > 证书管理”，默认进入“PKI 实体”页签的页面，如下图所示。

图5-1 PKI 实体



(2) 单击<新建>按钮，进入新建 PKI 实体的配置页面，如下图所示。

图5-2 新建 PKI 实体



(3) 配置新建 PKI 实体的信息，详细配置如下表所示。

(4) 单击<确定>按钮完成操作。

表5-3 新建 PKI 实体的详细配置

配置项	说明
PKI实体名称	设置要新建的PKI实体的名称
通用名	设置实体的通用名，比如用户名称
实体IP地址	设置实体的IP地址
FQDN	设置实体的FQDN（Fully Qualified Domain Name，完全合格域名） FQDN是实体在网络中的唯一标识，由一个主机名和域名组成，可被解析为IP地址。例如，www是一个主机名，whatever.com是一个域名，则www.whatever.com就是一个FQDN
国家/地区	设置实体所属的国家或地区代码
州省	设置实体所属的州省
地理区域	设置实体所在地理区域的名称
组织	设置实体所属组织的名称
部门	设置实体所属部门的名称

5.4 新建PKI域

(1) 在导航栏中选择“认证 > 证书管理”。

(2) 单击“PKI 域”页签，进入 PKI 域的显示页面，如下图所示。

图5-3 PKI 域



(3) 单击<新建>按钮，进入新建 PKI 域的配置页面，如下图所示。

图5-4 新建 PKI 域



(4) 配置 PKI 域的信息，详细配置如下表所示。

(5) 单击<确定>按钮完成操作。

表5-4 新建 PKI 域的详细配置

配置项	说明
PKI域名称	设置要新建的PKI域的名称

配置项	说明
CA标识符	设置设备信任的CA标识符 在申请证书时，是通过一个可信实体认证机构，来完成实体证书的注册颁发，因此必须指定一个信任的CA名称，将设备与该CA进行绑定，该设备证书的申请、获取、废除及查询均通过该CA执行 当采用离线方式申请证书时，此项可以不配置，否则必须配置
本端实体	设置本端PKI实体名称 向CA发送证书申请请求时，必须指定所使用的实体名，以向CA表明自己的身份 可选的PKI实体名称需通过新建PKI实体来配置
注册机构	设置证书申请的注册审理机构 • CA：表示由 CA 来完成注册机构的功能 • RA：表示有独立的 RA 作为注册审理机构 PKI推荐独立使用RA作为注册审理机构
证书申请URL	设置注册服务器的URL 证书申请之前必须指定注册服务器的URL，随后实体可通过简单证书注册协议（SCEP，Simple Certification Enrollment Protocol）向该服务器提出证书申请，SCEP是专门用于与认证机构进行通信的协议 当采用离线方式申请证书时，此项可以不配置，否则必须配置 提示 目前，注册服务器 URL 的配置不支持域名解析
LDAP服务器IP地址 端口 版本	设置LDAP服务器的IP地址、端口号和版本号 要获取本地证书，必须正确配置LDAP服务器
证书申请方式	设置在线证书申请的方式，有手动和自动两种方式
挑战码 确认挑战码	证书申请方式选择“Auto”时，设置挑战码，即撤销证书时使用的密码 输入的挑战码和确认挑战码必须一致
根证书指纹散列算法 根证书指纹	设置验证CA根证书时所使用的指纹 当设备从CA获得根证书时，需要验证CA根证书的指纹，即根证书内容的散列值，该值对于每一个证书都是唯一的。如果CA根证书的指纹与在PKI域中配置的指纹不同，则设备将拒绝接收根证书 • 当根证书指纹散列算法选择“MD5”时，使用 MD5 指纹验证 CA 根证书，输入的根证书指纹必须为 32 个字符，并且以 16 进制的形式输入 • 当根证书指纹散列算法选择“SHA1”时，使用 SHA1 指纹验证 CA 根证书，输入的根证书指纹必须为 40 个字符，并且以 16 进制的形式输入 • 当根证书指纹散列算法选择空时，将不对根证书指纹进行验证，需要用户自行确认 CA 服务器是否可信 提示 当证书申请方式选择“Auto”时，必须设置验证根证书时所使用的指纹；当证书申请方式选择“Manual”时，可以不设置验证根证书时所使用的指纹，则在获取 CA 证书时将不对根证书指纹进行验证，需要用户自行确认 CA 服务器是否可信
证书查询次数	设置客户端发送证书申请状态查询的周期和每个周期内发送查询的次数

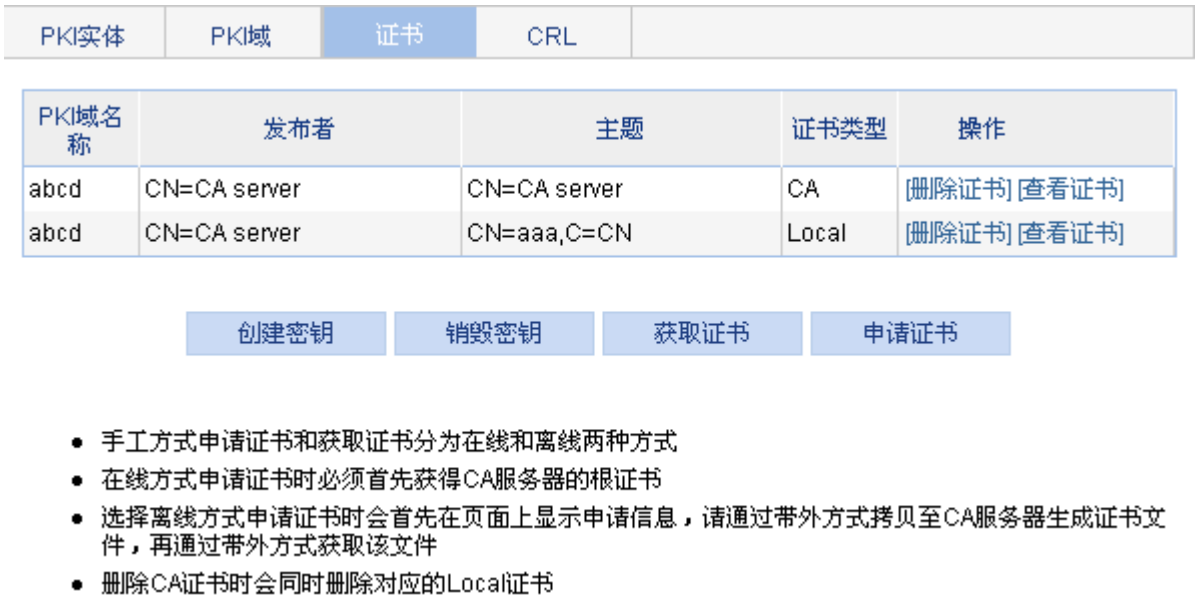
配置项	说明
证书查询间隔	实体在发送证书申请后，如果CA采用手工验证申请，证书的发布会需要很长时间。在此期间，客户端需要定期发送状态查询，以便在证书签发后能及时获取到证书
启用CRL查询	设置在证书验证时是否进行CRL检查
CRL更新间隔	启用CRL查询时，设置CRL更新间隔，即使用证书的PKI实体从CRL存储服务器下载CRL的时间间隔 缺省情况下，CRL的更新间隔由CRL文件中的下次更新域决定
获取CRL的URL	启用CRL查询时，设置CRL发布点的URL，支持IP地址和DNS域名两种表示方式 需要注意的是，未配置CRL发布点的URL时，通过SCEP协议获取CRL，该操作在获取CA证书和本地证书之后进行

5.5 生成RSA密钥对

(1) 在导航栏中选择“认证 > 证书管理”。

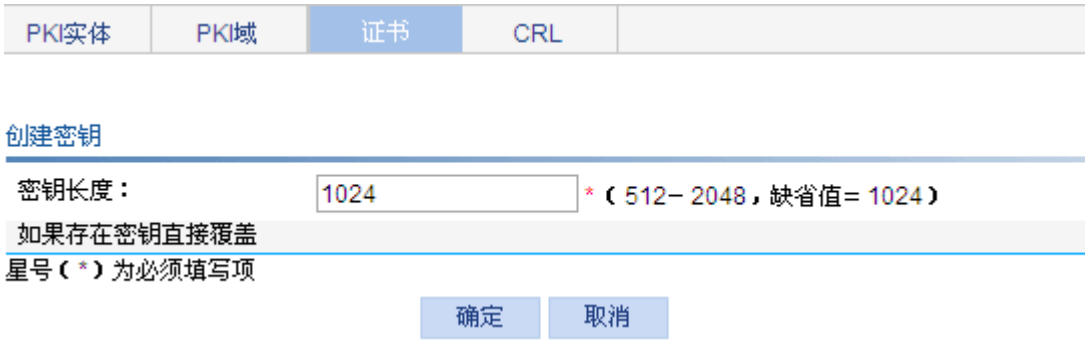
(2) 单击“证书”页签，进入 PKI 证书的显示页面，如下图所示。

图5-5 证书



(3) 单击页面上的<创建密钥>按钮，进入生成 RSA 密钥对的配置页面，如下图所示。

图5-6 创建密钥



(4) 设置 RSA 密钥的长度。

(5) 单击<确定>按钮完成操作。

5.6 销毁RSA密钥对

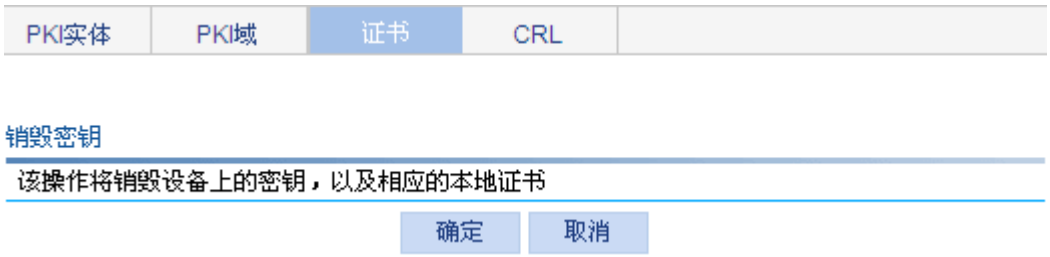
(1) 在导航栏中选择“认证 > 证书管理”。

(2) 单击“证书”页签，进入PKI证书的显示页面，如 图 5-5 所示。

(3) 单击页面上的<销毁密钥>按钮，进入销毁 RSA 密钥对的配置页面，如下图所示。

(4) 单击<确定>按钮将销毁设备上已存在的 RSA 密钥对和对应的本地证书。

图5-7 销毁密钥



5.7 获取和查看证书

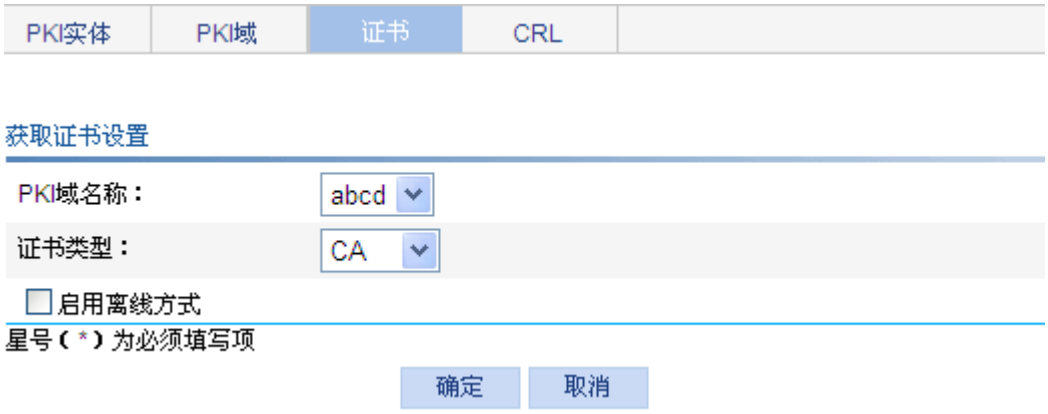
用户通过此配置可以将已存在的 CA 证书或本地证书获取至本地。获取证书有两种方式：离线方式和在线方式。离线方式下获取证书需要通过带外方式（如 FTP、磁盘、电子邮件等）取得证书，然后将其导入至本地。成功获取到本地的证书被保存在设备的根目录下，文件名称为 *domain-name*_ca.cer（CA 证书）、*domain-name*_local.cer（本地证书）。

(1) 在导航栏中选择“认证 > 证书管理”。

(2) 单击“证书”页签，进入PKI证书的显示页面，如 图 5-5 所示。

(3) 单击页面上的<获取证书>按钮，进入获取 PKI 证书的配置页面，如下图所示。

图5-8 获取证书设置



(4) 配置获取 PKI 证书所需的信息，详细配置如下表所示。

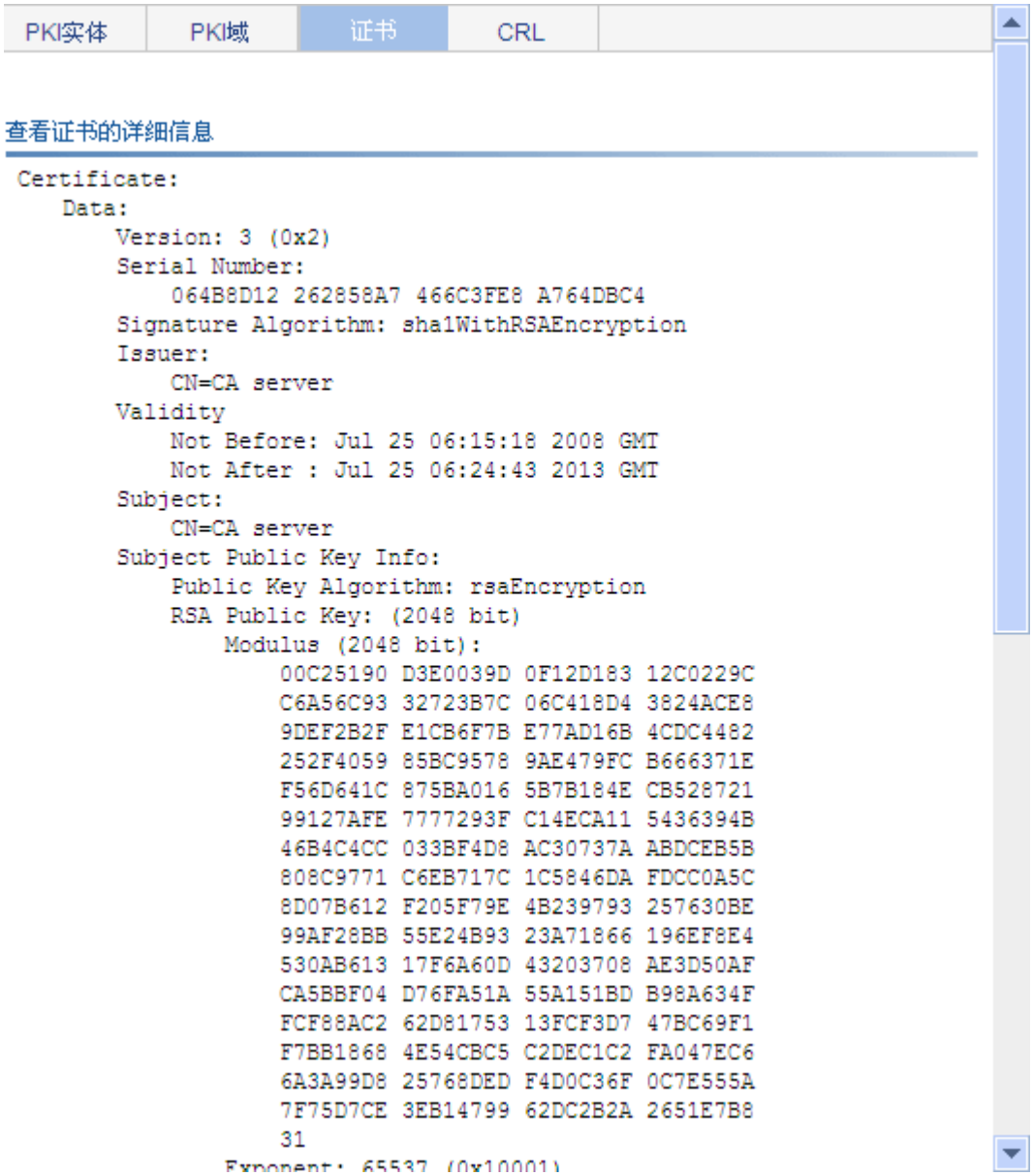
(5) 单击<确定>按钮完成操作。

表5-5 获取 PKI 证书的详细配置

配置项	说明
PKI域名称	设置证书所在的PKI域
证书类型	设置要获取的证书的为CA证书或Local证书
启用离线方式	设置是否启用离线方式（如FTP、磁盘、电子邮件等）获取证书
从设备取得文件	当启用离线方式时，设置要导入的证书文件的存放路径和文件名
从PC取得文件	• 当证书文件保存在设备上时，选择“从设备取得文件”，并选择证书文件在设备上的存放路径和文件名。如果不指定具体的文件，则默认为设备根目录下名为 *domain-name*_ca.cer（CA 证书）或 *domain-name*_local.cer（本地证书）的文件 • 当证书文件保存在本地主机上时，选择“从 PC 取得文件”，并设置证书文件在 PC 上的存放路径和文件名，以及文件上传到设备后存放在哪个分区
口令	当启用离线方式时，设置导入证书的口令，该口令在导出证书时指定，用于保护私钥的口令

(6) 获取证书后，在 PKI 证书显示页面中单击某证书对应的<查看证书>按钮，查看该证书的详细信息，如下图所示。

图5-9 查看证书的详细信息



5.8 申请本地证书

(1) 在导航栏中选择“认证 > 证书管理”。

(2) 单击“证书”页签，进入PKI证书的显示页面，如 图 5-5 所示。

(3) 单击页面上的<申请证书>按钮，进入申请本地证书的配置页面，如下图所示。

图5-10 申请证书设置



(4) 配置申请本地证书所需的信息，详细配置如下表所示。

表5-6 申请本地证书的详细配置

配置项	说明
PKI域名称	设置证书所在的PKI域
挑战码	设置挑战码，即撤销证书时使用的密码
启用离线方式	设置是否启用离线方式（如电话、磁盘、电子邮件等）申请本地证书

(5) 单击<确定>按钮。此时，如果采用在线方式申请证书，则会弹出提示框“证书申请已提交。”，再次单击<确定>按钮完成操作；如果采用离线方式申请证书，则页面上将显示离线申请证书的信息，如下图所示，用户可以将这些信息通过带外方式发送给 CA 进行证书申请。

图5-11 离线申请证书的信息



5.9 获取和查看CRL

(1) 在导航栏中选择“认证 > 证书管理”。

(2) 单击“CRL”页签，进入 CRL 的显示页面，如下图所示。

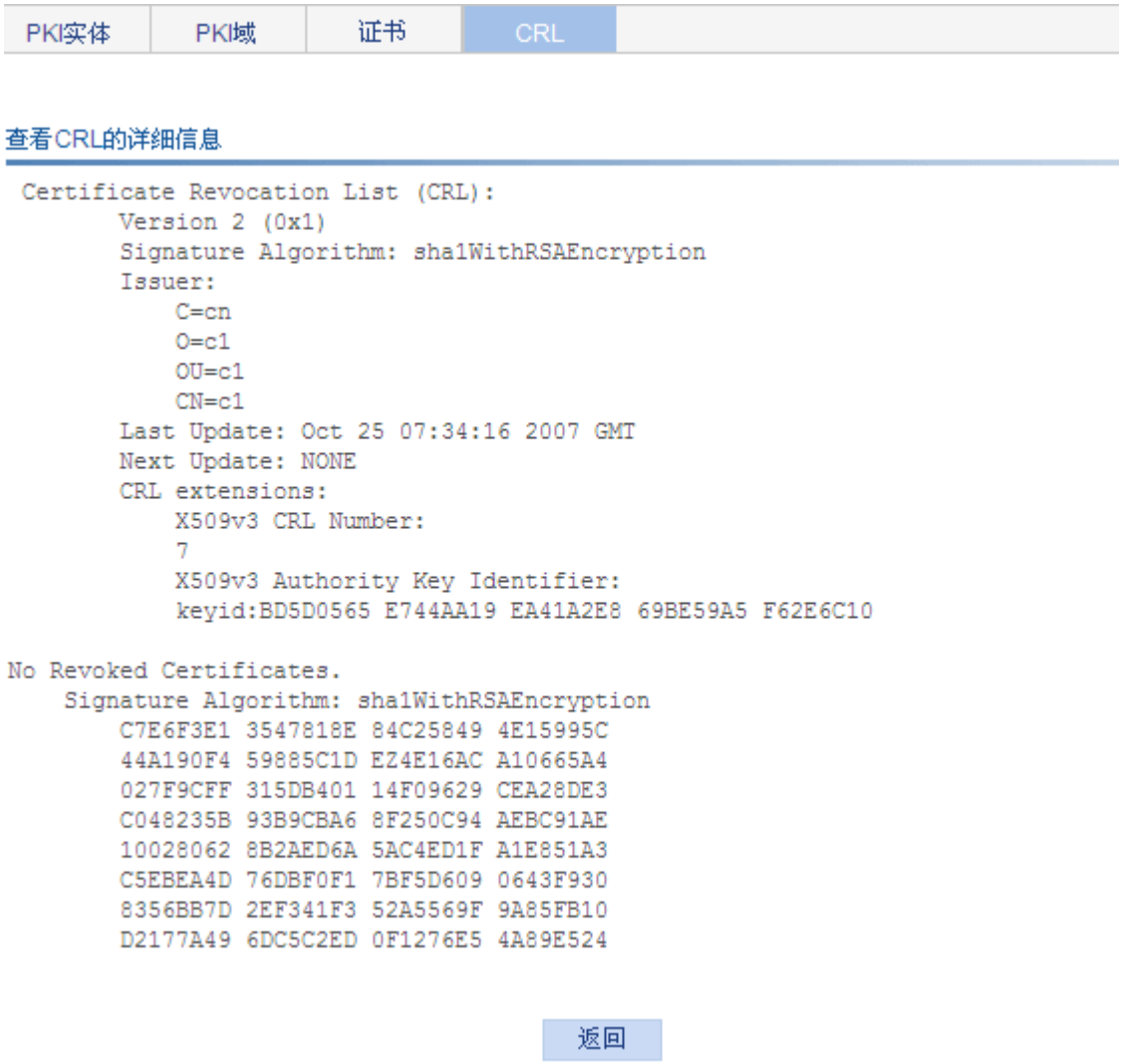
图5-12 CRL



(3) 在列表中单击某 PKI 域对应的操作列的<获取 CRL>按钮，可将其 CRL 获取到本地。

(4) 获取 CRL 后，在列表中单击该 PKI 域对应的<查看 CRL>按钮，可查看其 CRL 的详细信息，如下图所示。

图5-13 查看 CRL 的详细信息



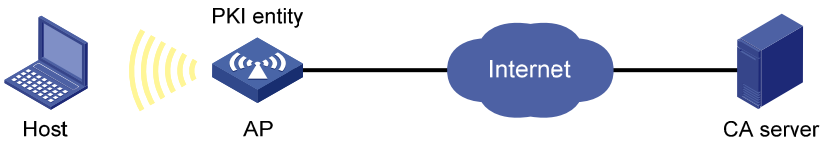
5.10 PKI典型配置举例

1. 组网需求

在作为 PKI 实体的设备 AP 上进行相关配置，实现以下需求：

- AP 向 CA 服务器申请本地证书，CA 服务器上采用 RSA Keon 软件。
- 获取 CRL 为证书验证做准备。

图5-14 PKI 实体向 CA 申请证书配置组网图



2. 配置CA服务器

(1) 创建 CA 服务器 myca。

在本例中，CA 服务器上首先需要进行基本属性 Nickname 和 Subject DN 的配置。其它属性选择默认值。其中，Nickname 为可信任的 CA 名称，Subject DN 为 CA 的 DN 属性，包括 CN、OU、O 和 C。

(2) 配置扩展属性。

基本属性配置完毕之后，还需要在生成的 CA 服务器管理页面上对“Jurisdiction Configuration”进行配置，主要内容包括：根据需要选择合适的扩展选项；启动自动颁发证书功能；添加可以自动颁发证书的地址范围。

(3) 配置 CRL 发布。

CA 服务器的基本配置完成之后，需要进行 CRL 的相关配置。本例中选择 CRL 的发布方式为 HTTP，自动生成 CRL 发布点的 URL 为 http://4.4.4.133:447/myca.crl。

说明

以上配置完成之后，还需要保证设备的系统时钟与 CA 的时钟同步才可以正常使用设备来申请证书和获取 CRL。

3. 配置AP

(1) 新建 PKI 实体。

步骤 1：在导航栏中选择“认证 > 证书管理”，默认进入“PKI 实体”页签的页面。

步骤 2：单击<新建>按钮。

步骤 3：进行如下配置，如下图所示。

- 输入 PKI 实体名称为“aaa”。
- 输入通用名为“ap”。

步骤 4：单击<确定>按钮完成操作。

图5-15 新建 PKI 实体



(2) 新建 PKI 域。

步骤 1：单击“PKI 域”页签。

步骤 2：单击<新建>按钮。

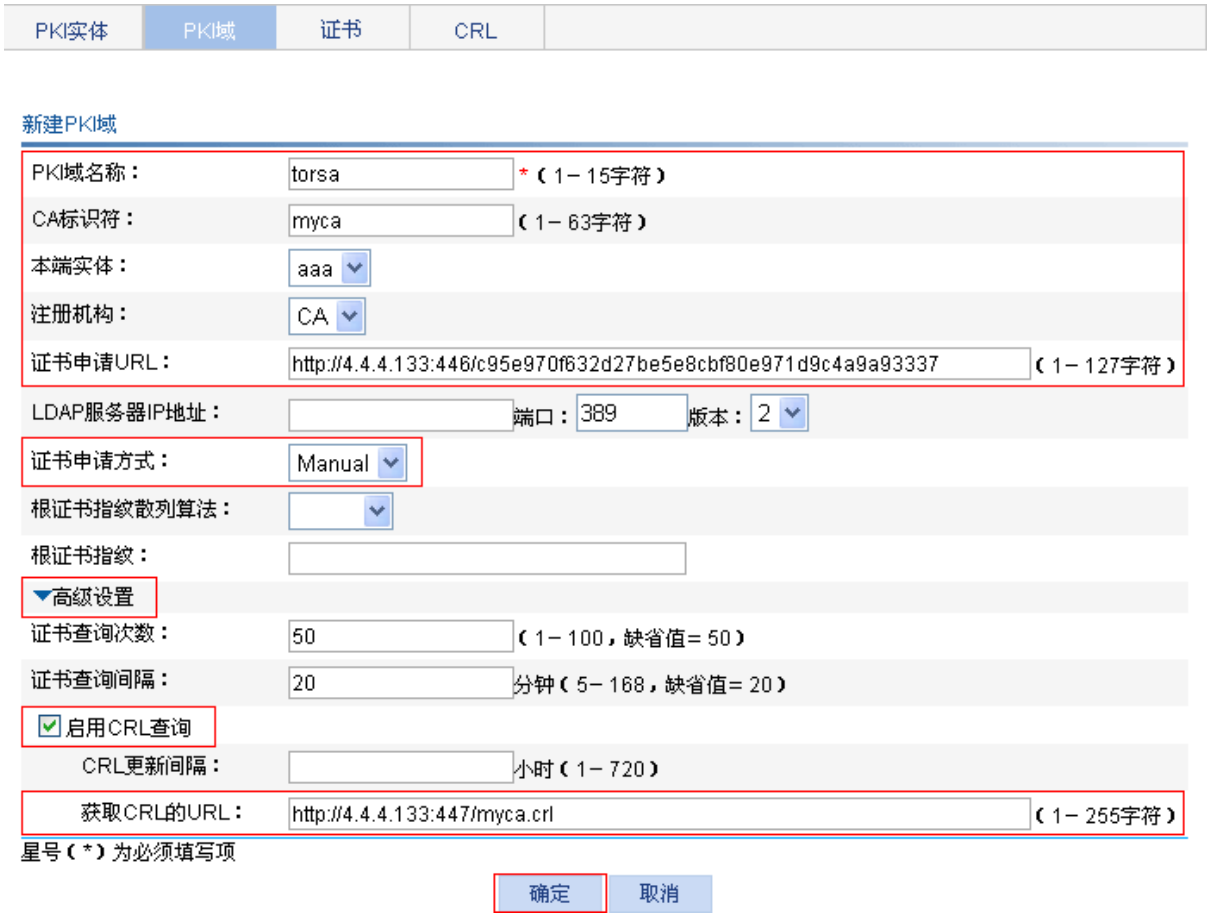
步骤 3：进行如下配置，如下图所示。

- 输入 PKI 域名称为“torsa”。
- 输入 CA 标识符为“myca”。
- 选择本端实体为“aaa”。
- 选择注册机构为“CA”。
- 以“http://host:port/Issuing Jurisdiction ID”（其中的 Issuing Jurisdiction ID 为 CA 服务器上生成的 16 进制字符串）的格式输入证书申请 URL 为“http://4.4.4.133:446/c95e970f632d27be5e8cbf80e971d9c4a9a93337”。
- 选择证书申请方式为“Manual”。
- 单击“高级设置”前的扩展按钮。
- 选中“启用 CRl 查询”前的复选框。
- 输入获取 CRL 的 URL 为“http://4.4.4.133:447/myca.crl”。

步骤 4：单击<确定>按钮，页面弹出对话框提示“未指定根证书指纹，在获取 CA 证书时将不对根证书指纹进行验证，确认要继续吗？”

步骤 5：单击对话框中的<确定>按钮完成操作。

图5-16 新建 PKI 域



(3) 生成 RSA 密钥对。

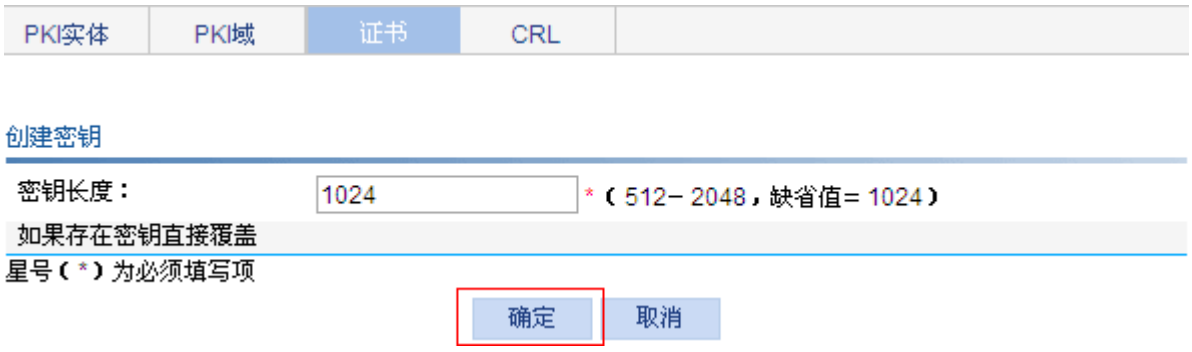
步骤 1：单击“证书”页签。

步骤 2：单击<创建密钥>按钮。

步骤 3：如下图所示，输入密钥长度为“1024”。

步骤 4：单击<确定>按钮开始生成 RSA 密钥对。

图5-17 生成 RSA 密钥对



(4) 获取 CA 证书至本地。

步骤 1：生成密钥对成功后，在“证书”页签的页面单击<获取证书>按钮。

步骤 2：进行如下配置，如下图所示。

- 选择 PKI 域为“torsa”。
- 选择证书类型为“CA”。

步骤 3：单击<确定>按钮开始获取 CA 证书。

图5-18 获取 CA 证书至本地



(5) 申请本地证书。

步骤 1：获取 CA 证书成功后，在“证书”页签的页面单击<申请证书>按钮。

步骤 2：进行如下配置，如下图所示。

- 选择 PKI 域为“torsa”。
- 选中“挑战码”前的单选按钮，输入挑战码为“challenge-word”。

步骤 3：单击<确定>按钮开始申请本地证书，弹出“证书申请已提交”的提示框。

步骤 4：单击提示框中的<确定>按钮完成操作。

图5-19 申请证书设置



(6) 获取 CRL 至本地。

步骤 1：单击“CRL”页签。

步骤 2：如下图所示，单击 PKI 域“torsa”对应的<获取 CRL>按钮开始获取 CRL。

图5-20 获取 CRL 至本地



4. 配置结果验证

完成上述配置后，可以在“证书”页签的页面中查看获取的 CA 证书和本地证书的详细信息；可以在“CRL”页签的页面中查看获取的 CRL 文件的详细信息。

5.11 注意事项

配置 PKI 时需要注意如下事项：

(1) 申请本地证书时，必须保证实体时钟与 CA 的时钟同步，否则申请证书的有效期会出现异常。

(2) Windows 2000 CA 服务器对证书申请的数据长度有一定的限制。PKI 实体身份信息配置项超过一定数据长度时，申请证书没有回应。

(3) 当采用 Windows Server 作为 CA 时，需要安装 SCEP 插件。此时，配置 PKI 域时，需要指定注册机构为 RA。

(4) 当采用 RSA Keon 软件作为 CA 时，不需要安装 SCEP 插件。此时，配置 PKI 域时，需要指定注册机构为 CA。

目 录

1 安全配置 ····· 1-1
1.1 安全简介 ····· 1-1
1.1.1 入侵检测 ····· 1-1
1.1.2 黑白名单 ····· 1-2
1.2 配置入侵检测 ····· 1-2
1.2.1 入侵检测设置 ····· 1-2
1.2.2 查看历史记录 ····· 1-3
1.2.3 查看统计信息 ····· 1-3
1.3 配置黑白名单 ····· 1-4
2 用户隔离 ····· 2-1
2.2 配置用户隔离 ····· 2-1

1 安全配置

1.1 安全简介

802.11 网络很容易受到各种网络威胁的影响，如未经授权的 AP 用户、Ad-hoc 网络、DoS 攻击等。WIDS（Wireless Intrusion Detection System，无线入侵检测系统）可以对有恶意的用户攻击和入侵行为进行早期检测和防范。

无线安全提供了如下功能：

- 入侵检测
- 黑白名单

1.1.1 入侵检测

为了及时发现 WLAN 网络的恶意或者无意的攻击，通过记录信息或者发送日志信息的方式通知网络管理者。目前设备支持的入侵检测主要包括泛洪攻击检测、Spoof 检测以及 Weak IV 检测。

1. 泛洪攻击检测

泛洪攻击（Flooding 攻击）是指 WLAN 设备会在短时间内接收了大量的同种类型的报文。此时 WLAN 设备会被泛洪的攻击报文淹没而无法处理合法无线客户端的报文。

攻击检测通过持续地监控每台无线客户端的流量大小来预防这种泛洪攻击。当流量超出可容忍的上限时，该无线客户端将被认定在实施泛洪攻击。如果在 WLAN 设备上开启动态黑名单功能，此时被检测到的攻击设备将被加入黑名单，在后续一段时间内将被禁止接入 WLAN 网络。

入侵检测支持对下列报文的泛洪攻击检测：

- 认证请求/解除认证请求（Authentication / De-authentication）；
- 关联请求/解除关联请求/重新关联请求（Association / Disassociation / Reassociation）；
- 探查请求（Probe Request）；
- 802.11 Null 数据帧；
- 802.11 Action 帧。

2. Spoofing攻击检测

Spoofing 攻击是指潜在的攻击者会仿冒其他设备的名义发送攻击报文，以达到破坏无线网络正常工作的目的。例如：无线网络中的客户端已经和 AP 关联，并处于正常工作状态，此时如果有攻击者仿冒 AP 的名义给客户端发送解除认证报文就可能导致客户端下线，同样如果攻击者仿冒客户端的名义给 AP 发送解除认证报文也会影响无线网络的正常工作。

目前，Spoofing 攻击检测支持对仿冒 AP 名义发送的广播解除认证和广播解除关联报文进行检测。当接收到这两种报文时，设备会将其定义为 Spoofing 攻击并被记录到日志中。

3. Weak IV攻击检测

使用 WEP 加密的时候，WLAN 设备对于每一个报文都会使用 IV（Initialization Vector，初始化向量），IV 和 Key 一起作为输入来生成 Key Stream，使相同密钥产生不同加密效果。当一个 WEP 报文被发送时，用于加密报文的 IV 也作为报文头的一部分被发送。如果 WLAN 设备使用不安全的方法生

成 IV，例如始终使用固定的 IV，就可能会暴露共享的密钥，如果潜在的攻击者获得了共享的密钥，攻击者将能够控制网络资源。

检测 IDS 攻击可以通过识别每个 WEP 报文的 IV 来预防这种攻击，当一个有 Weak IV 的报文被检测到时，这个检测将立刻被记录到日志中。

1.1.2 黑白名单

1. 黑白名单列表

在 WLAN 网络环境中，可以通过黑白名单功能设定一定的规则过滤无线客户端，实现对无线客户端的接入控制。

黑白名单维护三种类型的列表。

- 白名单列表：该列表包含允许接入的无线客户端的 MAC 地址。如果使用了白名单，则只有白名单中指定的无线客户端可以接入到 WLAN 网络中，其他的无线客户端将被拒绝接入。
- 静态黑名单列表：该列表包含拒绝接入的无线客户端的 MAC 地址。
- 动态黑名单列表：当 WLAN 设备检测到来自某一设备的非法攻击时，可以选择将该设备动态加入到黑名单中，拒绝接收任何来自于该设备的报文，直至该动态黑名单表项老化为止，从而实现对 WLAN 网络的安全保护。

2. 黑白名单的处理过程

黑白名单按照以下步骤对接收到的 802.11 报文进行过滤，只有满足条件的报文允许通过，其他的所有的报文都会被丢弃。

(1) 当 AP 接收到一个 802.11 帧时，将针对该 802.11 帧的源 MAC 进行过滤；

(2) 如果设置了白名单列表，但接收帧的源 MAC 不在白名单列表内，该帧将被丢弃；

(3) 如果源 MAC 在白名单内，该帧将被作为合法帧进一步处理；

(4) 如果没有设置白名单列表，则继续搜索静态和动态的黑名单列表。如果源 MAC 在静态或动态黑名单列表内，该帧将被丢弃；

(5) 如果源 MAC 没有在静态或动态黑名单列表内，或者黑名单列表为空，则该帧将被作为合法帧进一步处理。

1.2 配置入侵检测

1.2.1 入侵检测设置

(1) 在界面左侧的导航栏中选择“安全> 入侵检测”，默认进入“入侵检测设置”页签的页面，如下图所示。

图1-1 入侵检测设置



(2) 配置入侵检测，详细配置如下表所示。

表1-1 入侵检测设置的详细配置

配置项	说明
泛洪攻击检测	选中该复选框，则表示启动泛洪攻击检测 缺省情况下，泛洪攻击检测处于关闭状态
Spoofing攻击检测	选中该复选框，则表示启动Spoofing攻击检测 缺省情况下，Spoofing检测处于关闭状态
Weak IV攻击检测	选中该复选框，则表示Weak IV攻击检测 缺省情况下，Weak IV攻击检测处于关闭状态

(3) 单击<确定>按钮完成操作。

1.2.2 查看历史记录

(1) 在界面左侧的导航栏中选择“安全> 入侵检测”。

(2) 选择“历史记录”页签，进入查看历史记录的页面，如下图所示。

图1-2 查看历史记录



1.2.3 查看统计信息

(1) 在界面左侧的导航栏中选择“安全> 入侵检测”。

(2) 选择“统计信息”页签，进入查看统计信息的页面，如下图所示。

图1-3 统计信息各字段说明

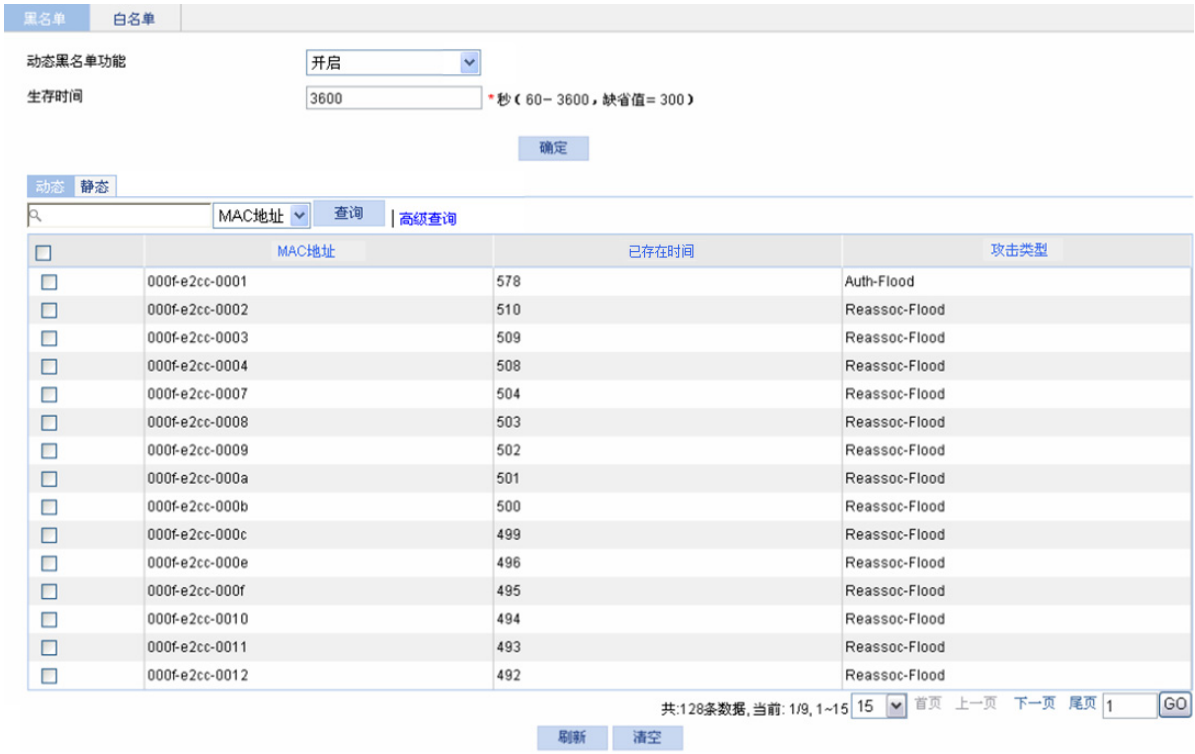


1.3 配置黑白名单

1. 配置动态黑名单

(1) 在界面左侧的导航栏中选择“安全> 黑白名单”，默认进入“黑名单”页签的页面，如下图所示。

图1-4 动态黑名单配置页面



(2) 配置动态黑名单，详细配置如下表所示。

表1-2 动态黑名单的详细配置

配置项	说明
动态黑名单功能	开启：开启动态黑名单列表功能 关闭：关闭动态黑名单列表功能 **提示** 在开启动态黑名单前，需要在“入侵检测设置”页面，选中“泛洪攻击检测”前的复选框
已存在时间	设置动态黑名单中的对应表项的生存时间，被加入到动态黑名单中的MAC表项在经过生存时间后将被删除

(3) 单击<确定>按钮完成操作。

说明

目前在动态黑名单支持检测的攻击类型有以下几种：“Assoc-Flood（关联请求泛洪攻击）”、“Reassoc-Flood（重关联请求泛洪攻击）”、“Disassoc-Flood（解除关联请求泛洪攻击）”、“ProbeReq-Flood（探查请求泛洪攻击）”、“Action-Flood（802.11 Action 帧泛洪攻击）”、“Auth-Flood（认证请求泛洪攻击）”、“Deauth-Flood（解除认证请求泛洪攻击）”和“NullData-Flood（802.11 Null 数据帧泛洪攻击）”。

2. 配置静态黑名单

(1) 在界面左侧的导航栏中选择“安全> 黑白名单”，默认进入“黑名单”页签的页面。

(2) 选择“静态”页签，进入静态黑名单的配置页面。

(3) 单击<新建静态表项>按钮，进入新建静态黑名单表项的页面，如下图所示。

图1-5 新建静态黑名单表项



(4) 新建静态黑名单表项，详细配置如下表所示。

表1-3 新建静态黑名单表项的详细配置

配置项	说明
MAC地址	选中“MAC地址”前面单选按钮，在输入框中添加指定的MAC地址到静态黑名单
选择当前连接客户端	从当前连接的客户端中，通过指定客户端MAC地址的方式把某些客户端加入到静态黑名单

(5) 单击<确定>按钮完成操作。

3. 配置白名单

(1) 在界面左侧的导航栏中选择“安全> 黑白名单”。

(2) 选择“白名单”页签，进入白名单的配置页面。

(3) 单击<新建>按钮，进入新建白名单表项的页面，如下图所示。

图1-6 新建白名单表项



(4) 新建白名单表项，详细配置如下表所示。

表1-4 新建白名单表项的详细配置

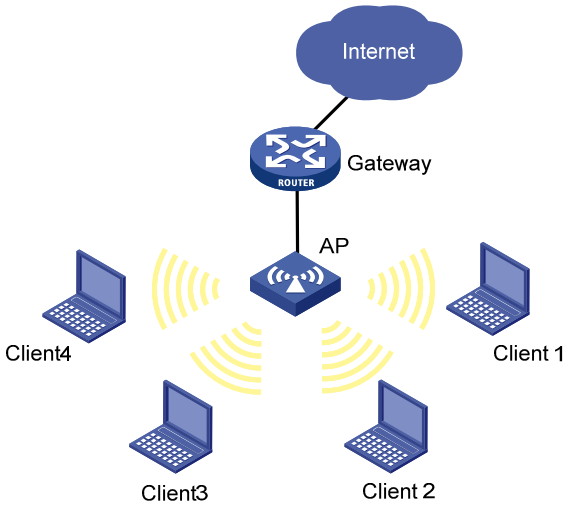
配置项	说明
MAC地址	选中“MAC地址”前面单选按钮，在输入框中添加指定的MAC地址到白名单
选择当前连接客户端	从当前连接的客户端中，通过指定客户端MAC地址的方式把某些客户端加入到白名单

(5) 单击<确定>按钮完成操作。

2 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(单播/广播)相互不能转发，从而使无线用户之间不能直接进行通讯。

图2-1 用户隔离组网图

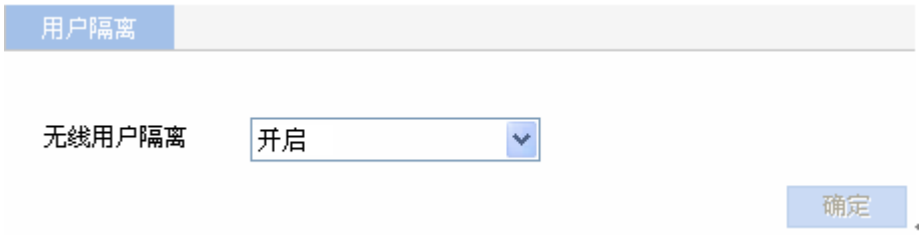


在上图中，在 AP 上开启用户隔离功能后，Client 1～Client 4 之间不能互通，也无法学习到对方的 MAC 地址和 IP 地址。

2.2 配置用户隔离

(1) 在界面左侧的导航栏中选择“安全> 用户隔离”，进入用户隔离的配置页面，如下图所示。

图2-2 配置用户隔离



(2) 配置用户隔离，详细配置如下表所示。

表2-1 用户隔离详细配置

配置项	说明
无线用户隔离	• 开启：启用无线用户二层隔离功能，使能用户隔离后无线用户之间不能互通 • 关闭：关闭无线用户二层隔离功能 缺省情况下，无线用户二层隔离功能处于开启状态

(3) 单击<确定>按钮完成操作。

目 录

1 ACL和QoS ····· 1-1
1.1 概述 ····· 1-1
1.1.1 ACL简介 ····· 1-1
1.1.2 QoS简介 ····· 1-1
1.2 配置ACL ····· 1-2
1.2.1 ACL配置任务简介 ····· 1-2
1.2.2 配置时间段 ····· 1-4
1.2.3 新建ACL ····· 1-5
1.2.4 配置IPv4 基本ACL规则 ····· 1-6
1.2.5 配置IPv4 高级ACL规则 ····· 1-7
1.2.6 配置二层ACL规则 ····· 1-10
1.2.7 新建IPv6 ACL ····· 1-11
1.2.8 配置IPv6 基本ACL规则 ····· 1-12
1.2.9 配置IPv6 高级ACL规则 ····· 1-13
1.3 配置QoS策略 ····· 1-15
1.3.1 QoS策略配置任务简介 ····· 1-15
1.3.2 新建类 ····· 1-16
1.3.3 配置分类规则 ····· 1-17
1.3.4 新建流行为 ····· 1-20
1.3.5 配置流行为的动作 ····· 1-21
1.3.6 新建策略 ····· 1-23
1.3.7 配置策略中类和流行为的对应关系 ····· 1-23
1.3.8 在端口上应用策略 ····· 1-24
1.3.9 在无线服务上应用策略 ····· 1-25
1.4 配置信任模式 ····· 1-27
1.4.1 配置信任模式 ····· 1-27
1.5 ACL和QoS典型配置举例 ····· 1-29
1.6 注意事项 ····· 1-38
2 无线服务质量配置 ····· 2-1
2.1 无线服务质量简介 ····· 2-1
2.1.1 常见术语 ····· 2-1
2.1.2 WMM协议概述 ····· 2-1

2.2 配置无线服务质量 2-3
2.2.1 开启无线服务质量 2-3
2.2.2 SVP服务设置 2-4
2.2.3 CAC准入控制策略设置 2-5
2.2.4 射频EDCA设置 2-6
2.2.5 用户EDCA设置 2-7
2.2.6 显示射频信息 2-8
2.2.7 显示客户端信息 2-10
2.3 配置限速 2-12
2.4 配置智能带宽保障 2-13
2.5 无线服务质量配置举例 2-16
2.5.1 CAC服务典型配置举例 2-16
2.5.2 静态限速配置举例 2-18
2.5.3 动态限速配置举例 2-19
2.5.4 智能带宽保障配置举例 2-20

1 ACL和QoS

1.1 概述

1.1.1 ACL简介

ACL（Access Control List，访问控制列表）是一或多条规则的集合，用于识别报文流。这里的规则是指描述报文匹配条件的判断语句，匹配条件可以是报文的源地址、目的地址、端口号等。网络设备依照这些规则识别出特定的报文，并根据预先设定的策略对其进行处理。

由 ACL 定义的报文匹配规则可以应用于诸如安全、QoS 等业务中，有关 ACL 在这些业务中的具体应用，请参见相关的配置手册。

根据规则制定依据的不同，可以将 ACL 分为如下表所示的几种类型。

表1-1 ACL 的分类

ACL 类型	编号范围	适用的 IP 版本	规则制订依据
基本ACL	2000～2999	IPv4	报文的源IP地址
		IPv6	报文的源IPv6地址
高级ACL	3000～3999	IPv4	报文的源IP地址、目的IP地址、报文优先级、IP承载的协议类型及特性等三、四层信息
		IPv6	报文的源IPv6地址、目的IPv6地址、报文优先级、IPv6承载的协议类型及特性等三、四层信息
二层ACL	4000～4999	IPv4&IPv6	报文的源MAC地址、目的MAC地址、802.1p优先级、链路层协议类型等二层信息

说明

- ACL 本身只能识别报文，而无法对识别出的报文进行处理，对这些报文的具体处理方法由应用 ACL 的业务模块来决定。
- 关于 ACL 的详细介绍请参见“ACL 和 QoS 配置指导”中的“ACL”。

1.1.2 QoS简介

QoS（Quality of Service，服务质量）是各种存在服务供需关系的场合中普遍存在的概念，它评估服务方满足客户服务需求的能力。评估通常不是精确的评分，而是注重分析在什么条件下服务是好的，在什么情况下还存在着不足，以便有针对性地做出改进。

在 Internet 中，QoS 所评估的就是网络转发分组的服务能力。由于网络提供的服务是多样的，因此对 QoS 的评估可以基于不同方面。通常所说的 QoS，是对分组转发过程中为延迟、抖动、丢包率等核心需求提供支持的服务能力的评估。

1. 传统的分组转发业务

传统的 IP 网络无区别地对待所有的报文，设备处理报文采用的策略是 FIFO（First In First Out，先入先出），它依照报文到达时间的先后顺序分配转发所需要的资源。所有报文共享网络和设备的资源，至于得到资源的多少完全取决于报文到达的时机。这种服务策略称作 Best-Effort，它尽最大的努力将报文送到目的地，但对分组转发的延迟、抖动、丢包率和可靠性等需求不提供任何承诺和保证。

传统的 Best-Effort 服务策略只适用于对带宽、延迟不敏感的 WWW、文件传输、e-mail 等业务。

2. 新业务引发的新需求

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

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

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

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



说明

关于 QoS 的详细介绍请参见“ACL 和 QoS 配置指导”中的“QoS”。

1.2 配置ACL

1.2.1 ACL配置任务简介

1. 配置IPv4 基本ACL

IPv4 基本 ACL 根据报文的源 IP 地址来制订规则，对 IPv4 报文进行匹配。

表1-2 IPv4 基本 ACL 配置步骤

步骤	配置任务	说明
1	1.2.2 配置时间段	可选
2	新建IPv4基本ACL	必选 具体配置请参见“1.2.3 新建ACL”
3	1.2.4 配置IPv4基本ACL规则	必选

2. 配置IPv4 高级ACL

IPv4 高级 ACL 可根据报文的源 IP 地址、目的 IP 地址、报文优先级、IP 承载的协议类型及特性（如 TCP/UDP 的源端口和目的端口、TCP 报文标识、ICMP 协议的消息类型和消息码等）等信息来制定规则，对 IPv4 报文进行匹配。用户可利用 IPv4 高级 ACL 制订比 IPv4 基本 ACL 更准确、丰富、灵活的规则。

表1-3 IPv4 高级 ACL 配置步骤

步骤	配置任务	说明
1	1.2.2 配置时间段	可选
2	新建IPv4高级ACL	必选 具体配置请参见“1.2.3 新建ACL”
3	1.2.5 配置IPv4高级ACL规则	必选

3. 配置二层ACL

二层 ACL 可根据报文的源 MAC 地址、目的 MAC 地址、802.1p 优先级、链路层协议类型等二层信息来制订规则，对报文进行匹配。

表1-4 二层 ACL 配置步骤

步骤	配置任务	说明
1	1.2.2 配置时间段	可选
2	新建二层ACL	必选 具体配置请参见“1.2.3 新建ACL”
3	1.2.6 配置二层ACL规则	必选

4. 配置IPv6 基本ACL

IPv6 基本 ACL 根据报文的源 IPv6 地址来制订规则，对 IPv6 报文进行匹配。

表1-5 IPv6 基本 ACL 配置步骤

步骤	配置任务	说明
1	1.2.2 配置时间段	可选
2	新建IPv6基本ACL	必选 具体配置请参见“1.2.7 新建IPv6 ACL”
3	1.2.8 配置IPv6基本ACL规则	必选

5. 配置IPv6 高级ACL

IPv6 高级 ACL 可根据报文的源 IPv6 地址、目的 IPv6 地址、报文优先级、IPv6 承载的协议类型及特性（如 TCP/UDP 的源端口和目的端口、TCP 报文标识、ICMPv6 协议的消息类型和消息码等）等信息来制定规则，对 IPv6 报文进行匹配。用户可利用 IPv6 高级 ACL 制订比 IPv6 基本 ACL 更准确、丰富、灵活的规则。

表1-6 IPv6 高级 ACL 配置步骤

步骤	配置任务	说明
1	1.2.2 配置时间段	可选
2	新建IPv6高级ACL	必选 具体配置请参见“1.2.7 新建IPv6 ACL”
3	1.2.9 配置IPv6高级ACL规则	必选

1.2.2 配置时间段

每条 ACL 规则都可引用一个时间段，该规则只在指定的时间段内生效。时间段的具体配置过程如下：

(1) 在导航栏中选择“QoS > 时间段”。

(2) 单击“新建”页签，进入时间段的配置页面，如下图所示。

图1-1 时间段新建



(3) 配置时间段的信息，详细配置如下表所示。

(4) 单击<应用>按钮完成操作。

表1-7 时间段的详细配置

配置项	说明
时间段名称	设置时间段的名称

配置项		说明	
周期时间段	开始时间	设置一个周期时间范围的开始时间	选中“周期时间段”前面的复选框后可用
	结束时间	设置一个周期时间范围的结束时间，必须大于开始时间	
	星期日～星期六	设置要配置的时间范围在每星期几有效。可在星期日～星期六前的复选框中勾选	
绝对时间段	从	设置一个绝对时间范围从某年某月某日的某一时间开始	选中“绝对时间段”前面的复选框后可用
	到	设置一个绝对时间范围到某年某月某日的某一时间结束，必须大于有效时间范围的开始时间	

1.2.3 新建ACL

(1) 在导航栏中选择“QoS > ACL IPv4”。

(2) 单击“新建”页签，进入 ACL 的新建页面，如下图所示。

图1-2 ACL 新建



(3) 配置 ACL 的信息，详细配置如下表所示。

(4) 单击<应用>按钮完成操作。

表1-8 新建 IPv4 ACL 的详细配置

配置项	说明
访问控制列表ID	设置ACL的编号 • 2000～2999 为 IPv4 基本 ACL • 3000～3999 为 IPv4 高级 ACL • 4000～4999 为二层 ACL IPv4基本ACL和IPv4高级ACL的编号只在IPv4中唯一
匹配规则	设置ACL中各规则的匹配顺序 • 用户配置：按用户的配置顺序进行规则匹配 • 自动：系统自动排序，即按深度优先的原则进行规则匹配
描述	设置ACL的描述信息

1.2.4 配置IPv4 基本ACL规则

(1) 在导航栏中选择“QoS > ACL IPv4”。

(2) 单击“基本配置”页签，进入 IPv4 基本 ACL 规则的配置页面，如下图所示。

图1-3 IPv4 基本 ACL 规则配置



(3) 配置 IPv4 基本 ACL 规则的信息，详细配置如下表所示。

(4) 单击<新建>按钮完成操作。

表1-9 IPv4 基本 ACL 规则的详细配置

配置项	说明
访问控制列表	设置规则所属的IPv4基本ACL
规则ID	设置规则的ID 如果不指定，系统将为该规则自动指定一个规则ID 提示 如果指定的规则 ID 已经存在，则将该规则修改为新指定的配置
操作	设置对匹配该规则的IPv4报文所进行的操作 • 允许：表示允许匹配该规则的 IPv4 报文通过 • 禁止：表示禁止匹配该规则的 IPv4 报文通过
分片报文	设置该规则仅对非首片分片报文有效，对首片分片报文和非分片报文无效 如不设置，则规则对非分片报文和分片报文均有效
记录日志	设置对匹配该规则的IPv4报文记录日志 日志内容包括：ACL规则ID、报文通过或被丢弃、IP承载的上层协议类型、源/目的地址、源/目的端口号、报文的数目
源IP地址	设置IPv4报文的源IP地址和通配符（即通配符掩码） 均要求为点分十进制格式
源地址通配符	
时间段	设置规则生效的时间段

1.2.5 配置IPv4 高级ACL规则

(1) 在导航栏中选择“QoS > ACL IPv4”。

(2) 单击“高级配置”页签，进入 IPv4 高级 ACL 规则的配置页面，如下图所示。

图1-4 IPv4 高级 ACL 规则配置



(3) 配置 IPv4 高级 ACL 规则的信息，详细配置如下表所示。

(4) 单击<新建>按钮完成操作。

表1-10 IPv4 高级 ACL 规则的详细配置

配置项	说明
访问控制列表	设置规则所属的IPv4高级ACL
规则ID	设置规则的ID 如果不指定，系统将为该规则自动指定一个规则ID 提示 如果指定的规则 ID 已经存在，则将该规则修改为新指定的配置

配置项			说明
操作			设置对匹配该规则的IPv4报文所进行的操作 • 允许：表示允许匹配该规则的 IPv4 报文通过 • 禁止：表示禁止匹配该规则的 IPv4 报文通过
分片报文			设置该规则仅对非首片分片报文有效，对首片分片报文和非分片报文无效 如不设置，则规则对非分片报文和分片报文均有效
记录日志			设置对匹配该规则的IPv4报文记录日志 日志内容包括：ACL规则ID、报文通过或被丢弃、IP承载的上层协议类型、源/目的地址、源/目的端口号、报文的数目
IP地址过滤	源IP地址		设置IPv4报文的源IP地址和通配符（即通配符掩码），均要求为点分十进制格式
	源地址通配符		
	目的IP地址		设置IPv4报文的目的IP地址和通配符（即通配符掩码），均要求为点分十进制格式
	目的地址通配符		
协议			设置IP承载的协议类型 选择“1 ICMP”协议后，需配置ICMP类型；选择“6 TCP”或“17 UDP”协议后，可配置TCP/UDP类型
ICMP类型	选择ICMP		设置规则的ICMP报文的消息类型和消息码信息 只有配置项“协议”选择为“1 ICMP”时，才可以配置 在“选择ICMP”下拉框中选择一种ICMP报文类型。如果选择“其他”，则下面的ICMP类型、ICMP码必选输入；否则，下面显示的ICMP类型、ICMP码为系统默认的标准值，不可修改
	ICMP类型		
	ICMP码		
TCP/UDP端口	已连接		设置对TCP连接报文的处理规则 只有配置项“协议”选择为“6 TCP”时，才可以配置 对于路由器，定义规则匹配带有ack或者rst标志的TCP连接报文；对于交换机，请以各产品实际情况为准
	源	操作	设置TCP/UDP报文的源端口信息和目的端口信息 只有配置项“协议”选择为“6 TCP”或“17 UDP”时，才可以配置 分别在“源”和“目的”中的“操作”下拉框中选择端口操作符 • 选择“无限制”时，后面的两个“端口”配置项不可以配置 • 选择“在某个范围内”时，后面的两个“端口”配置项都要配置，共同确定一个端口号范围 • 选择其它选项时，后面的两个“端口”配置项中只有第一个要配置，第二个不可以配置
		端口	
		端口	
	目的	操作	
		端口	
		端口	
优先级过滤	DSCP		设置DSCP优先级
	ToS		设置ToS优先级
	Precedence		设置IP优先级
时间段			设置规则生效的时间段

1.2.6 配置二层ACL规则

(1) 在导航栏中选择“QoS > ACL IPv4”。

(2) 单击“链路层配置”页签，进入二层 ACL 规则的配置页面，如下图所示。

图1-5 链路层 ACL 配置



(3) 配置二层 ACL 规则的信息，详细配置如下表所示。

(4) 单击<新建>按钮完成操作。

表1-11 二层 ACL 规则的详细配置

配置项	说明
访问控制列表	设置规则所属的二层ACL
规则ID	设置规则的ID 如果不指定，系统将为该规则自动指定一个规则ID 提示 如果指定的规则 ID 已经存在，则将该规则修改为新指定的配置
操作	设置对匹配该规则的报文所进行的操作 • 允许：表示允许匹配该规则的报文通过 • 禁止：表示禁止匹配该规则的报文通过

配置项		说明	
MAC地址过滤器	源MAC地址	设置报文的源MAC地址和掩码	
	源MAC掩码		
	目的MAC地址	设置报文的目的MAC地址和掩码	
	目的MAC掩码		
COS(802.1p priority)		设置规则的802.1p优先级	
类型过滤器	LSAP类型	设置规则中LLC封装中的DSAP字段和SSAP字段 • LSAP 类型：表示数据帧的封装格式 • LSAP 掩码：表示类型掩码，用于指定屏蔽位	提示 LSAP 类型/掩码和协议类型/掩码只能选择其中一个
	LSAP掩码		
	协议类型	设置规则中的链路层协议类型 • 协议类型：表示数据帧的类型，对应 Ethernet_II 类型和 Ethernet_SNAP 类型帧中的 type-code 域 • 协议掩码：表示类型掩码，用于指定屏蔽位	
	协议掩码		
时间段		设置规则生效的时间段	

1.2.7 新建IPv6 ACL

(1) 在导航栏中选择“QoS > ACL IPv6”。

(2) 单击“新建”页签，进入 IPv6 ACL 的新建页面，如下图所示。

图1-6 IPv6 ACL 新建



(3) 配置 IPv6 ACL 的信息，详细配置如下表所示。

(4) 单击<应用>按钮完成操作。

表1-12 新建 IPv6 ACL 的详细配置

配置项	说明
访问控制列表ID	设置IPv6 ACL的编号 • 2000～2999 为 IPv6 基本 ACL • 3000～3999 为 IPv6 高级 ACL IPv6基本ACL和IPv6高级ACL的编号只在IPv6中唯一
匹配规则	设置IPv6 ACL中各规则的匹配顺序 • 用户配置：按用户的配置顺序进行规则匹配 • 自动：系统自动排序，即按深度优先的原则进行规则匹配
描述	设置IPv6 ACL的描述信息

1.2.8 配置IPv6 基本ACL规则

(1) 在导航栏中选择“QoS > ACL IPv6”。

(2) 单击“基本配置”页签，进入 IPv6 基本 ACL 规则的配置页面，如下图所示。

图1-7 IPv6 基本 ACL 规则配置



(3) 配置 IPv6 基本 ACL 规则的信息，详细配置如下表所示。

(4) 单击<新建>按钮完成操作。

表1-13 IPv6 基本 ACL 规则的详细配置

配置项	说明
访问控制列表	设置规则所属的IPv6基本ACL
规则ID	设置规则的ID 如果不指定，系统将为该规则自动指定一个规则ID 提示 如果指定的规则 ID 已经存在，则将该规则修改为新指定的配置
操作	设置对匹配该规则的IPv6报文所进行的操作 • 允许：表示允许匹配该规则的 IPv6 报文通过 • 禁止：表示禁止匹配该规则的 IPv6 报文通过
分片报文	设置该规则仅对非首片分片报文有效，对首片分片报文和非分片报文无效 如不设置，则规则对非分片报文和分片报文均有效
记录日志	设置对匹配该规则的IPv6报文记录日志 日志内容包括：ACL规则ID、报文通过或被丢弃、IP承载的上层协议类型、源/目的IPv6地址、源/目的端口号、报文的数目
源IP地址	设置定IPv6报文的源IPv6地址和地址前缀长度 IPv6地址的格式类似于X:X::X:X。IPv6地址共128bit，每16bit为一段，段之间用“:”分隔，每段都可以用4位十六进制数表示
源地址前缀	
时间段	设置规则生效的时间段

1.2.9 配置IPv6 高级ACL规则

(1) 在导航栏中选择“QoS > ACL IPv6”。

(2) 单击“高级配置”页签，进入 IPv6 高级 ACL 规则的配置页面，如下图所示。

图1-8 IPv6 高级 ACL 配置



(3) 配置 IPv6 高级 ACL 规则的信息，详细配置如下表所示。

(4) 单击<新建>按钮完成操作。

表1-14 IPv6 高级 ACL 规则的详细配置

配置项	说明
访问控制列表	设置规则所属的IPv6高级ACL
规则ID	设置规则的ID 如果不指定，系统将为该规则自动指定一个规则ID 提示 如果指定的规则 ID 已经存在，则将该规则修改为新指定的配置

配置项			说明
操作			设置对匹配该规则的IPv6报文所进行的操作 • 允许：表示允许匹配该规则的 IPv6 报文通过 • 禁止：表示禁止匹配该规则的 IPv6 报文通过
分片报文			设置该规则仅对非首片分片报文有效，对首片分片报文和非分片报文无效 如不设置，则规则对非分片报文和分片报文均有效
记录日志			设置对匹配该规则的IPv6报文记录日志 日志内容包括：ACL规则ID、报文通过或被丢弃、IP承载的上层协议类型、源/目的IPv6地址、源/目的端口号、报文的数目
IP地址过滤	源IP地址		设置IPv6报文的源IPv6地址和地址前缀长度 IPv6地址的格式类似于X:X::X:X。IPv6地址共128bit，每16bit为一段，段之间用“:”分隔，每段都可以用4位十六进制数表示
	源地址前缀		
	目的IP地址		设置IPv6报文的目的IPv6地址和地址前缀长度 IPv6地址的格式类似于X:X::X:X。IPv6地址共128bit，每16bit为一段，段之间用“:”分隔，每段都可以用4位十六进制数表示
	目的地址前缀		
协议			设置IPv6承载的协议类型 选择“58 ICMPv6”协议后，需配置ICMP类型；选择“6 TCP”或“17 UDP”协议后，可以配置TCP/UDP类型
ICMPv6类型	选择ICMPv6		设置规则的ICMPv6报文的消息类型和消息码信息 只有配置项“协议”选择为“58 ICMPv6”时，才可以配置 在“选择ICMPv6”下拉框中选择一种ICMPv6报文格式。如果选择“其他”，则下面的ICMPv6类型、ICMPv6码必选输入；否则，下面的ICMPv6类型、ICMPv6码为系统默认的标准值，不可修改
	ICMPv6类型		
	ICMPv6码		
TCP/UDP端口	源	操作	设置TCP/UDP报文的源端口信息和目的端口信息 只有配置项“协议”选择为“6 TCP”或“17 UDP”时，才可以配置 分别在“源”和“目的”中的“操作”下拉框中选择端口操作符 • 选择“无限制”时，后面的两个“端口”配置项不可以配置 • 选择“在某个范围内”时，后面的两个“端口”配置项都要配置，共同确定一个端口号范围 • 选择其它选项时，后面的两个“端口”配置项中只有第一个要配置，第二个不可以配置
		端口	
		端口	
	目的	操作	
		端口	
		端口	
时间段			设置规则生效的时间段

1.3 配置QoS策略

1.3.1 QoS策略配置任务简介

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

(1) 类

类是用来识别流的。

类的要素包括：类的名称和类的规则。

用户可以定义一系列的规则，来对报文进行分类。同时用户可以指定规则之间的关系：and 和 or。

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

(2) 流行为

流行为用来定义针对报文所做的 QoS 动作。

流行为的要素包括：流行为的名称和流行为中定义的动作。

用户可以在一个流行为中定义多个动作。

(3) 策略

策略用来将指定的类和指定的流行为绑定起来。

策略的要素包括：策略名称、绑定在一起的类和流行为的名称。

QoS 策略支持即基于端口的应用方式，即 QoS 策略对端口接收或者发送的流量生效。一个策略可以在多个端口上得到应用。端口的每个方向（出/入两个方向）只能应用一个策略。

QoS 策略配置的推荐步骤如下表所示。

表1-15 QoS 策略配置步骤

步骤	配置任务		说明
1	配置类	1.3.2 新建类	必选 新建一个类，并配置该类下的规则之间的逻辑关系
		1.3.3 配置分类规则	必选 配置类中报文所匹配的规则
2	配置流行为	1.3.4 新建流行为	必选 新建一个流行为
		1.3.5 配置流行为的动作	必选 配置流行为的各种动作
3	配置策略	1.3.6 新建策略	必选 新建一个策略
		1.3.7 配置策略中类和流行为的对应关系	必选 在策略中为类指定采用的流行为 策略下每个类只能与一个流行为关联，如果一个策略下的某个类与多个流行为配置了关联，则最后的配置将覆盖前面的配置
4	1.3.8 在端口上应用策略		二者至少选其一 在指定的端口或无线服务上应用QoS策略
5	1.3.9 在无线服务上应用策略		

1.3.2 新建类

(1) 在导航栏中选择“QoS > 类”。

(2) 单击“新建”页签，进入类的新建页面，如下图所示。

图1-9 类新建



(3) 配置类的信息，详细配置如下表所示。

(4) 单击<新建>按钮完成操作。

表1-16 新建类的详细配置

配置项	说明
类名称	为要新建的类指定一个类名称
操作	指定类下的规则之间的逻辑关系： • And：逻辑与的关系，即数据包必须匹配全部规则才属于该类 • Or：逻辑或的关系，即数据包只要匹配其中任何一个规则就属于该类

1.3.3 配置分类规则

(1) 在导航栏中选择“QoS > 类”。

(2) 单击“设置”页签，进入类的设置页面，如下图所示。

图1-10 类设置



(3) 配置分类规则的信息，详细配置如下表所示。

(4) 单击<应用>按钮，弹出配置进度对话框。

(5) 看到配置成功的提示后，在对话框中单击<关闭>按钮完成操作。

表1-17 分类规则的详细配置

配置项	说明
请选择一个类名称	在下拉框中选择一个已存在的类名称
匹配每个报文	设置匹配所有报文的规则 选中前面的复选框， 表示匹配所有的报文

配置项		说明
DSCP		设置匹配DSCP的规则 一个类下可配置多条这样的规则，各个配置之间互相不覆盖 每次最多可以配置8个不同的DSCP值；如果一次配置中有多个DSCP值相同，系统默认为一个；多个不同的DSCP值是或的关系；每次配置后，DSCP值将自动按照从小到大的顺序排序显示
IP优先级		设置匹配IP优先级的规则 一个类下可配置多条这样的规则，各个配置之间互相不覆盖 每次最多可以配置8个不同的IP优先级值；如果一次配置中有多个IP优先级值相同，系统默认为一个；多个不同的IP优先级值是或的关系；每次配置后，IP优先级值将自动按照从小到大的顺序排序显示
类名称		设置匹配QoS类的规则  提示 设备不支持类名称设置
入接口		设置匹配入接口的规则  提示 设备不支持入接口设置
RTP Port		设置匹配RTP协议的端口范围 from为起始端口号start port；to为结束端口号end port  提示 设备不支持 RTP Port 设置
Dot1p	运营商网络802.1p	设置匹配运营商网络802.1p优先级的规则 一个类下可配置多条这样的规则，各个配置之间互相不覆盖 每次最多可以配置8个不同的Dot1p值；如果一次配置中有多个Dot1p值相同，系统默认为一个；多个不同的Dot1p值是或的关系；每次配置后，Dot1p值将自动按照从小到大的顺序排序显示  提示 设备不支持运营商网络 802.1p 设置
	用户网络802.1p	设置匹配用户网络802.1p优先级的规则 一个类下可配置多条这样的规则，各个配置之间互相不覆盖 每次最多可以配置8个不同的Dot1p值；如果一次配置中有多个Dot1p值相同，系统默认为一个；多个不同的Dot1p值是或的关系；每次配置后，Dot1p值将自动按照从小到大的顺序排序显示
MAC地址	源MAC地址	设置匹配报文源MAC地址的规则 一个类下可配置多条这样的规则，各个配置之间互相不覆盖 匹配源MAC地址规则只对以太网类型的接口有意义
	目的MAC地址	设置匹配报文目的MAC地址的规则 一个类下可配置多条这样的规则，各个配置之间互相不覆盖 匹配目的MAC地址规则只对以太网类型的接口有意义

配置项		说明
VLAN	运营商网络号	设置匹配运营商网络VLAN ID的规则 一个类下可配置多条这样的规则，各个配置之间互相不覆盖 每次可以配置多个VLAN ID值，如果一次配置中有多个VLAN ID值相同，系统默认为一个；多个不同的VLAN ID值是或的关系。有两种输入方式： • 输入一个连续的 VLAN ID 范围，其中包含的 VLAN ID 个数没有限制，如：10-500 • 输入不连续的 VLAN ID 或范围，其中最多可以包含 8 个 VLAN ID，如：3,5-7,10 提示 设备不支持运营商网络号设置
	用户网络号	设置匹配用户网络VLAN ID的规则 一个类下可配置多条这样的规则，各个配置之间互相不覆盖 每次可以配置多个VLAN ID值，如果一次配置中有多个VLAN ID值相同，系统默认为一个；多个不同的VLAN ID值是或的关系。有两种输入方式： • 输入一个连续的 VLAN ID 范围，其中包含的 VLAN ID 个数没有限制，如：10-500 • 输入不连续的 VLAN ID 或范围，其中最多可以包含 8 个 VLAN ID，如：3,5-7,10
访问控制列表	ACL IPv4	设置匹配IPv4 ACL的规则
	ACL IPv6	设置匹配IPv6 ACL的规则

1.3.4 新建流行为

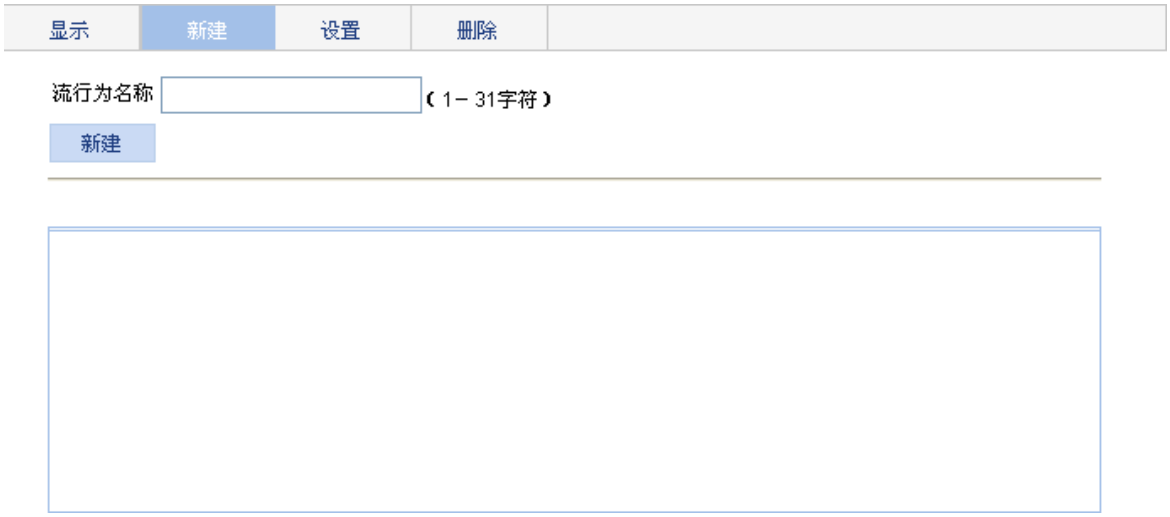
(1) 在导航栏中选择“QoS > 流行为”。

(2) 单击“新建”页签，进入流行为的新建页面，如下图所示。

(3) 设置流行为的名称。

(4) 单击<新建>按钮完成操作。

图1-11 流行为新建



1.3.5 配置流行为的动作

(1) 在导航栏中选择“QoS > 流行为”。

(2) 单击“设置”页签，进入流行为的设置页面，如下图所示。

图1-12 流行为设置



(3) 配置流行为的动作信息，详细配置如下表所示。

(4) 单击<应用>按钮，弹出配置进度对话框。

(5) 看到配置成功的提示后，在对话框中单击<关闭>按钮完成操作。

表1-18 流行为动作的详细配置

配置项	说明
请选择一个流行为	在下拉框中选择一个已存在的流行为名称

配置项			说明
流量监管	使能/禁止		设置使能或禁止流量监管
	CIR		设置承诺信息速率，流量的平均速率
	CBS		设置承诺突发尺寸，每个时间间隔可发送的位数
	Red	丢包	设置数据包的流量不符合承诺速率时，对数据包采取的动作 选中“Red”前的复选框后，可点击后面两个单选按钮进行选择： • 丢包：表示丢弃数据包 • 发送：表示发送数据包 • 设置 DSCP 后发送：表示设置 DSCP 后发送数据包
		发送	
		设置DSCP后发送	
标记QoS值	IP优先级		设置标记报文的IP优先级 选中前面的复选框后，在后面的下拉框中选择IP优先级，选择Not Set表示取消标记报文的IP优先级的设置 提示 设备不支持 IP 优先级的设置
	IEEE802.1p优先级		设置标记报文的802.1p优先级 选中前面的复选框后，在后面的下拉框中选择802.1p优先级，选择Not Set表示取消标记报文的802.1p优先级的设置
	本地优先级		设置标记报文的本地优先级 选中前面的复选框后，在后面的下拉框中选择本地优先级，选择Not Set表示取消标记报文的本地优先级的设置
	DSCP		设置标记报文的DSCP值 选中前面的复选框后，在后面的下拉框中选择DSCP值，选择Not Set表示取消标记报文的DSCP值的设置 提示 设备不支持 DSCP 的设置
队列	EF	带宽限制	设置加速转发（Expedited Forwarding）的最大带宽限制 提示 设备不支持队列的设置
		CBS	设置加速转发的承诺突发尺寸
		百分比	设置加速转发可用带宽的百分比
		CBS-Ratio	设置加速转发允许的突发因子
	AF	带宽限制	设置确保转发（Assured Forwarding）的最小带宽保证
		百分比	设置确保转发可用带宽的百分比
	WFQ		设置为缺省类配置采用公平队列，并指定公平队列的数目 公平队列的数目必须为2的幂数
包过滤			设置包过滤动作 选中前面的复选框后，在后面的下拉框中进行选择： • Permit：表示发送数据包 • Deny：表示丢弃数据包 • Not Set：表示取消包过滤动作设置

配置项	说明
流量统计	设置流量统计动作 选中前面的复选框后，在后面的下拉框中选择Enable或Disable流量统计动作 提示 设备不支持流量统计的设置

1.3.6 新建策略

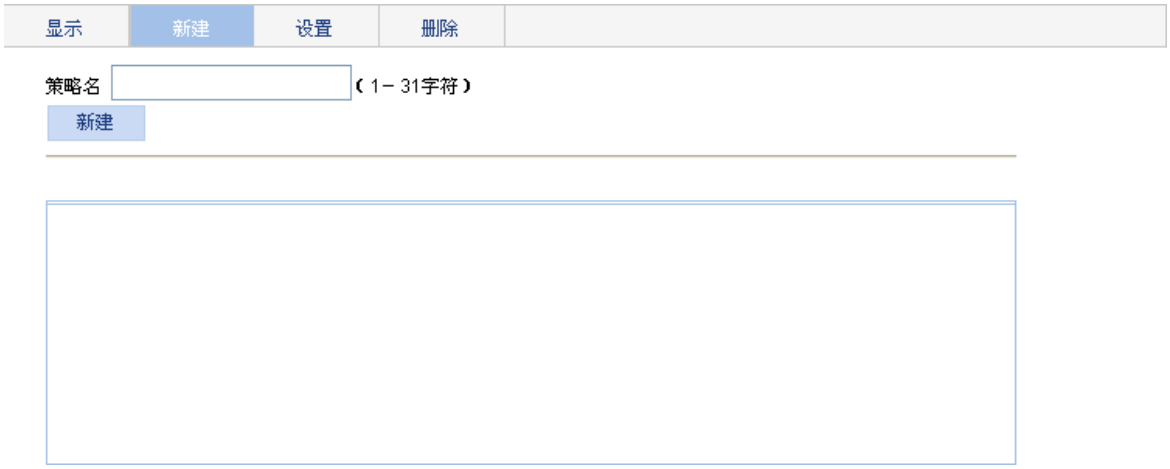
(1) 在导航栏中选择“QoS > QoS Policy”。

(2) 单击“新建”页签，进入策略的新建页面，如下图所示。

(3) 设置策略的名称。

(4) 单击<新建>按钮完成操作。

图1-13 策略新建

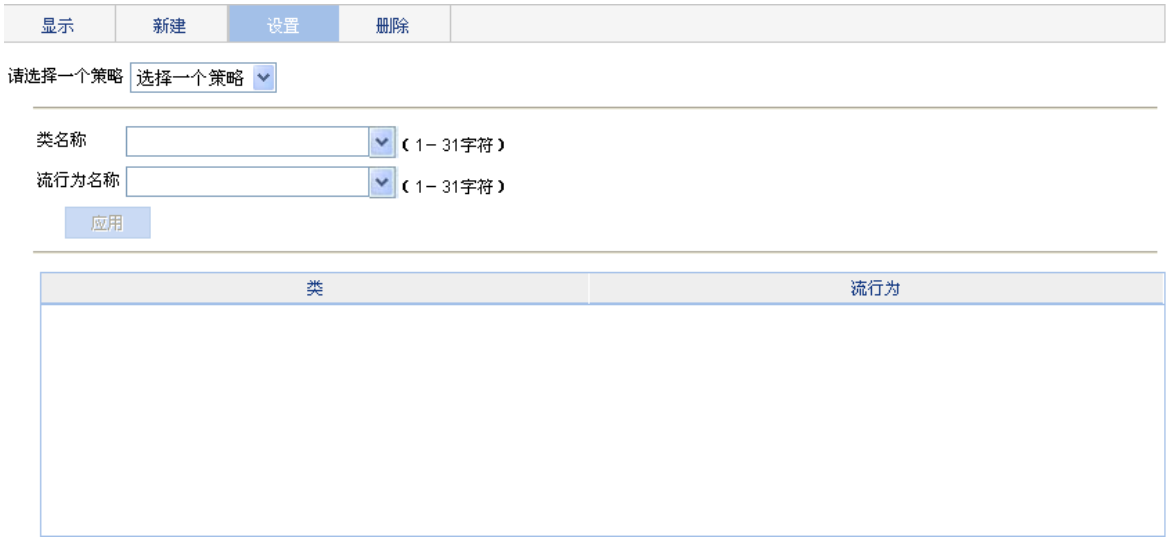


1.3.7 配置策略中类和流行为的对应关系

(1) 在导航栏中选择“QoS > QoS Policy”。

(2) 单击“设置”页签，进入策略的设置页面，如下图所示。

图1-14 策略设置



(3) 配置策略中类和流行为对应关系，详细配置如下表所示。

(4) 单击<应用>按钮完成操作。

表1-19 策略中类和流行为对应关系的详细配置

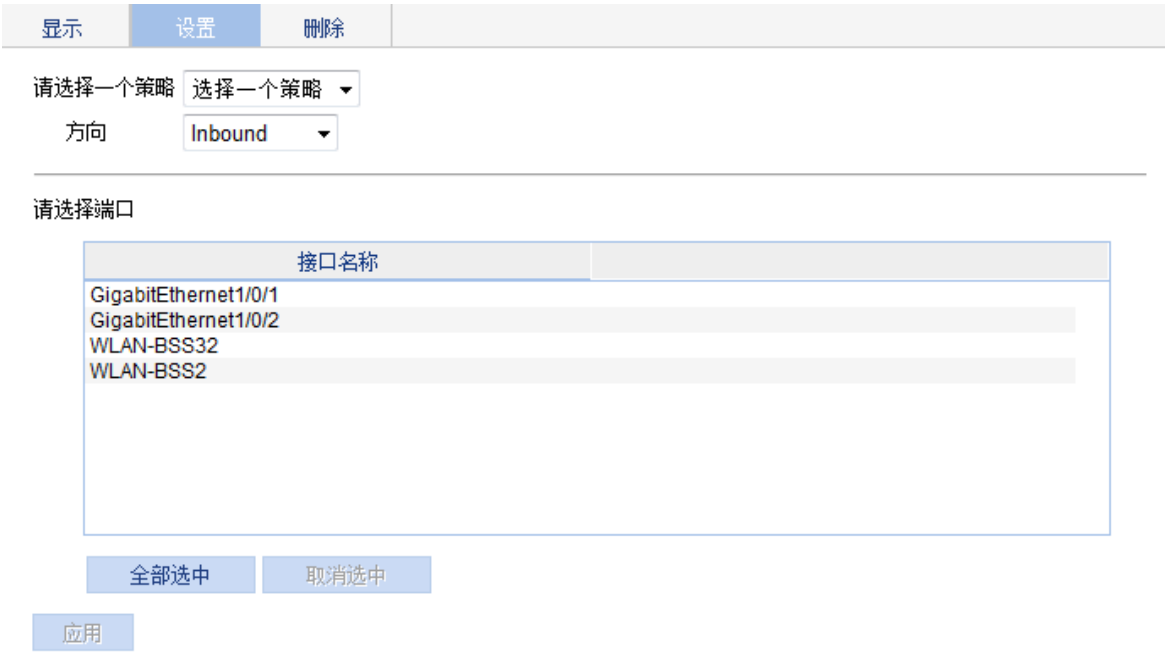
配置项	说明
请选择一个策略	在下拉框中选择一个已存在的策略名
类名称	在下拉框中选择一个已存在的类名称
流行为名称	在下拉框中选择一个已存在的流行为名称

1.3.8 在端口上应用策略

(1) 在导航栏中选择“QoS > 端口策略”。

(2) 单击“设置”页签，进入端口策略的设置页面，如下图所示。

图1-15 端口策略



(3) 配置在端口上应用策略，详细配置如下表所示。

(4) 单击<应用>按钮完成操作。

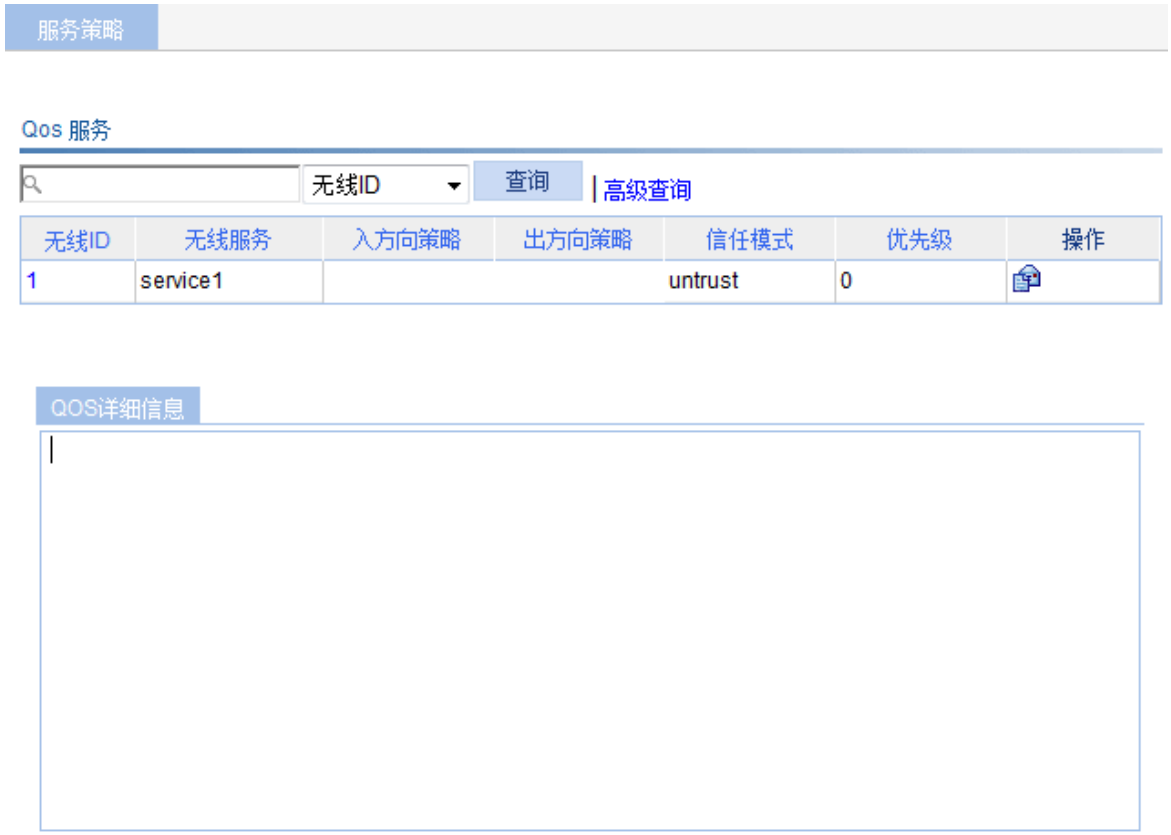
表1-20 在端口上应用策略的详细配置

配置项	说明
请选择一个策略	在下拉框中选择一个已存在的策略名
方向	设置应用QoS策略的方向 • Inbound：表示对端口接收到的报文应用 QoS 策略 • Outbound：表示对端口发送的报文应用 QoS 策略
请选择端口	设置要应用该QoS策略的端口 在端口列表选择框中点击进行选择，可以选择一个或多个端口

1.3.9 在无线服务上应用策略

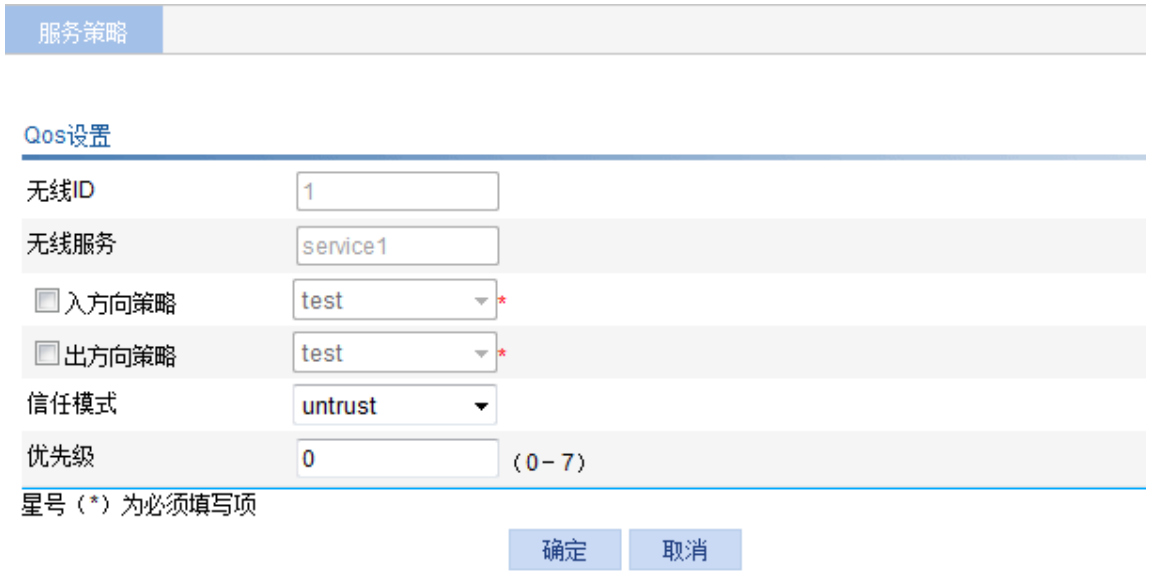
(1) 在导航栏中选择“QoS > 服务策略”，进入服务策略的设置页面，如下图所示。

图1-16 服务策略



(2) 单击无线服务对应的图标，进入如下图所示服务策略的设置页面。

图1-17 服务策略设置



(3) 配置在无线服务上应用策略，详细配置如下表所示。

(4) 单击<确定>按钮完成操作。

表1-21 在无线服务上应用策略的详细配置

配置项	说明
无线ID	显示无线服务的ID
无线服务	显示要应用QoS策略的无线服务
入方向策略	设置入方向上应用的QoS策略，表示对无线服务接收到的报文应用该QoS策略
出方向策略	设置出方向上应用的QoS策略，表示对无线服务发送的报文应用该QoS策略
信任模式	设置优先级信任模式 • Untrust：不信任报文的优先级 • dscp：信任报文自带的 DSCP 优先级，以此优先级进行优先级映射 • 802.11e：信任 802.11 报文携带的 dot11e 优先级，以此优先级进行优先级映射
优先级	设置本地优先级值

1.4 配置信任模式

报文在进入设备以后，设备会根据自身情况和相应规则（primap、remark）分配或修改报文的各种优先级的值，为队列调度和拥塞控制服务。

优先级映射功能通过报文所携带的优先级字段来映射其他优先级字段值，就可以获得各种用以决定报文调度能力的各种优先级字段，从而可以全面有效的控制报文的转发调度能力。

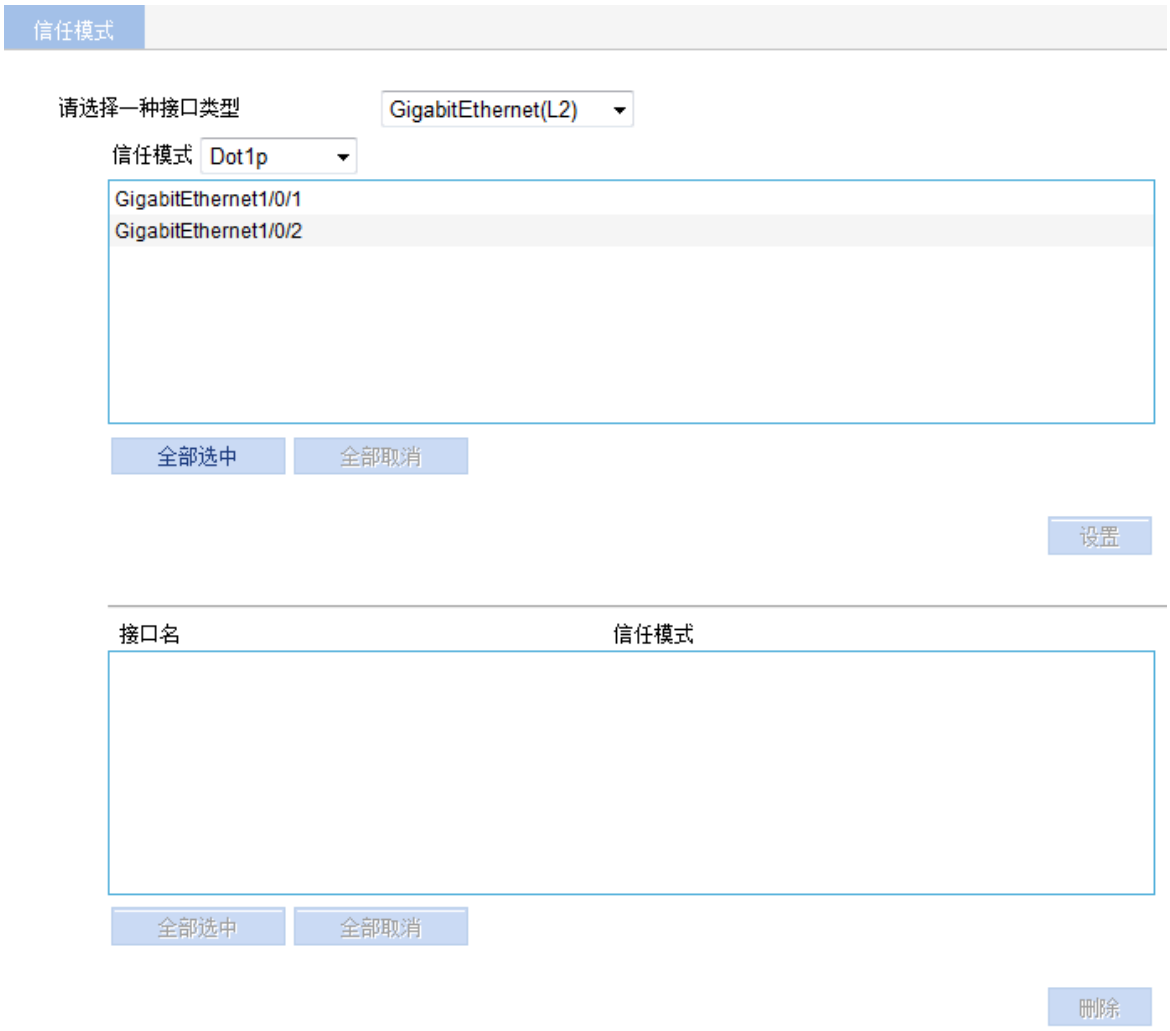
设备提供了多张优先级映射表，分别对应相应的优先级映射关系，可以通过查找缺省优先级映射表来为报文分配相应的优先级。

可以通过配置信任模式来实现优先级映射功能。如果配置了信任模式，即表示设备信任当前进来流量的报文优先级，会自动解析报文的优先级或者标志位，然后按照映射表映射到报文的优先级字段。需要注意的是，如果接收到的报文中没有携带指定的优先级，则用端口优先级字段，按照映射表映射到报文的优先级字段。

1.4.1 配置信任模式

(1) 在导航栏中选择“QoS > 信任模式”，进入信任模式设置页面，如下图所示。

图1-18 信任模式



(2) 配置信任模式，详细配置如下表所示。

(3) 单击<设置>按钮完成操作。

表1-22 端口优先级信任模式的详细配置

配置项	说明
请选择一种接口类型	设置待配置接口的类型 可选的接口类型请以设备的实际情况为准

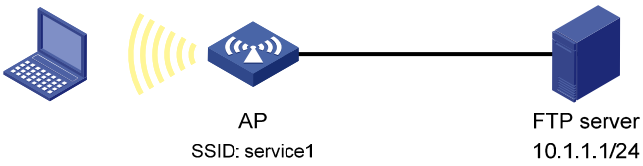
配置项	说明
信任模式	设置接口的优先级信任模式 • Dot1p：信任报文自带的 802.1p 优先级，以此优先级进行优先级映射 • Dscp：信任 IP 报文自带的 DSCP，以此优先级进行优先级映射 • Dot11e：信任 802.11 报文携带的 dot11e 优先级，以此优先级进行优先级映射。此选项只在接口类型为 WLAN-BSS 时显示 提示 不同的接口类型支持的信任模式不相同，请以信任模式下拉菜单中实际显示的优先级信任模式为准
选择接口	设置要配置端口优先级信任模式的接口名 列表选择框中为指定接口类型的端口列表，在其中点击进行选择，可以选择一个或多个接口

1.5 ACL和QoS典型配置举例

1. 组网需求

- 如下图所示，无线网络中 AP 与 FTP 服务器（IP 地址为 10.1.1.1/24）相连，无线用户通过名为 service1 的 SSID 接入无线网络。
- 要求正确配置 ACL 和 QoS 策略，禁止无线用户在每天的 8:00～18:00 访问 FTP 服务器。

图1-19 ACL 和 QoS 配置组网图



2. 配置思路

采用如下思路进行配置：

(1) 配置限制用户在每天的 8:00～18:00 访问 FTP 服务器的 ACL 规则。

(2) 配置 QoS 策略为：匹配该 ACL 规则的类，采取丢弃数据包的动作。

(3) 在无线服务 service1 的入方向上应用该 QoS 策略。

3. 配置步骤

说明

进行下面的配置前，假设 AP 上已经配置了无线服务 service1。无线服务的详细配置请参见“无线服务”。

(1) 定义每天 8:00 至 18:00 的周期时间段。

步骤 1：在导航栏中选择“QoS > 时间段”。

步骤 2：单击“新建”页签。

步骤 3：进行如下配置，如下图所示。

- 输入时间段名称为“test-time”。
- 选中“周期时间段”前的复选框。
- 设置开始时间为“8:0”，结束时间为“18:0”。
- 选中“星期日”～“星期六”前的复选框。

步骤 4：单击<应用>按钮完成操作。

图1-20 定义每天 8:00 至 18:00 的周期时间段



(2) 新建高级 IPv4 ACL。

步骤 1：在导航栏中选择“QoS > ACL IPv4”。

步骤 2：单击“新建”页签。

步骤 3：如下图所示，输入访问控制列表 ID 为“3000”。

步骤 4：单击<应用>按钮完成操作。

图1-21 新建高级 IPv4 ACL



(3) 配置到 FTP 服务器的访问规则。

步骤 1：单击“高级配置”页签。

步骤 2：进行如下配置，如下图所示。

- 选择访问控制列表为“3000”。
- 选中“规则 ID”前的复选框，输入规则 ID 为“2”。
- 选择操作为“允许”。
- 选中“目的 IP 地址”前的复选框，输入目的 IP 地址为“10.1.1.1”，输入目的地址通配符为“0.0.0.0”。
- 选择时间段为“test-time”。

步骤 3：单击<新建>按钮完成操作。

图1-22 配置到 FTP 服务器的访问规则



(4) 新建类。

步骤 1：在导航栏中选择“QoS > 类”。

步骤 2：单击“新建”页签。

步骤 3：如下图所示，输入类名称为“class1”。

步骤 4：单击<新建>按钮完成操作。

图1-23 新建类



(5) 配置分类规则。

步骤 1：单击“设置”页签。

步骤 2：进行如下配置，如下图所示。

- 选择类名称为“class1”。
- 选中“ACL IPv4”前的复选框，选择访问控制列表 ID 为“3000”。

步骤 3：单击<应用>按钮，弹出配置进度对话框。

步骤 4：看到配置成功的提示后，在对话框中单击<关闭>按钮完成操作。

图1-24 配置分类规则



(6) 新建流行为。

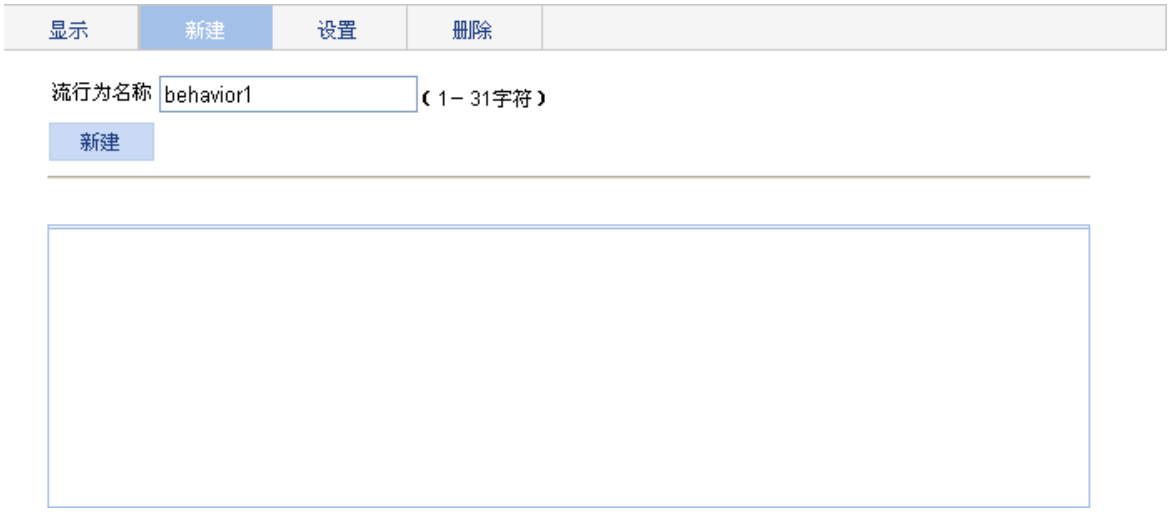
步骤 1：在导航栏中选择“QoS > 流行为”。

步骤 2：单击“新建”页签。

步骤 3：如下图所示，输入流行为名称为“behavior1”。

步骤 4：单击<新建>按钮完成操作。

图1-25 新建流行为



(7) 配置流行为的动作。

步骤 1：单击“设置”页签。

步骤 2：进行如下配置，如下图所示。

- 选择流行为为“behavior1”。
- 选中“包过滤”前的复选框，选择行为为“Deny”。

步骤 3：单击<应用>按钮，弹出配置进度对话框。

步骤 4：看到配置成功的提示后，在对话框中单击<关闭>按钮完成操作。

图1-26 配置流行为的动作



(8) 新建策略。

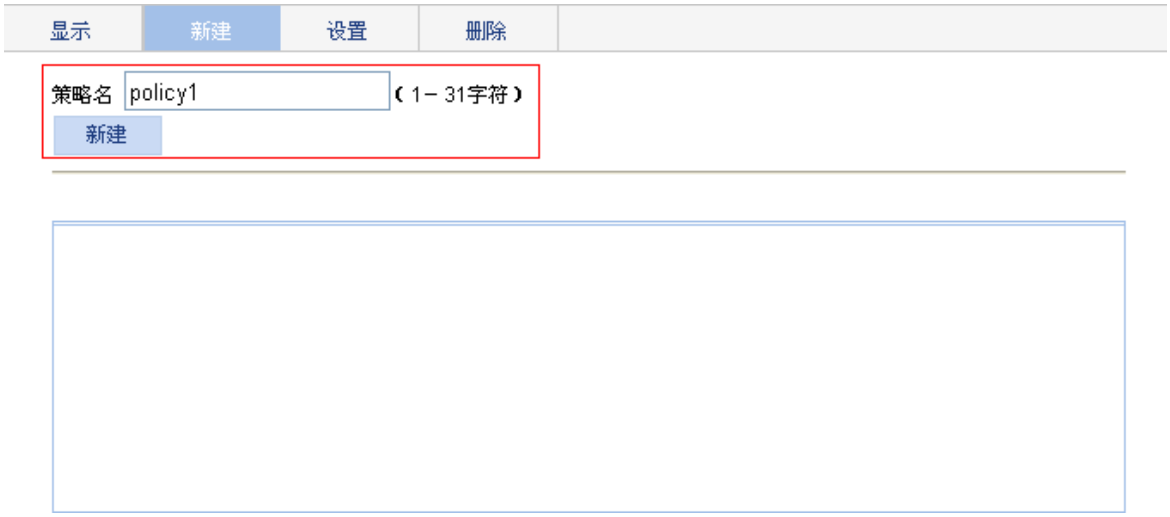
步骤 1：在导航栏中选择“QoS > QoS Policy”。

步骤 2：单击“新建”页签。

步骤 3：如下图所示，输入策略名为“policy1”。

步骤 4：单击<新建>按钮完成操作。

图1-27 新建策略



(9) 配置策略中类和流行为的对应关系。

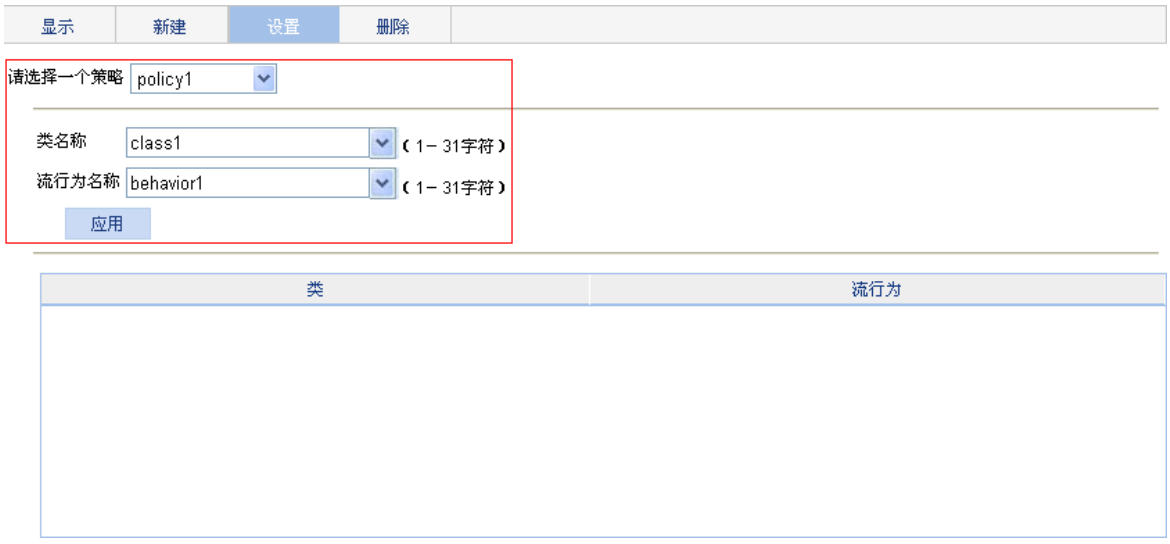
步骤 1：单击“设置”页签。

步骤 2：进行如下配置，如下图所示。

- 选择策略为“policy1”。
- 选择类名称为“class1”。
- 选择流行为名称为“behavior1”。

步骤 3：单击<应用>按钮完成操作。

图1-28 配置策略中类和流行为的对应关系



(10) 在无线服务 service1 的入方向上应用 QoS 策略。

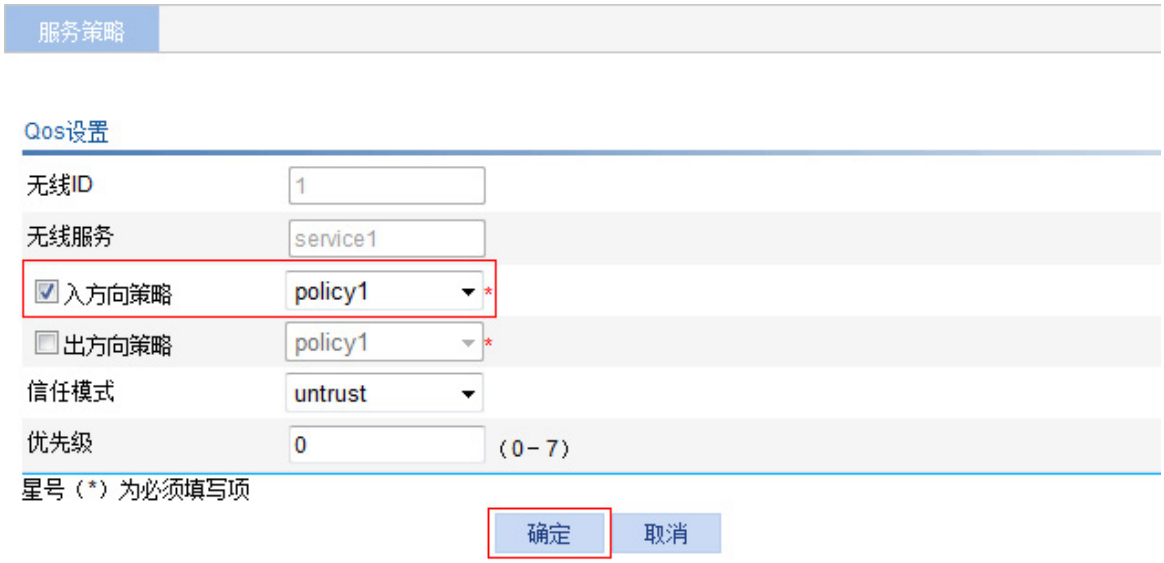
步骤 1：在导航栏中选择“QoS > 服务策略”。

步骤 2：单击无线服务 service1 对应的 图标。

步骤 3：如下图所示，选中“入方向策略”前的复选框，选择 QoS 策略为“policy1”。

步骤 4：单击<确定>按钮完成操作。

图1-29 在无线服务 service1 的入方向上应用 QoS 策略



4. 配置结果验证

完成上述配置后，QoS 策略被成功的应用到无线服务 service1，无线用户在每天的 8:00～18:00 无法访问 IP 地址为 10.1.1.1/24 的 FTP 服务器，其他时间可以访问。

1.6 注意事项

配置 ACL 和 QoS 时，需要注意如下事项：

(1) 新建或修改后的 ACL 规则不能和已经存在的规则相同，否则会导致新建或修改不成功，系统会提示这条规则已经存在。

(2) 当 ACL 的匹配顺序为“用户配置”时，用户可以修改该 ACL 中的任何一条已经存在的规则，在修改 ACL 中的某条规则时，该规则中没有修改到的部分仍旧保持原来的状态；当 ACL 的匹配顺序为“自动”时，用户不能修改该 ACL 中的任何一条已经存在的规则，否则系统会提示错误信息。

(3) 配置端口限速和流行为中的流量监管时，所配置的 CBS 值与 CIR 值的比例如果小于 100:16，则可能会影响对突发流量的处理效果。

(4) 如果 QoS 策略在定义流分类规则时引用了 ACL，则 QoS 策略应用在不同接口上的处理过程不同。设备上哪些接口是软件口、哪些接口是硬件口，请以设备的实际情况为准。具体处理过程如下：

- 若 QoS 策略应用到软件口上，当分类规则中引用的 ACL 规则的操作为禁止时，则跳出该分类规则，继续进行后续规则的查找。
- 若 QoS 策略应用到硬件口上，则忽略 ACL 规则的操作，以流行为中定义的动作为准，报文匹配只使用 ACL 中的分类域。

(5) 如果 QoS 策略应用在端口的出方向，则 QoS 策略对本地协议报文不起作用。（本地协议报文的含义及其作用如下：某些内部发起的报文是维持设备正常运行的重要的协议报文，为了确保这些报文能够被不受影响的发送出去，遂将其定义为本地协议报文，使得 QoS 不对其进行处理，降低了因配置 QoS 而误将这些报文丢弃或进行其他处理的风险。

2 无线服务质量配置

2.1 无线服务质量简介

802.11 网络提供基于 CSMA/CA（Carrier Sense Multiple Access with Collision Avoidance，载波监听/冲突避免）信道竞争机制的无线接入服务，接入 WLAN 网络的所有客户端享有公平的信道竞争机会，承载在 WLAN 上的所有业务使用相同的信道竞争参数。但实际应用中，不同的业务在带宽、时延、抖动等方面的要求往往不同，需要 WLAN 网能根据承载业务提供有区分的接入服务。

IEEE 802.11e 为基于 802.11 协议的 WLAN 体系添加了 QoS 特性，在 IEEE 802.11e 标准化之前，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。

2.1.1 常见术语

(1) 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服务质量。

(2) 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。

(3) AC

AC（Access Category，接入类），WMM 将 WLAN 数据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）四个接入类，每个接入类使用独立的优先级队列发送数据。WMM 保证越高优先级队列中的报文，抢占信道的能力越强。

(4) CAC

CAC（Connect Admission Control，连接准入控制），限制能使用高优先级队列（AC-VO 和 AC-VI 队列）的客户端个数，从而保证已经使用高优先级队列的客户端能够有足够的带宽保证。

(5) 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。

(6) SVP

SVP（SpectraLink Voice Priority，SpectraLink 语音优先级）是 SpectraLink 公司为向语音通话提供 QoS 保障而设计的语音优先协议。

2.1.2 WMM协议概述

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 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。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，所以整个网络设备的信道竞争机会相同。

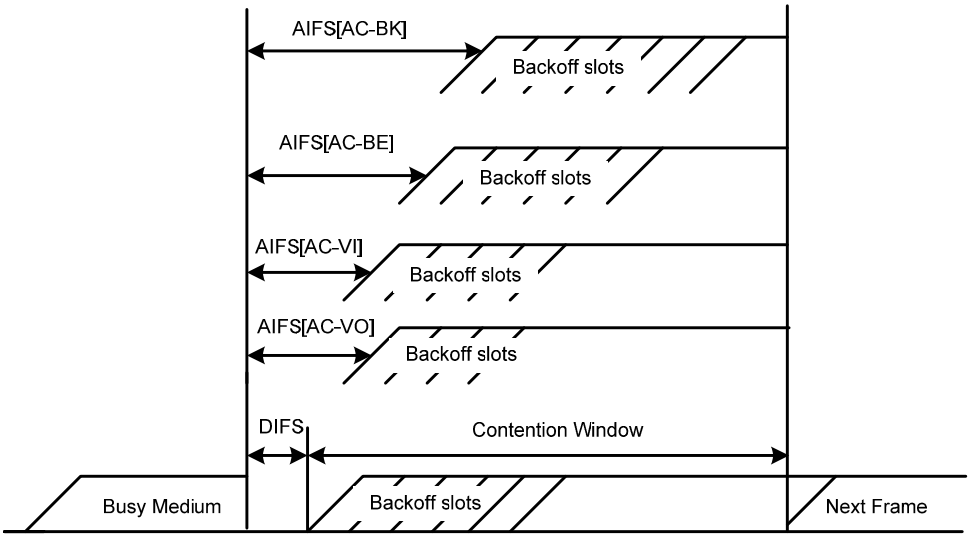
1. EDCA参数

WMM 协议通过对 802.11 协议的增强，改变了整个网络完全公平的竞争方式，将数据报文分为 4 个 AC，高优先级的 AC 占用信道的机会大于低优先级的 AC，从而使不同的 AC 能获得不同级别的服务。

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 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，为下图中 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，为下图中 Backoff slots 时间段；
- TXOPLimit（Transmission Opportunity Limit，传输机会限制），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。

图2-1 WMM 对每个 AC 赋予不同的信道竞争参数



2. CAC准入策略

CAC 的基本原理是客户端只有获得 AP 的批准，才能以高优先级的 AC 发送数据，否则只能使用低优先级的 AC，保证了已经获得批准的客户端能够获得需要的带宽。这里将各种传输报文分为两类：实时业务流（需要 CAC 控制的流，包括 AC-VO 和 AC-VI）和普通数据流（不需要 CAC 控制的流，包括 AC-BE 和 AC-BK）。

如果客户端需要使用高优先级的 AC，则需要进行请求，AP 按照如下介绍的算法，计算是否允许客户端使用，并将结果回应给客户端。

- 基于信道利用率的准入策略：计算 1 秒内所有已接入的高优先级 AC 占用信道的时间，以及请求以高优先级接入的 AC 占用信道的时间，二者相加，如果小于或等于用户配置的最大信道占用时间，则允许该流以请求的优先级接入。否则，拒绝请求。
- 基于用户数量的准入策略：如果高优先级 AC 中客户端数量加上请求接入的客户端，小于或等于用户配置的该高优先级 AC 的最大用户数，则允许该流的请求。否则，拒绝请求。如果一个客户端同时接入 AC-VO 和 AC-VI 优先级业务流，接入客户端的个数按 1 计算。

3. U-APSD节能模式

U-APSD 是对原有节能模式的改进。客户端在关联时可以指定某些 AC 具有触发属性，某些 AC 具有发送属性，以及触发后最多允许发送的数据报文数量。触发和发送属性还可以在通过连接准入控制创建流的时候进行更改。客户端休眠后，发往客户端的属于具有发送属性 AC 的数据报文将被缓存在发送缓存队列中，客户端需要发送属于具有触发属性 AC 的报文以获取发送缓存队列中的报文。AP 收到触发报文后，按照接入时确定的发送报文数量，发送属于发送队列的报文。没有发送属性的 AC 仍然使用 802.11 定义的传统方式存储和传送。

4. SVP服务

SVP 服务实现对 SVP 报文（即 IP 协议号为 119）的区别处理，将 SVP 报文映射为指定的接入类，放入指定的发送队列中。

5. ACK策略

协议规定 ACK 策略有两种：Normal ACK 和 No ACK。

- No ACK（No Acknowledgment）策略是在无线报文传输过程中，不使用 ACK 报文进行接收确认的一种策略。No ACK 策略可以用于通信环境较好，干扰较小的应用场合，可以有效提高传输效率。但是如果在通信环境较差的场合使用 No ACK 策略，报文的发送方将不会对丢包进行重发，将导致丢包率增大的问题，反而导致整体性能的下降。
- Normal ACK 策略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 ACK 进行确认。

2.2 配置无线服务质量

2.2.1 开启无线服务质量

(1) 在界面左侧的导航栏中选择“QoS > 无线服务质量”，默认进入“服务质量设置”页签的页面，如下图所示。

图2-2 无线服务质量



(2) 在列表中找到要进行配置的射频单元，选中其前面的复选框。

(3) 单击<开启>按钮完成操作。缺省情况下，无线服务质量处于开启状态。

说明

WMM 协议是 802.11n 和 802.11ac 协议所依赖的基础，所以当 Radio 工作在 802.11n(5GHz)、802.11n(2.4GHz)或 802.11ac(5GHz)射频模式时，WMM 功能必须处于开启状态，否则可能会导致所关联的客户端无法正常通信。

2.2.2 SVP服务设置

(1) 在界面左侧的导航栏中选择“QoS > 无线服务质量”，默认进入“服务质量设置”页签的页面，如下图所示。

图2-3 无线服务质量



(2) 在列表中选择要进行配置的射频单元，单击对应的图标，进入服务质量设置的配置页面，如下图所示。

图2-4 SVP 映射接入类设置



(3) 配置 SVP 映射接入类，详细配置如下表所示。

(4) 单击<确定>按钮完成操作。

表2-1 SVP 映射接入类的详细配置

配置项	说明
射频单元	显示选中的射频单元

配置项	说明
SVP报文映射	选中SVP报文映射前的复选框，选择SVP服务使用的映射接入类 • AC-VO：AC-VO（语音流）接入类 • AC-VI：AC-VI（视频流）接入类 • AC-BE：AC-BE（尽力而为流）接入类 • AC-BK：AC-BK（背景流）接入类

说明

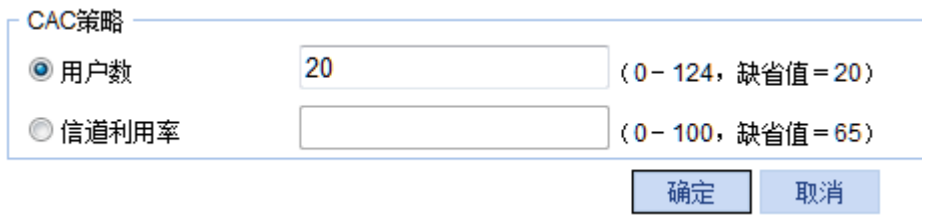
SVP 映射只针对非 WMM 客户端接入，对 WMM 客户端不起作用。

2.2.3 CAC准入控制策略设置

(1) 在界面左侧的导航栏中选择“QoS > 无线服务质量”，默认进入“服务质量设置”页签的页面。

(2) 在列表中找到要进行配置的射频单元，单击对应的图标，进入服务质量设置的配置页面，如下图所示。

图2-5 CAC 准入控制策略设置



(3) 配置 CAC 准入控制策略，详细配置如下表所示。

(4) 单击<确定>按钮完成操作。

表2-2 CAC 准入控制策略的详细配置

配置项	说明
用户数	基于用户数的准入策略 即允许接入的客户端的最大个数，如果一个客户端同时接入AC-VO和AC-VI优先级业务流，接入客户端的个数按1计算 缺省情况下，CAC策略是基于用户数的准入策略，用户数为20
信道利用率	基于信道利用率的准入策略 即单位时间内，允许接入AC-VO和AC-VI优先级的业务流占用信道的有效时间与总共时间的百分比，有效时间为用于实际收发数据的时间

2.2.4 射频EDCA设置

射频 EDCA 参数设置完成对 AP 使用的 EDCA 参数的配置。

(1) 在界面左侧的导航栏中选择“QoS > 无线服务质量”，默认进入“服务质量设置”页签的页面。

(2) 在列表中选择要进行配置的射频单元，单击对应的图标，进入服务质量设置的配置页面。

(3) 在“射频 EDCA”列表中找到要进行修改的优先级类型（这里以 AC_BK 优先级为例），单击对应的图标，进入射频 EDCA 参数的配置页面，如下图所示。

图2-6 射频 EDCA 设置



(4) 配置射频 EDCA 参数，详细配置如下表所示。

(5) 单击<确定>按钮完成操作。

表2-3 射频 EDCA 设置的详细配置

配置项	说明
射频单元	显示选中的AP射频单元
优先级类型	显示进行配置的优先级类型
AIFSN	AP采用的仲裁帧间隙数
TXOP Limit	AP采用的传输机会限制
ECWmin	AP采用的最小竞争窗口指数
ECWmax	AP采用的最大竞争窗口指数
No ACK	选中“No ACK”前的复选框，表示AP采取No ACK（No Acknowledgment）策略 缺省情况下，ACK策略为Normal ACK

射频 EDCA 参数的缺省情况请参见下表。

表2-4 AP 使用的 EDCA 参数的缺省值

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

说明

- ECWmin 的值不能大于 ECWmax。
- AP 选择 802.11b 射频模式时，建议将 AC-BK、AC-BE、AC-VI、AC-VO 的 TXOP-Limit 参数的值分别配置为 0、0、188、102。

2.2.5 用户EDCA设置

用户 EDCA 参数设置完成对接入无线客户端使用的 EDCA 参数的配置。

(1) 在界面左侧的导航栏中选择“QoS > 无线服务质量”，默认进入“服务质量设置”页签的页面。

(2) 在列表中选择要进行配置的射频单元，单击对应的图标，进入服务质量设置的配置页面。

(3) 在“用户 EDCA”列表中选择要进行修改的优先级类型（这里以 AC_BK 优先级为例），单击对应的图标，进入用户 EDCA 参数的配置页面，如下图所示。

图2-7 用户 EDCA 设置



(4) 配置用户 EDCA 参数，详细配置如下表所示。

(5) 单击<确定>按钮完成操作。

表2-5 用户 EDCA 设置的详细配置

配置项	说明
射频单元	显示选中的AP射频单元
优先级类型	显示进行配置的优先级类型
AIFSN	客户端采用的仲裁帧间隙数
TXOP Limit	客户端采用的传输机会限制
ECWmin	客户端采用的最小竞争窗口指数
ECWmax	客户端采用的最大竞争窗口指数

配置项	说明
CAC	客户端使用连接准入控制 • 开启：使用连接准入控制 • 关闭：禁止连接准入控制 AC-VO和AC-VI支持CAC，缺省情况下，CAC处于关闭状态。 AC-BE和AC-BK不支持CAC功能，不可配置该选项

用户 EDCA 参数的缺省情况请参见下表。

表2-6 用户 EDCA 参数的缺省值

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

说明

- ECWmin 的值不能大于 ECWmax。
- 如果所有客户端应用 802.11b 射频模式，建议将 AC-VI、AC-VO 的 TXOP Limit 参数的值分别配置为 188、102。
- 如果网络中既有使用 802.11b射频卡又有使用 802.11g射频卡的客户端，则建议按TXOP Limit参数值使用 表 2-6 中缺省值。
- 如果某优先级队列的 CAC 功能被启动，则高于此优先级队列的 CAC 功能会同时被启用。例如，启动 AC-VI 优先级 CAC 功能，则 AC-VO 优先级也同时启动 CAC 功能，但是，启动 AC-VO 优先级的 CAC 功能，AC-VI 优先级的 CAC 功能不会被启用。

2.2.6 显示射频信息

(1) 在界面左侧的导航栏中选择“QoS > 无线服务质量”。

(2) 选择“射频信息”页签，进入射频信息的显示页面。

(3) 点击指定的射频单元后，可以查看相关的详细信息，如下图所示。显示信息各字段的说明如下表所示。

图2-8 显示射频信息

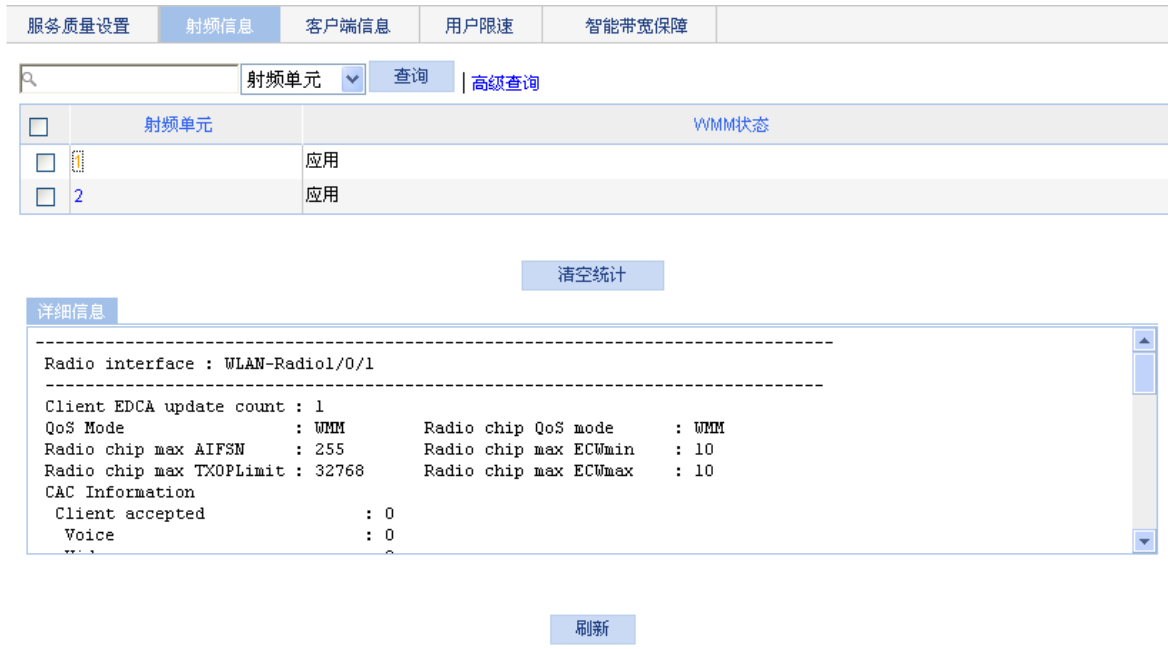


表2-7 射频显示信息描述表

字段	描述
Radio interface	WLAN射频接口
Client EDCA update count	客户端EDCA参数更新次数
QoS mode	QoS模式，WMM：启用QoS模式，None：不启用QoS模式
Radio chip QoS mode	射频芯片是否支持QoS模式
Radio chip max AIFSN	射频芯片支持的AIFSN值的最大值
Radio chip max ECWmin	射频芯片支持的ECWmin值的最大值
Radio chip max TXOPLimit	射频芯片支持的TXOPLimit值的最大值
Radio chip max ECWmax	射频芯片支持的ECWmax值的最大值
Client accepted	Radio下已准入的Client数量，包括Voice队列下和Video队列下准入的Client数量
Total request mediumtime(us)	所有队列申请的时间，包括Voice队列下和Video队列下申请的时间
Calls rejected due to insufficient resource	因资源不足拒绝的请求数量
Calls rejected due to invalid parameters	因参数无效拒绝的请求数量
Calls rejected due to invalid mediumtime	因接入时间无效拒绝的请求数量
Calls rejected due to invalid delaybound	因延迟时间无效拒绝的请求数量
Admission Control Policy	准入控制策略
Threshold users count	准入控制策略使用的门限值

字段	描述
CAC-Free's AC Request Policy	对没有开启CAC功能的AC采用的回应策略 Response Success表示回应成功
CAC Unauthed Frame Policy	对CAC未授权报文的处理策略： • Discard 表示丢弃报文 • Downgrade 表示将报文的优先级降低处理 • Disassociate 表示将断开与客户端的连接
CAC Medium Time Limitation(us)	CAC策略允许的接入时间上限，单位为微秒
CAC AC-VO's Max Delay(us)	CAC策略允许的语音流延迟上限，单位为微秒
CAC AC-VI's Max Delay(us)	CAC策略允许的视频流延迟上限，单位为微秒
SVP packet mapped AC number	SVP报文映射到的AC的编号
ECWmin	ECWmin的值
ECWmax	ECWmax的值
AIFSN	AIFSN的值
TXOPLimit	TXOP limit的值
AckPolicy	设备使用的ACK策略
CAC	表示此队列是否受CAC的限制，Disabled表示不受限制，Enabled表示受限制

2.2.7 显示客户端信息

(1) 在界面左侧的导航栏中选择“QoS > 无线服务质量”。

(2) 选择“客户端信息”页签，进入客户端信息的显示页面。

(3) 点击指定的客户端后，可以查看相关的详细信息，如下图所示。显示信息各字段的说明如下表所示。

图2-9 显示客户端信息



表2-8 客户端显示信息描述表

字段	描述
MAC address	Client的MAC地址
SSID	SSID名
QoS Mode	QoS模式： • WMM：QoS 客户端 • None：非 QoS 客户端
Max SP length	最大服务时间长度
AC	接入队列
State	AC队列的APSD属性 • T 表示本 AC 有 trigger-enabled 属性 • D 表示本 AC 有 delivery-enabled 属性 • T | D 表示上面的两个属性都有 • L 表示本 AC 有 Legacy 属性
Assoc State	Client接入时指定的AC的APSD属性
Uplink CAC packets	上行CAC的报文数
Uplink CAC bytes	上行CAC的字节数
Downlink CAC packets	下行CAC的报文数
Downlink CAC bytes	下行CAC的字节数

字段	描述
Downgrade packets	降级处理的报文数
Downgrade bytes	降级处理的字节数
Discard packets	丢弃处理的报文数
Discard bytes	丢弃处理的字节数

2.3 配置限速

WLAN 网络中每一个 AP 可提供的可用带宽有限，且由接入的无线客户端共享，部分客户端占用过多带宽，势必导致其他客户端使用受到影响。通过配置用户限速功能，可以限制部分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。基于客户端的速率限制功能有两种模式：

- 动态模式：配置同一 BSS 下所有接入客户端可共享的总带宽，每个客户端的限制速率是配置速率值/客户端数量。例如，配置 10Mbps 速率，有 5 个用户上线，则每个用户的可用带宽限制为 2Mbps。
- 静态模式。配置同一 BSS 下每个客户端限制使用的最大带宽。例如，配置 1Mbps 速率，则每个上线的客户端的可用带宽限制为 1Mbps。接入客户端数增加至一定数量时，如果所有接入客户端理论允许的总带宽超出 AP 可提供的有效带宽，那么每个客户端将不能保证获得的指定带宽。

(1) 在界面左侧的导航栏中选择“QoS > 无线服务质量”。

(2) 选择“用户限速”页签，进入用户限速的配置页面。

(3) 在列表中选择要进行配置的无线服务，单击对应的图标，进入用户限速设置的配置页面。

图2-10 用户限速



(4) 配置用户限速，详细配置如下表所示。

(5) 单击<确定>按钮完成操作。

表2-9 用户限速的详细配置

配置项	说明
无线ID	显示无线服务的ID信息
无线服务	显示已有的无线服务

配置项	说明
方向	包括入方向和出方向 • 入方向：从客户端到 AP • 出方向：从 AP 到客户端
模式	模式，包括动态和静态两种模式 • 静态模式：所有客户端的限速值为固定值 • 动态模式：所有客户端的限速值为共享速率/客户端总数
速率	• 选择静态模式时，显示固定速率，表示设置的速率值为每个客户端的带宽 • 选择动态模式时，显示共享速率，表示设置的速率值为所有客户端的总带宽

2.4 配置智能带宽保障

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。当某一个 BSS 的流量非常大时，会挤占其它 BSS 的可用带宽。如果简单地对某个 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。

在这种情况下，可以开启智能带宽保障功能，在流量未拥塞时，确保所有 BSS 的报文都可以通过；在流量拥塞时，确保每个 BSS 可以保证各自配置的保障带宽。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，SSID 1、SSID 2 及 SSID 3 分别配置保障带宽为 25%、25%及 50%。当网络空闲时，SSID1 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 至少可以占有其自己的保障带宽部分（25%）。

说明

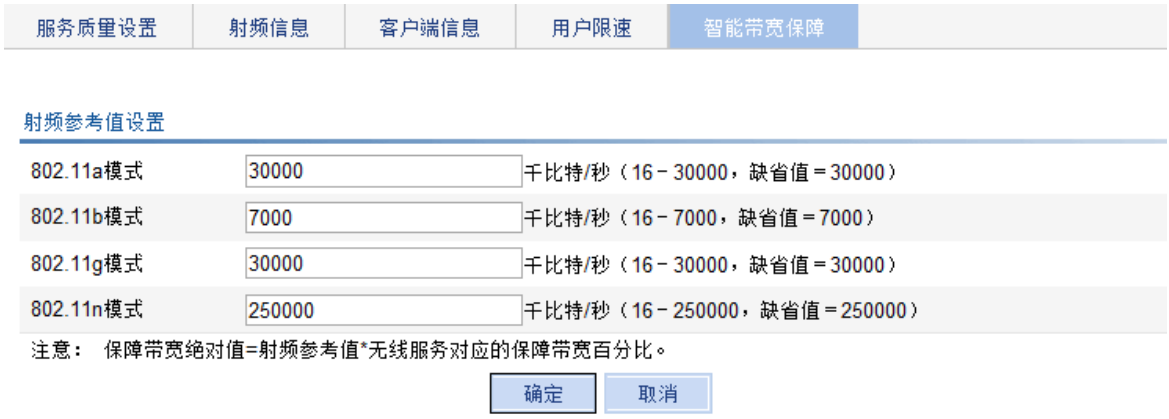
- 保障带宽仅对 AP 到客户端方向上的流量生效。
- 802.11ac 模式下，不支持智能带宽保障功能。

1. 设置射频参考值

(1) 在导航栏中选择“QoS > 无线服务质量”。

(2) 选择“智能带宽保障”页签，进入如下图所示页面。

图2-11 设置射频参考值



(3) 配置射频参考值，详细配置如下表所示。

(4) 单击<确定>按钮完成操作。

表2-10 射频参考值的详细配置

配置项	说明
802.11a模式	射频带宽参考值 **说明** 设置的射频带宽参考值应接近并略小于实际可达的流量上限
802.11b模式	
802.11g模式	
802.11n模式	

说明

修改射频参考值后，对于已经开启智能带宽保障功能的射频，修改的射频参考值不会生效。必须关闭相应的射频，再重新使能射频，修改后的配置才会生效。

2. 设置带宽保障值

(1) 在带宽保障设置列表中选择要进行配置的射频，单击对应的图标，进入带宽设置页面，如下图所示。

图2-12 带宽设置



(2) 配置保障带宽，详细配置如下表所示。

(3) 单击<确定>按钮完成操作。

表2-11 保障带宽的详细配置

配置项	说明
保障带宽(%)	设置无线服务在当前射频上占用的带宽百分比 **说明** 在同一射频上绑定的所有无线服务的保障带宽百分比之和不能超过 100%

3. 开启带宽保障功能

完成设置后，页面自动跳转到智能带宽保障页面，在该页面上需要开启带宽保障功能。

(1) 在列表里选择需要应用带宽保障设置的射频模式，选中前面的复选框。

(2) 单击<开启>按钮完成操作。

图2-13 开启带宽保障



4. 查看带宽信息

(1) 在导航栏中选择“QoS > 无线服务质量”。

(2) 选择“智能带宽保障”页签，进入智能带宽保障配置页面。

(3) 点击指定的射频单元后，可以查看当前射频绑定的无线服务及每个无线服务配置的保障带宽，如下图所示。

图2-14 查看带宽信息



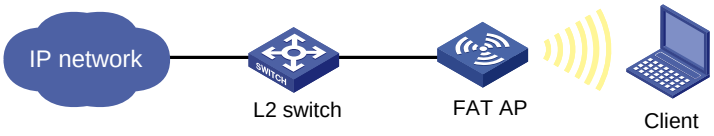
2.5 无线服务质量配置举例

2.5.1 CAC服务典型配置举例

1. 组网需求

无线接入点连接以太网，并启用 WMM 功能。要求使用用户数判断策略，只允许 10 个客户端可以和 AP 建立 AC-VO 和 AC-VI 的业务流，保证使用高优先级 AC-VO 和 AC-VI 队列的客户端能够有足够的带宽保证。

图2-15 CAC 服务组网图



2. 配置步骤

(1) 配置无线服务

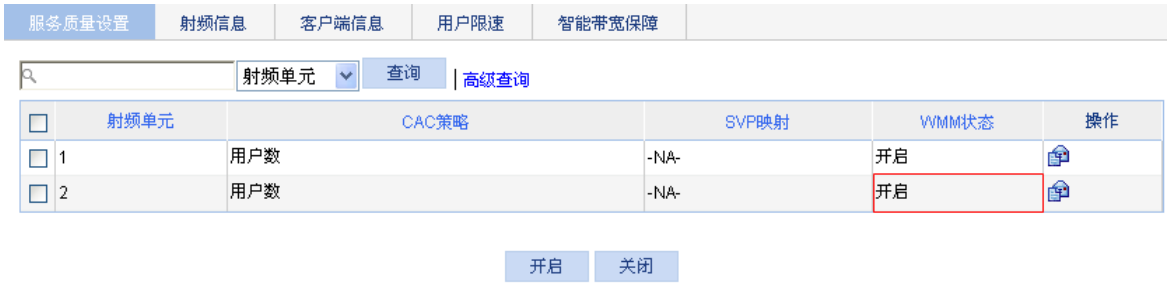
相关配置请参见“无线服务”，可以完全参照相关举例完成配置。

(2) 配置无线服务质量

步骤 1：在界面左侧的导航栏中选择“QoS > 无线服务质量”，进入“服务质量设置”页签的页面。

步骤 2：确认 WMM 状态处于开启状态，如下图所示。

图2-16 无线服务质量



步骤 3：在列表中选择要进行配置的射频单元，单击对应的图标，进入服务质量设置的配置页面。

步骤 4：在“用户 EDCA”列表中选择要进行修改的优先级类型（AC_VO），单击对应的图标。

步骤 5：进入“用户 EDCA”参数设置页面后选择 CAC 功能为“开启”，如下图所示。

步骤 6：单击<确定>按钮完成操作。

图2-17 开启 CAC



步骤 7：使用相同的方法开启 AC_VI 的 CAC 功能，具体过程略。

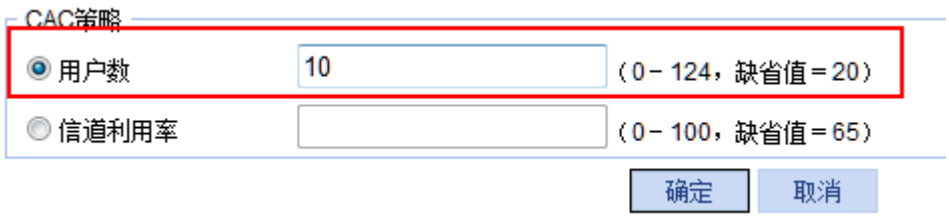
步骤 8：在界面左侧的导航栏中选择“QoS > 无线服务质量”，进入“服务质量设置”页签的页面。

步骤 9：在列表中选择要进行配置的射频单元，单击对应的图标，进入服务质量设置的配置页面。

步骤 10：选中“用户数”前的单选框，输入 10。

步骤 11：单击<确定>按钮完成操作。

图2-18 CAC 用户数配置



3. 验证配置结果

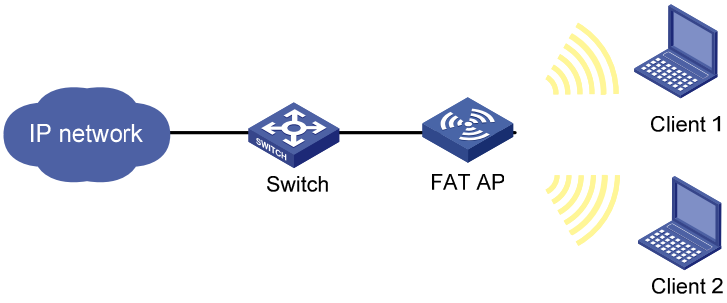
如果 AP 上高优先级 AC 中客户端数量加上请求接入的客户端数量，小于或等于用户配置的高优先级 AC 的最大用户数 10（本例中为 10），则允许用户的请求。对超过最大用户数的客户端发送的报文进行降级处理。

2.5.2 静态限速配置举例

1. 组网需求

两个客户端通过名为 service1 的 SSID 接入无线网络，限定每个客户端从客户端到 AP 的方向上使用的最大带宽为 128kbps。

图2-19 静态限速配置举例组网图



2. 配置步骤

(1) 配置无线服务

相关配置请参见“无线服务”，可以完全参照相关举例完成配置。

(2) 配置静态限速

步骤 1：在界面左侧的导航栏中选择“QoS > 无线服务质量”。

步骤 2：选择“用户限速”页签，进入用户限速页面。

步骤 3：在列表中选择无线服务 service1，单击入方向对应的图标，进入用户限速设置的配置页面。

步骤 4：进行如下配置，如下图所示。

- 模式下拉框中选择“静态”。
- 固定速率中输入 128。

步骤 5：单击<确定>按钮完成操作。

图2-20 配置静态限速



3. 验证配置结果

(1) Client 1 和 Client 2 通过名为 service1 的 SSID 接入无线网络。

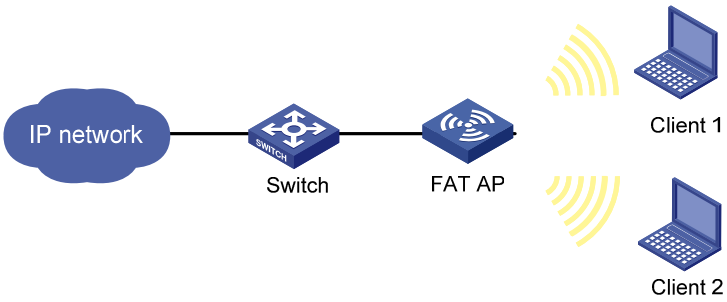
(2) 从 Client 1 侧到 AP 侧方向上的可使用的带宽被限制在 128kbps 左右；从 Client 2 侧到 AP 侧方向上的可使用的带宽也被限制在 128kbps 左右。

2.5.3 动态限速配置举例

1. 组网需求

客户端通过名为 service2 的 SSID 接入无线网络，要求接入的客户端在出方向上都要平等地共享设定的 8000kbps 总带宽。

图2-21 动态限速配置举例组网图



2. 配置步骤

(1) 配置无线服务

相关配置请参见“无线服务”，可以完全参照相关举例完成配置。

(2) 配置动态限速

步骤 1：在界面左侧的导航栏中选择“QoS > 无线服务质量”。

步骤 2：选择“用户限速”页签，进入用户限速页面。

步骤 3：在列表中选择无线服务 service2，单击出方向对应的图标，进入用户限速设置的配置页面。

步骤 4：进行如下配置，如下图所示。

- 模式下拉框中选择“动态”。
- 共享速率中输入 8000。

步骤 5：单击<确定>按钮完成操作。

图2-22 配置动态限速



3. 验证配置结果

(1) 只有 Client 1 通过 service2 接入无线网络，可使用的带宽被限制在 8000kbps 左右。

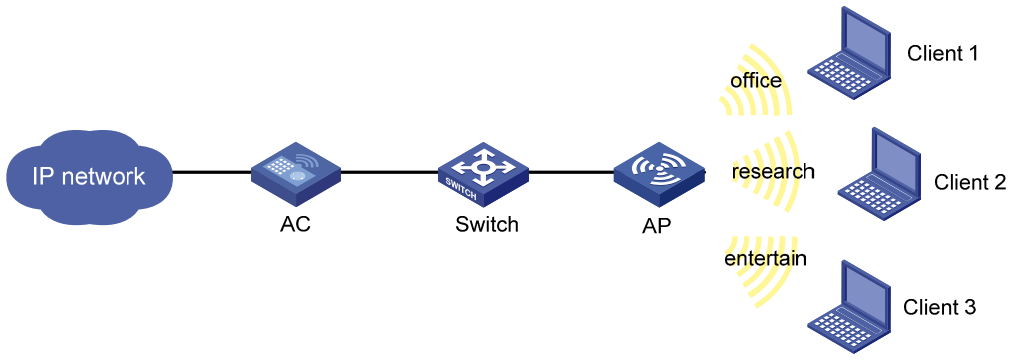
(2) Client 2 也通过 service2 接入无线网络后，Client 1、Client 2 可使用的带宽分别被限制在 4000kbps 左右。

2.5.4 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 office 无线服务的带宽保障为 20%，research 无线服务的带宽保障为 80%，entertain 无线服务没有分配带宽保障。

图2-23 智能带宽保障配置举例组网图



2. 配置步骤

(1) 配置无线服务

相关配置请参见“无线服务”，可以完全参照相关举例完成配置。

(2) 配置智能带宽保障

步骤 1：在界面左侧的导航栏中选择“QoS > 无线服务质量”。

步骤 2：选择“智能带宽保障”页签，进入智能带宽保障配置页面。

步骤 3：802.11n 模式射频参考值使用缺省值“200000”，如下图所示。

步骤 4：单击<确定>按钮完成操作。

图2-24 配置射频参考值



设置带宽保障百分比。

步骤 5：在列表中选择 802.11n 射频，单击对应的图标，进入保障带宽百分比配置页面。

步骤 6：进行如下配置，如下图所示。

- 设置 office 无线服务的保障带宽百分比为“20”。
- 设置 research 无线服务的保障带宽百分比为“80”。
- 设置 entertain 无线服务的保障带宽百分比为“0”。

步骤 7：单击<确定>按钮完成操作。

图2-25 配置带宽保障百分比



步骤 8：返回智能带宽保障配置页面后，选中 802.11n 射频前面的复选框，如下图所示。

步骤 9：单击<开启>按钮完成操作。

图2-26 开启带宽保障



3. 验证配置结果

- 如果 AP 向所有客户端发送的总流量小于 200000kpbs。在这种情况下，AP 向 Client 1～Client 3 实际发送的流量不会受限制。
- 如果 AP 分别向 Client 1 和 Client 2 发送大于 40000kbps 以及 160000kbps 的流量，并且向所有客户端发送的总流量大于 200000kpbs。在这种情况下，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，设备会优先保证 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 40000kbps 以及 160000kbps 左右，向其它数据流（Client 3）发送的流量会受到限制。

4. 注意事项

(1) 保障带宽绝对值根据射频带宽参考值及无线服务百分比相乘计算得出。

(2) 设置的射频带宽参考值应接近并略小于实际可达的流量上限。

(3) 保障带宽仅对 AP 到客户端方向上的流量生效。

目 录

1 高级设置 ····· 1-1
1.1 高级设置简介 ····· 1-1
1.1.1 区域码 ····· 1-1
1.1.2 形态切换 ····· 1-1
1.1.3 常发模式 ····· 1-1
1.1.4 上行链路检测 ····· 1-1
1.1.5 信道利用率 ····· 1-2
1.1.6 频谱导航 ····· 1-2
1.1.7 组播优化功能 ····· 1-2
1.2 无线高级设置 ····· 1-4
1.2.1 设置区域码 ····· 1-4
1.2.2 形态切换 ····· 1-4
1.2.3 常发模式 ····· 1-5
1.2.4 上行链路检测 ····· 1-6
1.2.5 信道利用率 ····· 1-7
1.2.6 配置频谱导航 ····· 1-9
1.2.7 配置组播优化功能 ····· 1-11
1.3 高级设置配置举例 ····· 1-13
1.3.1 频谱导航配置举例 ····· 1-13
1.3.2 组播优化功能配置举例 ····· 1-15

1 高级设置

1.1 高级设置简介

高级设置提供了如下功能：

- 区域码
- 形态切换
- 常发模式
- 上行链路检测
- 信道利用率
- 频谱导航
- 组播优化

1.1.1 区域码

不同国家或地区对射频使用有不同的管制要求，区域码决定了可以使用的工作频段、信道，以及合法的发射功率级别等。在配置 WLAN 设备时，必须正确地设置国家或地区码，以确保不违反当地的管制规定。

1.1.2 形态切换

对于同时支持 Fat 和 Fit 形态的 AP 设备，通过形态切换功能，可以将设备从 Fat AP 切换为 Fit AP。此功能常用于网络扩容时，对于前期采用数量较少的 Fat AP 构建的 WLAN 网络，用户在扩容到较大网络规模后，可以通过将 Fat AP 切换为 Fit AP，便于实施集中管理和控制。

1.1.3 常发模式

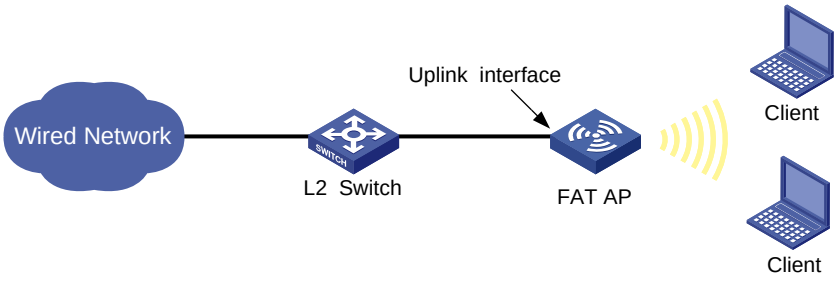
常发模式属于测试专用功能，一旦启用会对正常业务造成影响，建议用户不要使用。

1.1.4 上行链路检测

FAT AP通常需要通过以太网接口接入上行网络，如 图 1-1 所示。如果AP的上行以太网口出现故障，将导致AP及关联到AP的无线客户端无法继续访问上行网络。开启上行链路检测后（上行链路检测设置请参见“1.2.4 上行链路检测”），一旦出现AP的上行链路故障，AP将停止提供无线接入服务，无线客户端将无法搜索到该AP的SSID，直至故障AP上行链路恢复正常工作后，无线客户端将可以重新接入该AP。

上行链接检测功能，保证了在无线客户端所关联的 AP 出现上行链路故障后，在同一区域还有其他正常工作 AP 覆盖的情况下，无线客户端可以通过关联到其他正常工作的 AP 接入上行网络。

图1-1 上行链路检测组网图



1.1.5 信道利用率

信道利用率检测提供了一种评估信道忙闲程度的检测工具。信道利用率检测会对当前区域码所支持的信道进行逐个检测，输出的信道利用率结果可以指导工程人员和用户对信道进行合理选择，避免用户使用负载较高的信道。

在信道利用率检测期间，AP 不能提供任何形式的无线服务，所有已关联的客户端会被强制下线，AP 接收的无线报文也会被直接丢弃。

1.1.6 频谱导航

在实际无线网络环境中，某些客户端只能工作在 2.4GHz 频段上，也有一部分客户端可以同时支持 2.4GHz 和 5GHz 频段，如果支持双频的客户端都工作在 2.4GHz 频段上，会导致 2.4GHz 射频过载，5GHz 射频相对空余。在这种情况下，可以在设备上开启频谱导航功能。频谱导航功能可以将支持双频工作的客户端优先接入 5GHz 射频，使得两个频段上的客户端数量相对均衡，从而提高整网性能。

开启频谱导航功能后，AP 会对发起连接请求的客户端进行导航，将其均衡地连接至该 AP 的不同射频上。首先当客户端与某个 AP 连接时，若该客户端只支持单频 2.4GHz，则 AP 会在拒绝若干次后允许其关联。若客户端支持双频，AP 则会将客户端优先引导至 5GHz 射频上。若客户端只支持单频 5GHz，则会直接关联至 AP 的 5GHz 射频上。在双频客户端关联到 5GHz 射频前，AP 会检查 5GHz 射频接收到的客户端的 RSSI 值，若该 RSSI 值低于设定值，则不会将此客户端导航至 5GHz 射频。

如果 5GHz 射频上已连接的客户端数量达到门限，且 5GHz 射频与 2.4GHz 射频上连接的客户端差达到或超过差值门限，AP 会拒绝客户端接入 5GHz 射频，且允许新客户端接入 2.4GHz 射频（即不会引导双频客户端优先接入 5GHz 射频）。如果客户端反复向该 AP 的 5GHz 射频上发起关联请求，且 AP 拒绝客户端关联请求次数达到/超过设定的最大拒绝关联请求次数，那么该 AP 会认为此时该客户端不能连接到其它任何的 AP，在这种情况下，AP 上的 5GHz 射频也会接受该客户端的关联请求。

1.1.7 组播优化功能

设备在发送无线组播数据报文时，会有如下两个特点。

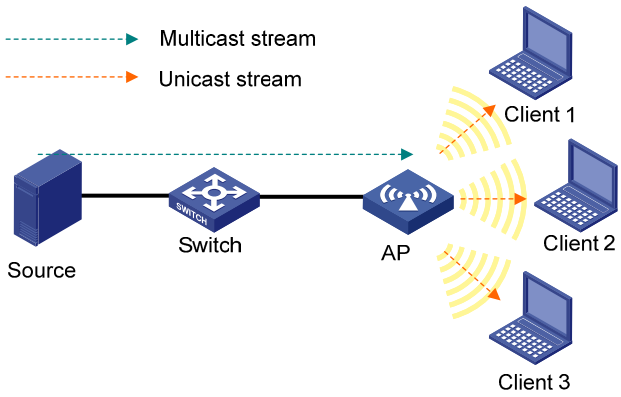
- 没有相应的确认机制，因此无法对丢失的报文进行重传，导致有些情况组播报文丢失严重。
- 无线组播报文的速率是在强制速率中选取的最低发送速率，因此组播数据的传输效率较低。

组播传输的特点可能无法满足某些对组播流有较高要求的应用，如对延迟不十分敏感，但要求报文流有较高完整性要求的应用，如高清视频点播。为了满足上述需求，可开启组播优化功能，使得 AP 向客户端发送组播报文时，将组播数据报文转换为单播数据报文，转换后的无线单播数据报文不但具有重传确认机制及更高速率，并且具有 Video 的优先级，可以优先被发送。

说明

如无特殊说明，下文描述的单播报文均指具有 Video 的优先级的无线单播数据报文。

图1-2 开启组播优化后数据传输示意图



开启组播优化功能后，AP 会监听客户端上报的组播报告报文和离开报文进行组播优化表项维护。当 AP 收到客户端的组播报告报文时，会添加或是更新组播优化表项，并更新客户端允许的组播源地址（对于 IGMPv3 和 MLDv2 报文）。当收到客户端的组播离开报文或是组播优化表项老化时间超时后，则删除对应的组播优化表项。关闭组播优化功能时，整个组播优化表项会被删除。

建立组播表项后，AP 会监听从组播源发往客户端的下行非 IGMP 和 MLD 的组播数据报文，查询组播优化表项，检查报文中的组播组地址。若在表项中存在该组播组地址，则遍历加入该组播地址的所有客户端，将组播数据报文转换为单播数据报文，并单播发送给对应客户端；若没有该组播组地址，则正常发送组播数据报文。

为了避免客户端数量过多，导致性能下降，用户可以设置支持组播优化的最大客户端数量。在某个射频下，接入组播组的客户端数量超过阈值时，设备有两种处理方式：

- 组播优化功能暂停。新接入的客户端可以加入组播组，能够收到组播报文，并生成组播优化表项，但是会导致该射频下的接入组播组的所有客户端的组播优化功能失效。当接入组播组的客户端数量小于阈值时，组播优化功能重新生效。
- 拒绝新客户端进行组播优化。新接入的客户端可以加入组播组，即生成 IGMP-Snooping 表项，但不会生成组播优化表项。如果组播优化表项中已经存在新客户端请求加入的组播组（由其它客户端生成的），则该客户端将无法接收组播数据报文；反之，如果组播优化表项中不存在新客户端请求加入的组播组，则该客户端依然可以收到组播数据报文。

注意

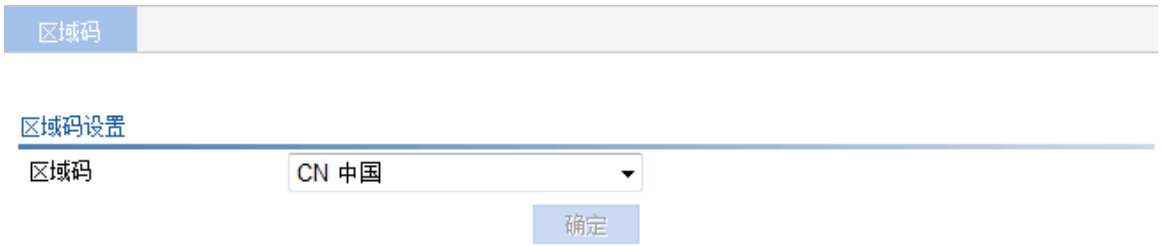
如果先配置组播优化功能暂停方式（在组播优化功能暂停方式下，超出阈值的客户端也能生成组播优化表项），然后将处理方式修改为拒绝新客户端进行组播优化方式，这些已存在的组播优化表项仍会生效。

1.2 无线高级设置

1.2.1 设置区域码

(1) 在导航栏中选择“高级设置> 区域码”，进入区域码的配置页面，如下图所示。

图1-3 区域码



(2) 配置区域码，详细配置如下表所示。

(3) 单击<确定>按钮完成操作。

表1-1 区域码的详细配置

配置项	说明
区域码	在下拉框中选择区域码 在配置WLAN设备时，必须正确地设置国家或地区码，以确保不违反当地的管制规定

说明

如果区域码设置选框显灰，则表示该 AP 产品已遵照相应国家或地区的管制要求进行了区域码锁定，在这种情况下，用户不能更改此项设置。

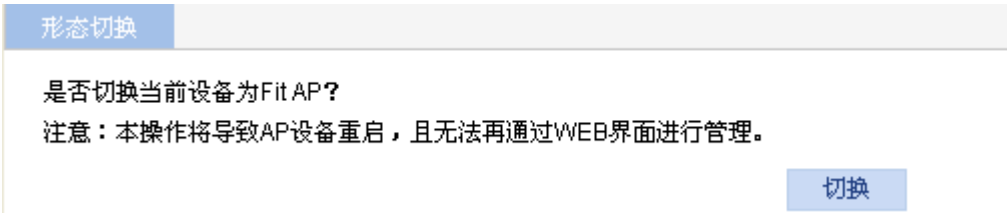
1.2.2 形态切换

通过 WEB 页面配置，将设备从 Fat AP 模式切换为 Fit AP 模式。

(1) 在导航栏中选择“高级设置> 形态切换”，进入形态切换页面，如下图所示。

(2) 单击<切换>按钮完成操作。

图1-4 形态切换



说明

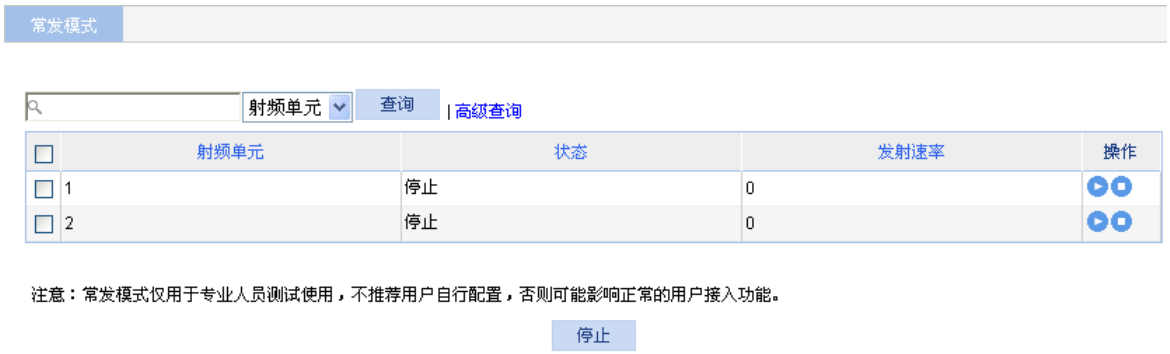
为了保证设备成功完成模式切换，在配置“形态切换”前，请根据实际情况完成以下确认：

如果采用 FIT AP 从 AC 上自动下载应用程序的方式，请确保组网方式已按照 Fit AP 组网方式进行了调整，网络中已部署有 AC 或有线无线一体化交换机，并且对应 AP 型号的应用程序已加载到 AC 或有线无线一体化交换机上。否则，切换到 Fit 形态后的 AP 将无法正常工作。

1.2.3 常发模式

(1) 在导航栏中选择“高级设置> 常发模式”，进入常发模式配置页面，如下图所示。

图1-5 常发模式



(2) 在列表中找到要进行配置的射频单元后，单击射频对应的图标，可以进入配置页面进行发射速率选择页面。发射速率值与使用的射频模式有关：

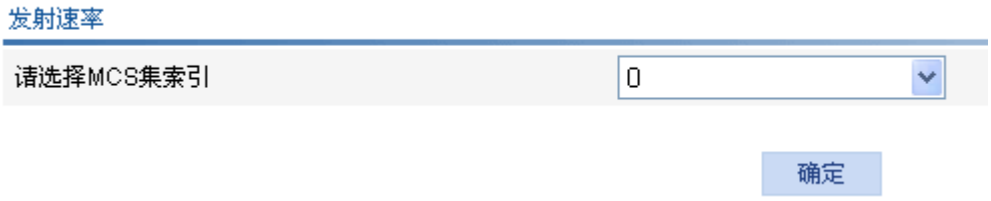
- 当射频模式为 802.11a/b/g 时，进入如下图所示配置页面，通过下拉框选择指定的发射速率。

图1-6 发射速率（802.11a/b/g）



- 当射频模式为 802.11n 时，进入如图所示配置页面，通过选择 MCS 索引值的方式指定 802.11n 射频速率。关于 MCS 的介绍请参见“射频”。

图1-7 发射速率（802.11n）



- 当射频模式为 802.11ac 时，进入如下图所示配置页面，通过选择 VHT MCS 和 VHT NSS 索引值的方式指定 802.11ac 射频速率。关于 VHT MCS 和 VHT NSS 的介绍请参见“射频”。

图1-8 发射速率（802.11ac）



(3) 单击<确定>按钮完成操作。

可以使用下列方法停止常发模式：

- 单击射频对应的图标。
- 在列表中选中需要停止常发模式的射频单元，单击<停止>按钮。

停止常发模式后，页面上的“发射速率”栏显示值为 0。

1.2.4 上行链路检测

(1) 在导航栏中选择“高级设置> 上行链路检测”，进入上行链路检测页面，如下图所示。

图1-9 上行链路检测



说明

该页面显示的接口信息与设备的型号有关，请以设备的实际情况为准。

(2) 配置上行链路检测，详细配置如下表所示。

(3) 单击<确定>按钮完成操作。

表1-2 上行链路检测的详细配置

配置项	说明
接口名称	显示可以配置为上行接口的所有接口
链路状态	up：表示链路状态为up down：表示链路状态为down 说明 Radio接口的上行链路状态为该接口上绑定的WDS的链路状态
上行链路	选中复选框后，表示把该接口对应的链路设置为上行链路。

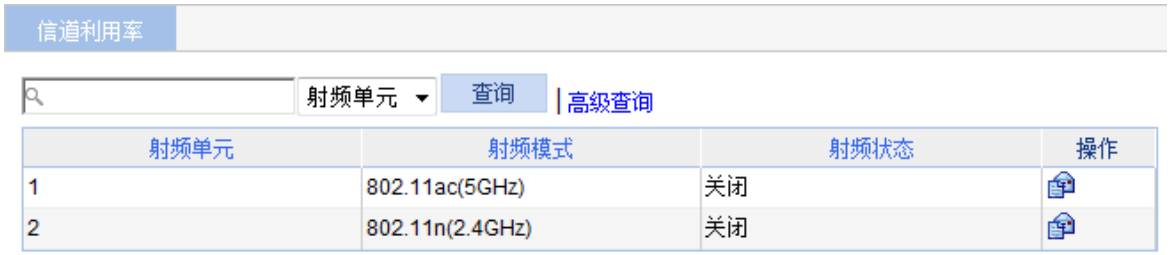
说明

如果所配置的上行链路都处于 down 状态，设备将不能提供无线接入服务。

1.2.5 信道利用率

(1) 在导航栏中选择“高级设置 > 信道利用率”，进入信道利用率页面，如下图所示。

图1-10 信道利用率



(2) 单击列表中对应的图标，进入信道利用率检测的配置页面，如下图所示。

图1-11 信道利用率检测



(3) 配置信道利用率，详细配置如下表所示。

(4) 单击<开始>按钮进行信道利用率检测。

表1-3 信道利用率的详细配置

配置项	说明
射频单元	显示选择的AP射频单元
射频模式	显示选择的AP射频模式
每个信道检测时间	配置每个信道的检测时间，单位为秒 缺省情况下，每个信道的检测时间为3秒

说明

在获取信道利用率检测结果前，请不要在同一射频上再次开启信道利用率检测。

1.2.6 配置频谱导航

说明

- 开启频谱导航后，客户端的关联效率将受到影响，因此不建议在普遍使用单频 2.4GHz 客户端的场景下开启本功能。
- 对于要求低延迟的网络环境，不建议开启频谱导航。

设备各款型对于本节所描述的特性支持情况有所不同，详细差异信息如下：

产品系列	型号	特性	描述
WA2600系列	WA2610H	频谱导航	不支持
WA4600系列	WA4620i-ACN/WA4620E-ACN		支持
WA4300系列	WA4320H-ACN		支持
	WA4320i-ACN/WA4320i-X		支持
	WA4320-TS/WA4320-TQ/WA4320-TQ-V		支持
	WA4320X		支持
	WA4320-ACN/WA4320/WA4320-ACN-SI/ WA4320-ACN-C/WA4320-ACN-D/WA4320-ACN-E/WA4320-ACN-PI		支持
	WA4330-ACN		支持
LA4300系列	LA4310/LA4310V/LA4320/LA4320V/LA4320X		LA4310/LA4310V不支持，LA4320/LA4320V/LA4320X支持
小贝系列	WAP722/WAP722E/WAP722S		支持
	WAP712/WAP712C		支持

1. 配置准备

为使频谱导航功能能够正常运行，需完成以下任务：

- 确认客户端接入的无线服务的快速关联处于关闭状态。缺省情况下，快速关联功能处于关闭状态。快速关联功能的配置请参见“无线服务”。
- AP 的两个射频模式分别为 5GHz 和 2.4GHz，客户端接入的无线服务绑定在同一 AP 的两个射频上。

2. 配置频谱导航

(1) 在导航栏中选择“高级设置> 频谱导航”，进入如下图所示页面。

图1-12 配置频谱导航



(2) 配置频谱导航，详细配置如下表所示。

(3) 单击<确定>按钮完成操作。

表1-4 AP 预配置信息的详细配置

配置项	说明
频谱导航	• 开启：开启全局频谱导航功能 • 关闭：关闭全局频谱导航功能 缺省情况下，全局频谱导航功能处于关闭状态
连接数门限	连接数门限：5GHz射频上客户端连接数门限
差值门限	差值门限：客户端连接数差值门限，即*gap* = 5GHz射频上客户端的数量－2.4GHz射频上客户端的数量 如果5GHz射频上已连接的客户端数量达到连接数门限，且5GHz射频与2.4GHz射频上连接的客户端差达到或超过差值门限，AP会拒绝客户端接入5GHz射频，且允许新客户端接入2.4GHz射频（即不会引导双频客户端优先接入5GHz射频）
最大拒绝次数	设备拒绝5GHz客户端关联请求的最大次数 AP的5GHz射频已经处于过载状态时，如果客户端反复向AP的5GHz射频发起关联请求，且AP拒绝客户端关联请求次数达到/超过设定的最大拒绝关联请求次数，那么该AP会认为此时该客户端不能连接到其它任何的AP，在这种情况下，AP上的5GHz射频也会接受该客户端的关联请求
RSSI门限	频谱导航的RSSI门限 只有当AP的5GHz射频上检测到客户端的RSSI值达到/超过配置的门限值，AP会引导其优先接入AP的5GHz射频。若检测到客户端的RSSI值低于的门限值，则不会将此客户端导航至5GHz射频
老化时间	客户端信息的老化时间 当客户端请求连接AP时，AP会记录客户端的相关信息。在到达老化时间前，AP接收到客户端的Probe Request或Association Request，那么AP会刷新客户端信息，重新计算客户端信息的老化时间。到达老化时间仍得不到刷新的客户端信息将被AP删除。删除客户端信息后，AP在计算频谱导航时不会计算该客户端

1.2.7 配置组播优化功能

1. 开启组播优化功能

(1) 在导航栏中选择“高级设置> 组播优化”，进入组播优化配置页面，如下图所示。

图1-13 配置组播优化



(2) 配置组播优化，详细配置如下表所示。

(3) 单击<确定>按钮完成操作。

表1-5 组播优化的详细配置

配置项	说明
老化时间	配置组播优化表项老化时间。在此时间段内，如果AP没有收到客户端发送的组播报告报文，则删除对应的组播优化表项
优化客户端上限	配置在一个射频上支持组播优化的最大客户端数量。不同型号的设备支持的取值范围不同，请以设备的实际情况为准 提示 • 需要注意的是，当一个客户端加入某个射频下多个组播组时，会累加计数。例如，在同一个射频上，如果一个客户端分别加入两个组播地址，则组播优化的客户端数量记做 2 • 每个客户端最多能加入 8 个组播组

配置项	说明
超出上限处理方式	• 暂停全部优化：在某个射频下，接入组播组的客户端数量超过阈值时，新接入的客户端可以加入组播组，能够收到组播报文，并生成组播优化表项，但是会导致该射频下的接入组播组的所有客户端的组播优化功能失效。当接入组播组的客户端数量小于阈值时，组播优化功能重新生效 • 排除新客户端。在某个射频下，接入组播组的客户端数量超过阈值后，新接入的客户端可以加入组播组，即生成 IGMP-Snooping 表项，但不会生成组播优化表项。如果组播优化表项中已经存在新客户端请求加入的组播组（由其它客户端生成的），则该客户端将无法接收组播数据报文；反之，如果组播优化表项中不存在新客户端请求加入的组播组，则该客户端依然可以收到组播数据报文 缺省情况下，客户端数量超过阈值后的处理方式为暂停组播优化功能 提示 如果先配置暂停全部优化方式（在暂停全部优化方式下，超出阈值的客户端也能生成组播优化表项），然后将处理方式修改为“排除新客户端”方式，这些已存在的组播优化表项仍会生效

(4) 在指定无线服务前选中复选框，应用组播优化功能。

(5) 单击<开启>按钮完成操作。

2. 查看组播优化信息

(1) 在导航栏中选择“高级设置 > 组播优化”，进入组播优化配置页面，如下图所示。

(2) 点击指定的射频后，可以查看该射频的组播优化信息。

图1-14 查看组播优化信息



表1-6 组播优化信息描述表

字段	描述
Total clients	加入组播优化表项的客户端总数 当一个客户端加入某个射频下多个组播组时，会累加计数。例如，在同一个射频上，如果一个客户端分别加入两个组播地址，则组播优化的客户端数量记做2

字段	描述
Action	• 当前组播优化运行状态： • Optimize：优化中 • Halt：暂停组播优化功能
Multicast Address	• 客户端加入的组播地址
MAC Address	• 客户端的 MAC 地址

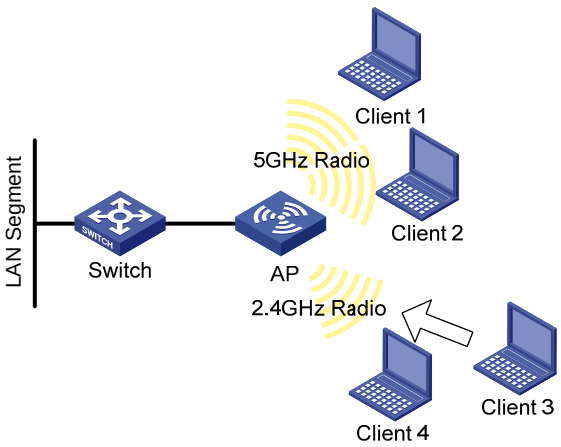
1.3 高级设置配置举例

1.3.1 频谱导航配置举例

1. 组网需求

Client 1～Client 4 需要接入 AP 1，其中 AP 1 的两个射频模式分别为 5GHz 和 2.4GHz，Client 1、Client 2 与 Client 3 为双频客户端，Client4 为单频 2.4GHz 客户端。要求使用频谱导航功能，充分利用 AP 1 的两个射频，使两个频段上的客户端数量相对均衡。

图1-15 频谱导航组网图



2. 配置AP

说明

为使频谱导航功能能够正常运行，需要在设备上确认客户端接入的无线服务的快速关联处于关闭状态。缺省情况下，快速关联功能处于关闭状态。

(1) 创建无线服务

步骤 1：在导航栏中选择“无线服务 > 接入服务”。

步骤 2：单击<新建>按钮，进入接入服务新建页面。

步骤 3：进行如下配置。

- 设置无线服务名称为“band-navigation”。

- 选择无线服务类型为“Clear”。

步骤 4：单击<确定>按钮完成操作。

步骤 5：开启无线服务。在导航栏中选择“无线服务 > 接入服务”，进入接入服务配置页面。

步骤 6：选中“band-navigation”前的复选框，

步骤 7：单击<开启>按钮完成操作。

(2) 绑定 AP 的射频

步骤 1：在导航栏中选择“无线服务 > 接入服务”。

步骤 2：单击无线服务“band-navigation”对应的图标。

步骤 3：选中“802.11ac(GHz)”和“802.11n(2.4GHz)”前的复选框。

步骤 4：单击<绑定>按钮完成操作。

图1-16 绑定 AP 的射频



(3) 开启 802.11ac(GHz)和 802.11n(2.4GHz)射频

缺省情况下，802.11ac(GHz)和 802.11n(2.4GHz)射频处于开启状态，此步骤可选。

(4) 配置频谱导航

步骤 1：在导航栏中选择“高级设置> 频谱导航”，进入如下图所示页面。

步骤 2：进行如下配置，如下图所示。

- 开启频谱导航。
- 输入连接数门限为 2，差值门限为 1，最大拒绝次数为 1。
- 其它参数保持缺省值。

步骤 3：单击<确定>按钮完成操作。

图1-17 配置频谱导航



3. 验证配置结果

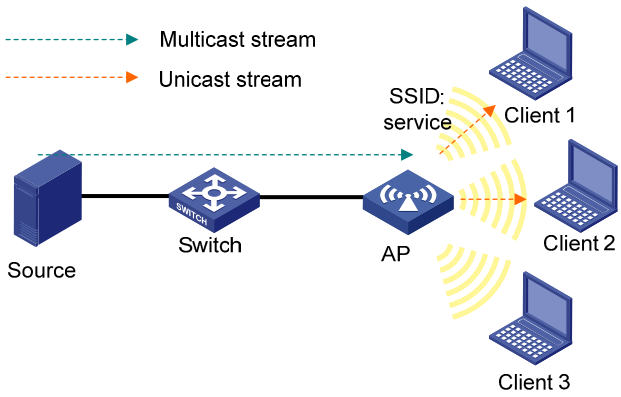
Client 1、Client 2 优先接入到 AP 1 的 5GHz 射频上，Client 4 只能接入到 AP 1 的 2.4GHz 射频上。此时由于 5GHz 射频上已连接的客户端数量达到门限 2，且 5GHz 射频与 2.4GHz 射频上连接的客户端差值达到门限 1，所以当 Client 3 想接入 AP 1 时，会关联至 AP 1 的 2.4GHz 射频上。

1.3.2 组播优化功能配置举例

1. 组网需求

在如下图所示的无线环境中，开启组播优化功能，将组播数据报文转换为单播数据报文并发送给客户端。

图1-18 组播优化功能配置组网图



2. 配置AP

步骤 1：在导航栏中选择“高级设置> 组播优化”，进入组播优化的配置页面，如下图所示。

步骤 2：配置组播优化，详细配置如下表所示。

- 设置老化时间为 300。

- 设置优化客户端上限为 2。
- 设置超出上限处理方式为“排除新客户端”。

步骤 3：单击<确定>按钮完成操作。

步骤 4：在指定无线服务前选中复选框，应用组播优化功能。

步骤 5：单击<开启>按钮完成操作。

图1-19 配置组播优化



3. 验证配置步骤

Client 1 和 Client 2 通过 AP 的某个射频接入到名为 service 的无线服务，并加入组播组，使在组播优化信息页面可以查看到组播优化表项的信息。Client 1 和 Client 2 加入组播组时，组播优化功能能够正常工作，当 Client 3 加入组播组时，客户端数量超过设置的阈值，Client 3 无法加入组播优化表项。