H3C WAC380 系列多业务无线控制器

Web 网管配置指导

新华三技术有限公司
http://www.h3c.com

资料版本：6W103-20180628
产品版本：WAC380-CMW710-R5221P01

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

本配置指导主要介绍 H3C WAC380 系列无线控制器的 Web 配置指导。

前言部分包含如下内容：

读者对象

本手册主要适用于如下工程师：

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

本书约定

1. 命令行格式约定

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

2. 图形界面格式约定

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

3. 各类标志

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

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

4. 图标约定

本书使用的图标及其含义如下：

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

5. 示例约定

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

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

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：info@h3c.com

感谢您的反馈，让我们做得更好！

目 录

1 对浏览器、屏幕分辨率和操作系统的要求

- 建议使用以下浏览器访问 Web：Chrome 35.0.1916.114 及以上版本、Internet Explorer 10 及以上版本、Firefox 30.0.0.5269 及以上版本、Safari 5.1 及以上版本。使用其它浏览器访问可能会出现不支持或显示效果不佳。
- 使用的浏览器必须要设置能接受第一方 Cookie（即来自站点的 Cookie），并启用活动脚本（或 JavaScript），才能正常访问 Web。以上功能在不同浏览器中的名称及设置方法可能不同，请以实际情况为准。
- 使用 Internet Explorer 浏览器时，还必须启用以下两个功能，才能正常访问 Web：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。
- 更改设备的软件版本后，建议在登录 Web 页面之前先清除浏览器的缓存，以便正确地显示 Web 页面。
- 请使用分辨率在 1024×768 以上的台式机、笔记本或平板电脑访问。

2 初次登录Web

设备支持 HTTP（Hypertext Transfer Protocol，超文本传输协议）和 HTTPS（Hypertext Transfer Protocol Secure，超文本传输协议的安全版本）两种 Web 访问方式。

设备出厂时已经缺省启用了 HTTP 和 HTTPS 服务，并且设置有缺省的 Web 登录信息，用户可以直接使用缺省登录信息通过 HTTP 或 HTTPS 服务登录设备的 Web 界面。缺省的 Web 登录信息包括：

- 用户名：admin
- 密码：admin
- 用户角色：network-admin
- 设备（Vlan-interface1）的 IP 地址：192.168.0.100

采用缺省登录信息 Web 登录设备的步骤如下：

(1) 连接设备和 PC

用以太网线将 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，保证其能与设备互通

通过 Console 登录到设备执行 **display interface vlan-interface 1** 命令的方式获取设备当前的 IP 地址。将 PC 的 IP 地址设置为与设备 IP 地址在同一个网段。

(3) 启动浏览器

在 PC 上启动浏览器，在地址栏中输入设备地址，然后回车，进入设备的 Web 登录页面。通过 HTTP 方式访问 Web 时，输入的设备地址格式为“http://*ip-address*:80”（“http://”可以省略）；通过 HTTPS 方式访问 Web 时，输入的设备地址格式为“https://*ip-address*:443”。其中，*ip-address* 为设备的 IP 地址；80 和 443 分别为 HTTP 服务和 HTTPS 服务的缺省端口号，可以省略。

(4) 输入登录信息

在登录页面中输入用户名 admin 和密码 admin，单击<登录>按钮即可登录 Web。

(5) 修改登录信息

登录设备后，单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 服务 > IP 服务”，进入“IP”页面修改设备的 IP 地址；单击“系统”菜单页面左侧导航栏的“系统 > 管理员”，进入“管理员”配置页面修改用户 admin 的密码，以提高安全性，或者创建新的管理员，以方便对设备进行管理。

说明

同时通过 Web 登录设备的最大用户数为 64。

---

3 退出Web

为保证设备的安全性，用户在 Web 上完成操作后应及时退出登录。

在 Web 页面上单击右上角的<admin>按钮，然后单击“退出登录”，即可退出 Web。

需要注意的是：

- 退出 Web 时，系统不会自动保存当前配置。因此，建议用户在退出 Web 前先点击页面右上方的<admin>按钮，然后单击“保存”或单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“系统 > 管理”，然后单击页面上方的“配置文件”，再单击<保存当前配置>按钮来保存当前配置。
- 直接关闭浏览器不能使用户退出 Web。

目 录

1 Web页面布局介绍

图1-1 Web 页面布局

（1）标识和辅助区	（2）导航栏
（3）执行区	（4）状态栏

如 图 1-1 所示，Web页面有以下几个功能区域：

- 标识和辅助区：该区域用来显示公司 Logo 和设备型号，并提供语言切换、更改登录用户密码、保存当前配置、退出登录功能。点击 “  ” 可以切换语言、更改登录用户密码、保存当前配置、退出登录、网站地图和微信扫码关注功能。
- 导航栏：以树的形式组织设备的 Web 功能菜单。用户在导航栏中可以方便的选择功能菜单，选择结果显示在执行区中。
- 执行区：进行配置操作、信息查看、操作结果显示的区域。
- 状态栏：显示设备当前的状态和统计信息。

2 Web页面分类

根据执行区内容的不同，Web 页面分为特性页面、表项显示页面和配置页面三种。

2.1 特性页面

如 图 2-1 所示，特性页面显示了该特性包含的表项的统计信息、该特性支持的主要功能等。

图2-1 特性页面示意图

2.2 表项显示页面

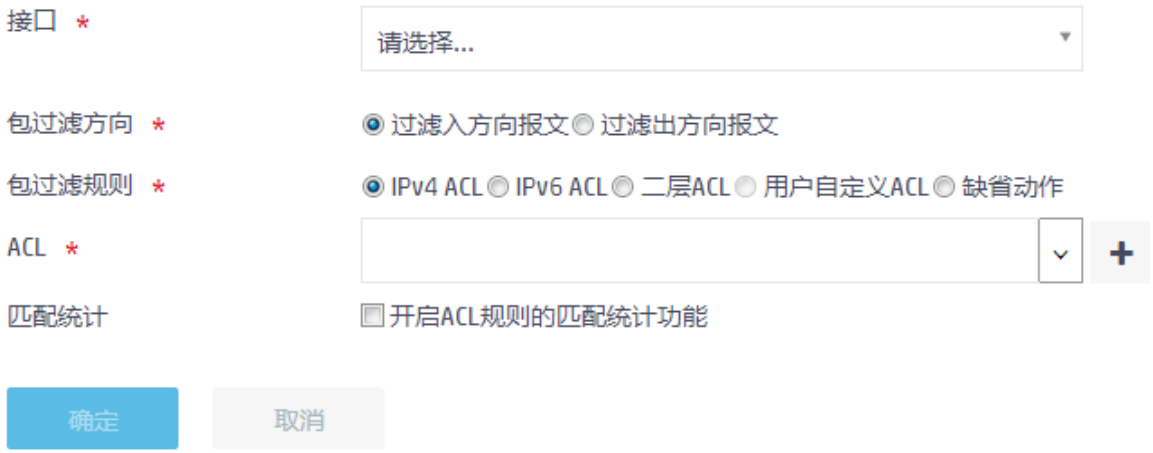
如 图 2-2 所示，表项显示页面用来显示表项的具体信息。点击标题项（如“接口”），可以根据该标题项对表项信息进行升序或降序排列。

图2-2 表项显示页面示意图

2.3 配置页面

如 图 2-3 所示，配置页面用来完成某项配置任务，如添加、修改一条表项。某项配置任务需要的所有配置均可在该页面上完成，不需要在页面之间跳转，以方便用户使用。例如，在配置包过滤策略时需要创建并关联ACL，在包过滤策略的配置页面上点击“ ”即可创建ACL，无需跳转到ACL的配置页面。

图2-3 配置页面示意图



3 Web常用按钮和图标

Web页面上常用的按钮、图标及其功能，如 表 3-1 所示。

表3-1 Web 常用按钮和图标

按钮和图标	功能说明
	查看某个功能或参数的在线帮助信息
	进入下一级页面进行配置或查看当前配置信息
	表项的统计计数
	显示功能当前的开启/关闭状态，点击该按钮可以修改开启/关闭状态
	刷新表项内容
	刷新统计或显示信息
	显示更多内容
	筛选按钮，用于按条件进行筛选

	• 表项显示页面上，用于添加一条表项
	• 配置页面上，具有如下功能：
	  ○ 用于对当前表项的添加进行确认，并新增一条表项
	  ○ 添加一个 ACL 或策略等，以避免配置过程中在页面之间进行跳转

	在文本框中输入查询关键字，点击该按钮对表项进行简单查询
	高级查询按钮，点击该按钮后可以输入多个条件对表项进行组合条件查询
 或	表项导出按钮
	表项显示页面上，将鼠标放在某一条表项上，将在表项的最右端显示该图标 该图标用于显示当前表项的详情。
	表项显示页面上，将鼠标放在某一条表项上，将在表项的最右端显示 该图标用于删除当前表项
	表项显示页面上，将在页面的左上方显示该图标 该图标用于删除所有表项
	用于选择显示表项中的哪些标题项
	用于进入高级设置页面
	表项显示页面上，将鼠标放在某一条表项上，将在表项的最右端显示 该图标用于修改和编辑当前表项

按钮和图标	功能说明
	快速配置按钮，用于对某项服务进行快速配置
	提示按钮，点击该按钮后将对相关功能和服务进行解释
	添加按钮，用于添加新的配置表项

4 Web常用操作

Web 页面上常用的操作包括保存当前配置、显示表项详情、重启设备等。

4.1 保存当前配置

对设备执行配置操作后，建议及时保存当前配置，以免配置丢失。保存当前配置的方法有以下两种：

- 点击页面右上方标识和辅助区内的“admin”按钮，然后单击“保存”，保存配置。
- 单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“系统 > 管理”，然后单击页面上方的“配置文件”，再单击<保存当前配置>按钮来保存当前配置。

4.2 显示表项详情或修改表项设置

在表项显示页面上，将鼠标放在某一条表项上，将在表项的最右端显示详情图标“ ”。点击该图标进入详情页面后，可以显示表项的详细信息。

4.3 重启设备

执行某些操作后，需要重启设备才能使配置生效。重启设备的方法为：单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“系统 > 管理”，然后单击页面上方的“重启”，再单击重启设备按钮。

在重启设备前，建议先保存当前配置，以免配置丢失。

目 录

1 简介

用户登录 Web 后，能够看到的页面导航内容、能够执行的操作与该用户的用户角色有关。所有配置操作的缺省用户角色要求为 network-admin。查看操作的缺省用户角色为所有角色。

用户角色为 network-admin 的用户登录后，Web 页面导航栏分为系统和网络两部分。系统上的一级菜单包括概览、网络配置、网络安全、系统、工具；网络上的一级菜单包括概览、快速配置、监控、无线配置、网络安全、系统、工具、报告。点击一级菜单，会展开子菜单，子菜单由分类和特性名称组成。依次点击“一级菜单->特性名称”可以进入相应的 Web 页面对该特性进行配置。

1.1 系统

系统主要是对设备的基本功能及有线网络的特性和功能进行查看和配置。

1.2 网络

网络主要是对无线网络的特性和功能进行查看和配置。

1.3 AP节点

AP 节点主要是根据 AP 节点对特性和功能进行查看和配置。

2 系统页面包含的特性及其支持的功能

2.1 概览

显示日志信息、当前的 AP 信息、系统利用率、无线服务、客户端、流量监控等系统信息。

2.2 网络配置

网络配置菜单包含的特性及其支持的功能如 表 2-1 所示。

表2-1 网络配置菜单包含的特性及其支持的功能

分类	特性名称	功能
漫游	漫游	• 显示 WLAN 客户端漫游信息和漫游组信息 • 创建漫游组
接口	接口	• 查看设备支持的接口列表以及接口的主要属性（状态、IP 地址、速率、双工模式、描述） • 删除逻辑接口、编辑接口等
	链路聚合	创建、修改、删除二层聚合组
	PPPoE配置	添加、删除、修改PPPoE Client
VLAN	VLAN	• 基于端口划分 VLAN • 创建 VLAN 接口
	MAC	• 创建和删除静态 MAC 地址表项、动态 MAC 地址表项和黑洞 MAC 地址表项 • 显示已有的 MAC 地址表项
	STP	• 全局和接口开启/关闭 STP 功能 • 配置 STP、RSTP、MSTP 和 PVST 工作模式 • 配置实例优先级 • 配置多生成树域
路由	路由表	查看IPv4和IPv6路由表项，包括路由表的概要信息和统计信息
	静态路由	• 查看 IPv4 和 IPv6 静态路由表项 • 创建、修改和删除 IPv4、IPv6 静态路由表项
服务-IP服务	IP	• 配置接口 IP 地址获取方式（DHCP 或者手工配置） • 修改接口的 IP 地址和 MTU 值 • 创建 LoopBack 接口

分类	特性名称	功能
	IPv6	• 配置接口 IPv6 地址获取方式（手工指定、自动获取或自动生成） • 修改接口的 IPv6 地址 • 创建 Loopback 接口

服务-DHCP/DNS	DHCP	• DHCP 服务器功能
		  ○ 配置 DHCP 服务
		  ○ 配置接口工作在 DHCP 服务器模式
		  ○ 配置 DHCP 地址池
		  ○ 配置 IP 地址冲突检测功能
		• DHCP 中继功能
		  ○ 配置 DHCP 服务
		  ○ 配置接口工作在 DHCP 中继模式，指定对应的 DHCP 服务器地址
		• 配置是否记录 DHCP 中继表项，中继表项定时刷新功能和刷新时间间隔

	DHCP Snooping	• 配置端口为信任或非信任端口 • 配置 DHCP Snooping 表项记录功能和表项备份机制 • DHCP Snooping 端口设置，包括 MAC 地址检查、请求方向报文检查、接受 DHCP 报文限速和 DHCP Snooping 表项最大学习数 • 配置接口是否开启 Option 82 功能。若开启该功能，则可以配置 Option 82 的处理方式，填充模式和填充内容
	IPv4 DNS	• 配置静态、动态域名解析 • 配置 DNS 代理 • 配置域名后缀
	动态DNS	• 管理动态 DNS 策略 • 配置动态 DNS 策略关联接口
	IPv6 DNS	• 配置静态、动态 IPv6 域名解析 • 配置 IPv6 DNS 代理 • 配置 IPv6 域名后缀
服务-Multicast	IGMP Snooping	• 在 VLAN 上开启/关闭 IGMP Snooping 功能 • 查询 IGMP Snooping 表项 • 配置丢弃未知组播数据报文功能 • 配置 IGMP 查询器相关功能 • 配置端口快速离开功能 • 限制端口加入的组播组数量

分类	特性名称	功能
	MLD Snooping	• 在 VLAN 上开启/关闭 MLD Snooping 功能 • 查询 MLD Snooping 表项 • 配置丢弃未知 IPv6 组播数据报文功能 • 配置 MLD 查询器相关功能 • 配置端口快速离开功能 • 限制端口加入的 IPv6 组播组数量
服务-ARP	ARP	• 添加静态 ARP 表项 • 清除静态、动态 ARP 表项 • 配置 ARP 代理 • 配置免费 ARP • 配置 ARP 攻击防御
服务-ND	ND	• 添加静态 ND 表项 • 清除静态、动态 ND 表项 • 开启/关闭链路本地 ND 表项资源占用最小化 • 配置跳数限制 • 配置 RA 前缀，包括前缀及长度，有效生命期和首选生命期等 • 配置接口的 RA 设置，包括是否抑制 RA 报文，RA 报文最大和最小发送间隔，是否设置被管理地址标志位，是否携带 MTU 选项、是否指定跳数限制、是否设置其他信息标志位，路由器生存时间、邻居请求重传间隔、路由器优先级、保持邻居可达时间等 • 在接口上开启普通 ND 代理和本地 ND 代理 • 设置接口的 ND 规则，包括动态表项数量限制和重复地址检测请求次数
服务-NAT	NAT	• 配置动态转换、静态转换、内部服务器、NAT444 动态/静态转换 • 配置 NAT 地址组、NAT444 地址组、端口块组、服务器组 • 配置 PAT 方式地址转换模式、DNS 映射、NAT Hairpin • 开启 NAT ALG 功能 • 查看 NAT 日志
服务-管理协议	HTTP/HTTPS	• 启用/禁用设备 HTTP/HTTPS 登录功能 • 配置登录用户连接的超时时间 • 配置 HTTP/HTTPS 的服务端口号 • 使用 ACL 过滤登录用户
	FTP	• 开启 FTP 服务器功能 • 配置设备发送的 FTP 报文的 DSCP 优先级

分类	特性名称	功能
		• 使用 ACL 过滤 FTP 用户 • 配置 FTP 连接的空闲超时时间 • 配置 SSL 服务策略
	Telnet	• 启用/禁用设备 Telnet 登录功能 • 配置 IPv4/IPv6 Telnet 报文的 DSCP 优先级 • 使用 ACL 过滤登录用户
	NTP	• 启用/禁用 NTP 服务 • 配置本地时钟的 IP 地址和所处层数 • 配置身份验证密钥
	LLDP	• 开启/关闭 LLDP 功能 • 开启/关闭 CDP 兼容模式 • 配置协议相关参数 • 查看、配置接口状态 • 查看 LLDP 邻居 • 配置 LLDP 发送的 TLV 类型
	设置	• 开启或关闭日志输出到日志缓冲区的功能，并配置日志缓冲区可存储的信息条数 • 配置日志主机的地址及端口号

2.3 网络安全

网络安全菜单包含的特性及其支持的功能如 表 2-2 所示。

表2-2 网络安全菜单包含的特性及其支持的功能

分类	特性名称	功能
包过滤	包过滤	• 创建、修改和删除基于接口的包过滤策略、基于 VLAN 的包过滤策略、基于全局的包过滤策略 • 配置包过滤缺省动作
流策略	QoS策略	创建、修改和删除基于接口的QoS策略、基于VLAN的QoS策略、基于全局的QoS策略
	优先级映射	• 查询和配置端口优先级，配置端口优先级信任模式 • 查询和修改 802.1p 优先级到本地优先级映射表、DSCP 到 802.1p 优先级映射表、DSCP 到 DSCP 映射表
访问控制	802.1X	• 开启和关闭 802.1X 功能 • 配置 802.1X 的认证方法

分类	特性名称	功能
		• 配置端口接入控制方式 • 配置端口的最大用户数 • 配置 802.1X 高级功能
认证	ISP域	配置ISP域
	RADIUS	配置RADIUS方案
用户管理	本地用户	• 添加、编辑、删除、导入、导出本地用户 • 添加、编辑、删除本地用户组

2.4 系统

系统菜单包含的特性及其支持的功能如 表 2-3 所示。

表2-3 系统菜单包含的特性及其支持的功能

分类	特性名称	功能
事件日志	事件日志	查询、统计、删除日志信息
资源	IPv4 ACL	• 创建基本或高级 IPv4 ACL、基本或高级 IPv6 ACL、二层 ACL • 修改、删除在本页面和其他业务模块（如包过滤）页面创建的 ACL
	IPv6 ACL	
	二层	
	时间段	创建、修改和删除时间段
文件管理	文件管理	上传、下载和删除文件
管理员	管理员	• 创建、修改、删除角色 • 创建、修改、删除管理员，并指定管理员对应的角色，以控制管理员的访问权限 • 管理密码
管理	系统设置	• 配置设备的名称、位置和联系方式 • 配置系统时间
	配置文件	• 保存、导出当前配置 • 导入配置 • 查看当前配置 • 将设备恢复到出厂配置
	软件更新	• 升级系统软件 • 查看系统软件列表，包括设备本次启动使用的软件列表、下次启动的主用软件列表
	重启	重启设备
	关于	显示设备的基本信息，比如：设备名称、序列号、设备型号、设备描述、设备位置、联系方式以及版

分类	特性名称	功能
		本信息、电子标签、法律声明等

2.5 工具

工具菜单包含的特性及其支持的功能如 表 2-4 所示。

表2-4 工具菜单包含的特性及其支持的功能

分类	特性名称	功能
调试	诊断	收集诊断信息，用于定位问题

3 网络页面包含的特性及其支持的功能

3.1 概览

显示日志信息、当前的 AP 信息系统利用率、无线服务、客户端、流量监控等系统信息。

3.2 快速配置

快速配置菜单包含的特性及其支持的功能如 表 3-1 所示。

表3-1 快速配置菜单包含的特性及其支持的功能

分类	特性名称	功能
新增AP	新增AP	手工添加新AP
新增无线服务	新增无线服务	• 配置无线服务 • 配置链路层认证 • 开启/关闭授权功能和入侵检测功能 • 配置密钥管理 • 绑定 AP
新增新用户	新增新用户	添加一个新用户

3.3 监控

监控菜单包含的特性及其支持的功能如 表 3-2 所示。

表3-2 监控菜单包含的特性及其支持的功能

分类	特性名称	功能
无线网络	无线服务	查看无线服务列表
AP	AP	查看AP的统计信息
	AP组	查看AP组列表
客户端	客户端	查看客户端的统计信息
无线安全	WIPS	查看WIPS的统计信息
射频监控	射频优化	查看射频信道和功率调整信息
	频谱分析	查看频谱分析的详细信息
探针	客户端	查看用户相关信息
应用	Bonjour	• 查看 Bonjour 网关发现的 Bonjour 服务信息 • 清除 Bonjour 服务资源信息

分类	特性名称	功能
	组播优化	查看IPv4/IPv6的组播统计信息

3.4 无线配置

无线配置菜单包含的特性及其支持的功能如 表 3-3 所示。

表3-3 无线配置菜单包含的特性及其支持的功能

分类	特性名称	功能
无线网络	无线网络	• 查看、增加、删除、修改无线服务 • 配置链路层认证 • 开启/关闭授权功能和入侵检测功能 • 配置密钥管理 • 绑定 AP
AP管理	AP	添加、修改、删除和查询AP
	AP组	创建、查询、修改和删除AP组
	AP全局配置	• 配置 AP 区域码 • 开启/关闭区域码锁定 • 开启/关闭 AP 版本升级 • 开启/关闭自动 AP • 开启/关闭自动固化
	AP预配置	查看、修改AP预配置
	AP组预配置	查看、修改AP组预配置
无线QoS	客户端限速	• 查看客户端限速详细信息 • 配置基于客户端类型的客户端限速 • 配置基于无线服务的客户端限速 • 配置基于 AP/AP 组射频的客户端限速
	智能带宽保障	• 查看智能带宽保障详细信息 • 配置射频最大带宽 • 基于 AP 和 AP 组配置智能带宽保障
	无线多媒体	• 查看无线 QoS 状态和信息 • 查看射频EDCA参数 • 查看射频与客户端协商参数 • 查看客户端的 WMM 统计信息 • 查看传输流信息

分类	特性名称	功能
无线安全	WIPS	• 查看 WIPS 详细信息 • 开启 WIPS 功能 • 配置虚拟安全域 • 配置分类策略 • 配置攻击检测策略 • 配置 Signature 策略 • 配置反制策略 • 配置 AP 分类规则 • 配置 Signature 规则 • 配置忽略告警信息 MAC 地址列表
	黑白名单	• 配置白名单 • 配置静态和动态黑名单
射频管理	射频配置	查看AP组内所有AP型号和AP射频的详细信息
	射频优化	• 查看射频信道和功率调整信息 • 一键优化信道和功率 • 配置 AP 和 AP 组 RRM • 配置 RRM 保持调整组 • 配置 Baseline • 查看 RRM 历史调整信息
	频谱分析	• 开启频谱分析功能 • 配置干扰设备类型 • 导入干扰设备特征库 • 配置告警功能
	负载均衡	• 开启负载均衡功能 • 配置负载均衡模式 • 配置负载均衡组 • 配置负载均衡参数
	频谱导航	• 开启/关闭全局频谱导航功能 • 开启/关闭 AP 和 AP 组的频谱导航功能 • 配置频谱导航参数
探针	探针	开启/关闭、查看AP射频的探针开关
应用	Mesh服务	• 快速配置 Mesh 网络

分类	特性名称	功能
		• 配置和查看 Mesh Profile • 配置和查看 Mesh 策略 • 查看邻居探测请求发送功能 • 查看绑定信息 • 查看邻居白名单统计 • 查看 Mesh 链路统计信息
	组播优化	• 配置和查看 IPv4 组播优化 • 配置和查看 IPv6 组播优化
	无线定位	• 全局配置报文限速、报文过滤、报文稀释功能 • 配置 Aeroscout 定位、蓝牙定位、CUPID 定位和指纹定位功能
	Bonjour网关	• 开启/关闭 Bonjour 网关功能 • 创建和激活 Bonjour 服务类型 • 切换 Bonjour 网关模式 • 配置 Bonjour 策略

3.5 网络安全

网络安全菜单包含的特性及其支持的功能如 表 3-4 所示。

表3-4 网络安全菜单包含的特性及其支持的功能

分类	特性名称	功能
包过滤	包过滤	• 创建、修改和删除基于接口的包过滤策略、基于 VLAN 的包过滤策略、基于全局的包过滤策略 • 配置包过滤缺省动作
流策略	QoS策略	创建、修改和删除基于接口的QoS策略、基于VLAN的QoS策略、基于全局的QoS策略
	优先级映射	查询和配置802.1p优先级到本地优先级映射表、DSCP到802.1p优先级映射表、DSCP到DSCP映射表
访问控制	802.1X	• 开启和关闭 802.1X 功能 • 配置 802.1X 的认证方法 • 配置端口接入控制方式 • 配置端口的最大用户数 • 配置 802.1X 高级功能
认证	ISP域	配置ISP域
	RADIUS	配置RADIUS方案

分类	特性名称	功能
BYOD	BYOD规则	查看和配置DHCP规则、HTTP规则、MAC规则
	BYOD授权	查询和修改BYOD授权
用户管理	本地认证	• 添加、编辑、删除、导入、导出本地用户 • 添加、编辑本地用户组
来宾管理	来宾用户	查询、导出和添加来宾用户
	导入来宾用户	导入来宾用户
	批量创建来宾用户	批量创建来宾用户
	审批注册用户	审批注册用户
	来宾业务参数	配置来宾业务参数
接入管理	端口安全	配置端口安全功能
	Portal	配置Portal认证

3.6 系统

系统菜单包含的特性及其支持的功能如 表 3-5 所示。

表3-5 系统菜单包含的特性及其支持的功能

分类	特性名称	功能
资源	IPv4 ACL	• 创建基本或高级 IPv4 ACL、基本或高级 IPv6 ACL、二层 ACL • 修改、删除在本页面和其他业务模块（如包过滤）页面创建的 ACL
	IPv6 ACL	
	二层	
	时间段	创建、修改和删除时间段

3.7 工具

工具菜单包含的特性及其支持的功能如 表 3-6 所示。

表3-6 工具菜单包含的特性及其支持的功能

分类	特性名称	功能
无线报文捕获	无线报文捕获	查看无线报文捕获列表
RF Ping	RF Ping	进行无线链路质量检测
调试	诊断	收集诊断信息，用于定位问题

3.8 报告

报告菜单包含的特性及其支持的功能如 表 3-7 所示。

表3-7 报告菜单包含的特性及其支持的功能

分类	特性名称	功能
客户端统计	帧统计	按帧和字节数查看客户端报文统计信息
	字节数统计	
	帧总计	
	字节总计	
AP统计	AP统计	查看AP信息汇总列表
无线服务统计	无线服务统计	查看无线服务统计信息列表

4 AP节点支持的功能

AP节点导航栏会显示当前设备的AP组和AP信息，并与网络页面中的[无线配置/AP管理]导航栏下的AP页签相关联，点击AP节点中的AP名称后会直接跳转到AP配置页面，进行AP的配置和管理。AP页签功能请参见 表 3-3。

目 录

1 网络配置

1.1 漫游

1.1.1 WLAN漫游简介

在 ESS（Extended Service Set，拓展服务集）区域中，WLAN 客户端从一个 AP 上接入转移到另一个 AP 上接入的过程叫做漫游。在漫游过程中，客户端需要维持原有的 IP 地址、授权信息等，确保已有业务不中断。

为了提高用户体验，缩短客户端漫游时间，AC 支持快速漫游，即使用 RSN+802.1X 认证接入的客户端在漫游到新 AP 时不再需要进行 802.1X 认证。

1.1.2 漫游基本概念

- IACTP（Inter Access Controller Tunneling Protocol，接入控制器间隧道协议）：H3C 公司自主研发的隧道协议，该协议提供了 AC 间报文的通用封装和传输机制。提供漫游服务的 AC 之间会建立 IACTP 隧道，用于保证 AC 间控制报文以及客户端漫游信息的安全传输。
- HA（Home Agent，本地代理）：客户端跨 AC 漫游后，与该客户端初始上线 AP 相连接的 AC 即为 HA。
- FA（Foreign Agent，外地代理）：客户端跨 AC 漫游后，客户端与某个不是 HA 的 AC 进行关联，该 AC 即为 FA。

1.1.3 漫游组网方式

1. AC内漫游

如 图 1-1 所示，当前网络中只有一台AC，客户端可以从同一AC内的一个AP漫游到另一个AP上接入，称为AC内漫游（Intra-AC roaming）。

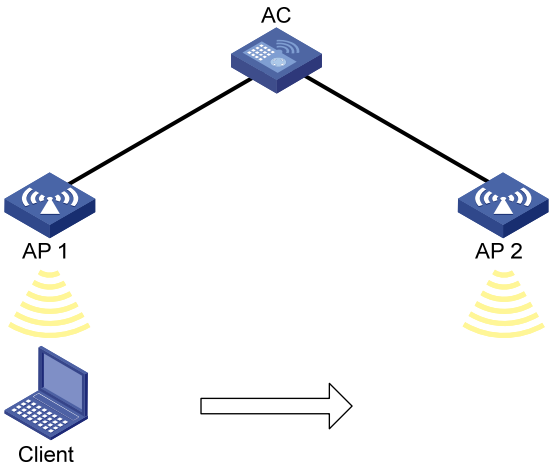
客户端完成 AC 内漫游的过程如下：

(1) 客户端在 AP 1 上初始上线，在 AC 上会创建该客户端的漫游表项信息；

(2) 客户端漫游到 AP 2，AC 查找该客户端的漫游表项，并根据是否是 RSN+802.1X 认证方式决定是否对其进行快速漫游；

(3) 如果进行快速漫游，客户端不需要再次认证，即可在 AP 2 上成功上线；否则需要重新认证。

图1-1 AC 内漫游



2. AC间漫游

如 图 1-2 所示，当前网络中存在多台AC，客户端除了在AC内漫游，还可能从一个AC内的AP漫游到另一个AC内的AP上接入，称为AC间漫游（Inter-AC roaming）。该组网方式下，通过创建漫游组，统一管理参与漫游的AC，没有加入漫游组的AC将不参与漫游。

客户端完成 AC 间漫游的过程如下：

(1) 客户端在 AP 2 上初始上线，在 AC 1 上会创建该客户端的漫游表项，并通过 IACTP 隧道将漫游表项同步到漫游组成员 AC 2 上；

(2) 客户端漫游到 AP 3，AC 2 查找该客户端的漫游表项，根据是否是 RSN+802.1X 认证方式决定是否对其进行快速漫游；

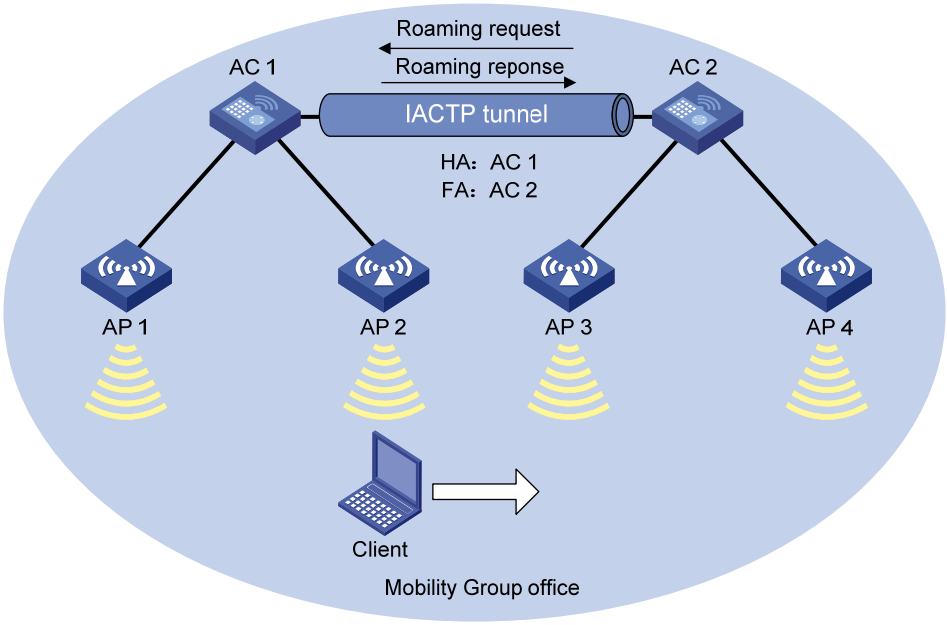
(3) 如果进行快速漫游，客户端不需要再次认证，即可在 AP 3 上成功上线；否则需要重新认证；

(4) 客户端在 AP 3 上线，AC 2 会给 AC 1 发送漫游请求消息；

(5) AC 1 收到漫游请求消息，并校验漫游信息是否正确。如果校验失败，则给 AC 2 回复漫游失败的漫游响应消息。如果校验成功，AC 1 添加该客户端的漫游轨迹和漫出信息，并给 AC 2 回复漫游成功的漫游响应信息；

(6) AC 2 收到 AC 1 回复的漫游响应信息。如果漫游失败，AC 2 将通知客户端下线；如果漫游成功，AC 2 添加该客户端的漫入信息。

图1-2 AC 间漫游



1.2 链路聚合

以太网链路聚合通过将多条以太网物理链路捆绑在一起形成一条以太网逻辑链路，实现增加链路带宽的目的，同时这些捆绑在一起的链路通过相互动态备份，可以有效地提高链路的可靠性。

1.2.1 聚合组

链路捆绑是通过接口捆绑实现的，多个以太网接口捆绑在一起后形成一个聚合组，而这些被捆绑在一起的以太网接口就称为该聚合组的成员端口。每个聚合组唯一对应着一个逻辑接口，称为聚合接口。聚合组与聚合接口的编号是相同的，例如聚合组 1 对应于聚合接口 1。

二层聚合组/二层聚合接口：二层聚合组的成员端口全部为二层以太网接口，其对应的聚合接口称为二层聚合接口。

聚合接口的速率和双工模式取决于对应聚合组内的选中端口：聚合接口的速率等于所有选中端口的速率之和，聚合接口的双工模式则与选中端口的双工模式相同。

1.2.2 选中/非选中状态

聚合组内的成员端口具有以下两种状态：

- 选中（Selected）状态：此状态下的成员端口可以参与数据的转发，处于此状态的成员端口称为“选中端口”。
- 非选中（Unselected）状态：此状态下的成员端口不能参与数据的转发，处于此状态的成员端口称为“非选中端口”。

1.2.3 操作Key

操作 Key 是系统在进行链路聚合时用来表征成员端口聚合能力的一个数值，它是根据成员端口上的一些信息（包括该端口的速率、双工模式等）的组合自动计算生成的，这个信息组合中任何一项的变化都会引起操作 Key 的重新计算。在同一聚合组中，所有的选中端口都必须具有相同的操作 Key。

1.2.4 属性类配置

属性类配置：包含的配置内容如 表 1-1 所示。在聚合组中，只有与对应聚合接口的属性类配置完全相同的成员端口才能够成为选中端口。

表1-1 属性类配置

配置项	内容
VLAN配置	端口上允许通过的VLAN、端口缺省VLAN、VLAN报文是否带Tag配置

1.2.5 聚合模式

链路聚合分为静态聚合和动态聚合两种模式，处于静态聚合模式下的聚合组称为静态聚合组，处于动态聚合模式下的聚合组称为动态聚合组。

静态聚合和动态聚合工作时首先要选取参考端口，之后再确定成员端口的状态。

1. 静态聚合

(1) 选择参考端口

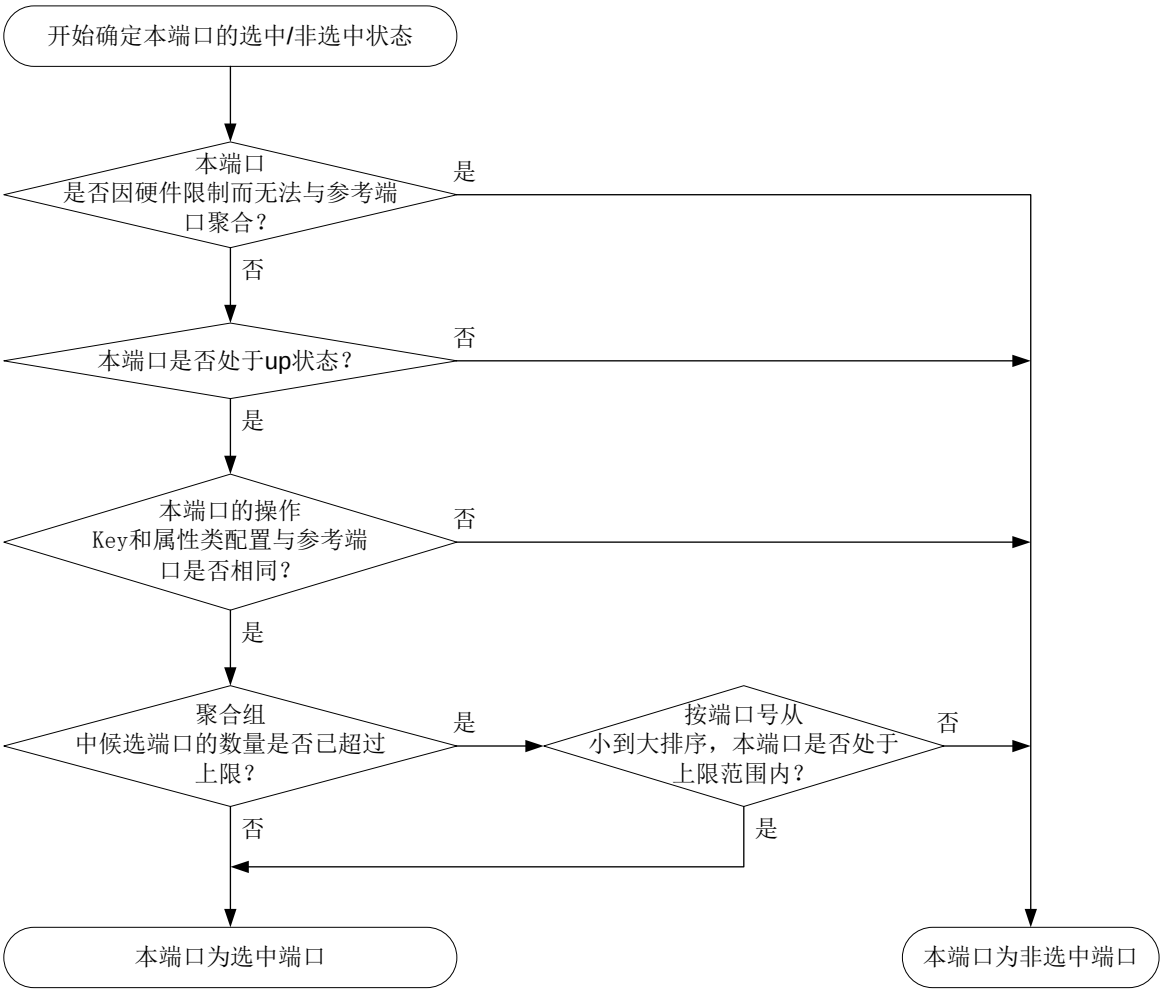
参考端口从本端的成员端口中选出，其操作 Key 和属性类配置将作为同一聚合组内的其他成员端口的参照，只有操作 Key 和属性类配置与参考端口一致的成员端口才能被选中。

对于聚合组内处于 up 状态的端口，按照端口的高端口优先级->全双工/高速率->全双工/低速率->半双工/高速率->半双工/低速率的优先次序，选择优先次序最高、且属性类配置与对应聚合接口相同的端口作为参考端口；如果多个端口优先次序相同，首先选择原来的选中端口作为参考端口；如果此时多个优先次序相同的端口都是原来的选中端口，则选择其中端口号最小的端口作为参考端口；如果多个端口优先次序相同，且都不是原来的选中端口，则选择其中端口号最小的端口作为参考端口。

(2) 确定成员端口状态

静态聚合组内成员端口状态的确定流程如 图 1-3 所示。

图1-3 静态聚合组内成员端口状态的确定流程



2. 动态聚合

动态聚合模式通过 LACP（Link Aggregation Control Protocol，链路聚合控制协议）协议实现，动态聚合组内的成员端口可以收发 LACPDU（Link Aggregation Control Protocol Data Unit，链路聚合控制协议数据单元），本端通过向对端发送 LACPDU 通告本端的信息。当对端收到该 LACPDU 后，将其中的信息与所在端其他成员端口收到的信息进行比较，以选择能够处于选中状态的成员端口，使双方可以对各自接口的选中/非选中状态达成一致。

(1) 选择参考端口

参考端口从聚合链路两端处于 up 状态的成员端口中选出，其操作 Key 和属性类配置将作为同一聚合组内的其他成员端口的参照，只有操作 Key 和属性类配置与参考端口一致的成员端口才能被选中。

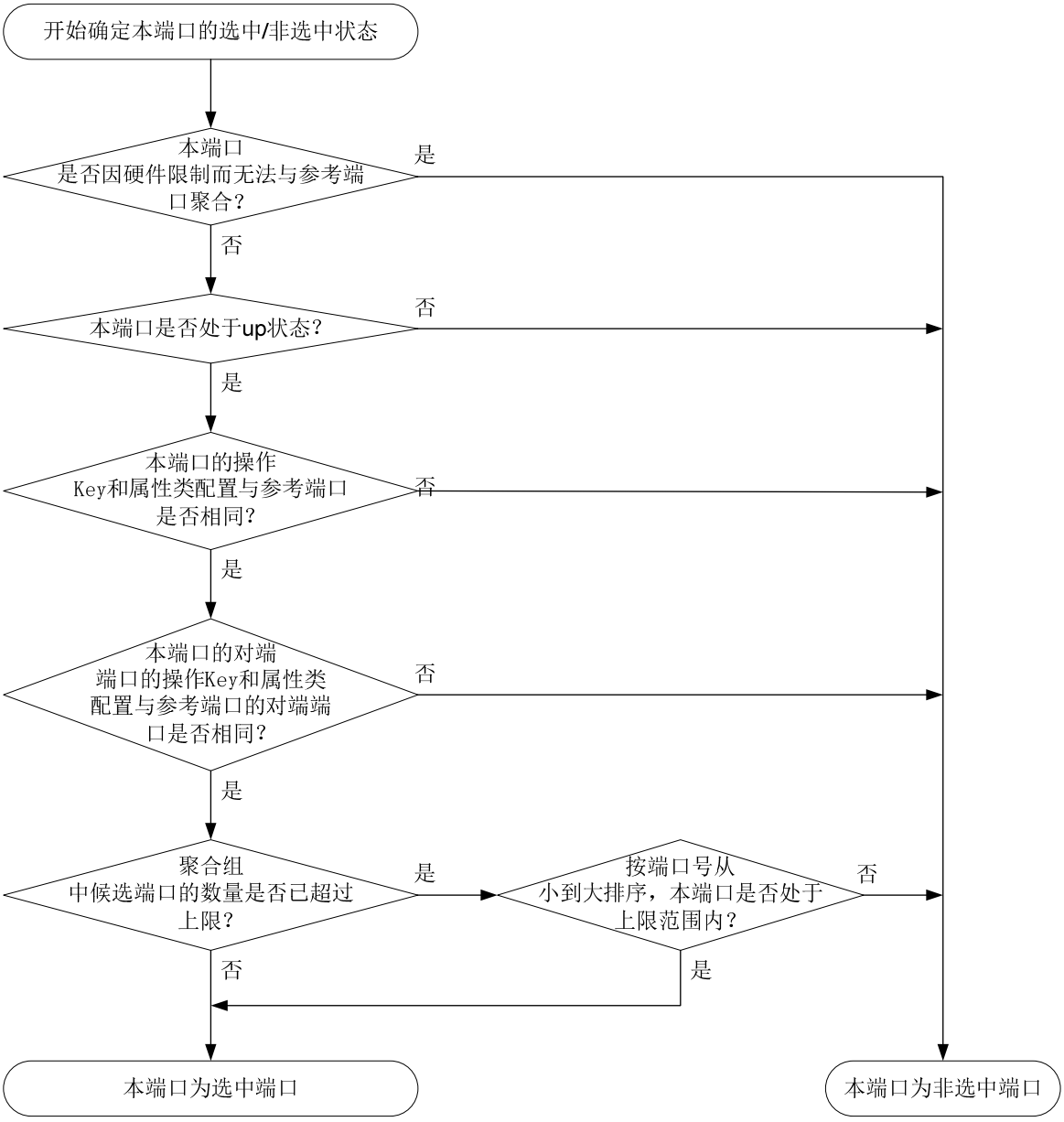
- 首先，从聚合链路的两端选出设备 ID（由系统的 LACP 优先级和系统的 MAC 地址共同构成）较小的一端：先比较两端的系统 LACP 优先级，优先级数值越小其设备 ID 越小；如果优先级相同再比较其系统 MAC 地址，MAC 地址越小其设备 ID 越小。
- 其次，对于设备 ID 较小的一端，再比较其聚合组内各成员端口的端口 ID（由端口优先级和端口的编号共同构成）：先比较端口优先级，优先级数值越小其端口 ID 越小；如果优先级相同再

比较其端口号，端口号越小其端口 ID 越小。端口 ID 最小、且属性类配置与对应聚合接口相同的端口作为参考端口。

(2) 确定成员端口的状态

在设备ID较小的一端，动态聚合组内成员端口状态的确定流程如 图 1-4 所示。

图1-4 动态聚合组内成员端口状态的确定流程



与此同时，设备 ID 较大的一端也会随着对端成员端口状态的变化，随时调整本端各成员端口的状态，以确保聚合链路两端成员端口状态的一致。

3. 静态聚合和动态聚合的优点

静态聚合和动态聚合的优点分别为：

- 静态聚合模式：一旦配置好后，端口的转发流量的状态就不会受网络环境的影响，比较稳定。
- 动态聚合模式：能够根据对端和本端的信息调整端口的转发流量的状态，比较灵活。

1.3 PPPoE

PPPoE（Point-to-Point Protocol over Ethernet，在以太网上承载 PPP 协议）的提出，解决了 PPP 无法应用于以太网的问题，是对 PPP 协议的扩展。

1.3.1 PPPoE概述

PPPoE 描述了在以太网上建立 PPPoE 会话及封装 PPP 报文的方法。要求通信双方建立的是点到点关系，而不是在以太网中所出现的点到多点关系。

PPPoE 利用以太网将大量主机组成网络，然后通过一个远端接入设备为以太网上的主机提供互联网接入服务，并对接入的每台主机实现控制、认证、计费功能。由于很好地结合了以太网的经济性及 PPP 良好的可扩展性与管理控制功能，PPPoE 被广泛应用于小区接入组网等环境中。

PPPoE 协议将 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。关于 PPPoE 的详细介绍，可以参考 RFC 2516。

1.3.2 PPPoE组网结构

说明

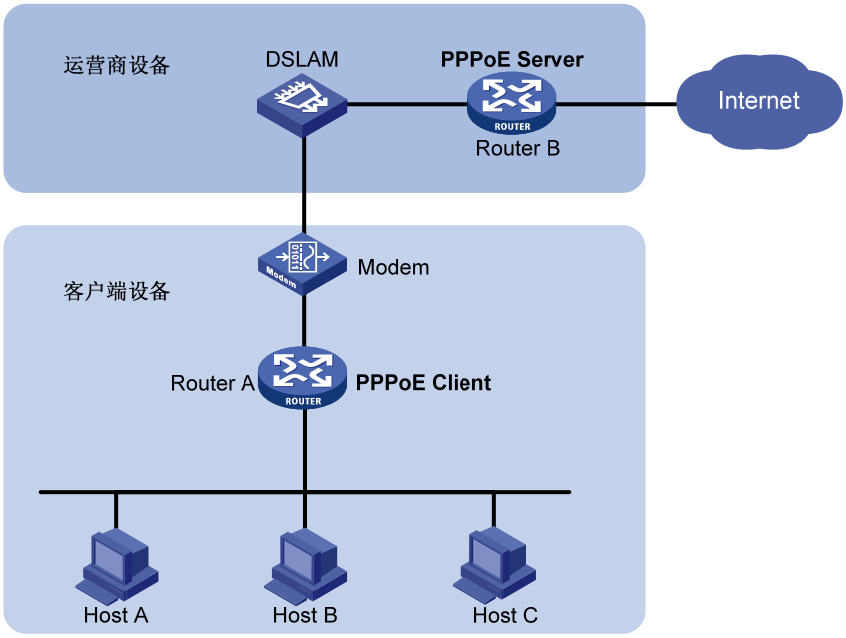
目前设备作为 PPPoE Client 接入网络。

PPPoE 使用 Client/Server 模型。PPPoE Client 向 PPPoE Server 发起连接请求，两者之间会话协商通过后，就建立 PPPoE 会话，此后 PPPoE Server 向 PPPoE Client 提供接入控制、认证、计费等功能。

常见组网如下：

在两台路由器之间建立 PPPoE 会话，所有主机通过同一个 PPPoE 会话传送数据，主机上不用安装 PPPoE 客户端拨号软件，一般是一个企业共用一个账号接入网络（图中 PPPoE Client 位于企业/公司内部，PPPoE Server 是运营商的设备）。

图1-5 PPPoE 组网结构图



1.4 VLAN

VLAN（Virtual Local Area Network，虚拟局域网）技术可以把一个物理 LAN 划分成多个逻辑的 LAN——VLAN，每个 VLAN 是一个广播域。处于同一 VLAN 的主机能够直接互通，而处于不同 VLAN 的主机不能够直接互通。

1.4.1 基于端口划分VLAN

VLAN 可以基于端口进行划分。它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，端口就可以转发该 VLAN 的报文。

在某 VLAN 内，可根据需要配置端口加入 Untagged 端口列表或 Tagged 端口列表（即配置端口为 Untagged 端口或 Tagged 端口），从 Untagged 端口发出的该 VLAN 报文不带 VLAN Tag，从 Tagged 端口发出的该 VLAN 报文带 VLAN Tag。

端口的链路类型分为三种。在端口加入某 VLAN 时，对不同链路类型的端口加入的端口列表要求不同：

- Access：端口只能发送一个 VLAN 的报文，发出去的报文不带 VLAN Tag。该端口只能加入一个 VLAN 的 Untagged 端口列表。
- Trunk：端口能发送多个 VLAN 的报文，发出去的端口缺省 VLAN 的报文不带 VLAN Tag，其他 VLAN 的报文都必须带 VLAN Tag。在端口缺省 VLAN 中，该端口只能加入 Untagged 端口列表；在其他 VLAN 中，该端口只能加入 Tagged 端口列表。
- Hybrid：端口能发送多个 VLAN 的报文，端口发出去的报文可根据需要配置某些 VLAN 的报文带 VLAN Tag，某些 VLAN 的报文不带 VLAN Tag。在不同 VLAN 中，该端口可以根据需要加入 Untagged 端口列表或 Tagged 端口列表。

1.4.2 VLAN接口

不同VLAN间的主机不能直接通信，通过设备上的VLAN接口，可以实现VLAN间的三层互通。VLAN接口是一种三层的虚拟接口，它不作为物理实体存在于设备上。每个 VLAN 对应一个 VLAN 接口，VLAN 接口的 IP 地址可作为本 VLAN 内网络设备的网关地址，对需要跨网段的报文进行基于 IP 地址的三层转发。

1.5 MAC

MAC（Media Access Control，媒体访问控制）地址表记录了 MAC 地址与接口的对应关系，以及接口所属的 VLAN 等信息。设备在转发报文时，根据报文的目的 MAC 地址查询 MAC 地址表，如果MAC地址表中包含与报文目的MAC地址对应的表项，则直接通过该表项中的出接口转发该报文；如果 MAC 地址表中没有包含报文目的 MAC 地址对应的表项时，设备将采取广播的方式通过对应 VLAN 内除接收接口外的所有接口转发该报文。

1.5.1 MAC地址表分类

MAC 地址表项分为以下几种：

- 动态 MAC 地址表项：可以由用户手工配置，也可以由设备通过源 MAC 地址学习自动生成，用于目的是某个 MAC 地址的报文从对应接口转发出去，表项有老化时间。手工配置的动态 MAC 地址表项优先级等于自动生成的 MAC 地址表项。
- 静态 MAC 地址表项：由用户手工配置，用于目的是某个 MAC 地址的报文从对应接口转发出去，表项不老化。静态 MAC 地址表项优先级高于自动生成的 MAC 地址表项。

1.5.2 MAC地址表项老化时间

MAC 地址表中自动生成的表项并非永远有效，每一条表项都有一个生存周期，这个生存周期被称作老化时间。配置动态 MAC 地址表项的老化时间后，超过老化时间的动态 MAC 地址表项会被自动删除，设备将重新进行 MAC 地址学习，构建新的动态 MAC 地址表项。如果在到达生存周期前某表项被刷新，则重新计算该表项的老化时间。

用户配置的老化时间过长或者过短，都可能影响设备的运行性能：

- 如果用户配置的老化时间过长，设备可能会保存许多过时的 MAC 地址表项，从而耗尽 MAC 地址表资源，导致设备无法根据网络的变化更新 MAC 地址表。
- 如果用户配置的老化时间太短，设备可能会删除有效的 MAC 地址表项，导致设备广播大量的数据报文，增加网络的负担。

用户需要根据实际情况，配置合适的老化时间。如果网络比较稳定，可以将老化时间配置得长一些或者配置为不老化；否则，可以将老化时间配置得短一些。比如在一个比较稳定的网络，如果长时间没有流量，动态 MAC 地址表项会被全部删除，可能导致设备突然广播大量的数据报文，造成安全隐患，此时可将动态 MAC 地址表项的老化时间设得长一些或不老化，以减少广播，增加网络稳定性和安全性。动态 MAC 地址表项的老化时间作用于全部接口上。

1.5.3 接口MAC地址学习

缺省情况下，MAC 地址学习功能处于开启状态。有时为了保证设备的安全，需要关闭 MAC 地址学习功能。常见的危及设备安全的情况是：非法用户使用大量源 MAC 地址不同的报文攻击设备，导致设备 MAC 地址表资源耗尽，造成设备无法根据网络的变化更新 MAC 地址表。关闭 MAC 地址学习功能可以有效防止这种攻击。在开启全局的 MAC 地址学习功能的前提下，用户可以关闭单个接口的 MAC 地址的学习功能。

如果MAC地址表过于庞大，可能导致设备的转发性能下降。通过配置接口的MAC地址数学习上限，用户可以控制设备维护的 MAC 地址表的表项数量。当接口学习到的 MAC 地址数达到上限时，该接口将不再对 MAC 地址进行学习，同时，用户还可以根据需要选择是否允许系统转发源 MAC 不在 MAC 地址表里的报文。

1.6 STP

生成树协议运行于二层网络中，通过阻塞冗余链路构建出无数据环路的树型网络拓扑，并在设备或数据链路故障时，重新计算出新的树型拓扑。

生成树协议包括 STP、RSTP、PVST 和 MSTP。

- STP：由 IEEE 制定的 802.1D 标准定义，是狭义的生成树协议。
- RSTP：由 IEEE 制定的 802.1w 标准定义，它在 STP 基础上进行了改进，实现了网络拓扑的快速收敛。其“快速”体现在，当一个端口被选为根端口和指定端口后，其进入转发状态的延时将大大缩短，从而缩短了网络最终达到拓扑稳定所需要的时间。
- PVST：PVST 为每个 VLAN 维护一个单独的生成树实例。每个 VLAN 都将运行单个生成树，允许以每个 VLAN 为基础开启或关闭生成树。每个 VLAN 内的生成树实例都有单独的网络拓扑结构，相互之间没有影响。
- MSTP：由 IEEE 制定的 802.1s 标准定义，它可以弥补 STP 和 RSTP 的缺陷，既可以快速收敛，也能使不同 VLAN 的流量沿各自的路径转发，从而为冗余链路提供了更好的负载分担机制。

1.6.1 生成树工作模式

生成树的工作模式有以下几种：

- STP 模式：设备的所有端口都将向外发送 STP BPDU。如果端口的对端设备只支持 STP，可选择此模式。
- RSTP 模式：设备的所有端口都向外发送 RSTP BPDU。当端口收到对端设备发来的 STP BPDU 时，会自动迁移到 STP 模式；如果收到的是 MSTP BPDU，则不会进行迁移。
- PVST 模式：对于 Access 端口，PVST 将根据该 VLAN 的状态发送 RSTP 格式的 BPDU。对于 Trunk 端口和 Hybrid 端口，PVST 将在缺省 VLAN 内根据该 VLAN 的状态发送 RSTP 格式的 BPDU，而对于其他本端口允许通过的 VLAN，则发送 PVST 格式的 BPDU。
- MSTP 模式：设备的所有端口都向外发送 MSTP BPDU。当端口收到对端设备发来的 STP BPDU 时，会自动迁移到 STP 模式；如果收到的是 RSTP BPDU，则不会进行迁移。

1.6.2 MSTP基本概念

MSTP 把一个交换网络划分成多个域，这些域称为 MST（Multiple Spanning Tree Regions，多生成树域）域。每个域内形成多棵生成树，各生成树之间彼此独立并分别与相应的 VLAN 对应，每棵生成树都称为一个 MSTI（Multiple Spanning Tree Instance，多生成树实例）。CST（Common Spanning Tree，公共生成树）是一棵连接交换网络中所有 MST 域的单生成树。IST（Internal Spanning Tree，内部生成树）是 MST 域内的一棵生成树，它是一个特殊的 MSTI，通常也称为 MSTI 0，所有 VLAN 缺省都映射到 MSTI 0 上。CIST（Common and Internal Spanning Tree，公共和内部生成树）是一棵连接交换网络内所有设备的单生成树，所有 MST 域的 IST 再加上 CST 就共同构成了整个交换网络的一棵完整的单生成树。

其中，对于属于同一 MST 域的设备具有下列特点：

- 都使能了生成树协议。
- 域名相同。
- VLAN 与 MSTI 间映射关系的配置相同。
- MSTP 修订级别的配置相同。
- 这些设备之间有物理链路连通。

1.6.3 生成树端口角色

生成树可能涉及到的端口角色有以下几种：

- 根端口（Root Port）：在非根桥上负责向根桥方向转发数据的端口就称为根端口，根桥上没有根端口。
- 指定端口（Designated Port）：负责向下游网段或设备转发数据的端口就称为指定端口。
- 替换端口（Alternate Port）：是根端口或主端口的备份端口。当根端口或主端口被阻塞后，替换端口将成为新的根端口或主端口。
- 备份端口（Backup Port）：是指定端口的备份端口。当指定端口失效后，备份端口将转换为新的指定端口。当使能了生成树协议的同一台设备上的两个端口互相连接而形成环路时，设备会将其中一个端口阻塞，该端口就是备份端口。
- 主端口（Master Port）：是将 MST 域连接到总根的端口（主端口不一定在域根上），位于整个域到总根的最短路径上。主端口是 MST 域中的报文去往总根的必经之路。主端口在 IST/CIST 上的角色是根端口，而在其他 MSTI 上的角色则是主端口。

STP 只涉及根端口、指定端口和替换端口三种端口角色，RSTP 的端口角色中新增了备份端口，MSTP 涉及所有的端口角色。

1.6.4 生成树端口状态

RSTP和MSTP中的端口状态可分为三种，如 表 1-2 所示。

表1-2 RSTP 和 MSTP 中的端口状态

状态	描述
Forwarding	该状态下的端口可以接收和发送BPDU，也转发用户流量
Learning	是一种过渡状态，该状态下的端口可以接收和发送BPDU，但不转发用户流量

状态	描述
Discarding	该状态下的端口可以接收和发送BPDU，但不转发用户流量

STP 定义了五种端口状态：Disabled、Blocking、Listening、Learning 和 Forwarding。其中 Disabled、Blocking 和 Listening 状态都对应 RSTP/MSTP 中的 Discarding 状态。

1.7 路由表

实现了对路由表的查看，包括路由表的概要信息和统计信息。

1.8 静态路由

静态路由是一种特殊的路由，由管理员手工配置。当网络结构比较简单时，只需配置静态路由就可以使网络正常工作。静态路由不能自动适应网络拓扑结构的变化，当网络发生故障或者拓扑发生变化后，必须由管理员手工修改配置。

缺省路由是在没有找到匹配的路由表项时使用的路由。配置 IPv4 缺省路由时，指定目的地址为 0.0.0.0/0；配置 IPv6 缺省路由时，指定目的地址为::/0。

1.9 IP

1.9.1 IP地址分类和表示

IP 地址是每个连接到 IPv4 网络上的设备的唯一标识。IP 地址长度为 32 比特，通常采用点分十进制方式表示，即每个 IP 地址被表示为以小数点隔开的 4 个十进制整数，每个整数对应一个字节，如 10.1.1.1。

IP 地址由两部分组成：

- 网络号码字段（Net-id）：用于区分不同的网络。网络号码字段的前几位称为类别字段（又称为类别比特），用来区分 IP 地址的类型。
- 主机号码字段（Host-id）：用于区分一个网络内的不同主机。

IP地址分为 5 类，每一类地址范围如 表 1-3 所示。目前大量使用的IP地址属于A、B、C三类。

表1-3 IP 地址分类

地址类型	地址范围	说明
A	0.0.0.0～127.255.255.255	IP地址0.0.0.0仅用于主机在系统启动时进行临时通信，并且永远不是有效目的地址 127.0.0.0网段的地址都保留作环回测试，发送到这个地址的分组不会输出到链路上，它们被当作输入分组在内部进行处理
B	128.0.0.0～191.255.255.255	-
C	192.0.0.0～223.255.255.255	-
D	224.0.0.0～239.255.255.255	组播地址
E	240.0.0.0～255.255.255.255	255.255.255.255用于广播地址，其它地址保留今后使用

1.9.2 子网和掩码

随着 Internet 的快速发展，IP 地址已近枯竭。为了充分利用已有的 IP 地址，可以使用子网掩码将网络划分为更小的部分（即子网）。通过从主机号码字段部分划出一些比特位作为子网号码字段，能够将一个网络划分为多个子网。子网号码字段的长度由子网掩码确定。

子网掩码是一个长度为 32 比特的数字，由一串连续的“1”和一串连续的“0”组成。“1”对应于网络号码字段和子网号码字段，而“0”对应于主机号码字段。

多划分出一个子网号码字段会浪费一些 IP 地址。例如，一个 B 类地址可以容纳 65534（2^{16}-2，去掉主机号码字段全 1 的广播地址和主机号码字段全 0 的网段地址）个主机号码。但划分出 9 比特长的子网字段后，最多可有 512（2^9）个子网，每个子网有 7 比特的主机号码，即每个子网最多可有 126（2^7-2，去掉主机号码字段全 1 的广播地址和主机号码字段全 0 的网段地址）个主机号码。因此主机号码的总数是 512*126=64512 个，比不划分子网时要少 1022 个。

若不进行子网划分，则子网掩码为默认值，此时子网掩码中“1”的长度就是网络号码的长度，即 A、B、C 类 IP 地址对应的子网掩码默认值分别为 255.0.0.0、255.255.0.0 和 255.255.255.0。

1.9.3 IP地址的配置方式

接口获取 IP 地址有以下几种方式：

- 通过手动指定 IP 地址
- 通过 DHCP 分配得到 IP 地址

1.9.4 接口MTU

当设备收到一个报文后，如果发现报文长度比转发接口的 MTU 值大，则进行下列处理：

- 如果报文不允许分片，则将报文丢弃；
- 如果报文允许分片，则将报文进行分片转发。

为了减轻转发设备在传输过程中的分片和重组数据包的压力，更高效的利用网络资源，请根据实际组网环境设置合适的接口 MTU 值，以减少分片的发生。

1.10 IPv6

IPv6（Internet Protocol Version 6，互联网协议版本 6）是网络层协议的第二代标准协议，也被称为 IPng（IP Next Generation，下一代互联网协议），它是 IETF（Internet Engineering Task Force，互联网工程任务组）设计的一套规范，是 IPv4 的升级版本。IPv6 和 IPv4 之间最显著的区别为：地址的长度从 32 比特增加到 128 比特。

1.10.1 IPv6 地址表示方式

IPv6 地址被表示为以冒号（:）分隔的一连串 16 比特的十六进制数。每个 IPv6 地址被分为 8 组，每组的 16 比特用 4 个十六进制数来表示，组和组之间用冒号隔开，比如：2001:0000:130F:0000:0000:09C0:876A:130B。

为了简化 IPv6 地址的表示，对于 IPv6 地址中的“0”可以有下面的处理方式：

- 每组中的前导“0”可以省略，即上述地址可写为 2001:0:130F:0:0:9C0:876A:130B。
- 如果地址中包含一组或连续多组均为 0 的组，则可以用双冒号“::”来代替，即上述地址可写为 2001:0:130F::9C0:876A:130B。

IPv6 地址由两部分组成：地址前缀与接口标识。其中，地址前缀相当于 IPv4 地址中的网络号码字段部分，接口标识相当于 IPv4 地址中的主机号码部分。

地址前缀的表示方式为：IPv6 地址/前缀长度。其中，前缀长度是一个十进制数，表示 IPv6 地址最左边多少位为地址前缀。

1.10.2 IPv6 地址分类

IPv6 主要有三种类型的地址：单播地址、组播地址和任播地址。

- 单播地址：用来唯一标识一个接口，类似于 IPv4 的单播地址。发送到单播地址的数据报文将被传送给此地址所标识的接口。
- 组播地址：用来标识一组接口（通常这组接口属于不同的节点），类似于 IPv4 的组播地址。发送到组播地址的数据报文被传送给此地址所标识的所有接口。
- 任播地址：用来标识一组接口（通常这组接口属于不同的节点）。发送到任播地址的数据报文被传送给此地址所标识的一组接口中距离源节点最近（根据使用的路由协议进行度量）的一个接口。

IPv6 中没有广播地址，广播地址的功能通过组播地址来实现。

IPv6 地址类型是由地址前面几位（称为格式前缀）来指定的，主要地址类型与格式前缀的对应关系如 表 1-4 所示。

表1-4 IPv6 地址类型与格式前缀的对应关系

地址类型		格式前缀（二进制）	IPv6 前缀标识	简介
单播地址	未指定地址	00...0 (128 bits)	::/128	不能分配给任何节点。在节点获得有效的IPv6地址之前，可在发送的IPv6报文的源地址字段填入该地址，但不能作为IPv6报文中的目的地址
	环回地址	00...1 (128 bits)	::1/128	不能分配给任何物理接口。它的作用与在IPv4中的环回地址相同，即节点用来给自己发送IPv6报文
	链路本地地址	1111111010	FE80::/10	用于邻居发现协议和无状态自动配置中链路本地上节点之间的通信。使用链路本地地址作为源或目的地址的数据报文不会被转发到其他链路上
	全球单播地址	其他形式	-	等同于IPv4公网地址，提供给网络服务提供商。这种类型的地址允许路由前缀的聚合，从而限制了全球路由表项的数量
组播地址		11111111	FF00::/8	-
任播地址		从单播地址空间中进行分配，使用单播地址的格式		-

1.10.3 IEEE EUI-64 生成接口标识

IPv6 单播地址中的接口标识符用来唯一标识链路上的一个接口。目前 IPv6 单播地址基本上都要求接口标识符为 64 位。

不同接口的 IEEE EUI-64 格式的接口标识符的生成方法不同，分别介绍如下：

- 所有 IEEE 802 接口类型（例如，以太网接口、VLAN 接口）：IEEE EUI-64 格式的接口标识符是从接口的链路层地址（MAC 地址）变化而来的。IPv6 地址中的接口标识符是 64 位，而 MAC 地址是 48 位，因此需要在 MAC 地址的中间位置（从高位开始的第 24 位后）插入十六进制数 FFFE（1111111111111110）。为了使接口标识符的作用范围与原 MAC 地址一致，还要将 Universal/Local (U/L)位（从高位开始的第 7 位）进行取反操作。最后得到的这组数就作为 EUI-64 格式的接口标识符。
- Tunnel 接口：IEEE EUI-64 格式的接口标识符的低 32 位为 Tunnel 接口的源 IPv4 地址，ISATAP 隧道的接口标识符的高 32 位为 0000:5EFE，其他隧道的接口标识符的高 32 位为全 0。
- 其他接口类型（例如，Serial 接口）：IEEE EUI-64 格式的接口标识符由设备随机生成。

1.10.4 接口上全球单播地址的配置方法

IPv6 全球单播地址可以通过下面几种方式配置：

- 采用 EUI-64 格式形成：当配置采用 EUI-64 格式形成 IPv6 地址时，接口的 IPv6 地址的前缀需要手工配置，而接口标识符则由接口自动生成。
- 手工配置：用户手工配置 IPv6 全球单播地址。
- 无状态自动配置：根据接收到的 RA 报文中携带的地址前缀信息及使用 EUI-64 功能生成的接口标识，自动为接口生成 IPv6 全球单播地址。
- 有状态获取地址：通过 DHCPv6 服务器自动获取 IPv6 地址。

一个接口上可以配置多个全球单播地址。

1.10.5 接口上链路本地地址的配置方法

IPv6 的链路本地地址可以通过两种方式获得：

- 自动生成：设备根据链路本地地址前缀（FE80::/10）及使用 EUI-64 功能生成的接口标识，自动为接口生成链路本地地址。
- 手工指定：用户手工配置 IPv6 链路本地地址。

每个接口只能有一个链路本地地址，为了避免链路本地地址冲突，推荐使用链路本地地址的自动生成方式。

配置链路本地地址时，手工指定方式的优先级高于自动生成方式。即如果先采用自动生成方式，之后手工指定，则手工指定的地址会覆盖自动生成的地址；如果先手工指定，之后采用自动生成的方式，则自动配置不生效，接口的链路本地地址仍是手工指定的。此时，如果删除手工指定的地址，则自动生成的链路本地地址会生效。

1.11 NAT

NAT（Network Address Translation，网络地址转换）是将 IP 数据报文头中的 IP 地址转换为另一个 IP 地址的过程。在实际应用中，NAT 主要应用在连接两个网络的边缘设备上，用于实现允许内部网络用户访问外部公共网络以及允许外部公共网络访问部分内部网络资源（例如内部服务器）的目的。NAT 最初的设计目的是实现私有网络访问公共网络的功能，后扩展为实现任意两个网络间进行访问时的地址转换应用。

1.11.1 动态转换

动态地址转换是指内部网络和外部网络之间的地址映射关系在建立连接的时候动态产生。该方式通常适用于内部网络有大量用户需要访问外部网络的组网环境。动态地址转换存在两种转换模式：

- NO-PAT 模式

NO-PAT（Not Port Address Translation）模式下，一个外网地址同一时间只能分配给一个内网地址进行地址转换，不能同时被多个内网地址共用。当使用某外网地址的内网用户停止访问外网时，NAT 会将其占用的外网地址释放并分配给其他内网用户使用。

该模式下，NAT 设备只对报文的 IP 地址进行 NAT 转换，同时会建立一个 NO-PAT 表项用于记录 IP 地址映射关系，并可支持所有 IP 协议的报文。

- PAT 模式

PAT（Port Address Translation）模式下，一个 NAT 地址可以同时分配给多个内网地址共用。该模式下，NAT 设备需要对报文的 IP 地址和传输层端口同时进行转换，且只支持 TCP、UDP 和 ICMP（Internet Control Message Protocol，因特网控制消息协议）查询报文。

采用 PAT 方式可以更加充分地利用 IP 地址资源，实现更多内部网络主机对外部网络的同时访问。

1.11.2 内部服务器

在实际应用中，内网中的服务器可能需要对外部网络提供一些服务，例如给外部网络提供 Web 服务，或是 FTP 服务。这种情况下，NAT 设备允许外网用户通过指定的 NAT 地址和端口访问这些内部服务器，NAT 内部服务器的配置就定义了 NAT 地址和端口与内网服务器地址和端口的映射关系。NAT 内部服务器支持以下几种内网和外网的地址、端口映射关系。

表1-5 NAT 内部服务器的地址与端口映射关系

外网	内网
一个外网地址	一个内网地址
一个外网地址、一个端口号	一个内网地址、一个内网端口号
一个外网地址，N个连续的外网端口号	一个内网地址，一个内网端口
	N个连续的内网地址，一个内网端口号
	一个内网地址，N个连续的内网端口号
N个连续的外网地址	一个内网地址
	N个连续的内网地址
N个连续的外网地址连续，一个外网端口号	一个内网地址，一个内网端口号

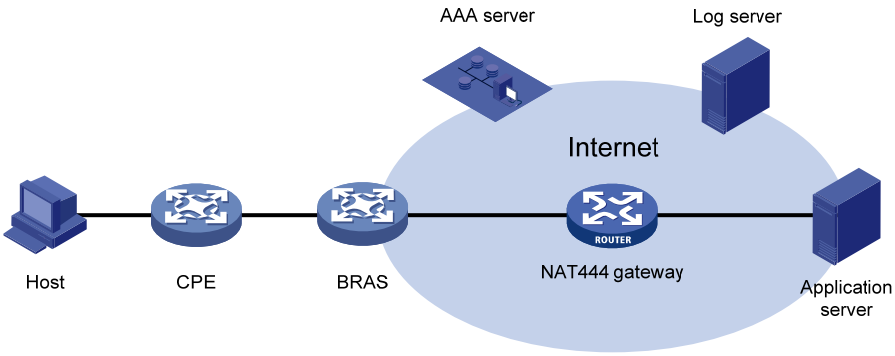
外网	内网
	N个连续的内网地址，一个内网端口号
	一个内网地址，N个连续的内网端口号
一个外网地址，一个外网端口号	一个内部服务器组
一个外网地址，N个连续的外网端口号	
N个连续的外网地址，一个外网端口号	

1.11.3 NAT 444 地址转换

NAT444 是运营商网络部署 NAT 的整体解决方案，它基于 NAT444 网关，结合 AAA 服务器、日志服务器等配套系统，提供运营商级的 NAT，并支持用户溯源等功能。在众多 IPv4 向 IPv6 网络过渡的技术中，NAT444 仅需在运营商侧引入二次 NAT，对终端和应用服务器端的更改较小，并且 NAT444 通过端口块分配方式解决用户溯源等问题，因此成为了运营商的首选 IPv6 过渡方案。

NAT444 解决方案的架构如 图 1-6 所示。

图1-6 NAT444 解决方案架构



- CPE：实现用户侧地址转换。
- BRAS：负责接入终端，并配合 AAA 完成用户认证、授权和计费。
- NAT444 网关：实现运营商级地址转换。
- AAA 服务器：负责用户认证、授权和计费等。
- 日志服务器：接受和记录用户访问信息，响应用户访问信息查询。

NAT444 网关设备进行的地址转换（以下称为“NAT444 地址转换”）是一种 PAT 方式的动态地址转换，但与普通 PAT 方式动态地址转换不同的是，NAT444 地址转换是基于端口块（即一个端口范围）的方式来复用公网 IP 地址的，即一个私网 IP 地址在一个时间段内独占一个公网 IP 地址的某个端口块。例如：假设私网 IP 地址 10.1.1.1 独占公网 IP 地址 202.1.1.1 的一个端口块 10001～10256，则该私网 IP 向公网发起的所有连接，源 IP 地址都将被转换为同一个公网 IP 地址 202.1.1.1，而源端口将被转换为端口块 10001～10256 之内的一个端口。

1. NAT444 静态转换

NAT444 静态地址转换是指，NAT 网关设备根据配置自动计算私网 IP 地址到公网 IP 地址、端口块的静态映射关系，并创建静态端口块表项。当私网 IP 地址成员中的某个私网 IP 地址向公网发起新建连接时，根据私网 IP 地址匹配静态端口块表项，获取对应的公网 IP 地址和端口块，并从端口块中动态为其分配一个公网端口，对报文进行地址转换。

配置 NAT444 静态地址转换时，需要创建一个端口块组，并在端口块组中配置私网 IP 地址成员、公网 IP 地址成员、端口范围和端口块大小。假设端口块组中每个公网 IP 地址的可用端口块数为 m（即端口范围除以端口块大小），则端口块静态映射的算法如下：按照从小到大的顺序对私网 IP 地址成员中的所有 IP 地址进行排列，最小的 m 个私网 IP 地址对应最小的公网 IP 地址及其端口块，端口块按照起始端口号从小到大的顺序分配；次小的 m 个私网 IP 地址对应次小的公网 IP 地址及其端口块，端口块的分配顺序相同；依次类推。

2. NAT444 动态转换

NAT444 动态地址转换融合了普通 NAT 动态地址转换和 NAT444 静态地址转换的特点。当内网用户向公网发起连接时，首先根据动态地址转换中的 ACL 规则进行过滤，决定是否需要进行源地址转换。对于需要进行源地址转换的连接，当该连接为该用户的首次连接时，从所匹配的动态地址转换配置引用的 NAT 地址组中获取一个公网 IP 地址，从该公网 IP 地址中动态分配一个端口块，创建动态端口块表项，然后从端口块表项中动态分配一个公网端口，进行地址转换。对该用户后续连接的转换，均从生成的动态端口块表项中分配公网端口。当该用户的所有连接都断开时，回收为其分配的端口块资源，删除相应的动态端口块表项。

NAT444 动态地址转换支持增量端口块分配。当为某私网 IP 地址分配的端口块资源耗尽（端口块中的所有端口都被使用）时，如果该私网 IP 地址向公网发起新的连接，则无法再从端口块中获取端口，无法进行地址转换。此时，如果预先在相应的 NAT 地址组中配置了增量端口块数，则可以为该私网 IP 地址分配额外的端口块，进行地址转换。

1.11.4 高级设置

1. NAT地址组

一个 NAT 地址组是多个地址组成员的集合。当需要对到达外部网络的数据报文进行地址转换时，报文的源地址将被转换为地址组成员中的某个地址。

2. NAT444 地址组

NAT444 地址组与 NAT 地址组的配置基本相同，所不同的是，NAT444 地址组必须配置端口块参数（端口范围、端口块大小和增量端口块数）以实现基于端口块的 NAT444 地址转换。

3. 端口块组

配置 NAT444 端口块静态映射需要创建一个端口块组，并在接口的出方向上应用该端口块组。端口块组中需要配置私网 IP 地址成员、公网 IP 地址成员、端口范围和端口块大小，系统会根据端口块组中的配置自动计算私网 IP 地址到公网 IP 地址、端口块的静态映射关系，创建静态端口块表项，并根据表项进行 NAT444 地址转换。

4. 服务器组

在配置内部服务器时，将内部服务器的内网信息指定为一个内部服务器组，组内的多台主机可以共同对外提供某种服务。外网用户向内部服务器指定的外网地址发起应用请求时，NAT 设备可根据内

网服务器的权重和当前连接数，选择其中一台内网服务器作为目的服务器，实现内网服务器负载分担。

5. PAT方式地址转换模式

目前，PAT 支持两种不同的地址转换模式：

- Endpoint-Independent Mapping（不关心对端地址和端口转换模式）：只要是来自相同源地址和源端口号的报文，不论其目的地址是否相同，通过 PAT 映射后，其源地址和源端口号都被转换为同一个外部地址和端口号，该映射关系会被记录下来并生成一个 EIM 表项；并且 NAT 设备允许所有外部网络的主机通过该转换后的地址和端口来访问这些内部网络的主机。这种模式可以很好的支持位于不同 NAT 网关之后的主机进行互访。
- Address and Port-Dependent Mapping（关心对端地址和端口转换模式）：对于来自相同源地址和源端口号的报文，相同的源地址和源端口号并不要求被转换为相同的外部地址和端口号，若其目的地址或目的端口号不同，通过 PAT 映射后，相同的源地址和源端口号通常会被转换成不同的外部地址和端口号。与 Endpoint-Independent Mapping 模式不同的是，NAT 设备只允许这些目的地址对应的外部网络的主机可以通过该转换后的地址和端口来访问这些内部网络的主机。这种模式安全性好，但由于同一个内网主机地址转换后的外部地址不唯一，因此不便于位于不同 NAT 网关之后的主机使用内网主机转换后的地址进行互访。

6. DNS映射

通过配置 DNS 映射，可以在 DNS 服务器位于外网的情况下，实现内网用户可通过域名访问位于同一内网的内部服务器的功能。DNS 映射功能需要和内部服务器配合使用，由内部服务器对外提供服务的外网 IP 地址和端口号，由 DNS 映射建立“内部服务器域名<-->外网 IP 地址+外网端口号+协议类型”的映射关系。

NAT 设备对来自外网的 DNS 响应报文进行 DNS ALG 处理时，由于载荷中只包含域名和应用服务器的外网 IP 地址（不包含传输协议类型和端口号），当接口上存在多条 NAT 服务器配置且使用相同的外网地址而内网地址不同时，DNS ALG 仅使用 IP 地址来匹配内部服务器可能会得到错误的匹配结果。因此需要借助 DNS 映射的配置，指定域名与应用服务器的外网 IP 地址、端口和协议的映射关系，由域名获取应用服务器的外网 IP 地址、端口和协议，进而（在当前 NAT 接口上）精确匹配内部服务器配置获取应用服务器的内网 IP 地址。

7. NAT Hairpin

通过在内网侧接口上使能 NAT hairpin 功能，可以实现内网用户使用 NAT 地址访问内网服务器或内网其它用户。NAT hairpin 功能需要与内部服务器、出方向动态地址转换或出方向静态地址转换配合工作，且这些配置所在的接口必须在同一个接口板，否则 NAT hairpin 功能无法正常工作。

该功能在不同工作方式下的具体转换过程如下：

- C/S 方式：NAT 在内网接口上同时转换访问内网服务器的报文的源和目的 IP 地址，其中，目的 IP 地址转换通过匹配某外网接口上的内部服务器配置来完成，源地址转换通过匹配内部服务器所在接口上的出方向动态地址转换或出方向静态地址转换来完成。
- P2P 方式：内网各主机首先向外网服务器注册自己的内网地址信息，该地址信息为外网侧出方向地址转换的 NAT 地址，然后内网主机之间通过使用彼此向外网服务器注册的外网地址进行互访。该方式下，外网侧的出方向地址转换必须配置为 PAT 转换方式，并使能 EIM 模式。

8. 开启NAT ALG功能

通过开启指定应用协议类型的 ALG 功能，实现对应用层报文数据载荷字段的分析和 NAT 处理。

9. NAT日志

(1) NAT 会话日志

NAT 会话日志是为了满足网络管理员安全审计的需要，对 NAT 会话（报文经过设备时，源或目的信息被 NAT 进行过转换的连接）信息进行的记录，包括 IP 地址及端口的转换信息、用户的访问信息以及用户的网络流量信息。

有三种情况可以触发设备生成 NAT 会话日志：

- 新建 NAT 会话。
- 删除 NAT 会话。新增高优先级的配置、删除配置、报文匹配规则变更、NAT 会话老化以及执行删除 NAT 会话的命令时，都可能导致 NAT 会话被删除。
- 存在 NAT 活跃流。NAT 活跃流是指在一定时间内存在的 NAT 会话。当设置的生成活跃流日志的时间间隔到达时，当前存在的 NAT 会话信息就被记录并生成日志。

(2) NAT444 日志

NAT444 日志分为 NAT444 用户日志和 NAT444 告警信息日志。

NAT444 用户日志是为了满足互联网用户溯源的需要，在 NAT444 地址转换中，对每个用户的私网 IP 地址进行端口块分配或回收时，都会输出一条基于用户的日志，记录私网 IP 地址和端口块的映射关系。在进行用户溯源时，只需根据报文的公网 IP 地址和端口找到对应的端口块分配日志信息，即可确定私网 IP 地址。

有两种情况可以触发设备输出 NAT444 用户日志：

- 端口块分配：端口块静态映射方式下，在某私网 IP 地址的第一个新建连接通过端口块进行地址转换时输出日志；端口块动态映射方式下，在为某私网 IP 地址分配端口块或增量端口块时输出日志。
- 端口块回收：端口块静态映射方式下，在某私网 IP 地址的最后一个连接拆除时输出日志；端口块动态映射方式下，在释放端口块资源（并删除端口块表项）时输出日志。

在 NAT444 地址转换中，如果可为用户分配的公网 IP 地址、端口块或端口块中的端口都被占用，则该用户的后续连接由于没有可用的资源无法对其进行地址转换，相应的报文将被丢弃。为了监控公网 IP 地址和端口块资源的使用情况，可以对端口用满和资源用满两种情况记录告警信息日志。

- 端口用满告警：在私网 IP 地址对应的端口块中的所有端口都被占用的情况下，输出告警信息日志。对于端口块动态映射方式，如果配置了增量端口块分配，则当首次分配的端口块中的端口都被占用时，并不输出日志；只有当增量端口块中的端口也都被占用时，才会输出日志。
- 资源用满告警：在 NAT444 端口块动态映射中，如果所有资源（公网 IP 地址、端口块）都被占用，则输出日志。

1.11.5 注意事项

- 入方向的静态地址转换通常用于与接口上的出方向动态地址转换、内部服务器或出方向静态地址转换配合以实现双向 NAT，不建议单独配置。
- 若接口上同时存在普通 NAT 静态地址转换、普通 NAT 动态地址转换、NAT444 端口块静态映射、NAT444 端口块动态映射和内部服务器的配置，则在地址转换过程中，它们的优先级从高到低依次为：内部服务器；普通 NAT 静态地址转换；NAT444 端口块静态映射；NAT444 动态转换和普通 NAT 动态地址转换，系统对二者不做区分，统一按照 ACL 编号由大到小的顺序匹配。

- 各地址组成员的 IP 地址段不能互相重叠。
- 配置的所有地址组成员包含的地址总数不能少于安全引擎（或安全插卡）的数量。
- 内部服务器组成员按照权重比例对外提供服务，权重值越大的内部服务器组成员对外提供服务的比重越大。
- 在配置 NAT444 日志功能前，必须先配置将用户定制日志发送到日志主机的功能，否则无法产生 NAT444 告警信息日志。

1.12 DHCP

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请求分配网络配置参数的申请，服务器返回为客户端分配的 IP 地址等配置信息，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）。如果 DHCP 客户端和 DHCP 服务器处于不同物理网段时，客户端可以通过 DHCP 中继与服务器通信，获取 IP 地址及其他配置信息。

1.12.1 DHCP服务器

在以下场合通常利用 DHCP 服务器来完成 IP 地址分配：

- 网络规模较大，手工配置需要很大的工作量，并难以对整个网络进行集中管理。
- 网络中主机数目大于该网络支持的 IP 地址数量，无法给每个主机分配一个固定的 IP 地址。例如，Internet 接入服务提供商限制同时接入网络的用户数目，用户必须动态获得自己的 IP 地址。
- 网络中只有少数主机需要固定的 IP 地址，大多数主机没有固定的 IP 地址需求。

DHCP 服务器通过地址池来保存为客户端分配的 IP 地址、租约时长、网关信息、域名后缀、DNS 服务器地址、WINS 服务器地址、NetBIOS 节点类型和 DHCP 选项信息。服务器接收到客户端发送的请求后，选择合适的地址池，并将该地址池中的信息分配给客户端。

DHCP 服务器在将 IP 地址分配给客户端之前，还需要进行 IP 地址冲突检测。

1. DHCP地址池

地址池的地址管理方式有以下几种：

- 静态绑定 IP 地址，即通过将客户端的硬件地址或客户端 ID 与 IP 地址绑定的方式，实现为特定的客户端分配特定的 IP 地址。
- 动态选择 IP 地址，即在地址池中指定可供分配的 IP 地址范围，当收到客户端的 IP 地址申请时，从该地址范围中动态选择 IP 地址，分配给该客户端。

在 DHCP 地址池中还可以指定这两种类型地址的租约时长。

DHCP 服务器为客户端分配 IP 地址时，地址池的选择原则如下：

(1) 如果存在将客户端 MAC 地址或客户端 ID 与 IP 地址静态绑定的地址池，则选择该地址池，并将静态绑定的 IP 地址和其他网络参数分配给客户端。

(2) 如果不存在静态绑定的地址池，则按照以下方法选择地址池：

- 如果客户端与服务器在同一网段，则将 DHCP 请求报文接收接口的 IP 地址与所有地址池配置的网段进行匹配，并选择最长匹配的网段所对应的地址池。
- 如果客户端与服务器不在同一网段，即客户端通过 DHCP 中继获取 IP 地址，则将 DHCP 请求报文中 giaddr 字段指定的 IP 地址与所有地址池配置的网段进行匹配，并选择最长匹配的网段所对应的地址池。

2. DHCP服务器分配IP地址的次序

DHCP 服务器为客户端分配 IP 地址的优先次序如下：

(1) 与客户端 MAC 地址或客户端 ID 静态绑定的 IP 地址。

(2) DHCP 服务器记录的曾经分配给客户端的 IP 地址。

(3) 客户端发送的 DHCP-DISCOVER 报文中 Option 50 字段指定的 IP 地址。Option 50 为客户端请求的 IP 地址选项（Requested IP Address），客户端通过在 DHCP-DISCOVER 报文中添加该选项来指明客户端希望获取的 IP 地址。该选项的内容由客户端决定。

(4) 按照动态分配地址选择原则，顺序查找可供分配的 IP 地址，选择最先找到的 IP 地址。

(5) 如果未找到可用的 IP 地址，则从当前匹配地址池中依次查询租约过期、曾经发生过冲突的 IP 地址，如果找到则进行分配，否则将不予处理。

3. DHCP选项

DHCP 利用选项字段传递控制信息和网络配置参数，实现地址动态分配的同时，为客户端提供更加丰富的网络配置信息。

Web 页面为 DHCP 服务器提供了灵活的选项配置方式，在以下情况下，可以使用 Web 页面 DHCP 选项功能：

- 随着 DHCP 的不断发展，新的 DHCP 选项会陆续出现。通过该功能，可以方便地添加新的 DHCP 选项。
- 有些选项的内容，RFC 中没有统一规定。厂商可以根据需要定义选项的内容，如 Option 43。通过 DHCP 选项功能，可以为 DHCP 客户端提供厂商指定的信息。
- Web 页面只提供了有限的配置功能，其他功能可以通过 DHCP 选项来配置。例如，可以通过 Option 4，IP 地址 1.1.1.1 来指定为 DHCP 客户端分配的时间服务器地址为 1.1.1.1。
- 扩展已有的 DHCP 选项。当前已提供的方式无法满足用户需求时（比如通过 Web 页面最多只能配置 8 个 DNS 服务器地址，如果用户需要配置的 DNS 服务器地址数目大于 8，则 Web 页面无法满足需求），可以通过 DHCP 选项功能进行扩展。

常用的DHCP选项配置如 表 1-6 所示。

表1-6 常用 DHCP 选项配置

选项编号	选项名称	推荐的选项填充类型
3	Router Option	IP地址
6	Domain Name Server Option	IP地址
15	Domain Name	ASCII字符串
44	NetBIOS over TCP/IP Name Server Option	IP地址
46	NetBIOS over TCP/IP Node Type Option	十六进制数串
66	TFTP server name	ASCII字符串

选项编号	选项名称	推荐的选项填充类型
67	Bootfile name	ASCII字符串
43	Vendor Specific Information	十六进制数串

4. DHCP服务器的IP地址冲突检测功能

为防止 IP 地址重复分配导致地址冲突，DHCP 服务器为客户端分配地址前，需要先对该地址进行探测。

DHCP 服务器的地址探测是通过 ping 功能实现的，通过检测是否能在指定时间内得到 ping 响应来判断是否存在地址冲突。DHCP 服务器发送目的地址为待分配地址的 ICMP 回显请求报文。如果在指定时间内收到回显响应报文，则认为存在地址冲突。DHCP 服务器从地址池中选择新的 IP 地址，并重复上述操作。如果在指定时间内没有收到回显响应报文，则继续发送 ICMP 回显请求报文，直到发送的回显显示报文数目达到最大值。如果仍然没有收到回显响应报文，则将地址分配给客户端，从而确保客户端获得的 IP 地址唯一。

1.12.2 DHCP中继

由于在 IP 地址动态获取过程中采用广播方式发送请求报文，因此 DHCP 只适用于 DHCP 客户端和服务器处于同一个子网内的情况。为进行动态主机配置，需要在所有网段上都设置一个 DHCP 服务器，这显然是很不经济的。

DHCP 中继功能的引入解决了这一难题：客户端可以通过 DHCP 中继与其他网段的 DHCP 服务器通信，最终获取到 IP 地址。这样，多个网络上的 DHCP 客户端可以使用同一个 DHCP 服务器，既节省了成本，又便于进行集中管理。

1. DHCP中继用户地址表项记录功能

为了防止非法主机静态配置一个 IP 地址并访问外部网络，设备支持 DHCP 中继用户地址表项记录功能。

启用该功能后，当客户端通过 DHCP 中继从 DHCP 服务器获取到 IP 地址时，DHCP 中继可以自动记录客户端 IP 地址与硬件地址的绑定关系，生成 DHCP 中继的用户地址表项。

本功能与其他 IP 地址安全功能（如 ARP 地址检查和授权 ARP）配合，可以实现只允许匹配用户地址表项中绑定关系的报文通过 DHCP 中继。从而，保证非法主机不能通过 DHCP 中继与外部网络通信。

2. DHCP中继动态用户地址表项定时刷新功能

DHCP 客户端释放动态获取的 IP 地址时，会向 DHCP 服务器单播发送 DHCP-RELEASE 报文，DHCP 中继不会处理该报文的内容。如果此时 DHCP 中继上记录了该 IP 地址与 MAC 地址的绑定关系，则会造成 DHCP 中继的用户地址表项无法实时刷新。为了解决这个问题，DHCP 中继支持动态用户地址表项的定时刷新功能。

DHCP 中继动态用户地址表项定时刷新功能开启时，DHCP 中继每隔指定时间采用客户端获取到的 IP 地址和 DHCP 中继接口的 MAC 地址向 DHCP 服务器发送 DHCP-REQUEST 报文：

- 如果 DHCP 中继接收到 DHCP 服务器响应的 DHCP-ACK 报文或在指定时间内没有接收到 DHCP 服务器的响应报文，则表明这个 IP 地址已经可以进行分配，DHCP 中继会删除动态用

户地址表中对应的表项。为了避免地址浪费，DHCP 中继收到 DHCP-ACK 报文后，会发送 DHCP-RELEASE 报文释放申请到的 IP 地址。

- 如果 DHCP 中继接收到 DHCP 服务器响应的 DHCP-NAK 报文，则表示该 IP 地址的租约仍然存在，DHCP 中继不会删除该 IP 地址对应的表项。

1.13 DHCP Snooping

DHCP Snooping 是 DHCP 的一种安全特性，具有如下功能：

1. 保证客户端从合法的服务器获取IP地址

网络中如果存在私自架设的非法 DHCP 服务器，则可能导致 DHCP 客户端获取到错误的 IP 地址和网络配置参数，从而无法正常通信。为了使 DHCP 客户端能通过合法的 DHCP 服务器获取 IP 地址，DHCP Snooping 安全机制允许将端口设置为信任端口和不信任端口：

- 信任端口正常转发接收到的 DHCP 报文。
- 不信任端口接收到 DHCP 服务器响应的 DHCP-ACK 和 DHCP-OFFER 报文后，丢弃该报文。

在 DHCP Snooping 设备上指向 DHCP 服务器方向的端口需要设置为信任端口，其他端口设置为不信任端口，从而保证 DHCP 客户端只能从合法的 DHCP 服务器获取 IP 地址，私自架设的伪 DHCP 服务器无法为 DHCP 客户端分配 IP 地址。

2. 记录DHCP Snooping表项

DHCP Snooping 通过监听 DHCP-REQUEST 报文和信任端口收到的 DHCP-ACK 报文，记录 DHCP Snooping 表项，其中包括客户端的 MAC 地址、DHCP 服务器为 DHCP 客户端分配的 IP 地址、与 DHCP 客户端连接的端口及 VLAN 等信息。利用这些信息可以实现 ARP Detection 功能，即根据 DHCP Snooping 表项来判断发送 ARP 报文的用户是否合法，从而防止非法用户的 ARP 攻击。

3. 备份DHCP Snooping表项

DHCP Snooping 设备重启后，设备上记录的 DHCP Snooping 表项将丢失。如果 DHCP Snooping 与其他模块配合使用，则表项丢失会导致这些模块无法通过 DHCP Snooping 获取到相应的表项，进而导致 DHCP 客户端不能顺利通过安全检查、正常访问网络。

DHCP Snooping 表项备份功能将 DHCP Snooping 表项保存到指定的文件中，DHCP Snooping 设备重启后，自动根据该文件恢复 DHCP Snooping 表项，从而保证 DHCP Snooping 表项不会丢失。

4. 支持Option 82 功能

Option 82 记录了 DHCP 客户端的位置信息。管理员可以利用该选项定位 DHCP 客户端，实现对客户端的安全和计费等控制。Option 82 包含两个子选项：Circuit ID 和 Remote ID。

支持 Option 82 功能是指设备接收到 DHCP 请求报文后，根据报文中是否包含 Option 82 以及用户配置的处理策略及填充模式等对报文进行相应的处理，并将处理后的报文转发给 DHCP 服务器。当设备接收到 DHCP 服务器的响应报文时，如果报文中含有 Option 82，则删除 Option 82，并转发给 DHCP 客户端；如果报文中不含有 Option 82，则直接转发。

具体的处理方式见 表 1-7。

表1-7 Option 82 处理方式

收到 DHCP 请求报文	处理策略	DHCP Snooping 对报文的处理
收到的报文中带有Option 82	Drop	丢弃报文
	Keep	保持报文中的Option 82不变并进行转发
	Replace	根据DHCP Snooping上配置的填充模式、内容、格式等填充Option 82，替换报文中原有的Option 82并进行转发
收到的报文中不带有Option 82	-	根据DHCP Snooping上配置的填充模式、内容、格式等填充Option 82，添加到报文中并进行转发

1.14 DNS

DNS（Domain Name System，域名系统）是一种用于 TCP/IP 应用程序的分布式数据库，提供域名与地址之间的转换。IPv4 DNS 提供域名和 IPv4 地址之间的转换，IPv6 DNS 提供域名和 IPv6 地址之间的转换。

设备作为 DNS 客户端，当用户在设备上进行某些应用（如 Telnet 到一台设备或主机）时，可以直接使用便于记忆的、有意义的域名，通过域名系统将域名解析为正确的地址。

域名解析分为动态域名解析和静态域名解析两种。动态域名解析和静态域名解析可以配合使用。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。由于动态域名解析需要域名服务器的配合，会花费一定的时间，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。

1.14.1 动态域名解析

使用动态域名解析时，需要手工指定域名服务器的地址。

动态域名解析通过向域名服务器查询域名和地址之间的对应关系来实现将域名解析为地址。

动态域名解析支持域名后缀列表功能。用户可以预先设置一些域名后缀，在域名解析的时候，用户只需要输入域名的部分字段，系统会自动将输入的域名加上不同的后缀进行解析。例如，用户想查询域名 aabbcc.com，那么可以先在后缀列表中配置 com，然后输入 aabbcc 进行查询，系统会自动将输入的域名与后缀连接成 aabbcc.com 进行查询。

使用域名后缀的时候，根据用户输入域名方式的不同，查询方式分成以下几种情况：

- 如果用户输入的域名中没有“.”，比如 aabbcc，系统认为这是一个主机名，会首先加上域名后缀进行查询，如果所有加后缀的域名查询都失败，将使用最初输入的域名（如 aabbcc）进行查询。
- 如果用户输入的域名中间有“.”，比如 www.aabbcc，系统直接用它进行查询，如果查询失败，再依次加上各个域名后缀进行查询。
- 如果用户输入的域名最后有“.”，比如 aabbcc.com.，表示不需要进行域名后缀添加，系统直接用输入的域名进行查询，不论成功与否都直接返回结果。就是说，如果用户输入的字符中最后一个字符为“.”，就只根据用户输入的字符进行查找，而不会去匹配用户预先设置的域名后缀，因此最后这个“.”，也被称为查询终止符。带有查询终止符的域名，称为 FQDN（Fully Qualified Domain Name，完全合格域名）。

1.14.2 静态域名解析

手工建立域名和地址之间的对应关系。当用户使用域名进行某些应用时，系统查找静态域名解析表，从中获取指定域名对应的地址。

1.14.3 DNS代理

DNS 代理（DNS proxy）用来在 DNS client 和 DNS server 之间转发 DNS 请求和应答报文。局域网内的 DNS client 把 DNS proxy 当作 DNS server，将 DNS 请求报文发送给 DNS proxy。DNS proxy 将该请求报文转发到真正的 DNS server，并将 DNS server 的应答报文返回给 DNS client，从而实现域名解析。

使用 DNS proxy 功能后，当 DNS server 的地址发生变化时，只需改变 DNS proxy 上的配置，无需改变局域网内每个 DNS client 的配置，从而简化了网络管理。

1.15 动态DNS

DNS 仅仅提供了域名和地址之间的静态对应关系，当节点的地址发生变化时，DNS 无法动态地更新域名和地址的对应关系。此时，如果仍然使用域名访问该节点，通过域名解析得到的地址是错误的，从而导致访问失败。

DDNS（Dynamic Domain Name System，动态域名系统）用来动态更新 DNS 服务器上域名和地址之间的对应关系，保证通过域名解析到正确的地址。

使用 DDNS 服务前，用户需要先登录 DDNS 服务器，注册账户。设备作为 DDNS 客户端，在地址变化时，向 DDNS 服务器发送更新域名和地址对应关系的 DDNS 更新请求，更新请求中携带用户的账户信息（用户名和密码）。DDNS 服务器对账户信息认证通过后，通知 DNS 服务器动态更新域名和地址之间的对应关系。

目前，只有 IPv4 域名解析支持 DDNS，IPv6 域名解析不支持 DDNS，即只能通过 DDNS 动态更新域名和 IPv4 地址之间的对应关系。

为了简化配置，设备通过 DDNS 策略来管理和维护 DDNS 客户端的参数，如 DDNS 服务提供商信息（即 DDNS 服务器信息）、用户的账户信息（用户名和密码）、更新时间间隔、关联的 SSL 客户端策略等。创建 DDNS 策略后，可以在不同的接口上应用相同的 DDNS 策略，从而简化 DDNS 的配置。

1.16 IPv6 DNS

DNS（Domain Name System，域名系统）是一种用于 TCP/IP 应用程序的分布式数据库，提供域名与地址之间的转换。IPv4 DNS 提供域名和 IPv4 地址之间的转换，IPv6 DNS 提供域名和 IPv6 地址之间的转换。

设备作为 DNS 客户端，当用户在设备上进行某些应用（如 Telnet 到一台设备或主机）时，可以直接使用便于记忆的、有意义的域名，通过域名系统将域名解析为正确的地址。

域名解析分为动态域名解析和静态域名解析两种。动态域名解析和静态域名解析可以配合使用。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。由于动态域名解析需要域名服务器的配合，会花费一定的时间，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。

1.16.1 动态域名解析

使用动态域名解析时，需要手工指定域名服务器的地址。

动态域名解析通过向域名服务器查询域名和地址之间的对应关系来实现将域名解析为地址。

动态域名解析支持域名后缀列表功能。用户可以预先设置一些域名后缀，在域名解析的时候，用户只需要输入域名的部分字段，系统会自动将输入的域名加上不同的后缀进行解析。例如，用户想查询域名 aabbcc.com，那么可以先在后缀列表中配置 com，然后输入 aabbcc 进行查询，系统会自动将输入的域名与后缀连接成 aabbcc.com 进行查询。

使用域名后缀的时候，根据用户输入域名方式的不同，查询方式分成以下几种情况：

- 如果用户输入的域名中没有“.”，比如 aabbcc，系统认为这是一个主机名，会首先加上域名后缀进行查询，如果所有加后缀的域名查询都失败，将使用最初输入的域名（如 aabbcc）进行查询。
- 如果用户输入的域名中间有“.”，比如 www.aabbcc，系统直接用它进行查询，如果查询失败，再依次加上各个域名后缀进行查询。
- 如果用户输入的域名最后有“.”，比如 aabbcc.com.，表示不需要进行域名后缀添加，系统直接用输入的域名进行查询，不论成功与否都直接返回结果。就是说，如果用户输入的字符中最后一个字符为“.”，就只根据用户输入的字符进行查找，而不会去匹配用户预先设置的域名后缀，因此最后这个“.”，也被称为查询终止符。带有查询终止符的域名，称为 FQDN（Fully Qualified Domain Name，完全合格域名）。

1.16.2 静态域名解析

手工建立域名和地址之间的对应关系。当用户使用域名进行某些应用时，系统查找静态域名解析表，从中获取指定域名对应的地址。

1.16.3 DNS代理

DNS 代理（DNS proxy）用来在 DNS client 和 DNS server 之间转发 DNS 请求和应答报文。局域网内的 DNS client 把 DNS proxy 当作 DNS server，将 DNS 请求报文发送给 DNS proxy。DNS proxy 将该请求报文转发到真正的 DNS server，并将 DNS server 的应答报文返回给 DNS client，从而实现域名解析。

使用 DNS proxy 功能后，当 DNS server 的地址发生变化时，只需改变 DNS proxy 上的配置，无需改变局域网内每个 DNS client 的配置，从而简化了网络管理。

1.17 IGMP Snooping

IGMP snooping（Internet Group Management Protocol snooping，互联网组管理协议窥探）运行在二层设备上，通过侦听三层设备与接收者主机间的 IGMP 报文建立 IGMP snooping 转发表，并根据该表指导组播数据的转发。

IGMP snooping 转发表的表项由 VLAN、组播组地址、组播源地址和成员端口四个元素构成，其中成员端口是指二层设备上朝向组播组成员的端口。

1.18 MLD Snooping

MLD snooping（Multicast Listener Discovery snooping，组播侦听者发现协议窥探）运行在二层设备上，通过侦听三层设备与接收者主机间的 MLD 报文建立 MLD snooping 转发表，并根据该表指导 IPv6 组播数据的转发。

MLD snooping 转发表的表项由 VLAN、IPv6 组播组地址、IPv6 组播源地址和成员端口四个元素构成，其中成员端口是指二层设备上朝向 IPv6 组播组成员的端口。

1.19 ARP

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。

设备通过 ARP 协议解析到目的 MAC 地址后，将会在自己的 ARP 表中增加 IP 地址和 MAC 地址映射关系的表项，以用于后续到同一目的地报文的转发。

ARP 表项分为两种：动态 ARP 表项、静态 ARP 表项。

1.19.1 动态ARP表项

动态 ARP 表项由 ARP 协议通过 ARP 报文自动生成和维护，可以被老化，可以被新的 ARP 报文更新，可以被静态 ARP 表项覆盖。当到达老化时间、接口状态 down 时，系统会删除相应的动态 ARP 表项。

动态 ARP 表项可以固化为静态 ARP 表项，但被固化后无法再恢复为动态 ARP 表项。

为了防止部分接口下的用户占用过多的 ARP 资源，可以通过设置接口学习动态 ARP 表项的最大个数来进行限制。

1.19.2 静态ARP表项

静态 ARP 表项通过手工创建或由动态 ARP 表项固化而来，不会被老化，不会被动态 ARP 表项覆盖。

配置静态 ARP 表项可以增加通信的安全性。静态 ARP 表项可以限制和指定 IP 地址的设备通信时只使用指定的 MAC 地址，此时攻击报文无法修改此表项的 IP 地址和 MAC 地址的映射关系，从而保护了本设备和指定设备间的正常通信。

在配置静态 ARP 表项时，如果管理员希望用户使用某个固定的 IP 地址和 MAC 地址通信，可以将该 IP 地址与 MAC 地址绑定；如果进一步希望限定用户只在指定 VLAN 的特定接口上连接，则需要进一步指定报文转发的 VLAN 和出接口。

一般情况下，ARP 动态执行并自动寻求 IP 地址到以太网 MAC 地址的解析，无需管理员的介入。

说明

当静态 ARP 表项中的 IP 地址与 VLAN 虚接口的 IP 地址属于同一网段时，该静态 ARP 表项才能正常指导转发。

1.19.3 代理ARP

如果 ARP 请求是从一个网络的主机发往同一网段却不在同一物理网络上的另一台主机，那么连接它们的具有代理 ARP 功能的设备就可以回答该请求，这个过程称作代理 ARP。

代理 ARP 功能屏蔽了分离的物理网络这一事实，使用户使用起来，好像在同一个物理网络上。

代理 ARP 分为普通代理 ARP 和本地代理 ARP，二者的应用场景有所区别：

- 普通代理 ARP：想要互通的主机分别连接到设备的不同三层接口上，且这些主机不在同一个广播域中。
- 本地代理 ARP：想要互通的主机连接到设备的同一个三层接口上，且这些主机不在同一个广播域中。

在配置本地代理 ARP 时，用户也可以指定进行 ARP 代理的 IP 地址范围。

1.19.4 免费ARP

免费 ARP 报文是一种特殊的 ARP 报文，该报文中携带的发送端 IP 地址和目标 IP 地址都是本机 IP 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 地址是否与本机的 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 报文通知其它设备更新 ARP 表项。

1. 学习免费ARP报文功能

启用了学习免费 ARP 报文功能后，设备会根据收到的免费 ARP 报文中携带的信息（发送端 IP 地址、发送端 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 报文中的发送端 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。

关闭学习免费 ARP 报文功能后，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，可以关闭学习免费 ARP 报文功能，以节省 ARP 表项资源。

2. 回复免费ARP报文功能

开启回复免费 ARP 报文功能后，当设备收到非同一网段的 ARP 请求时发送免费 ARP 报文。关闭该功能后，设备收到非同一网段的 ARP 请求时不发送免费 ARP 报文。

3. 接口定时发送免费ARP报文功能

用户可以配置某些接口定时发送免费 ARP 报文，以便及时通知下行设备更新 ARP 表项或者 MAC 地址表项，主要应用场景如下：

- 防止仿冒网关的 ARP 攻击

如果攻击者仿冒网关发送免费 ARP 报文，就可以欺骗同网段内的其它主机，使得被欺骗的主机访问网关的流量被重定向到一个错误的 MAC 地址，导致其它主机用户无法正常访问网络。

为了降低这种仿冒网关的 ARP 攻击所带来的影响，可以在网关的接口上启用定时发送免费 ARP 功能。启用该功能后，网关接口上将按照配置的时间间隔周期性发送接口主 IP 地址和手工配置的从 IP 地址的免费 ARP 报文。这样，每台主机都可以学习到正确的网关，从而正常访问网络。

- 防止主机 ARP 表项老化

在实际环境中，当网络负载较大或接收端主机的 CPU 占用率较高时，可能存在 ARP 报文被丢弃或主机无法及时处理接收到的 ARP 报文等现象。这种情况下，接收端主机的动态 ARP 表项会因超时而老化，在其重新学习到发送设备的 ARP 表项之前，二者之间的流量就会发生中断。

为了解决上述问题，可以在网关的接口上启用定时发送免费 ARP 功能。启用该功能后，网关接口上将按照配置的时间间隔周期性发送接口主 IP 地址和手工配置的从 IP 地址的免费 ARP 报文。这样，接收端主机可以及时更新 ARP 映射表，从而防止了上述流量中断现象。

1.19.5 ARP攻击防御

ARP 协议有简单、易用的优点，但是也因为其没有任何安全机制而容易被攻击发起者利用。目前 ARP 攻击和 ARP 病毒已经成为局域网安全的一大威胁，为了避免各种攻击带来的危害，设备提供了多种技术对攻击进行防范、检测和解决。

不同设备支持配置的 ARP 攻击防御功能如下：

- 网关设备支持配置的功能包括：ARP 黑洞路由、ARP 源抑制、源 MAC 地址一致性检查、ARP 主动确认、源 MAC 地址固定的 ARP 攻击检测、授权 ARP 和 ARP 扫描；
- 接入设备支持配置的功能包括：ARP 网关保护、ARP 过滤保护和 ARP Detection。

1. ARP防止IP报文攻击功能

如果网络中有主机通过向设备发送大量目标 IP 地址不能解析的 IP 报文来攻击设备，则会造成下面的危害：

- 设备向目的网段发送大量 ARP 请求报文，加重目的网段的负载。
- 设备会试图反复地对目标 IP 地址进行解析，增加了 CPU 的负担。

为避免这种 IP 报文攻击所带来的危害，设备提供了下列两个功能：

- ARP 黑洞路由功能：开启该功能后，一旦接收到目标 IP 地址不能解析的 IP 报文，设备立即产生一个黑洞路由，使得设备在一段时间内将去往该地址的报文直接丢弃。等待黑洞路由老化时间过后，如有报文触发则再次发起解析，如果解析成功则进行转发，否则仍然产生一个黑洞路由将去往该地址的报文丢弃。这种方式能够有效地防止 IP 报文的攻击，减轻 CPU 的负担。
- ARP 源抑制功能：如果发送攻击报文的源是固定的，可以采用 ARP 源抑制功能。开启该功能后，如果网络中每 5 秒内从某 IP 地址向设备某接口发送目的 IP 地址不能解析的 IP 报文超过了设置的阈值，则设备将不再处理由此 IP 地址发出的 IP 报文直至该 5 秒结束，从而避免了恶意攻击所造成的危害。

2. ARP报文源MAC地址一致性检查功能

ARP 报文源 MAC 地址一致性检查功能主要应用于网关设备上，防御以太网数据帧首部中的源 MAC 地址和 ARP 报文中的源 MAC 地址不同的 ARP 攻击。

配置本特性后，网关设备在进行 ARP 学习前将对 ARP 报文进行检查。如果以太网数据帧首部中的源 MAC 地址和 ARP 报文中的源 MAC 地址不同，则认为是攻击报文，将其丢弃；否则，继续进行 ARP 学习。

3. ARP主动确认功能

ARP 的主动确认功能主要应用于网关设备上，防止攻击者仿冒用户欺骗网关设备。

启用 ARP 主动确认功能后，设备在新建或更新 ARP 表项前需进行主动确认，防止产生错误的 ARP 表项。

使能严格模式后，新建 ARP 表项前，ARP 主动确认功能会执行更严格的检查：

- 收到目标 IP 地址为自己的 ARP 请求报文时，设备会发送 ARP 应答报文，但不建立 ARP 表项；
- 收到 ARP 应答报文时，需要确认本设备是否对该报文中的源 IP 地址发起过 ARP 解析：若发起过解析，解析成功后则设备启动主动确认功能，主动确认流程成功完成后，设备可以建立该表项；若未发起过解析，则设备丢弃该报文。

4. 源MAC地址固定的ARP攻击检测功能

本特性根据 ARP 报文的源 MAC 地址对上送 CPU 的 ARP 报文进行统计，在 5 秒内，如果收到同一源 MAC 地址（源 MAC 地址固定）的 ARP 报文超过一定的阈值，则认为存在攻击，系统会将此 MAC 地址添加到攻击检测表项中。在该攻击检测表项老化之前，如果设置的检查模式为过滤模式，则会打印日志信息并且将该源 MAC 地址发送的 ARP 报文过滤掉；如果设置的检查模式为监控模式，则只打印日志信息，不会将该源 MAC 地址发送的 ARP 报文过滤掉。

对于网关或一些重要的服务器，可能会发送大量 ARP 报文，为了使这些 ARP 报文不被过滤掉，可以将这类设备的 MAC 地址配置成保护 MAC 地址，这样，即使该设备存在攻击也不会被检测、过滤。

5. 授权ARP功能

所谓授权 ARP，就是动态学习 ARP 的过程中，只有和 DHCP 服务器生成的租约或 DHCP 中继生成的安全表项一致的 ARP 报文才能够被学习。

使能接口的授权 ARP 功能后，系统会禁止该接口学习动态 ARP 表项，可以防止用户仿冒其他用户的 IP 地址或 MAC 地址对网络进行攻击，保证只有合法的用户才能使用网络资源，增加了网络的安全性。

6. ARP扫描功能

启用 ARP 扫描功能后，设备会对局域网内的邻居自动进行扫描（向邻居发送 ARP 请求报文，获取邻居的 MAC 地址，从而建立动态 ARP 表项）。

ARP 扫描功能一般与 ARP 固化功能配合使用。ARP 固化功能用来将当前的 ARP 动态表项（包括 ARP 扫描生成的动态 ARP 表项）转换为静态 ARP 表项。通过对动态 ARP 表项的固化，可以有效防止攻击者修改 ARP 表项。

建议在网吧这种环境稳定的小型网络中使用这两个功能。

7. ARP网关保护功能

在设备上不与网关相连的接口上配置此功能，可以防止伪造网关攻击。

在接口上配置此功能后，当接口收到 ARP 报文时，将检查 ARP 报文的源 IP 地址是否和配置的被保护网关的 IP 地址相同。如果相同，则认为此报文非法，将其丢弃；否则，认为此报文合法，继续进行后续处理。

8. ARP过滤保护功能

ARP 过滤保护功能用来限制接口下允许通过的 ARP 报文，可以防止仿冒网关和仿冒用户的攻击。

在接口上配置此功能后，当接口收到 ARP 报文时，将检查 ARP 报文的源 IP 地址和源 MAC 地址是否和允许通过的 IP 地址和 MAC 地址相同：

- 如果相同，则认为此报文合法，继续进行后续处理；
- 如果不相同，则认为此报文非法，将其丢弃。

9. ARP Detection功能

ARP Detection 功能主要应用于接入设备上，对于合法用户的 ARP 报文进行正常转发，否则直接丢弃，从而防止仿冒用户、仿冒网关的攻击。

ARP Detection 包含三个功能：用户合法性检查、ARP 报文有效性检查、ARP 报文强制转发。

(1) 用户合法性检查

如果仅在 VLAN 上开启 ARP Detection 功能，则仅进行用户合法性检查。

对于 ARP 信任接口，不进行用户合法性检查；对于 ARP 非信任接口，需要进行用户合法性检查，以防止仿冒用户的攻击。

用户合法性检查是根据 ARP 报文中源 IP 地址和源 MAC 地址检查用户是否是所属 VLAN 所在接口上的合法用户，包括基于 IP Source Guard 静态绑定表项的检查、基于 DHCP Snooping 表项的检查。只要符合任何一个，就认为该 ARP 报文合法，进行转发。如果所有检查都没有找到匹配的表项，则认为是非法报文，直接丢弃。

(2) ARP 报文有效性检查

对于 ARP 信任接口，不进行报文有效性检查；对于 ARP 非信任接口，需要根据配置对 MAC 地址和 IP 地址不合法的报文进行过滤。可以选择配置源 MAC 地址、目的 MAC 地址或 IP 地址检查模式。

- 源 MAC 地址的检查模式：会检查 ARP 报文中的源 MAC 地址和以太网报文头中的源 MAC 地址是否一致，一致则认为有效，否则丢弃报文。
- 目的 MAC 地址的检查模式（只针对 ARP 应答报文）：会检查 ARP 应答报文中的目的 MAC 地址是否为全 0 或者全 1，是否和以太网报文头中的目的 MAC 地址一致。全 0、全 1、不一致的报文都是无效的，需要被丢弃。
- IP 地址检查模式：会检查 ARP 报文中的源 IP 或目的 IP 地址，如全 1、或者组播 IP 地址都是不合法的，需要被丢弃。对于 ARP 应答报文，源 IP 和目的 IP 地址都进行检查；对于 ARP 请求报文，只检查源 IP 地址。

(3) ARP 报文强制转发

对于从 ARP 信任接口接收到的 ARP 报文不受此功能影响，按照正常流程进行转发；对于从 ARP 非信任接口接收到的并且已经通过用户合法性检查的 ARP 报文的处理过程如下：

- 对于 ARP 请求报文，通过信任接口进行转发。
- 对于 ARP 应答报文，首先按照报文中的以太网目的 MAC 地址进行转发，若在 MAC 地址表中没有查到目的 MAC 地址对应的表项，则将此 ARP 应答报文通过信任接口进行转发。

1.20 ND

IPv6 邻居发现（Neighbor Discovery，ND）协议使用五种类型的ICMPv6 消息（如 表 1-8 所示），实现地址解析、验证邻居是否可达、重复地址检测、路由器发现/前缀发现、地址自动配置和重定向等功能。

表1-8 ND 使用的 ICMPv6 消息

ICMPv6 消息	类型号	作用
邻居请求消息NS（Neighbor	135	获取邻居的链路层地址

ICMPv6 消息	类型号	作用
Solicitation）		验证邻居是否可达
		进行重复地址检测
邻居通告消息NA（Neighbor Advertisement）	136	对NS消息进行响应
		节点在链路层变化时主动发送NA消息，向邻居节点通告本节点的变化信息
路由器请求消息RS（Router Solicitation）	133	节点启动后，通过RS消息向路由器发出请求，请求前缀和其他配置信息，用于节点的自动配置
路由器通告消息RA（Router Advertisement）	134	对RS消息进行响应
		在没有抑制RA消息发布的条件下，路由器会周期性地发布RA消息，其中包括前缀信息选项和一些标志位的信息
重定向消息（Redirect）	137	当满足一定的条件时，缺省网关通过向源主机发送重定向消息，使主机重新选择正确的下一跳地址进行后续报文的发送

1.20.1 邻居表项

邻居表项保存的是设备在链路范围内的邻居信息，设备邻居表项可以通过邻居请求消息 NS 及邻居通告消息 NA 来动态创建，也可以通过手工配置来静态创建。

目前，静态邻居表项有两种配置方式：

- 配置本节点的三层接口相连的邻居节点的 IPv6 地址和链路层地址。
- 配置本节点 VLAN 中的二层端口相连的邻居节点的 IPv6 地址和链路层地址。

对于 VLAN 接口，可以采用上述两种方式来配置静态邻居表项：

- 采用第一种方式配置静态邻居表项后，设备还需要解析该 VLAN 下的二层端口信息。
- 采用第二种方式配置静态邻居表项后，需要保证该二层端口属于指定的 VLAN，且该 VLAN 已经创建了 VLAN 接口。

1.20.2 RA报文

设备为同一链路上的主机发布 RA 报文，主机可以根据 RA 报文中的信息进行无状态自动配置等操作。设备可以抑制 RA 报文的发送，也可以周期性发送 RA 报文，相邻两次 RA 报文发送时间间隔是在最大时间间隔与最小时间间隔之间随机选取的一个值。最小时间间隔应该小于等于最大时间间隔的 0.75 倍。

RA报文中的参数和参数描述如 表 1-9 所示。

表1-9 RA 报文中的参数

参数	描述
地址前缀/前缀长度	主机根据该地址前缀/前缀长度生成对应的IPv6地址，完成无状态自动配置操作
有效生命期	表示前缀有效期。在有效生命期内，通过该前缀自动生成的地址可以正常使用；有效生命期过期后，通过该前缀自动生成的地址变为无效，将被删除

参数	描述
首选生命期	表示首选通过该前缀无状态自动配置地址的时间。首选生命期过期后，节点通过该前缀自动配置的地址将被废止。节点不能使用被废止的地址建立新的连接，但是仍可以接收目的地址为被废止地址的报文。首选生命期必须小于或等于有效生命期
不用于无状态配置标识	选择了该标识，则指定前缀不用于无状态地址配置
不是直连可达标识	选择了该标识，则表示该前缀不是当前链路上直连可达的
MTU	发布链路的MTU，可以用于确保同一链路上的所有节点采用相同的MTU值
不指定跳数限制标识	选择了该标识，则表示RA消息中不带有本设备的跳数限制
被管理地址配置标志位（M flag）	用于确定主机是否采用有状态自动配置获取IPv6地址 如果选择了该标志位，主机将通过有状态自动配置（例如DHCPv6服务器）来获取IPv6地址；否则，将通过无状态自动配置获取IPv6地址，即根据自己的链路层地址及路由器发布的前缀信息生成IPv6地址
其他信息配置标志位（O flag）	用于确定主机是否采用有状态自动配置获取除IPv6地址外的其他信息 如果选择了其他信息配置标志位，主机将通过有状态自动配置（例如DHCPv6服务器）来获取除IPv6地址外的其他信息；否则，将通过无状态自动配置获取其他信息
路由器生存时间（Router Lifetime）	用于设置发布RA消息的路由器作为主机的默认路由器的时间。主机根据接收到的RA消息中的路由器生存时间参数值，就可以确定是否将发布该RA消息的路由器作为默认路由器。发布RA消息中路由器生存时间为0的路由器不能作为默认路由器
邻居请求重传间隔（Retrans Timer）	设备发送NS消息后，如果未在指定的时间间隔内收到响应，则会重新发送NS消息
配置路由优先级 (Router Preference)	用于设置发布RA消息的路由器的路由器优先级，主机根据接收到的RA消息中的路由器优先级，可以选择优先级最高的路由器作为默认网关。在路由器的优先级相同的情况下，遵循“先来先用”的原则，优先选择先接收到的RA消息对应的发送路由器作为默认网关
保持邻居可达时间（Reachable Time）	当通过邻居可达性检测确认邻居可达后，在所设置的可达时间内，设备认为邻居可达；超过设置的时间后，如果需要向邻居发送报文，会重新确认邻居是否可达

1.20.3 ND代理功能

如果 NS 请求是从一个网络的主机发往同一网段却不在同一物理网络上的另一台主机，那么连接它们的具有代理功能的设备就可以代答该请求，回应 NA 报文，这个过程称作 ND 代理（ND Proxy）。

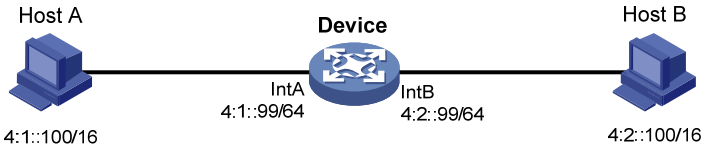
ND Proxy 功能屏蔽了分离的物理网络这一事实，使用户使用起来，好像在同一个物理网络上。

ND Proxy 功能根据应用场景不同分为普通 ND Proxy 和本地 ND Proxy。

1. 普通ND Proxy

普通ND Proxy的典型应用环境如 图 1-7 所示。Device通过两个三层接口Int A和Int B连接两个网络，两个三层接口的IPv6 地址不在同一个网段，接口地址分别为 4:1::99/64、4:2::99/64。但是两个网络内的主机Host A和Host B的地址通过掩码的控制，既与相连设备的接口地址在同一网段，同时二者也处于同一个网段。

图1-7 普通 ND 代理的典型应用环境



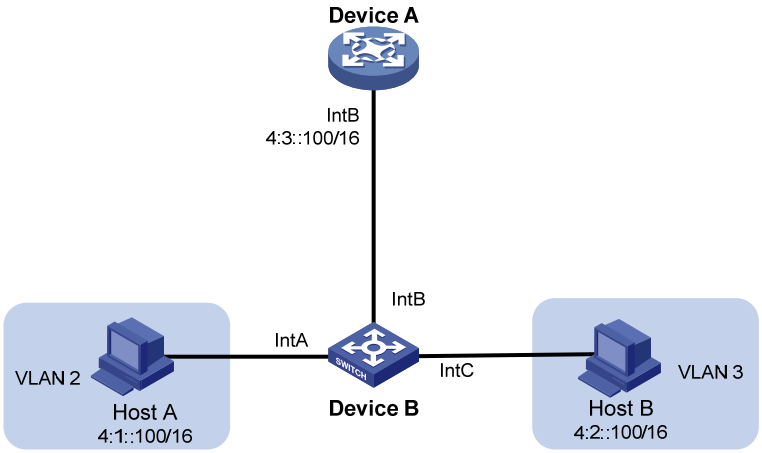
在这种组网情况下，当 Host A 需要与 Host B 通信时，由于目的 IPv6 地址与本机的 IPv6 地址为同一网段，因此 Host A 会直接发出请求 Host B 硬件地址的 NS 请求。但是，此时的两台主机处于不同的广播域中，Host B 无法收到 Host A 的 NS 请求报文，当然也就无法应答。

通过在 Device 上启用普通 ND Proxy 功能，可以解决此问题。在接口 Int A 和 Int B 上启用普通 ND Proxy 后，Router 可以应答 Host A 的 NS 请求。同时，Device 作为 Host B 的代理，把其它主机发送过来的报文转发给 Host B。这样，实现 Host A 与 Host B 之间的通信。

2. 本地ND Proxy

本地ND Proxy的应用场景如 图 1-8 所示。Host A属于VLAN 2，Host B属于VLAN 3，它们分别连接到端口Int A和Int C上。

图1-8 本地 ND 代理的应用场景



在这种组网情况下，当 Host A 需要与 Host B 通信时，由于目的 IPv6 地址与本机的 IPv6 地址为同一网段，因此 Host A 会直接发出请求 Host B 硬件地址的 NS 请求。但是，因为连接两台主机处于不同的 VLAN 中，Host B 无法收到 Host A 的 NS 请求报文。

通过在 Device A 上启用本地 ND Proxy 功能，可以解决此问题。在接口 Int B 上启用本地 ND Proxy 后，Device A 会代替 Host B 回应 NA，Host A 发给 Host B 的报文就会通过 Device A 进行转发，从而实现 Host A 与 Host B 之间的通信。

1.21 HTTP/HTTPS

为了方便用户对网络设备进行配置和维护，设备提供了 Web 登录功能。用户可以通过 PC 登录到设备上，使用 Web 界面直观地配置和维护设备。

设备支持的 Web 登录方式有以下两种：

- HTTP 登录方式：HTTP（Hypertext Transfer Protocol，超文本传输协议）用来在 Internet 上传递 Web 页面信息。目前，设备支持的 HTTP 协议版本为 HTTP/1.0。
- HTTPS 登录方式：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，能对客户端与设备之间交互的数据进行加密，能为设备制定基于证书属性的访问控制策略，提高了数据传输的安全性和完整性，保证合法客户端可以安全地访问设备，禁止非法客户端访问设备，从而实现了对设备的安全管理。

  采用 HTTPS 登录时，设备上只需使能 HTTPS 服务，用户即可通过 HTTPS 登录设备。此时，设备使用的证书为自签名证书，使用的 SSL 参数为各个参数的缺省值。（自签名证书指的是服务器自己生成的证书，无需从 CA 获取）

通过引用 ACL（Access Control List，访问控制列表），可以对访问设备的登录用户进行控制：

- 当未引用 ACL、引用的 ACL 不存在或者引用的 ACL 为空时，允许所有登录用户访问设备；
- 当引用的 ACL 非空时，则只有 ACL 中 permit 的用户才能访问设备，其它用户不允许访问设备，可以避免非法用户使用 Web 页面登录设备。

1.22 FTP

FTP 用于在 FTP 服务器和 FTP 客户端之间传输文件，是 IP 网络上传输文件的通用协议。本设备可作为 FTP 服务器，使用 20 端口传输数据，使用 21 端口传输控制消息。

1.23 Telnet

设备可以开启 Telnet 服务器功能，以便用户能够通过 Telnet 登录到设备进行远程管理和监控。

通过引用 ACL（Access Control List，访问控制列表），可以对访问设备的登录用户进行控制：

- 当未引用 ACL、引用的 ACL 不存在或者引用的 ACL 为空时，允许所有登录用户访问设备。
- 当引用的 ACL 非空时，则只有 ACL 中 permit 的用户才能访问设备，其它用户不允许访问设备，可以避免非法用户通过 Telnet 访问设备。

1.24 NTP

NTP（Network Time Protocol，网络时间协议）可以用来在分布式时间服务器和客户端之间进行时间同步，使网络内所有设备的时间保持一致，从而使设备能够提供基于统一时间的多种应用。

NTP 通过时钟层数来定义时钟的准确度。时钟层数的取值范围为 1～15，取值越小，时钟准确度越高。

在某些网络中，例如无法与外界通信的孤立网络，网络中的设备无法与权威时钟进行时间同步。此时，可以从该网络中选择一台时钟较为准确的设备，指定该设备与本地时钟进行时间同步，即采用本地时钟作为参考时钟，使得该设备的时钟处于同步状态。该设备作为时间服务器为网络中的其他设备提供时间同步，从而实现整个网络的时间同步。

通过 Web 页面可以配置本地时钟作为参考时钟。

1.25 LLDP

LLDP（Link Layer Discovery Protocol，链路层发现协议）提供了一种标准的链路层发现方式，可以将本端设备的信息（包括主要能力、管理地址、设备标识、接口标识等）组织成不同的 TLV（Type/Length/Value，类型/长度/值），并封装在 LLDPDU（Link Layer Discovery Protocol Data Unit，链路层发现协议数据单元）中发布给与自己直连的邻居，邻居收到这些信息后将其以标准 MIB（Management Information Base，管理信息库）的形式保存起来，以供网络管理系统查询及判断链路的通信状况。

1.25.1 LLDP代理

LLDP 代理是 LLDP 协议运行实体的一个抽象映射。一个接口下，可以运行多个 LLDP 代理。目前 LLDP 定义的代理类型包括：最近桥代理、最近非 TPMR 桥代理和最近客户桥代理。LLDP 在相邻的代理之间进行协议报文交互，并基于代理创建及维护邻居信息。

1.25.2 LLDP报文的发送机制

在指定类型 LLDP 代理下，当端口工作在 TxRx 或 Tx 模式时，设备会以报文发送时间间隔为周期，向邻居设备发送 LLDP 报文。如果设备的本地配置发生变化则立即发送 LLDP 报文，以将本地信息的变化情况尽快通知给邻居设备。但为了防止本地信息的频繁变化而引起 LLDP 报文的大量发送，可以配置限制发送报文速率的令牌桶大小来作限速处理。

当设备的工作模式由 Disable/Rx 切换为 TxRx/Tx，或者发现了新的邻居设备（即收到一个新的 LLDP 报文且本地尚未保存发送该报文设备的信息）时，该设备将自动启用快速发送机制，即将 LLDP 报文的发送周期设置为快速发送周期，并连续发送指定数量（快速发送 LLDP 报文的个数）的 LLDP 报文后再恢复为正常的发送周期。

1.25.3 LLDP报文的接收机制

当端口工作在 TxRx 或 Rx 模式时，设备会对收到的 LLDP 报文及其携带的 TLV 进行有效性检查，通过检查后再将邻居信息保存到本地，并根据 Time To Live TLV 中 TTL（Time To Live，生存时间）的值来设置邻居信息在本地设备上的老化时间，若该值为零，则立刻老化该邻居信息。

由于 TTL＝Min（65535，（TTL 乘数×LLDP 报文的发送间隔＋1）），即取 65535 与（TTL 乘数×LLDP 报文的发送间隔＋1）中的最小值，因此通过调整 TTL 乘数可以控制本设备信息在邻居设备上的老化时间。

1.25.4 端口初始化时间

当端口的 LLDP 工作模式发生变化时，端口将对协议状态机进行初始化操作。为了避免端口工作模式频繁改变而导致端口不断执行初始化操作，可配置端口初始化延迟时间，当端口工作模式改变时延迟一段时间再执行初始化操作。

1.25.5 LLDP Trap功能

如果开启了发送 LLDP Trap 功能，设备可以通过向网管系统发送 Trap 信息以通告如发现新的 LLDP 邻居、与原来邻居的通信链路发生故障等重要事件。

1.25.6 LLDP TLV

TLV 是组成 LLDP 报文的单元，每个 TLV 都代表一个信息。LLDP 可以封装的 TLV 包括基本 TLV、802.1 TLV、802.3 TLV 和 LLDP-MED（Link Layer Discovery Protocol Media Endpoint Discovery，链路层发现协议媒体终端发现） TLV。

基本 TLV 是网络设备管理基础的一组 TLV，802.1 TLV、802.3 TLV 和 LLDP-MED TLV 则是由标准组织或其他机构定义的 TLV，用于增强对网络设备的管理，可根据实际需要选择是否在 LLDPDU 中发送。

1.26 设置

1.26.1 日志信息等级

设备产生的日志信息按严重性可划分为如 表 1-10 所示的八个等级，各等级的严重性依照数值从 0～7 依次降低。

表1-10 日志信息等级列表

数值	信息等级	描述
0	emergency	表示设备不可用的信息，如系统授权已到期
1	alert	表示设备出现重大故障，需要立刻做出反应的信息，如流量超出接口上限
2	critical	表示严重信息，如设备温度已经超过预警值，设备电源、风扇出现故障等
3	error	表示错误信息，如接口链路状态变化等
4	warning	表示警告信息，如接口连接断开，内存耗尽告警等
5	notification	表示正常出现但是重要的信息，如通过终端登录设备，设备重启等
6	informational	表示需要记录的通知信息，如通过命令行输入命令的记录信息，执行**ping**命令的日志信息等
7	debugging	表示调试过程产生的信息

1.26.2 日志信息输出方向

系统可以向日志缓冲区（logbuffer）、日志主机（loghost）等方向发送日志信息。日志信息的各个输出方向相互独立，可在页面中分别设置。

2 网络安全

2.1 包过滤

包过滤是指采用 ACL 规则对接口、VLAN 或全局入方向或出方向的报文进行过滤，即对匹配上 ACL 规则的报文按照其中定义的匹配动作允许或拒绝通过，对未匹配上任何 ACL 规则的报文则按照指定的缺省动作进行处理。

2.2 QoS策略

QoS 即服务质量。对于网络业务，影响服务质量的因素包括传输的带宽、传送的时延、数据的丢包率等。在网络中可以通过保证传输的带宽、降低传送的时延、降低数据的丢包率以及时延抖动等措施来提高服务质量。

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，灵活地进行 QoS 配置。

2.2.1 类

类用来定义一系列的规则来对报文进行分类。

2.2.2 流行为

流行为用来定义针对报文所做的 QoS 动作。

2.2.3 策略

策略用来将指定的类和流行为绑定起来，对符合分类条件的报文执行流行为中定义的动作。

2.2.4 应用策略

QoS 策略支持以下应用方式：

- 基于接口应用 QoS 策略：QoS 策略对通过接口接收或发送的流量生效。接口的每个方向（出和入两个方向）只能应用一个策略。如果 QoS 策略应用在接口的出方向，则 QoS 策略对本地协议报文不起作用。一些常见的本地协议报文如下：链路维护报文等。
- 基于全局应用 QoS 策略：QoS 策略对所有流量生效。

2.3 优先级映射

报文在进入设备以后，设备会根据映射规则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，就可以获得决定报文调度能力的各种优先级字段，从而为全面有效的控制报文的转发调度等级提供依据。

2.3.1 端口优先级

如果配置了优先级信任模式，即表示设备信任所接收报文的优先级，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参数。

如果没有配置优先级信任模式，并且配置了端口优先级值，则表明设备不信任所接收报文的优先级，而是使用端口优先级，按照映射表映射到报文的优先级参数。

1. 配置端口优先级

按照接收端口的端口优先级，设备通过一一映射为报文分配优先级。

2. 配置优先级信任模式

根据报文自身的优先级，查找优先级映射表，为报文分配优先级参数，可以通过配置优先级信任模式的方式来实现。

在配置接口上的优先级模式时，用户可以选择下列信任模式：

- Untrust：不信任任何优先级。
- Dot1p：信任报文自带的 802.1p 优先级，以此优先级进行优先级映射。
- DSCP：信任 IP 报文自带的 DSCP 优先级，以此优先级进行优先级映射。

2.3.2 优先级映射表

报文在进入设备以后，设备会根据映射规则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，就可以获得决定报文调度能力的各种优先级字段，从而为全面有效的控制报文的转发调度等级提供依据。

设备中提供了三张优先级映射表，分别 802.1p 优先级到本地优先级映射表、DSCP 到 802.1p 优先级映射表和 DSCP 到 DSCP 映射表。如果缺省优先级映射表无法满足用户需求，可以根据实际情况对映射表进行修改。

2.4 802.1X

802.1X 协议是一种基于端口的网络接入控制协议，即在局域网接入设备的端口上对所接入的用户和设备进行认证，以便控制用户设备对网络资源的访问。

2.4.1 802.1X的体系结构

802.1X 系统中包括三个实体：

- 客户端：请求接入局域网的用户终端，由局域网中的设备端对其进行认证。客户端上必须安装支持 802.1X 认证的客户端软件。
- 设备端：局域网中控制客户端接入的网络设备，位于客户端和认证服务器之间，为客户端提供接入局域网的端口，并通过与认证服务器的交互来对所连接的客户端进行认证。
- 认证服务器端：用于对客户端进行认证、授权和计费，通常为 RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）服务器。认证服务器根据设备端发送来的客户端认证信息来验证客户端的合法性，并将验证结果通知给设备端，由设备端决定是否允许客户端接入。

2.4.2 802.1X的认证方法

在接入设备上，802.1X 认证方法有三种方式：

- CHAP 或 PAP 认证方法。在这种方式下，设备对 EAP 认证过程进行终结，将收到的 EAP 报文中的客户端认证信息封装在标准的 RADIUS 报文中，与服务器之间采用 PAP 或 CHAP 方法进行认证。CHAP 以密文的方式传送密码，而 PAP 是以明文的方式传送密码。
- EAP 认证方法。在这种方式下，设备端对收到的 EAP 报文进行中继，使用 EAPOR（EAP over RADIUS）封装格式将其承载于 RADIUS 报文中发送给 RADIUS 服务器。

2.4.3 接入控制方式

端口支持以下两种接入控制方式：

- 基于端口认证：只要该端口下的第一个用户认证成功后，其它接入用户无须认证就可使用网络资源，但是当第一个用户下线后，其它用户也会被拒绝使用网络。
- 基于 MAC 认证：该端口下的所有接入用户均需要单独认证，当某个用户下线后，也只有该用户无法使用网络。

2.4.4 授权状态

端口支持以下三种授权状态：

- 强制授权：表示端口始终处于授权状态，允许用户不经认证即可访问网络资源。
- 强制非授权：表示端口始终处于非授权状态。设备端不为通过该端口接入的客户端提供认证服务。
- 自动识别：表示端口初始状态为非授权状态，仅允许 EAPOL 报文收发，不允许用户访问网络资源；如果用户通过认证，则端口切换到授权状态，允许用户访问网络资源。

2.4.5 周期性重认证

该功能开启后，设备会根据周期性重认证时间间隔定期向该端口在线 802.1X 用户发起重认证，以检测用户连接状态的变化、确保用户的正常在线，并及时更新服务器下发的授权属性（例如 ACL、VLAN、User Profile）。

2.4.6 在线用户握手

该功能开启后，设备会根据周期发送握手请求报文时间间隔定期向通过 802.1X 认证的在线用户发送握手报文，以定期检测用户的在线情况。如果设备连续多次没有收到客户端的响应报文，则会将用户置为下线状态。

2.4.7 安全握手

在线用户握手功能处于开启状态的前提下，还可以通过开启在线用户握手安全功能，来防止在线的 802.1X 认证用户使用非法的客户端与设备进行握手报文的交互，而逃过代理检测、双网卡检测等 iNode 客户端的安全检查功能。

2.4.8 认证触发

设备端主动触发方式用于支持不能主动发送 EAPOL-Start 报文的客户端，例如 Windows XP 自带的 802.1X 客户端。设备主动触发认证的方式分为以下两种：

- 单播触发：当设备收到源 MAC 地址未知的报文时，主动向该 MAC 地址单播发送 Identity 类型的 EAP-Request 帧来触发认证。若设备端在设置的时长内没有收到客户端的响应，则重发该报文。
- 组播触发：设备每隔一定时间（缺省为 30 秒）主动向客户端组播发送 Identity 类型的 EAP-Request 帧来触发认证。

2.4.9 Auth-Fail VLAN

802.1X Auth-Fail VLAN 功能允许用户在认证失败的情况下访问某一特定 VLAN 中的资源。需要注意的是，这里的认证失败是认证服务器因某种原因明确拒绝用户认证通过，比如用户密码错误，而不是认证超时或网络连接等原因造成的认证失败。

1. 基于端口认证

在接入控制方式为基于端口认证的端口上配置 Auth-Fail VLAN 后，若该端口上有用户认证失败，则该端口会离开当前的 VLAN 被加入到 Auth-Fail VLAN，所有在该端口接入的用户将被授权访问 Auth-Fail VLAN 里的资源。

当加入 Auth-Fail VLAN 的端口上有用户发起认证并失败，则该端口将会仍然处于 Auth-Fail VLAN 内；如果认证成功，则该端口会离开 Auth-Fail VLAN，之后端口加入 VLAN 情况与认证服务器是否下发授权 VLAN 有关，具体如下：

- 若认证服务器下发了授权 VLAN，则端口加入下发的授权 VLAN 中。用户下线后，端口会离开下发的授权 VLAN，若端口上配置了 Guest VLAN，则加入 Guest VLAN，否则加入缺省 VLAN。
- 若认证服务器未下发授权 VLAN，则端口回到缺省 VLAN 中。用户下线后，端口仍在缺省 VLAN 中。

2. 基于MAC认证

在接入控制方式为基于 MAC 认证的端口上配置 Auth-Fail VLAN 后，该端口上认证失败的用户将被授权访问 Auth-Fail VLAN 里的资源。

当 Auth-Fail VLAN 中的用户再次发起认证时，如果认证成功，则设备会根据认证服务器是否下发 VLAN 决定将该用户加入到下发的授权 VLAN 中，或使其回到端口的缺省 VLAN 中；如果认证失败，则该用户仍然留在该 Auth-Fail VLAN 中。

2.4.10 Guest VLAN

802.1X Guest VLAN 功能允许用户在未认证的情况下，访问某一特定 VLAN 中的资源。

当端口上处于 Guest VLAN 中的用户发起认证且失败时：如果端口配置了 Auth-Fail VLAN，则该端口会被加入 Auth-Fail VLAN；如果端口未配置 Auth-Fail VLAN，则该端口仍然处于 Guest VLAN 内。

当端口上处于 Guest VLAN 中的用户发起认证且成功时，端口会离开 Guest VLAN，之后端口加入 VLAN 情况与认证服务器是否下发 VLAN 有关，具体如下：

若认证服务器下发 VLAN，则端口加入下发的 VLAN 中。用户下线后，端口离开下发的 VLAN 回到初始 VLAN 中，该初始 VLAN 为端口加入 Guest VLAN 之前所在的 VLAN。

若认证服务器未下发 VLAN，则端口回到初始 VLAN 中。用户下线后，端口仍在该初始 VLAN 中。

根据端口的接入控制方式不同，Guest VLAN 的生效情况有所不同。

1. 基于端口认证

在接入控制方式为基于端口认证的端口上配置 Guest VLAN 后，若全局和端口上都使能了 802.1X，端口授权状态为 auto，且端口处于激活状态，则该端口就被立即加入 Guest VLAN，所有在该端口接入的用户将被授权访问 Guest VLAN 里的资源。

2. 基于MAC认证

在接入控制方式为基于 MAC 认证的端口上配置 Guest VLAN 后，端口上未认证的用户将被授权访问 Guest VLAN 里的资源。

2.4.11 Critical VLAN

802.1X Critical VLAN 功能允许用户在认证时，当所有认证服务器都不可达的情况下访问某一特定 VLAN 中的资源。目前，只采用 RADIUS 认证方式的情况下，在所有 RADIUS 认证服务器都不可达后，端口才会加入 Critical VLAN。若采用了其它认证方式，则端口不会加入 Critical VLAN。

根据端口的接入控制方式不同，Critical VLAN 的生效情况有所不同。

1. 基于端口认证

在接入控制方式为基于端口认证的端口上配置 Critical VLAN 后，若该端口上有用户认证时，所有认证服务器都不可达，则该端口会被加入到 Critical VLAN，之后所有在该端口接入的用户将被授权访问 Critical VLAN 里的资源。在用户进行重认证时，若所有认证服务器都不可达，且端口指定在此情况下强制用户下线，则该端口也会被加入到 Critical VLAN。

已经加入 Critical VLAN 的端口上有用户发起认证时，如果所有认证服务器不可达，则端口仍然在 Critical VLAN 内；如果服务器可达且认证失败，且端口配置了 Auth-Fail VLAN，则该端口将会加入 Auth-Fail VLAN，否则回到端口的缺省 VLAN 中；如果服务器可达且认证成功，则该端口加入 VLAN 的情况与认证服务器是否下发 VLAN 有关，具体如下：

若认证服务器下发了授权 VLAN，则端口加入下发的授权 VLAN 中。用户下线后，端口会离开下发的授权 VLAN，若端口上配置了 Guest VLAN，则加入 Guest VLAN，否则加入缺省 VLAN。

若认证服务器未下发授权 VLAN，则端口回缺省 VLAN 中。用户下线后，端口仍在缺省 VLAN 中。

2. 基于MAC认证

在接入控制方式为基于 MAC 认证的端口上配置 Critical VLAN 后，若该端口上有用户认证时，所有认证服务器都不可达，则端口将允许 Critical VLAN 通过，用户将被授权访问 Critical VLAN 里的资源。

当 Critical VLAN 中的用户再次发起认证时，如果所有认证服务器不可达，则用户仍然在 Critical VLAN 中；如果服务器可达且认证失败，且端口配置了 Auth-Fail VLAN，则该用户将会加入 Auth-Fail VLAN，否则回到端口的缺省 VLAN 中；如果服务器可达且认证成功，则设备会根据认证服务器是否下发授权 VLAN 决定将该用户加入下发的授权 VLAN 中，或使其回到端口的缺省 VLAN 中。

2.4.12 端口的强制认证ISP域

在端口上指定强制认证域为 802.1X 接入提供了一种安全控制策略。所有从该端口接入的 802.1X 用户将被强制使用指定的认证域来进行认证、授权和计费，从而防止用户通过恶意假冒其它域账号从本端口接入网络。另外，管理员也可以通过配置强制认证域对不同端口接入的用户指定不同的认证域，从而增加了管理员部署 802.1X 接入策略的灵活性。

2.4.13 EAD快速部署

EAD（Endpoint Admission Defense，端点准入防御）作为一个网络端点接入控制方案，它通过安全客户端、安全策略服务器、接入设备以及第三方服务器的联动，加强了对用户的集中管理，提升了网络的整体防御能力。但是在实际的应用过程中 EAD 客户端的部署工作量很大，例如，需要网络管理员手动为每一个 EAD 客户端下载、升级客户端软件，这在 EAD 客户端数目较多的情况下给管理员带来了操作上的不便。

802.1X 认证支持的 EAD 快速部署功能就可以解决以上问题，它允许未通过认证的 802.1X 用户访问一个指定的 IP 地址段（称为 Free IP），并可以将用户发起的 HTTP 访问请求重定向到该 IP 地址段中的一个指定的 URL，实现用户自动下载并安装 EAD 客户端的目的。

2.4.14 配置 802.1X SmartOn功能

开启了 SmartOn 功能的端口上收到 802.1X 客户端发送的 EAPOL-Start 报文后，将向其回复单播的 EAP-Request/Notification 报文，并开启 SmartOn 通知请求超时定时器定时器等待客户端响应的 EAP-Response/Notification 报文。若 SmartOn 通知请求超时定时器超时后客户端仍未回复，则设备会重发 EAP-Request/Notification 报文，并重新启动该定时器。当重发次数达到规定的最大次数后，会停止对该客户端的 802.1X 认证；若在重发次数达到最大次数之前收到了该 Notification 报文的回复报文，则获取该报文中携带的 Switch ID 和 SmartOn 密码的 MD5 摘要，并与设备本地配置的 SmartOn 的 Switch ID 以及 SmartOn 密码的 MD5 摘要值比较，若相同，则继续客户端的 802.1X 认证，否则中止客户端的 802.1X 认证。

802.1X SmartOn 功能与在线用户握手功能互斥，建议两个功能不要同时开启。

2.5 ISP域

设备对用户的管理是基于 ISP（Internet Service Provider，互联网服务提供者）域的，一个 ISP 域对应着一套实现 AAA（Authentication、Authorization、Accounting，认证、授权、计费）的配置策略，它们是管理员针对该域用户制定的一套认证、授权、计费方法，可根据用户的接入特征以及不同的安全需求组合使用。

设备支持的认证方法包括：

- 不认证：对用户非常信任，不对其进行合法性检查，一般情况下不采用这种方法。
- 本地认证：认证过程在接入设备上完成，用户信息（包括用户名、密码和各种属性）配置在接入设备上。优点是速度快，可以降低运营成本；缺点是存储信息量受设备硬件条件限制。
- 远端认证（RADIUS）：认证过程在接入设备和远端的服务器之间完成，接入设备和远端服务器之间通过 RADIUS 协议通信。优点是用户信息集中在服务器上统一管理，可实现大容量、

高可靠性、支持多设备的集中式统一认证。当远端服务器无效时，可配置备选认证方式完成认证。

设备支持的授权方法包括：

- 不授权：接入设备不请求授权信息，不对用户可以使用的操作以及用户允许使用的网络服务进行授权。此时，认证通过的 login 用户只有系统所给予的缺省用户角色，其中 FTP/SFTP/SCP 用户的工作目录是设备的根目录，但并无访问权限；认证通过的非 login 用户，可直接访问网络。
- 本地授权：授权过程在接入设备上进行，根据接入设备上为本地用户配置的相关属性进行授权。
- 远端授权（RADIUS）：授权过程在接入设备和远端服务器之间完成。RADIUS 协议的认证和授权是绑定在一起的，不能单独使用 RADIUS 进行授权。RADIUS 认证成功后，才能进行授权，RADIUS 授权信息携带在认证回应报文中下发给用户。当远端服务器无效时，可配置备选授权方式完成授权。

设备支持的计费方法包括：

- 不计费：不对用户计费。
- 本地计费：计费过程在接入设备上完成，实现了本地用户连接数的统计和限制，并没有实际的费用统计功能。
- 远端计费（RADIUS）：计费过程在接入设备和远端的服务器之间完成。当远端服务器无效时，可配置备选计费方式完成计费。

每个用户都属于一个 ISP 域。为便于对不同接入方式的用户进行区分管理，提供更为精细且有差异化的认证、授权、计费服务，设备将用户划分为以下几个类型：

- LAN 接入用户：例如 802.1X 认证用户。
- 登录用户：例如 Telnet、FTP、终端接入用户（即从 Console、AUX 等接口登录的用户）。
- Portal 用户。

在多 ISP 的应用环境中，不同 ISP 域的用户有可能接入同一台设备，因此系统中可以存在多个 ISP 域，其中包括一个缺省存在的名称为 system 的 ISP 域。如果某个用户在登录时没有提供 ISP 域名，系统将把它归于缺省的 ISP 域。系统缺省的 ISP 域可以手工修改为一个指定的 ISP 域。

用户认证时，设备将按照如下先后顺序为其选择认证域：接入模块指定的认证域-->用户名中指定的 ISP 域-->系统缺省的 ISP 域。其中，仅部分接入模块支持指定认证域，例如 802.1X 认证。

2.6 RADIUS

2.6.1 RADIUS协议简介

RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）是一种分布式的、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。

- RADIUS 客户端：一般位于接入设备上，可以遍布整个网络，负责将用户信息传输到指定的 RADIUS 服务器，然后根据服务器返回的信息进行相应处理（如接受/拒绝用户接入）。
- RADIUS 服务器：一般运行在中心计算机或工作站上，维护用户的身份信息和与其相关的网络服务信息，负责接收接入设备发送的认证、授权、计费请求并进行相应的处理，然后给接入设备返回处理结果（如接受/拒绝认证请求）。

RADIUS 协议使用 UDP 作为封装 RADIUS 报文的传输层协议，通过使用共享密钥机制来保证客户端和 RADIUS 服务器之间消息交互的安全性。

当接入设备对用户提供 AAA（Authentication、Authorization、Accounting，认证、授权、计费）服务时，若要对用户采用 RADIUS 服务器进行认证、授权、计费，则作为 RADIUS 客户端的接入设备上需要配置相应的 RADIUS 服务器参数。

2.6.2 RADIUS增强功能

1. Accounting-on功能

设备重启后，重启前的原在线用户可能会被 RADIUS 服务器认为仍然在线而短时间内无法再次登录。为了解决这个问题，需要开启 Accounting-on 功能。

开启了 Accounting-on 功能后，设备会在重启后主动向 RADIUS 服务器发送 Accounting-on 报文来告知自己已经重启，并要求 RADIUS 服务器停止计费且强制通过本设备上线的用户下线。若设备发送 Accounting-on 报文后 RADIUS 服务器无响应，则会在按照一定的时间间隔尝试重发几次。

2. Session control功能

H3C 的 IMC RADIUS 服务器使用 session control 报文向设备发送授权信息的动态修改请求以及断开连接请求。设备上开启接收 session control 报文的开关后，会打开知名 UDP 端口 1812 来监听并接收 RADIUS 服务器发送的 session control 报文。

需要注意的是，该功能仅能和 H3C 的 IMC RADIUS 服务器配合使用。

2.7 本地认证

本地认证泛指由接入设备对用户进行认证、授权和计费，进行本地认证的用户的信息（包括用户名、密码和各种属性）配置在接入设备上。

为使某个请求网络服务的用户可以通过本地认证，需要在设备上添加相应的用户条目。所谓用户，是指在设备上设置的一组用户属性的集合，该集合以用户名唯一标识。

为了简化用户的配置，增强用户的可管理性，引入了用户组的概念。用户组是一系列公共用户属性的集合，某些需要集中管理的公共属性可在用户组中统一配置和管理，属于该用户组的所有用户都可以继承这些属性。

3 系统

3.1 ACL

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。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。

3.1.1 ACL分类

ACL包括 表 3-1 所列的几种类型，它们的主要区别在于规则制订依据不同：

表3-1 ACL 分类

ACL 分类		规则制定依据
IPv4 ACL	基本ACL	依据报文的源IPv4地址制订规则
	高级ACL	依据报文的源/目的IPv4地址、源/目的端口号、优先级、承载的IPv4协议类型等三、四层信息制订规则
IPv6 ACL	基本ACL	依据报文的源IPv6地址制订规则
	高级ACL	依据报文的源/目的IPv6地址、源/目的端口号、优先级、承载的IPv6协议类型等三、四层信息制订规则
二层ACL		依据报文的源/目的MAC地址、802.1p优先级、链路层协议类型等二层信息
自定义ACL		以报文头为基准，指定从报文的第几个字节开始与掩码进行“与”操作，并将提取出的字符串与用户定义的字符串进行比较，从而找出相匹配的报文

3.1.2 ACL规则匹配顺序

一个 ACL 中可以包含多条规则，设备将报文按照一定顺序与这些规则进行匹配，一旦匹配上某条规则便结束匹配过程。规则匹配顺序有两种：

- 配置顺序：按照规则编号由小到大进行匹配。
- 自动排序：按照“深度优先”原则由深到浅进行匹配，见 表 3-2（自定义ACL不支持自动排序）：

表3-2 各类型 ACL 的“深度优先”排序法则

ACL 分类		规则制定依据
IPv4 ACL	基本ACL	1. 先比较源 IPv4 地址的范围，较小者（即通配符掩码中“0”位较多者）优先 2. 如果源 IPv4 地址范围相同，再比较配置的先后次序，先配置者优先
	高级ACL	1. 先比较协议范围，指定有 IPv4 承载的协议类型者优先 2. 如果协议范围相同，再比较源 IPv4 地址范围，较小者优先 3. 如果源 IPv4 地址范围也相同，再比较目的 IPv4 地址范围，较小者优先

ACL 分类		规则制定依据
		4. 如果目的 IPv4 地址范围也相同，再比较 TCP/UDP 端口号的覆盖范围，较小者优先 **5.** 如果 TCP/UDP 端口号的覆盖范围无法比较，则比较配置的先后次序，先配置者优先
IPv6 ACL	基本ACL	**1.** 先比较源 IPv6 地址的范围，较小者（即前缀较长者）优先 **2.** 如果源 IPv6 地址范围相同，再比较配置的先后次序，先配置者优先
	高级ACL	**1.** 先比较协议范围，指定有 IPv6 承载的协议类型者优先 **2.** 如果协议范围相同，再比较源 IPv6 地址范围，较小者优先 **3.** 如果源 IPv6 地址范围也相同，再比较目的 IPv6 地址范围，较小者优先 **4.** 如果目的 IPv6 地址范围也相同，再比较 TCP/UDP 端口号的覆盖范围，较小者优先 **5.** 如果 TCP/UDP 端口号的覆盖范围无法比较，则比较配置的先后次序，先配置者优先
二层ACL		**1.** 先比较源 MAC 地址范围，较小者（即掩码中“1”位较多者）优先 **2.** 如果源 MAC 地址范围相同，再比较目的 MAC 地址范围，较小者优先 **3.** 如果目的 MAC 地址范围也相同，再比较配置的先后次序，先配置者优先

说明

- 比较 IPv4 地址范围的大小，就是比较 IPv4 地址通配符掩码中“0”位的多少。
- 比较 IPv6 地址范围的大小，就是比较 IPv6 地址前缀的长短：前缀越长，范围越小。
- 比较 MAC 地址范围的大小，就是比较 MAC 地址掩码中“1”位的多少：“1”位越多，范围越小。

3.1.3 ACL规则编号

每条规则都有自己的编号，这个编号可由手工指定或由系统自动分配。由于规则编号可能影响规则的匹配顺序，因此当系统自动分配编号时，为方便后续在已有规则之间插入新规则，通常在相邻编号之间留有一定空间，这就是规则编号的步长。系统自动分配编号的方式为：从 0 开始，按照步长分配一个大于现有最大编号的最小编号。比如原有编号为 0、5、9、10 和 12 的五条规则，步长为 5，则系统将自动为下一条规则分配编号 15。如果步长发生了改变，则原有全部规则的编号都将自动从 0 开始按新步长重新排列。比如原有编号为 0、5、9、10 和 15 的五条规则，当步长变为 2 后，这些规则的编号将依次变为 0、2、4、6 和 8。

3.2 时间段

时间段（Time Range）定义了一个时间范围。用户通过创建一个时间段并在某业务中将其引用，就可使该业务在此时间段定义的时间范围内生效。但如果一个业务所引用的时间段尚未配置或已被删除，该业务将不会生效。

譬如，当一个 ACL 规则只需在某个特定时间范围内生效时，就可以先配置好这个时间段，然后在配置该 ACL 规则时引用此时间段，这样该 ACL 规则就只能在该时间段定义的时间范围内生效。

时间段可分为以下两种类型：

- 周期时间段：表示以一周为周期（如每周一的 8 至 12 点）循环生效的时间段。
- 绝对时间段：表示在指定时间范围内（如 2011 年 1 月 1 日 8 点至 2011 年 1 月 3 日 18 点）生效时间段。

每个时间段都以一个名称来标识，一个时间段内可包含一或多个周期时间段和绝对时间段。当一个时间段内包含有多个周期时间段和绝对时间段时，系统将先分别取各周期时间段的并集和各绝对时间段的并集，再取这两个并集的交集作为该时间段最终生效的时间范围。

3.3 文件管理

3.3.1 文件系统

设备上的一个存储介质即称为一个文件系统。

1. 文件系统的命名

本设备除了固定存储介质外还支持可插拔存储介质 U 盘，可插拔存储介质的文件系统名称由存储介质的位置、存储介质类型、存储介质编号和冒号组成：

- 存储介质的位置：请参见本文档的 2. 存储介质位置。
- 存储介质类型：U 盘的类型名称为“usb”。
- 存储介质编号：同类型的存储介质以英文小写字母 a 开始进行排序，例如“usba”表示第一个 U 盘。
- 冒号：作为存储介质名称的结束符，例如第一个 U 盘的完整名称为“usba:”

2. 存储介质位置

说明

文件系统名称中的英文字符输入时区分大小写，必须为小写字符。

3. 缺省文件系统

缺省文件系统是指用户登录设备后默认工作在的文件系统。用户在对文件或者文件夹进行操作时，如果不指定文件系统，则表示对设备的缺省文件系统进行操作。例如，在保存当前配置时，如果不输入任何保存位置信息，则下次启动配置文件将保存在缺省文件系统的根目录下。

4. 目录

本设备的文件系统采用树形目录结构。

根目录

根目录用“/”来表示。

(1) 工作目录

工作目录也被称为当前工作目录。

用户登录设备后，缺省的工作目录为设备 Flash 的根目录。

(2) 文件夹的命名

文件夹名称中可以包含数字、字母或特殊字符（除了*|\/?<>":）。给文件夹命名时，首字母请不要使用“.”。因为系统会把名称首字母为“.”的文件夹当成隐藏文件夹。

(3) 常用文件夹

设备出厂时会携带一些文件夹，在运行过程中可能会自动产生一些文件夹，这些文件夹包括：

- diagfile：用于存放诊断信息文件的文件夹
- logfile：用于存放日志文件的文件夹
- seclog：用于存放安全日志文件的文件夹
- versionInfo：用于存放版本信息文件的文件夹
- 其它名称的文件夹

5. 文件

(1) 文件的命名

文件名中可以输入以数字、字母、特殊字符为组合的字符串（除了*|\/?<>":）。给文件命名时，首字母请不要使用“.”。因为系统会把名称首字母为“.”的文件当成隐藏文件。

(2) 常见文件类型

设备出厂时会携带一些文件，在运行过程中可能会自动产生一些文件，这些文件包括：

- xx.ipe（复合软件包套件，是启动软件包的集合）
- xx.bin（启动软件包）
- xx.cfg（配置文件）
- xx.mdb（二进制格式的配置文件）
- xx.log（用于存放日志的文件）
- 其它后缀的文件

(3) 隐藏文件和文件夹

文件/文件夹分为隐藏的、非隐藏的。因为有些系统文件/文件夹是隐藏文件/文件夹，所以对于隐藏文件/文件夹，请不要修改或删除，以免影响对应功能；对于非隐藏的文件/文件夹，请完全了解它的作用后再执行文件/文件夹操作，以免误删重要文件/文件夹。

3.3.2 使用限制和注意事项

- 设备在执行文件系统操作过程中，禁止对存储介质进行插拔操作。否则，可能会引起文件系统的损坏。
- 当用户占用可插拔存储介质的资源（如用户正在访问某个目录）时，存储介质被强制拔出。此时，请先释放占用的存储介质的资源，再插入存储介质。否则，存储介质被插入后可能不能被识别。
- 当需要对 U 盘进行写文件系统操作，请确保没有将 U 盘写保护。如果 U 盘写保护了，这些操作将执行失败。其它文件系统操作不受写保护开关影响。

3.3.3 文件操作

文件操作是指对指定的文件路径下的文件进行相应操作，目前文件操作分为以下三类：

- 上传：设备支持上传版本文件、配置文件、证书、本地 Portal 页面、map 文件、特殊 AP 版本文件等。
- 下载：设备支持下载版本文件、配置文件、一键诊断信息及之前上传的信息文件等。
- 删除：设备支持选择删除设备上的非隐性文件。

说明

目前删除之后的文件无法恢复，请确保删除文件准确无误。

3.4 管理员

管理员通过 HTTP、HTTPS、SSH、Telnet、FTP、PAD、终端接入（即从 Console 口接入）方式登录到设备上之后，可以对设备进行配置和管理。对登录用户的管理和维护主要涉及以下几个部分：

- 帐户管理：对用户的基本信息（用户名、密码）以及相关属性的管理。
- 角色管理：对用户可执行的系统功能以及可操作的系统资源权限的管理。
- 密码管理：对用户登录密码的设置、老化、更新以及用户登录状态等方面的管理。

3.4.1 帐户管理

为使请求某种服务的用户可以成功登录设备，需要在设备上添加相应的帐户。所谓用户，是指在设备上设置的一组用户属性的集合，该集合以用户名唯一标识。一个有效的用户条目中可包括用户名、密码、角色、可用服务、密码管理等属性。

3.4.2 角色管理

对登录用户权限的控制，是通过为用户赋予一定的角色来实现。一个角色中定义了允许用户执行的系统功能以及可操作的系统资源，具体实现如下：

- 通过角色规则实现对系统功能的操作权限的控制。例如，定义用户角色规则允许用户配置 A 功能，或禁止用户配置 B 功能。
- 通过资源控制策略实现对系统资源（接口、VLAN）的操作权限的控制。例如，定义资源控制策略允许用户操作 VLAN 10，禁止用户操作接口 GigabitEthernet1/0/1。

1. 角色规则

一个角色中可以包含多条规则，规则定义了允许/禁止用户操作某类实体的权限。

系统支持的实体类型包括：

- 命令行：控制用户权限的最小单元，具体可分为读、写、执行类型的命令行。
- 特性：与一个功能相关的所有命令的集合。系统中的所有特性及其包含的命令都是系统预定义的，不允许用户自定义。
- 特性组：一个或者多个特性的集合。系统预定义了两个特性组 L2 和 L3。L2 中包含了所有的二层协议相关功能的命令，L3 中包含了所有三层协议相关功能的命令。管理员可以根据需要自定义特性组，但不能修改和删除系统预定义的特性组 L2 和 L3。各个特性组之间包含的特性允许重叠。

- Web 菜单：通过 Web 对设备进行配置时，各配置页面以 Web 菜单的形式组织，按照层次关系，形成多级菜单的树形结构。
- XML 元素：与 Web 菜单类似，XML 对于配置对象的组织也呈现树状结构，每一个 XML 元素代表 XML 配置中的一个 XML 节点。
- SNMP OID：对象标识符，SNMP 协议通过 OID 唯一标识一个被管理对象。

对实体的操作权限包括：

- 读权限：可查看指定实体的配置信息和维护信息。
- 写权限：可配置指定实体的相关功能和参数。
- 执行权限：可执行特定的功能，如与 FTP 服务器建立连接。

定义一个规则，就等于约定允许或禁止用户针对某类实体具有哪些操作权限，具体分为：

- 控制命令行的规则：用来控制一条命令或者与指定的命令特征字符串相匹配的一类命令是否允许被执行。
- 控制特性的规则：用来控制特性包含的命令是否允许被执行。因为特性中的每条命令都属于读类型、写类型或执行类型，所以在定义该类规则时，可以精细地控制特性所包含的读、写或执行类型的命令能否被执行。
- 控制特性组的规则：此规则和基于特性的规则类似，区别是一条基于特性组的规则中可同时对多个特性包含的命令进行控制。
- 控制 Web 菜单的规则：用来控制指定的 Web 菜单选项是否允许被操作。因为每个菜单项中的操作控件具有相应的读，写或执行属性，所以定义基于 Web 菜单的规则时，可以精细地控制菜单项中读、写或执行控件的操作。
- 控制 XML 元素的规则：用来控制指定的 XML 元素是否允许被执行。XML 元素也具有读，写或执行属性。
- 控制 OID 的规则：用来控制指定的 OID 是否允许被 SNMP 访问。OID 具有读，写和执行属性。

一个用户角色中可以定义多条规则，各规则以创建时指定的编号为唯一标识，被授权该角色的用户可以执行的命令为这些规则中定义的可执行命令的并集。若这些规则定义的权限内容有冲突，则规则编号大的有效。例如，规则 1 允许执行命令 A，规则 2 允许执行命令 B，规则 3 禁止执行命令 A，则最终规则 2 和规则 3 生效，即禁止执行命令 A，允许执行命令 B。

2. 资源控制策略

资源控制策略规定了用户对系统资源的操作权限。

- 对于登录命令行的用户而言，对接口/VLAN 的操作是指创建并进入接口视图/VLAN 视图、删除和应用接口/VLAN（在 **display** 命令中指定接口/VLAN 参数并不属于应用接口/VLAN 范畴）。
- 对于登录 Web 页面的用户而言，对接口/VLAN 的操作是指创建接口/VLAN、配置接口/VLAN 的属性、删除接口/VLAN 和应用接口/VLAN。

资源控制策略需要与角色规则相配合才能生效。在用户执行命令的过程中，系统对该命令涉及的系统资源使用权限进行动态检测，因此只有用户同时拥有执行该命令的权限和使用该资源的权限时，才能执行该命令。例如，若管理员为某用户角色定义了一条规则允许用户创建 VLAN，且同时指定用户具有操作 VLAN 10 的权限，则当用户被授权此角色并试图创建 VLAN 10 时，操作会被允许，但试图创建其它 VLAN 时，操作会被禁止。若管理员并没有为该角色定义允许用户创建 VLAN 的规则，则用户即便拥有该 VLAN 资源的操作权限，也无法执行相关的操作。

3. 缺省角色

系统预定义了多种角色，角色名和对应的权限如 表 3-3 所示。这些角色缺省均具有操作所有系统资源的权限，但具有不同的系统功能操作权限。如果系统预定义的用户角色无法满足权限管理需求，管理员还可以自定义用户角色来对用户权限做进一步控制。

表3-3 系统预定义的角色名和对应的权限

角色名	权限
network-admin	可操作系统所有功能和资源（除安全日志文件管理相关命令**display security-logfile summary**、**info-center security-logfile directory**、**security-logfile save**之外）
network-operator	• 可执行系统所有功能和资源的相关 **display** 命令（除 **display history-command all**、**display security-logfile summary** 等命令，具体请通过 **display role** 命令查看） • 如果用户采用本地认证方式登录系统并被授予该角色，则可以修改自己的密码 • 可执行进入 XML 视图的命令 • 可允许用户对所有 Web 菜单选项进行读操作 • 可允许用户对所有 XML 元素进行读操作 • 可允许用户对所有 SNMP OID 进行读操作
level-*n* (*n* = 0～15)	• level-0：可执行命令 **ping**、**tracert**、**ssh2**、**telnet** 和 **super**，且管理员可以为其配置权限 • level-1：具有 level-0 用户角色的权限，并且可执行系统所有功能和资源的相关 **display** 命令（除 **display history-command all** 之外），以及管理员可以为其配置权限 • level-2～level-8 和 level-10～level-14：无缺省权限，需要管理员为其配置权限 • level-9：可操作系统中绝大多数的功能和所有的资源，且管理员可以为其配置权限，但不能操作 **display history-command all** 命令、RBAC 的命令（Debug 命令除外）、文件管理、设备管理以及本地用户特性。对于本地用户，若用户登录系统并被授予该角色，可以修改自己的密码 • level-15：具有与 network-admin 角色相同的权限
security-audit	安全日志管理员，仅具有安全日志文件的读、写、执行权限，具体如下： • 可执行安全日志文件管理相关的命令（**display security-logfile summary**、**info-center security-logfile directory**、**security-logfile save**）。安全日志文件管理相关命令的介绍，请参见“网络管理与监控”中的“信息中心” • 可执行安全日志文件操作相关的命令，例如 **more** 显示安全日志文件内容；**dir**、**mkdir** 操作安全日志文件目录等，具体命令的介绍请参见“基础配置命令参考”中的“文件系统管理” 以上权限，仅安全日志管理员角色独有，其它任何角色均不具备
guest-manager	来宾用户管理员，只能查看和配置来宾用户管理相关Web页面，无命令行控制权限

说明

- 只有具有 network-admin 或者 level-15 用户角色的用户登录设备后才可以执行 RBAC 特性的所有命令、修改用户线视图下的相关配置（包括 **user-role**、**authentication-mode**、**protocol inbound** 和 **set authentication password**）以及执行创建/修改/删除本地用户和本地用户组；其它角色的用户，即使被授权对本地用户和本地用户组的操作权限，也仅仅具有修改自身密码的权限，没有除此之外的对本地用户和本地用户组的任何操作权限。
- 预定义的用户角色中，仅用户角色 level-0～level-14 可以通过自定义规则和资源控制策略调整自身的权限。需要注意的是，这种修改对于 **display history-command all** 命令不生效，即不能通过添加对应的规则来更改它的缺省执行权限。

4. 为用户赋予角色

根据用户登录方式的不同，为用户授权角色分为以下两类：

- 对于通过本地 AAA 认证登录设备的用户，由本地用户配置决定为其授权的用户角色。
- 对于通过 AAA 远程认证登录设备的用户，由 AAA 服务器的配置决定为其授权的用户角色。

将有效的角色成功授权给用户后，登录设备的用户才能以各角色所具有的权限来配置、管理或者监控设备。如果用户没有被授权任何角色，将无法成功登录设备。

一个用户可同时拥有多个角色。拥有多个角色的用户可获得这些角色中被允许执行的功能以及被允许操作的资源的集合。

5. 规则配置指导

定义控制命令行的规则时，通过输入命令特征字符串来指定要控制命令行的范围。特征字符串的输入需要遵循以下规则：

- 在输入命令特征字符串时必须指定该命令所在的视图，进入各视图的命令特征字符串由分号（;）分隔。分号将命令特征字符串分成多个段，每一个段代表一个或一系列命令，后一个段中的命令是执行前一个段中命令所进入视图下的命令。一个段中可以包含多个星号（*），每个星号（*）代表了 0 个或多个任意字符。例如：命令特征字符串“system ; interface * ; ip * ;” 代表从系统视图进入到任意接口视图后，以 **ip** 开头的所有命令。
- 当最后一个段中的最后一个可见字符为分号时，表示所指的命令范围不再扩展，否则将向子视图中的命令扩展。例如：命令特征字符串“system ; radius scheme * ;”代表系统视图下以 **radius scheme** 开头的所有命令；命令特征字符串“system ; radius scheme * ”代表系统视图下以 **radius scheme** 开头的所有命令，以及进入子视图（RADIUS 方案视图）下的所有命令。
- 当星号（*）出现在一个段的首部时，其后面不能再出现其它可打印字符，且该段必须是命令特征字符串的最后一个段。例如：命令特征字符串“system ; *”就代表了系统视图下的所有命令，以及所有子视图下的命令。
- 当星号（*）出现在一个段的中间时，该段必须是命令特征字符串的最后一个段。例如：命令特征字符串“debugging * event”就代表了用户视图下所有模块的事件调试信息开关命令。
- 一个段中必须至少出现一个可打印字符，不能全部为空格或 Tab。
- 对于能在任意视图下执行的命令（例如 **display** 命令）以及用户视图下的命令（例如 **dir** 命令），在配置包含此类命令的规则时，不需要在规则的命令匹配字符串中指定其所在的视图。

用户执行命令时，系统遵循以下匹配规则：

- 命令关键字与命令特征字符串是采用前缀匹配算法进行匹配的，即只要命令行中关键字的首部若干连续字符或全部字符与规则中定义的关键字相匹配，就认为该命令行与此规则匹配。因此，命令特征字符串中可以包括完整的或部分的命令关键字。例如，若规则“rule 1 deny command dis arp source *”生效，则命令 **display arp source-mac interface** 和命令 **display arp source-suppression** 都会被禁止执行。
- 基于命令的规则只对指定视图下的命令生效。若用户输入的命令在当前视图下不存在而在其父视图下被查找到时，用于控制当前视图下的命令的规则不会对其父视图下的命令执行权限进行控制。例如，定义一条规则“rule 1 deny command system ; interface * ; *”禁止用户执行接口视图下的任何命令。当用户在接口视图下输入命令 **acl basic** 3000 时，该命令仍然可以成功执行，因为系统在接口视图下搜索不到指定的 **acl** 命令时，会回溯到系统视图（父视图）下执行，此时该规则对此命令不生效。
- **display** 命令中的重定向符（“|”、“>”、“>>”）及其后面的关键字不被作为命令行关键字参与规则的匹配。例如，若规则“rule 1 permit command display debugging”生效，则命令 **display debugging > log** 是被允许执行的，其中的关键字**> log** 将被忽略，RBAC 只对重定向符前面的命令行 **display debugging** 进行匹配。但是，如果在规则中配置了重定向符，则 RBAC 会将其作为普通字符处理。例如，若规则“rule 1 permit command display debugging > log”生效，则命令 **display debugging > log** 将会匹配失败，因为其中的关键字**> log** 被 RBAC 忽略了，最终是命令 **display debugging** 与规则进行匹配。因此，配置规则时不要使用重定向符。

用户访问 SNMP OID 时，系统遵循以下匹配规则：

- 与用户访问的 OID 形成最长匹配的规则生效。例如用户访问的 OID 为 1.3.6.1.4.1.25506.141.3.0.1，角色中存在“rule 1 permit read write oid 1.3.6”，“rule 2 deny read write oid 1.3.6.1.4.1”和“rule 3 permit read write oid 1.3.6.1.4”，其中 rule 2 与用户访问的 OID 形成最长匹配，则认为 rule 2 与 OID 匹配，匹配的结果为用户的此访问请求被拒绝。
- 对于定义的 OID 长度相同的规则，规则编号大的生效。例如用户访问的 OID 为 1.3.6.1.4.1.25506.141.3.0.1，角色中存在“rule 1 permit read write oid 1.3.6”，“rule 2 deny read write oid 1.3.6.1.4.1”和“rule 3 permit read write oid 1.3.6.1.4.1”，其中 rule 2 和 rule 3 与访问的 OID 形成最长匹配，则 rule 3 生效，匹配的结果为用户的访问请求被允许。

3.4.3 密码管理

为了提高用户登录密码的安全性，可通过定义密码管理策略对用户的登录密码进行管理，并对用户的登录状态进行控制。

1. 密码长度检查

管理员可以限制用户密码的最小长度。当设置用户密码时，如果输入的密码长度小于设置的最小长度，系统将不允许设置该密码。

2. 密码组合检查

管理员可以设置用户密码的组成元素的组合类型，以及至少要包含每种元素的个数。密码的组成元素包括以下 4 种类型：

- [A～Z]

- [a～z]
- [0～9]
- 32 个特殊字符（空格~`!@#$%^&*()_+-={}|[]\:";'<>,./）

密码元素的组合类型有 4 种，具体涵义如下：

- 组合类型为 1 表示密码中至少包含 1 种元素；
- 组合类型为 2 表示密码中至少包含 2 种元素；
- 组合类型为 3 表示密码中至少包含 3 种元素；
- 组合类型为 4 表示密码中包含 4 种元素。

当用户设置密码时，系统会检查设定的密码是否符合配置要求，只有符合要求的密码才能设置成功。

3. 密码复杂度策略

为确保用户的登录密码具有较高的复杂度，要求管理员为其设置的密码必须符合一定的复杂度要求，只有符合要求的密码才能设置成功。目前，可配置的复杂度要求包括：

- 密码中不能包含连续三个或以上的相同字符。例如，密码“a111”就不符合复杂度要求。
- 密码中不能包含用户名或者字符顺序颠倒的用户名。例如，用户名为“abc”，那么“abc982”或者“2cba”之类的密码就不符合复杂度要求。

4. 密码更新管理

管理员可以设置用户登录设备后修改自身密码的最小间隔时间。当用户登录设备修改自身密码时，如果距离上次修改密码的时间间隔小于配置值，则系统不允许修改密码。例如，管理员配置用户密码更新间隔时间为 48 小时，那么用户在上次修改密码后的 48 小时之内都无法成功进行密码修改操作。

有两种情况下的密码更新并不受该功能的约束：用户首次登录设备时系统要求用户修改密码；密码老化后系统要求用户修改密码。

5. 密码老化管理

当用户登录密码的使用时间超过老化时间后，需要用户更换密码。如果用户输入的新密码不符合要求，或连续两次输入的新密码不一致，系统将要求用户重新输入。对于 FTP 用户，密码老化后，只能由管理员修改 FTP 用户的密码；对于 Telnet、SSH、Terminal（通过 Console 口或 AUX 口登录设备）用户可自行修改密码。

6. 密码过期提醒

在用户登录时，系统判断其密码距离过期的时间是否在设置的提醒时间范围内。如果在提醒时间范围内，系统会提示该密码还有多久过期，并询问用户是否修改密码。如果用户选择修改，则记录新的密码及其设定时间。如果用户选择不修改或者修改失败，则在密码未过期的情况下仍可以正常登录。对于 FTP 用户，只能由管理员修改 FTP 用户的密码；对于 Telnet、SSH、Terminal（通过 Console 口或 AUX 口登录设备）用户可自行修改密码。

7. 密码老化后允许登录

管理员可以设置用户密码过期后在指定的时间内还能登录设备指定的次数。这样，密码老化的用户不需要立即更新密码，依然可以登录设备。例如，管理员设置密码老化后允许用户登录的时间为 15 天、次数为 3 次，那么用户在密码老化后的 15 天内，还能继续成功登录 3 次。

8. 密码历史记录

系统保存用户密码历史记录。当用户修改密码时，系统会要求用户设置新的密码，如果新设置的密码以前使用过，且在当前用户密码历史记录中，系统将给出错误信息，提示用户密码更改失败。另外，用户更改密码时，系统会将新设置的密码逐一与所有记录的历史密码以及当前密码比较，要求新密码至少要与旧密码有 4 字符不同，且这 4 个字符必须互不相同，否则密码更改失败。

可以配置每个用户密码历史记录的最大条数，当密码历史记录的条数超过配置的最大历史记录条数时，新的密码历史记录将覆盖该用户最老的一条密码历史记录。

由于为用户配置的密码在哈希运算后以密文的方式保存，配置一旦生效后就无法还原为明文密码，因此，用户的当前登录密码，不会被记录到该用户的密码历史记录中。

9. 密码尝试次数限制

密码尝试次数限制可以用来防止恶意用户通过不断尝试来破解密码。

每次用户认证失败后，系统会将该用户加入密码管理的黑名单。可加入密码管理功能黑名单的用户包括：FTP 用户和通过 VTY 方式访问设备的用户。不会加入密码管理功能黑名单的用户包括：用户名不存在的用户、通过 Console 口或 AUX 口连接到设备的用户。

当用户连续尝试认证的失败累加次数达到设置的尝试次数时，系统对用户的后续登录行为有以下三种处理措施：

- 永久禁止该用户登录。只有管理员把该用户从密码管理的黑名单中删除后，该用户才能重新登录。
- 禁止该用户一段时间后，再允许其重新登录。当配置的禁止时间超时或者管理员将其从密码管理的黑名单中删除，该用户才可以重新登录。
- 不对该用户做禁止，允许其继续登录。在该用户登录成功后，该用户会从密码管理的黑名单中删除。

10. 用户帐号闲置时间管理

管理员可以限制用户帐号的闲置时间，禁止在闲置时间之内始终处于不活动状态的用户登录。若用户自从最后一次成功登录之后，在配置的闲置时间内再未成功登录过，那么该闲置时间到达之后此用户帐号立即失效，系统不再允许使用该帐号的用户登录。

3.5 系统设置

系统设置功能用来对设备的名称、位置等信息以及设备时间进行设置。

3.5.1 系统时间获取方式

为了便于管理，并保证与其它设备协调工作，设备需要准确的系统时间。系统时间由 GMT 时间、本地时区和夏令时运算之后联合决定。用户有两种方式获取 GMT 时间：

- 手工配置 GMT 时间。
- 通过 NTP/SNTP 协议获取 GMT 时间。

通过 NTP/SNTP 协议获取的 GMT 时间比命令行配置的 GMT 时间更精确。

3.5.2 NTP/SNTP简介

NTP（Network Time Protocol，网络时间协议）可以用来在分布式时间服务器和客户端之间进行时间同步，使网络内所有设备的时间保持一致，从而使设备能够提供基于统一时间的多种应用。

SNTP（Simple NTP，简单 NTP）采用与 NTP 相同的报文格式及交互过程，但简化了 NTP 的时间同步过程，以牺牲时间精度为代价实现了时间的快速同步，并减少了占用的系统资源。在时间精度要求不高的情况下，可以使用 SNTP 来实现时间同步。

3.5.3 NTP/SNTP时钟源工作模式

NTP支持服务器模式和对等体模式两种时钟源工作模式，如 表 3-3 所示。在服务器模式中，设备只能作为客户端；在对等体模式中，设备只能作为主动对等体。

SNTP 只支持服务器模式这一种时钟源工作模式。在该模式中，设备只能作为客户端，从 NTP 服务器获得时间同步，不能作为服务器为其他设备提供时间同步。

表3-4 NTP 时钟源工作模式

模式	工作过程	时间同步方向	应用场合
服务器模式	客户端上需要手工指定NTP服务器的地址。客户端向NTP服务器发送NTP时间同步报文。NTP服务器收到报文后会自动工作在服务器模式，并回复应答报文 一个客户端可以配置多个时间服务器，如果客户端从多个时间服务器获取时间同步，则客户端收到应答报文后，进行时钟过滤和选择，并与优选的时钟进行时间同步	客户端能够与NTP服务器的时间同步 NTP服务器无法与客户端的时间同步	该模式通常用于下级的设备从上级的时间服务器获取时间同步
对等体模式	主动对等体（Symmetric active peer）上需要手工指定被动对等体（Symmetric passive peer）的地址。主动对等体向被动对等体发送NTP时间同步报文。被动对等体收到报文后会自动工作在被动对等体模式，并回复应答报文 如果主动对等体可以从多个时间服务器获取时间同步，则主动对等体收到应答报文后，进行时钟过滤和选择，并与优选的时钟进行时间同步	主动对等体和被动对等体的时间可以互相同步 如果双方的时钟都处于同步状态，则层数大的时钟与层数小的时钟的时间同步	该模式通常用于同级的设备间互相同步，以便在同级的设备间形成备份。如果某台设备与所有上级时间服务器的通信出现故障，则该设备仍然可以从同级的时间服务器获得时间同步

3.5.4 NTP/SNTP时钟源身份验证

NTP/SNTP 时钟源身份验证功能可以用来验证接收到的 NTP 报文的合法性。只有报文通过验证后，设备才会接收该报文，并从中获取时间同步信息；否则，设备会丢弃该报文。从而，保证设备不会与非法的时间服务器进行时间同步，避免时间同步错误。

目 录

1 无线配置

1.1 无线网络

1.1.1 无线接入

无线网络为用户提供 WLAN 接入服务。无线服务的骨干网通常使用有线电缆作为线路连接安置在固定网络，接入点设备安置在需要覆盖无线网络的区域，用户在该区域内就可以通过无线接入的方式接入无线网络。

1. 无线服务

无线服务即一类无线服务属性的集合，如无线网络的 SSID、认证方式（开放系统认证或者共享密钥认证）等。

2. SSID

SSID（Service Set Identifier，服务集标识符），就是无线网络的名称。

3. 隐藏SSID

AP 将 SSID 置于 Beacon 帧中向外广播发送。若 BSS（Basic Service Set，基本服务集）的客户端数量已达到上限或 BSS 一段时间内不可用即客户端不能上线，不希望其它客户端上线，则可以配置隐藏 SSID。若配置了隐藏 SSID，AP 不将 SSID 置于 Beacon 帧中，还可以借此保护网络免遭攻击。为了进一步保护无线网络，AP 对于广播 Probe Request 帧也不会回复。此时客户端若想连接此 BSS，则需要手工指定该 SSID，这时客户端会直接向该 AP 发送认证及关联报文连接该 BSS。

4. 数据转发

可以在 AC 上将客户端数据报文转发位置配置在 AC 或者 AP 上。

- 将数据报文转发位置配置在 AC 上时，为集中式转发，客户端的数据流量由 AP 通过 CAPWAP 隧道透传到 AC，由 AC 转发数据报文；
- 将数据报文转发位置配置在 AP 上时，为本地转发，客户端的数据流量直接由 AP 进行转发。将转发位置配置在 AP 上缓解了 AC 的数据转发压力；
- 将转发位置配置在 AP 上时，可以指定 VLAN，即只有处于指定 VLAN 的客户端，在 AP 上转发其数据流量。

5. 绑定无线服务

无线服务跟 AP 的 Radio 存在多对多的映射关系，将无线服务绑定在某个 AP 的射频上，AP 会根据射频上绑定的无线服务的属性创建 BSS。BSS 是无线服务提供服务的基本单元。在一个 BSS 的服务区域内（这个区域是指射频信号覆盖的范围），客户端能够通过同一个 SSID 访问网络。

绑定无线服务时，可以进行如下配置：

- 可以为该 BSS 指定一个 VLAN 组，该 BSS 下连接的客户端会被均衡地分配在 VLAN 组的所有 VLAN 中，既能将客户端划分在不同广播域中，又能充分利用不连续的地址段为客户端分配 IP 地址。
- 可以绑定 NAS-Port-ID 和 NAS-ID，用于网络服务提供者标识客户端的接入位置，区分流量来源。按照网络服务提供者的标准，不同的 NAS-Port-ID 对应不同的位置信息。

- 可以配置 SSID 隐藏。

1.1.2 链路层认证

最初 802.11 的安全机制被称为 Pre-RSNA 安全机制，它的认证机制不完善，容易被攻破，存在安全隐患，且在 WEP 加密机制中，由于连接同一 BSS 下的所有客户端都使用同一加密密钥和 AP 进行通信，一旦某个用户的密钥泄露，那么所有用户的数据都可能被窃听或篡改，所以 IEEE 制订了 802.11i 协议来加强无线网络的安全性。

但 802.11i 仅对无线网络的数据报文进行加密保护，而不对管理帧进行保护，所以管理帧的机密性、真实性、完整性无法保证，容易受到仿冒或监听，例如：恶意攻击者通过获取设备的 MAC 地址并仿冒设备恶意拒绝客户端认证或恶意结束设备与客户端的关联。802.11w 无线加密标准建立在 802.11i 框架上，通过保护无线网络的管理帧来解决上述问题，进一步增强无线网络的安全性。

1. Pre-RSNA安全机制

Pre-RSNA 安全机制采用开放式系统认证（Open system authentication）和共享密钥认证（Shared key authentication）两种认证方式来进行客户端认证，并且采用 WEP 加密方式对数据进行加密来保护数据机密性，以对抗窃听。WEP 加密使用 RC4 加密算法（一种流加密算法）实现数据报文的加密，WEP 加密支持 WEP40、WEP104 和 WEP128 三种密钥长度。

2. RSNA安全机制

802.11i 安全机制又被称为 RSNA（Robust Security Network Association，健壮安全网络连接）安全机制，包括 WPA（Wi-Fi Protected Access，Wi-Fi 保护访问）和 RSN（Robust Security Network，健壮安全网络）两种安全模式，采用 AKM（Authentication and Key Management，身份认证与密钥管理）对用户身份的合法性进行认证，对密钥的生成、更新进行动态管理，并且采用 TKIP（Temporal Key Integrity Protocol，临时密钥完整性协议）和 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）加密机制对报文进行加密。

AKM 分为 802.1X、Private-PSK 和 PSK 和三种模式：

- 802.1X：采用 802.1X 认证对用户进行身份认证，并在认证过程中生成 PMK（Pairwise Master Key，成对主密钥），客户端和 AP 使用该 PMK 生成 PTK（Pairwise Transient Key，成对临时密钥）。
- Private-PSK：采用 PSK（Pre-Shared Key，预共享密钥）认证进行身份认证，使用客户端的 MAC 地址作为 PSK 密钥生成 PMK，客户端和 AP 使用该 PMK 生成 PTK。
- PSK：采用 PSK 认证进行身份认证，并通过 PSK 密钥生成 PMK，客户端和 AP 使用该 PMK 生成 PTK。

(1) 密钥种类

802.11i 协议中密钥主要包括 PTK 和 GTK（Group Temporal Key，群组临时密钥）两种：

- PTK 用于保护单播数据。
- GTK 用于保护组播和广播数据。

(2) WPA 安全模式密钥协商

WPA 是一种比 WEP 加密性能更强的安全机制。在 802.11i 协议完善前，采用 WPA 为用户提供一个临时性的 WLAN 安全增强解决方案。在 WPA 安全网络中，客户端和 AP 通过使用 EAPOL-Key 报文进行四次握手协商出 PTK，通过使用 EAPOL-Key 报文进行二次组播握手协商出 GTK。

(3) RSN 安全模式密钥协商

RSN 是按照 802.11i 协议为用户提供的一种 WLAN 安全解决方案。在 RSN 网络中，客户端和 AP 通过使用 EAPOL-Key 类型报文进行四次握手协商出 PTK 和 GTK。

(4) 密钥更新

如果客户端长时间使用一个密钥，或携带当前网络正在使用的组播密钥离线，此时网络被破坏的可能性很大，安全性就会大大降低。WLAN 网络通过身份认证与密钥管理中的密钥更新机制来提高 WLAN 网络安全性。密钥更新包括 PTK 更新和 GTK 更新。

- PTK 更新：PTK 更新是对单播数据报文的加密密钥进行更新的一种安全手段，采用重新进行四次握手协商出新的 PTK 密钥的更新机制，来提高安全性。
- GTK 更新：GTK 更新是对组播数据报文的加密密钥进行更新的一种安全手段，采用重新进行两次组播握手协商出新的 GTK 密钥的更新机制，来提高安全性。

(5) 忽略授权信息

授权信息包括 VLAN、ACL 和 User Profile，分为 RADIUS 服务器下发的授权信息和设备本地下发的授权信息。若用户不想使用授权信息，则可以配置忽略授权信息。

(6) 入侵检测

当设备检测到一个未通过认证的用户试图访问网络时，如果开启入侵检测功能，设备将对其所在的 BSS 采取相应的安全策略。

入侵检测所采取的安全模式，包括以下几种：

- 将用户 MAC 地址加入到阻止 MAC 地址列表：缺省模式。如果设备检测到未通过认证用户的关联请求报文，临时将该报文的源 MAC 地址加入阻塞 MAC 地址列表中，在一段时间内，源 MAC 地址为此非法 MAC 地址的无线客户端将不能和 AP 建立连接，在这段时间过后恢复正常。该 MAC 地址的阻塞时间由阻塞非法入侵用户时长决定。
- 关闭收到非法报文的无线服务：关闭收到未通过认证用户的关联请求报文的 BSS 一段时间，该时间由临时关闭服务时长决定。
- 关闭所有无线服务：直接关闭收到未通过认证用户的关联请求报文的 BSS 所提供的服务，直到用户在 Radio 口上重新生成该 BSS。

(7) 加密套件

由于 WEP 加密易破解，一旦攻击者收集到足够多的有效数据帧进行统计分析，那么将会造成数据泄露，无线网络将不再安全。802.11i 增加了 TKIP 和 CCMP 两种加密套件来保护用户数据安全，以下分别介绍。

a. TKIP

TKIP 加密机制依然使用 RC4 算法，所以不需要升级原来无线设备的硬件，只需通过软件升级的方式就可以提高无线网络的安全性。相比 WEP 加密机制，TKIP 有如下改进：

- 通过增长了算法的 IV（Initialization Vector，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；
- 采用和 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；
- 支持 TKIP 反制功能。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 TKIP 反制功能，此时，AP 将通过关闭一段时间无线服务的方式，实现对无线网络攻击的防御。

b. CCMP

CCMP 加密机制使用 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，CCMP 使得无线网络安全有了极大的提高。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使用不同的 PN，在一定程度上提高安全性。

1.1.3 认证模式

1. 静态PSK密钥

PSK 认证方式需要在 AP 侧预先输入预共享密钥，在客户端关联过程中，手动输入该密钥，AP 和客户端通过四次握手密钥协商来验证客户端的预共享密钥的合法性，若 PTK 协商成功，则证明该用户合法，以此来达到认证的目的。

2. 802.1X认证

设备端支持采用 EAP 中继方式或 EAP 终结方式与远端 RADIUS 服务器交互。若用户认证位置在 AP 上，则 AP 为认证设备，由 AP 处理认证过程，若用户认证位置在 AC 上，则 AC 为认证设备，由 AC 处理认证过程。

- 握手功能：使能 802.1X 握手功能之后，设备将定期向通过 802.1X 认证的在线用户发送握手报文，即单播 EAP-Request/Identity 报文，来检测用户的在线状态。
- 安全握手功能：802.1X 安全握手是指在握手报文中加入验证信息，以防止非法用户仿冒正常用户的在线的 802.1X 的客户端与设备进行握手报文的交互。使能 802.1X 安全握手功能后，支持安全握手的客户端需要在每次向设备发送的握手应答报文中携带验证信息，设备将其与认证服务器下发的验证信息进行对比，如果不一致，则强制用户下线。
- 在无线服务下启动了 802.1X 的周期性重认证功能后，设备会根据周期性重认证定时器设定的时间间隔定期向在线 802.1X 用户发起重认证，以检测用户连接状态的变化、确保用户的正常在线，并及时更新服务器下发的授权属性（例如 ACL、VLAN、User Profile）。

3. 静态WEP密钥

在 Pre-RSNA 安全机制的 WEP 加密机制中，由于连接同一 BSS 下的所有客户端都使用同一加密密钥和 AP 进行通信，一旦某个用户的密钥泄露，那么所有用户的数据都可能被窃听或篡改，因此 802.11 提供了动态 WEP 加密机制。在动态 WEP 加密机制中，加密单播数据帧的 WEP 密钥是由客户端和认证服务器通过 802.1X 认证协商产生，保证了每个客户端使用不同的 WEP 单播密钥，从而提高了单播数据帧传输的安全性。组播密钥是 WEP 密钥，若未配置 WEP 密钥，则 AP 使用随机算法产生组播密钥。

当客户端通过 802.1X 认证后，AP 通过发送 RC4 EAPOL-Key 报文将组播密钥及密钥 ID 以及单播密钥的密钥 ID（固定为 4）分发给客户端。

1.2 AP管理

随着无线网络的大规模发展，当大量部署 AP（Access Point，接入点）时，AP 升级软件、射频参数的配置和调整等管理工作将给用户带来高昂的管理成本。为解决这一问题，WLAN 采用 AC+Fit AP 架构，即通过 AC（Access Controller，接入控制器）对下属的 AP 进行集中控制和管理，AP 不需

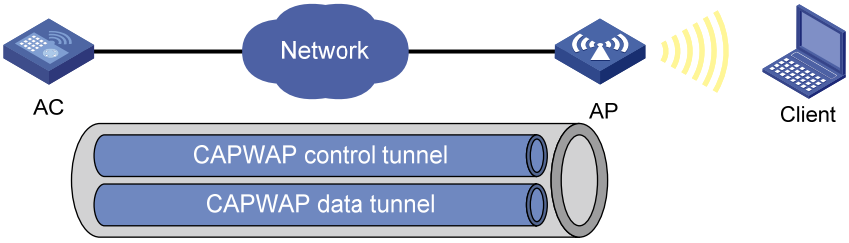
要任何配置，所有的配置都保存在 AC 上并由 AC 下发，同时由 AC 对 AP 进行统一的管理和维护，AP 和 AC 间采用 CAPWAP（Controlling and Provisioning of Wireless Access Point，无线接入点控制与供应）隧道进行通讯，用于传递数据报文和控制报文。

1.2.1 CAPWAP隧道

CAPWAP 隧道为 AP 和 AC 之间的通信提供了通用的封装和传输机制，CAPWAP 隧道使用 UDP 协议作为传输协议，并支持 IPv4 和 IPv6 协议。

如 图 1-1 所示，AC通过CAPWAP协议与AP建立控制隧道和数据隧道，AC通过控制隧道对AP进行管理和监控，通过数据隧道转发客户端的数据报文。

图1-1 CAPWAP 隧道典型组网图



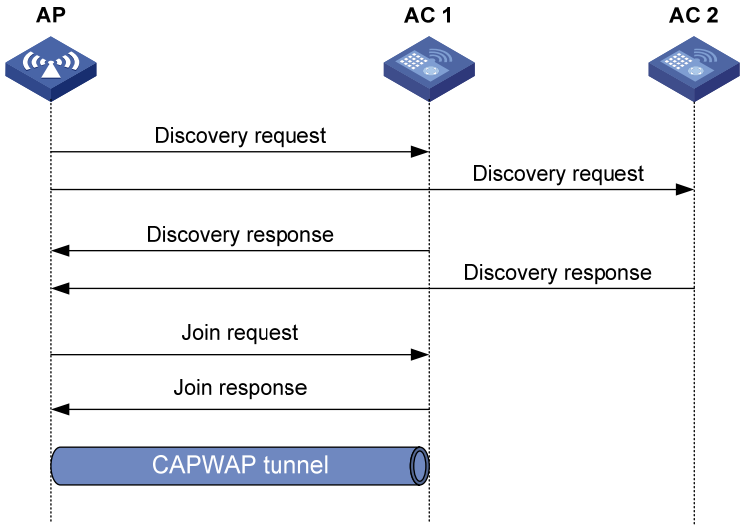
2. 获取AC地址

AP 零配置启动后，AP 会自动创建 VLAN-interface 1，并在该接口上默认开启 DHCP 客户端、DHCPv6 客户端和 DNS 客户端功能，完成上述操作后，AP 将使用获取的 AC 地址发现 AC 并建立 CAPWAP 隧道。AP 获取 AC 地址的方式如下：

- 静态配置：通过预配置为 AP 手工指定 AC 的 IP 地址。
- DHCP 选项：通过 DHCP 服务器返回的 Option 138 或 Option 43 选项获取 AC 地址。若通过两个选项都获取了 AC 地址，则 AP 选择从 Option 138 获取的地址作为 AC 地址，并向 AC 地址发送单播 Discovery request 报文来发现、选择 AC 并建立 CAPWAP 隧道。有关 Option 选项的详细介绍请参见“系统功能介绍”中的 DHCP 及 DNS。
- DNS：AP 通过 DHCP 服务器获取 AC 的域名后缀及 DNS server 的 IP 地址，再将从自身获取的主机名与域名后缀形成 AC 的完整域名进行 DNS 解析，获取 AC 地址，AP 向获取的所有 AC 地址发送单播 Discovery request 报文来发现、选择 AC 并建立 CAPWAP 隧道。
- 广播：AP 通过向 IPv4 广播地址 255.255.255.255 发送 Discovery request 广播报文来发现、选择 AC 并建立隧道。
- IPv4 组播：AP 通过向 IPv4 组播地址 224.0.1.140 发送 Discovery request 组播报文来发现、选择 AC 并建立隧道。
- IPv6 组播：AP 通过向 IPv6 组播地址 FF0E::18C 发送 Discovery request 组播报文来发现、选择 AC 并建立隧道。

3. CAPWAP建立隧道过程

图1-2 CAPWAP 隧道建立过程



AP 发现 AC 并建立 CAPWAP 隧道过程如下：

(1) AP 向 AC 地址发送 Discovery request 报文。

(2) AC 收到 Discovery request 报文后，根据本地策略和报文内容决定是否对 AP 进行回复 Discovery response 报文，Discovery response 报文中会携带优先级值、AC 上是否存在该 AP 的信息和 AC 上的负载信息等，以此实现 AC 选择 AP。

(3) AP 收到各个 AC 的 Discovery response 报文后，根据报文中携带的内容，选择最优 AC。

(4) AP 向选择的最优 AC 发送 Join request 报文。

(5) AC 根据报文内容，检查是否为该 AP 提供服务，并回复 Join response 报文。

(6) AP 若收到 Result Code 为失败的 Join response 报文，则不建立隧道；若 AP 收到 Result Code 为成功的 Join response 报文，则 AP 和 AC 成功建立隧道。

AP 依次使用静态配置、DHCP 选项、DNS、广播、IPv4 组播和 IPv6 组播获取的 AC 地址进行发现 AC 并建立隧道过程，若某一种方式成功建立 CAPWAP 隧道，则停止发现 AC 的过程。

1.2.2 AP组

AP 组用来实现对批量 AP 的配置管理，通过使 AP 继承其所属组的配置来达到对大量 AP 的配置的目的。AP 组配置，全局配置及 AP 配置共同构成了分级继承的 AP 运行配置。在大规模无线网络中，同一 AC 管理的 AP 数量可达几万台，对每一台 AP 逐一配置将导致网络管理难度极大提高。AP 组用来降低逐个配置 AP 的操作成本，用户可以创建多个组，对不同的组用户可以根据需要配置不同的 AP 配置。

所有 AP 缺省情况下均属于默认组，默认组组名为 default-group，默认组不需创建、不可删除。

AP 组可以指定多个 AP 名称、AP 序列号、AP MAC 地址和 AP IP 地址四种入组规则，AP 的入组匹配顺序为：优先根据 AP 名字入组规则匹配入组，其次是 AP 序列号入组规则，然后是 AP MAC 地址入组规则，最后是 AP IP 地址入组规则，若未匹配到任何入组规则，则 AP 将被加入到默认组。

需要注意的是：

- AP 必须属于一个 AP 组，且只能属于一个 AP 组。
- 同一入组规则不能重复出现在不同的 AP 组中，若将同一入组规则配置在新 AP 组中，将导致原 AP 组中对应的入组规则自动删除（相当于迁移组）。
- 默认组不能配置 AP 名字、AP 序列号、AP MAC 和 AP IP 地址四种入组规则。
- 删除 AP 入组规则，AP 会根据 AP 的入组规则匹配顺序重新匹配 AP 组。比如，删除某一 AP 组下的一个 AP 名字入组规则，该 AP 会优先进入指定了该 AP 序列号的 AP 组，如果匹配不到 AP 序列号，则该 AP 会优先进入指定了该 AP MAC 地址入组规则的 AP 组，如果匹配不到 AP MAC 地址，则该 AP 会优先进入指定了该 AP IP 地址入组规则的 AP 组，如果仍然匹配不到，则该 AP 会进入默认组。
- AP 组下有 AP 已经入组（手工 AP 或自动 AP），则该 AP 组不允许删除；配置了入组规则，但是没有 AP 入组的 AP 组可以被删除。
- AP 的生效配置取决于 AP、AP 组及 AP 全局配置中优先级最高的配置，优先级从高到低为 AP 配置、AP 组配置、全局配置。若优先级高的配置不存在，则 AP 使用优先级低的配置。若都不存在 AP 的配置，则使用缺省值。

1.2.3 全局配置

全局配置作用于所有 AP 组下的 AP，由于全局配置的优先级最低，所以仅当 AP 和 AP 组下无配置时，才会继承全局配置。AP、AP 组及全局配置的优先级从高到低为 AP 视图配置、AP 组视图配置、全局视图配置。若优先级高的配置不存在，则 AP 使用优先级低的配置；若都不存在 AP 的配置，则使用优先级最低的视图下的缺省配置。

1.2.4 预配置

通常情况下，可以通过终端连接到 AP 之后，对 AP 进行配置，但这种逐台配置 AP 的操作方式不利于大规模的 AP 部署以及集中化管理。AP 预配置提供了一种在 AC 上对 AP 的基本网络参数进行配置，并将预配置信息下发至 AP 的方法。下发到 AP 的配置会保存为 AP 私有预配置文件 wlan_ap_prvs.xml，当 AP 重启时，该私有预配置文件才会生效。

需要注意的是：

- AC 只能将预配置信息发送给与它建立 CAPWAP 隧道的 AP，同时只有主 AC 才能对已经与它建立 CAPWAP 隧道的 AP 进行预配置。
- 一些预配置可以在 AP 预配置下和 AP 组预配置下都进行配置，则优先使用 AP 预配置下的配置。

预配置提供的配置包括：

- 配置 AP 与指定的 AC 建立 CAPWAP 隧道。
- 配置 AP 的 IP 地址。
- 配置 AP 的网关地址。
- 配置 AP 发现 AC 时使用的域名服务器的域名后缀。
- 配置 AP 发现 AC 时使用的域名服务器的 IP 地址。
- 配置 802.1X Client。

1.2.5 区域码

区域码决定了射频可以使用的工作频段、信道、发射功率级别等。在配置 WLAN 设备时，必须正确地设置区域码，以确保不违反当地的管制规定。为了防止区域码的修改导致射频的工作频段、信道等与所在国家或地区的管制要求冲突，可以开启区域码锁定功能。

1.2.6 自动AP

在无线网络中部署的 AP 数量较多时，开启自动 AP 功能可以简化配置。开启自动 AP 功能后，无需配置手工 AP 配置，AP 和 AC 就可以建立 CAPWAP 连接，AC 将以 AP 的 MAC 地址来命名上线的自动 AP。在 AP 发现 AC 过程中，AP 优先选择存在手工 AP 的 AC 建立 CAPWAP 隧道连接，若不存在手工 AP 配置，则 AP 会从开启自动 AP 功能的 AC 中，选择最优 AC 进行 CAPWAP 隧道连接。自动 AP 功能生成的 AP，没有提供 AP 视图进行相关参数配置，自动 AP 需要固化为手工 AP 或者通过 AP 组进行配置。

出于网络安全因素考虑，自动 AP 应配合固化功能或 AP 认证功能共同使用。若配置固化功能时，用户应在自动 AP 第一次接入后，将所有自动 AP 固化为手工 AP 并关闭自动 AP 功能。

1.2.7 AC备份

在集中式转发模式下，AC 在汇聚层上承担了大量 AP 的状态维护和数据转发工作。AC 设备的故障将导致无线网络的服务中断。

通过 AC 备份功能，可以将两台 AC 相连，构建一个备份组，备份组中的两台 AC 分别为主 AC 和备 AC，主备 AC 通过 WHA（WLAN High Availability，无线局域网高可靠性）数据备份通道进行 AP 数据的同步，当主 AC 发生故障时，备 AC 能够立即接管当前所有在线 AP，使业务流量不中断。

1.2.8 配置准备

CAPWAP 隧道的建立需要 DHCP 和 DNS 的配合。因此，首先需要完成以下配置任务：

- AP 需要获取到自身的 IP 地址，因此需要在 DHCP server 上配置地址池为 AP 分配 IP 地址。
- 若获取 AC 地址的方式为 DHCP 选项方式，则需要在 DHCP server 上将对应地址池的 Option 138 或 Option 43 配置为 AC 的 IPv4 地址，或使用 Option 52 配置 AC 的 IPv6 地址。
- 若获取 AC 地址的方式为 DNS 方式，则需要在 DHCP server 对应的地址池上配置 DNS server 的 IP 地址和 AC 的域名后缀。并在 DNS server 上创建区域，添加 AC 的 IP 地址和域名的映射。
- 保证 AC 和 AP 之间的路由可达。

有关 DHCP 和域名解析的详细介绍和相关配置，请参见“系统功能介绍”中的 DHCP 及 DNS。

1.3 客户端限速

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

1.3.1 客户端限速模式

客户端限速功能有两种工作模式：

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

动态模式与静态模式仅用于配置基于无线服务模板或基于射频方式的客户端限速功能。

1.3.2 客户端限速方式

客户端限速功能有三种配置方式：

- 基于客户端类型：该方式配置的客户端限速对所有客户端生效，每种类型的客户端的速率都不能超过配置的限速值。
- 基于无线服务模板：该方式配置的客户端限速对使用同一个无线服务接入的所有客户端生效。
- 基于射频：该方式配置的客户端限速对使用同一个射频接入的所有客户端生效。

如果同时配置多种方式或不同模式的客户端限速，则多个配置将同时生效，每个客户端的限速值为多种方式及不同模式中的限速速率最小值。

1.4 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。当某个 BSS 的流量非常大时，会挤占其它 BSS 的可用带宽。如果直接对单个 BSS 的报文进行限速，在总体流量较小时，又会导致闲置带宽被浪费。

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

智能带宽保障功能只能对由 AP 发送至客户端的流量（即出方向流量）进行控制。

1.5 无线多媒体

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

IEEE 802.11e 为基于 802.11 协议的 WLAN 体系添加了 QoS 功能，Wi-Fi 组织为了满足不同 WLAN 厂商对 QoS 的需求，定义了 WMM（Wi-Fi Multimedia，Wi-Fi 多媒体）协议。WMM 协议用于保证优先发送高优先级的报文，从而保证语音、视频等应用在无线网络中有更好的服务质量。

1.5.1 WMM状态

在 WMM 状态页面中可以查看 AC 连接的各 AP 是否开启 WMM 功能。

1.5.2 WMM配置

在 WMM 配置页面中，可以配置每个 AP 的 SVP 映射、连接准入控制策略以及允许接入的客户端最大数等信息。

SVP 映射是指将 IP 头中 Protocol ID 为 119 的 SVP 报文放入指定的 AC-VI 或 AC-VO 队列中，保证 SVP 报文比其他数据报文具有更高的优先级。没有进行 SVP 映射时，SVP 报文将进入 AC-BE 队列。

CAC（Connect Admission Control，连接准入控制）用来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。如果客户端需要使用高优先级的 AC，则需要进行请求，AP 按照基于信道利用率的准入策略或基于用户数量的准入策略算法，计算是否允许客户端使用高优先级 AC，并将结果回应给客户端。当单独或同时开启 AC-VO、AC-VI 队列的 CAC 功能时，如果客户端申请 AC 失败，设备会对其进行降级至 AC-BE 处理。

1.5.3 EDCA参数

在 EDCA 参数页面中，可以查看和修改 EDCA 参数和 ACK 策略。

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。

WMM 协议为 AC 定义了以下 EDCA 参数：

- AIFSN（Arbitration Inter Frame Spacing Number，仲裁帧间隙数）：在 802.11 协议中，空闲等待时长（DIFS）为固定值，而 WMM 针对不同 AC 配置退避前需要等待的时隙，AIFSN 数值越小，用户的空闲等待时间越短。
- 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，该 AC 中报文的平均退避时间越长。
- TXOP Limit（Transmission Opportunity Limit，传输机会限制）：AC 中的报文每次竞争成功后，可占用信道的最大时长。这个数值越大，用户一次能占用信道的时长越大。如果是 0，则每次占用信道后只能发送一个报文。

ACK 策略有两种：Normal ACK 和 No ACK。

- Normal ACK 策略：接收者在接收到每个单播报文后，都要回复 ACK 进行确认。
- No ACK（No Acknowledgment）策略：在无线报文交互过程中，不使用 ACK 报文进行接收确认。在通信质量较好、干扰较小的情况下，No ACK 策略能有效提高报文传输效率。但是，在通信质量较差的情况下，如果使用 No ACK 策略，则会造成丢包率增大的问题。

1.5.4 射频与客户端协商参数

在射频与客户端协商参数页面中，用户除了可以查看和修改 EDCA 参数，还可以开启或关闭连接准入控制策略功能。

1.5.5 客户端的WMM统计信息

在客户端的 WMM 统计信息页面中，用户除了可以查看 SSID 等设备的基本信息和数据流量统计信息，还可以查看到客户端接入时指定的 AC 的 APSD 属性。

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

1.5.6 传输流信息

在传输流信息页面中，用户可以查看包括来自有线网络报文的用户优先级、传输流标识、流方向、允许富余带宽等传输流信息。

1.6 WIPS

WIPS（Wireless Intrusion Prevention System，无线入侵防御系统）是针对 802.11 协议开发的二层协议检测和防护功能。WIPS 通过 AC 与 Sensor（开启 WIPS 功能的 AP）对信道进行监听及分析处理，从中检测出威胁网络安全、干扰网络服务、影响网络性能的无线行为或设备，并提供对入侵的无线设备的反制，为无线网络提供一套完整的安全解决方案。

WIPS 由 Sensor、AC 以及网管软件组成。Sensor 负责收集无线信道上的原始数据，经过简单加工后，上传至 AC 进行综合分析。AC 会分析攻击源并对其实施反制，同时向网管软件输出日志信息。网管软件提供丰富的图形界面，提供系统控制、报表输出、告警日志管理功能。

WIPS 支持以下功能：

- 攻击检测：提供多种攻击方式的攻击检测功能。
- 设备分类：通过侦听无线信道的 802.11 报文来识别无线设备，并对其进行分类。
- 反制：对非法设备进行攻击，使其它设备无法关联到非法设备，从而保护用户网络的安全。

1.6.1 开启WIPS

开启 WIPS 功能前，需要将 AP 加入到指定 VSD（Virtual Security Domain，虚拟安全域）中。该 AP 也称为 Sensor。

1.6.2 配置虚拟安全域

通过在虚拟安全域上应用分类策略、攻击检测策略、Signature 策略或反制策略，使已配置的分类策略、攻击检测策略、Signature 策略或反制策略在虚拟安全域内的 Radio 上生效。

1.6.3 配置分类策略

1. 分类策略

可以通过两种配置方式实现设备分类，其中手工分类的优先级高于自动分类。

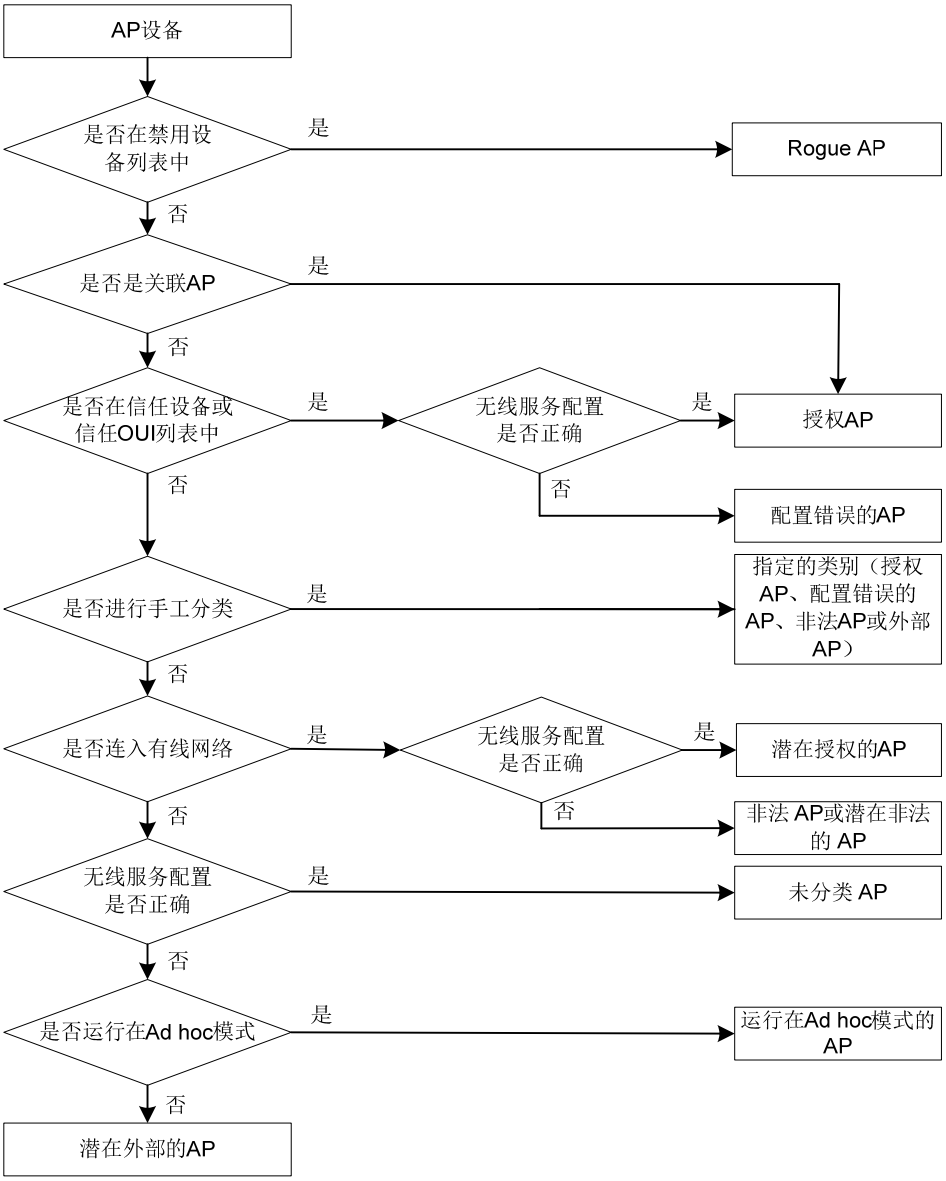
- 自动分类：通过信任设备列表、信任 OUI 列表和静态禁用设备列表对所有设备进行分类；或通过自定义的 AP 分类规则对 AP 设备进行分类。
- 手工分类：通过手动指定 AP 的类型对设备进行分类。

2. AP的分类类别

WIPS 将检测到的 AP 分为以下几类：

- 授权 AP（Authorized AP）：允许在无线网络中使用的 AP。包括已经关联到 AC 上且不在禁用列表中的 AP 和手动指定的授权 AP。
- 非法 AP（Rouge AP）：不允许在无线网络中使用的 AP。包括禁用设备列表中的 AP、不在 OUI 配置文件中的 AP 和手动指定的非法 AP。
- 配置错误的 AP（Misconfigured AP）：无线服务配置错误，但是允许在无线网络中使用的 AP。例如，在信任设备列表中，但使用了非法 SSID 的 AP；在 OUI 配置文件中，但不在禁用设备列表的 AP；在信任 OUI 或是信任设备列表中，但是未与 AC 关联的 AP。
- 外部 AP（External AP）：其他无线网络中的 AP。WIPS 可能会检测到邻近网络中的 AP，例如邻近公司或个人住宅中的 AP。
- Ad hoc：运行在 Ad hoc 模式的 AP。WIPS 通过检测 Beacon 帧将其分类为 Ad hoc。
- 潜在授权的 AP（Potential-authorized AP）：无法确定但可能是授权的 AP。如果 AP 既不在信任设备或信任 OUI 列表中也不在禁用设备列表中，那么该 AP 很可能是授权的 AP，如 Remote AP。
- 潜在非法的 AP（Potential-rogue AP）：无法确定但可能是非法的 AP。如果 AP 既不在信任设备或信任 OUI 列表中也不在禁用设备列表中，而且它的无线服务配置也不正确，那么，如果检测到它的有线端口可能连接到网络中，则认为其为潜在非法的 AP；如果能确定其有线端口连接到网络中，则认为其为非法 AP，如恶意入侵者私自接入网络的 AP。
- 潜在外部的 AP（Potential-external AP）：无法确定但可能是外部的 AP。如果 AP 既不在信任设备或信任 OUI 列表中也不在禁用设备列表中，而且它的无线服务配置也不正确，同时也没有检测到它的有线端口连接到网络中，则该 AP 很可能是外部的 AP。
- 未分类 AP（Uncategorized AP）：无法确定归属类别的 AP。
- WIPS对检测到的AP的分类处理流程如 图 1-3 所示：

图1-3 WIPS 对检测到的 AP 设备的分类处理流程示意图



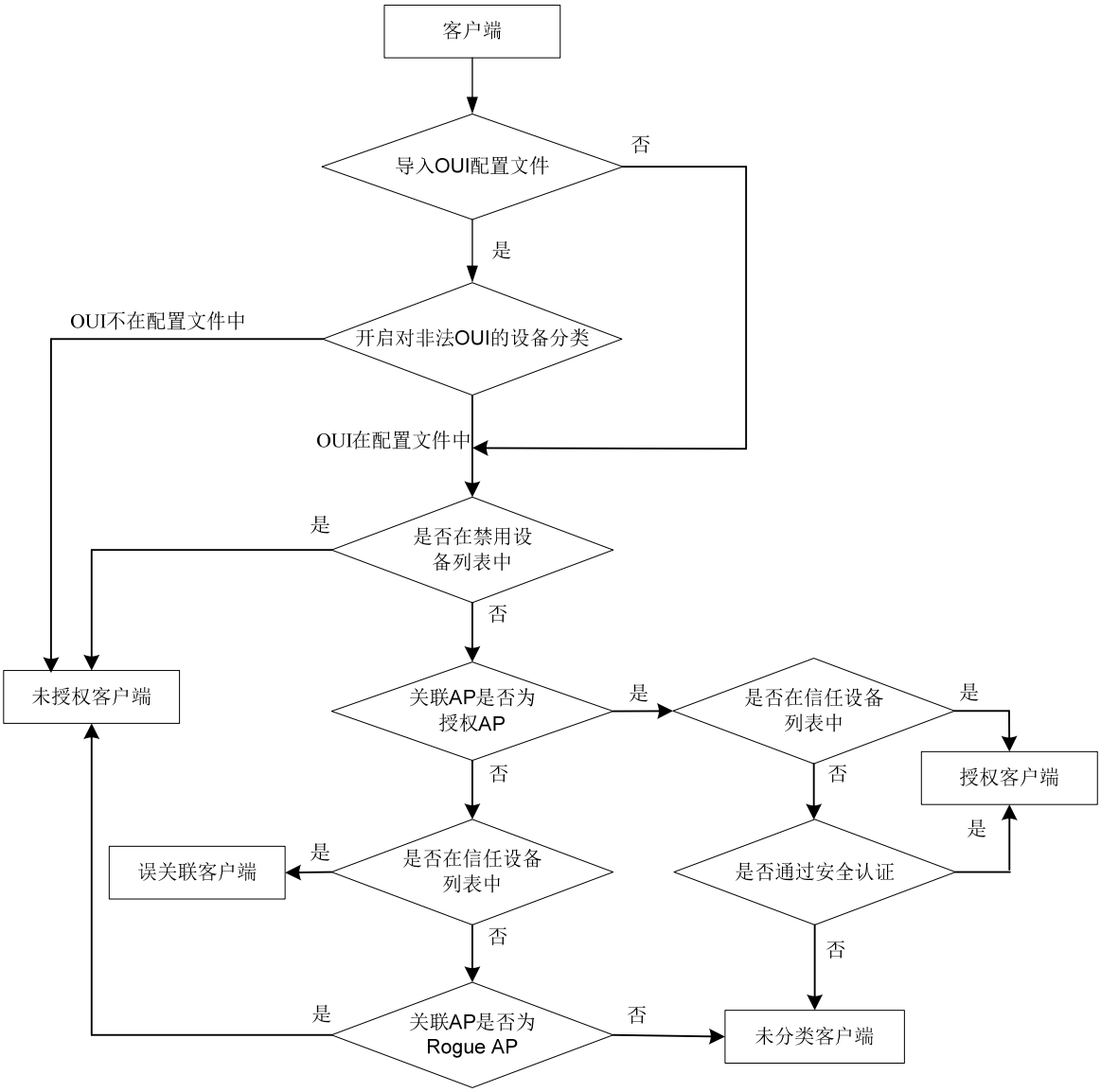
3. 客户端的分类类别

WIPS 将检测到的客户端分为以下几类：

- 授权客户端（Authorized Client）：允许使用的客户端，如关联到授权 AP 上的受信任的客户端或通过加密认证方式关联到授权 AP 上的客户端都是授权的客户端。
- 未授权客户端（Unauthorized Client）：不允许使用的客户端。如在禁用设备列表中的客户端、连接到 Rogue AP 上的客户端以及不在 OUI 配置文件中的客户端都是未授权客户端。
- 错误关联客户端（Misassociation Client）：信任设备列表中的客户端关联到非授权 AP 上。错误关联的客户端可能会对网络信息安全带来隐患。
- 未分类客户端（Uncategorized Client）：无法确定归属类别的客户端。

WIPS对检测到的客户端的分类处理流程如 图 1-4 所示：

图1-4 WIPS 对检测到的客户端的分类处理流程示意图



1.6.4 配置攻击检测策略

WIPS 通过分析侦听到的 802.11 报文，来检测针对 WLAN 网络的无意或者恶意的攻击，并以告警的方式通知网络管理员。

1. 表项学习速率和表项时间参数

如果攻击者通过发送大量报文来增加 WIPS 的处理开销等。通过检测周期内学习到设备的表项来判断是否需要对表项学习进行限速处理。设备在统计周期内学习到的 AP 或客户端表项达到触发告警阈值，设备会发送告警信息，并停止学习 AP 表项和客户端表项。

2. 泛洪攻击检测

泛洪攻击是指通过向无线设备发送大量同类型的报文，使无线设备会被泛洪攻击报文淹没而无法处理合法报文。WIPS 通过持续地监控 AP 或客户端的流量来检测泛洪攻击。当大量同类型的报文超出上限时，认为无线网络正受到泛洪攻击。

目前 WIPS 能够防范的泛洪攻击包括：

- Probe-request/Association-request/Reassociation-request 帧泛洪攻击

攻击者通过模拟大量的客户端向 AP 发送 Probe-request/Association-request/Reassociation-request 帧，AP 收到大量攻击报文后无法处理合法客户端的 Probe-request /Association-request/Reassociation-request 帧。

- Authentication 帧泛洪攻击

攻击者通过模拟大量的客户端向 AP 发送 Authentication 帧，AP 收到大量攻击报文后无法处理合法客户端的 Authentication 帧。

- Beacon 帧泛洪攻击

该攻击是通过发送大量的 Beacon 帧使客户端检测到多个虚假 AP，导致客户端选择正常的 AP 进行连接时受阻。

- Block ACK 泛洪攻击

该攻击通过仿冒客户端发送伪造的 Block ACK 帧来影响 Block ACK 机制的正常运行，导致通信双方丢包。

- RTS/CTS 泛洪攻击

在无线网络中，通信双方需要遵循虚拟载波侦听机制，通过 RTS（Request to Send，发送请求）/CTS（Clear to Send，清除发送请求）交互过程来预留无线媒介，通信范围内的其它无线设备在收到 RTS 和（或）CTS 后，将根据其中携带的信息来延迟发送数据帧。RTS/CTS 泛洪攻击利用了虚拟载波侦听机制的漏洞，攻击者能通过泛洪发送 RTS 和（或）CTS 来阻塞 WLAN 网络中合法无线设备的通信。

- Deauthentication 帧泛洪攻击

攻击者通过仿冒 AP 向与其关联的客户端发送 Deauthentication 帧，使得被攻击的客户端与 AP 的关联断开。这种攻击非常突然且难以防范。单播 Deauthentication 帧攻击是针对某一个客户端，而广播 Deauthentication 帧攻击是针对与该 AP 关联的所有客户端。

- Disassociation 帧泛洪攻击

攻击原理同 Disassociation 帧泛洪攻击。攻击者是通过仿冒 AP 向与其关联的客户端发送 Disassociation 帧，使得被攻击的客户端与 AP 的关联断开。这种攻击同样非常突然且难以防范。

- EAPOL-Start 泛洪攻击

IEEE 802.1X 标准定义了一种基于 EAPOL（EAP over LAN，局域网上的可扩展认证协议）的认证协议，该协议通过客户端发送 EAPOL-Start 帧开始一次认证流程。AP 接收到 EAPOL-Start 后会回复一个 EAP-Identity-Request，并为该客户端分配一些内部资源来记录认证状态。攻击者可以通过模拟大量的客户端向 AP 发送 EAPOL-Start 来耗尽该 AP 的资源，使 AP 无法处理合法客户端的认证请求。

- Null-data 泛洪攻击

该攻击通过仿冒合法客户端向与其关联的 AP 发送 Null-data 帧，使得 AP 误认为合法的客户端进入省电模式，将发往该客户端的数据帧进行暂存。如果攻击者持续发送 Null-data 帧，当暂存帧的存储时间超过 AP 暂存帧老化时间后，AP 会将暂存帧丢弃，妨害了合法客户端的正常通信。

- EAPOL-Logoff 泛洪攻击

在 EAPOL 认证环境中，当通过认证的客户端需要断开连接时，会发送一个 EAPOL-Logoff 帧来关闭与 AP 间的会话。但 AP 对接收到的 EAPOL-Logoff 帧不会进行认证，因此攻击者通过仿冒合法客户端向 AP 发送 EAPOL-Logoff 帧，可以使 AP 关闭与该客户端的连接。如果攻击者持续发送仿冒的 EAPOL-Logoff 帧，将使被攻击的客户端无法保持同 AP 间的连接。

- EAP-Success/Failure 泛洪攻击

在使用 802.1X 认证的 WLAN 环境中，当客户端认证成功时，AP 会向客户端发送一个 EAP-Success 帧（code 字段为 success 的 EAP 帧）；当客户端认证失败时，AP 会向客户端发送一个 EAP-Failure 帧（code 字段为 failure 的 EAP 帧）。攻击者通过仿冒 AP 向请求认证的客户端发送 EAP-Failure 帧或 EAP-Success 帧来破坏该客户端的认证过程，通过持续发送仿冒的 EAP-Failure 帧或 EAP-Success 帧，可以阻止被攻击的客户端与 AP 间的认证。

3. 畸形报文检测

畸形报文攻击是指攻击者向受害客户端发送有缺陷的报文，使得客户端在处理这样的报文时会出现崩溃。WIPS 利用 Sensor 监听无线信道来获取无线报文，通过报文解析检测出具有某些畸形类型特征的畸形报文，并发送告警。

目前支持的畸形报文检测包括：

- IE 重复的畸形报文

该检测是针对所有管理帧的检测。当解析某报文时，该报文所包含的某 IE 重复出现时，则判断该报文为重复 IE 畸形报文。因为厂商自定义 IE 是允许重复的，所以检测 IE 重复时，不检测厂商自定义 IE。

- Fata-Jack 畸形报文

该检测是针对 Authentication 帧的检测。Fata-jack 畸形类型规定，当身份认证算法编号即 Authentication algorithm number 的值等于 2 时，则判定该帧为 Fata-jack 畸形报文。

- IBSS 和 ESS 置位异常的畸形报文

该检测是针对 Beacon 帧和探查响应帧进行的检测。当报文中的 IBSS 和 ESS 都置位为 1 时，由于此种情况在协议中没有定义，所以该报文被判定为 IBSS 和 ESS 置位异常的畸形报文。

- 源地址为广播或者组播的认证和关联畸形报文

该检测是针对所有管理帧的检测。当检测到该帧的 TO DS 等于 1 时，表明该帧为客户端发给 AP 的，如果同时又检测到该帧的源 MAC 地址为广播或组播，则该帧被判定为 Invalid-source-address 畸形报文。

- 畸形 Association-request 报文

该检测是针对认证请求帧的检测。当收到认证请求帧中的 SSID 的长度等于 0 时，判定该报文为畸形关联请求报文。

- 畸形 Authentication 报文

该检测是针对认证帧的检测。当检测到以下情况时请求认证过程失败，会被判断为认证畸形报文。

  - 当对认证帧的身份认证算法编号（Authentication algorithm number）的值不符合协议规定，并且其值大于 3 时；

- 当标记客户端和 AP 之间的身份认证的进度的 Authentication Transaction Sequence Number 的值等于 1，且状态代码 status code 不为 0 时；
- 当标记客户端和 AP 之间的身份认证的进度的 Authentication Transaction Sequence Number 的值大于 4 时。

- 含有无效原因值的解除认证畸形报文

该检测是针对解除认证畸形帧的检测。当解除认证畸形帧携带的 Reason code 的值属于集合[0，67～65535]时，则属于协议中的保留值，此时判定该帧为含有无效原因值的解除认证畸形报文。

- 含有无效原因值的解除关联畸形报文

该检测是针对解除关联帧的检测。当解除关联帧携带的 Reason code 的值属于集合[0，67～65535]时，则属于协议中的保留值，此时判定该帧为含有无效原因值的解除关联畸形报文。

- 畸形 HT IE 报文

该检测是针对 Beacon、探查响应帧、关联响应帧、重关联请求帧的检测。当检测到以下情况时，判定为 HT IE 的畸形报文，发出告警，在静默时间内不再告警。

- 解析出 HT Capabilities IE 的 SM Power Save 值为 2 时；
- 解析出 HT Operation IE 的 Secondary Channel Offset 值等于 2 时。

- IE 长度非法的畸形报文

该检测是针对所有管理帧的检测。信息元素（Information Element，简称 IE）是管理帧的组成元件，每种类型的管理帧包含特定的几种 IE。报文解析过程中，当检测到该报文包含的某个 IE 的长度为非法时，该报文被判定为 IE 长度非法的畸形报文。

- 报文长度非法的畸形报文

该检测是针对所有管理帧的检测。当解析完报文主体后，IE 的剩余长度不等于 0 时，则该报文被判定为报文长度非法的畸形报文。

- 无效探查响应报文

该检测是针对探查响应报文。当检测到该帧为非 Mesh 帧，但同时该帧的 SSID Length 等于 0，这种情况不符合协议（协议规定 SSID Length 等于 0 的情况是 Mesh 帧），则判定为无效探查响应报文。

- Key 长度超长的 EAPOL 报文

该检测是针对 EAPOL-Key 帧的检测。当检测到该帧的 TO DS 等于 1 且其 Key Length 大于 0 时，则判定该帧为 Key 长度超长的 EAPOL 报文。Key length 长度异常的恶意的 EAPOL-Key 帧可能会导致 DOS 攻击。

- SSID 长度超长的畸形报文

该检测是针对 Beacon、探查请求、探查响应、关联请求帧的检测。当解析报文的 SSID length 大于 32 字节时，不符合协议规定的 0～32 字节的范围，则判定该帧为 SSID 超长的畸形报文。

- 多余 IE 畸形报文

该检测是针对所有管理帧的检测。报文解析过程中，当检测到既不属于报文应包含的 IE，也不属于 reserved IE 时，判断该 IE 为多余 IE，则该报文被判定为多余 IE 的畸形报文。

- Duration 字段超大的畸形报文

该检测是针对单播管理帧、单播数据帧以及 RTS、CTS、ACK 帧的检测。如果报文解析结果中该报文的 Duration 值大于指定的门限值，则为 Duration 超大的畸形报文。

4. 攻击检测

- Spoofing

Spoofing 攻击是指攻击者仿冒其他设备，从而威胁无线网络的安全。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/解除关联报文就可能导致客户端下线，从而达到破坏无线网络正常工作的目的；又或者攻击者仿冒成合法的 AP 来诱使合法的客户端关联，攻击者仿冒成合法的客户端与 AP 关联等，从而可能导致用户账户信息泄露。

目前支持的 Spoofing 检测包括：AP 地址仿冒和客户端地址仿冒

- Weak IV

WEP 安全协议使用的 RC4 加密算法存在一定程度的缺陷，当其所用的 IV 值不安全时会大大增加其密钥被破解的可能性，该类 IV 值即被称为 Weak IV。WIPS 特性通过检测每个 WEP 报文的 IV 值来预防这种攻击。

- Windows 网桥

当一个连接到有线网络的无线客户端使用有线网卡建立了 Windows 网桥时，该无线客户端就可以通过连接外部 AP 将外部 AP 与内部有线网络进行桥接。此组网方式会使外部 AP 对内部的有线网络造成威胁。WIPS 会对已关联的无线客户端发出的数据帧进行分析，来判断其是否存在于 Windows 网桥中。

- 设备禁用 802.11n 40MHz

支持 802.11n 标准无线设备可以支持 20MHz 和 40MHz 两种带宽模式。在无线环境中，如果与 AP 关联的某个无线客户端禁用了 40MHz 带宽模式，会导致 AP 与该 AP 关联的其它无线客户端也降低无线通信带宽到 20MHz，从而影响到整个网络的通信能力。WIPS 通过检测无线客户端发送的探测请求帧来发现禁用 40MHz 带宽模式的无线客户端。

- Omerta

Omerta 是一个基于 802.11 协议的 DoS 攻击工具，它通过向信道上所有发送数据帧的客户端回应解除关联帧，使客户端中断与 AP 的关联。Omerta 发送的解除关联帧中的原因代码字段为 0x01，表示未指定。由于正常情况下不会出现此类解除关联帧，因此 WIPS 可以通过检测每个解除关联帧的原因代码字段来检测这种攻击。

- 未加密授权 AP/未加密信任客户端

在无线网络中，如果有授权 AP 或信任的无线客户端使用的配置是未加密的，网络攻击者很容易通过监听来获取无线网络中的数据，从而导致网络信息泄露。WIPS 会对信任的无线客户端或授权 AP 发出的管理帧或数据帧进行分析，来判断其是否使用了加密配置。

- 热点攻击

热点攻击指恶意 AP 使用热点 SSID 来吸引周围的无线客户端来关联自己。攻击者通过伪装成公共热点来引诱这些无线客户端关联自己。一旦无线客户端与恶意 AP 关联上，攻击者就会发起一系列的安全攻击，获取用户的信息。用户通过在 WIPS 中配置热点文件，来指定 WIPS 对使用这些热点的 AP 和信任的无线客户端进行热点攻击检测。

- 绿野模式

当无线设备使用 802.11n 绿野模式时，不可以和其他 802.11a/b/g 设备共享同一个信道。通常当一台设备侦听到有其他设备占用信道发送和接收报文的时候，会延迟报文的发送直到信道空闲时再发

送。但是 802.11a/b/g 设备不能和绿野模式的 AP 进行通信，无法被告知绿野模式的 AP 当前信道是否空闲，会立刻发送自己的报文。这可能会导致报文发送冲突、差错和重传。

- 关联/重关联 DoS 攻击

关联/重关联 DoS 攻击通过模拟大量的客户端向 AP 发送关联请求/重关联请求帧，使 AP 的关联列表中存在大量虚假的客户端，达到拒绝合法客户端接入的目的。

- 中间人

在中间人攻击中，攻击者在合法 AP 和合法客户端的数据通路中间架设自己的设备，并引诱合法客户端下线并关联到攻击者的设备上，此时攻击者就可以劫持合法客户端和合法 AP 之间的会话。在这种情况下，攻击者可以删除，添加或者修改数据包内的信息，获取验证密钥、用户密码等机密信息。中间人攻击是一种组合攻击，客户端在关联到蜜罐 AP 后攻击者才会发起中间人攻击，所以在配置中间人攻击检测之前需要开启蜜罐 AP 检测。

- 无线网桥

攻击者可以通过接入无线网桥侵入公司网络的内部，对网络安全造成隐患。WIPS 通过检测无线网络环境中是否存在无线网桥数据以确定周围环境中是否存在无线网桥。当检测到无线网桥时，WIPS 系统即产生告警，提示当前无线网络环境存在安全隐患。如果该无线网桥是 Mesh 网络时，则记录该 Mesh 链路。

- AP 信道变化

AP 设备在完成部署后通常是固定不动的，正常情况下 WIPS 通过检测发现网络环境的中 AP 设备的信道是否发生变化。

- 广播解除关联帧/解除认证帧

当攻击者仿冒成合法的 AP，发送目的 MAC 地址为广播地址的解除关联帧或者解除认证帧时，会使合法 AP 下关联的客户端下线，对无线网络造成攻击。

- AP 扮演者攻击

在 AP 扮演者攻击中，攻击者会安装一台恶意 AP 设备，该 AP 设备的 BSSID 和 ESSID 与真实 AP 一样。当该恶意 AP 设备在无线环境中成功扮演了真实 AP 的身份后，就可以发起热点攻击，或欺骗检测系统。WIPS 通过检测收到 Beacon 帧的间隔小于 Beacon 帧中携带的间隔值次数达到阈值来判断其是否为攻击者扮演的恶意 AP。

- AP 泛洪

AP 设备在完成部署后通常是固定不动的，正常情况下 WIPS 通过检测发现网络环境的中 AP 设备的数目达到稳定后不会大量增加。当检测到 AP 的数目超出预期的数量时， WIPS 系统即产生告警，提示当前无线网络环境存在安全隐患。

- 蜜罐 AP

攻击者在合法 AP 附近搭建一个蜜罐 AP，通过该 AP 发送与合法 AP SSID 相似的 Beacon 帧或 Probe Response 帧，蜜罐 AP 的发送信号可能被调得很大以诱使某些授权客户端与之关联。当有客户端连接到蜜罐 AP，蜜罐 AP 便可以向客户端发起某些安全攻击，如端口扫描或推送虚假的认证页面来骗取客户端的用户名及密码信息等。因此，需要检测无线环境中对合法设备构成威胁的蜜罐 AP。WIPS 系统通过对外部 AP 使用的 SSID 进行分析，若与合法 SSID 的相似度值达到一定阈值就发送蜜罐 AP 告警。

- 节电攻击

对于处于非节电模式下的无线客户端，攻击者可以通过发送节电模式开启报文（Null 帧），诱使 AP 相信与其关联的无线客户端始终处于睡眠状态，并为该无线客户端暂存帧。被攻击的无线客户端因为处于非节电模式而无法获取这些暂存帧，在一定的时间之后暂存帧会被自动丢弃。WIPS 通过检测节电模式开启/关闭报文的比例判断是否存在节电攻击。

- 软 AP

软 AP 是指客户端上的无线网卡在应用软件的控制下对外提供 AP 的功能。攻击者可以利用这些软 AP 所在的客户端接入公司网络，并发起网络攻击。WIPS 通过检测某个 MAC 地址在无线客户端和 AP 这两个角色上的持续活跃时长来判断其是否是软 AP，不对游离的客户端进行软 AP 检测。

- 非法信道

用户可以设置合法信道集合，并开启非法信道检测，如果 WIPS 在合法信道集合之外的其它信道上监听到无线通信，则认为在监听到无线通信的信道上存在入侵行为。

1.6.5 Signature检测

Signature 检测是指用户可以根据实际的网络状况来配置 Signature 规则，并通过该规则来实现自定义攻击行为的检测。WIPS 利用 Sensor 监听无线信道来获取无线报文，通过报文解析，检测出具有某些自定义类型特征的报文，并将分析检测的结果进行归类处理。

每个 Signature 检测规则中最多支持配置 6 条子规则，分别对报文的 6 种特征进行定义和匹配。当 AC 解析报文时，如果发现报文的特征能够与已配置的子规则全部匹配，则认为该报文匹配该自定义检测规则，AC 将发送告警信息或记录日志。

可以通过子规则定义的 6 种报文特征包括：

- 帧类型
- MAC 地址
- 序列号
- SSID
- SSID 长度
- 自定义报文位置

1.6.6 反制

在无线网络中设备分为两种类型：非法设备和合法设备。非法设备可能存在安全漏洞或被攻击者操纵，因此会对用户网络的安全造成严重威胁或危害。反制功能可以对这些设备进行攻击使其他无线终端无法关联到非法设备。

1.6.7 配置忽略告警信息的MAC地址列表

对于可以忽略 WIPS 告警信息的设备列表中的无线设备，WIPS 仍然会对其做正常的监测，但是不会产生与该设备相关的任何 WIPS 告警信息。

1.7 黑白名单

1.7.1 黑白名单简介

无线网络很容易受到各种网络威胁的影响，非法设备对于无线网络来说是一个很严重的威胁，因此需要对客户端的接入进行控制。通过黑名单和白名单功能来过滤客户端，对客户端进行控制，防止非法客户端接入无线网络，可以有效的保护企业网络不被非法设备访问，从而保证无线网络的安全。

1. 白名单

白名单定义了允许接入无线网络的客户端 MAC 地址表项，不在白名单中的客户端不允许接入。白名单表项只能手工添加和删除。

2. 黑名单

黑名单定义了禁止接入无线网络的客户端 MAC 地址表项，在黑名单中的客户端不允许接入。黑名单分为静态黑名单和动态黑名单，以下分别介绍。

(1) 静态黑名单

用户手工添加、删除的黑名单称为静态黑名单，当无线网络明确拒绝某些客户端接入时，可以将这些客户端加入静态黑名单。

(2) 动态黑名单

设备通过检测而自动生成和删除的黑名单称为动态黑名单，当 AP 检测到来自某一客户端的攻击报文时，会将该客户端的 MAC 地址动态加入到动态黑名单中，在动态黑名单表项老化时间内拒绝该客户端接入无线网络。

1.7.2 黑白名单过滤机制

当收到客户端关联请求报文或 AP 发送的 Add mobile 报文时，AC 将使用白名单和黑名单对客户端的 MAC 地址进行过滤。静态黑名单和白名单对所有与 AC 相连的 AP 生效，而动态黑名单只会对接收到攻击报文的 AP 生效。具体的过滤机制如下：

- 当 AC 上存在白名单时，将判断客户端的 MAC 地址是否在白名单中，如果在白名单中，则允许客户端通过任意 AP 接入无线网络，否则将拒绝该客户端接入。
- 当 AC 上不存在白名单时，则首先判断客户端的 MAC 地址是否在静态黑名单中，如果客户端在静态黑名单中，则拒绝该客户端通过任何 AP 接入无线网络。如果该客户端不在静态黑名单中，则继续判断其是否在动态黑名单中。如果在动态黑名单中，则不允许该客户端通过动态黑名单中指定的 AP 接入无线网络，但可以通过其它 AP 接入；如果不在动态黑名单中，则允许客户端通过任意 AP 接入。

1.8 射频管理

射频是一种高频交流变化电磁波，表示具有远距离传输能力、可以辐射到空间的电磁频率。WLAN 是利用射频作为传输媒介，进行数据传输无线通信技术之一。

射频的频率介于 300KHz 和约 300GHz 之间，WLAN 使用的射频频率范围为 2.4GHz 频段（2.4GHz～2.4835GHz）和 5GHz 频段（5.150GHz～5.350GHz 和 5.725GHz～5.850GHz）。

1.8.1 射频模式

按 IEEE 定义的 802.11 无线网络通信标准划分，射频模式主要有 802.11a、802.11b、802.11g、802.11n 和 802.11ac：

- 802.11a：工作频率为 5GHz，由于选择了 OFDM（Orthogonal Frequency Division Multiplexing，正交频分复用）技术，能有效降低多路径衰减的影响和提高频谱的利用率，使 802.11a 的物理层速率可达 54Mbps。但是在传输距离上存在劣势。
- 802.11b：工作频率为 2.4GHz，相比 5GHz 能够提供更大的传输距离，数据传输速率最高达 11Mbps。由于早期的无线通信更加追求传输距离，所以 802.11b 比 802.11a 更早被投入使用。
- 802.11g：工作频率为 2.4GHz，可以兼容 802.11b。802.11g 借用了 802.11a 的成果，在 2.4GHz 频段采用了 OFDM 技术，最高速率可以达到 54Mbps。
- 802.11n：工作于双频模式（2.4GHz 和 5GHz 两个工作频段），能够与 802.11a/g 标准兼容。802.11n 的数据传输速率达 100Mbps 以上，理论最高可达 600Mbps，使无线局域网平滑地和有线网络结合，全面提升了网络吞吐量。
- 802.11ac：是 802.11n 的继承者，理论最高速率可达 6900Mbps，全面提升了网络吞吐量。

表1-1 WLAN 的几种主要射频模式比较

协议	频段	最大速度	范围（室内）	范围（室外）
802.11a	5GHz	54Mbps	约50米	约100米
802.11b	2.4GHz	11Mbps	约300米	约600米
802.11g	2.4GHz	54Mbps	约300米	约600米
802.11n	2.4GHz/5GHz	600Mbps	约300米	约600米
802.11ac	5GHz	6900Mbps	约30米	约60米

不同的射频模式所支持的信道、功率有所不同，所以射频模式修改时，如果新的射频模式不支持原来配置的的信道、功率，则 AP 会根据新射频模式自动调整这些参数。

注意

修改射频模式时，会导致当前在线客户端下线。

在指定了射频模式以后，可以进行射频功能配置，具体情况如下：

- 如果指定的射频模式为 **802.11a**、**802.11b**或 **802.11g**，则可以配置射频基础功能，有关射频基础功能配置的详细介绍，请参见“射频基础功能”
- 如果指定的射频模式为 **802.11n**，则可以配置射频基础功能和 802.11n功能，有关 802.11n功能配置的详细介绍，请参见“802.11n功能”。
- 如果指定的射频模式为 **802.11ac**，则可以配置射频基础功能、802.11n功能和 802.11ac功能，有关 802.11ac功能配置的详细介绍，请参见“802.11ac功能”。

1.8.2 信道

信道是具有一定频宽的射频。在 WLAN 标准协议里，2.4GHz 频段被划分为 13 个相互交叠的信道，每个信道的频宽是 20MHz，信道间隔为 5MHz。这 13 个信道里有 3 个独立信道，即没有相互交叠的信道，目前普遍使用的三个互不交叠的独立信道号为 1、6、11。

5GHz 频段拥有更高的频率和频宽，可以提供更高的速率和更小的信道干扰。WLAN 标准协议将 5GHz 频段分为 24 个频宽为 20MHz 的信道，且每个信道都为独立信道。各个国家开放的信道不一样，目前中国 5GHz 频段开放使用的信道号是 36、40、44、48、52、56、60、64、149、153、157、161 和 165。

1.8.3 功率

射频功率是指天线在无线介质中所辐射的功率，反映的是 WLAN 设备辐射信号的强度。射频功率越大，射频覆盖的范围越广，客户端在同一位置收到的信号强度越强，也就越容易干扰邻近的网络。随着传输距离的增大，信号强度随之衰减。

1.8.4 速率

射频速率是客户端与 WLAN 设备之间的数据传输速度。不同的射频模式，根据所使用扩频、编码和调制技术，对应不同的传输速率。802.11a、802.11b、802.11g、802.11n 和 802.11ac 的速率支持情况如下：

- 802.11a：6Mbps、9Mbps、12Mbps、18Mbps、24Mbps、36Mbps、48Mbps、54Mbps。
- 802.11b：1Mbps、2Mbps、5.5Mbps、11Mbps。
- 802.11g：1Mbps、2Mbps、5.5Mbps、6Mbps、9Mbps、11Mbps、12Mbps、18Mbps、24Mbps、36Mbps、48Mbps、54Mbps。
- 802.11n：根据不同信道带宽可支持不同的速率组合，具体请参见“MCS”
- 802.11ac：根据不同信道带宽和空间流数量可支持不同的速率组合，具体请参见“VHT-MCS”。

1.8.5 MCS

IEEE 802.11n 除了向前兼容 IEEE 802.11a/b/g 的速率外，还定义了新的速率调制与编码策略，即 MCS（Modulation and Coding Scheme，调制与编码策略）。

无线数据传输的物理速率受到编码方式、调制方式、载波比特率、空间流数量、数据子信道数等多种因素的影响，不同的因素组合将产生不同的物理速率。MCS 使用索引的方式将每种组合以及由该组合产生的物理速率进行排列，形成索引值与速率的对应表，称为 MCS 表。802.11n 的 MCS 表共有两个子表，分别用于保存信道带宽为 20MHz 和 40MHz 时的物理速率。索引值的取值范围为 0～76，能够描述 77 种物理速率，两个 MCS 子表中的索引值相互独立。

802.11n规定，当带宽为 20MHz时，MCS0～15 为AP必须支持的MCS索引，MCS0～7 是客户端必须支持的MCS索引，其余MCS索引均为可选速率。表 1-2 和 表 1-3 分别列举了带宽为 20MHz和带宽为 40MHz的MCS速率表。

说明

完整的 MCS 对应速率表可参见 IEEE 802.11n-2009 标准协议。

表1-2 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
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

表1-3 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

MCS 索引	空间流数量	调制方式	速率(Mb/s)	
			800ns GI	400ns GI
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

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，且当 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，且当 MCS＝15 时，速率值最大。

MCS 分为三类：

- 基本 MCS 集：客户端必须支持的基本 MCS 集，才能够与 AP 以 802.11n 模式进行连接。
- 支持 MCS 集：AP 所能够支持的更高的 MCS 集合，用户可以配置支持 MCS 集让客户端在支持基本 MCS 的前提下选择更高的速率与 AP 进行数据传输。
- 组播 MCS 集：AP 以组播方式对其 BSS 内的客户端发送消息所使用的速率。

1.8.6 VHT-MCS

802.11ac中定义的VHT-MCS表在表项内容上与 802.11n的MCS表完全相同，只是在子表划分方式上存在区别，VHT-MCS根据信道带宽和空间流数量的组合来划分子表。802.11ac支持 20MHz、40MHz、80MHz和 160MHz（80+80MHz）四种带宽，最多支持 8 条空间流，因此VHT-MCS表共划分为 32 个子表。每个子表中的MCS索引独立编号，目前编号范围为 0～9。AP支持的VHT-MCS表仅有 12 套，具体如 表 1-4～表 1-15 所示。

说明

完整的 VHT-MCS 对应速率表可参见 IEEE 802.11ac-2013 标准协议。

表1-4 VHT-MCS 对应速率表（20MHz，1NSS）

VHT-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

VHT-MCS 索引	空间流数量	调制方式	速率(Mb/s)	
			800ns GI	400ns GI
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	1	256-QAM	78.0	86.7
9	Not valid			

表1-5 VHT-MCS 对应速率表（20MHz，2NSS）

VHT-MCS 索引	空间流数量	调制方式	速率(Mb/s)	
			800ns GI	400ns GI
0	2	BPSK	13.0	14.4
1	2	QPSK	26.0	28.9
2	2	QPSK	39.0	43.3
3	2	16-QAM	52.0	57.8
4	2	16-QAM	78.0	86.7
5	2	64-QAM	104.0	115.6
6	2	64-QAM	117.0	130.0
7	2	64-QAM	130.0	144.4
8	2	256-QAM	156.0	173.3
9	Not valid			

表1-6 VHT-MCS 对应速率表（20MHz，3NSS）

VHT-MCS 索引	空间流数量	调制方式	速率(Mb/s)	
			800ns GI	400ns GI
0	3	BPSK	19.5	21.7
1	3	QPSK	39.0	43.3
2	3	QPSK	58.5	65.0
3	3	16-QAM	78.0	86.7
4	3	16-QAM	117.0	130.0
5	3	64-QAM	156.0	173.3
6	3	64-QAM	175.5	195.0
7	3	64-QAM	195.0	216.7
8	3	256-QAM	234.0	260.0

VHT-MCS 索引	空间流数量	调制方式	速率(Mb/s)	
			800ns GI	400ns GI
9	3	256-QAM	260.0	288.9

表1-7 VHT-MCS 对应速率表（20MHz，4NSS）

VHT-MCS 索引	空间流数量	调制方式	速率(Mb/s)	
			800ns GI	400ns GI
0	4	BPSK	26.0	28.9
1	4	QPSK	52.0	57.8
2	4	QPSK	78.0	86.7
3	4	16-QAM	104.0	115.6
4	4	16-QAM	156.0	173.3
5	4	64-QAM	208.0	231.1
6	4	64-QAM	234.0	260.0
7	4	64-QAM	260.0	288.9
8	4	256-QAM	312.0	346.7
9	Not valid			

表1-8 VHT-MCS 对应速率表（40MHz，1NSS）

VHT-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	1	256-QAM	162.0	180.0
9	1	256-QAM	180.0	200.0

表1-9 VHT-MCS 对应速率表（40MHz，2NSS）

VHT-MCS 索引	空间流数量	调制方式	速率(Mb/s)	
			800ns GI	400ns GI
0	2	BPSK	27.0	30.0
1	2	QPSK	54.0	60.0
2	2	QPSK	81.0	90.0
3	2	16-QAM	108.0	120.0
4	2	16-QAM	162.0	180.0
5	2	64-QAM	216.0	240.0
6	2	64-QAM	243.0	270.0
7	2	64-QAM	270.0	300.0
8	2	256-QAM	324.0	360.0
9	2	256-QAM	360.0	400.0

表1-10 VHT-MCS 对应速率表（40MHz，3NSS）

VHT-MCS 索引	空间流数量	调制方式	速率(Mb/s)	
			800ns GI	400ns GI
0	3	BPSK	40.5	45.0
1	3	QPSK	81.0	90.0
2	3	QPSK	121.5	135.0
3	3	16-QAM	162.0	180.0
4	3	16-QAM	243.0	270.0
5	3	64-QAM	324.0	360.0
6	3	64-QAM	364.5	405.0
7	3	64-QAM	405.0	450.0
8	3	256-QAM	486.0	540.0
9	3	256-QAM	540.0	600.0

表1-11 VHT-MCS 对应速率表（40MHz，4NSS）

VHT-MCS 索引	空间流数量	调制方式	速率(Mb/s)	
			800ns GI	400ns GI
0	4	BPSK	54.0	60.0
1	4	QPSK	108.0	120.0
2	4	QPSK	162.0	180.0
3	4	16-QAM	216.0	240.0

VHT-MCS 索引	空间流数量	调制方式	速率(Mb/s)	
			800ns GI	400ns GI
4	4	16-QAM	324.0	360.0
5	4	64-QAM	432.0	480.0
6	4	64-QAM	486.0	540.0
7	4	64-QAM	540.0	600.0
8	4	256-QAM	648.0	720.0
9	4	256-QAM	720.0	800.0

表1-12 VHT-MCS 对应速率表（80MHz，1NSS）

VHT-MCS 索引	空间流数量	调制方式	速率(Mb/s)	
			800ns GI	400ns GI
0	1	BPSK	29.3	32.5
1	1	QPSK	58.5	65.0
2	1	QPSK	87.8	97.5
3	1	16-QAM	117.0	130.0
4	1	16-QAM	175.5	195.0
5	1	64-QAM	234.0	260.0
6	1	64-QAM	263.0	292.5
7	1	64-QAM	292.5	325.0
8	1	256-QAM	351.0	390.0
9	1	256-QAM	390.0	433.3

表1-13 VHT-MCS 对应速率表（80MHz，2NSS）

VHT-MCS 索引	空间流数量	调制方式	速率(Mb/s)	
			800ns GI	400ns GI
0	2	BPSK	58.5	65.0
1	2	QPSK	117.0	130.0
2	2	QPSK	175.5	195.0
3	2	16-QAM	234.0	260.0
4	2	16-QAM	351.0	390.0
5	2	64-QAM	468.0	520.0
6	2	64-QAM	526.5	585.0
7	2	64-QAM	585.0	650.0
8	2	256-QAM	702.0	780.0

VHT-MCS 索引	空间流数量	调制方式	速率(Mb/s)	
			800ns GI	400ns GI
9	2	256-QAM	780.0	866.7

表1-14 VHT-MCS 对应速率表（80MHz，3NSS）

VHT-MCS 索引	空间流数量	调制方式	速率(Mb/s)	
			800ns GI	400ns GI
0	3	BPSK	87.8	97.5
1	3	QPSK	175.5	195.0
2	3	QPSK	263.3	292.5
3	3	16-QAM	351.0	390.0
4	3	16-QAM	526.5	585.0
5	3	64-QAM	702.0	780.0
6	Not valid			
7	3	64-QAM	877.5	975.0
8	3	256-QAM	1053.0	1170.0
9	3	256-QAM	1170.0	1300.0

表1-15 VHT-MCS 对应速率表（80MHz，4NSS）

VHT-MCS 索引	空间流数量	调制方式	速率(Mb/s)	
			800ns GI	400ns GI
0	4	BPSK	117.0	130.0
1	4	QPSK	234.0	260.0
2	4	QPSK	351.0	390.0
3	4	16-QAM	468.0	520.0
4	4	16-QAM	702.0	780.0
5	4	64-QAM	936.0	1040.0
6	4	64-QAM	1053.0	1170.0
7	4	64-QAM	1170.0	1300.0
8	4	256-QAM	1404.0	1560.0
9	4	256-QAM	1560.0	1733.3

和 MCS 一样，VHT-MCS 也分为三类：基本 VHT-MCS 集、支持 VHT-MCS 集和组播 VHT-MCS 集，每类的意义也和 MCS 相同。

1.8.7 射频基础功能

1. 射频工作信道

配置射频工作信道的目的是尽量减少和避免射频的干扰。干扰主要来自两方面：一种是 WLAN 设备间的干扰，比如相邻 WLAN 设备使用相同信道，会造成相互干扰；另一种是 WLAN 设备和其他无线射频之间的干扰，比如 WLAN 设备使用的信道上有雷达信号则必须立即让出该信道。

射频工作的信道可以手工配置或者由系统自动选择。

- 如果用户配置了手工信道，所配置的信道将一直被使用而不能自动更改，除非发现雷达信号。如果因为发现雷达信号而进行信道切换，AP 会在 30 分钟后将信道切换回手工指定的信道，并静默一段时间，如果在静默时间内没有发现雷达信号，则开始使用该信道；如果发现雷达信号，则再次切换信道。
- AP 默认采用自动信道模式，随机选择工作信道。

2. 射频最大传输功率

射频的最大传输功率只能在射频支持的功率范围内进行选取，即保证射频的最大传输功率在合法范围内。射频支持的功率范围由国家码、信道、AP 型号、射频模式、天线类型、带宽等属性决定，修改上述属性，射频支持的功率范围和最大传输功率将自动调整为合法值。

3. 功率锁定

如果先开启功率调整，再配置功率锁定，AC 会自动将当前传输功率设置并锁定为自动功率调整后的功率值，在 AC 重启后，AP 能继续使用锁定的功率调整值。

如果先配置功率锁定命令，后开启功率调整功能，由于功率已经被锁定，功率调整功能不会运行，所以在开启功率调整功能前，请确保功率没有被锁定。

功率锁定后，如果信道发生调整，并且锁定的功率值大于调整后使用信道支持的最大功率，设备会将功率值调整为信道支持的最大功率。

有关自动功率调整相关配置的详细介绍请参见“网络 > 无线配置 > 射频资源 > 射频优化”页面。

4. 射频速率

射频速率可以分为以下四种：

- 禁用速率：AP 禁用的速率。
- 强制速率：客户端关联 AP 时，AP 要求客户端必须支持的速率。
- 支持速率：AP 所支持的速率。客户端关联 AP 后，可以在 AP 支持的“支持速率集”中选用更高的速率发送报文。当受干扰、重传、丢包等影响较大时，AP 会自动降低对客户端的发送速率；当受影响较小时，AP 会自动升高对客户端的发送速率。
- 组播速率：AP 向客户端发送组播和广播报文的速率。组播速率必须在强制速率中选取，且只能配置一个速率值或由 AP 自动选择合适的速率。

5. 前导码类型

说明

只有 2.4GHz 射频，才支持配置前导码类型。

前导码是数据报文头部的一组 Bit 位，用于同步发送端与接收端的传输信号。前导码的类型有两种，长前导码和短前导码。短前导码能使网络性能更好，默认使用短前导码。如果需要兼容网络中一些较老的客户端时可以使用长前导码保持兼容。

6. 射频覆盖范围

天线发出的电磁波在介质中传播的时候，随着距离的增加以及周围环境因素的影响，信号强度逐渐降低。电磁波的覆盖范围主要与环境的开放程度、障碍物的材质类型有关。设备在不加外接天线的情况下，传输距离约 300 米，若空间中有隔离物，传输大约在 35～50 米左右。

如果借助于外接天线，覆盖范围则可以达到 30～50 公里甚至更远，这要视天线本身的增益而定。

7. 发送Beacon帧的时间间隔

在 WLAN 环境中，AP 通过不断广播 Beacon 帧来让客户端发现自己。AP 发送 Becaon 帧时间间隔越小，AP 越容易被客户端发现，但 AP 的功耗越大。

8. 禁止 802.11b客户端接入

当射频模式为 802.11g 或 802.11gn 时，为了提高传输速率，可以通过开启禁止 802.11b 客户端接入功能来隔离低速率的 802.11b 客户端的影响；当开启禁止 802.11b 客户端接入功能后，不允许客户端以 802.11b 模式接入。

9. RTS门限

在无线环境中，为了避免冲突的产生，无线设备在发送数据前会执行冲突避免，即使用 RTS/CTS（Request to Send/Clear to Send，请求发送/允许发送）帧或 CTS-to-self（反身 CTS）帧来清空传送区域，取得信道使用权。但是如果每次发送数据前都执行冲突避免，则会降低过多的传输量，浪费了无线资源。因此，802.11 协议规定仅当发送帧长超过 RTS 门限的帧时，需要执行冲突避免；帧长小于 RTS 门限的帧，则可以直接发送。

当网络中设备较少时，产生干扰的概率较低，可以适当增大 RTS 门限以减少冲突避免的执行次数，提高吞吐量。当网络中设备较多时，可以通过降低 RTS 门限，增加冲突避免的执行次数来减少干扰。

10. 802.11g保护功能

说明

只有当射频**模式**为 802.11g 或 802.11n（2.4GHz）时，才支持配置 802.11g 保护功能。

当网络中同时存在 802.11b 和 802.11g 的客户端，由于调制方式不同，802.11b 客户端无法解析 802.11g 信号，会导致 802.11b 与 802.11g 网络之间彼此造成干扰。802.11g 保护功能用于避免干扰情况的发生，通过使 802.11g 和 802.11n 设备发送 RTS/CTS 报文或 CTS-to-self 报文来取得信道使用权，确保 802.11b 客户端能够检测到 802.11g 和 802.11n 客户端正在进行数据传输，实现冲突避免。

开启 802.11g 保护功能后，当 AP 在其工作信道上扫描到 802.11b 信号，则会在传输数据前通过发送 RTS/CTS 报文或 CTS-to-self 报文进行冲突避免，并通知客户端开始执行 802.11g 保护功能；如果未检测到 802.11b 信号，则不会采取上述动作。

当 802.11b 客户端在开启了 802.11g 或 802.11n（2.4GHz）的 AP 上接入时，AP 上的 802.11g 保护功能将自动开启并生效。

11. 帧的分片门限

帧的分片是将一个较大的帧分成更小的分片，每个分片独立进行传输和确认。当帧的实际大小超过指定的分片门限值时，该帧将被分片传输。

在干扰较大的无线环境，建议适当降低帧的分片门限值，增加帧的分片数量，则当传输受到干扰时，仅需要重传未成功发送的分片，从而提高吞吐量。

12. 帧的最大重传次数

在无线网络中传输的单播数据，必须得到接收端的应答，否则便认为传送失败。设备会对传送失败的帧进行重传，如果在达到最大重传次数时，仍然没有传送成功，则丢弃该帧，并将此状况告知上层协议。

每个帧或帧片段都分别对应一个重传计数器。无线设备上具有两个重传计数器：短帧重传计数器与长帧重传计数器。长度小于 RTS 门限值的帧视为短帧；长度超过 RTS 门限值的帧则为长帧。当帧传送失败，对应的重传计数器累加，然后重新传送帧，直至达到最大重传次数。

区分短帧和长帧的主要目的是为了让网络管理人员利用不同长度的帧来调整重传策略。由于发送长帧前需要执行冲突避免，因此长帧比短帧占用了更多的缓存空间和传输时间。在配置帧的最大重传次数时，适当减少长帧的最大重传次数，可以减少所需要的缓存空间和传输时间。

1.8.8 802.11n功能

说明

如果多个用户登录到 AC 设备上对某台 AP 配置 802.11n 功能，同一时间只有一个用户可以配置成功。

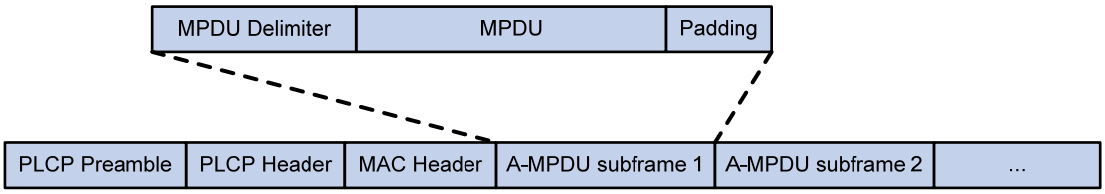
IEEE 802.11n 协议的制定，旨在提供高带宽、高质量的 WLAN 服务，使无线局域网达到以太网的性能水平。802.11n 通过物理层和 MAC（Media Access Control，媒体访问控制）层的优化来提高 WLAN 的吞吐能力，从而提高传输速率。

802.11n 的物理层建立在 OFDM 系统之上，采用 MIMO（Multiple Input,Multiple Output，多输入多输出）、40MHz 传输带宽、Short GI（Short Guard Interval，短保护间隔）、STBC（Space-Time Block Coding，空时块编码）、LDPC（Low-Density Parity Check，低密度奇偶校验）等技术使物理层达到高吞吐（High Throughput）的效果，并采用 A-MPDU（Aggregate MAC Protocol Data Unit，聚合 MAC 协议数据单元）、A-MSDU（Aggregate MAC Service Data Unit，聚合 MAC 服务数据单元）、BA（Block Acknowledgment，块确认）等技术，提高 MAC 层的传输效率。

1. A-MPDU功能

802.11n 标准中采用 A-MPDU 聚合帧格式，减少了每个传输帧中的附加信息，同时也减少了所需要的 ACK 帧的数目，从而降低了协议的负荷，有效的提高了网络吞吐量。A-MPDU 是将多个 MPDU（MAC Protocol Data Unit，MAC 协议数据单元）聚合为一个 A-MPDU，这里的 MPDU 为经过 802.11 封装的数据报文。A-MPDU 抢占一次信道并使用一个 PLCP（Physical Layer Convergence Procedure，物理层汇聚协议）头来提升信道利用率。一个 A-MPDU 中的所有 MPDU 必须拥有相同的 QoS 优先级，由同一设备发送，并被唯一的一个设备接收。

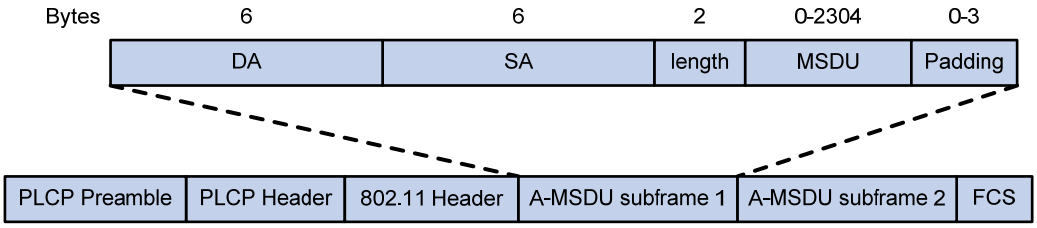
图1-5 A-MPDU 报文格式图



2. A-MSDU功能

A-MSDU 技术是指把多个 MSDU（MAC Service Data Unit，MAC 服务数据单元）聚合成一个较大的载荷。目前，MSDU 仅指 Ethernet 报文。通常，当 AP 或客户端从协议栈收到 MSDU 报文时，会封装 Ethernet 报文头，封装之后称之为 A-MSDU Subframe；而在通过射频发送出去前，需要一一将其转换成 802.11 报文格式。而 A-MSDU 技术旨在将若干个 A-MSDU Subframe 聚合到一起，并封装为一个 802.11 报文进行发送。从而减少了发送每一个 802.11 报文所需的 PLCP Preamble、PLCP Header 和 802.11MAC Header 的开销，提高了报文发送的效率。

图1-6 A-MSDU 报文格式图



A-MSDU 是将多个 MSDU 组合在一起发送，这些 MSDU 必须拥有相同的 QoS 优先级，而且必须由同一设备发送，并被唯一的一个设备接收。当一个设备接收到一个 A-MSDU 时，需要将这个 A-MSDU 分解成多个 MSDU 后分别处理。

3. Short-GI功能

Short GI 是 802.11n 针对 802.11a/g 所做的改进。射频在使用 OFDM 调制方式发送数据时，整个帧是被划分成不同的数据块进行发送的，为了数据传输的可靠性，数据块之间会有 GI（Guard Interval，保护间隔），用以保证接收侧能够正确的解析出各个数据块。无线信号的空间传输会因多径等因素在接收侧形成时延，如果后面的数据块发送的过快，会和前一个数据块形成干扰，GI 就是用来规避这个干扰的。802.11a/g 的 GI 时长为 800ns，在多径效应不严重时，可以使用 Short GI，Short GI 时长为 400ns，在使用 Short GI 的情况下，可提高 10%的传输速率。另外，Short GI 与带宽无关，支持 20MHz、40MHz 带宽。

4. LDPC功能

802.11n 引入了 LDPC（Low-Density Parity Check，低密度奇偶校验）机制，该机制通过校验矩阵定义了一类线性码，并在码长较长时需要校验矩阵满足“稀疏性”，即校验矩阵中 1 的个数远小于 0。在 802.11n 出现以前，所有以 OFDM 为调制方式的设备都使用卷积作为前向纠错码。802.11n 引入了 LDPC 校验码，将传输的信噪比增加到了 1.5 到 3dB 之间，使传输质量得到提升。对 LDPC 的支持需要设备间的协商，以保证设备双方都支持 LDPC 校验。

5. STBC功能

802.11n 引入了 STBC（Space-Time Block Coding，空时块编码）机制，该机制可以将空间流编码成时空流，是 802.11n 中使用的一个简单的可选的发送分集机制。该机制的优点是不要求客户端具有高的数据传输速率，就可以得到强健的链路性能。STBC 是完全开环的，不要求任何反馈或额外的系统复杂度，但是会降低效率。

6. MCS索引

当非 802.11n 客户端上线时，将使用基础速率传输单播数据。当 802.11n 客户端上线时，将使用 MCS 索引所代表的调制与编码策略传输单播数据。

当未配置组播 MCS 索引时，802.11n 客户端和 AP 之间将使用组播速率发送组播数据；当配置了组播 MCS 索引且客户端都是 802.11n 客户端时，AP 和客户端将使用组播 MCS 索引所代表的调制与编码策略传输组播数据。当配置了组播索引且存在非 802.11n 客户端时，AP 和客户端将使用基础模式的组播速率传输组播数据，即 802.11a/b/g 的组播速率。

需要注意的是：

- 组播 MCS 索引需要小于或等于最大基本 MCS 索引，最大基本 MCS 需要小于或等于最大支持 MCS 索引。
- 配置的 802.11n 基本 MCS 最大索引值 index 表示射频的 802.11n 基本 MCS 的最大索引值，即该射频的 802.11n 基本 MCS 集是 0～index。
- 配置的 802.11n 支持 MCS 最大索引值 index 表示射频的 802.11n 支持 MCS 的最大索引值，即该射频的 802.11n 支持 MCS 集是 0～index。
- 配置的 802.11n 组播 MCS 索引值 index 表示射频发送 802.11n 组播报文使用的 MCS 索引。

7. 仅允许 802.11n及 802.11ac客户端接入功能

开启仅允许 802.11n 及 802.11ac 客户端接入功能后，仅允许 802.11n 及 802.11ac 客户端接入，不允许 802.11a/b/g 客户端接入，可以隔离低速率的客户端的影响，提高 802.11n 设备的传输速率。

8. 802.11n信道带宽

802.11n 沿用了 802.11a/b/g 的信道结构。20MHz 信道划分为 64 个子信道，为了防止相邻信道干扰，在 802.11a/g 中，需预留 12 个子信道，同时，需用 4 个子信道充当导频（pilot carrier）以监控路径偏移，因此 20MHz 带宽的信道在 802.11a/g 中用于传输数据的子信道数为 48 个；而在 802.11n 中，只需预留 8 个子信道，加上充当导频的 4 个子信道，20MHz 带宽的信道在 802.11n 中用于传输数据的子信道数为 52 个，提高了传输速率。

802.11n 将两个相邻的 20MHz 带宽绑定在一起，组成一个 40MHz 通讯带宽（其中一个为主信道，另一个为辅信道）来提高传输速率。

射频的带宽配置及芯片的支持能力决定了射频工作在 20MHz 的带宽还是工作在 20/40MHz 的带宽。

9. MIMO模式

MIMO 是指一个天线采用多条流进行无线信号的发送和接收。MIMO 能够在不增加带宽的情况下成倍的提高信息吞吐量和频谱利用率。MIMO 模式包括以下四种：

- **1x1**：采用一条流进行无线信号的发送和接收。
- **2x2**：采用两条流进行无线信号的发送和接收。
- **3x3**：采用三条流进行无线信号的发送和接收。
- **4x4**：采用四条流进行无线信号的发送和接收。

支持流的数量与 AP 型号有关，请以设备的实际情况为准。

10. AP绿色节能功能

开启绿色节能功能后，在没有用户与 Radio 关联时，Radio 将工作在 1x1 模式（仅采用一条流进行无线信号的发送和接收），节省用电量。

11. 802.11n保护功能

说明

本功能所指的 802.11n 包括 802.11n 和 802.11ac。

当网络中同时存在 802.11n 和非 802.11n 的客户端，由于调制方式不同，非 802.11n 客户端无法解析 802.11n 信号，会导致非 802.11n 与 802.11n 网络之间彼此造成干扰。802.11n 保护功能用于避免干扰情况的发生，通过使 802.11n 设备发送 RTS/CTS 报文或 CTS-to-self 报文来取得信道使用权，确保非 802.11n 客户端能够检测到 802.11n 客户端正在进行数据传输，实现冲突避免。

开启 802.11n 保护功能后，当 AP 在其工作信道上扫描到非 802.11n 信号，则会在传输数据前通过发送 RTS/CTS 报文或 CTS-to-self 报文进行冲突避免，并通知客户端开始执行 802.11n 保护功能；如果未检测到非 802.11n 信号，则不会采取上述动作。

当非 802.11n 客户端在开启了 802.11n 或 802.11ac 的 AP 上接入时，AP 上的 802.11n 保护功能将自动开启并生效。

12. 智能天线功能

开启智能天线功能之后，AP 能够根据客户端的当前位置和信道信息，自动调整信号的发送参数，使射频能够集中发送至接收方所处的位置，从而提高客户端的信号质量和稳定性。

针对不同使用环境，本设备提供以下几种智能天线策略：

- 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。
- 高可靠性策略：优化噪声影响，抵抗局部干扰源，保证客户端带宽，降低客户端下线几率。本策略适用于对于带宽稳定要求较高的环境。
- 高吞吐量策略：提高收发信号强度，增加吞吐量。本策略适用于对于性能要求较高的环境。

1.8.9 802.11ac功能

说明

如果多个用户登录到 AC 设备上对某台 AP 配置 802.11ac 功能，同一时间只有一个用户可以配置成功。

802.11ac 是 802.11n 的继承者，它采用并扩展了源自 802.11n 的众多概念，包括更宽的射频带宽（提升至 160MHz）、更多的 MIMO 空间流（增加到 8）、多用户的 MIMO、以及更高阶的调制方式（达到 256QAM），从而进一步提高了 WLAN 的传输速率。

1. NSS

当802.11ac客户端上线时，将使用NSS（Number of Spatial Streams，空间流数）所对应的VHT-MCS索引所代表的调制与编码策略传输单播数据。

当非 802.11ac 客户端上线时，将使用基础速率或 MCS 所代表的调制与编码策略传输单播数据。

当未配置组播 NSS 时，802.11ac 客户端和 AP 之间将使用组播速率或组播 MCS 所代表的调制与编码策略发送组播数据。

当配置了组播 NSS 且客户端都是 802.11ac 客户端时，AP 和客户端将使用 VHT-MCS 索引所代表的调制与编码策略传输组播数据。

当配置了组播 NSS 且存在非 802.11ac 客户端时，AP 和客户端将使用基础模式的组播速率或 MCS 所代表的调制与编码策略传输组播数据，即 802.11a/b/g/n 的组播速率。

需要注意的是：

- 组播 NSS 需要小于或等于最大基本 NSS，最大基本 NSS 需要小于或等于最大支持 NSS。
- 配置的 802.11ac 基本 NSS 最大数值 number 表示射频的 802.11ac 最大基本 NSS，即该射频的 802.11ac 基本 NSS 是 1～number。
- 配置的 802.11ac 支持 NSS 最大数值 number 表示射频的 802.11ac 最大支持 NSS，即该射频的 802.11ac 支持 NSS 是 1～number。
- 配置的 802.11ac 组播 NSS 数值 number 表示射频发送 802.11ac 组播报文使用的 NSS。配置的 VHT-MCS 索引值 index 表示射频发送 802.11ac 组播报文使用的对应 NSS 的 VHT-MCS 索引。

2. 仅允许 802.11ac客户端接入功能

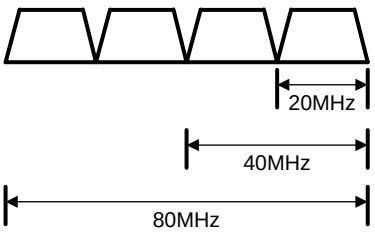
开启仅允许 802.11ac 客户端接入功能后，仅允许 802.11ac 客户端接入，不允许 802.11a/b/g/n 客户端接入，可以隔离低速率的客户端的影响，提高 802.11ac 设备的传输速率。

3. 802.11ac信道带宽

802.11ac 将信道带宽从 802.11n 的 20MHz/40MHz 提升到了 80MHz。带宽的提升带来了可用数据子载波的增加。

802.11ac 沿用了 802.11n 的信道带宽划定方式，通过将相邻的信道合并得到更大带宽的信道。在 802.11ac 中，可以将相邻的两个 20Mhz 信道合并得到带宽为 40Mhz 的信道，也可以将两个 40Mhz 带宽的信道合并，得到带宽为 80Mhz 的信道。

图1-7 802.11ac 信道带宽划定方式示意图



1.9 射频优化

WLAN RRM（Radio Resource Management，射频资源管理）是一种可升级的射频管理解决方案，通过“采集（AP 实时收集射频环境信息）—>分析（AC 对 AP 收集的数据进行分析评估）—>决策（根据分析结果，AC 统筹分配信道和发送功率）—>执行（AP 执行 AC 设置的配置，进行射频资源调优）”的方法，提供一套系统化的实时智能射频管理方案，使无线网络能够快速适应无线环境变化，保持最优的射频资源状态。WLAN RRM 主要通过信道调整和功率调整的方式来优化射频的服务质量。

1.9.1 信道调整

信道调整是指 AC 在调整周期到达时，通过计算信道质量，挑选出质量最优的信道应用到 Radio 上。影响信道质量的因素包括：

- 误码率：包括无线报文传输过程中物理层的误码率和 CRC 错误。
- 干扰：802.11 信号或非 802.11 信号对无线接入服务产生的影响。
- 重传：由于 AP 没有收到 ACK 报文造成的数据重传。
- 雷达信号：在工作信道上检测到雷达信号。在这种情况下，AC 会立即通知 AP 切换工作信道。

信道调整的工作流程如下：

(1) AC 检测当前工作信道，如果信道质量变差达到任意一个调整门限，则 AC 通过计算信道质量，挑选出质量最优的新信道。调整门限包括 CRC 错误门限、信道干扰门限和重传门限。

(2) AC 比较新旧信道的信道质量，只有在新旧信道的信道质量差超过容限系数时，AP 才会应用新信道。

1.9.2 功率调整

功率调整就是在整个无线网络的运行过程中，AC 能够根据实时的无线环境情况，动态地调整 Radio 的发送功率，使 Radio 的发送功率在能够覆盖足够范围的情况下减少对其他 Radio 的干扰。Radio 的发送功率增加或减少取决于以下因素：

- 邻居 Radio 数（邻居 Radio 指的是一个 Radio 能探测到的、由同一 AC 管理的其他 Radio）；
- 在邻居 Radio 的功率排名中指定 Radio；
- 指定邻居 Radio 接收到本 Radio 的功率值和设置的功率调整门限值的比较情况。

增加邻居 Radio 或某个邻居 Radio 发生故障或离线时，AP 会根据由邻居 Radio 的功率排名中指定 Radio 探测到本 AP 的 Radio 功率值和功率调整门限值的比较结果调整自身的发送功率。如果 AP 上某个 Radio 的邻居数达到触发功率调整的最大邻居数，AP 会根据以下原则来调整功率：

- 如果指定的邻居 Radio 接收到该 AP 上某 Radio 的功率大于配置的门限值，且差值超过 6，那么本 AP 会减小该 Radio 的功率。
- 如果指定的邻居 Radio 接收到该 AP 上某 Radio 的功率小于配置的门限值，且差值超过 3，那么本 AP 会增大该 Radio 的功率。

如果 Radio 的邻居 Radio 数小于触发功率调整的最大邻居数，AP 会将该 Radio 的功率调整到最大值。

AP 支持三种功率调整模式，它们分别适用于不同的无线环境：

- 自定义模式：缺省的功率调整模式，当覆盖模式与高密模式均无法达到理想效果时，可以通过手动配置功率调整参数来进行功率调整。
- 覆盖模式：该模式下功率调整方式偏向于扩大 AP 信号的覆盖范围，适用于 AP 数量较少的无线环境。
- 高密模式：该模式下的功率调整方式偏向于避免 AP 之间的信号干扰，适用于 AP 数量较多，存在大量信号重叠区域的无线环境。

高密模式和覆盖模式为系统预定义的功率调整模式，在这两种模式下，功率调整的相关参数为系统预设，不能修改。只有在自定义模式下，用户才能设置功率调整参数。

1.9.3 射频扫描

自动信道调整、自动功率调整功能处于关闭状态时，如果希望信道利用率与干扰率依旧能够实时显示，需要开启射频扫描功能。

开启射频扫描功能后，AP 将对无线环境进行扫描与数据采集工作，周期性的将数据上报给 AC，由 AC 生成信道报告和邻居报告，二者用于信道利用率、干扰率的统计。

1.9.4 RRM保持调整组

启用信道或功率调整功能后，每隔一定时间 AC 就会重新计算 Radio 的信道质量或功率大小，如果计算结果满足设定的调整条件，则会进行信道或功率的调整。但在某些干扰严重的环境，频繁调整信道或功率很可能会影响用户的正常使用。在这种情况下，可以通过配置 RRM 保持调整组，保证在一定时间内稳定 RRM 保持调整组内 Radio 的信道和功率。对于没有加入到 RRM 保持调整组的 Radio，其信道和功率将正常调整。

1.9.5 Baseline

Baseline（射频工作参数基线）保存了 Radio 的即时工作信道和传输功率，以及对应的射频参数信息。如果当前 Radio 的工作信道与功率值合适，则可以将 Radio 的信道、功率值存储为射频工作参数基线，在需要的时候重新应用这些保存的值。

射频工作参数基线保存、应用范围有三种：某 AP 下的一个 Radio、某 AP 组下同一型号 AP 的同一类型 Radio、同一 AC 下的所有 AP 的 Radio。

如果某个 Radio 满足下列条件之一，则射频工作参数基线中保存的工作信道与功率值均不会应用到对应的 Radio。

- 射频不存在；
- 射频状态为 Down；
- 射频工作参数基线中保存的射频类型与实际射频类型不匹配；
- 射频工作参数基线中保存的 AP 的区域码与实际情况不匹配；
- 无线服务未生效；
- 射频工作参数基线中保存的射频工作信道不合法；
- 射频工作参数基线中保存的射频带宽与实际射频带宽不匹配；
- 射频工作信道已手动配置为固定值；
- 工作信道被锁定；

- 当前工作信道处于信道保持调整期；
- 射频功率被锁定；
- 当前射频功率处于功率保持调整期；
- 射频工作参数基线中保存的射频功率小于配置的最小传输功率；
- 射频工作参数基线中保存的射频功率大于配置的最大传输功率。

1.10 负载均衡

1.10.1 负载均衡简介

WLAN 负载均衡用于在高密度无线网络环境中平衡 Radio 的负载，充分地保证每个 AP 的性能和无线客户端的带宽。

启动负载均衡的 WLAN 环境要求为：相互进行负载均衡的 AP 必须要连到同一 AC 上，并且客户端能扫描到相互进行负载均衡的 Radio，客户端接入的 SSID 快速关联功能处于关闭状态。

1.10.2 负载均衡类型

目前，AC 支持两种类型的负载均衡：基于 Radio 的负载均衡和基于负载均衡组的负载均衡。

- 基于 Radio 的负载均衡是针对 AC 上的所有 Radio 进行的负载均衡。
- 基于负载均衡组的负载均衡可以限制负载均衡的范围，在跨 AP 的多个 Radio 之间进行负载均衡。创建负载均衡组后，AC 将以负载均衡组为单位，在各个组内的 Radio 间进行会话模式、流量模式或带宽模式的负载均衡，没有加入到任何负载均衡组的 Radio 不会参与负载均衡。

1.10.3 负载均衡模式

- 会话模式：当 Radio 上的在线客户端数量达到或超过会话门限值并且与同一 AC 内其他 Radio 上的在线客户端数量最小者的差值达到或超过会话差值门限值，Radio 才会开始运行负载均衡。
- 流量模式：当 Radio 上的流量达到或超过流量门限值并且与同一 AC 内其他 Radio 上的流量最小者的差值达到或超过流量差值门限值，Radio 才会开始运行负载均衡。
- 带宽模式：当 Radio 上的带宽达到或超过带宽门限值并且与同一 AC 内其他 Radio 上的带宽最小者的差值达到或超过带宽差值门限值，Radio 才会开始运行负载均衡。

1.10.4 负载均衡参数

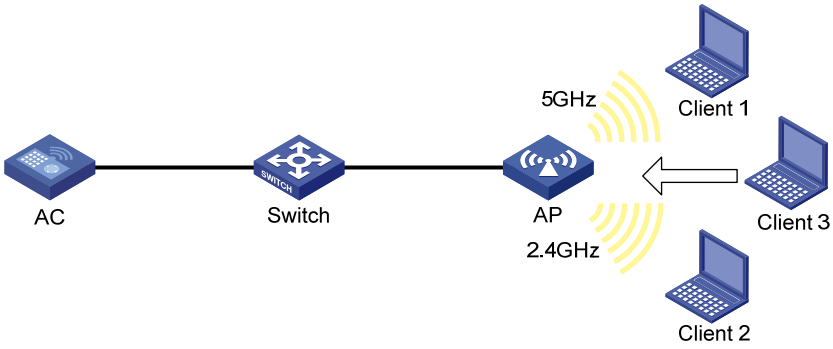
- 负载均衡 RSSI 门限：在进行负载均衡计算时，一个客户端可能会被多个 Radio 检测到，如果某个 Radio 检测到该客户端的 RSSI 值低于设定值，则该 Radio 将判定该客户端没有被检测到。如果只有过载的 Radio 可以检测到某客户端，其他 Radio 由于检测到该客户端的 RSSI 值低于设定值，将判定该客户端没有被检测到，则 AC 会通过让过载的 Radio 减少拒绝该客户端关联请求的最大次数，增大该客户端接入的概率。
- 设备拒绝客户端关联请求的最大次数：如果客户端反复向某个 Radio 发起关联请求，且 Radio 拒绝客户端关联请求次数达到设定的最大拒绝关联请求次数，那么该 Radio 会认为此时该客户端不能连接到其它任何的 Radio，在这种情况下， Radio 会接受该客户端的关联请求。

1.11 频谱导航

在实际无线网络环境中，有些客户端只能工作在 2.4GHz 频段上，有些客户端可以工作在 2.4GHz 频段或者 5GHz 频段，这有可能导致 2.4GHz 射频过载，5GHz 射频相对空余。在这种情况下，可以使用频谱导航功能，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。

如 图 1-8 所示，无线网络中存在三个客户端，AP上开启 5GHz射频和 2.4GHz射频，Client1 关联到AP的 5GHz射频，Client2 关联到AP的 2.4GHz射频。AC上开启频谱导航功能后，当Client3 准备接入无线网络时，如果对 5GHz射频进行关联，将直接关联成功，如果对 2.4GHz射频进行关联，将被AC拒绝。

图1-8 启动频谱导航的 WLAN 环境



1.12 探针

在 AP 的 Radio 接口上开启探针功能后，AP 通过对信道进行扫描，收集客户端信息并生成客户端表项，实现对客户端的监测。开启探针功能后，可以在“网络 > 监控 > 探针”页面中查看监测到的信息。

AP 的 Radio 接口不能同时开启 WIPS 功能和探针功能。

1.13 无线定位

无线定位技术是利用基于 WiFi 技术的 RFID（Radio Frequency Identification，射频识别）和支持 Wi-Fi 标准的设备发送的无线报文，实现对无线设备的定位、追踪和监测。目前，设备支持 AeroScout 定位、蓝牙定位、CUPID 定位和指纹定位四种定位方式。

1.13.1 无线定位系统的组成

无线定位系统由以下三类设备组成：

- 被定位的设备：可以向周围发送无线报文的设备，对于 AeroScout 定位来说，分为 Tag（AeroScout 公司生产的一种定位设备）和 MU（除 Tag 外的其他设备）两种类型。
- 定位信息接收设备：符合 802.11 标准要求的 AP 或其它接收设备。
- 定位服务器：运行定位软件的服务器。

定位信息接收设备将搜集到的定位信息发送到定位服务器，定位服务器通过软件计算出被定位设备的位置信息。

1.13.2 无线定位的工作过程简介

无线定位的工作过程为：

(1) AP 发现定位服务器

- 对于 AeroScout 定位，定位服务器在发起定位信息搜集时，首先向 AP 发起协商，通知 AP 需要搜集的设备类型，Tag 设备使用的组播地址等。AP 在收到定位服务器发送的报文后，会将报文中的 IP 地址和端口号保存，用来向定位服务器发送搜集到的定位信息。随后，AP 将开始搜集定位信息。
- 对于其他定位方式，AP 会根据配置的定位服务器地址发送收集到的定位信息。

(2) AP 搜集定位信息

AP 在收到由被定位设备发出的无线报文后，会将报文与搜集到的定位信息一起封装为定位协议的协议报文（下文中简称为定位报文）发送给定位服务器。

(3) 定位服务器进行定位计算

定位服务器收到定位报文后，提取报文中的定位信息并按照定位算法进行计算，得到被定位设备的位置信息。

1.13.3 接收报文相关处理

1. 信道匹配

在无线网络中，AP 可能收到非工作信道上的无线报文，由于 AP 接收到此类报文的 RSSI 要比报文所在信道的真实 RSSI 值低，不适合定位服务器进行定位计算。因此，AeroScout 定位方式中提供了信道匹配功能，AP 在接收到无线报文后，将按以下方法对 Tag 设备和 MU 设备进行信道匹配处理：

- Tag 设备会将每个无线报文在多个信道上进行发送，并且携带信道信息，以适应周围接收无线报文的不同 AP。AP 在收到无线报文后，将报文中携带的信道信息与当前工作信道进行比较，如果信道一致，则将该报文封装后发送给定位服务器，如果信道不一致，直接丢弃该报文。
- MU 设备发送的无线报文中不携带信道信息，由 AP 完成信道匹配难度较大，所以 AP 在收到 MU 设备发送的无线报文后，直接封装发送给定位服务器，由定位服务器完成信道匹配工作。

2. 报文稀释

由于 AP 需要将与自己关联和非关联的客户端定位报文都发送给定位服务器，报文数量可能非常庞大。通过报文稀释功能，可以有效减少 AP 向定位服务器发送的报文数量。报文稀释功能是指 AP 每收到一定数量的报文后，才会向定位服务器发送一个报文。例如，将稀释因子配置为 100，则 AP 在收到 100 个来自同一客户端的无线报文（不包括管理报文和广播报文）后，才会将其封装成定位报文并向定位服务器发送。

此外，在稀释超时时间内，若 AP 收到的报文数量没有达到稀释因子数，则将最近接收到的无线报文发送给定位服务器，避免报文搜集周期过长，影响定位的准确性。

2 网络安全

2.1 QoS策略

QoS 即服务质量。对于网络业务，影响服务质量的因素包括传输的带宽、传送的时延、数据的丢包率等。在网络中可以通过保证传输的带宽、降低传送的时延、降低数据的丢包率以及时延抖动等措施来提高服务质量。

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，灵活地进行 QoS 配置。

2.1.1 类

类用来定义一系列的规则来对报文进行分类。

2.1.2 流行为

流行为用来定义针对报文所做的 QoS 动作。

2.1.3 策略

策略用来将指定的类和流行为绑定起来，对符合分类条件的报文执行流行为中定义的动作。

2.1.4 应用策略

QoS 策略支持以下应用方式：

- 基于接口应用 QoS 策略：QoS 策略对通过接口接收或发送的流量生效。接口的每个方向（出和入两个方向）只能应用一个策略。如果 QoS 策略应用在接口的出方向，则 QoS 策略对本地协议报文不起作用。一些常见的本地协议报文如下：链路维护报文等。
- 基于全局应用 QoS 策略：QoS 策略对所有流量生效。

2.2 优先级映射

报文在进入设备以后，设备会根据映射规则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，就可以获得决定报文调度能力的各种优先级字段，从而为全面有效的控制报文的转发调度等级提供依据。

2.2.1 端口优先级

如果配置了优先级信任模式，即表示设备信任所接收报文的优先级，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参数。

如果没有配置优先级信任模式，并且配置了端口优先级值，则表明设备不信任所接收报文的优先级，而是使用端口优先级，按照映射表映射到报文的优先级参数。

1. 配置端口优先级

按照接收端口的端口优先级，设备通过一一映射为报文分配优先级。

2. 配置优先级信任模式

根据报文自身的优先级，查找优先级映射表，为报文分配优先级参数，可以通过配置优先级信任模式的方式来实现。

在配置接口上的优先级模式时，用户可以选择下列信任模式：

- Untrust：不信任任何优先级。
- Dot1p：信任报文自带的 802.1p 优先级，以此优先级进行优先级映射。
- DSCP：信任 IP 报文自带的 DSCP 优先级，以此优先级进行优先级映射。

2.2.2 优先级映射表

报文在进入设备以后，设备会根据映射规则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，就可以获得决定报文调度能力的各种优先级字段，从而为全面有效的控制报文的转发调度等级提供依据。

设备中提供了三张优先级映射表，分别 802.1p 优先级到本地优先级映射表、DSCP 到 802.1p 优先级映射表和 DSCP 到 DSCP 映射表。如果缺省优先级映射表无法满足用户需求，可以根据实际情况对映射表进行修改。

2.3 802.1X

802.1X 协议是一种基于端口的网络接入控制协议，即在局域网接入设备的端口上对所接入的用户和设备进行认证，以便控制用户设备对网络资源的访问。

2.3.1 802.1X的体系结构

802.1X 系统中包括三个实体：

- 客户端：请求接入局域网的用户终端，由局域网中的设备端对其进行认证。客户端上必须安装支持 802.1X 认证的客户端软件。
- 设备端：局域网中控制客户端接入的网络设备，位于客户端和认证服务器之间，为客户端提供接入局域网的端口，并通过与认证服务器的交互来对所连接的客户端进行认证。
- 认证服务器端：用于对客户端进行认证、授权和计费，通常为 RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）服务器。认证服务器根据设备端发送来的客户端认证信息来验证客户端的合法性，并将验证结果通知给设备端，由设备端决定是否允许客户端接入。

2.3.2 802.1X的认证方法

在接入设备上，802.1X 认证方法有三种方式：

- CHAP 或 PAP 认证方法。在这种方式下，设备对 EAP 认证过程进行终结，将收到的 EAP 报文中的客户端认证信息封装在标准的 RADIUS 报文中，与服务器之间采用 PAP 或 CHAP 方法进行认证。CHAP 以密文的方式传送密码，而 PAP 是以明文的方式传送密码。

- EAP 认证方法。在这种方式下，设备端对收到的 EAP 报文进行中继，使用 EAPOR（EAP over RADIUS）封装格式将其承载于 RADIUS 报文中发送给 RADIUS 服务器。

2.3.3 接入控制方式

端口支持以下两种接入控制方式：

- 基于端口认证：只要该端口下的第一个用户认证成功后，其它接入用户无须认证就可使用网络资源，但是当第一个用户下线后，其它用户也会被拒绝使用网络。
- 基于 MAC 认证：该端口下的所有接入用户均需要单独认证，当某个用户下线后，也只有该用户无法使用网络。

2.3.4 授权状态

端口支持以下三种授权状态：

- 强制授权：表示端口始终处于授权状态，允许用户不经认证即可访问网络资源。
- 强制非授权：表示端口始终处于非授权状态。设备端不为通过该端口接入的客户端提供认证服务。
- 自动识别：表示端口初始状态为非授权状态，仅允许 EAPOL 报文收发，不允许用户访问网络资源；如果用户通过认证，则端口切换到授权状态，允许用户访问网络资源。

2.3.5 周期性重认证

该功能开启后，设备会根据周期性重认证时间间隔定期向该端口在线 802.1X 用户发起重认证，以检测用户连接状态的变化、确保用户的正常在线，并及时更新服务器下发的授权属性（例如 ACL、VLAN、User Profile）。

2.3.6 在线用户握手

该功能开启后，设备会根据周期发送握手请求报文时间间隔定期向通过 802.1X 认证的在线用户发送握手报文，以定期检测用户的在线情况。如果设备连续多次没有收到客户端的响应报文，则会将用户置为下线状态。

2.3.7 安全握手

在线用户握手功能处于开启状态的前提下，还可以通过开启在线用户握手安全功能，来防止在线的 802.1X 认证用户使用非法的客户端与设备进行握手报文的交互，而逃过代理检测、双网卡检测等 iNode 客户端的安全检查功能。

2.3.8 认证触发

设备端主动触发方式用于支持不能主动发送 EAPOL-Start 报文的客户端，例如 Windows XP 自带的 802.1X 客户端。设备主动触发认证的方式分为以下两种：

- 单播触发：当设备收到源 MAC 地址未知的报文时，主动向该 MAC 地址单播发送 Identity 类型的 EAP-Request 帧来触发认证。若设备端在设置的时长内没有收到客户端的响应，则重发该报文。

- 组播触发：设备每隔一定时间（缺省为 30 秒）主动向客户端组播发送 Identity 类型的 EAP-Request 帧来触发认证。

2.3.9 Auth-Fail VLAN

802.1X Auth-Fail VLAN 功能允许用户在认证失败的情况下访问某一特定 VLAN 中的资源。需要注意的是，这里的认证失败是认证服务器因某种原因明确拒绝用户认证通过，比如用户密码错误，而不是认证超时或网络连接等原因造成的认证失败。

1. 基于端口认证

在接入控制方式为基于端口认证的端口上配置 Auth-Fail VLAN 后，若该端口上有用户认证失败，则该端口会离开当前的 VLAN 被加入到 Auth-Fail VLAN，所有在该端口接入的用户将被授权访问 Auth-Fail VLAN 里的资源。

当加入 Auth-Fail VLAN 的端口上有用户发起认证并失败，则该端口将会仍然处于 Auth-Fail VLAN 内；如果认证成功，则该端口会离开 Auth-Fail VLAN，之后端口加入 VLAN 情况与认证服务器是否下发授权 VLAN 有关，具体如下：

若认证服务器下发了授权 VLAN，则端口加入下发的授权 VLAN 中。用户下线后，端口会离开下发的授权 VLAN，若端口上配置了 Guest VLAN，则加入 Guest VLAN，否则加入缺省 VLAN。

若认证服务器未下发授权 VLAN，则端口回到缺省 VLAN 中。用户下线后，端口仍在缺省 VLAN 中。

2. 基于MAC认证

在接入控制方式为基于 MAC 认证的端口上配置 Auth-Fail VLAN 后，该端口上认证失败的用户将被授权访问 Auth-Fail VLAN 里的资源。

当 Auth-Fail VLAN 中的用户再次发起认证时，如果认证成功，则设备会根据认证服务器是否下发 VLAN 决定将该用户加入到下发的授权 VLAN 中，或使其回到端口的缺省 VLAN 中；如果认证失败，则该用户仍然留在该 Auth-Fail VLAN 中。

2.3.10 Guest VLAN

802.1X Guest VLAN 功能允许用户在未认证的情况下，访问某一特定 VLAN 中的资源。

当端口上处于 Guest VLAN 中的用户发起认证且失败时：如果端口配置了 Auth-Fail VLAN，则该端口会被加入 Auth-Fail VLAN；如果端口未配置 Auth-Fail VLAN，则该端口仍然处于 Guest VLAN 内。

当端口上处于 Guest VLAN 中的用户发起认证且成功时，端口会离开 Guest VLAN，之后端口加入 VLAN 情况与认证服务器是否下发 VLAN 有关，具体如下：

若认证服务器下发 VLAN，则端口加入下发的 VLAN 中。用户下线后，端口离开下发的 VLAN 回到初始 VLAN 中，该初始 VLAN 为端口加入 Guest VLAN 之前所在的 VLAN。

若认证服务器未下发 VLAN，则端口回到初始 VLAN 中。用户下线后，端口仍在该初始 VLAN 中。

根据端口的接入控制方式不同，Guest VLAN 的生效情况有所不同。

1. 基于端口认证

在接入控制方式为基于端口认证的端口上配置 Guest VLAN 后，若全局和端口上都使能了 802.1X，端口授权状态为 auto，且端口处于激活状态，则该端口就被立即加入 Guest VLAN，所有在该端口接入的用户将被授权访问 Guest VLAN 里的资源。

2. 基于MAC认证

在接入控制方式为基于 MAC 认证的端口上配置 Guest VLAN 后，端口上未认证的用户将被授权访问 Guest VLAN 里的资源。

2.3.11 Critical VLAN

802.1X Critical VLAN 功能允许用户在认证时，当所有认证服务器都不可达的情况下访问某一特定 VLAN 中的资源。目前，只采用 RADIUS 认证方式的情况下，在所有 RADIUS 认证服务器都不可达后，端口才会加入 Critical VLAN。若采用了其它认证方式，则端口不会加入 Critical VLAN。

根据端口的接入控制方式不同，Critical VLAN 的生效情况有所不同。

1. 基于端口认证

在接入控制方式为基于端口认证的端口上配置 Critical VLAN 后，若该端口上有用户认证时，所有认证服务器都不可达，则该端口会被加入到 Critical VLAN，之后所有在该端口接入的用户将被授权访问 Critical VLAN 里的资源。在用户进行重认证时，若所有认证服务器都不可达，且端口指定在此情况下强制用户下线，则该端口也会被加入到 Critical VLAN。

已经加入 Critical VLAN 的端口上有用户发起认证时，如果所有认证服务器不可达，则端口仍然在 Critical VLAN 内；如果服务器可达且认证失败，且端口配置了 Auth-Fail VLAN，则该端口将会加入 Auth-Fail VLAN，否则回到端口的缺省 VLAN 中；如果服务器可达且认证成功，则该端口加入 VLAN 的情况与认证服务器是否下发 VLAN 有关，具体如下：

若认证服务器下发了授权 VLAN，则端口加入下发的授权 VLAN 中。用户下线后，端口会离开下发的授权 VLAN，若端口上配置了 Guest VLAN，则加入 Guest VLAN，否则加入缺省 VLAN。

若认证服务器未下发授权 VLAN，则端口回缺省 VLAN 中。用户下线后，端口仍在缺省 VLAN 中。

2. 基于MAC认证

在接入控制方式为基于 MAC 认证的端口上配置 Critical VLAN 后，若该端口上有用户认证时，所有认证服务器都不可达，则端口将允许 Critical VLAN 通过，用户将被授权访问 Critical VLAN 里的资源。

当 Critical VLAN 中的用户再次发起认证时，如果所有认证服务器不可达，则用户仍然在 Critical VLAN 中；如果服务器可达且认证失败，且端口配置了 Auth-Fail VLAN，则该用户将会加入 Auth-Fail VLAN，否则回到端口的缺省 VLAN 中；如果服务器可达且认证成功，则设备会根据认证服务器是否下发授权 VLAN 决定将该用户加入下发的授权 VLAN 中，或使其回到端口的缺省 VLAN 中。

2.3.12 端口的强制认证ISP域

在端口上指定强制认证域为 802.1X 接入提供了一种安全控制策略。所有从该端口接入的 802.1X 用户将被强制使用指定的认证域来进行认证、授权和计费，从而防止用户通过恶意假冒其它域账号从本端口接入网络。另外，管理员也可以通过配置强制认证域对不同端口接入的用户指定不同的认证域，从而增加了管理员部署 802.1X 接入策略的灵活性。

2.3.13 EAD快速部署

EAD（Endpoint Admission Defense，端点准入防御）作为一个网络端点接入控制方案，它通过安全客户端、安全策略服务器、接入设备以及第三方服务器的联动，加强了对用户的集中管理，提升

了网络的整体防御能力。但是在实际的应用过程中 EAD 客户端的部署工作量很大，例如，需要网络管理员手动为每一个 EAD 客户端下载、升级客户端软件，这在 EAD 客户端数目较多的情况下给管理员带来了操作上的不便。

802.1X 认证支持的 EAD 快速部署功能就可以解决以上问题，它允许未通过认证的 802.1X 用户访问一个指定的 IP 地址段（称为 Free IP），并可以将用户发起的 HTTP 访问请求重定向到该 IP 地址段中的一个指定的 URL，实现用户自动下载并安装 EAD 客户端的目的。

2.3.14 配置 802.1X SmartOn功能

开启了 SmartOn 功能的端口上收到 802.1X 客户端发送的 EAPOL-Start 报文后，将向其回复单播的 EAP-Request/Notification 报文，并开启 SmartOn 通知请求超时定时器定时器等待客户端响应的 EAP-Response/Notification 报文。若 SmartOn 通知请求超时定时器超时后客户端仍未回复，则设备会重发 EAP-Request/Notification 报文，并重新启动该定时器。当重发次数达到规定的最大次数后，会停止对该客户端的 802.1X 认证；若在重发次数达到最大次数之前收到了该 Notification 报文的回复报文，则获取该报文中携带的 Switch ID 和 SmartOn 密码的 MD5 摘要，并与设备本地配置的 SmartOn 的 Switch ID 以及 SmartOn 密码的 MD5 摘要值比较，若相同，则继续客户端的 802.1X 认证，否则中止客户端的 802.1X 认证。

802.1X SmartOn 功能与在线用户握手功能互斥，建议两个功能不要同时开启。

2.4 ISP域

设备对用户的管理是基于 ISP（Internet Service Provider，互联网服务提供者）域的，一个 ISP 域对应着一套实现 AAA（Authentication、Authorization、Accounting，认证、授权、计费）的配置策略，它们是管理员针对该域用户制定的一套认证、授权、计费方法，可根据用户的接入特征以及不同的安全需求组合使用。

设备支持的认证方法包括：

- 不认证：对用户非常信任，不对其进行合法性检查，一般情况下不采用这种方法。
- 本地认证：认证过程在接入设备上完成，用户信息（包括用户名、密码和各种属性）配置在接入设备上。优点是速度快，可以降低运营成本；缺点是存储信息量受设备硬件条件限制。
- 远端认证（RADIUS）：认证过程在接入设备和远端的服务器之间完成，接入设备和远端服务器之间通过 RADIUS 协议通信。优点是用户信息集中在服务器上统一管理，可实现大容量、高可靠性、支持多设备的集中式统一认证。当远端服务器无效时，可配置备选认证方式完成认证。

设备支持的授权方法包括：

- 不授权：接入设备不请求授权信息，不对用户可以使用的操作以及用户允许使用的网络服务进行授权。此时，认证通过的 login 用户只有系统所给予的缺省用户角色，其中 FTP/SFTP/SCP 用户的工作目录是设备的根目录，但并无访问权限；认证通过的非 login 用户，可直接访问网络。
- 本地授权：授权过程在接入设备上进行，根据接入设备上为本地用户配置的相关属性进行授权。
- 远端授权（RADIUS）：授权过程在接入设备和远端服务器之间完成。RADIUS 协议的认证和授权是绑定在一起的，不能单独使用 RADIUS 进行授权。RADIUS 认证成功后，才能进行授

权，RADIUS 授权信息携带在认证回应报文中下发给用户。当远端服务器无效时，可配置备选授权方式完成授权。

设备支持的计费方法包括：

- 不计费：不对用户计费。
- 本地计费：计费过程在接入设备上完成，实现了本地用户连接数的统计和限制，并没有实际的费用统计功能。
- 远端计费（RADIUS）：计费过程在接入设备和远端的服务器之间完成。当远端服务器无效时，可配置备选计费方式完成计费。

每个用户都属于一个 ISP 域。为便于对不同接入方式的用户进行区分管理，提供更为精细且有差异化的认证、授权、计费服务，设备将用户划分为以下几个类型：

- LAN 接入用户：例如 802.1X 认证用户。
- 登录用户：例如 Telnet、FTP、终端接入用户（即从 Console、AUX 等接口登录的用户）。
- Portal 用户。

在多 ISP 的应用环境中，不同 ISP 域的用户有可能接入同一台设备，因此系统中可以存在多个 ISP 域，其中包括一个缺省存在的名称为 system 的 ISP 域。如果某个用户在登录时没有提供 ISP 域名，系统将把它归于缺省的 ISP 域。系统缺省的 ISP 域可以手工修改为一个指定的 ISP 域。

用户认证时，设备将按照如下先后顺序为其选择认证域：接入模块指定的认证域-->用户名中指定的 ISP 域-->系统缺省的 ISP 域。其中，仅部分接入模块支持指定认证域，例如 802.1X 认证。

2.5 RADIUS

2.5.1 RADIUS协议简介

RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）是一种分布式的、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。

- RADIUS 客户端：一般位于接入设备上，可以遍布整个网络，负责将用户信息传输到指定的 RADIUS 服务器，然后根据服务器返回的信息进行相应处理（如接受/拒绝用户接入）。
- RADIUS 服务器：一般运行在中心计算机或工作站上，维护用户的身份信息和与其相关的网络服务信息，负责接收接入设备发送的认证、授权、计费请求并进行相应的处理，然后给接入设备返回处理结果（如接受/拒绝认证请求）。

RADIUS 协议使用 UDP 作为封装 RADIUS 报文的传输层协议，通过使用共享密钥机制来保证客户端和 RADIUS 服务器之间消息交互的安全性。

当接入设备对用户提供 AAA（Authentication、Authorization、Accounting，认证、授权、计费）服务时，若要对用户采用 RADIUS 服务器进行认证、授权、计费，则作为 RADIUS 客户端的接入设备上需要配置相应的 RADIUS 服务器参数。

2.5.2 RADIUS增强功能

1. Accounting-on功能

设备重启后，重启前的原在线用户可能会被 RADIUS 服务器认为仍然在线而短时间内无法再次登录。为了解决这个问题，需要开启 Accounting-on 功能。

开启了 Accounting-on 功能后，设备会在重启后主动向 RADIUS 服务器发送 Accounting-on 报文来告知自己已经重启，并要求 RADIUS 服务器停止计费且强制通过本设备上线的用户下线。若设备发送 Accounting-on 报文后 RADIUS 服务器无响应，则会在按照一定的时间间隔尝试重发几次。分布式设备单板重启时，Accounting-on 功能的实现需要和 H3C IMC 网管系统配合使用。

2. Session control功能

H3C 的 IMC RADIUS 服务器使用 session control 报文向设备发送授权信息的动态修改请求以及断开连接请求。设备上开启接收 session control 报文的开关后，会打开知名 UDP 端口 1812 来监听并接收 RADIUS 服务器发送的 session control 报文。

需要注意的是，该功能仅能和 H3C 的 IMC RADIUS 服务器配合使用。

2.6 BYOD

BYOD（Bring Your Own Device）指携带自己的设备办公，这些设备主要是指个人电脑、手机、平板电脑等终端设备。BYOD 解决方案可以为企业和用户提供基于用户身份信息、终端信息、接入场景的认证、授权服务。

2.6.1 BYOD规则

BYOD 规则是用户终端特征与用户终端类型的一种映射关系。在用户认证的过程中，接入设备获取到用户终端的相关特征（例如 DHCP Option 55 指纹信息）后，可根据 BYOD 规则识别出用户所使用的终端类型。

目前 BYOD 支持的用户终端特征包括：DHCP Option 55、HTTP User Agent 和 MAC 地址。

- DHCP Option55：DHCP 请求参数列表选项，终端利用该选项指明需要从服务器获取哪些网络配置参数。
- HTTP UserAgent：属于 HTTP 请求报文头域的一部分，用于携带终端访问 Web 页面时所使用的操作系统（包括版本号）、浏览器（包括版本号）等信息。
- MAC 地址：终端的 MAC OUI 信息或终端所属的 MAC 地址范围。

同一个特征只能对应一种终端类型，但一种终端类型可以对应多个特征。不同终端特征的识别优先级由高到低为：DHCP Option 55 指纹->HTTP User Agent 指纹->MAC 地址指纹。

系统中已经预定义了一系列常用的 BYOD 规则，用户也可以根据实际组网需求通过命令行添加规则。

2.6.2 BYOD授权

BYOD 授权是指，用户通过本地认证之后，设备通过匹配该用户的终端特征来给用户授予相关的网络访问权限。BYOD 授权是通过用户组实现的。每一个用户都属于一个用户组，用户组中定义了基于终端类型的授权属性。用户在认证过程中，接入设备通过 BYOD 规则来识别用户的终端类型，并根据识别出的终端类型为其授权相应的授权属性。

2.7 本地认证

本地认证泛指由接入设备对用户进行认证、授权和计费，进行本地认证的用户的信息（包括用户名、密码和各种属性）配置在接入设备上。

为使某个请求网络服务的用户可以通过本地认证，需要在设备上添加相应的用户条目。所谓用户，是指在设备上设置的一组用户属性的集合，该集合以用户名唯一标识。

为了简化用户的配置，增强用户的可管理性，引入了用户组的概念。用户组是一系列公共用户属性的集合，某些需要集中管理的公共属性可在用户组中统一配置和管理，属于该用户组的所有用户都可以继承这些属性。

2.8 来宾管理

随着无线智能终端的快速发展，对于来公司参观的访客，公司需要提供一些网络服务。这些访客成员通常为供应商、贵宾、听众或者是其他合作伙伴等。当访客用自己的手机、笔记本、IPAD 等终端接入公司网络时，涉及到用户账号注册，以及访问权限控制的问题。为了简化访客的注册和审批流程，以及对访客权限的管理控制，提供了来宾用户管理功能，具体包括：

- 手工添加来宾用户：手工创建来宾用户，并配置相应的来宾用户属性。
- 导入来宾用户：将指定路径 CSV 文件的来宾帐户信息导入到设备上，并生成相应的来宾用户。
- 批量创建来宾用户：批量生成一系列来宾用户，相应的用户名和密码按照指定规律生成。
- 导出来宾用户：将设备上的来宾帐户信息导出到指定路径 CSV 文件中供其它设备使用。
- 来宾用户的注册与审批，具体过程如下：

(1) 来宾用户通过设备推出的 Portal Web 页面填写注册信息，主要包括用户名、密码和电子邮箱地址，并提交该信息。

(2) 设备收到来宾用户的注册信息后，记录该注册信息，并向来宾管理员发送一个注册申请通知邮件。

(3) 来宾管理员收到注册申请通知邮件之后，在 Web 页面上对注册用户进行编辑和审批。

(4) 如果该注册用户在等待审批时间超时前被来宾管理员审批通过，则设备将自动创建一个来宾用户，并生成该用户的相关属性。若该注册用户在等待审批时间超时后还未被审批通过，则设备将会删除本地记录的该用户注册信息。

(5) 来宾用户创建之后，设备将自动发送邮件通知来宾用户或来宾接待人用户注册成功，向他们告知来宾用户的密码及有效期信息。

(6) 来宾用户收到注册成功通知后，将可以使用注册的帐户访问网络。

- 来宾用户过期自动删除功能：设备定时检查本地来宾用户是否过期并自动删除过期的用户。
- 邮件通知功能：向来宾、来宾接待人、来宾管理员发送帐户审批、密码信息的邮件。

2.9 接入管理

2.9.1 端口安全

端口安全是一种基于 MAC 地址对网络接入进行控制的安全机制，是对已有的 802.1X 认证和 MAC 地址认证的扩充。这种机制通过检测端口收到的数据帧中的源 MAC 地址来控制非授权设备或主机对网络的访问，通过检测从端口发出的数据帧中的目的 MAC 地址来控制对非授权设备的访问。

端口安全的主要功能是通过定义各种端口安全模式，让设备学习到合法的源 MAC 地址，以达到相应的网络管理效果。启动了端口安全功能之后，当发现非法报文时，系统将触发相应特性，并按照预先指定的方式进行处理，既方便用户的管理又提高了系统的安全性。这里的非法报文是指：

- MAC 地址未被端口学习到的用户报文；

- 未通过认证的用户报文。

2.9.2 Portal

Portal 在英语中是入口的意思。Portal 认证通常也称为 Web 认证，即通过 Web 页面接受用户输入的用户名和密码，对用户进行身份认证，以达到对用户访问进行控制的目的。在采用了 Portal 认证的组网环境中，未认证用户上网时，接入设备强制用户登录到特定站点，用户可以免费访问其中的服务；当用户需要使用互联网中的其它信息时，必须在 Portal Web 服务器提供的网站上进行 Portal 认证，只有认证通过后才可以使用这些互联网中的设备或资源。

根据是否为用户主动发起认证，可以将 Portal 认证分为主动认证和强制认证两种类型：用户可以主动访问已知的 Portal Web 服务器网站，输入用户名和密码进行认证，这种开始 Portal 认证的方式称作主动认证；用户访问任意非 Portal Web 服务器网站时，被强制访问 Portal Web 服务器网站，继而开始 Portal 认证的过程称作强制认证。

Portal 认证是一种灵活的访问控制技术，可以在接入层以及需要保护的关键数据入口处实施访问控制，具有如下优势：

- 可以不安装客户端软件，直接使用 Web 页面认证，使用方便。
- 可以为运营商提供方便的管理功能和业务拓展功能，例如运营商可以在认证页面上开展广告、社区服务、信息发布等个性化的业务。
- 支持多种组网型态，例如二次地址分配认证方式可以实现灵活的地址分配策略且能节省公网 IP 地址，可跨三层认证方式可以跨网段对用户作认证。

3 工具

3.1 无线报文捕获

无线报文捕获是一种报文捕获及分析特性，该特性能够捕获设备接口的入方向报文并对报文进行解析处理，便于用户分析接口接收到的报文；还可以将报文数据存储为 pcap 格式的文件，方便用户后续查看。

目前支持以下两种报文捕获的方式：

- 本地报文捕获

本地报文捕获方式下，设备将捕获的报文自动上传到 FTP 服务器。

- 远程报文捕获

远程报文捕获方式下，设备与第三方报文捕获软件 Wireshark 客户端建立连接，并将捕获的报文发送给 Wireshark 客户端，供用户在 Wireshark 客户端上查看。Wireshark 客户端连接到 AP 的 RPCAP 服务端口，就可以获取到指定的 Radio 口捕获的从客户端发往 AP 的报文。

3.1.1 无线报文捕获过滤规则

无线报文捕获可以使用捕获过滤表达式指定捕获过滤规则，对进入指定物理接口的报文进行过滤，满足捕获过滤规则的报文则被捕获。捕获过滤规则由关键字、逻辑操作符、运算操作符和比较操作符等组合而成。有关无线报文捕获更多规则的详细介绍，请参见网址：http://wiki.wireshark.org/CaptureFilters。

3.1.2 关键字

捕获过滤规则使用的关键字分为常量关键字和变量关键字。

1. 常量关键字

常量关键字是固定的字符串，可以分为以下几类：协议类型、传输方向和传输方向的类型等。

表3-1 常量关键字

常量关键字类型	描述	关键字
协议	捕获指定的协议报文。如果没有指明协议类型，默认捕获所有Packet Capture支持的协议	支持的协议有：ip，ip6，arp，tcp，udp，icmp等
报文传输方向	捕获指定传输方向的报文。如果没有指定本关键字，默认报文传输方向为源或目的方向	• src：表示源方向 • dst：表示目的方向 • src or dst：表示源或目的方向
报文传输方向类型	捕获指定的报文传输方向类型的报文。如果没有指定本类关键字，默认报文传输方向类型为主机	• host：表示主机 • net：表示网段 • port：表示端口号

常量关键字类型	描述	关键字
		• portrange：表示端口号范围
特殊关键字	-	• broadcast：表示捕获广播报文 • multicast：表示捕获组播报文、广播报文 • less：表示小于等于 • greater：表示大于等于 • len：表示报文长度 • vlan：表示捕获 VLAN 报文

2. 变量关键字

变量关键字形式固定，但内容可变。捕获过滤规则的变量关键字不可以单独使用，其前需要使用常量关键字对其进行修饰。

需要注意的是，所有的协议类型常量关键字、broadcast 和 multicast 关键字不能对变量关键字进行修饰。其它的常量关键字不可单独使用，其后需要使用变量关键字。

表3-2 变量关键字

变量关键字类型	举例
整型	将整型用二进制、八进制、十进制或十六进制形式表示。例如：port 23，表示端口号为23
整型范围	将整型范围用二进制、八进制、十进制、十六进制形式和“-”表示。例如：portrange 100-200，表示端口号范围为100到200
IPv4地址	使用点分十进制格式表示。例如：src 1.1.1.1，表示源主机IPv4地址是1.1.1.1（在没有指定报文传输方向类型时，报文传输方向类型默认为host）
IPv6地址	使用冒号分十六进制格式表示。例如：dst host 1::1，表示报文的目的主机IPv6地址是1::1
IPv4网段	使用IPv4地址和掩码或者IPv4网络号表示。以下两种表达式等价： • src 1.1.1，表示源主机的 IPv4 网段为 1.1.1 • src net 1.1.1.0/24，表示源主机的 IPv4 网段为 1.1.1.0/24
IPv6网段	使用IPv6地址和网络前缀表示。例如：dst net 1::/64，表示目的IPv6网段为1::/64 • 需要注意的是，指定 IPv6 网段变量关键字时，必须指定 net 常量关键字

3.1.3 捕获过滤操作符

1. 逻辑操作符

逻辑操作符的逻辑运算顺序为从左到右，下表为逻辑操作符的分类举例。

表3-3 逻辑操作符

逻辑操作符	描述
!或者not	非操作符。表示对捕获过滤规则取反操作

逻辑操作符	描述
&&或者and	与操作符。表示连接多个捕获过滤规则。当此操作符连接多个过滤规则时，报文若符合此操作符连接的全部过滤规则，才会过滤成功，否则，过滤失败。
||或者or	或操作符。表示对多个捕获过滤规则进行选择。当此操作符连接多个过滤规则时，报文若不符合此操作符连接的全部过滤规则，才会过滤失败，否则，过滤成功。

其中非操作符优先级最高，与操作符和或操作符的优先级相同。

2. 运算操作符

表3-4 运算操作符

运算操作符	描述
+	加法运算符，用来将其两侧的值加到一起
-	减法运算符，用来将它前面的数值中减去它后面的数值
*	乘法运算符，用来将其两侧的值相乘
/	除法运算符，用来将其左边的值被右边的值除
&	按位与，用来将其两侧的数值逐位进行比较产生一个新值。对于每一位，只有两个操作数的对应位都为1时结果才为1
|	按位或，用来将其两侧的操作数逐位进行比较产生一个新值。对于每一位，如果其中任意操作数中对应的位为1，那么结果位就为1
<<	按位左移，用来将其左侧操作数的每位向左移动，移动的位数由其右侧操作数指定
>>	按位右移，用来将其左侧操作数的每位向右移动，移动的位数由其右侧操作数指定
[ ]	取位运算符，与协议类型关键字结合使用。例如：ip[6]，表示IP报文偏移6个字节后，取得的一个字节的值

3. 比较操作符

下表为比较操作符的分类举例。

表3-5 比较操作符分类

比较操作符	描述
=	相等，判断两侧操作数是否相等。例如：ip[6]=0x1c，表示捕获IPv4报文数据域偏移6字节，取得的一个字节值为0x1c的报文
!=	不等，判断两侧操作数是否不等。例如：len!=60，表示捕获报文长度不等于60字节的报文
>	大于，判断左侧操作数大于右侧操作数。例如：len>100，表示捕获报文长度大于100字节的报文
<	小于，判断左侧操作数小于右侧操作数。例如：len<100，表示捕获报文长度小于100字节的报文
>=	大于等于，判断左侧操作数大于等于右侧操作数；与常量关键字greater等价。例如：len>=100，表示捕获报文长度大于等于100字节的报文
<=	小于等于，判断左侧操作数小于等于右侧操作数；与常量关键字less等价。例如：len<=100，表示捕获报文长度小于等于100字节的报文

3.1.4 捕获过滤表达式

捕获过滤表达式由关键字、逻辑操作符、运算操作符和比较操作符之间的多种组合而成。以下为典型捕获过滤表达式：

1. 逻辑操作符表达式

由关键字和逻辑运算符组合的捕获过滤表达式。例如：not port 23 and not port 22，表示捕获端口号既不是 23，又不是 22 的报文；port 23 or icmp，表示捕获端口号是 23 或 icmp 协议的报文。

由逻辑操作符连接的多个变量关键字，可以使用同一个常量关键字进行修饰（就近原则），例如：src 192.168.56.1 or 192.168.27，表示捕获的源 IPv4 地址为 192.168.56.1 或者源 IPv4 网段为 192.168.27 的报文。上述表达式与“src 192.168.56.1 or src 192.168.27”等价。

2. *expr relop expr*表达式

由关键字、运算操作符和比较操作符组合的捕获过滤表达式。其中，*expr* 是算术表达式；*relop* 为比较操作符。例如：len+100>=200，表示捕获长度大于等于 100 字节的报文。

3. *proto* [*expr*:*size*]表达式

由协议类型关键字和运算操作符“[ ]”组合的捕获过滤表达式。其中，*proto* 表示协议类型，*expr* 为算术表达式，表示偏移量，*size* 为整数，表示字节个数，缺省值为 1。*proto* [*expr*:*size*]的返回值为从 *proto* 协议报文数据区域起始位置，偏移 *expr* 个字节开始，取 *size* 个字节的数据。例如：ip[0]&0xf != 5，表示捕获第一个字节与 0x0f 按位相与得到的值不是 5 的 IP 报文。

expr:*size* 也可以使用名字表示。例如：icmptype 表示 ICMP 报文的类型域，则表达式：icmp[icmptype]=0x08，表示捕获 icmp 的 type 字段的值为 0x08 的报文。

4. vlan *vlan_id*表达式

由关键字 vlan，逻辑操作符等组合的捕获过滤表达式。其中，*vlan_id* 为整型，表示 VLAN 编号。例如，vlan 1 and ip6，表示捕获 VLAN 编号为 1 的 IPv6 报文。

需要注意的是：

- 如果用户需要对带 VLAN 的报文进行捕获过滤，必须使用此类捕获过滤表达式且关键字 vlan 要在其它捕获过滤条件之前指定，否则不能正常过滤。例如：icmp，表示捕获不带 vlan 的 icmp 报文。
- 如果捕获过滤规则之前没有指定 vlan，则认为这些捕获过滤规则只对不带 vlan 的报文进行捕获过滤，即对带 vlan 的报文不捕获。例如：
  - !tcp and vlan 1：表示捕获不带 vlan 标记的 tcp 报文以外的且属于 vlan 1 的报文。
  - icmp and vlan 1：icmp 表示捕获不带 vlan 标记的 icmp 协议报文，而 vlan 1 表示捕获 vlan 标记为 1 的报文，所以该捕获过滤表达式前后矛盾，因此不会收到任何报文，对于此类捕获过滤规则，只要没有语法错误，命令行均会下发成功，用户需要自己保证逻辑的正确性。
  - RF Ping
  - RF Ping 即无线链路质量检测。该检测过程中，AP 根据客户端上线时协商的速率集，以每个速率发送 5 个空数据报文进行链路质量检测。AP 根据客户端的响应报文可以获取 AP 与客户端之间的无线链路质量信息，如信号强度、报文重传次数、RTT（Round-trip Time，往返时间）等。

目 录

1 系统功能配置举例

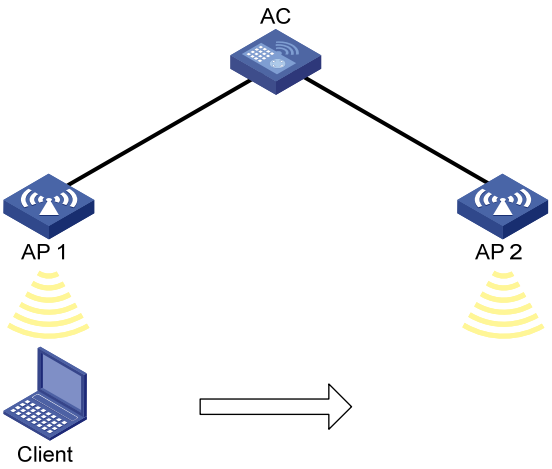
1.1 网络配置功能配置举例

1.1.1 AC内漫游配置举例

1. 组网需求

如 图 1-1 所示，仅有一台AC，要求客户端在AC内的不同AP间进行漫游。

图1-1 AC 内漫游配置组网图



2. 配置步骤

(1) 配置无线服务

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > 无线网络”，进入“无线网络”页面配置无线服务，配置步骤为：

- 创建一个无线服务，名称为 service。
- 配置 SSID 为 roaming。
- 开启无线服务。

(2) 配置 AP

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > AP 管理”，进入“AP”页面配置 AP，配置步骤为：

- 进入 AP 1 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 AP 1 的射频。
- 进入 AP 2 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 AP 2 的射频。

3. 验证配置

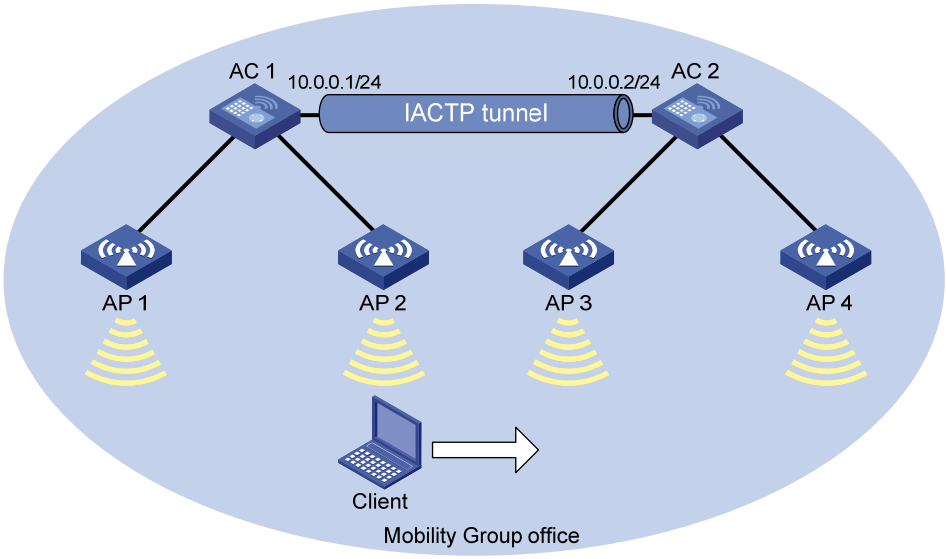
单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 漫游”，进入“漫游”页面查看客户端漫游前和漫游后所关联的 AC 和 AP。

1.1.2 AC间漫游配置举例

1. 组网需求

如 图 1-2 所示，在一个无线网络中，有两台AC，现要求客户端可以在AC内漫游，也可以跨AC漫游。

图1-2 AC 间漫游配置组网图



2. 配置步骤

(1) 配置 AC 1

配置无线服务

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > 无线网络”，进入“无线网络”页面配置无线服务，配置步骤为：

- 创建一个无线服务，名称为 service 的。
- 配置 SSID 为 roaming。
- 开启无线服务。

配置 AP

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > AP 管理”，进入“AP”页面配置 AP，配置步骤为：

- 进入 AP 1 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 AP 1 的射频。
- 进入 AP 2 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 AP 2 的射频。

配置漫游组

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 漫游”，进入“漫游”页面配置漫游，配置步骤为：

- 创建名称为 office 的漫游组。
- 选择隧道 IP 地址类型为 IPv4。
- 选择隧道的源 IPv4 地址为 10.0.0.1。
- 添加漫游组成员 IPv4 地址为 10.0.0.2。

- 配置漫游组状态为开启。

(2) 配置 AC 2

配置无线服务

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > 无线网络”，进入“无线网络”页面配置无线服务，配置步骤为：

- 创建一个无线服务，名称为 service。
- 配置 SSID 为 roaming。
- 开启无线服务。

配置 AP

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > AP 管理”，进入“AP”页面配置 AP，配置步骤为：

- 进入 AP 3 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 AP 3 的射频。
- 进入 AP 4 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 AP 4 的射频。

配置漫游组

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 漫游”，进入“漫游”页面配置漫游，配置步骤为：

- 创建名称为 office 的漫游组。
- 选择隧道 IP 地址类型为 IPv4。
- 选择隧道的源 IPv4 地址为 10.0.0.2。
- 添加漫游组成员 IPv4 地址为 10.0.0.1。
- 配置漫游组状态为开启。

3. 验证配置

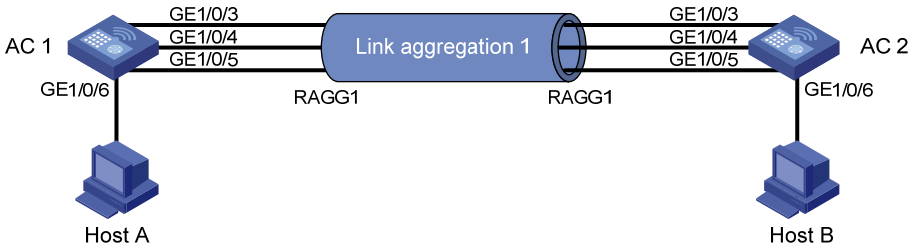
单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 漫游”，进入“漫游”页面查看客户端漫游前和漫游后所关联的 AC 和 AP。

1.1.3 二层以太网静态链路聚合配置举例

1. 组网需求

- AC 1 与 AC 2 通过各自的二层以太网接口 GigabitEthernet1/0/3～GigabitEthernet1/0/5 相互连接。
- 在 AC 1 和 AC 2 上分别配置二层静态链路聚合组，以提高链路的可靠性。

图1-3 以太网链路聚合配置组网图



2. 配置步骤

(1) 配置以太网链路聚合

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 接口”，进入“链路聚合”页面配置链路聚合，配置步骤为：

- 在 AC 1 上添加二层聚合组 1，指定聚合模式为静态聚合，将接口 GigabitEthernet1/0/3～GigabitEthernet1/0/5 加入到该聚合组中。
- AC 2 配置与 AC 1 相同。

(2) 配置 VLAN

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > VLAN”，进入“VLAN”页面配置 VLAN，配置步骤为：

- 在 AC 1 上创建 VLAN 10。进入 VLAN 10 的详情页面，将与 Host A 相连的接口 GigabitEthernet1/0/6 加入 VLAN 10 的 Untagged 端口列表，将接口 GigabitEthernet1/0/3～GigabitEthernet1/0/5 加入 VLAN 10 的 Tagged 端口列表。
- AC 2 配置与 AC 1 相同。

3. 验证配置

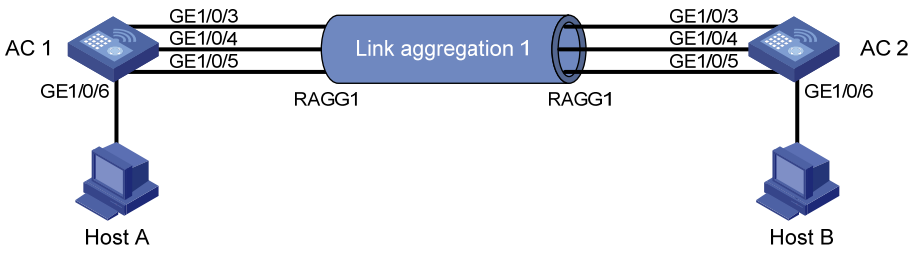
完成上述配置后，在“链路聚合”页面中可以看到 GigabitEthernet1/0/3～GigabitEthernet1/0/5 已经加入到静态聚合组 1。Host A 能够 Ping 通 Host B。AC 1 与 AC 2 之间的一条链路故障后，Host A 仍然能够 Ping 通 Host B。

1.1.4 二层以太网动态链路聚合配置举例

1. 组网需求

- AC 1 与 AC 2 通过各自的二层以太网接口 GigabitEthernet1/0/3～GigabitEthernet1/0/5 相互连接。
- 在 AC 1 和 AC 2 上分别配置二层动态链路聚合组，以提高链路的可靠性。

图1-4 以太网链路聚合配置组网图



2. 配置步骤

(1) 配置以太网链路聚合

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 接口”，进入“链路聚合”页面配置链路聚合，配置步骤为：

- 在 AC 1 上添加二层聚合组 1，指定聚合模式为动态聚合，将接口 GigabitEthernet1/0/3～GigabitEthernet1/0/5 加入到该聚合组中。

- AC 2 配置与 AC 1 相同。

(2) 配置 VLAN

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > VLAN”，进入“VLAN”页面配置 VLAN，配置步骤为：

- 在 AC 1 上创建 VLAN 10。进入 VLAN 10 的详情页面，将与 Host A 相连的接口 GigabitEthernet1/0/6 加入 VLAN 10 的 Untagged 端口列表，将接口 GigabitEthernet1/0/3～GigabitEthernet1/0/5 加入 VLAN 10 的 Tagged 端口列表。
- AC 2 配置与 AC 1 相同。

3. 验证配置

完成上述配置后，在“链路聚合”页面中可以看到 GigabitEthernet1/0/3～GigabitEthernet1/0/5 已经加入到动态聚合组 1。Host A 能够 Ping 通 Host B。AC 1 与 AC 2 之间的一条链路故障后，Host A 仍然能够 Ping 通 Host B。

1.1.5 PPPoE Client配置举例

1. 组网需求

AC 作为 PPPoE 客户端通过 GigabitEthernet 1/0/1 连接到网络，要求：

- PPPoE 服务器与设备路由可达，GigabitEthernet 1/0/1 为三层物理口。
- PC 通过 Telnet 设备的 GE1/0/2 IP 连接到 Web 页面。

图1-5 PPPoE Client 组网图

2. 配置步骤

说明

- “链路空闲超时断线”中所设置的空闲时长为发报文空闲时长。
- 配置 PPPoE 客户端时需要勾选“删除该接口已存在的配置”选项，请根据实际情况选择合理三层物理接口。
- 完成 PPPoE 配置后请勿为该接口配置静态地址或者通过 DHCP 方式获取地址。

PPPoE 服务器为设备分配用户名和密码。（略）

配置 PPPoE 客户端。

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 接口”，进入“接口”页面后，点击上方“PPPoE 配置”页签，进入 PPPoE 配置页面。配置步骤为：

(1) 点击左侧  按钮，进入添加配置页面。

(2) 选择需配置的三层物理接口，组网中为 GigabitEthernet 1/0/1。

(3) 输入用户名和密码，并选择在线方式。

(4) 选择开启 NAT 地址转换功能和删除该接口已存在的地址配置，并点击<确定>按钮，完成配置。

3. 验证配置

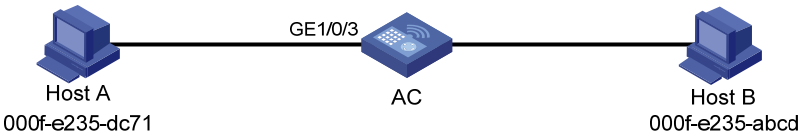
完成上述配置，可通过配置静态路由信息，并进行发送报文，查看流量信息进行验证。

1.1.6 MAC地址配置举例

1. 组网需求

- 现有一台用户主机 Host A，它的 MAC 地址为 000f-e235-dc71，属于 VLAN 1，连接 AC 的端口 GigabitEthernet1/0/3。为防止假冒身份的非法用户骗取数据，在设备的 MAC 地址表中为该用户主机添加一条静态表项。
- 另有一台用户主机 Host B，它的 MAC 地址为 000f-e235-abcd，属于 VLAN 1。由于该用户主机曾经接入网络进行非法操作，为了避免此种情况再次发生，在设备上添加一条黑洞 MAC 地址表项，使该用户主机接收不到报文。
- 配置设备的动态 MAC 地址表项老化时间为 500 秒。

图1-6 MAC 地址配置组网图



2. 配置步骤

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > VLAN”，进入“MAC”页面配置 MAC 地址，配置步骤为：

- 增加一条静态 MAC 地址表项，MAC 地址为 000f-e235-dc71，出接口为 GigabitEthernet1/0/3，且该接口属于 VLAN 1。
- 增加一条黑洞 MAC 地址表项，MAC 地址为 000f-e235-abcd，属于 VLAN 1。
- 进入配置页面，配置动态 MAC 地址表项的老化时间为 500 秒。

3. 验证配置

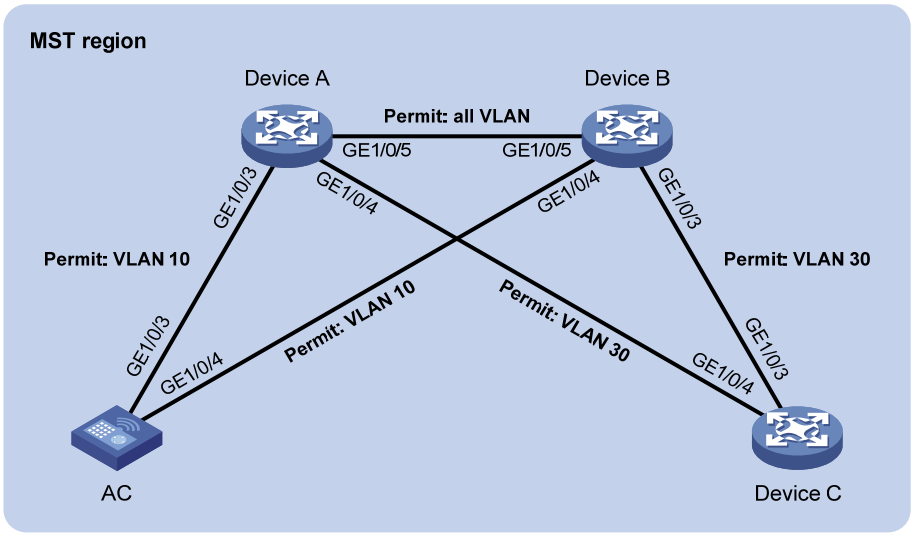
完成上述配置后，在“MAC 地址表”页面中可以看到已经创建的 MAC 地址表项，并且 Host B 无法 Ping 通 Host A。

1.1.7 MSTP配置举例

1. 组网需求

- 网络中所有设备都属于同一个 MST 域。Device A 和 Device B 为汇聚层设备，AC 和 Device C 为接入层设备。
- 通过配置 MSTP，使不同 VLAN 的报文按照不同的 MSTI 转发：VLAN 10 的报文沿 MSTI 1 转发，VLAN 30 沿 MSTI 2 转发。

图1-7 MSTP 配置组网图



2. 配置步骤

(1) 配置 VLAN

对于 AC 设备，单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > VLAN”，进入“VLAN”页面配置 VLAN。

- Device A 上的配置：
  - 创建 VLAN 10 和 VLAN 30。
  - 进入 VLAN 10 的详情页面，将接口 GigabitEthernet1/0/3 和 GigabitEthernet1/0/5 加入 VLAN 10 的 Tagged 端口列表。
  - 进入 VLAN 30 的详情页面，将接口 GigabitEthernet1/0/4 和 GigabitEthernet1/0/5 加入 VLAN 30 的 Tagged 端口列表。
- Device B 上的配置：
  - 创建 VLAN 10 和 VLAN 30。
  - 进入 VLAN 10 的详情页面，将接口 GigabitEthernet1/0/4 和 GigabitEthernet1/0/5 加入 VLAN 10 的 Tagged 端口列表。
  - 进入 VLAN 30 的详情页面，将接口 GigabitEthernet1/0/3 和 GigabitEthernet1/0/5 加入 VLAN 30 的 Tagged 端口列表。
- AC 上的配置：
  - 创建 VLAN 10。
  - 进入 VLAN 10 的详情页面，将接口 GigabitEthernet1/0/3 和 GigabitEthernet1/0/4 加入 VLAN 10 的 Tagged 端口列表。
- Device C 上的配置：
  - 创建 VLAN 30。
  - 进入 VLAN 30 的详情页面，将接口 GigabitEthernet1/0/3 和 GigabitEthernet1/0/4 加入 VLAN 30 的 Tagged 端口列表。

(2) 配置 MSTP

对于 AC 设备，单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > VLAN”，进入“STP”页面配置 MSTP，配置步骤为：

- Device A～Device C 和 AC 上开启 STP 功能，设置工作模式为 MSTP。
- Device A～Device C 和 AC 上，在域设置页面，配置 MST 域的域名为 Web，将 VLAN 10、30 分别映射到 MSTI 1、2 上，并配置 MSTP 的修订级别为 0。

3. 验证配置

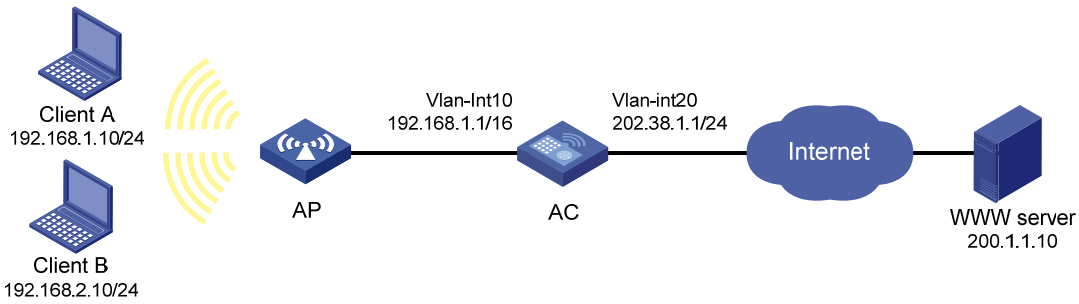
完成上述配置后，在生成树状态中可以看到各个接口的端口角色、端口状态等信息。

1.1.8 内网用户通过NAT地址访问外网（动态地址转换）

1. 组网需求

- 某公司内网使用的 IP 地址为 192.168.0.0/16。
- 该公司拥有 202.38.1.2 和 202.38.1.3 两个外网 IP 地址。
- 需要实现，内部网络中 192.168.1.0/24 网段的用户可以访问 Internet，其它网段的用户不能访问 Internet。使用的外网地址为 202.38.1.2 和 202.38.1.3。

图1-8 内网用户通过 NAT 访问外网



2. 配置步骤

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 服务 > NAT”，进入“NAT”页面，单击“动态转换”后进行配置，配置步骤为：

- 添加 NAT 动态转换规则，并指定 ACL 2000，该 ACL 仅允许源 IP 地址为 192.168.1.0、通配符掩码为 0.0.0.255 的网段的用户进行地址转换。
- 添加编号为 0 的 NAT 地址组，起始地址为 202.38.1.2，结束地址为 202.38.1.3。
- 在接口 Vlan-interface20 上应用上述的 NAT 动态转换规则。

3. 验证配置

以上配置完成后，Client A 能够访问 WWW server，Client B 无法访问 WWW server。

1.1.9 外网用户通过外网地址访问内网服务器

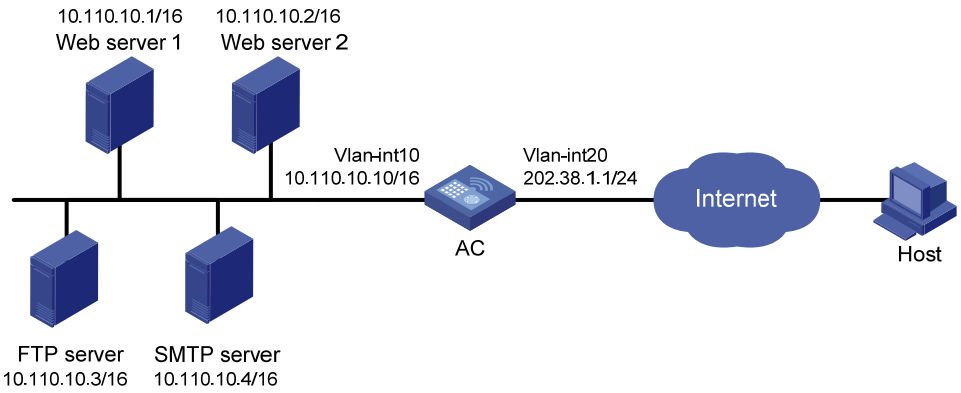
1. 组网需求

某公司内部对外提供 Web、FTP 和 SMTP 服务，而且提供两台 Web 服务器。公司内部网址为 10.110.0.0/16。其中，内部 FTP 服务器地址为 10.110.10.3/16，内部 Web 服务器 1 的 IP 地址为

10.110.10.1/16，内部 Web 服务器 2 的 IP 地址为 10.110.10.2/16，内部 SMTP 服务器 IP 地址为 10.110.10.4/16。公司拥有 202.38.1.1 至 202.38.1.3 三个公网 IP 地址。需要实现如下功能：

- 外部的主机可以访问内部的服务器。
- 选用 202.38.1.1 作为公司对外提供服务的 IP 地址，Web 服务器 2 对外采用 8080 端口。

图1-9 外网用户通过外网地址访问内网服务器



2. 配置步骤

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 服务 > NAT”，进入“NAT”页面，单击“内部服务器”后进行配置，配置步骤为：

- 选择接口 Vlan-interface20。
- 添加 NAT 内部 FTP 服务器，指定 IP 协议类型为 TCP，映射方式为“外网地址单一，未使用外网端口或外网端口单一”，外网 IP 地址为 202.38.1.1，端口号为 21；内部服务器 IP 地址为 10.110.10.3，端口号为 21。
- 添加 NAT 内部 Web 服务器 1，指定 IP 协议类型为 TCP，映射方式为“外网地址单一，未使用外网端口或外网端口单一”，外网 IP 地址为 202.38.1.1，端口号为 80；内部服务器 IP 地址为 10.110.10.1，端口号为 80。
- 添加 NAT 内部 Web 服务器 2，指定 IP 协议类型为 TCP，映射方式为“外网地址单一，未使用外网端口或外网端口单一”，外网 IP 地址为 202.38.1.1，端口号为 80；内部服务器 IP 地址为 10.110.10.2，端口号为 80。
- 添加 NAT 内部 SMTP 服务器，指定 IP 协议类型为 TCP，映射方式为“外网地址单一，未使用外网端口或外网端口单一”，外网 IP 地址为 202.38.1.1，端口号为 25；内部服务器 IP 地址为 10.110.10.4，端口号为 25。

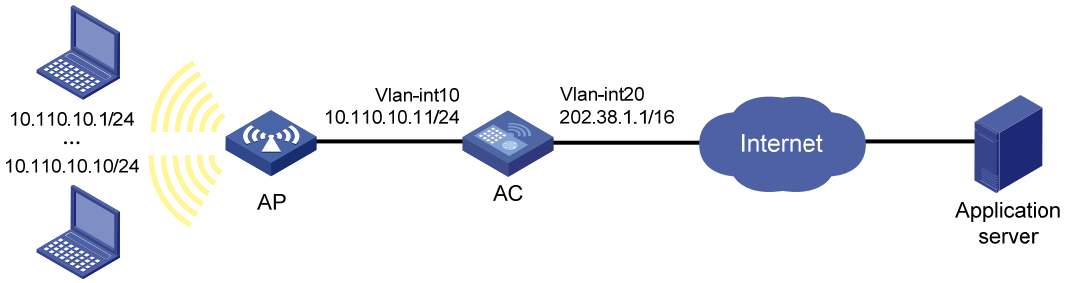
3. 验证配置

以上配置完成后，外网 Host 能够通过 NAT 地址访问各内网服务器。

1.1.10 NAT444 端口块静态映射配置举例

1. 组网需求

内部网络用户 10.110.10.1～10.110.10.10 使用外网地址 202.38.1.100 访问 Internet。内网用户地址基于 NAT444 端口块静态映射方式复用外网地址 202.38.1.100，外网地址的端口范围为 10001～15000，端口块大小为 500。



2. 配置步骤

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 服务 > NAT”，进入“NAT”页面，单击“NAT444 静态转换”后进行配置，配置步骤为：

- 添加 NAT444 端口块组 1，指定公网地址的端口块范围为 10001～15000，端口块大小为 500，私网地址成员的起始 IP 地址为 10.110.10.1，结束地址为 10.110.10.10；公网地址成员的起始 IP 地址为 202.38.1.100。
- 在接口 Vlan-interface20 上引用端口块组 1。

3. 验证配置

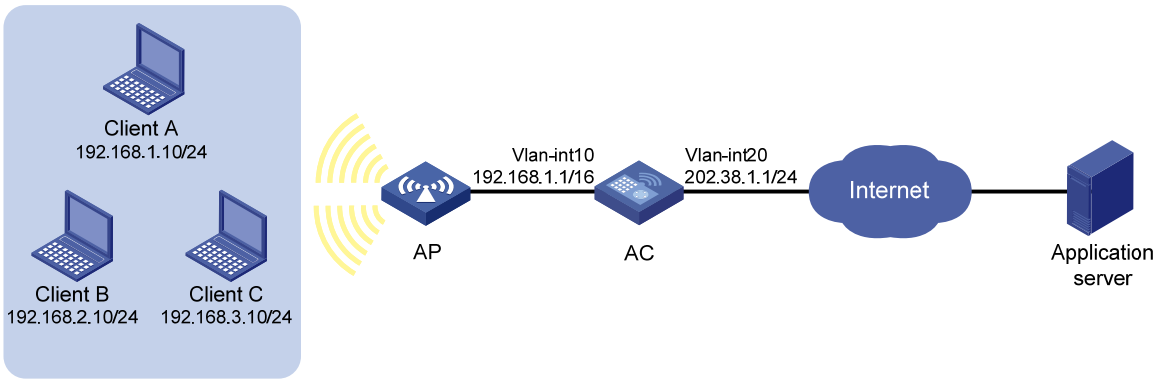
以上配置完成后，内网 Client 可以访问外网服务器。

1.1.11 NAT444 端口块动态映射配置举例

1. 组网需求

- 某公司内网使用的 IP 地址为 192.168.0.0/16。
- 该公司拥有 202.38.1.2 和 202.38.1.3 两个外网 IP 地址。

需要实现，内部网络中的 192.168.1.0/24 网段的用户可以访问 Internet，其它网段的用户不能访问 Internet。基于 NAT444 端口块动态映射方式复用两个外网地址 202.38.1.2 和 202.38.1.3，外网地址的端口范围为 1024～65535，端口块大小为 300。当为某用户分配的端口块资源耗尽时，再为其增量分配 1 个端口块。



2. 配置步骤

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 服务 > NAT”，进入“NAT”页面，单击“NAT444 动态转换”后进行配置，配置步骤为：

- 添加 NAT444 地址组 0，指定端口范围为 1024～65535，端口块大小为 300，增量端口块数为 1，地址组成员的起始 IP 地址为 202.38.1.2，结束地址为 202.38.1.3。
- 添加 IPv4 ACL 2000，该 ACL 仅允许源 IP 地址为 192.168.1.0、通配符掩码为 0.0.0.255 的网段的用户进行地址转换。
- 在接口 Vlan-interface20 上使用 NAT444 地址组 0 中的地址对匹配 ACL 2000 的报文进行源地址转换。

3. 验证配置

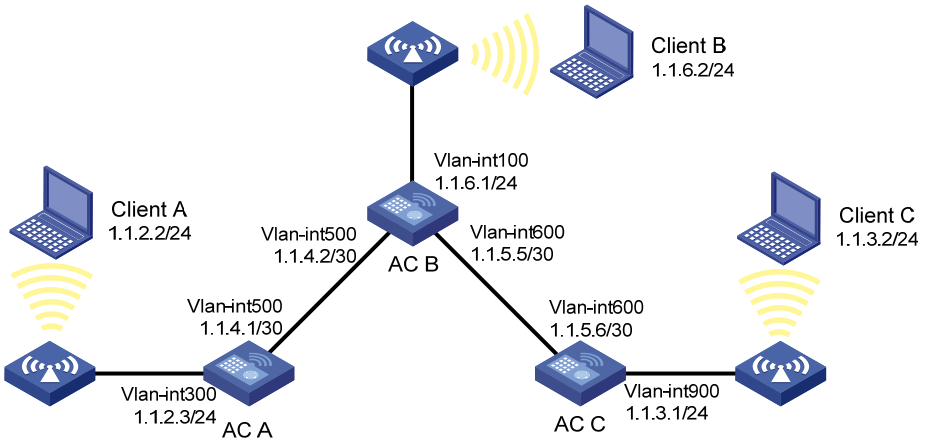
以上配置完成后，Client A 能够访问外网服务器，Client B 和 Client C 无法访问外网服务器。

1.1.12 IPv4 静态路由基本功能配置举例

1. 组网需求

AC各接口和无线客户端的IP地址和掩码如 图 1-9 所示。要求采用静态路由，使图中任意无线客户端之间都能互通。

图1-10 IPv4 静态路由配置组网图



2. 配置步骤

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 >路由”，进入“静态路由”页面配置 IPv4 静态路由，三台 AC 上的配置分别为：

- 在 AC A 上创建一条 IPv4 静态路由表项，指定目的 IP 地址为 0.0.0.0，掩码长度为 0，下一跳地址为 1.1.4.2，该路由用来匹配所有的目的 IP 地址。
- 在 AC B 上创建到达 Client A 所在网段和 Client C 所在网段的两条 IPv4 静态路由表项：
  - 到达 Client C 所在网段的路由：目的 IP 地址为 1.1.3.0，掩码长度为 24，下一跳地址为 1.1.5.6；
  - 到达 Client A 所在网段的路由：目的 IP 地址为 1.1.2.0，掩码长度为 24，下一跳地址为 1.1.4.1。
- 在 AC C 上创建一条 IPv4 静态路由表项，指定目的 IP 地址为 0.0.0.0、掩码长度为 0、下一跳地址为 1.1.5.5，该路由用来匹配所有的目的 IP 地址。

3. 验证配置

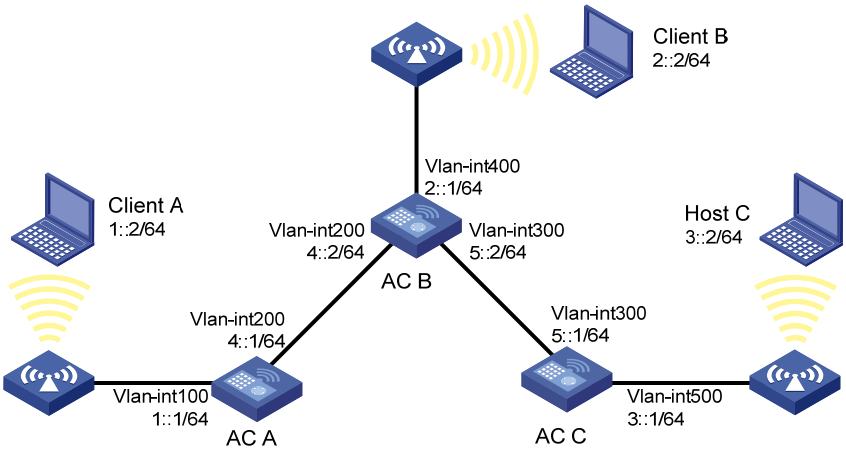
完成上述配置后，在任意一台无线客户端上都可以 ping 通另外两台无线客户端。

1.1.13 IPv6 静态路由基本功能配置举例

1. 组网需求

AC各接口和无线客户端的IPv6 地址和前缀长度如 图 1-10 所示。要求采用静态路由，使图中任意无线客户端之间都能互通。

图1-11 IPv6 静态路由配置组网图



2. 配置步骤

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 >路由”，进入“静态路由”页面配置 IPv6 静态路由，三台 AC 上的配置分别为：

- 在 AC A 上创建一条 IPv6 静态路由表项，指定目的 IPv6 地址为::，前缀长度为 0，下一跳地址为 4::2，该路由用来匹配所有的目的 IPv6 地址。
- 在 AC B 上创建到达 Client A 所在网段和 Client C 所在网段的两条 IPv6 静态路由表项：
  - 到达 Client C 所在网段的路由：目的 IPv6 地址为 3::2，前缀长度为 64，下一跳地址为 5::1；
  - 到达 Client A 所在网段的路由：目的 IPv6 地址为 1::2，前缀长度为 64，下一跳地址为 4::1。

- 在 AC C 上创建一条 IPv6 静态路由表项，指定目的 IPv6 地址为::，前缀长度为 0，下一跳地址为 5::2，该路由用来匹配所有的目的 IPv6 地址。

3. 验证配置

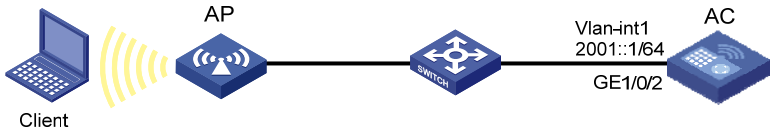
完成上述配置后，在任意一台无线客户端上都可以 ping 通另外两台无线客户端。

1.1.14 IPv6 地址静态配置举例

1. 组网需求

- 将 AP、AC 的以太网端口分别加入相应的 VLAN 里，在 VLAN 接口上配置 IPv6 地址，验证它们之间的互通性。
- AC 的 VLAN 接口 1 的全球单播地址为 2001::1/64。
- Client 上安装了 IPv6，根据 IPv6 邻居发现协议自动配置 IPv6 地址。

图1-12 IPv6 地址静态配置组网图



2. 配置步骤

(1) 配置 AC

配置 AC 基本功能（详细介绍请参见“WLAN 配置指导”中的“WLAN 接入”）（略）

(2) 配置 IPv6 地址

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 服务 > IP 服务”，进入“IPv6”页面配置 IPv6 地址，手工配置 VLAN1 接口地址为 2001::1，前缀长度为 64。

(3) 配置 VLAN 接口 1 允许发布 RA 消息

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 服务> ND”，进入“ND”页面，单击“高级设置 > 接口上的 RA 设置”，允许 VLAN 接口 1 发布 RA 消息。

(4) 配置 Client

Client 上安装 IPv6，根据 IPv6 邻居发现协议自动配置 IPv6 地址。

3. 验证配置

在 Client 上使用 Ping 测试和 AC 的互通性；在 AC 上使用 Ping 测试和 Client 的互通性。

1.1.15 DHCP服务器动态分配地址配置举例

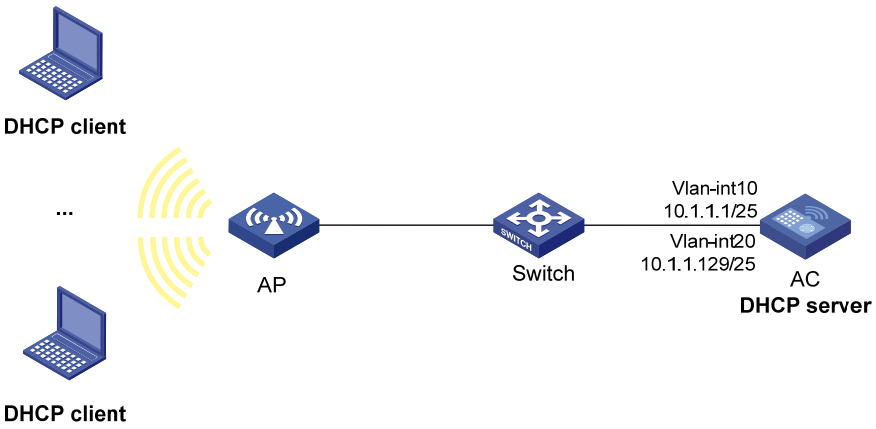
1. 组网需求

- 作为 DHCP 服务器的 AC 为网段 10.1.1.0/24 中的 AP 和客户端动态分配 IP 地址，该地址池网段分为两个子网网段：10.1.1.0/25 和 10.1.1.128/25；

- AC 的两个 VLAN 接口，VLAN 接口 10 和 VLAN 接口 20 的地址分别为 10.1.1.1/25 和 10.1.1.129/25；
- 为 AP 分配 10.1.1.0/25 网段的 IP 地址，为 DHCP client 分配 10.1.1.128/25 网段的 IP 地址。

2. 组网图

图1-13 DHCP 动态分配地址配置组网图



3. 配置步骤

在 AC 上创建 VLAN 10 和 VLAN 20，并配置 VLAN 接口 10 和 VLAN 接口 20 的地址。

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > VLAN”，进入“VLAN”页面创建 VLAN 并配置 VLAN 接口，配置步骤为：

- 创建 VLAN10，配置 VLAN 接口 10 的 IP 地址为 10.1.1.1/25。
- 创建 VLAN20，配置 VLAN 接口 20 的 IP 地址为 10.1.1.129/25。

配置 DHCP 服务器。

单击“系统”菜单页面左侧导航栏的“网络配置 > 服务 > DHCP/DNS”，进入“DHCP”页面配置 DHCP 服务器，配置步骤为：

- 开启 DHCP 服务。
- 配置 VLAN 接口 10 和 VLAN 接口 20 工作在 DHCP 服务器模式。
- 在地址池页面，创建名称为 pool1 的地址池，配置该地址池动态分配的地址段为 10.1.1.0/25，在地址池选项中配置网关地址为 10.1.1.1。
- 在地址池页面，创建名称为 pool2 的地址池，配置该地址池动态分配的地址段为 10.1.1.128/25，在地址池选项中配置网关地址为 10.1.1.129。
- 在高级设置页面，配置冲突地址检查功能中的发送回显请求报文的最大数目为 1，等待回显响应报文的超时时间为 500 毫秒。

配置无线服务。

单击“网络”菜单页面左侧导航栏的“无线配置 > 无线网络”，进入“无线网络”页面配置无线服务，配置步骤为：

- 创建一个无线服务，名称为 service。
- 配置 SSID 为 office。

- 配置缺省 VLAN 为 20。
- 开启无线服务。

配置 AP。

单击“网络”菜单页面左侧导航栏的“无线配置 > AP 管理”，进入“AP”页面配置 AP，配置步骤为：

- 添加一个 AP，配置 AP 名称为 AP 1，配置 AP 型号及序列号。
- 进入 AP 1 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 AP 1 的 5GHz 射频。

配置 AP 射频。

单击“网络”菜单页面左侧导航栏的“无线配置 > AP 管理”，进入“AP”页面配置 AP 1 的 5GHz 射频状态为开启。

4. 验证配置

配置完成后，10.1.1.0/25 和 10.1.1.128/25 网段的 AP 和客户端可以从 DHCP 服务器 AC 申请到相应网段的 IP 地址和网络配置参数。

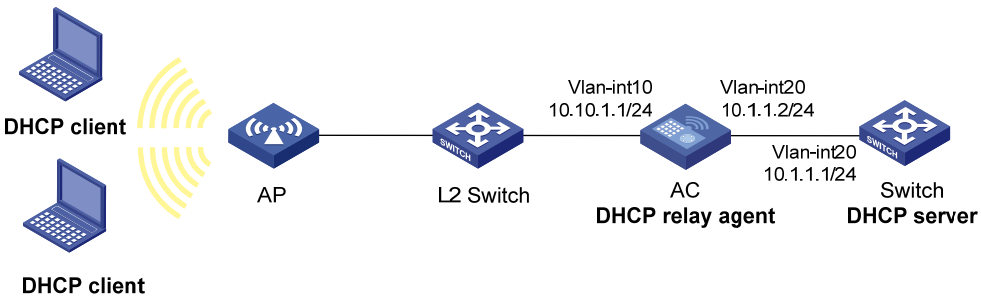
1.1.16 DHCP中继配置举例

1. 组网需求

- DHCP 客户端所在网段为 10.10.1.0/24，DHCP 服务器的 IP 地址为 10.1.1.1/24；
- 由于 DHCP 客户端和 DHCP 服务器不在同一网段，因此，需要在客户端所在网段设置 DHCP 中继设备，以便客户端可以从 DHCP 服务器申请到 10.10.1.0/24 网段的 IP 地址及相关配置信息；
- AC 作为 DHCP 中继通过端口（属于 VLAN10）连接到 DHCP 客户端所在的网络，VLAN 接口 10 的 IP 地址为 10.10.1.1/24，VLAN 接口 20 的 IP 地址为 10.1.1.2/24。

2. 组网图

图1-14 组网图



3. 配置步骤

配置各接口的 IP 地址。（略）

配置 DHCP 服务器。（略）

配置 AC 基本功能。（略）

配置 DHCP 中继。

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 服务 > DHCP/DNS”，进入“DHCP”页面配置 DHCP 中继，配置步骤为：

- 开启 DHCP 服务。
- 配置 VLAN 接口 10 为 DHCP 中继。
- 配置 DHCP 服务器 IP 地址为 10.1.1.1。

4. 验证配置

配置完成后，DHCP 客户端可以通过 DHCP 中继从 DHCP 服务器获取 IP 地址及相关配置信息。

1.1.17 DHCP Snooping配置举例

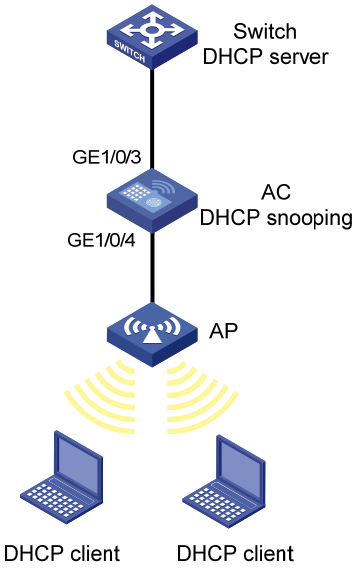
1. 组网需求

AC 通过以太网端口 GigabitEthernet 1/0/3 连接到 DHCP 服务器，通过以太网端口 GigabitEthernet 1/0/4 连接到 AP。要求：

- 与合法 DHCP 服务器相连的端口可以转发 DHCP 服务器的响应报文，而其他端口不转发 DHCP 服务器的响应报文。
- 记录 DHCP-REQUEST 报文和信任端口收到的 DHCP-ACK 报文中 DHCP 客户端 IP 地址及 MAC 地址的绑定信息。

2. 组网图

图1-15 DHCP Snooping 配置组网图



3. 配置步骤

配置 DHCP 服务器。（略）

配置 AC 基本功能。（略）

配置 DHCP Snooping。

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 服务 > DHCP/DNS”，进入“DHCP Snooping”页面配置 DHCP Snooping，配置步骤为：

- 开启 DHCP Snooping 功能。
- 设置 GigabitEthernet1/0/3 端口为信任端口。
- 在 GigabitEthernet1/0/4 上启用 DHCP Snooping 表项功能。

4. 验证配置

配置完成后，在 AC 上可查询到获取到的 DHCP Snooping 表项。

1.1.18 静态IPv4 DNS配置举例

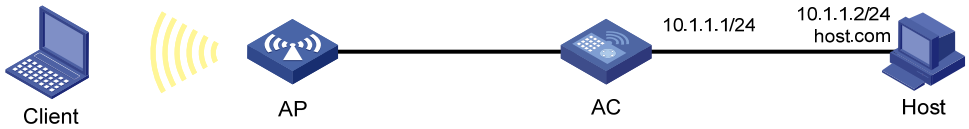
1. 组网需求

为了避免记忆复杂的 IP 地址，AC 希望通过便于记忆的主机名访问某一主机。在 AC 上手工配置 IP 地址对应的主机名，利用静态域名解析功能，就可以实现通过主机名访问该主机。

在本例中，AC 访问的主机 IP 地址为 10.1.1.2，主机名为 host.com。

2. 组网图

图1-16 静态 IPv4 DNS 配置举例组网图



3. 配置步骤

配置主机名 host.com 对应的 IP 地址为 10.1.1.2。

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 服务 > DHCP/DNS”，进入“IPv4 DNS”页面配置静态域名解析，配置步骤为：

配置静态域名解析：主机名为 host.com，对应的 IPv4 地址为 10.1.1.2。

4. 验证配置

在 AC 上执行 **ping host.com** 命令，可以解析到 host.com 对应的 IP 地址为 10.1.1.2，并能够 ping 通主机。

1.1.19 动态IPv4 DNS配置举例

1. 组网需求

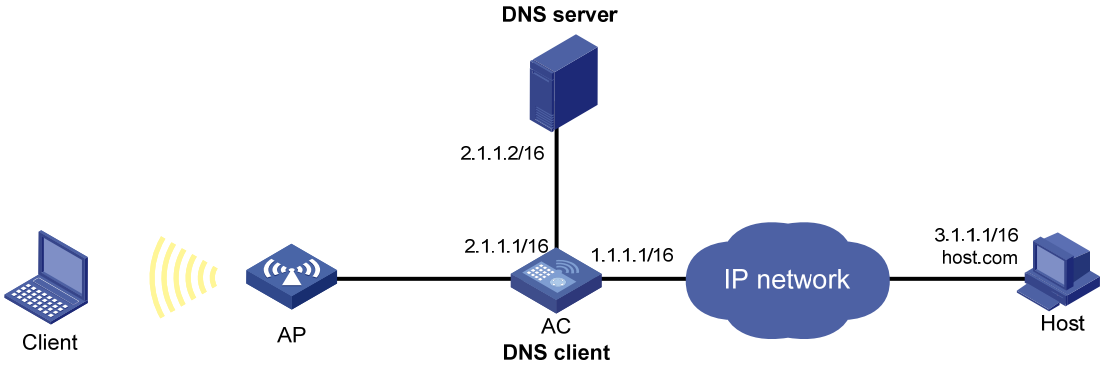
为了避免记忆复杂的 IP 地址，AC 希望通过便于记忆的域名访问某一主机。如果网络中存在域名服务器，则可以利用动态域名解析功能，实现通过域名访问主机。

在本例中：

- 域名服务器的 IP 地址是 2.1.1.2/16，域名服务器上包含域名“host”和 IP 地址 3.1.1.1/16 的对应关系。
- AC 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。
- AC 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。

2. 组网图

图1-17 动态 IPv4 DNS 配置举例组网图



3. 配置步骤

在 DNS 服务器上添加域名 host.com 和 IP 地址 3.1.1.1 的映射关系。（略）

在各设备上配置静态路由或动态路由协议，使得各设备之间路由可达。（略）

配置 DNS 客户端。

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 服务 > DHCP/DNS”，进入“IPv4 DNS”页面配置域名服务器，配置步骤为：

配置域名服务器地址为 2.1.1.2。在高级设置页面，配置域名后缀为 com。

4. 验证配置

完成上述配置后，在 AC 上执行 **ping host** 命令，可以解析到 host 对应的 IP 地址为 3.1.1.1，并能够 ping 通主机。

1.1.20 IPv4 DNS proxy配置举例

1. 组网需求

某局域网内拥有多台设备，每台设备上都指定了域名服务器的 IP 地址，以便直接通过域名访问外部网络。当域名服务器的 IP 地址发生变化时，网络管理员需要更改局域网内所有设备上配置的域名服务器 IP 地址，工作量将会非常巨大。

通过 DNS proxy 功能，可以大大减少网络管理员的工作量。当域名服务器 IP 地址改变时，只需更改 DNS proxy 上的配置，即可实现局域网内设备通过新的域名服务器解析域名。

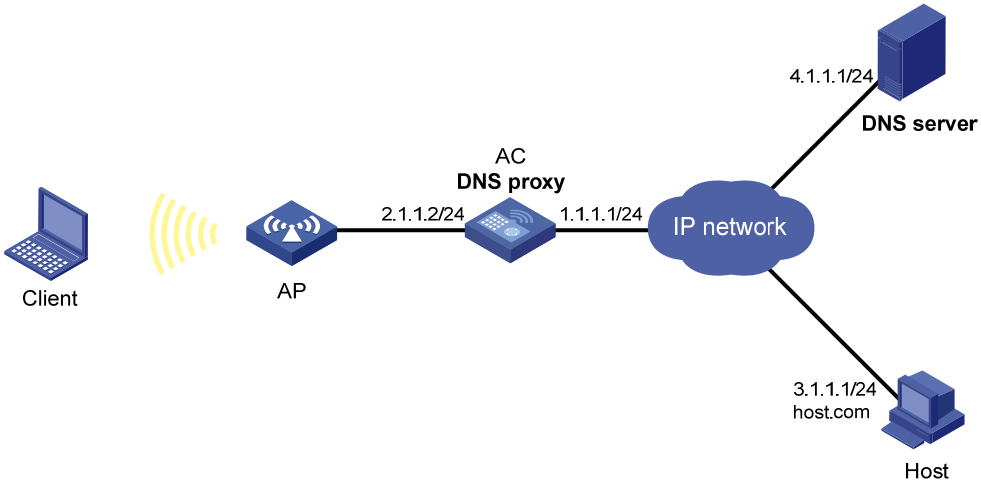
在本例中，具体配置步骤为：

(1) 局域网中的某台设备 AC 配置为 DNS proxy，DNS proxy 上指定域名服务器 IP 地址为真正的域名服务器的地址 4.1.1.1。

(2) 局域网中的其他设备上，域名服务器的 IP 地址配置为 DNS proxy 的地址，域名解析报文将通过 DNS proxy 转发给真正的域名服务器。

2. 组网图

图1-18 IPv4 DNS proxy 配置举例组网图



3. 配置步骤

在各设备上配置静态路由或动态路由协议，使得各设备之间路由可达。（略）

(1) 配置 DNS 服务器。（略）

(2) 配置 AC 作为 DNS proxy。

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 服务 > DHCP/DNS”，进入“IPv4 DNS”页面配置域名服务器，配置步骤为：

配置域名服务器的 IP 地址为 4.1.1.1。在高级设置页面，开启 DNS proxy 功能。

(3) 配置 DNS 客户端 Client，配置 DNS 服务器的 IP 地址为 2.1.1.2。

4. 验证配置

在 Client 上执行 **ping host.com** 命令，可以 ping 通主机，且对应的目的地址为 3.1.1.1。

1.1.21 静态IPv6 DNS配置举例

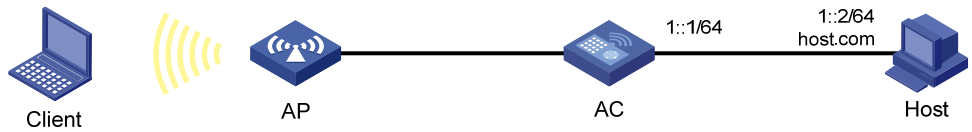
1. 组网需求

为了避免记忆复杂的 IPv6 地址，AC 希望通过便于记忆的主机名访问某一主机。在 AC 上手工配置 IPv6 地址对应的主机名，利用静态域名解析功能，就可以实现通过主机名访问该主机。

在本例中，AC 访问的主机 IP 地址为 1::2，主机名为 host.com。

2. 组网图

图1-19 静态 IPv6 DNS 配置举例组网图



3. 配置步骤

配置主机名 host.com 对应的 IPv6 地址为 1::2。

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 服务 > DHCP/DNS”，进入“IPv6 DNS”页面配置静态域名解析，配置步骤为：

配置静态域名解析：主机名为 host.com，对应的 IPv6 地址为 1::2。

4. 验证配置

在 AC 上执行 **ping ipv6 host.com** 命令，可以解析到 host.com 对应的 IPv6 地址为 1::2，并能够 ping 通主机。

1.1.22 动态IPv6 DNS配置举例

1. 组网需求

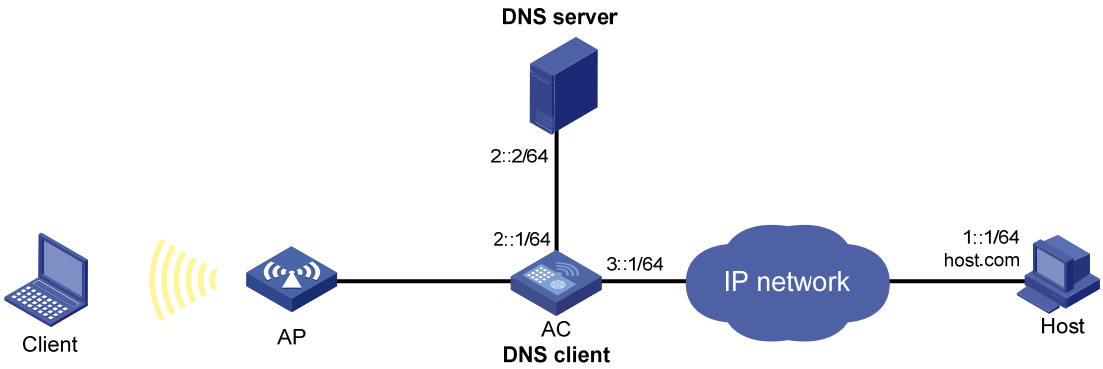
为了避免记忆复杂的 IPv6 地址，AC 希望通过便于记忆的域名访问某一主机。如果网络中存在域名服务器，则可以利用动态域名解析功能，实现通过域名访问主机。

在本例中：

- 域名服务器的 IPv6 地址是 2::2/64，域名服务器上包含域名“host”和 IPv6 地址 1::1/64 的对应关系。
- AC 作为 DNS 客户端，使用动态域名解析功能，将域名解析为 IPv6 地址。
- AC 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、IPv6 地址为 1::1/64 的主机 Host。

2. 组网图

图1-20 动态 IPv6 DNS 配置举例组网图



3. 配置步骤

在 DNS 服务器上添加域名 host.com 和 IPv6 地址 1::1 的映射关系。（略）

在各设备上配置静态路由或动态路由协议，使得各设备之间路由可达。（略）

配置 DNS 客户端。

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 服务 > DHCP/DNS”，进入“IPv6 DNS”页面配置域名服务器，配置步骤为：

配置域名服务器地址为 2::2。在高级设置页面，配置域名后缀为 com。

4. 验证配置

完成上述配置后，在 AC 上执行 **ping ipv6 host** 命令，可以解析到 host 对应的 IPv6 地址为 1::1，并能够 ping 通主机。

1.1.23 IPv6 DNS proxy配置举例

1. 组网需求

某局域网内拥有多台设备，每台设备上都指定了域名服务器的 IPv6 地址，以便直接通过域名访问外部网络。当域名服务器的 IPv6 地址发生变化时，网络管理员需要更改局域网内所有设备上配置的域名服务器 IPv6 地址，工作量将会非常巨大。

通过 DNS proxy 功能，可以大大减少网络管理员的工作量。当域名服务器 IPv6 地址改变时，只需更改 DNS proxy 上的配置，即可实现局域网内设备通过新的域名服务器解析域名。

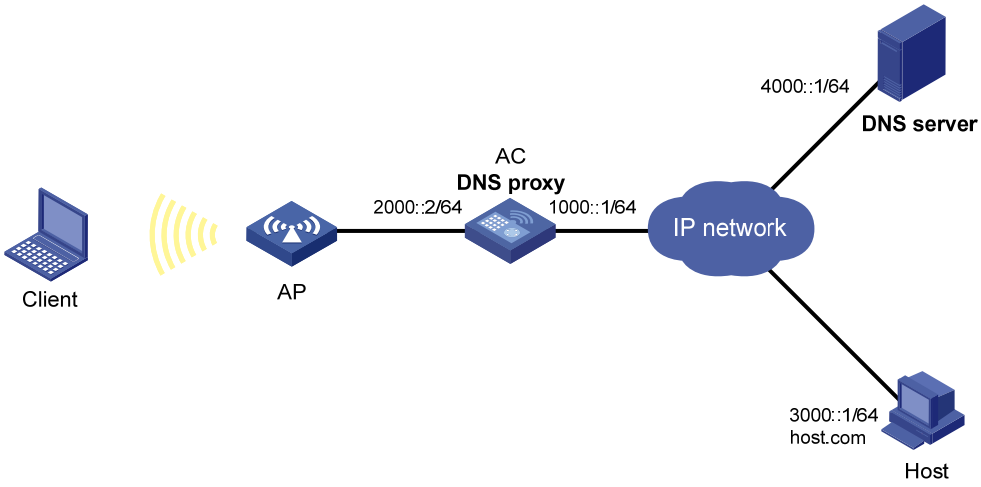
在本例中，具体配置步骤为：

(1) 局域网中的某台设备 AC 配置为 DNS proxy，DNS proxy 上指定域名服务器 IPv6 地址为真正的域名服务器的地址 4000::1

(2) 局域网中的其他设备上，域名服务器的 IPv6 地址配置为 DNS proxy 的地址，域名解析报文将通过 DNS proxy 转发给真正的域名服务器。

2. 组网图

图1-21 IPv6 DNS proxy 配置举例组网图



3. 配置步骤

在各设备上配置静态路由或动态路由协议，使得各设备之间路由可达。（略）

(1) 配置 DNS 服务器。（略）

(2) 配置 AC 作为 DNS proxy。

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 服务 > DHCP/DNS”，进入“IPv6 DNS”页面配置域名服务器，配置步骤为：

配置域名服务器的 IPv6 地址为 4000::1。在高级设置页面，开启 DNS proxy 功能。

(3) 配置 DNS 客户端 Client，配置 DNS 服务器的 IPv6 地址为 2000::2。

4. 验证配置

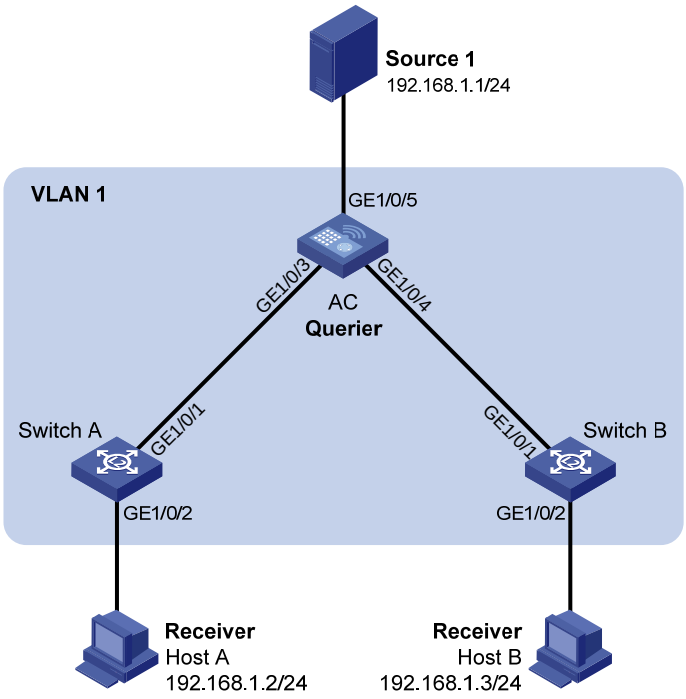
在 Client 上执行 **ping ipv6 host.com** 命令，可以 ping 通主机，且对应的目的地址为 3000::1。

1.1.24 IGMP Snooping配置举例

1. 组网需求

- 如下图所示，在一个没有三层网络设备的纯二层网络中，组播源 Source 1 向组播组 224.1.1.1 发送组播数据，Host A 和 Host B 都是该组播组的接收者，且都使用 IGMPv2。
- 由于该网络中没有可运行 IGMP 的三层网络设备，因此由 AC 来充当 IGMP 查询器，并将其发出的 IGMP 查询报文的源 IP 地址配置为非 0.0.0.0，以免影响 AC 和交换机上 IGMP snooping 转发表项的建立从而导致组播数据无法正常转发。
- 为防止 AC 和交换机在没有相应转发表项时将组播数据在 VLAN 内广播，在所有设备上都开启丢弃未知组播数据报文功能。

图1-22 IGMP Snooping 配置组网图



2. 配置步骤

(1) 配置 AC 作为 IGMP 查询器

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 服务> Multicast”，进入“IGMP Snooping”页面配置 IGMP Snooping，配置步骤为：

- 开启 IGMP Snooping 功能。
- 在 VLAN 1 内开启版本 2 的 IGMP snooping，并开启丢弃未知组播数据报文功能和充当 IGMP 查询器功能，然后将普遍组查询报文和特定组查询报文的源 IP 地址都配置为 192.168.1.10。

(2) 配置 Switch A 和 Switch B，在两台交换机的 VLAN 1 内开启版本 2 的 IGMP snooping，并开启丢弃未知组播数据报文功能。

3. 验证配置

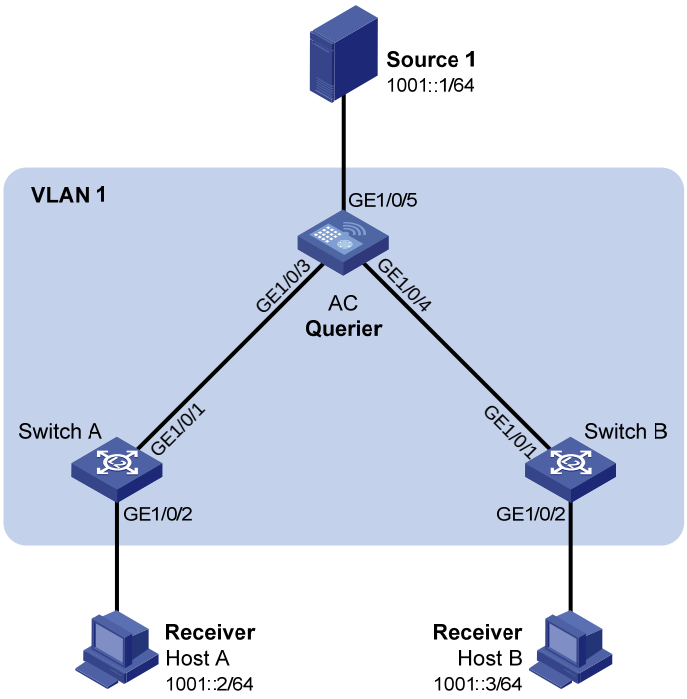
完成上述配置，并且接收者申请加入组播组 224.1.1.1 之后，在页面上可以看到该组播组对应的 IGMP snooping 转发表项。

1.1.25 MLD Snooping配置举例

1. 组网需求

- 如下图所示，在一个没有三层网络设备的纯二层网络中，组播源 Source 1 向 IPv6 组播组 FF1E::101 发送 IPv6 组播数据，Host A 和 Host B 都是该 IPv6 组播组的接收者，且都使用 MLDv1。
- 由于该网络中没有可运行 MLD 的三层网络设备，因此由 AC 来充当 MLD 查询器。
- 为防止 AC 和交换机在没有相应转发表项时将 IPv6 组播数据在 VLAN 内广播，在所有设备上都开启丢弃未知 IPv6 组播数据报文功能。

图1-23 MLD Snooping 配置组网图



2. 配置步骤

(1) 配置 AC 作为 MLD 查询器

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 服务> Multicast”，进入“MLD Snooping”页面配置 MLD Snooping，配置步骤为：

- 开启 MLD Snooping 功能。
- 在 VLAN 1 内开启版本 1 的 MLD snooping，并开启丢弃未知 IPv6 组播数据报文功能和充当 MLD 查询器功能。

(2) 配置 Switch A 和 Switch B，在两台交换机的 VLAN 1 内开启版本 1 的 MLD snooping，并开启丢弃未知 IPv6 组播数据报文功能。

3. 验证配置

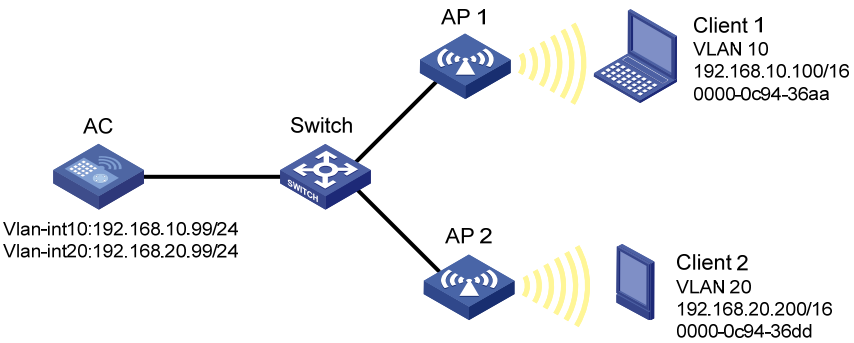
完成上述配置，并且接收者申请加入 IPv6 组播组 FF1E::101 之后，在页面上可以看到该 IPv6 组播组对应的 MLD snooping 转发表项。

1.1.26 代理ARP配置举例

1. 组网需求

- Client 1 和 Client 2 配置为同一网段的主机（Client 1 的 IP 地址是 192.168.10.100/16，Client 2 的 IP 地址是 192.168.20.200/16），但却被设备 AC 分在两个不同的子网（Client 1 属于 VLAN 10，Client 2 属于 VLAN 20）。
- Client 1 和 Client 2 没有配置缺省网关，要求在设备 AC 上开启代理 ARP 功能，使处在两个子网的 Client 1 和 Client 2 能互通。

图1-24 代理 ARP 配置组网图



2. 配置步骤

创建 VLAN 10 和 VLAN 20，并配置 VLAN 接口 10 和 VLAN 接口 20 的地址。

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > VLAN”，进入“VLAN”页面配置 VLAN，配置步骤为：

- 创建 VLAN 10，配置 VLAN 接口 10 的 IP 地址为 192.168.10.99/24。
- 创建 VLAN 20，配置 VLAN 接口 20 的 IP 地址为 192.168.20.99/24。

开启 VLAN 接口 10 和 VLAN 接口 20 的代理 ARP 功能。

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 服务 > ARP”，进入“ARP”页面，在“高级设置 > ARP 代理”页面开启 VLAN 接口 10 和 VLAN 接口 20 的代理 ARP 功能。

3. 验证配置

配置完成后，Client 1 和 Client 2 可以互相 ping 通。

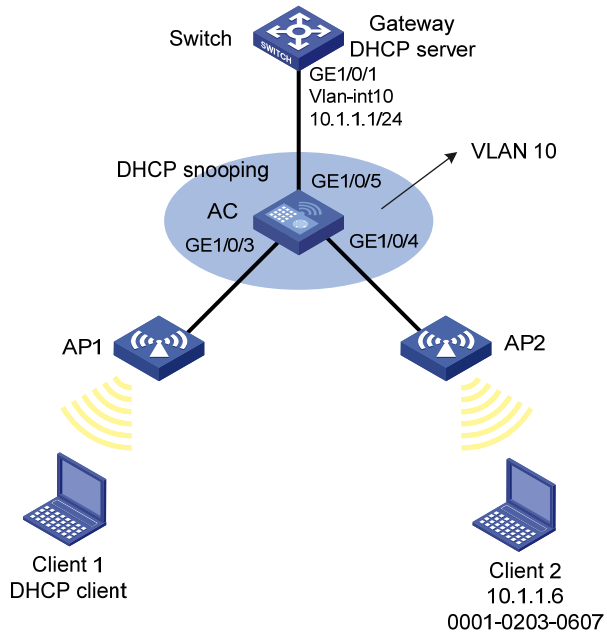
1.1.27 ARP攻击防御配置举例

1. 组网需求

- Switch 是 DHCP 服务器；

- Client 1 是 DHCP 客户端；用户 Client 2 的 IP 地址是 10.1.1.6，MAC 地址是 0001-0203-0607。
- AC 是 DHCP Snooping 设备，在 VLAN 10 内启用 ARP Detection 功能，对 DHCP 客户端和用户进行用户合法性检查和报文有效性检查。

图1-25 配置用户合法性检查和报文有效性检查组网图



2. 配置步骤

(1) 配置组网图中所有接口属于 VLAN 10 及 Switch 对应 VLAN 接口的 IP 地址（略）

(2) 配置 DHCP 服务器（略）

(3) 配置 DHCP 客户端 Client 1 和用户 Client 2（略）

(4) 配置 AC

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 服务 > DHCP/DNS”，进入“DHCP Snooping”页面，配置步骤为：

- 开启 DHCP Snooping 功能。
- 设置 GigabitEthernet1/0/5 端口为信任端口。
- 在 GigabitEthernet1/0/3 上启用 DHCP Snooping 表项记录功能。

单击“系统”菜单页面左侧导航栏的“网络配置 > 服务 > ARP”，进入“ARP”页面，在“高级设置 > ARP 攻击防御 > ARP Detection”页面开启 ARP Detection 功能，配置步骤为：

- 开启 VLAN10 的 ARP Detection 功能

接口状态缺省为非信任状态，上行接口配置为信任状态，下行接口按缺省配置。

- 在高级设置页面，设置接口 gigabitethernet 1/0/5 状态为信任状态
- 在高级设置页面，开启源 MAC 地址的检查、目的 MAC 地址的检查和 IP 地址的检查

完成上述配置后，对于接口 GigabitEthernet1/0/3 和 GigabitEthernet1/0/4 收到的 ARP 报文，先进行报文有效性检查，然后基于 DHCP Snooping 安全表项进行用户合法性检查。

3. 验证配置

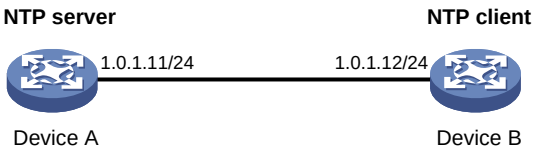
完成上述配置后，可在 AC 的“系统 > 网络配置 > 服务 > ARP”页面上看到 Client 1 的 ARP 表项，而无法看到 Client 2 的 ARP 表项。

1.1.28 NTP配置举例

1. 组网需求

- Device A 采用本地时钟作为参考时钟，使得自己的时钟处于同步状态。
- Device A 作为时间服务器为 Device B 提供时间同步。

图1-26 NTP 配置组网图



2. 配置步骤

(1) 配置 NTP 服务器 Device A

进入 Device A，单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 管理协议”，进入“NTP”页面配置 NTP 服务器，配置步骤为：

- 开启 NTP 服务。
- 配置本地时钟的 IP 地址为 127.127.1.0。
- 配置本地时钟所处的层数为 2。

(2) 配置 NTP 客户端 Device B

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“系统 > 管理”，进入“系统设置”页面配置系统时间，配置步骤为：

- 选择自动同步网络日期和时间，采用的协议为网络时间协议（NTP）。
- 指定 NTP 服务器（即时钟源）的 IP 地址为 1.0.1.11，并指定时钟源工作在服务器模式。

3. 验证配置

完成上述配置后，Device B 与 Device A 进行时间同步。此时 Device B 层数比 Device A 的层数大 1，为 3。

1.1.29 LLDP配置举例

1. 组网需求

通过在 AC 和 Switch 上配置 LLDP 功能，实现：

- AC 可以发现 Switch，并获取 Switch 的系统及配置等信息。
- Switch 不可以发现 AC。

图1-27 LLDP 配置组网图

2. 配置步骤

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 管理协议 > LLDP”，进入“LLDP”页面。两台设备上的配置分别为：

- 在 AC 上全局开启 LLDP 功能。进入接口状态页面，在接口 GigabitEthernet1/0/1 上开启 LLDP 功能。在接口设置页面，开启接口 GigabitEthernet1/0/1 的最近桥代理功能，并配置该接口的工作模式为 Rx：只接收 LLDP 报文，使得 AC 能够发现邻居。
- 在 Switch 上全局开启 LLDP 功能。进入接口状态页面，在接口 GigabitEthernet1/0/2 上开启 LLDP 功能。在接口设置页面，开启接口 GigabitEthernet1/0/2 的最近桥代理功能，并配置该接口的工作模式为 Tx：只发送 LLDP 报文，使得 Switch 不能够发现邻居。

3. 验证配置

完成上述配置后，在 AC 的 LLDP 邻居页面中可以看到 Switch 的信息，邻居关系建立；Switch 的 LLDP 邻居页面中没有邻居信息。

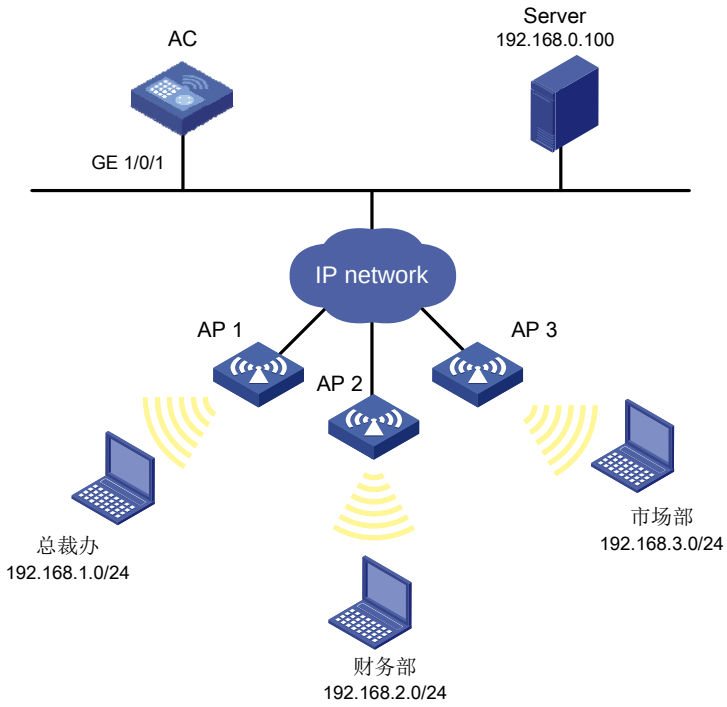
1.2 网络安全功能配置举例

1.2.1 通过ACL进行包过滤配置举例

1. 组网需求

某公司要求，允许总裁办在任意时间、财务部在工作时间（每周工作日的 8 点到 18 点）访问财务数据库服务器，禁止其它部门在任何时间、财务部在非工作时间访问该服务器。

图1-28 通过 ACL 进行包过滤配置组网图



2. 配置步骤

单击页面底部的<系统>按钮，然后单击左侧导航栏“网络安全 > 包过滤”，进入包过滤配置页面。配置步骤为：

- 创建接口包过滤策略，在 AC 的 VLAN 接口 10 的出方向上指定包过滤规则为 IPv4 ACL。
- 创建 IPv4 高级 ACL 3000，并按顺序制定三条规则：
  - 允许协议类型为 256（IP），源 IP 为 192.168.1.0、通配符掩码为 0.0.0.255，目的 IP 为 192.168.0.100、通配符掩码为 0 的报文通过。
  - 创建周期时间段 work，指定开始时间为 08：00，结束时间为 18：00，生效时间为每周一、周二、周三、周四和周五。允许协议类型为 256（IP），源 IP 为 192.168.2.0、通配符掩码为 0.0.0.255，目的 IP 为 192.168.0.100、通配符掩码为 0，生效时间段为 work 的报文通过。
  - 拒绝协议类型为 256（IP），目的 IP 为 192.168.0.100、通配符掩码为 0 的报文通过。
- 开启 ACL 规则的匹配统计功能。

3. 验证配置

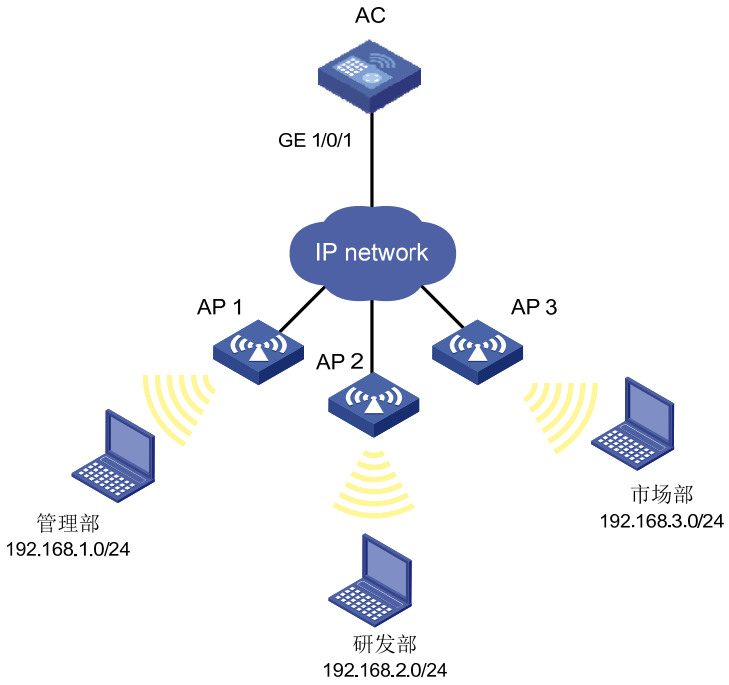
完成上述配置后，在页面上可以看到已经创建的 IPv4 高级 ACL 的规则状态和命中报文数。总裁办主机在任何时间都可以 ping 通财务数据库服务器；在工作时间财务部主机可以 ping 通该服务器；市场部在任何时间都不能 ping 通该服务器。

1.2.2 优先级映射配置举例

1. 组网需求

当三个部门访问 Internet 的流量发生拥塞时，要求按照依次发送管理部、市场部和研发部的流量。

图1-29 优先级映射配置组网图



2. 配置步骤

(1) 配置 QoS 策略

单击页面底部的<系统>按钮，然后单击左侧导航栏“网络安全 > 流策略”，进入 QoS 策略配置页面。在接口 GigabitEthernet1/0/2、GigabitEthernet1/0/3、GigabitEthernet1/0/4 的入方向上应用 QoS 策略后，修改应用的策略，创建如下三个 QoS 策略：

- 创建 IPv4 ACL 2001，添加一条允许源 IP 为 192.168.1.0、通配符掩码为 0.0.0.255 的报文通过的规则；定义匹配该 ACL 的类；指定流行为为重标记报文的 802.1p 优先级为 2。
- 创建 IPv4 ACL 2002，添加一条允许源 IP 为 192.168.2.0、通配符掩码为 0.0.0.255 的报文通过的规则；定义匹配该 ACL 的类；指定流行为为重标记报文的 802.1p 优先级为 0。
- 创建 IPv4 ACL 2003，添加一条允许源 IP 为 192.168.3.0、通配符掩码为 0.0.0.255 的报文通过的规则；定义匹配该 ACL 的类；指定流行为为重标记报文的 802.1p 优先级为 1。

(2) 配置优先级映射

完成上述配置后，单击页面上方的“优先级映射”，然后单击右上方的“端口优先级”，进入优先级映射配置页面。具体配置为：指定在接口 GigabitEthernet1/0/1、GigabitEthernet1/0/2、GigabitEthernet1/0/3、GigabitEthernet1/0/4 的优先级信任模式为信任 Dot1p 优先级。

单击<确定>后，返回优先级映射配置页面，然后单击右上方的“优先级映射表”，具体配置为：在 802.1p 优先级到本地优先级映射表中，输入值为 0、1、2 对应的输出值分别改为 0、1、2。

3. 验证配置

完成上述配置后，可以在 QoS 策略页面查看策略的应用状态。

1.3 系统功能配置举例

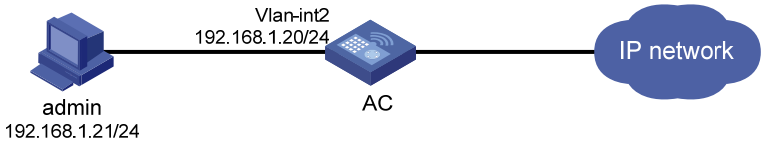
1.3.1 管理员配置举例

1. 组网需求

在 AC 上配置一个管理员帐户，用于用户采用 HTTP 方式登录 AC，具体要求如下：

- 用户使用管理员帐户登录时，AC 对其进行本地认证；
- 管理员帐户名称为 webuser，密码为 12345；
- 通过认证之后，用户被授予角色 network-admin。

图1-30 管理员配置组网图



2. 配置步骤

(1) 配置 VLAN 和 VLAN 接口

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > VLAN”，进入 VLAN 页面，创建 VLAN 2。进入 VLAN 2 的详情页面，将与管理员 PC 相连的接口加入 VLAN 2 的 Tagged 端口列表，并创建 VLAN 接口 2，配置 VLAN 接口 2 的 IP 地址为 192.168.1.20/24。

(2) 配置管理员账户

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“系统>管理员”，进入管理员页面，配置步骤为：

- 添加管理员。
- 配置用户名为 webuser，密码为 12345。
- 选择角色为 network-admin。
- 指定可用的服务为 HTTP 和 HTTPS。

3. 验证配置

(1) 完成上述配置后，在管理员页面上可以看到已成功添加的管理员帐户。

(2) 用户在 PC 的 Web 浏览器地址栏中输入 http://192.168.1.20 并回车后，浏览器将显示 Web 登录页面。用户在该登录页面中输入管理员帐户名称、密码以及验证码后，即可成功登录设备的 Web 页面进行相关配置。

2 网络功能配置举例

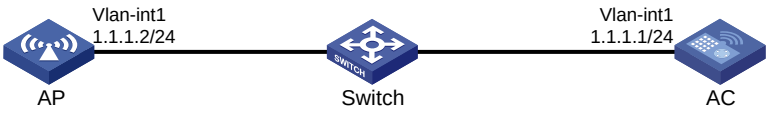
2.1 无线配置功能配置举例

2.1.1 配置通过DHCP发现方式建立CAPWAP隧道举例

1. 组网需求

如 图 2-1 所示，AP和AC通过交换机相连，AC作为DHCP服务器为AP提供DHCP服务。AP通过DHCP选项方式从DHCP服务器上获取AP和AC的IP地址，发现AC并与AC建立CAPWAP隧道连接。

图2-1 通过 DHCP 发现方式建立 CAPWAP 隧道典型组网图



2. 配置步骤

(1) 配置 AC 的 IP 地址

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > VLAN”，进入“VLAN”页面配置 VLAN 接口 1 的 IP 地址为 1.1.1.1/24。

(2) 配置 DHCP 服务

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 服务 > DHCP/DNS > DHCP”，进入“DHCP”页面配置 DHCP 服务，配置步骤为：

- 开启 DHCP 服务。
- 配置 VLAN 接口 1 工作在 DHCP 服务器模式。
- 进入“地址池 > 地址分配”页面，创建名称为 pool1 的地址池，配置该地址池动态分配的地址段为 1.1.1.0/24，在地址池选项中配置网关地址为 1.1.1.1。
- 进入“地址池 > 地址池选项”页面”，配置 DHCP 选项 43 为客户端分配 AC 的 IP 地址，选项内容为 800700000101010101。

(3) 配置 AP

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > AP管理 > AP”，进入“AP”页面配置 AP，配置步骤为：

- 配置 AP 名称为 AP1。
- 配置 AP 型号及序列号。

3. 验证配置

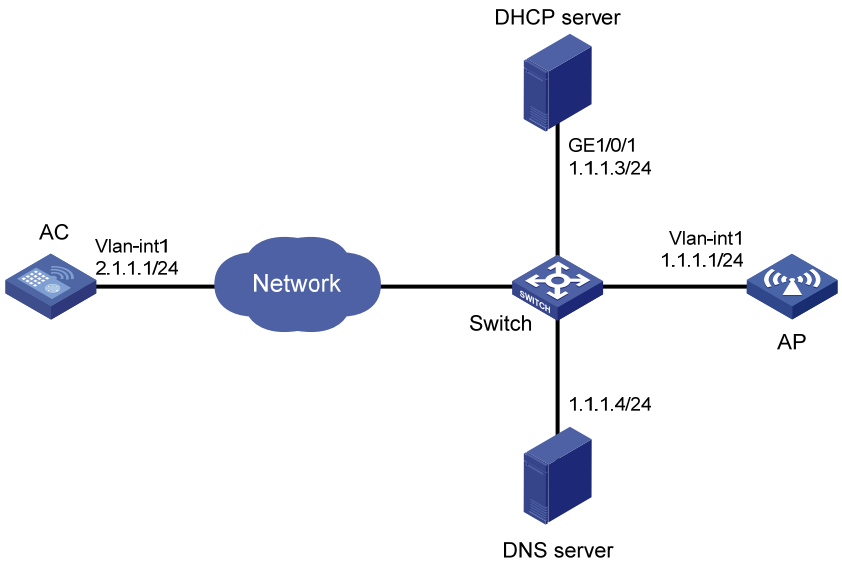
单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > AP管理 > AP”，进入“AP”页面可以查看到上线的 AP，通过查看详情可以看到 AP 获取到的 AP IP 地址、AC IP 地址和 AP 发现 AC 的方式。

2.1.2 配置通过DNS发现方式建立CAPWAP隧道举例

1. 组网需求

如 图 2-2 所示，DHCP server、DNS server、AP和AC通过交换机连接。由DHCP server为AP分配IP地址和AC的域名后缀，DNS server将AC的域名解析为AC的IP地址。

图2-2 通过 DNS 发现方式建立 CAPWAP 隧道典型组网图



2. 配置步骤

(1) 配置 DHCP server

在 DHCP server 上配置为 AP 分配 IP 地址和 AC 的域名后缀，分配的 IP 地址段为 1.1.1.0/24，AC 的域名后缀为 abc。（略）

(2) 配置 DNS server

在 DNS server 上添加 AC 域名和 AC IP 地址 1.1.1.1/24 的对应关系。（略）

(3) 配置 AC 的 IP 地址

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > VLAN”，进入“VLAN”页面配置 VLAN 接口 1 的 IP 地址为 1.1.1.1/24。

(4) 配置 AP

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > AP 管理 > AP”，进入“AP”页面配置 AP，配置步骤为：

- 配置 AP 名称为 AP1。
- 配置 AP 型号及序列号。

3. 验证配置

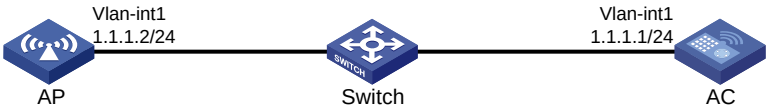
单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > AP 管理 > AP”，进入“AP”页面可以查看到上线的 AP，通过查看上线 AP 的详细信息可以看到 AP 获取到的 AP IP 地址、AC IP 地址和 AP 发现 AC 的方式。

2.1.3 配置开启自动AP功能建立CAPWAP隧道举例

1. 组网需求

如 图 2-3 所示，AP和AC通过交换机相连。在AC上开启自动AP功能，MAC地址为 0011-2200-0101 的AP通过DHCP选项方式获取到AC的IP地址，AP通过获取到的AC的IP地址发现AC并与AC建立CAPWAP隧道连接。

图2-3 开启自动 AP 功能建立 CAPWAP 隧道典型组网图



2. 配置步骤

(1) 配置 AC 的 IP 地址

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > VLAN”，进入“VLAN”页面配置 VLAN 接口 1 的 IP 地址为 1.1.1.1/24。

(2) 配置 DHCP 服务

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 服务 > DHCP/DNS > DHCP”，进入“DHCP”页面配置 DHCP 服务，配置步骤为：

- 开启 DHCP 服务。
- 配置 VLAN 接口 1 工作在 DHCP 服务器模式。
- 进入“地址池 > 地址分配”页面，创建名称为 pool1 的地址池，配置该地址池动态分配的地址段为 1.1.1.0/24，在地址池选项中配置网关地址为 1.1.1.1。
- 进入“地址池 > 地址池选项”页面”，配置 DHCP 选项 43 为客户端分配 AC 的 IP 地址，选项内容为 800700000101010101。

(3) 配置 AP

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > AP 管理 > AP 全局配置”，进入“AP 全局配置”页面开启自动 AP 功能。

3. 验证配置

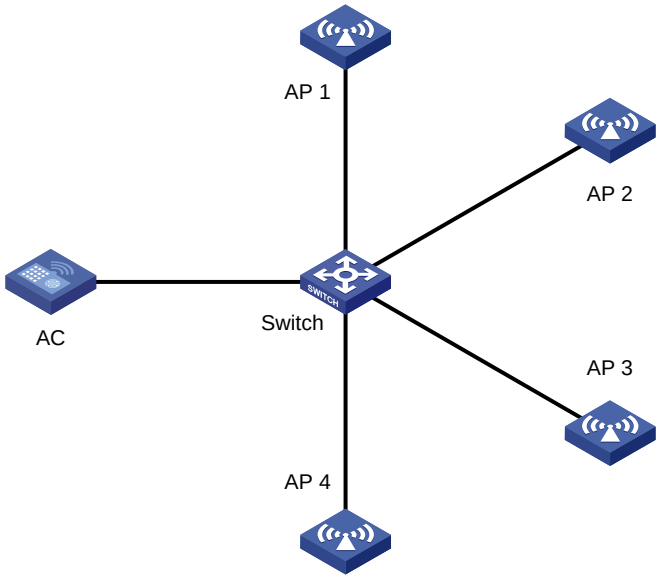
单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > AP 管理 > AP”，进入“AP”页面可以查看到上线的自动 AP。

2.1.4 AP组配置举例

1. 组网需求

如 图 2-4 所示，AC通过交换机和AP 1、AP 2、AP 3、AP 4 相连；将AP1 加入group1，AP 2、AP 3 和AP 4 加入group2。AP 1、AP 2、AP 3 和AP4 名字分别为ap1、ap2、ap3 和ap4。

图2-4 AP 组配置举例



2. 配置步骤

(1) 配置 AP 通过 DHCP 方式获取 AP IP 地址及 AC IP 地址（略）。

(2) 配置 AP 组

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > AP 管理 > AP 组”，进入“AP 组”页面，配置步骤为：

- 添加两个 AP 组，配置 AP 组名称为 group1 和 group2。
- 选中 AP 组，配置 AP 组 group1 的入组规则，创建 AP 名称入组规则，匹配数据为 ap1。
- 选中 AP 组，配置 AP 组 group2 的入组规则，创建 AP 名称入组规则，匹配数据为 ap2、ap3 和 ap4。

3. 验证配置

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > AP 管理 > AP 组”，进入“AP 组”页面，选中 AP 组，查看 AP 组 group1 和 group2 的 AP 列表，可以看到 ap1 加入到 AP 组 group1 中，ap2、ap3 和 ap4 加入到 AP 组 group2 中。

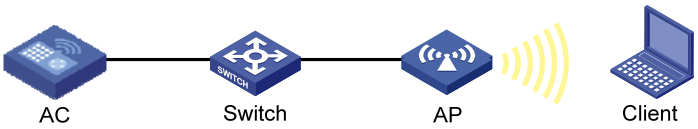
2.1.5 射频管理配置举例

1. 组网需求

如 图 2-5 所示，AP通过交换机与AC相连。对AP上的 5GHz射频进行配置，配置要求如下：

- 配置射频模式为 802.11ac，工作信道为 48，最大功率为 19dBm。
- 配置 802.11ac 的最大基本 NSS 为 2，最大支持 NSS 为 3，组播 NSS 为 2，VHT-MCS 索引值为 5。
- 配置 A-MPDU 功能、A-MSDU 功能来提高 AP 的吞吐量。

图2-5 射频管理基本功能配置组网图



2. 配置步骤

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > 射频资源 > 射频管理”，进入“射频管理”页面，配置步骤为：

- 在“AP 组内所有 AP 的射频”中选择对应名称 AP 的 5GHz 射频进行编辑，在“基础”页面，配置射频模式为 802.11ac（5GHz），工作信道为 48，最大功率为 19dBm。
- 配置 802.11ac 的最大基本 NSS 为 2，最大支持 NSS 为 3，组播 NSS 为 2，组播 VHT-MCS 为 5。
- 开启 A-MPDU 和 A-MSDU 功能。
- 开启射频。

3. 验证配置

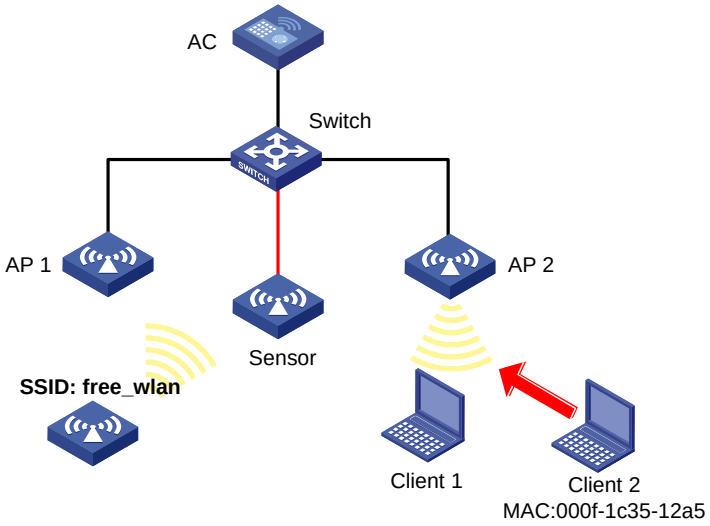
在 AP 节点导航栏中指定 AP 组下对应名称的 AP，单击页面左侧导航栏的“无线配置 > 射频管理”，进入“射频管理”页面，在“AP 组内所有 AP 的射频”中选择对应名称 AP 的 5GHz 射频，单击<编辑>按钮，可以查看 5GHz 射频上当前的配置。

2.1.6 WIPS分类与反制配置举例

1. 组网需求

如 图 2-6 所示，AP通过交换机与AC相连，AP 1 和AP 2 为Client提供无线服务，SSID为“abc”，在Sensor上开启WIPS功能，配置分类策略，将非法客户端的MAC地址（000f-1c35-12a5）添加到静态禁用列表中，将SSID“abc”添加到静态信任列表中，要求对检测到的潜在外部AP和非授权客户端进行反制。

图2-6 WIPS 分类与反制组网图



2. 配置步骤

(1) 配置手工 AP。

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > AP 管理”，进入“AP 管理”页面，配置步骤为：

- 创建 AP 名称为 Sensor。
- 配置 AP 的型号、序列号。

(2) 配置 WIPS 功能。

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > 无线安全”，进入“无线安全”页面，配置步骤为：

- 在配置虚拟安全域的框里单击右上角的“+”：创建虚拟安全域 VSD_1。
- 单击开启 WIPS，编辑名称为 Sensor 的 AP，选择开启 WIPS 的射频接口，并加入虚拟安全域 VSD_1 中。
- 单击分类策略，创建分类策略 class1，将 Client 2 的 MAC 地址配置为禁用 MAC 地址，将 SSID abc 添加到信任 SSID 中。
- 单击反制策略，创建反制策略 protect，反制未授权客户端和潜在外部 AP。
- 编辑虚拟安全域 VSD_1，应用分类策略 class1 和反制策略 protect。

3. 验证配置

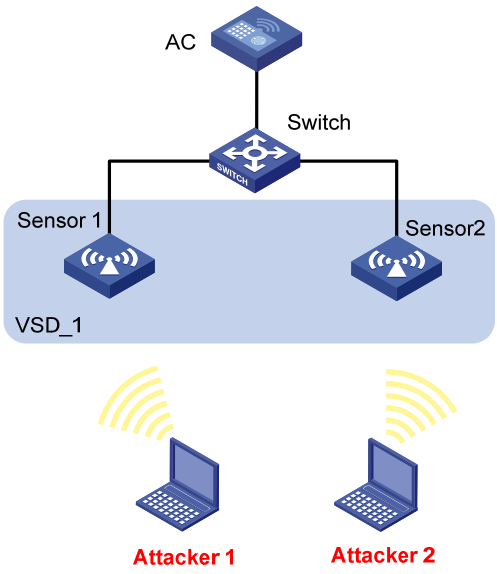
- 单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“监控 > 无线安全”，进入“无线安全”页面，在设备信息页面中可以查看无线设备的分类结果，在虚拟安全域 VSD_1，MAC 地址为 000f-e223-1616 的 AP 被分类成潜在外部 AP，MAC 地址为 000f-1c35-12a5 的客户端被分类为未授权的客户端。
- 单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“监控 > 无线安全”，进入“无线安全”页面，在反制记录页面中可以查看反制过的设备记录信息，在虚拟安全域 VSD_1，MAC 地址为 000f-1c35-12a5 的未授权客户端和 MAC 地址为 000f-e223-1616 的潜在外部 AP 被反制。

2.1.7 WIPS畸形报文检测和泛洪攻击检测配置举例

1. 组网需求

如 图 2-7 所示，AP通过交换机与AC相连，将两台AP分别配置为Sensor，配置虚拟安全域VSD_1，并配置两台Sensor属于这个虚拟安全域，当检测到攻击者对无线网络进行IE重复的畸形报文或Beacon帧泛洪攻击时，AP向AC发送告警信息。

图2-7 畸形报文检测和泛洪攻击检测组网图



2. 配置步骤

(1) 配置手工 AP。

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > AP 管理”，进入“AP 管理”页面，配置步骤为：

- 创建 AP 名称为 Sensor 1 和 Sensor 2。
- 配置 AP 的型号、序列号。

(2) 配置 WIPS 功能。

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > 无线安全”，进入“无线安全”页面，配置步骤为：

- 在配置虚拟安全域的框里单击右上角的“+”：创建虚拟安全域 VSD_1。
- 单击开启 WIPS，编辑名称为 Sensor 1 和 Sensor 2 的 AP，选择开启 WIPS 的射频接口，并加入虚拟安全域 VSD_1。
- 单击攻击检测策略，创建攻击检测策略，配置当检测到 IE 重复的畸形报文和 Beacon 帧泛洪攻击时，向 AC 发送日志信息或告警信息。检测 IE 重复的畸形报文的静默时间为 50 秒，检测 Beacon 帧的统计周期为 100 秒，触发阈值为 200，静默时间为 50 秒。
- 编辑虚拟安全域 VSD_1，应用攻击检测策略。

3. 验证配置

- 单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“监控 > 无线安全”，进入“无线安全”页面，当网络中没有攻击者时，查看攻击统计信息，畸形报文和泛洪报文的统计个数为 0。
- 单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“监控 > 无线安全”，进入“无线安全”页面，当检测到 IE 重复的畸形报文和 Beacon 帧泛洪攻击时，查看攻击统计信息，可以查看到 IE 重复的畸形报文和 Beacon 帧泛洪攻击的统计个数。

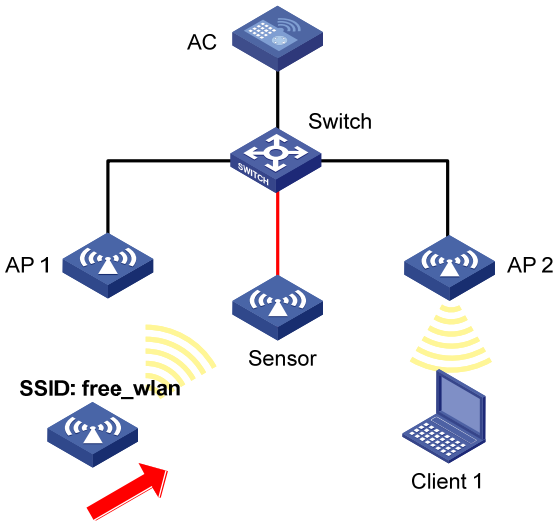
2.1.8 Signature检测配置举例

1. 组网需求

如 图 2-8 所示，AP通过交换机与AC相连，AP1 和AP2 为Client提供无线服务，SSID为“abc”，在Sensor上开启WIPS功能，配置Signature检测，检测无线环境中是否存在其他的无线服务，对SSID不是abc的Beacon帧进行检测， Sensor向AC发送告警信息。

2. 组网图

图2-8 WIPS 的攻击检测组网图



3. 配置步骤

(1) 配置手工 AP。

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > AP 管理”，进入“AP 管理”页面，配置步骤为：

- 创建 AP 名称为 Sensor。
- 配置 AP 的型号、序列号。

(2) 配置 WIPS 功能。

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > 无线安全”，进入“无线安全”页面，配置步骤为：

- 在配置虚拟安全域的框里单击右上角的“+”：创建虚拟安全域 vsd1。

- 单击开启 WIPS，编辑名称为 Sensor 的 AP，选择开启 WIPS 的射频接口，并加入虚拟安全域 vsd1 中。
- 单击 Signature 规则，创建 Signature 规则 1，配置子规则对 SSID 不是 abc 的 Beacon 帧进行检测。
- 单击 Signature 策略，创建 Signature 策略 sig1，应用 Signature 规则 1，配置统计周期为 5 秒，发出告警后的静默时间为 60 秒，统计次数的阈值为 60。
- 编辑虚拟安全域 vsd1，应用 Signature 策略。

4. 验证配置

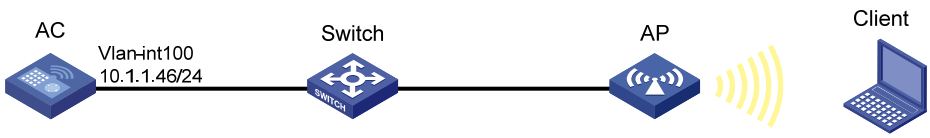
当检测到 SSID 为“free_wlan”的无线服务后，AC 会收到 Sensor 发送的告警信息。

2.1.9 共享密钥认证配置举例

1. 组网需求

AC 旁挂在 Switch 上，Switch 同时作为 DHCP server 为 AP 和 Client 分配 IP 地址。通过配置客户端在链路层使用 WEP 密钥 12345 接入无线网络。

图2-9 共享密钥认证配置组网图



2. 配置步骤

(1) 配置无线服务

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 无线网络”，进入“无线网络”页面，配置步骤为：

- 创建一个无线服务，名称为 service1。
- 配置 SSID 为 service。
- 开启无线服务。

(2) 配置认证模式为静态 WEP 密钥

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 无线网络”，在“无线网络”页面单击 service1 的编辑按钮，进入“链路层认证”页面，配置步骤为：

- 选择认证模式为静态 WEP 密钥。
- 选择密钥类型为 Passphrase
- 选择加密套件为 WEP40。
- 配置明文密钥为 12345。

(3) 将无线服务绑定到 AP

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 无线网络”，进入“无线网络”页面，配置步骤为：

- 选中创建的无线服务 service1，单击“绑定到 AP”按钮，进入到“绑定到 AP”页面。

- 选中 AP 的 5GHz 射频单元，单击“快速绑定”。

(4) 验证配置

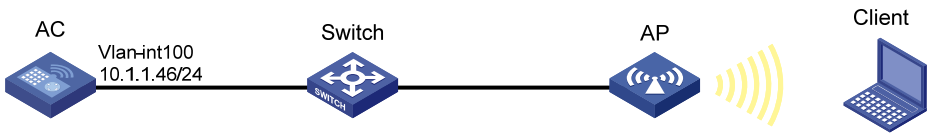
配置完成后，查看无线服务详情，可以看到已经创建的名称为 service1 无线服务以及配置的认证信息。

2.1.10 PSK身份认证与密钥管理模式和Bypass认证配置举例

1. 组网需求

- AC 旁挂在 Switch 上，Switch 同时作为 DHCP server 为 AP 和 Client 分配 IP 地址。通过配置客户端 PSK 密钥 12345678 接入无线网络。
- 客户端链路层认证使用开放式系统认证，用户接入认证使用 Bypass 认证的方式实现客户端可以不需要认证直接接入 WLAN 网络的目的。
- 通过配置客户端和 AP 之间的数据报文采用 PSK 身份认证与密钥管理模式来确保用户数据的传输安全。

图2-10 PSK+Bypass 认证配置组网图



2. 配置步骤

(1) 创建无线服务

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 无线网络”，进入“无线网络”页面，配置步骤为：

- 创建无线服务，名称为 service1。
- 配置 SSID 为 service。
- 开启无线服务。

(2) 配置认证模式为静态 PSK 密钥

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 无线网络”，在“无线网络”页面单击 service1 的编辑按钮，进入“链路层认证”页面，配置步骤为：

- 选择认证模式为静态 PSK 密钥。
- 选择安全模式为 WPA。
- 选择加密套件为 CCMP。
- 选择密钥类型为 Passphrase，明文密钥为 12345678。

(3) 将无线服务绑定到 AP

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 无线网络”，进入“无线网络”页面，配置步骤为：

- 选中创建的无线服务 service1，单击“绑定到 AP”按钮，进入到“绑定到 AP”页面。
- 选中 AP 的 5GHz 射频单元，单击“快速绑定”。

3. 验证配置

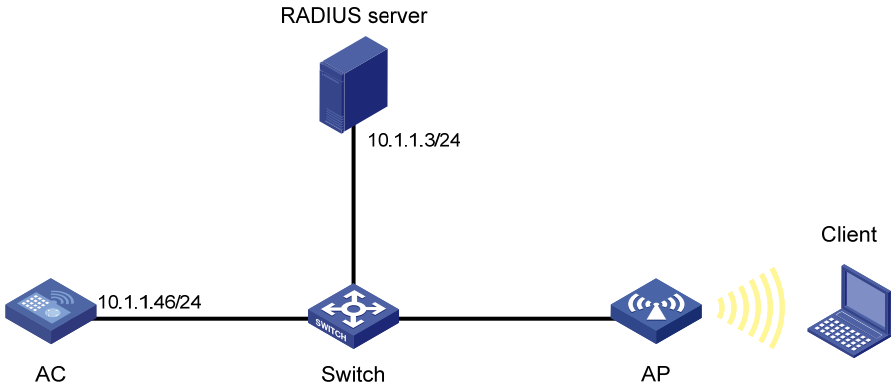
配置完成后，查看无线服务详情，可以看到已经创建的名称为 service1 无线服务以及配置的认证信息。

2.1.11 PSK身份认证与密钥管理模式和MAC地址认证配置举例

1. 组网需求

- AC 旁挂在 Switch 上，Switch 同时作为 DHCP server 为 AP 和 Client 分配 IP 地址。通过配置客户端 PSK 密钥 12345678 接入无线网络。
- 客户端链路层认证使用开放式系统认证，客户端通过 RADIUS 服务器进行 MAC 地址认证。
- 通过配置客户端和 AP 之间的数据报文采用 PSK 认证密钥管理模式来确保用户数据的传输安全。

图2-11 PSK 密钥管理模式和 MAC 认证配置组网图



2. 配置步骤

说明

- 在 RADIUS 服务器上配置，将 Client 的 MAC 地址作为认证的用户名和密码，且该 MAC 地址在配置时不能出现大写和连字符。完成 RADIUS 服务器的其它配置，并保证用户的认证/授权/计费功能正常运行。
- 完成设备上 RADIUS 和 Domain 域的配置。

(1) 配置无线服务

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 无线网络”，进入“无线网络”页面，配置步骤为：

- 创建一个无线服务，名称为 service1。
- 配置 SSID 为 service。
- 开启无线服务。

(2) 配置认证模式为静态 PSK 密钥和 MAC 地址认证

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 无线网络”，在“无线网络”页面单击 service1 的编辑按钮，进入“链路层认证”页面，配置步骤为：

- 选择认证模式为静态 PSK 密钥和 MAC 地址认证。
- 选择安全模式为 WPA。
- 选择加密套件为 CCMP。
- 选择密钥类型为 Passphrase，明文密钥为 12345678。
- 配置域名为 dom1。

(3) 将无线服务绑定到 AP

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 无线网络”，进入“无线网络”页面，配置步骤为：

- 选中创建的无线服务 service1，单击“绑定到 AP”按钮，进入到“绑定到 AP”页面。
- 选中 AP 的 5GHz 射频单元，单击“快速绑定”。

(4) 验证配置

配置完成后，查看无线服务详情，可以看到已经创建的名称为 service1 无线服务以及配置的认证信息。

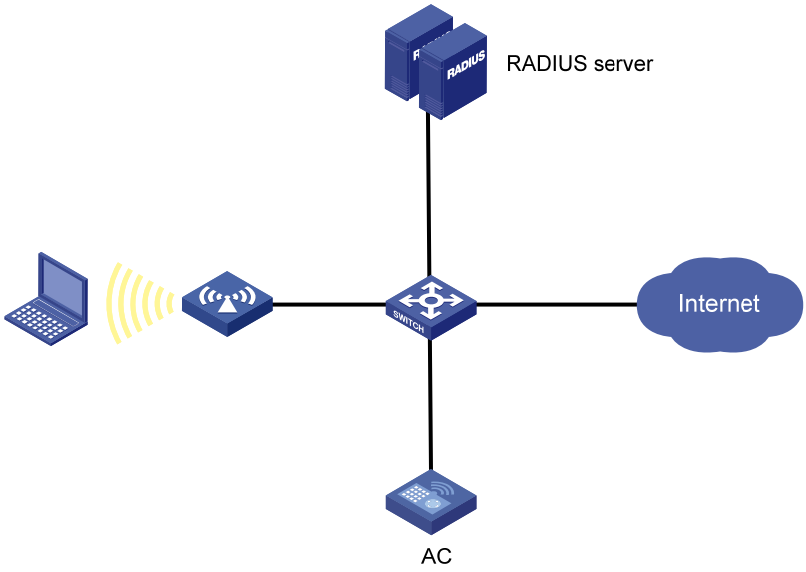
2.1.12 802.1X用户的RADIUS认证配置举例

1. 组网需求

用户接入无线网络，AC 对接入的用户进行 802.1X 认证以控制其访问 Internet，具体要求如下：

- RADIUS 服务器作为认证/授权/计费服务器与 AC 相连，其 IP 地址为 10.1.1.1/24。
- 端口 GigabitEthernet1/0/1 下的所有接入用户均需要单独认证，当某个用户下线时，也只有该用户无法使用网络。
- AC 对 802.1X 用户进行认证时，采用 RADIUS 认证方式，认证 ISP 域为 dm1X。
- AC 与 RADIUS 认证/授权和计费服务器交互报文时的共享密钥均为 name，认证/授权、计费的端口号分别为 1812 和 1813，向 RADIUS 服务器发送的用户名不携带域名。

图2-12 802.1X 用户的 RADIUS 认证配置组网图



2. 配置步骤

(1) 配置各接口的 IP 地址（略）

(2) 配置 RADIUS 方案

单击页面底部的<网络>按钮，然后单击左侧导航栏“网络安全 > 认证”，然后单击“RADIUS”，再单击<添加>按钮，添加 RADIUS 方案，配置步骤为：

- 方案名称为 802.1X。
- 指定主认证服务器 IP 地址为 10.1.1.1，端口号为 1812，共享密钥为 name。设置主认证服务器状态为活动。
- 指定主计费服务器 IP 地址为 10.1.1.1，端口号为 1813，共享密钥为 name。设置主计费服务器状态为活动。
- 在显示高级设置里指定发送给 RADIUS 服务器的用户名格式为不携带域名。

(3) 配置 ISP 域

单击左侧导航栏“网络安全 > 认证”，进入“ISP 域”页面配置，配置步骤为：

- 添加 ISP 域，名称为 dm1X，并将该 ISP 域的状态设置为活动。
- 指定接入方式为 LAN 接入。
- 指定 LAN 接入 AAA 方案的认证、授权和计费的方法均为 RADIUS，方案都选择 802.1X。
- 单击<确定>按钮。

(4) 配置 802.1X

单击左侧导航栏“无线配置 > 无线网络”，进入无线网络页面配置，单击<添加>按钮，配置步骤为：

- 基础设置部分配置无线服务名称和 SSID。
- 安全认证部分认证模式选择 802.1X 认证。
- 域名为 dm1X。
- 单击<确定>按钮。

(5) 配置 RADIUS 服务器

在 RADIUS 服务器上添加用户帐户，保证用户的认证/授权/计费功能正常运行。具体配置方法请参考关于 RADIUS 服务器的配置说明。

3. 验证配置

(1) 单击左侧导航栏“网络安全 > 认证”，然后单击“RADIUS”页签，可以看到已添加成功的 RADIUS 方案 802.1X 的概要信息。

(2) 单击左侧导航栏“网络安全 > 认证”，在 ISP 域页面上，可以看到已添加成功的 ISP 域的 dm1X 的概要信息。

(3) 用户启动 802.1X 客户端，输入正确的用户名和密码之后，可以成功上线。

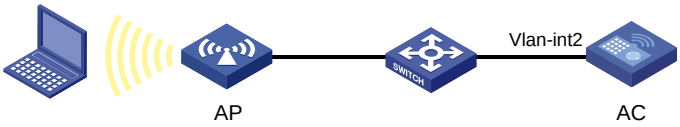
2.1.13 802.1X用户的本地认证配置举例

1. 组网需求

用户接入无线网络，AC 对接入的用户进行 802.1X 认证以控制其访问 Internet，具体要求如下：

- AC 对 802.1X 用户采用本地认证，认证域为 abc。
- 802.1X 用户的认证名为 dotuser，认证密码为 12345。

图2-13 802.1X 用户的本地认证配置组网图



2. 配置步骤

(1) 配置各接口的 IP 地址（略）

(2) 配置本地用户

单击页面底部的<网络>按钮，然后单击左侧导航栏“网络安全 > 用户管理”，进入“本地认证”页面配置，配置步骤为：

- 添加用户，用户名为 dotuser，密码为 12345。
- 指定可用服务为 LAN 接入。

(3) 配置 ISP 域

单击左侧导航栏“网络安全 > 认证”，进入“ISP 域”页面配置，配置步骤为：

- 添加 ISP 域，名称为 abc，并将该 ISP 域的状态设置为活动。
- 指定接入方式为 LAN 接入。
- 指定 LAN 接入 AAA 方案的认证方法为本地认证，授权方法为本地授权，计费方法为不计费。

(4) 配置 802.1X

单击左侧导航栏“无线配置 > 无线网络”页面配置，配置步骤为：

- 基础设置部分配置无线服务名称和 SSID。
- 安全认证部分认证模式选择 802.1X 认证。
- 域名为 abc。

3. 验证配置

(1) 完成上述配置后，单击左侧导航栏“网络安全 > 用户管理”，在“本地认证”页面上可以看到已成功添加的本地用户。

(2) 单击左侧导航栏“网络安全 > 认证”，在“ISP 域”页面上可以看到已经成功添加的 ISP 域。

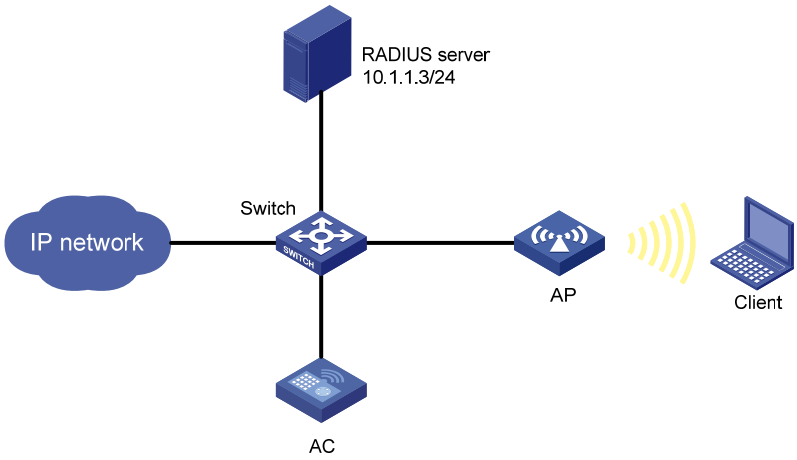
(3) 用户启动 802.1X 客户端，输入正确的用户名和密码之后，可以成功上线。

2.1.14 802.1X身份认证与密钥管理模式配置举例

1. 组网需求

- AP 旁挂在 Switch 上，Switch 同时作为 DHCP server 为 AP 和 Client 分配 IP 地址。
- 客户端链路层认证使用开放式系统认证，客户端通过 802.1X 接入认证的方式实现客户端可使用用户名 abcdef 和密码 123456 接入 WLAN 网络的目的。
- 通过配置客户端和 AP 之间的数据报文采用 802.1X 身份认证与密钥管理来确保用户数据的传输安全。

图2-14 802.1X 认证配置组网图



2. 配置步骤

说明

- 完成 RADIUS 服务器的配置，添加用户帐户，用户名为 abcedf，密码为 123456，并保证用户的认证/授权/计费功能正常运行。
- 完成设备上 RADIUS 和 Domain 域的配置。

(1) 配置无线服务

单击页面底部的<网络>按钮，然后单击左侧导航栏“无线配置 > 无线网络”，进入“无线网络”页面，配置步骤为：

- 单击<添加>按钮，创建一个无线服务，无线服务名称为 service1。
- 配置 SSID 为 service。
- 无线服务状态选择“开启”。

- 单击<确定>按钮。

(2) 配置认证模式为 802.1X 认证

完成上述配置后，会返回“全部网络 > 无线配置 > 无线网络 > 无线网络”页面，单击无线名称为“service1”表项后面的<编辑>按钮，再单击页面上方的“链路层认证”页签，进入认证配置页面，配置步骤为：

- 选择认证模式为 802.1X 认证。
- 选择安全模式为 WPA。
- 选择加密套件为 CCMP。
- 配置域名为 dom1。
- 单击<确定>按钮。

(3) 将无线服务绑定到 AP

进入“全部网络 > 无线配置 > 无线网络 > 无线网络”页面，配置步骤：

- 选中创建的无线服务 service1，单击“绑定到 AP”按钮，进入到“绑定到 AP”页面。
- 选中 AP 的 5GHz 射频单元，单击“快速绑定”。

(4) 验证配置

配置完成后，查看无线服务详情，可以看到已经创建的名称为 service1 无线服务以及配置的认证信息。

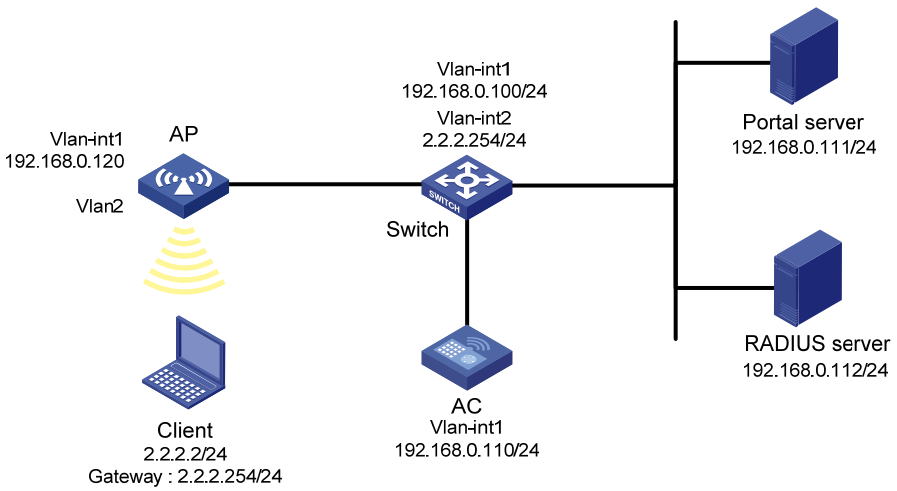
2.1.15 Portal直接认证配置举例

1. 组网需求

在本地转发模式下，对通过无线接入的用户采用直接认证方式。

- 无线客户端通过手工配置或 DHCP 获取的一个公网 IP 地址进行认证，在通过 Portal 认证前，只能访问 Portal Web 服务器；在通过 Portal 认证后，可以使用此 IP 地址访问非受限互联网资源。
- 采用一台 Portal 服务器承担 Portal 认证服务器和 Portal Web 服务器的职责。
- 采用 RADIUS 服务器作为认证/计费服务器。

图2-15 Portal 直接认证配置组网图



2. 配置步骤

说明

- 按照组网图配置设备各接口的 IP 地址，保证启动 Portal 之前各 Client、服务器和 AC 之间的路由可达。
- 完成 RADIUS 服务器上的配置，保证用户的认证/计费功能正常运行。
- 完成 AP 上的配置，保证 AP 与 AC 能够互通。
- 完成设备上 RADIUS 和 Domain 域的配置。

(1) 配置无线服务

单击页面底部的<网络>按钮，然后单击左侧导航栏“无线配置 > 无线网络”进入“无线网络”页面，配置步骤为：

- 单击<添加>按钮，创建一个无线服务，无线服务名称为 service1。
- 配置 SSID 为 service。
- 无线服务状态选择“开启”。
- 单击<确定>按钮。

(2) 配置认证模式为 Portal 认证

完成上述配置后，会返回“全部网络 > 无线配置 > 无线网络 > 无线网络”页面，单击无线名称为“service1”表项后面的<编辑>按钮，再单击页面上方的“链路层认证”，进入认证配置页面，配置步骤为：

- 选择认证模式为 Portal 认证。
- 配置域名为 dm1。
- 选择 Web 服务器名称为 newpt。
- 配置 BAS-IP 为 192.168.0.110。
- 单击<确定>按钮。

(3) 将无线服务绑定到 AP

进入“全部网络 > 无线配置 > 无线网络 > 无线网络”页面，配置步骤：

- 选中创建的无线服务 service1，单击“绑定到 AP”按钮，进入到“绑定到 AP”页面。
- 选中 AP 的 5GHz 射频单元，单击“绑定”按钮。
- 配置绑定到 VLAN 2，单击“确定”按钮。

(4) 验证配置

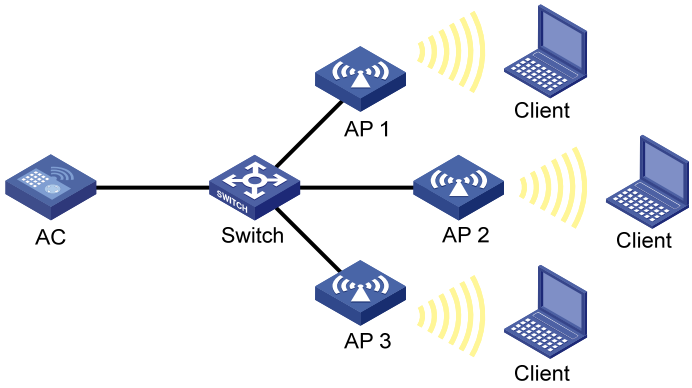
配置完成后，查看无线服务详情，可以看到已经创建的名称为 service1 无线服务以及配置的认证信息。

2.1.16 WLAN RRM信道调整配置举例

1. 组网需求

如 图 2-16 所示，客户端通过AP接入无线服务，当信道变差达到信道调整触发条件时，AC能自动切换信道，保证客户端的无线服务质量。要求AP 1 的Radio 1 避免进行频繁的信道调整。

图2-16 自动信道调整配置组网图



2. 配置步骤

(1) 配置 AP 射频的工作信道（缺省为自动选择，且信道不锁定）

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 射频管理”，进入“射频配置”页面，配置 AP 1、AP 2、AP 3 上射频的工作信道为“自动选择不锁定”。

(2) 配置 RRM

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 射频管理”，进入“射频优化”页面，配置步骤为：

- 在“AP RRM 配置”中开启 AP 1、AP 2、AP 3 上射频的自动信道调整功能，配置 CRC 错误门限为 30，信道干扰门限为 60，容限系数为 25。
- 在“RRM 保持调整组”中创建 ID 为 10 的 RRM 保持调整组，配置信道保持时长为 600 分钟，添加保持调整组成员为 AP 1 的 5GHz 射频单元。

3. 验证配置

(1) 调整周期超时后，如果某个 AP 的当前工作信道质量达到任意一个信道调整门限，AC 将为该 AP 进行信道调整。单击页面左侧导航栏的“ 监控 > 射频监控”，进入“射频优化”页面，可以查看信道调整前后，AP 所使用的信道和信道调整的详细信息。

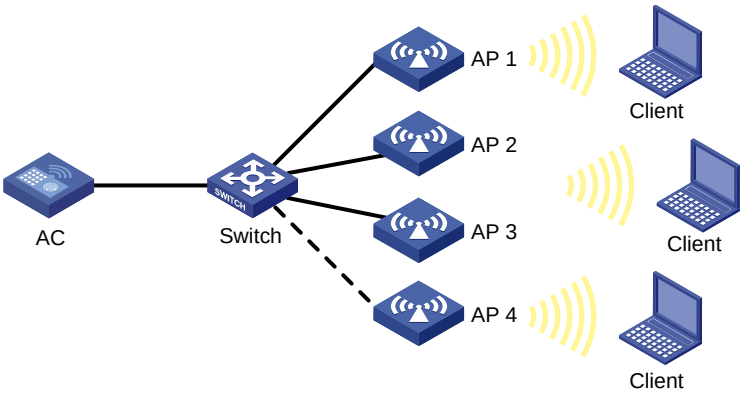
(2) 在调整周期超时后的 600 分钟内，AP 1 的 Radio 1 的信道不会进行调整。

2.1.17 WLAN RRM功率调整配置举例

1. 组网需求

如 图 2-17 所示，无线网络中原本存在AP 1～AP 3，每个AP上仅开启一个Radio，客户端通过AP 1接入无线网络。要求当AP 4 加入AC时，各AP能够自动调整发送功率，并且避免AP 1 的Radio 1 进行频繁的功率切换。

图2-17 自动功率调整配置组网图



2. 配置步骤

(1) 配置 AP 射频的功率锁定状态为关闭

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 射频管理”，进入“射频配置”页面，配置 AP 1、AP 2、AP 3 和 AP 4 的功率锁定状态为关闭。

(2) 配置 RRM

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 射频管理”，进入“射频优化”页面，配置步骤为：

- 在“AP RRM 配置”中开启 AP 1、AP 2、AP 3 和 AP 4 的自动功率调整功能，配置功率调整模式为自定义，最大邻居数为 3，功率调整门限为-70dBm，最小发射功率为 5dBm。
- 在“RRM 保持调整组”中创建 ID 为 10 的 RRM 保持调整组，配置功率保持时长为 100 分钟，添加保持调整组成员为 AP 1 的 5GHz 射频单元。

3. 验证配置

(1) 调整周期超时后，如果某个 AP 的当前发送功率达到功率调整门限，AC 将为该 AP 进行功率调整。单击页面左侧导航栏的“ 监控 > 射频监控”，进入“射频优化”页面，可以查看功率调整前后，AP 所使用的功率和功率调整的详细信息。

(2) 在调整周期超时后的 100 分钟内，AP 1 的 Radio 1 的功率不会进行调整。

2.1.18 会话模式的Radio负载均衡配置举例

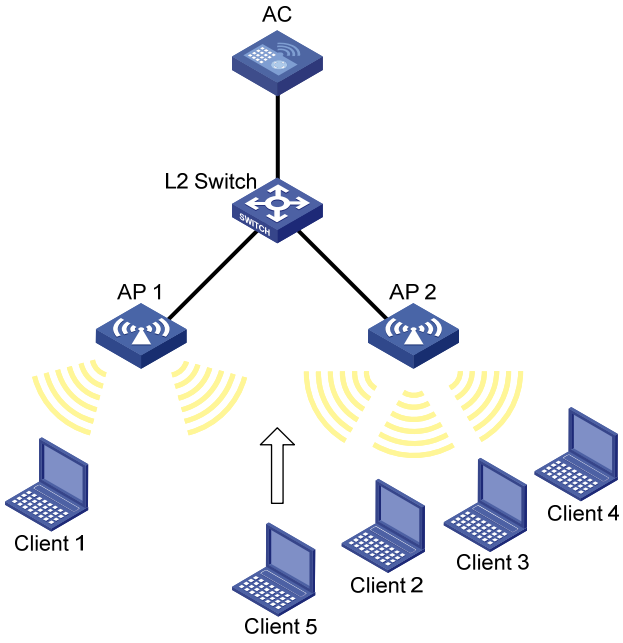
1. 组网需求

AC 连接了两个 AP，这两个 AP 的 Radio 覆盖区域有重叠，为了对这两个 AP 上 Radio 的接入载荷进行负载均衡，有以下要求：

- 负载均衡的评判依据为在线客户端数量。
- 当 Radio 上的在线客户端数量达到或超过 3，并且与另一个 Radio 上的在线客户端数量差值达到或超过 2，开始运行负载均衡。

2. 组网图

图2-18 会话模式的 Radio 负载均衡配置组网图



3. 配置步骤

(1) 配置无线服务

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 无线网络”，进入“无线网络”页面，配置步骤为：

- 创建一个无线服务，名称为 service。
- 配置 SSID 为 session-balance。
- 开启无线服务。

(2) 配置 AP

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > AP 管理”，进入“AP”页面配置 AP，配置步骤为：

- 配置 AP 名称为 AP1。
- 配置 AP 型号及序列号。
- 配置 AP 名称为 AP2。
- 配置 AP 型号及序列号。
- 进入 AP 1 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 AP 1 的射频。
- 进入 AP 2 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 AP 2 的射频。

(3) 配置负载均衡

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 射频管理”，进入“负载均衡”页面，配置步骤为：

- 点击“全局配置”的“更多”按钮进入“详细信息”页面，选择状态为“开启”。
- 选择模式为“会话模式”。

- 配置会话门限值为 3，会话差值门限值为 2。

4. 验证配置

当 Radio 上的在线客户端数量达到或超过 3，并且与另一个 Radio 上的在线客户端数量差值达到或超过 2，开始运行负载均衡。通过单击页面左侧导航栏的“ 监控 > 客户端”，进入“客户端”页面，可以查看到 AP 1 的 Radio 2 和 AP 2 的 Radio 2 上关联的客户端数量达到均衡。

2.1.19 流量模式的Radio负载均衡配置举例

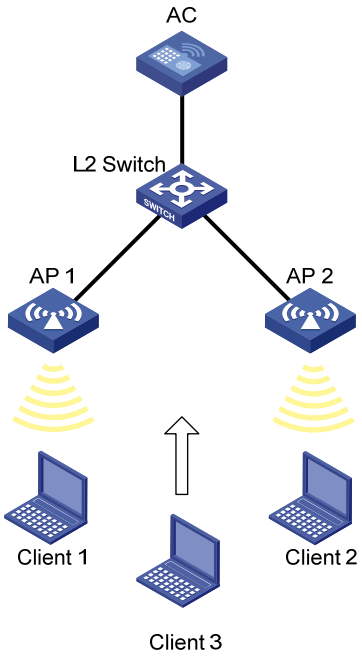
1. 组网需求

AC 连接了两个 AP，这两个 AP 的 Radio 覆盖区域有重叠，为了对这两个 AP 上 Radio 的接入载荷进行负载均衡，有以下要求：

- 负载均衡的评判依据为 Radio 的流量值。
- 当 Radio 上的流量达到或超过 30Mbps（即流量值为占 Radio 最大支持带宽的 20%），并且与另一个 Radio 上的流量差值达到或超过 15Mbps（即流量差值为占 Radio 最大支持带宽的 10%），开始运行负载均衡。

2. 组网图

图2-19 流量模式的 Radio 负载均衡配置组网图



3. 配置步骤

(1) 配置无线服务

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 无线网络”，进入“无线网络”页面，配置步骤为：

- 创建一个无线服务，名称为 service。
- 配置 SSID 为 traffic-balance。

- 开启无线服务。

(2) 配置 AP

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > AP 管理”，进入“AP”页面配置 AP，配置步骤为：

- 配置 AP 名称为 AP1。
- 配置 AP 型号及序列号。
- 配置 AP 名称为 AP2。
- 配置 AP 型号及序列号。
- 进入 AP 1 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 AP 1 的射频。
- 进入 AP 2 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 AP 2 的射频。

(3) 配置负载均衡

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 射频管理”，进入“负载均衡”页面，配置步骤为：

- 点击“全局配置”的“更多”按钮进入“详细信息”页面，选择状态为“开启”。
- 选择模式为“流量模式”。
- 配置流量门限值为 20，流量差值门限值为 10。

4. 验证配置

当 Radio 上的流量达到或超过 30Mbps，并且与另一个 Radio 上的流量差值达到或超过 15Mbps，开始运行负载均衡。通过单击页面左侧导航栏的“ 监控 > 客户端”，进入“客户端”页面，可以查看到 AP 1 的 Radio 2 和 AP 2 的 Radio 2 上关联的客户端数量达到均衡。

2.1.20 带宽模式的Radio负载均衡配置举例

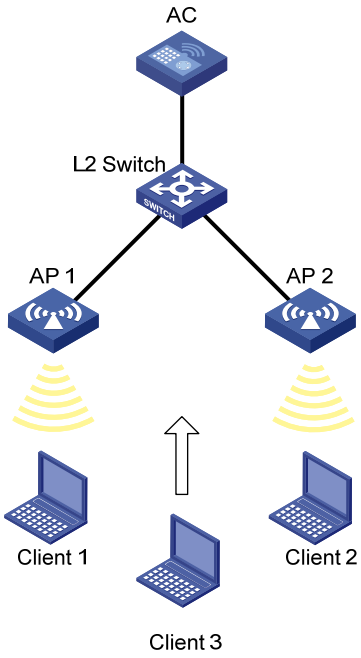
1. 组网需求

AC 连接了两个 AP，这两个 AP 的 Radio 覆盖区域有重叠，为了对这两个 AP 上 Radio 的接入载荷进行负载均衡，有以下要求：

- 负载均衡的评判依据为 Radio 的带宽值。
- 当 Radio 上的带宽达到或超过 12Mbps，并且与另一个 Radio 上的带宽差值达到或超过 3Mbps，开始运行负载均衡。

2. 组网图

图2-20 带宽模式的 Radio 负载均衡配置组网图



3. 配置步骤

(1) 配置无线服务

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 无线网络”，进入“无线网络”页面，配置步骤为：

- 创建一个无线服务，名称为 service。
- 配置 SSID 为 bandwidth-balance。
- 开启无线服务。

(2) 配置 AP

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > AP 管理”，进入“AP”页面配置 AP，配置步骤为：

- 配置 AP 名称为 AP1。
- 配置 AP 型号及序列号。
- 配置 AP 名称为 AP2。
- 配置 AP 型号及序列号。
- 进入 AP 1 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 AP 1 的射频。
- 进入 AP 2 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 AP 2 的射频。

(3) 配置负载均衡

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 射频管理”，进入“负载均衡”页面，配置步骤为：

- 点击“全局配置”的“更多”按钮进入“详细信息”页面，选择状态为“开启”。
- 选择模式为“带宽模式”。

- 配置带宽门限值为 12Mbps，带宽差值门限值为 3Mbps。

4. 验证配置

当 Radio 上的流量达到或超过 12Mbps，并且与另一个 Radio 上的流量差值达到或超过 3Mbps，开始运行负载均衡。通过单击页面左侧导航栏的“ 监控 > 客户端”，进入“客户端”页面，可以查看到 AP 1 的 Radio 2 和 AP 2 的 Radio 2 上关联的客户端数量达到均衡。

2.1.21 会话模式的负载均衡组配置举例

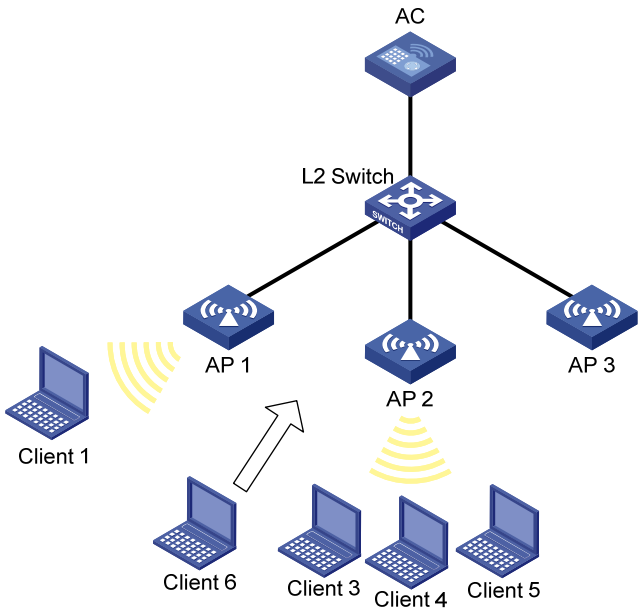
1. 组网需求

AC 连接了三个 AP，这三个 AP 的 radio 覆盖区域有重叠，为了对这三个 AP 上 Radio 的接入载荷进行负载均衡，有以下要求：

- 负载均衡的评判依据为在线客户端数量。
- 仅需要对 AP 1 的 Radio 2 和 AP 2 的 Radio 2 进行负载均衡。
- 当 Radio 上的在线客户端数量达到或超过 3，并且与另一个 Radio 上的在线客户端数量差值达到或超过 2，开始运行负载均衡。

2. 组网图

图2-21 会话模式的负载均衡组配置组网图



3. 配置步骤

(1) 配置无线服务

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 无线网络”，进入“无线网络”页面，配置步骤为：

- 创建一个无线服务，名称为 service。
- 配置 SSID 为 session-balance。
- 开启无线服务。

(2) 配置 AP

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > AP 管理”，进入“AP”页面配置 AP，配置步骤为：

- 配置 AP 名称为 AP1。
- 配置 AP 型号及序列号。
- 配置 AP 名称为 AP2。
- 配置 AP 型号及序列号。
- 配置 AP 名称为 AP3。
- 配置 AP 型号及序列号。
- 进入 AP 1 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 AP 1 的射频。
- 进入 AP 2 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 AP 2 的射频。
- 进入 AP 3 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 AP 3 的射频。

(3) 配置负载均衡

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 射频管理”，进入“负载均衡”页面，配置步骤为：

- 点击“全局配置”的“更多”按钮进入“详细信息”页面，选择状态为“开启”。
- 选择模式为“会话模式”。
- 配置会话门限值为 3，会话差值门限值为 2。
- 进入负载均衡组配置页面，创建负载均衡组 1
- 将 AP 1 的 Radio 2 和 AP 2 的 Radio 2 绑定到负载均衡组中。

4. 验证配置

AP 1 的 Radio 2 和 AP 2 的 Radio 2 在同一个负载均衡组中，AP 3 的 Radio 2 没有加入负载均衡组。由于负载均衡只对组内的 Radio 生效，所以 AP 3 的 Radio 2 不参与负载均衡。

当参与运行负载均衡的某个 Radio 上的在线客户端数量达到或超过 3，并且与另一个 Radio 上的在线客户端数量差值达到或超过 2，开始运行负载均衡。通过单击页面左侧导航栏的“ 监控 > 客户端”，进入“客户端”页面，可以查看到 AP 1 的 Radio 2 和 AP 2 的 Radio 2 上关联的客户端数量达到均衡。

2.1.22 流量模式的负载均衡组配置举例

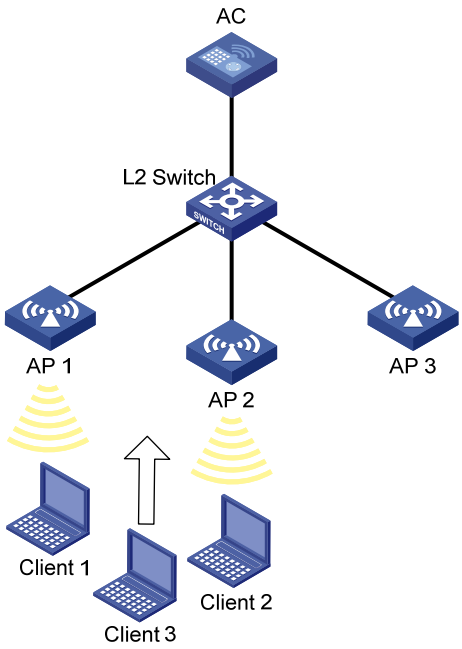
1. 组网需求

AC 连接了三个 AP，这三个 AP 的 radio 覆盖区域有重叠，为了对这三个 AP 上 Radio 的接入载荷进行负载均衡，有以下要求：

- 负载均衡的评判依据为 Radio 的流量值。
- 仅需要对 AP 1 的 Radio 2 和 AP 2 的 Radio 2 进行负载均衡。
- 当 Radio 上的流量达到或超过 30Mbps（即流量值为占 Radio 最大支持带宽的 20%），并且与另一个 Radio 上的流量差值达到或超过 15Mbps（即流量差值为占 Radio 最大支持带宽的 10%），开始运行负载均衡。

2. 组网图

图2-22 流量模式的负载均衡组网图



3. 配置步骤

(1) 配置无线服务

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 无线网络”，进入“无线网络”页面，配置步骤为：

- 创建一个无线服务，名称为 service。
- 配置 SSID 为 traffic-balance。
- 开启无线服务。

(2) 配置 AP

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > AP 管理”，进入“AP”页面配置 AP，配置步骤为：

- 配置 AP 名称为 AP1。
- 配置 AP 型号及序列号。
- 配置 AP 名称为 AP2。
- 配置 AP 型号及序列号。
- 配置 AP 名称为 AP3。
- 配置 AP 型号及序列号。
- 进入 AP 1 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 AP 1 的射频。
- 进入 AP 2 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 AP 2 的射频。
- 进入 AP 3 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 AP 3 的射频。

(3) 配置负载均衡

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 射频管理”，进入“负载均衡”页面，配置步骤为：

- 点击“全局配置”的“更多”按钮进入“详细信息”页面，选择状态为“开启”。
- 选择模式为“流量模式”。
- 配置流量门限值为 20，流量差值门限值为 10。
- 进入负载均衡组配置页面，创建负载均衡组 1
- 将 AP 1 的 Radio 2 和 AP 2 的 Radio 2 绑定到负载均衡组中。

4. 验证配置

AP 1 的 Radio 2 和 AP 2 的 Radio 2 在同一个负载均衡组中，AP 3 的 Radio 2 没有加入负载均衡组。由于负载均衡只对组内的 Radio 生效，所以 AP 3 的 Radio 2 不参与负载均衡。

当参与运行负载均衡的某个 Radio 上的流量达到或超过 30Mbps，并且与另一个 Radio 上的流量差值达到或超过 15Mbps，开始运行负载均衡。通过单击页面左侧导航栏的“ 监控 > 客户端”，进入“客户端”页面，可以查看到 AP 1 的 Radio 2 和 AP 2 的 Radio 2 上关联的客户端数量达到均衡。

2.1.23 带宽模式的负载均衡组配置举例

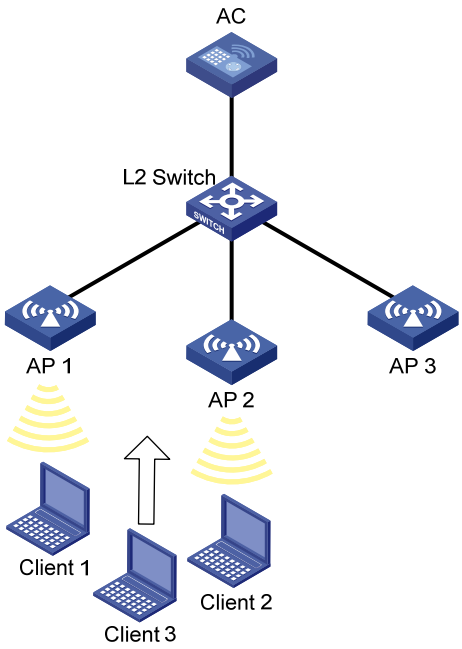
1. 组网需求

AC 连接了三个 AP，这三个 AP 的 radio 覆盖区域有重叠，为了对这三个 AP 上 Radio 的接入载荷进行负载均衡，有以下要求：

- 负载均衡的评判依据为 Radio 的带宽值。
- 仅需要对 AP 1 的 Radio 2 和 AP 2 的 Radio 2 进行负载均衡。
- 当 Radio 上的带宽达到或超过 12Mbps，并且与另一个 Radio 上的带宽差值达到或超过 3Mbps，开始运行负载均衡。

2. 组网图

图2-23 带宽模式的负载均衡组网图



3. 配置步骤

(1) 配置无线服务

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 无线网络”，进入“无线网络”页面，配置步骤为：

- 创建一个无线服务，名称为 service。
- 配置 SSID 为 bandwidth-balance。
- 开启无线服务。

(2) 配置 AP

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > AP 管理”，进入“AP”页面配置 AP，配置步骤为：

- 配置 AP 名称为 AP1。
- 配置 AP 型号及序列号。
- 配置 AP 名称为 AP2。
- 配置 AP 型号及序列号。
- 配置 AP 名称为 AP3。
- 配置 AP 型号及序列号。
- 进入 AP 1 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 AP 1 的射频。
- 进入 AP 2 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 AP 2 的射频。
- 进入 AP 3 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 AP 3 的射频。

(3) 配置负载均衡

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 射频管理”，进入“负载均衡”页面，配置步骤为：

- 点击“全局配置”的“更多”按钮进入“详细信息”页面，选择状态为“开启”。
- 选择模式为“带宽模式”。
- 配置带宽门限值为 12Mbps，带宽差值门限值为 3Mbps。
- 进入负载均衡组配置页面，创建负载均衡组 1
- 将 AP 1 的 Radio 2 和 AP 2 的 Radio 2 绑定到负载均衡组中。

4. 验证配置

AP 1 的 Radio 2 和 AP 2 的 Radio 2 在同一个负载均衡组中，AP 3 的 Radio 2 没有加入负载均衡组。由于负载均衡只对组内的 Radio 生效，所以 AP 3 的 Radio 2 不参与负载均衡。

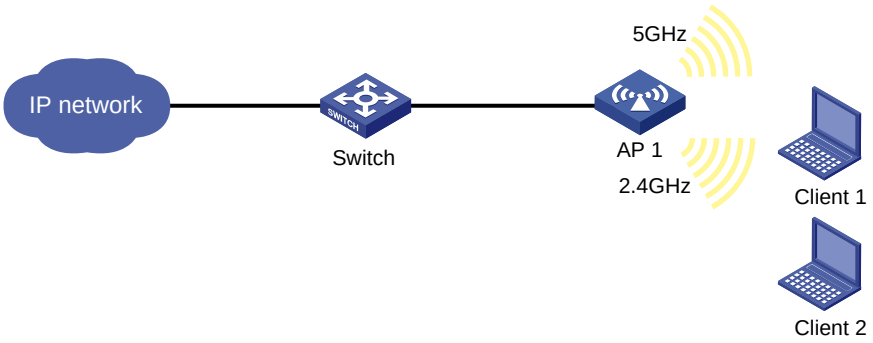
当参与运行负载均衡的某个 Radio 上的带宽达到或超过 12Mbps，并且与另一个 Radio 上的带宽差值达到或超过 3Mbps，开始运行负载均衡。通过单击页面左侧导航栏的“ 监控 > 客户端”，进入“客户端”页面，可以查看到 AP 1 的 Radio 2 和 AP 2 的 Radio 2 上关联的客户端数量达到均衡。

2.1.24 频谱导航配置举例

1. 组网需求

如 图 2-24 所示，AP通过交换机与AC相连，并开启 5GHz射频和 2.4GHz射频。由于网络中有些客户端仅支持 2.4GHz频段，有些客户端支持双频，就有可能导致 2.4GHz射频过载，5GHz射频相对空余。为了防止上述情况的出现，平衡两个频段的射频负载，开启频谱导航功能和频谱导航负载均衡功能。

图2-24 频谱导航配置组网图



2. 配置步骤

(1) 配置无线服务

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 无线网络”，进入“无线网络”页面，配置步骤为：

- 创建一个无线服务，名称为 service。
- 配置 SSID 为 band-navigation。
- 开启无线服务。
- 关闭快速关联。

(2)　配置 AP

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > AP 管理”，进入 AP 1 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 AP 1 的 5GHz 射频和 2.4GHz 射频。

(3)　配置频谱导航

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 射频管理”，进入“频谱导航”页面，配置步骤为：

- 在“全局配置”页面，配置全局频谱导航状态为开启，频谱导航负载均衡的连接数门限为 5，连接数差值门限为 2。
- 在“AP 配置”页面，配置 AP 频谱导航状态为开启。

3. 验证配置

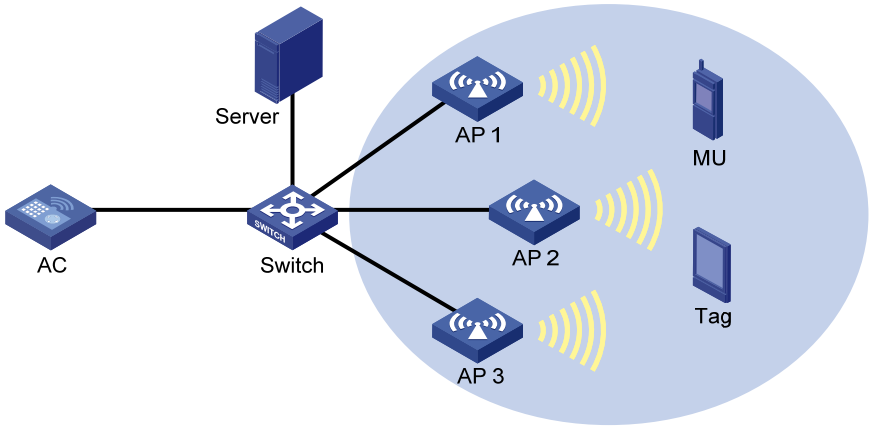
单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 监控 > 客户端”，进入“客户端”页面，可以查看到 AP 1 的 5GHz 射频和 2.4GHz 射频上关联的客户端数量处于均衡状态。

2.1.25 无线定位服务典型配置举例

1. 组网需求

在如下图所示的无线环境中，通过 AP 1、AP 2 和 AP 3 搜集 Tag 和 Mobile 设备的定位信息，然后提供给定位服务器进行定位。

图2-25 无线定位配置组网组



2. 配置步骤

(1)　配置定位服务器

- 在定位服务器上手工配置 AP 1～AP 3 的 IP 地址，或者选择广播方式发现 AP。
- 在定位服务器上完成和定位相关的配置。

(2)　配置 AP

在 AC 上，对 AP 1～AP 3 进行配置。这里以 AP 1 为例。

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > 无线网络”，进入“无线网络”页面配置无线服务，配置步骤为：

- 创建一个无线服务，名称为 market。
- 开启无线服务。

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > AP 管理”，进入“AP”页面配置 AP，配置步骤为：

- 配置 AP 名称为 AP1。
- 配置 AP 型号及序列号。
- 进入 AP 1 的配置页面，在“无线服务配置”页面中将无线服务 market 绑定到 AP 1 的 Radio1 射频。

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > 应用”，进入“无线定位”页面配置无线定位，配置步骤为：

- 单击“全局配置”的“更多”按钮，在“Aeroscout 定位配置”页面下开启 Aeroscout 定位。
- 单击“AP 配置”的“更多”按钮，对 AP1 进行编辑，在“通用配置”页面下开启忽略 Beacon 帧功能。在 Aeroscout 定位配置下，开启 Aeroscout 定位功能，配置 Radio1 为开启并且客户端类型选择 Mobile 设备和 TAG 设备。

3. 验证配置

在图形软件上用户可以通过地图、表格或者报告等形式获取到无线网络中 MU 和 Tag 设备的位置。

2.2 网络安全功能配置举例

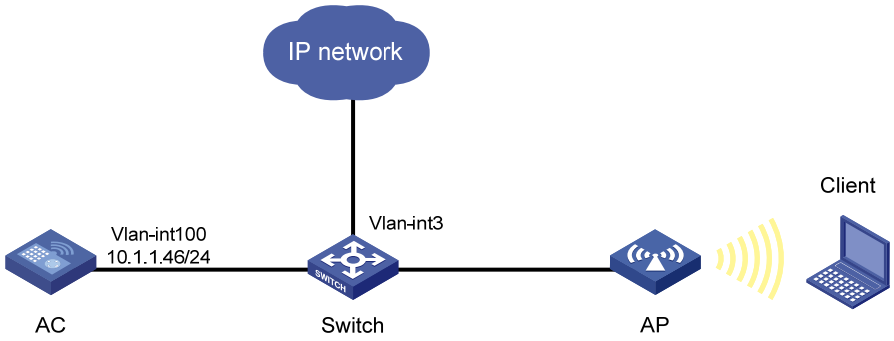
2.2.1 BYOD配置举例

1. 组网需求

用户通过 AC 接入网络，AC 对用户进行 802.1X 认证以控制其访问权限，具体要求如下：

- 802.1X 用户的认证名为 dotuser，认证密码为 12345。
- AC 使用开放式系统对 802.1X 用户进行本地认证、授权，认证域为 abc
- 终端类型为 Microsoft Windows 8 的 802.1X 用户通过认证后将被授权访问 VLAN 3。

图2-26 支持本地 BYOD 授权的 802.1X 用户认证、授权配置组网图



2. 配置步骤

(1) 配置各接口的 IP 地址（略）

(2) 配置无线服务

单击页面底部的<网络>按钮，然后单击左侧导航栏“无线配置 > 无线网络”，进入“无线网络”页面，配置步骤为：

- 单击<添加>按钮，创建一个无线服务，无线服务名称为 service1。
- 配置 SSID 为 service。
- 无线服务状态选择“开启”。
- 单击<确定>按钮。

(3) 配置认证模式为 802.1X 认证

完成上述配置后，会返回“全部网络 > 无线配置 > 无线网络 > 无线网络”页面，单击无线名称为“service1”表项后面的<编辑>按钮，再单击页面上方的“链路层认证”，进入认证配置页面，配置步骤为：

- 选择认证模式为 802.1X 认证。
- 选择安全模式为 WPA。
- 选择加密套件为 CCMP。
- 配置域名为 abc。
- 单击<确定>按钮。

(4) 将无线服务绑定到 AP

进入“全部网络 > 无线配置 > 无线网络 > 无线网络”页面，配置步骤为：

- 选中创建的无线服务 service1，单击“绑定到 AP”按钮，进入到“绑定到 AP”页面。
- 选中 AP 的 5GHz 射频单元，单击“快速绑定”。

(5) 配置 ISP 域

单击左侧导航栏“网络安全 > 认证”，进入“ISP 域”配置页面，配置步骤为：

- 单击<添加>按钮，添加 ISP 域，域名为 abc，并将该 ISP 域的状态设置为活动。
- 指定接入方式为 LAN 接入。
- 指定 LAN 接入 AAA 方案的认证方法为本地认证，授权方法为本地授权，计费方法为不计费。
- 单击<确定>按钮。

(6) 配置本地用户

单击左侧导航栏“网络安全 > 用户管理”，进入“本地认证”配置页面，配置步骤为：

- 单击页面右上方<用户组>按钮，然后单击<添加>按钮，添加用户组，用户组名为 windows8。
- 单击<确定>按钮，返回本地用户页面。
- 单击页面右上方<用户>按钮，然后单击<添加>按钮，添加用户，用户名为 dotuser，密码为 12345。
- 指定可用服务为 LAN 接入。
- 指定授权用户组为 windows8。
- 单击<确定>按钮。

(7) 配置 BYOD 授权

单击左侧导航栏“网络安全 > BYOD”，然后单击页面上方“BYOD 授权”，进入 BYOD 授权配置页面，单击用户组 windows8 表项后面的<编辑>按钮，为用户组 windows8 配置授权属性：设备类型为 Microsoft Windows 8、ACL 编号为 2000，授权 VLAN 为 VLAN 3。

然后单击表项右侧的<添加>按钮，最后单击<确定>。

(8) 配置 BYOD 规则

完成上述配置后会返回到 BYOD 授权页面，单击“BYOD 规则”，新建一条自定义 BYOD 规则：DHCP Option 55 为 1,15,3,6,44,46,47,31,33,121,249,252,43.33，终端类型为 Microsoft Windows 8。

3. 验证配置

以上配置完成后，使用 Microsoft Windows 8 终端的 802.1X 用户通过认证后，可访问 VLAN 3 中的网络资源。

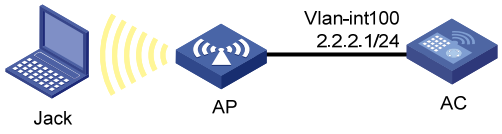
2.2.2 来宾用户管理配置举例

1. 组网需求

在 AC 上配置来宾管理功能，并为来宾 Jack 创建来宾用户 user1。具体要求如下：

- 为来宾 Jack 创建一个本地来宾用户 user1，并设置密码、所属用户组、个人相关信息、有效期、以及接待人信息。
- 配置设备为来宾用户业务发送电子邮件使用的 SMTP 服务器地址、发件人地址、来宾管理员的电子邮件地址。
- 配置设备发送给来宾用户、来宾接待人、来宾管理员的邮件标题和内容。
- 来宾用户账户过期后系统自动将其删除。

图2-27 来宾用户管理配置组网图



2. 配置步骤

(1) 配置各接口的 IP 地址（略）

(2) 配置无线服务（略）

(3) 添加来宾用户

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 网络安全 > 来宾管理”，进入“来宾用户”页面，配置步骤为：

- 添加用户，账号为 user1，密码为 123456。
- 指定来宾用户所属的用户组。（请根据实际需求选择）
- 配置来宾用户的姓名、公司名称、电子邮箱、联系电话、描述信息。（请根据实际情况配置）
- 配置来宾接待人的姓名、所属部门、电子邮箱。（请根据实际情况配置）
- 配置来宾用户的有效期。（请根据实际情况配置）

(4) 配置来宾业务参数

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 网络安全 > 来宾管理”，进入“来宾业务参数”页面，配置步骤为：

- 开启自动删除失效来宾用户功能。
- 配置发送电子邮件使用的 SMTP 服务器地址为 smtp://192.168.0.112/smtp。
- 配置发件人电子邮箱为 bbb@ccc.com。
- 配置来宾管理员电子邮箱为 guest-manager@ccc.com。
- 配置发送给来宾用户的通知邮件标题为 Guest account information，邮件内容为 A guest account has been created for your use. The username, password, and valid dates for the account are given below.。
- 配置发送给来宾管理员的通知邮件标题为 Guest register information，邮件内容为 A guest account has been registered. The username for the account is given below. Please approve the register information.。
- 配置发送给来宾接待人的通知邮件标题为 Guest account information，邮件内容为 A guest account has been created. The username, password, and valid dates for the account are given below.。

3. 验证配置

Jack 使用用户名 user1 和密码 123456 在账户有效期内进行本地认证，可以认证通过并接入网络。

2.3 工具功能配置举例

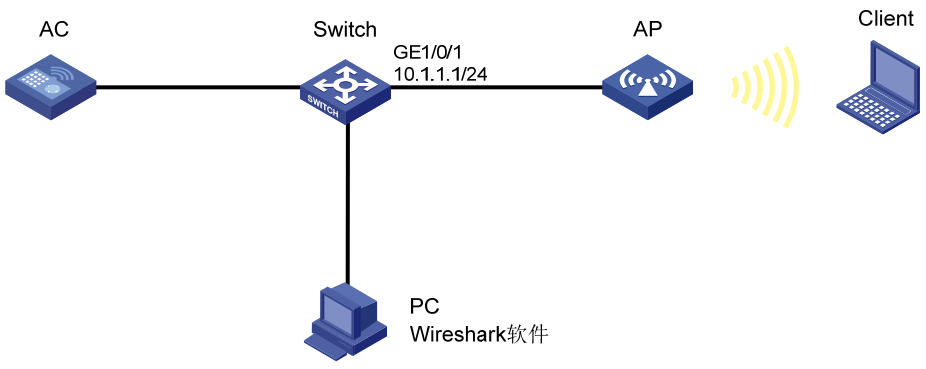
2.3.1 本地报文捕获配置举例

1. 组网需求

- 在 AP 的 Radio 1 上开启本地报文捕获功能，要求捕获 1KB 的协议类型为 TCP，且报文的源 IP 地址为 192.168.20.173 的报文。
- Switch 做为 FTP 服务器，保存 AP 发送的被捕获报文。

2. 组网图

图2-28 本地报文捕获组网图



3. 配置步骤

(1) 配置 Switch

在 Switch 上添加一个 FTP 用户 abc，并设置其认证密码为 123456，访问时使用的用户角色为 network-admin，授权访问目录为 Flash 的根目录，可以使用的服务类型为 FTP。

启动 Switch 的 FTP 服务功能。

(2) 在 AC 上配置本地报文捕获功能

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 工具 > 无线报文捕获”，进入“无线报文捕获”页面，配置步骤为：

- 选择 AP 的 Radio 1，开启本地报文捕获功能。
- 指定过滤规则为"src 192.168.20.173 and tcp"，捕获报文最大长度为 8000，存储捕获报文的文件大小为 1KB，FTP 服务器的 URL 地址为 ftp://10.1.1.1，登录 FTP 服务器的用户名为 abc，用户密码为 123456。

4. 验证配置

报文捕获成功后，在 PC 上使用 wireshark 软件与 FTP 服务器建立连接，可以解析报文文件。

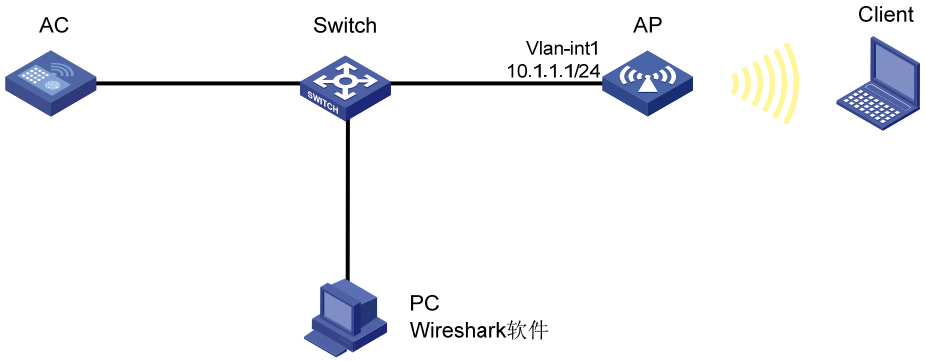
2.3.2 远程报文捕获配置举例

1. 组网需求

在 AP 的 Radio 1 上开启远程报文捕获功能，将捕获的报文上送到 Wireshark 软件上解析。

2. 组网图

图2-29 远程报文捕获组网图



3. 配置步骤

(1) 配置远程报文捕获功能

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 工具 > 无线报文捕获”，进入“无线报文捕获”页面，配置步骤为：

- 选择 AP 的 Radio 1，开启远程报文捕获功能。
- 指定 RPCAP 服务端口号为 2014。

(2) 配置 PC

- 在 PC 上打开 Wireshark 软件，菜单栏选择 Capture，在弹出的下拉菜单中选择 Options，弹出 Capture Options 对话框后，选择 remote 捕获方式，输入捕获地址 10.1.1.1 和端口号 2014，单击“OK”按钮，再单击“Start”按钮，此时在弹出的报文捕获窗口会看到捕获的报文。

图2-30 Wireshark 软件报文捕获窗口