H3C MER 系列路由器

用户手册

新华三技术有限公司
http://www.h3c.com

资料版本：6W102-20210226

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

前 言

《H3C MER 系列路由器 用户手册》将会详细地指导您如何通过 Web 设置页面或命令行对设备进行本地管理。

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”。

格　式	意　义
/	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

登录 Web 设置页面

说明

本章节仅介绍如何本地登录路由器的 Web 设置页面。如果您想实现远程登录路由器进行管理，需要先本地登录路由器，并开启其远程管理功能，相关的介绍请参见“远程管理”。

本章节主要包含以下内容：

准备工作

完成硬件安装后（安装过程请参见《H3C MER3200[5200]系列路由器 快速入门》及《H3C MER8300系列路由器 快速入门》），在登录路由器的 Web 页面前，您需要确保管理计算机和网络满足一些基本要求。

1管理计算机要求

请确认管理计算机已安装了以太网卡。

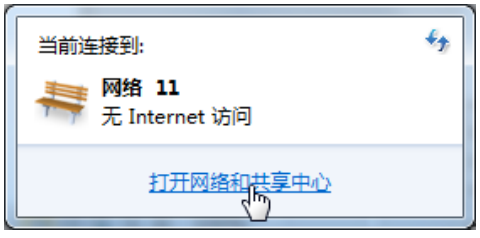
2建立网络连接

1. 设置管理计算机的 IP 地址

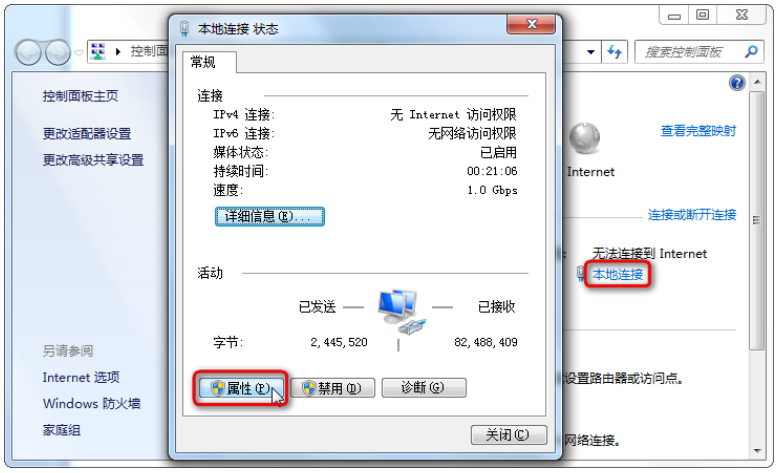
- 自动获取 IP 地址（推荐使用）：请将管理计算机设置成“自动获得 IP 地址”和“自动获得 DNS 服务器地址”（计算机系统的缺省配置），由路由器自动为管理计算机分配 IP 地址。
- 设置静态 IP 地址：请将管理计算机的 IP 地址与路由器的 LAN 口 IP 地址设置在同一网段内（LAN 口缺省的 IP 地址为 192.168.1.1，子网掩码为 255.255.254.0）。

操作步骤如下（以 Window 7 系统为例）：

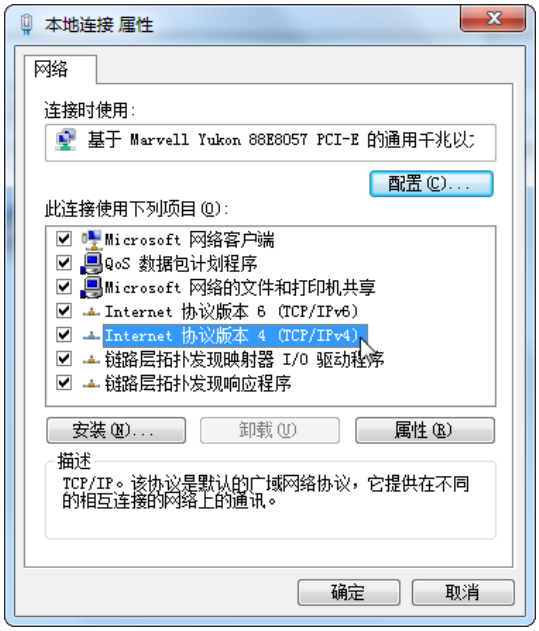
1. 单击桌面右下角的网络图标，如  ，选择“打开网络和共享中心”



2. 单击“本地连接”，单击<属性>按钮，进入“本地连接属性”窗口



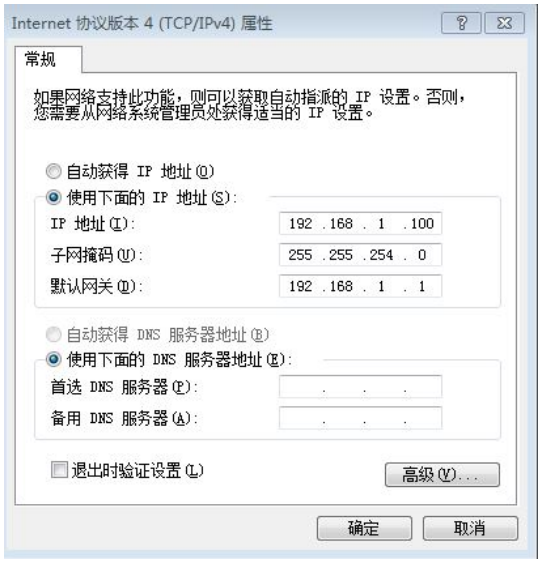
3. 双击“Internet 协议版本 4（TCP/IPv4）”



4. 配置计算机的 IP 地址

- 当路由器开启 DHCP 功能时，可选择自动获得 IP 地址和 DNS 服务器地址，或通过手动配置电脑 IP 地址，与路由器 IP 地址（缺省 192.168.1.1）保持同一网段
- 当路由器关闭 DHCP 功能时，只能通过手动配置电脑 IP 地址，与路由器 IP 地址（缺省 192.168.1.1）保持同一网段

设置好IP地址后，单击<确定>按钮，返回[本地连接 属性]对话框，再单击<确定>按钮

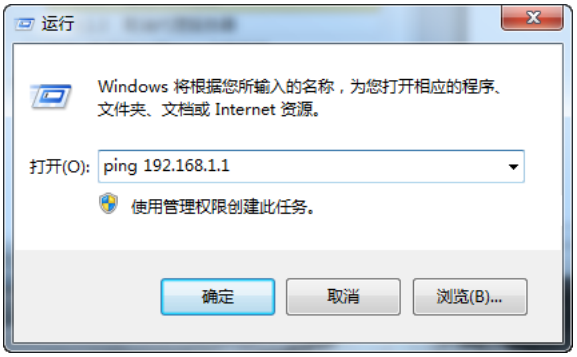


2. 确认管理计算机和路由器之间的网络是否连通

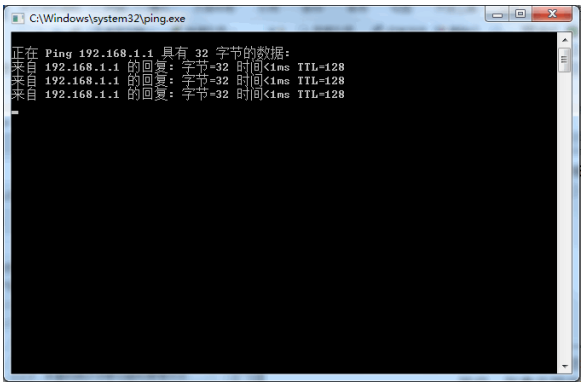
操作步骤如下：

5. 单击屏幕左下角<开始>按钮进入[开始]菜单，选择“运行”，弹出“运行”对话框

6. 输入“ping 192.168.1.1（路由器的 IP 地址，此处是缺省 IP 地址）”，单击<确定>按钮



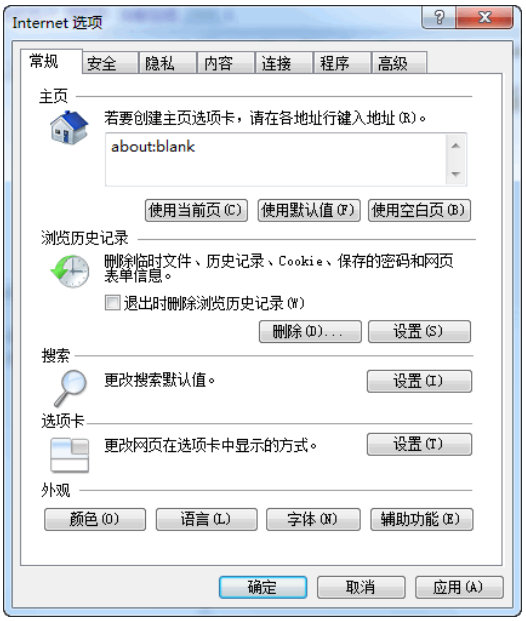
7. 如果在弹出的对话框中显示了从路由器侧返回的回应，则表示网络连通；否则请检查网络连接

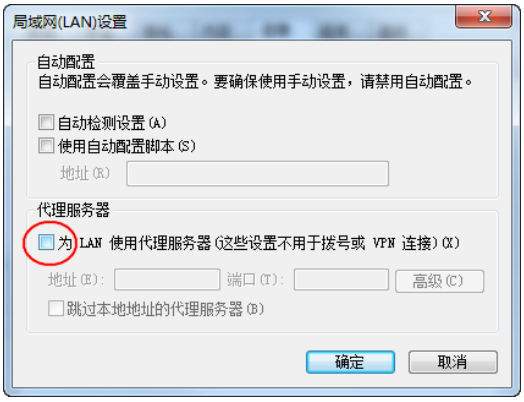


3取消代理服务器

如果当前管理计算机使用代理服务器访问因特网，则必须取消代理服务，操作步骤如下：

8. 在浏览器窗口中，选择[工具/Internet 选项]进入“Internet 选项”窗口



2.	选择“连接”页签，并单击<局域网设置（L）>按钮，进入“局域网（LAN）设置”页面。请确认未选中“为 LAN 使用代理服务器”选项；若已选中，请取消并单击<确定>按钮	

登录路由器Web设置页面

运行 Web 浏览器，在地址栏中输入“http://192.168.1.1”，回车后跳转到 Web 登录页面，如图 1-1 所示，输入用户名、密码（缺省均为 admin，区分大小写），首次登录路由器之后，系统会自动弹出“修改密码”页面，输入旧密码、新密码，并确认新密码，单击<确定>按钮即可进入 Web 设置页面。

图1 登录路由器 Web 设置页面

快速配置

本章节介绍快速配置的相关内容，包括：

简介

通过快速配置完成广域网 WAN 和局域网 LAN 的基本配置后，局域网内的用户便可以访问外网。

配置WAN

说明

MER3220/5200/8300 暂不支持 3G/4G Modem 接入广域网。

1配置需求

设备支持单 WAN 和双 WAN 两种广域网接入场景。如果用户仅租用了一个运营商网络，则选择单 WAN 场景；如果用户租用了两个运营商网络，则使用双 WAN 场景。单 WAN 和双 WAN 场景的配置方法相同。

设备可以通过物理接口或 3G/4G Modem 接入广域网。

2通过物理接口接入广域网配置步骤

(1) 单击导航树中[快速配置]菜单项，进入快速配置页面。

(2) 根据使用场景需求，选择“单 WAN 场景”或“双 WAN 场景”，设置广域网接入参数。

(3) 在“线路 1”或“线路 2”配置项处选择要接入广域网的物理接口 WANx。

(4) 根据用户实际的上网方式，在“连接模式”配置项处选择对应的连接模式：

- 如果选择连接模式为“PPPoE”：
  - 在“上网账号”配置项处，输入运营商提供的 PPPoE 接入用户名。
  - 在“上网口令”配置项处，输入运营商提供的 PPPoE 接入密码。
- 如果选择连接模式为“DHCP”，将自动从 DHCP 服务器获取接入广域网的公网 IP 地址。
- 如果选择连接模式为“固定地址”：
  - 在“IP 地址”配置项处，输入接入广域网的固定 IP 地址。
  - 在“子网掩码”配置项处，输入 IP 地址的掩码或掩码长度，例如 255.255.255.0 或 24。
  - 在“网关地址”配置项处，输入接入广域网的网关地址。
  - 在“DNS1”和“DNS2”配置项处，输入接入广域网的 DNS 服务器地址。注意设备优先使用 DNS1 进行域名解析。如果解析失败，则使用 DNS2 进行域名解析。

(5) 在“NAT 地址转换”配置项处，根据实际需求选择是否启用该功能。局域网中的多台设备共用同一个公网 IP 时需要启用此功能。

(6) 点击<下一步>按钮，完成 WAN 配置。

3通过 3G/4G Modem 接入广域网配置步骤

(1) 单击导航树中[快速配置]菜单项，进入快速配置页面。

(2) 根据使用场景需求，选择“单 WAN 场景”或“双 WAN 场景”，设置广域网接入参数。

(3) 在“线路 1”或“线路 2”配置项处选择 3G/4G Modem 对应的 Cellular 接口。

(4) 在“运营商”配置项处，根据实际使用的运营商情况选择“移动”、“联通”、“电信”或“自定义”：

- 如果选择运营商为“移动”、“联通”或“电信”：
  - 在“用户名”配置项处，输入从运营商处获取的用户名。
  - 在“密码”配置项处，输入从运营商处获取的密码。
- 如果选择连接模式为“自定义”：
  - 在“APN”配置项处，输入从运营商处获取的 APN。
  - 在“对端号”配置项处，输入从运营商处获取的拨号串。
  - 在“用户名”配置项处，输入从运营商处获取的用户名。
  - 在“密码”配置项处，输入从运营商处获取的密码。

当使用国外的运营商或其他物联网的 SIM 卡时，需要选择“自定义”连接模式。

(5) 在“制式选择”配置项处，选择当前运营商对应的网络制式。

(6) 在“NAT 地址转换”配置项处，根据实际需求选择是否启用该功能。局域网中的多台设备共用同一个公网 IP 时需要启用此功能。

(7) 点击<下一步>按钮，完成 WAN 配置。

配置LAN

完成 WAN 配置后，会进入到 LAN 配置的页面。

(1) 在“局域网 IP 地址”配置项处，输入设备在局域网中使用的 IP 地址。

(2) 在“子网掩码”配置项处，输入 IP 地址的掩码或掩码长度，例如 255.255.255.0 或 24。

(3) 在“DHCP 服务”配置项处，选择“启用”或“禁用”。如果设备需要作为 DHCP 服务器为局域网中的主机分配 IP 地址，则需要选择“启用”。

- 如选择“启用”：
  - 在“IP 分配范围”配置项处，输入待分配地址的起始 IP 地址和结束 IP 地址；
  - 在“网关地址”配置项处，输入设备为 DHCP 客户端分配的网关地址；
  - 在“DNS”配置项处，输入设备为 DHCP 客户端分配的 DNS 服务器的 IP 地址。
- 如选择“禁用”，则表示不启用设备的 DHCP 功能。

(4) 点击<下一步>按钮，完成 LAN 配置。

网络设置

外网配置

本章节介绍外网配置的相关内容，包括：

1简介

通常情况下，外网指的就是广域网（WAN，Wide Area Network），广域网是覆盖地理范围相对较广的数据通信网络，Internet 就是一个巨大的广域网。

通常在设备上会有多个 WAN 接口，通过配置 WAN 接口可以实现设备访问外网。

2场景定义

1. 配置需求

设备支持单 WAN 和多 WAN 两种广域网接入场景。如果用户仅租用了一个运营商网络，则选择单 WAN 场景；如果用户租用了两个运营商网络，则使用多 WAN 场景。单 WAN 和多 WAN 场景的配置方法相同。

2. 配置步骤

(1) 单击导航树中[网络配置/外网配置]菜单项，进入外网配置页面。

(2) 单击“场景定义”页签，进入场景定义配置页面。

(3) 根据使用场景需求，选择“单 WAN 场景”或“多 WAN 场景”。

(4) 选择要接入广域网的接口，该接口可以是设备上物理的 WAN 接口或 3G/4G Modem 对应的 Cellular 接口：

- 单 WAN 场景下，在“线路 1”配置项处选择接入广域网的接口。
- 多 WAN 场景下，在“线路 1”、“线路 2”、“线路 3”或“线路 4”配置项处选择多个接入广域网的接口。

(5) 点击<应用>按钮，完成场景定义配置。

3WAN 配置

1. 配置需求

设备支持通过物理接口和 3G/4G Modem 接入广域网，两种方式需要配置的参数不同。

2. 通过物理接口接入广域网配置步骤

(1) 单击导航树中[网络配置/外网配置]菜单项，进入外网配置页面。

(2) 单击“WAN 配置”页签，进入 WAN 配置页面。

(3) 在线路列表中，单击指定线路上“操作”区段的“修改”按钮，进入修改 WAN 配置页面。

(4) 根据用户实际的上网方式，在“连接模式”配置项处选择对应的连接模式：

- 如果选择连接模式为“PPPoE”：
  - 在“上网账号”配置项处，输入运营商提供的 PPPoE 接入用户名。
  - 在“上网口令”配置项处，输入运营商提供的 PPPoE 接入密码。
  - “在线方式”为“始终在线”。
- 如果选择连接模式为“DHCP”，将自动从 DHCP 服务器获取接入广域网的公网 IP 地址。
- 如果选择连接模式为“固定地址”：
  - 在“IP 地址”配置项处，输入接入广域网的固定 IP 地址。
  - 在“子网掩码”配置项处，输入 IP 地址的掩码或掩码长度，例如 255.255.255.0 或 24。
  - 在“网关地址”配置项处，输入接入广域网的网关地址。
  - 在“DNS1”和“DNS2”配置项处，输入接入广域网的 DNS 服务器地址。注意设备优先使用 DNS1 进行域名解析。如果解析失败，则使用 DNS2 进行域名解析。

(5) 在“MAC 地址”配置项处，根据实际需求选择“使用接口出厂 MAC 地址（例如：00-19-10-28-00-80）”或“使用静态指定的 MAC”。如果选择“使用静态指定的 MAC”，则在配置项处输入配置的静态 MAC 地址，通过运营商分配的公网地址访问外网时，需要配置静态 MAC 地址进行 MAC 地址绑定。

(6) 在“NAT 地址转换”配置项处，根据实际需求选择是否启用该功能。局域网中的多台设备共用同一个公网 IP 时需要启用此功能。

(7) 在“TCP MSS”配置项处，设置接口的 TCP 报文段的最大长度。

(8) 在“MTU”配置项处，输入接口允许通过的 MTU（Maximum Transmission Unit，最大传输单元）的大小。

(9) 在“链路探测”配置项处，根据实际情况选择是否启用该功能，如果选择启用：

- 在“探测地址”配置项处，输入链路探测的 IP 地址。
- 在“探测间隔”配置项处，输入链路探测的时间间隔。

启用链路探测功能后，可以对到达指定 IP 地址的链路状态进行判断，提高链路的可靠性。

(10) 点击<确定>按钮，完成 WAN 配置修改。

3. 通过 3G/4G Modem 接入广域网配置步骤

(1) 单击导航树中[网络配置/外网配置]菜单项，进入外网配置页面。

(2) 单击“WAN 配置”页签，进入 WAN 配置页面。

(3) 在线路列表中，单击指定线路上“操作”区段的“修改”按钮，进入修改 WAN 配置页面。

(4) 在“运营商”配置项处，根据实际使用的运营商情况选择“移动”、“联通”、“电信”或“自定义”：

- 如果选择运营商为“移动”、“联通”或“电信”：。
  - 在“用户名”配置项处，输入从运营商处获取的用户名。
  - 在“密码”配置项处，输入从运营商处获取的密码。
- 如果选择连接模式为“自定义”：
  - 在“APN”配置项处，输入从运营商处获取的 APN。

- 在“拨号串”配置项处，输入从运营商处获取的拨号串。
- 在“用户名”配置项处，输入从运营商处获取的用户名。
- 在“密码”配置项处，输入从运营商处获取的密码。

当使用国外的运营商或其他物联网的 SIM 卡时，需要选择“自定义”连接模式。

(5) 在“制式选择”配置项处，选择当前运营商对应的网络制式。

(6) 在“NAT 地址转换”配置项处，根据实际需求选择是否启用该功能。局域网中的多台设备共用同一个公网 IP 时需要启用此功能。

(7) 在“链路探测”配置项处，根据实际情况选择是否启用该功能，如果选择启用：

- 在“探测地址”配置项处，输入链路探测的 IP 地址。
- 在“探测间隔”配置项处，输入链路探测的时间间隔。

启用链路探测功能后，可以对到达指定 IP 地址的链路状态进行判断，提高链路的可靠性。

(8) PIN（Personal Identification Number，个人识别密码）码是保护 SIM 卡的一种安全措施，防止别人盗用 SIM 卡，可以点击<更多配置>按钮，进入 PIN 码配置页面：

- 根据需要决定是否勾选“开启 PIN 码认证功能”，如勾选，则在配置项处输 PIN 码。建议开启 PIN 码认证功能，提高设备安全性。
- 如果开启 PIN 码认证功能时输入的 PIN 码有误，可以点击<修改 PIN 码>按钮，进入修改 PIN 码配置页面：
  - 在“原 PIN 码”配置项处，输入原有的 PIN 码。
  - 在“新 PIN 码”配置项处，输入新的 PIN 码。
  - 在“确认新 PIN 码”配置项处，再次输入新的 PIN 码。
  - 点击<提交修改>按钮完成 PIN 码修改，点击<返回>按钮取消修改操作。
- 如果多次输入 PIN 码错误，需要点击<PIN 码解锁>按钮，进入 PIN 码解锁配置页面：
  - 在“PUK 码”配置项处，输入解锁的 PUK 码。
  - 在“新 PIN 码”配置项处，输入新的 PIN 码。
  - 在“确认新 PIN 码”配置项处，再次输入新的 PIN 码。
  - 点击<解锁>按钮完成 PIN 码解锁，点击<返回>按钮取消解锁操作。
- 如果需要重启 3G/4G Modem，可以点击<重启 Modem>按钮。

(9) 点击<保存配置>按钮，完成 WAN 配置修改。

4修改多 WAN 策略

1. 注意事项

只有多 WAN 场景可以进行本页面的配置。

2. 配置步骤

(1) 单击导航树中[网络配置/外网配置]菜单项，进入外网配置页面。

(2) 单击“修改多 WAN 策略”页签，进入修改多 WAN 策略配置页面。

(3) 根据实际应用，对多 WAN 策略进行修改：

- 如果多 WAN 属于相同的运营商，建议选择“平均分配负载分担”或“带宽比例负载分担”。如果多 WAN 链路的带宽一致，可以选择“平均分配负载分担”，否则选择“带宽比例负载分担”。
- 如果多 WAN 属于不同的运营商，建议选择“基于运营商的负载分担”或“多链路高级负载分担”。如果每个运营商提供的链路带宽一致，可以选择“基于运营商的负载分担”，否则选择“多链路高级负载分担”。
- 为了保持网络的稳定性，可以进行链路备份，选择“主链路（请选择作为主链路的 WAN 接口）”以及对应的“线路 n”，然后选择备份链路的“线路 m”。注意 n 和 m 不能一致，否则不能实现链路备份。

(4) 点击<应用>按钮，完成多 WAN 策略修改。

5保存接口上一跳

(1) 单击导航树中[网络配置/外网配置]菜单项，进入外网配置页面。

(2) 单击“保存接口上一跳”页签，进入配置页面。

(3) 选择“开启保存接口上一跳功能”或“关闭保存接口上一跳功能”。多 WAN 场景下，为了确保进入和离开局域网的报文通过同一个 WAN 接口转发，需要开启保存接口上一跳功能。

LAN配置

本章节介绍 LAN 配置的相关内容，包括：

1简介

本功能主要用于配置设备连接内网的 LAN 接口参数，开启 DHCP 服务，以及将接口加入 VLAN。

DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）是一个局域网协议，主要用于为局域网内的主机分配 IP 地址。DHCP 支持动态及静态地址分配机制：

- 动态地址分配功能配置在接口上，此功能给用户主机动态分配 IP 地址，时间到期或主机明确表示放弃该地址时，该地址可以被其他主机使用。该分配方式适用于局域网的主机获取有一定有效期限的地址的组网环境。
- 静态分配的 IP 地址不和接口绑定，仅需要与主机的网卡 MAC 地址进行绑定，具有永久使用权限。该分配方式适用于局域网的主机获取租期为无限长的 IP 地址的组网环境。

2配置 LAN 接口基本参数

1. 配置需求

为设备连接内网的 GE 接口配置 IP 地址，或创建 VLAN 与 VLAN 接口。

2. 配置步骤

(1) 单击导航树中[网络配置/LAN 配置]菜单项，进入 LAN 配置页面。

(2) 单击“LAN 配置”页签，进入 LAN 接口配置页面。

(3) 点击<添加>按钮，进入添加 LAN 接口页面。

(4) 在“LAN 接口类型”配置项处，选择配置的接口类型：

- 如果选择“VLAN 接口”，则表示创建 VLAN 与 VLAN 接口，还需要输入 VLAN ID。
- 如果选择“GE 接口”，则表示配置指定的 GE 接口，还需要选择 GE 接口。

(5) 在“接口 IP 地址”配置项处，输入接口的 IP 地址。

(6) 在“子网掩码”配置项处，输入 IP 地址的掩码或掩码长度，例如 255.255.255.0 或 24。

(7) 在“TCP MSS”配置项处，设置接口的 TCP 报文最大分段长度值。

(8) 在“MTU”配置项处，输入接口允许通过的 MTU 的大小。

(9) 如果还希望设备为连接到设备的客户端（如连接到设备的计算机等）动态分配 IP 地址，则需要勾选“开启 DHCP 服务”复选框，开启设备的 DHCP 服务。

(10) 点击<确定>按钮，完成配置。

3开启接口上的 DHCP 服务

1. 配置需求

如果希望设备可以为连接到该接口的客户端（如连接到设备的计算机等）动态分配 IP 地址，则需要开启指定接口上的 DHCP 服务。

2. 注意事项

接口上指定的地址池的地址范围不能与设备上 WAN 口的 IP 地址网段包含相同的 IP 地址。

3. 配置步骤

(1) 单击导航树中[网络配置/LAN 配置]菜单项，进入 LAN 配置页面。

(2) 单击“LAN 配置”页签，进入 LAN 接口配置页面。

(3) 在接口列表中，单击指定接口上“操作”区段的“修改”按钮，进入修改接口配置页面。

(4) 单击“开启 DHCP 服务”配置项。

(5) 在“地址池起始地址”和“地址池结束地址”配置项处，设置设备可分配给客户端的 IP 地址范围。

(6) 在“排除地址”配置项处，设置不能分配给客户端的 IP 地址。

如果地址池范围内的某些 IP 地址（如网关地址）不能分配给客户端，就需要将其配置为排除地址。

(7) 在“网关地址”和“DNS1”以及“DNS2”配置项处，输入客户端的网关地址和 DNS 服务器地址。

(8) 在“地址租约”配置项处，以分钟为单位设置 IP 地址的使用时间，比如设置 IP 地址租约为 5 天，则输入 7200。

(9) 点击<确定>按钮，完成配置。

4配置静态 DHCP

1. 配置需求

如果需要为某些客户端分配固定的 IP 地址，则需要配置静态 DHCP 将客户端的硬件地址与 IP 地址进行绑定。

2. 注意事项

静态绑定的客户端 IP 地址不能是设备上 WAN 口的 IP 地址网段包含的 IP 地址。

3. 配置准备

在任何一个接口上开启 DHCP 服务。如果仅需要使用静态 DHCP 方式分配 IP 地址，则还需要删除该接口上的 DHCP 参数配置。

4. 配置步骤

(1) 单击导航树中[网络配置/LAN 配置]菜单项，进入 LAN 配置页面。

(2) 单击“静态 DHCP”页签，进入静态 DHCP 配置页面。

(3) 点击<添加>按钮，进入新增 DHCP 静态绑定关系配置页面。

(4) 在“接口”配置项处，点击下拉单选择开启 DHCP 服务器功能的接口。

(5) 在“客户端 MAC”配置项处，输入客户端的 MAC 地址。对于 PC 类型的客户端，可以在网卡信息中查询到 MAC 地址；对于设备类型的客户端，可以通过 display interface 命令查询接口的 MAC 地址。

(6) 在“客户端 IP”配置项处，输入要分配给客户端的 IP 地址。

(7) 点击<确定>按钮，完成配置。

5配置 VLAN

1. 配置需求

需要将设备上的 LAN 接口加入指定的 VLAN，使得局域网内处于同一 VLAN 的主机能直接互通，处于不同 VLAN 的主机不能直接互通。

2. 注意事项

在端口详细配置页面配置端口的 PVID 时，只能指定已创建的 VLAN。

提示

PVID（Port VLAN ID，端口的缺省 VLAN）：当端口收到未携带 VLAN Tag 的报文时，即认为此报文所属的 VLAN 为端口的缺省 VLAN。

---

3. 配置准备

规划设备上 LAN 接口所属的 VLAN，并在 LAN 接口配置页面上，创建对应的 VLAN 接口。

4. 配置步骤

(1) 单击导航树中[网络配置/LAN 配置]菜单项，进入 LAN 配置页面。

(2) 单击“VLAN 划分”页签，进入 VLAN 划分页面。

(3) 在端口列表中，单击指定端口上“操作”区段的“修改”按钮，进入详细端口配置页面。

(4) 单击在 PVID 配置项处的下拉框，修改端口的 PVID。

(5) 配置端口加入或移除 VLAN：

- 单击待选 VLAN 下方的 VLAN 编号可以将端口加入该 VLAN，或通过待选 VLAN 下方的向右方向按钮将端口加入当前所有的待选 VLAN 中。
- 单击已选 VLAN 下方的 VLAN 编号可以将端口移除该 VLAN，或通过已选 VLAN 下方的向左方向按钮将端口从所有已加入的 VLAN 中移除。

(6) 点击<确定>按钮，完成配置。

NAT配置

本章节介绍 NAT 的相关内容，包括：

1简介

NAT（Network Address Translation，网络地址转换）是一种将内部网络私有 IP 地址，转换成公网 IP 地址的技术。拥有私有 IP 地址的内网用户无法直接访问 Internet，如果希望内网用户使用运营商提供的公网 IP 访问外网，或者允许外网用户使用公网 IP 访问内网资源，则需要配置 NAT。

NAT 支持如下两种地址转换方式：

- 端口映射：通过这种转换方式，可以实现利用一个公网地址和不同的协议端口同时对外网提供多个内网服务器（例如 Web\Mail\FTP 服务器）资源的目的。这种方式可以节约设备的公网 IP 地址资源。端口映射可以将内网中的一组 IP 地址和不同的协议端口映射到一个公网 IP 地址和对应的协议端口上，使得一个公网 IP 地址可以同时分配给多个内网 IP 地址使用。
- 一对一映射：这种方式适用于内外网之间存在固定访问需求的环境，比如某个网络管理员必须使用一个固定的外网 IP 去远程访问位于内网中对外提供服务的设备。一对一映射可以在设备上建立一个固定的一对一的映射关系，将内网中的一个私有 IP 地址转换为一个公网 IP 地址。

NAT 还提供如下高级功能：

- NAT hairpin：如果您的某些内网服务器通过公网 IP 地址对外提供服务，同时内网用户也有访问这些服务器的需求，为了确保这些内网用户访问内网服务器的流量也经过网关控制，则可以开启 NAT hairpin 功能。开启该功能后，内网用户将与外网用户一样，都可以使用公网 IP 地址访问内网服务器。
- NAT ALG：如果内部网络与外部网络之间存在应用层业务，例如 FTP/DNS，为了保证这些应用层协议的数据连接经过端口映射或一对一映射后还可以正确建立，就需要开启相应协议的 NAT ALG 功能。

2配置端口映射

(1) 单击导航树中[网络配置/NAT 配置]菜单项，进入 NAT 配置页面。

(2) 单击“端口映射”页签，进入端口映射配置页面。

(3) 点击<添加>按钮，进入添加 NAT 端口映射页面。

(4) 在“接口”配置项处，选择用于连接 Internet 的端口。

(5) 在“协议类型”配置项处，选择协议为“TCP”或“UDP”。

此处需要根据内部服务器采用的传输层协议类型选择 TCP 或 UDP，比如 FTP 服务器采用 TCP 协议，TFTP 采用 UDP 协议。

(6) 在“外部地址”配置项处，可以选择使用当前端口的 IP 地址，也可以使用设备上的其它公网 IP 地址。

(7) 在“外部端口”配置项处，选择 FTP、Telnet 或自定义端口。

如果您对外提供的服务不是 FTP 或 Telnet，请输入提供的服务所使用的端口号，比如 HTTP 服务端口号 80。

(8) 在“内部地址”配置项处，输入允许外部网络访问的内网 IP 地址。

(9) 在“内部端口”配置项处，输入内部网络资源使用的端口号。

(10) 点击<确定>按钮，完成配置。

3配置一对一映射

1. 注意事项

如果设备上仅有一个公网 IP 地址，不建议配置一对一映射来占用公网 IP 地址。

2. 配置步骤

(1) 单击导航树中[网络配置/NAT 配置]菜单项，进入 NAT 配置页面。

(2) 单击“一对一映射”页签，进入一对一映射配置页面。

(3) 点击<添加>按钮，进入添加 NAT 一对一映射页面。

(4) 在“内部地址”配置项处，输入内网 IP 地址。

(5) 在“外部地址”配置项处，输入拥有的公网 IP 地址。

(6) 点击<确定>按钮，完成配置。

(7) 在一对一映射配置页面上，开启一对一映射功能。

4配置 NAT hairpin

1. 配置准备

在配置 NAT hairping 前，需要完成如下配置中的一项或多项：

- 在端口映射配置页面上，配置内网服务器的 IP 地址/端口与公网 IP 地址/端口的映射关系。
- 在一对一映射配置页面上，配置内网用户 IP 地址与公网 IP 地址的映射关系。

2. 配置步骤

(1) 单击导航树中[网络配置/NAT 配置]菜单项，进入 NAT 配置页面。

(2) 完成“端口映射”或“一对一映射”的配置。

(3) 单击“高级配置”页签，进入高级配置页面。

(4) 开启 NAT hairpin 功能。

(5) 点击<应用>按钮，完成配置。

5配置 NAT ALG

(1) 单击导航树中[网络配置/NAT 配置]菜单项，进入 NAT 配置页面。

(2) 单击“高级配置”页签，进入高级配置页面。

(3) 启用指定协议的 NAT ALG 功能。

(4) 点击<应用>按钮，完成配置。

Mini AP 管理设置

AP管理设置

本章节介绍 AP 管理设置的相关内容，包括：

1简介

您可通过开启 AP 管理功能，集中管理不同 VLAN 下接入的 AP 设备。

2注意事项

AP 管理功能的默认管理 VLAN 为 VLAN1，如需选择其他 VLAN，请先单击导航树中的[网络设置]菜单项，进入 LAN 配置页面进行配置。

3配置步骤

(1) 单击导航树中[MiniAP 管理/AP 管理设置]菜单项，进入 AP 管理设置配置页面。

(2) 在“AP 管理功能”配置项处，选择“启用”。

(3) 在“AP 管理使用 VLAN”配置项处，选择设备需要管理的 VLAN。

(4) 点击<确定>按钮，开启 AP 管理设置服务。

在线AP管理

本章节介绍在线 AP 管理的相关内容，包括：

1简介

您可通过在线 AP 管理功能查看已上线的 AP 设备和客户端。本页面显示 AP 设备与客户端的详细信息，支持管理客户端的上线状态。用户可使用在线 AP 管理功能，选择 AP 绑定的服务模板，手动升级 AP 版本或 AP 同步 AC 下发的配置。

2在线 AP 列表

1. 注意事项

- 使用版本升级功能之前，请先将 AP 升级需要使用的软件版本上传到设备中。具体操作步骤，请单击导航树中[MiniAP 管理/版本管理]菜单项，进入版本管理页面进行相关配置。

- 未开启“强制 AP 和管理器上的版本一致”功能时，版本升级功能仅用于 AP 设备从低版本到高版本的升级操作。

2. 配置步骤

(1) 单击导航树中[MiniAP 管理/在线 AP 管理]菜单项，进入在线 AP 管理页面。

(2) 单击“在线 AP 列表”页签，进入在线 AP 列表页面。

(3) 在关键字自动查询配置项处，输入待查询 AP 设备的关键字，页面会自动显示出与关键字相关的 AP 设备列表。

(4) 单击“高级查询”按钮，进入高级查询配置页面，本页面可设定与 AP 设备相关的多个筛选条目，点击<查询>按钮，完成查询。

(5) 点击<刷新>按钮，完成在线 AP 列表的刷新。

(6) 在“自动刷新”配置项处，您可设置在线 AP 列表自动刷新的时间。

(7) 勾选 AP 型号前的复选框，可进行如下功能配置：

- 点击<绑定配置模板>按钮，选择 AP 绑定的服务模板。
- 点击<版本升级>按钮，AC 下发软件版本并升级该 AP 设备。
- 点击<配置同步>按钮，手动触发 AP 同步 AC 下发的配置。
- 点击<删除离线记录>按钮，删除离线设备的状态显示项。
- 点击<重启>按钮，重启 AP 设备。

(8) 在“每页显示”配置项处，设置当前显示页面的 AP 数据条数。

3客户端列表

1. 配置步骤

(1) 单击导航树中[MiniAP 管理/在线 AP 管理]菜单项，进入在线 AP 管理页面。

(2) 单击“客户端列表”页签，进入客户端列表配置页面。

(3) 在关键字自动查询配置项处，输入待查询客户端的关键字，页面会自动显示出与关键字相关的客户端列表。

(4) 单击<高级查询>按钮，进入高级查询配置页面，本页面可设定与客户端相关的多个筛选条目，点击<查询>按钮，完成查询。

(5) 点击<刷新>按钮，完成在线客户端列表的刷新。

(6) 在“自动刷新”配置项处，设置在线客户端列表自动刷新的时间。

(7) 勾选客户端前的复选框，点击<释放>按钮，断开客户端与无线服务的连接。

配置管理

本章节介绍 MiniAP 配置管理的相关内容，包括：

1简介

在无线网络覆盖的区域，当您需要使用无线接入的方式接入无线网络，请先使用配置管理功能进行无线基本配置，如配置无线服务模板，绑定服务模板等，使网络联通。

2无线基本配置

1. 注意事项

- 无线基本配置页面只提供 default 模板中 SSID-1、5G-SSID-1 的设置，如需配置其他服务模板，请进入配置模板管理进行配置。
- 修改服务模板中的加密方式、共享配置密钥等无线服务属性后，如 AP 中的配置未自动同步，需要手动点击<配置同步>按钮，将配置下发到 AP 设备。如需使用<配置同步>功能，请参考“在线 AP 管理”的联机章节。
- 配置无线服务模板时，需要同时配置 2.4G 与 5G 无线网络的相关参数信息。

2. 配置步骤

(1) 单击导航树中[MiniAP 管理/配置管理]菜单项，进入配置管理页面。

(2) 单击“无线基本配置”页签，进入无线基本配置页面。

(3) 配置无线网络 SSID 设置-2.4G：

- 在“SSID-1 名称”配置项处，输入 2.4G 无线服务的 SSID 名称。
- 在“加密方式”配置项处，选择客户端是否通过加密方式连接无线服务。
  为增强无线网络的安全性，推荐您使用 WPA-PSK/WPA2-PSK 安全模式进行加密。
- 在“共享密钥”配置项处，输入无线服务密钥。
- 当您选择通过加密方式接入无线服务时，需要设置共享密钥。

(4) 配置无线网络 SSID 设置-5G：

- 在“5G-SSID-1 名称”配置项处，输入 5G 无线服务的 SSID 名称。
- 在“加密方式”配置项处，选择客户端是否通过加密方式连接无线服务。
  为增强无线网络的安全性，推荐您使用 WPA-PSK/WPA2-PSK 安全模式进行加密。
- 在“共享密钥”配置项处，输入无线服务密钥。
- 当您选择通过加密方式接入无线服务时，需要设置共享密钥。

(5) 点击<应用>按钮，完成配置。

3配置模板管理

1. 配置步骤

(1) 单击导航树中[MiniAP 管理/配置管理]菜单项，进入配置管理页面。

(2) 单击“配置模板管理”页签，进入配置模板管理页面。

(3) 点击<添加>按钮，进入添加配置模板页面。

- 在“模板名称”配置项处，输入无线服务模板的名称。
- 在“模板描述”配置项处，输入该无线服务模板的相关描述信息。

- 在“无线网络基本设置-2.4G”配置项处，选择无线网络模式、频宽、信道和发射功率等参数信息。您的配置需要符合所在国家或区域的管制要求。
  - 点击<添加>按钮，进入添加 SSID 配置页面。
  - 勾选启用 SSID 复选框，在“SSID 名称”配置项处，输入 2.4G 无线服务的 SSID 名称。
  - 在“加密方式”配置项处，选择客户端是否通过加密方式连接无线服务。

    为增强无线网络的安全性，推荐您使用 WPA-PSK/WPA2-PSK 安全模式进行加密。
  - 在“共享密钥”配置项处，输入无线服务密钥。

    当您选择通过加密方式接入无线服务时，需要设置共享密钥。
  - 在“加密协议”配置项处，选择加密机制来保护您的数据安全。
  - 在“群组密钥更新周期”配置项处，设置加密密钥更新周期。

    设置密钥更新周期可以章节您提高 WLAN 网络的安全性。
  - 当您需要进一步设置客户端接入管理的相关功能时，请勾选高级设置复选框。勾选客户端隔离功能可以开启基于 SSID 的用户隔离，用以加强用户的安全性，并且减少用户产生的大量组播、广播报文对无线空口资源的占用；关闭 SSID 广播功能时，AP 在 Beacon 帧中广播的 SSID 信息为空，可以借此保护网络免遭攻击。客户端若想连接此 BSS，则需要手工指定该 SSID；设置客户端数量可以防止 SSID 接入的客户端数量过多而过载；设置桥接 VLAN 可以将 SSID 接入的客户端划分在不同广播域中，充分利用有限的 IP 地址资源。
  - 点击<确定>按钮，完成配置。
- 在“无线网络基本设置-5G”配置项处，选择无线网络模式、频宽、信道和发射功率等参数信息。
  - 点击<添加>按钮，进入添加 SSID 配置页面。
  - 勾选启用 SSID 复选框，在“SSID 名称”配置项处，输入 5G 无线服务的 SSID 名称。
  - 在“加密方式”配置项处，选择客户端是否通过加密方式连接无线服务。

    为增强无线网络的安全性，推荐您使用 WPA-PSK/WPA2-PSK 安全模式进行加密。
  - 在“共享密钥”配置项处，输入无线服务密钥。

    当您选择通过加密方式接入无线服务时，需要设置共享密钥。
  - 在“加密协议”配置项处，选择加密机制来保护您的数据安全。
  - 在“群组密钥更新周期”配置项处，设置加密密钥更新周期。

    设置密钥更新周期可以章节您提高 WLAN 网络的安全性。
  - 当您需要进一步设置客户端接入管理的相关功能时，请勾选高级设置复选框。勾选客户端隔离功能可以开启基于 SSID 的用户隔离，用以加强用户的安全性，并且减少用户产生的大量组播、广播报文对无线空口资源的占用；关闭 SSID 广播功能时，AP 在 Beacon 帧中广播的 SSID 信息为空，可以借此保护网络免遭攻击。客户端若想连接此 BSS，则需要手工指定该 SSID；设置客户端数量可以防止 SSID 接入的客户端数量过多而过载；设置桥接 VLAN 可以将 SSID 接入的客户端划分在不同广播域中，充分利用有限的 IP 地址资源。
  - 点击<确定>按钮，完成配置。

(4) 点击<确定>按钮，完成服务模板的配置。

4AP 配置管理

1. 配置步骤

(1) 单击导航树中[MiniAP 管理/配置管理]菜单项，进入配置管理页面。

(2) 单击“AP 配置管理”页签，进入 AP 配置管理页面。

(3) 在关键字自动查询配置项处，输入待查询 AP 的关键字，页面会自动显示出与关键字相关的 AP 列表。

(4) 单击<高级查询>按钮，进入高级查询配置页面，本页面可设定与 AP 相关的多个筛选条目，点击<查询>按钮，完成查询。

(5) 点击<添加>按钮，进入添加 AP 配置模板配置模板页面。

(6) 在“MAC 地址”配置项处，输入 AP 设备的 MAC 地址。

您可通过 AP 机身查找 AP 设备的 MAC 地址。

(7) 在“备注信息”配置项处，填写配置信息。

(8) 在“模板选择”配置项处，选择 AP 需要绑定的无线服务模板。

(9) 点击<确定>按钮，完成配置。

5无线高级配置

1. 注意事项

- 若同时启用“二层漫游”与“禁止弱信号客户端接入”功能时，“禁止弱信号客户端接入”需要比“二层漫游”低，否则“二层漫游”功能不生效。
- 客户端在 AC 内进行二层漫游时，要求两个 AP 处于相同的 VLAN 中，且 AP 绑定相同的 SSID，即服务模板也保持一致。

2. 配置步骤

(1) 单击导航树中[MiniAP 管理/配置管理]菜单项，进入配置管理页面。

(2) 单击“无线高级配置”页签，进入无线高级配置管理页面。您可视实际情况选择开启如下功能：

- 勾选二层漫游复选框，开启二层漫游功能。在“信号切换阀值”配置项处，输入信号切换阀值。

  WLAN 客户端从一个 AP 上接入转移到另一个 AP 上接入的过程称为漫游。在漫游期间，客户端的 IP 地址、授权信息等维持不变。开启“二层漫游”功能时，低于“信号切换阀值”的客户端会进行信号切换。
- 勾选禁止弱信号客户端接入复选框，在“禁止接入信号强度”配置项处，设置信号强度，低于“禁止接入信号强度”的客户端将无法接入无线网络。
- 勾选关闭广播探测复选框，该功能开启后，部分客户端无法扫描到本设备下挂 AP 的 SSID。

(3) 点击<确定>按钮，完成配置。

版本管理

本章节介绍版本管理的相关内容，包括：

- 简介

1简介

版本管理功能可以章节您升级 AP 的软件版本或者强制 AP 同步管理器上的软件版本。

2AP 版本上传

1. 注意事项

- AP 断电重连后会自动同步设备管理器中的软件版本。
- 升级 AP 的软件版本时，如果设备管理器中待升级的软件版本高于 AP 的软件版本，AP 会自动升级软件版本；反之，则需要开启“强制 AP 和管理器上的版本一致”，AP 才能自动升级到该软件版本。

2. 配置步骤

(1) 单击导航树中[MiniAP 管理/版本管理]菜单项，进入版本管理配置页面。

(2) 单击“AP 版本上传”页签，进入 AP 版本上传配置页面。

(3) 点击<选择文件>按钮，访问待升级的 AP 软件版本存放路径，选中版本文件，点击确定。

(4) 点击<上传>按钮，将待升级的 AP 软件版本上传到设备中。

(5) 点击版本文件右侧的<删除>按钮，点击<确认>，即可删除设备中的版本文件。

3AP 升级管理

1. 配置步骤

(1) 单击导航树中[MiniAP 管理/版本管理]菜单项，进入版本管理配置页面。

(2) 单击“AP 升级管理”页签，进入 AP 升级管理页面。

(3) 点击按钮并向右滑动，“开启强制 AP 和管理器上的版本一致”功能。

当设备管理器中待升级的软件版本低于 AP 的软件版本时，需要开启“强制 AP 和管理器上的版本一致”，AP 才能自动升级到该软件版本。

高级管理

本章节介绍 MiniAP 高级管理的相关内容，包括：

1简介

如果您想通过 Web 页面登陆 AP 设备，可通过高级管理功能统一设置下挂 AP 的 Web 页面登陆密码。

2注意事项

终端连接 AP 设备后单独设置的登录密码优先级高于 AC 统一下发的登录密码配置。

3配置步骤

(1) 单击导航树中[MiniAP 管理/高级管理]菜单项，进入高级管理配置页面。

(2) 勾选启用 AP 密码设置功能（手动设置 AP 密码），在“新密码”配置项处，输入新密码，在“确认密码”配置项处，再次输入新密码。在“密码提示”配置项处，输入密码提示信息。

(3) 点击<确认>按钮，完成配置。

上网行为管理

用户组

本章节介绍用户组的相关内容，包括：

1简介

用户组是一组用户主机名或 IP 地址的集合。每个用户组中可以添加若干成员，成员的类型包括主机名、IP 地址以及 IP 地址段。如果您的某些业务（例如带宽管理）需要使用用户组来识别用户报文，则需要提前配置符合业务需求的用户组。

2注意事项

- 添加到用户组中的 IP 地址只支持 IPv4 地址格式，不支持 IPv6 地址格式。
- 添加到用户组中的 IP 地址段的起始地址必须小于结束地址。

3配置步骤

(1) 单击导航树中[上网行为管理/用户组]菜单项，进入用户组配置页面。

(2) 点击<添加>按钮，进入新建用户组页面。

(3) 在“用户组名称”配置项处，输入用户组的名称。

(4) 在“描述信息”配置项处，输入用户组的描述信息。

(5) 配置用户组内容：

- 配置添加到用户组的主机名。
- 配置添加到用户组的单个 IP 地址。
- 配置添加到用户组 IP 地址段的起始 IP 地址及结束 IP 地址。
- 配置用户组排除的 IP 地址。

(6) 点击配置项右侧的<→>按钮，提交配置的用户组内容。

(7) 重复(5)、(6)步骤可完成多个同类型成员的添加。

(8) 点击<确定>按钮，完成新建用户组。

时间组

本章节介绍时间组的相关内容，包括：

1简介

如果您希望设备上的某些功能（例如带宽管理、上网行为管理）仅在特定时间生效，而其他时间不生效，可以创建一个时间组，并在配置相关功能时引用时间组。

一个时间组中可以配置一个或多个时间段。时间段的生效时间有如下两种方式：

- 周期性生效：以周作为周期，循环生效。例如，每周一的 8 至 12 点。
- 非周期生效：在指定的时间范围内生效。例如，2015 年 1 月 1 日 8 点至 2015 年 1 月 3 日 18 点。

如果一个时间组中配置了多个周期性生效和非周期生效的时间段，设备将取所有周期性生效时间段的并集和所有非周期生效时间段的并集，再取这两个并集的交集作为该时间组最终的生效时间。

例如，对名称为 test 的时间组配置如下时间段：

- 周期性生效的时间段为每周一至周五：
  - 上午 08：30～12：00；
  - 下午 13：30～18：00；
- 非周期时间段为 2019 年 4 月 1 日至 2019 年 4 月 30 日：
  - 上午 10：00～12：00；
  - 下午 14：00～16：00。

则该时间组在 2019 年 4 月份每周一至周五的上午 10 点至 12 点和下午 14 点至 16 点生效。

2注意事项

- 您最多可以创建 1024 个不同名称的时间组。
- 对于同一个时间组，不可以使用命令行和 web 页面混合配置。
- 一个时间组内最多可以配置 32 个周期性生效的时间段和 12 个非周期生效的时间段。

3配置步骤

如果您想创建一个仅含有周期性生效时间段的时间组，或一个仅含有非周期生效时间段的时间组，请按照如下配置步骤操作。

(1) 单击导航树中[上网行为管理/时间组]菜单项，进入时间组配置页面。

(2) 点击<添加>按钮，进入新建时间组页面。

(3) 在“时间组名称”配置项处，输入时间组的名称。

(4) 在“生效时间”配置项处，选择“周期性生效”或“非周期生效”，配置时间段。请选择其中一项进行配置。

- 周期性生效

  点选每周需要生效的具体天数，并在下面输入每天的具体生效时间，点击<加号>按钮，完成本时间段的配置。

- 非周期生效

  选择生效的起止日期，并在下面输入具体生效的起止时间，点击<加号>按钮，完成本时间段的配置。

(5) 点击<确定>按钮，完成时间组创建。

如果您想创建一个同时含有周期性生效时间段和非周期生效时间段的时间组，请按照如下配置步骤操作。

(6) 单击导航树中[上网行为管理/时间组]菜单项，进入时间组配置页面。

(7) 点击<添加>按钮，进入新建时间组页面。

(8) 在“时间组名称”配置项处，输入时间组的名称。

(9) 在“生效时间”配置项处，选择“周期性生效”。

(10) 点选每周需要生效的具体天数，并在下面输入每天的具体生效时间，点击<加号>按钮，完成本时间段的配置。

(11) 在“生效时间”配置项处，选择“非周期生效”。

(12) 选择生效的起止日期，并在下面输入具体生效的起止时间，点击<加号>按钮，完成本时间段的配置。

(13) 点击<确定>按钮，完成时间组创建。

如果您想将一个同时含有周期性生效时间段和非周期生效时间段的时间组，修改成一个只含有一种生效方式的时间组，请按照如下配置步骤操作。

(14) 单击导航树中[上网行为管理/时间组]菜单项，进入时间组配置页面。

(15) 在指定时间组的“操作”区段上，单击<编辑>按钮，进入修改时间组页面。

(16) 在“生效时间”配置项处，选择想删除的生效方式：“周期性生效”或“非周期生效”。

(17) 依次点击具体生效时间后面的<删除>按钮，删除所有的具体生效时间。

(18) 单击<确定>按钮，完成时间组的修改。

上网行为管理

本章节介绍上网行为管理的相关内容，包括：

1简介

上网行为管理功能是指对用户访问的应用以及网址进行控制，并可以配置用户组和时间段等限制条件对用户的上网行为进行更精细的控制。

2配置上网行为管理策略

1. 注意事项

因为网址过滤功能基于 HTTP 协议进行识别，所以设备上不应该阻断 HTTP 协议流量，即在应用控制功能中不能阻断 HTTP 协议，否则将影响设备对网址的识别，导致网址过滤功能不生效。

2. 配置步骤

(1) 单击导航树中[上网行为管理/上网行为管理]菜单项，进入上网行为管理配置页面。

(2) 在“上网行为管理策略”页签下，点击<添加>按钮，进入新建上网行为管理策略页面。

- 在“策略名”配置项处，配置上网行为管理策略名。
- 在“用户范围”配置项处，选择用户组。
- 在“限制时段”配置项处，选择时间组。
- 在“网址控制”配置项处，进行如下配置：
  - 选择网址分类：包括预定义和自定义网址分类，自定义网址分类的配置步骤请参见“配置自定义网址分类”。
  - 配置网址控制动作：对所选的网址分类执行的动作，包括放行和阻断。配置以上任何一个动作时，也可同时配置记录动作，对放行和阻断行为进行记录。
- 在“应用控制”配置项处，点击“选择网络应用”右侧的<详情>按钮，选择应用，并配置对该应用的访问执行的动作，包括如下：
  - 阻断：阻断对应用的访问。
  - 不阻断不限速：不对应用的访问进行限制。
  - 限速：对应用的访问进行限速，并通过点击右侧的<编辑>按钮，分别配置上下行最大带宽。

(3) 点击<确定>按钮，完成新建上网行为管理策略。

(4) 在上网行为管理页面，选择“全局控制”页签，点击<开启上网行为管理>按钮，使新建的上网行为管理策略生效。

3配置网址黑/白名单

1. 配置需求

当用户需要对指定的网址进行放行或阻断时，可通过开启 Web 白名单或黑名单实现。

2. 配置步骤

(1) 单击导航树中[上网行为管理/上网行为管理]菜单项，进入上网行为管理配置页面。

(2) 在“网址黑白名单”页签下，点击<启用 web 黑名单>或<启用 web 白名单>按钮，在网址关键字配置项中，输入网址。

(3) 点击右侧的<+>按钮，逐一添加网址。

(4) 点击<应用>按钮，完成 web 黑名单或白名单的配置。

4配置自定义网址分类

1. 配置需求

当设备已有的网址分类不能满足用户需求时，可通过自定义网址分类的方式按需添加网址。

2. 注意事项

自定义网址支持导出功能，当使用 IE 浏览器进行导出时，如果出现无法启动 Excel 的错误提示，请参考如下步骤修改浏览器配置：

单击浏览器的<工具>按钮，选择“Internet 选项”，进入 Internet 选项窗口；选择“安全”页签，单击<自定义级别>按钮，找到“对为标记为可安全执行脚本的 ActiveX 控件初始化并执行脚本”一项，选择“启用”。

3. 配置步骤

(1) 单击导航树中[上网行为管理/上网行为管理]菜单项，进入上网行为管理配置页面。

(2) 在“自定义网址”页签下，新建网址分类。

(3) 在默认网址分类下方的输入框中，配置新建网址分类的名称，点击右侧<+>按钮，新建一个空的网址分类成功，点击<编辑>按钮，进入设置网址关键字页面，向新建的网址分类中添加网址。

(4) 在“网址关键字”输入框中，配置网址，点击右侧的<+>按钮，逐条添加网址。

(5) 添加网址后，点击<确定>按钮，完成新建自定义网址分类。

审计日志

本章节介绍审计日志的相关内容，包括：

1简介

审计日志包括应用审计日志和网址控制日志，是上网行为管理功能的应用控制和网址控制产生的日志信息。日志内容包括用户的 IP 地址或用户名、访问的应用、访问的网址以及设备对访问行为执行的动作等，方便管理员对用户的上网行为进行分析与审计。

2配置步骤

(1) 单击导航树中[上网行为管理/审计日志]菜单项，进入审计日志页面。

(2) 在“应用审计日志”页签下，点击<开启日志>按钮。将同时开启应用控制和网址控制日志的显示功能，用户可通过切换“应用审计日志”页签和“网址过滤日志”页签，分别查看相应的日志信息。

(3) 在“应用审计日志”页签下，点击<关闭日志>按钮，将同时关闭应用控制和网址控制日志的显示功能，已生成的日志不会被删除，用户可通过点击<开启日志>按钮再次开启日志显示功能。

特征库管理

本章节介绍上网行为管理的相关内容，包括：

1简介

特征库是用来识别应用或网址的特征的集合，包括应用特征库和网址特征库。管理员需要及时更新设备中的特征库，对用户的上网行为进行更好的管理。

设备提供如下升级方式：

- 本地升级：管理员先手工从设备的官方网站获取最新的特征库，再导入到设备中进行升级。
- 在线升级：管理员触发在线升级功能后，设备自动从设备的官方网站获取最新的特征库文件，并自动导入设备中进行升级。

2注意事项

- 更新特征库时，请确保 License 已正确安装，并处于生效状态。
- 当系统内存处于告警门限状态时，请勿进行特征库更新，否则易导致设备特征库更新失败，进而影响上网行为管理功能的正常使用。
- 在线更新特征库时，需要确保设备能通过静态或动态域名解析方式获得官方网站的 IP 地址，并与之路由可达，否则设备更新特征库会失败。

3本地更新特征库

1. 配置步骤

(1) 单击导航树中[上网行为管理/特征库管理]菜单项，进入特征库管理页面。

(2) 在“应用特征库”或“网址特征库”页签下，点击<本地更新特征库>按钮，进入应用特征导入页面。

(3) 点击<选择文件>按钮，选择特征库文件。

(4) 点击<确定>按钮，完成本地更新特征库。

4在线更新特征库

1. 配置步骤

(1) 单击导航树中[上网行为管理/特征库管理]菜单项，进入特征库管理页面。

(2) 在“应用特征库”或“网址特征库”页签下，点击<在线更新特征库>按钮，完成在线更新特征库。

带宽管理

本章节介绍带宽管理的相关内容，包括：

1简介

带宽管理功能用于对流量进行限速，用户可基于用户组和时间段等限制条件对流量进行精细控制。对于需要保证时延的交互性应用流量，可通过启用绿色专用通道功能来保证带宽。

2配置带宽限速

1. 配置步骤

(1) 单击导航树中[上网行为管理/带宽管理]菜单项，进入带宽管理配置页面。

(2) 在“带宽限速”页签下，点击<添加>按钮，进入新建带宽策略页面。

- 在“应用接口”配置项处，选择接口，设备将基于该接口进行带宽管理。
- 在“用户范围”配置项处，选择用户组，设备将仅对该用户组内的成员进行带宽管理。
- 在“流量限制”配置项处，分别配置上传带宽、下载带宽和流量分配方式。若不配置上传或下载中任意一个方向的带宽值，则表示不对该方向的带宽进行限速。

  流量分配方式包括如下类型：

  – 共享式：分配的带宽为总带宽，由所有用户平均分配。

  – 独占式：分配的带宽为单用户的带宽，由单用户独享。
- 在“限制时段”配置项处，选择时间组。

(3) 点击<确定>按钮，完成新建带宽策略。

3配置绿色通道

1. 注意事项

请勿将绿色通道带宽设置过大，以免对普通流量产生影响。

2. 配置步骤

(1) 单击导航树中[上网行为管理/带宽管理]菜单项，进入带宽管理配置页面。

(2) 单击“绿色通道”页签，进入绿色通道配置页面。

(3) 勾选“启用绿色专用通道”复选框，开启带宽管理的绿色通道功能。

(4) 对于需要保证时延的交互性应用流量，需要用户根据实际情况自行配置应用的协议和端口号。只有匹配应用的流量才能进入绿色通道传输，具体配置步骤如下：

- 勾选“自定义应用端口匹配绿色通道”复选框，点击自定义应用端口配置项右侧的<添加>按钮，进入新建界面，配置应用名称、应用协议和端口号。
- 点击<确定>按钮，完成新建自定义应用。

(5) 配置绿色通道中需要传输的应用后，还可以针对通道中所有应用进行如下限制：

- 如果还希望对绿色通道中的流速上限进行限制，则需要勾选“限制绿色通道流速上限”复选框，并配置最大流速。
- 如果还希望对绿色通道中传输的数据包长度进行限制，则需要勾选“匹配绿色通道数据包长度”复选框，并配置数据包的最大长度。超过最大长度的数据包不会进入绿色通道传输。

(6) 点击<应用>按钮，完成绿色通道的配置。

网络安全

ARP攻击防御

本章节介绍 ARP 攻击防御的相关内容，包括：

1简介

ARP 协议本身存在缺陷，攻击者可以轻易地利用 ARP 协议的缺陷对其进行攻击。ARP 攻击防御技术提供了多种 ARP 攻击防御技术对局域网中的 ARP 攻击和 ARP 病毒进行防范、检测和解决。

ARP 攻击防御功能包括：

- 动态 ARP 表项学习：本功能支持开启和关闭接口的动态 ARP 表项学习功能，当执行关闭接口的动态 ARP 表项学习功能后，该接口无法再学习新的动态 ARP 表项，提高了安全性。当设备的某个接口已经学到了该接口下所有合法用户的 ARP 表项时，建议关闭动态 ARP 表项学习功能。
- 动态 ARP 管理：包括动态 ARP 表项管理功能和 ARP 扫描、固化功能。ARP 扫描、固化功能即对局域网内的用户进行自动扫描，并将生成的动态 ARP 表项固化为静态 ARP 表项。建议环境稳定的小型网络（如网吧）中配置本功能。先配置 ARP 扫描、固化功能，再关闭动态 ARP 表项学习功能，可以防止设备学习到错误的 ARP 表项。
- 攻击防御管理：包括静态 ARP 表项管理功能和仅允许 ARP 静态表项对应的用户访问外网功能。先配置 ARP 扫描、固化功能，再配置仅允许 ARP 静态表项对应的用户访问外网功能，可以防止攻击用户访问外网。

2动态 ARP 表项学习

(1) 单击导航树中[网络安全/ARP 攻击防御]菜单项，进入 ARP 攻击防御配置页面。

(2) 单击“动态 ARP 表项学习”页签，进入动态 ARP 表项学习配置页面。

(3) 在接口的“ARP 学习”项，设置是否允许学习动态 ARP 表项：

- 点击<开启>按钮，则该接口允许学习动态 ARP 表项；
- 点击<关闭>按钮，则该接口不允许学习动态 ARP 表项。

3动态 ARP 管理

(1) 单击导航树中[网络安全/ARP 攻击防御]菜单项，进入 ARP 攻击防御配置页面。

(2) 单击“动态 ARP 管理”页签，进入动态 ARP 表项管理配置页面。

(3) 可对已有的动态 ARP 表项执行以下管理操作：

- 点击<刷新>按钮，则可以刷新当前动态 ARP 表项的显示信息。

- 点击<清除>按钮，则可以清除当前显示的所有动态 ARP 表项。
- 选择指定的动态 ARP 表项，点击<删除>按钮，再点击<确定>按钮后，可以删除对应的动态 ARP 表项。

(4) 可对已有的动态 ARP 表项执行以下管理操作：

a. 点击<扫描>按钮，进入扫描配置页面。

b. 在“接口”配置项处，选择需要执行 ARP 扫描操作的接口。

c. 在“开始 IP 地址”和“结束 IP 地址”配置项处，设置 ARP 扫描操作的起止 IP 地址。此处指定起止 IP 地址需要和接口的 IP 地址处于同一网段。

d. 选择“对已存在 ARP 表项的 IP 地址也进行扫描”后，ARP 扫描功能会对开始 IP 地址和结束 IP 地址中的所有 IP 地址进行扫描，不会区分是否已存在 ARP 表项。

e. 选择指定的动态 ARP 表项，再点击<固化>按钮，则可以将这些动态 ARP 表项固化为静态 ARP 表项。

4攻击防御管理

1. 配置限制和指导

需要保证管理客户端的 ARP 表项是静态 ARP 表项，否则管理客户端可能无法工作。

2. 配置准备

如果需要执行批量添加静态 ARP 表项操作，还需要提前将记录静态 ARP 表项的文件保存在本地，然后再执行静态 ARP 表项的导入操作。建议通过 Web 页面导出一个 ARP 表项文件，在该文件中批量添加静态 ARP 表项后，再使用它进行导入操作。

3. 配置步骤

(1) 单击导航树中[网络安全/ARP 攻击防御]菜单项，进入 ARP 攻击防御配置页面。

(2) 单击“攻击防御管理”页签，进入攻击防御管理配置页面。

(3) 选择“仅允许 ARP 静态绑定的客户访问外网”，则只有静态 ARP 表项对应的客户可以访问外网，动态 ARP 表项对应的客户无法访问外网。选择“不限制”，则静态 ARP 表项和动态 ARP 表项对应的客户都能访问外网。

(4) 可对静态 ARP 表项执行以下管理操作：

- 点击<刷新>按钮，则可以刷新当前静态 ARP 表项的显示信息。
- 点击<导入>按钮，则可以批量导入静态 ARP 表项。
- 点击<导出>按钮，则可以批量导出静态 ARP 表项到文件中。
- 点击<添加>按钮，进入“添加 ARP 表项”页面。在“添加 ARP 表项”页面，输入静态 ARP 表项的 IP 地址和 MAC 地址，点击“确定”按钮，静态 ARP 表项添加成功。
- 选择指定的静态 ARP 表项，点击<删除>按钮，再点击<确定>按钮后，可以删除对应的静态 ARP 表项。

MAC地址过滤

本章节介绍 MAC 地址过滤的相关内容，包括：

1简介

如果您希望对某些设备发送过来的报文进行限制（允许或禁止其通过），则可以在三层接口上配置 MAC 地址过滤功能，本功能将根据接收报文的源 MAC 地址对其过滤。

配置方式有如下两种：

- 白名单：允许源 MAC 地址在白名单内的报文通过，其余禁止通过。
- 黑名单：禁止源 MAC 地址在黑名单内的报文通过，其余允许通过。

2注意事项

如果您想在管理员终端连接的接口上开启白名单方式的 MAC 地址过滤功能，请先确保管理员的终端 MAC 地址已添加到白名单中。

3配置步骤

MAC 地址过滤的配置方式有白名单和黑名单两种，下面以白名单为例进行配置步骤的讲解，黑名单的配置步骤同白名单。

(1) 单击导航树中[网络安全/MAC 地址过滤]菜单项，进入 MAC 地址过滤配置页面。

(2) 单击“MAC 过滤设置”页签，进入 MAC 过滤设置页面。

(3) 在指定接口的“过滤方式”区段上，选择“白名单”，并在“开启和关闭”区段上勾选“开启”。

(4) 点击<应用>按钮，开启 MAC 地址过滤。

(5) 单击“MAC 黑白名单管理”页签，进入 MAC 黑白名单管理设置页面。

(6) 单击“白名单”页签，进入白名单设置页面。

- 如果需要添加单个 MAC 地址，请执行以下步骤：

a. 点击<添加>按钮，进入添加源 MAC 地址页面。

b. 输入待过滤的源 MAC 地址。

c. 点击<确定>按钮，完成对白名单添加单个 MAC 地址的操作。

- 如果需要批量添加 MAC 地址，请执行以下步骤：

d. 点击<导出>按钮，选择“导出模板”。

e. 打开下载好的模板，添加待过滤的源 MAC 地址并在本地保存。

f. 点击<导入>按钮，进入导入源 MAC 地址页面。

g. 点击<选择文件>按钮，选择已编辑好的模板。

h. 点击<确定>按钮，完成对白名单批量添加 MAC 地址的操作。

防火墙

本章节介绍防火墙的相关内容，包括：

1简介

防火墙功能是通过一系列的安全规则匹配网络中的报文，并执行相应的动作，从而达到阻断非法报文传输、正常转发合法报文的目的，为用户的网络提供一道安全屏障。

2注意事项

当报文匹配到一个防火墙安全规则后，则不会继续向下匹配，所以请合理安排安全规则的优先级，避免报文匹配错误的规则而导致执行相反动作。

3配置准备

- 请提前完成外网配置页面的相关配置，才可创建防火墙安全规则。
- 若需指定防火墙安全规则的生效时间，请提前在时间组页面创建相应的时间组。

4配置步骤

(1) 单击导航树中[网络安全/防火墙]菜单项，进入防火墙配置页面。

(2) 点击<添加>按钮，进入创建安全规则页面。

(3) 在“接口”配置项处，选择应用的接口，该规则将对指定接口接收到的报文进行匹配。

(4) 在“协议”配置项处，选择该规则所匹配报文的协议类型。若需匹配某传输层协议的报文，则选择“TCP”或“UDP”；若需匹配 Ping、Tracert 等 ICMP 协议报文，则选择“ICMP”；若需匹配所有协议报文，则选择“所有协议”。

(5) 在“源 IP 地址/掩码”配置项处，配置该规则所匹配报文发送端的 IP 地址及掩码，输入“any”则代表匹配所有源 IP 地址。

(6) 在“目的 IP 地址/掩码”配置项处，配置该规则所匹配报文接收端的 IP 地址及掩码，输入“any”则代表匹配所有目的 IP 地址。

(7) 在“目的端口”配置项处，配置该规则所匹配报文的目的端口号，例如 HTTP 协议报文的目的端口号为 80。

(8) 在“规则生效时间”配置项处，选择该规则生效时间对应的时间组。

(9) 在“动作”配置项处，选择该规则所匹配报文的执行动作。

(10) 在“优先级”配置项处，选择该规则的优先级类型。

- 自动：系统自动为该规则分配优先级，即根据规则的配置顺序以 5 为步长进行依次分配。
- 自定义：用户自定义规则的优先级，数值越小则优先级越高。

(11) 在“描述”配置项处，配置该安全规则的描述信息。

(12) 点击<确定>按钮，完成创建安全规则。

DDoS攻击防御

本章节介绍 DDoS 攻击防御的相关内容，包括：

1简介

DDoS 攻击是一类广泛存在于互联网中的攻击，能造成比传统 DoS 攻击（拒绝服务攻击）更大的危害。配置本功能能让您的设备和网络免受如下 DDoS 攻击的困扰：

- 单包攻击：攻击者利用畸形报文发起攻击，旨在瘫痪目标系统。例如 Land 攻击报文是源 IP 和目的 IP 均为攻击目标 IP 的 TCP 报文，此攻击将耗尽目标服务器的连接资源，使其无法处理正常业务。
- 异常流攻击
  - 扫描攻击：攻击者对主机地址和端口进行扫描，探测目标网络拓扑以及开放的服务端口，为进一步侵入目标系统做准备。
  - 泛洪攻击：攻击者向目标系统发送大量伪造请求，导致目标系统疲于应对无用信息，从而无法为合法用户提供正常服务。

设备可防御的 DDoS 攻击包括：

- 单包攻击：Fraggle 攻击、Land 攻击、WinNuke 攻击、TCP Flag 攻击、ICMP 不可达报文攻击、ICMP 重定向报文攻击、Smurf 攻击、带源路由选项的 IP 报文攻击、带路由记录选项的 IP 报文攻击和超大 ICMP 报文攻击。
- 异常流攻击：扫描攻击、SYN flood 攻击、UDP flood 攻击和 ICMP flood 攻击。

2配置步骤

(1) 单击导航树中[网络安全/DDoS 攻击防御]菜单项，进入 DDoS 攻击防御配置页面。

(2) 单击“攻击防御”页签，进入攻击防御配置页面。

(3) 点击<添加>按钮，进入新建攻击防御页面。
  - 在“应用接口”配置项处，选择应用该 DDoS 攻击防御策略的接口。
  - 在“单包攻击防御”配置项处，选择需要开启防御的单包攻击类型。
    建议您开启全部单包攻击防御。
  - 在“异常流攻击防御”配置项处，选择需要开启防御的异常流攻击类型。
    - 启动扫描攻击防御后，可选择将源 IP 地址加入黑名单。在一定时间内，来自扫描攻击源的报文将被设备直接丢弃。被加入黑名单的 IP 地址可在黑名单管理页面查看。
    - 建议您根据网络流量类型开启对应的泛洪攻击防御。

(4) 点击<确定>按钮，完成配置。

连接限制

本章节介绍连接限制的相关内容，包括：

1简介

连接限制功能是一种安全机制，通过限制每个 IP 地址主动发起连接的个数，达到合理分配设备处理资源、防范恶意连接的效果。

如果设备发现来自某 IP 地址的 TCP 或 UDP 连接数目超过指定的数目，将禁止该连接建立。直到该连接数低于限制数时，其才被允许新建连接。

设备支持配置如下两种连接限制：

- 网络连接限制：在指定 IP 地址范围内，配置每个 IP 地址发起连接的个数限制。此方式用于对设备上的所有接口收到的连接进行控制。
- VLAN 网络连接限制：在指定 VLAN 接口上，配置每个 IP 地址发起连接的个数限制。此方式用于对指定 VLAN 接口收到的连接进行控制。

2配置网络连接限制数

(1) 单击导航树中[安全管理/连接限制]菜单项，进入连接限制配置页面。

(2) 单击“网络连接限制数”页签。

(3) 勾选“开启网络连接限制数”选项，进入网络连接限制数配置页面。

(4) 点击<添加>按钮，进入新建网络连接限制数规则页面。

(5) 在“起始 IP 地址”配置项处，输入地址范围的起始 IP 地址。

(6) 在“结束 IP 地址”配置项处，输入地址范围的结束 IP 地址。

(7) 在“每 IP 总连接数上限”配置项处，输入每个 IP 地址所允许发起连接的总个数上限。
相同源 IP，源端口、目的 IP、目的端口或报文协议不完全相同的连接均属于不同的连接。

(8) 在“每 IP TCP 连接数上限”配置项处，输入每个 IP 地址所允许发起的 TCP 连接的个数上限。您可以在上面设置的总连接限制数下，对 TCP 连接数进行单独限制。

(9) 在“每 IP UDP 连接数上限”配置项处，输入每个 IP 地址所允许发起的 UDP 连接的个数上限。您可以在上面设置的总连接限制数下，对 UDP 连接数进行单独限制。

(10) 在“描述”配置项处，输入规则描述信息。

(11) 点击<确定>按钮，完成配置。

3配置 VLAN 网络连接限制数

(1) 单击导航树中[安全管理/连接限制]菜单项，进入连接限制配置页面。

(2) 单击“VLAN 网络连接限制数”页签。

(3) 点击<添加>按钮，进入新建 VLAN 网络连接限制数规则页面。

(4) 在“VLAN 接口”下拉菜单处，选择应用此规则的 VLAN 接口。

(5) 选择“启动连接限制功能”选项。

(6) 在“每 IP 总连接数上限”配置项处，输入每个 IP 地址所允许发起连接的总个数上限。
相同源 IP，源端口、目的 IP、目的端口或报文协议不完全相同的连接均属于不同的连接。

(7) 在“每 IP TCP 连接数上限”配置项处，输入每个 IP 地址所允许发起的 TCP 连接的个数上限。您可以在上面设置的总连接限制数下，对 TCP 连接数进行单独限制。

(8) 在“每 IP UDP 连接数上限”配置项处，输入每个 IP 地址所允许发起的 UDP 连接的个数上限。您可以在上面设置的总连接限制数下，对 UDP 连接数进行单独限制。

(9) 在“描述”配置项处，输入规则描述信息。

(10) 点击<确定>按钮，完成配置。

虚拟网络

IPsec VPN

本章节介绍 IPsec VPN 的相关内容，包括：

1简介

IPsec VPN 是利用 IPsec 技术建立的虚拟专用网。IPsec 通过在特定通信方之间建立“通道”，来保护通信方之间传输的用户数据，该通道通常称为 IPsec 隧道。

IPsec 协议为 IP 层上的网络数据安全提供了一整套安全体系结构，包括安全协议 AH（Authentication Header，认证头）和 ESP（Encapsulating Security Payload，封装安全载荷）、IKE（Internet Key Exchange，互联网密钥交换）以及用于网络认证及加密的一些算法等。其中，AH 协议和 ESP 协议用于提供安全服务，IKE 协议用于密钥交换。

设备支持两种 IPsec VPN 组网方式：

- “中心—分支”方式组网：企业分支机构网关将主动与总部网关建立 IPsec 隧道，分支机构内部终端可以安全访问总部的网络资源。
- 对等方式组网：企业各分支网关之间均可主动建立 IPsec 隧道，来保护分支之间的数据通信。

2配置 IPsec 分支节点

1. 配置需求

“中心—分支”方式组网环境中的分支节点设备需要主动建立 IPsec 隧道与中心节点通信。

对等方式组网环境中的设备需要与对端设备主动建立 IPsec 隧道。

2. 配置步骤

IPsec 基本配置

(1) 单击导航树中[虚拟专网/IPsec VPN]菜单项，进入 IPsec VPN 配置页面。

单击“IPsec 策略”页签，进入 IPsec 策略配置页面。

(2) 点击<添加>按钮，进入添加 IPsec 策略页面。

(3) 在“名称”配置项处，输入 IPsec 策略的名称。

(4) 在“接口”配置项处，选择应用 IPsec 策略的接口。请注意，此接口需要与对端设备路由可达。

(5) 在“组网方式”配置项处，选择分支节点。

(6) 在“对端网关地址”配置项处，输入 IPsec 隧道对端的 IP 地址。通常为总部网关或对端分支机构网关的 WAN 口地址。

(7) 在“预共享密钥”配置项处，输入与对端设备相同的预共享密钥。该密钥需要提前进行协商和通告。

(8) 在“保护流配置”配置项处，进行如下配置：

a. 在“受保护协议”配置项处，选择受 IPsec 隧道保护的报文的协议类型。

b. 在“本端受保护网段/掩码”配置项处，输入本端受保护网段。

c. 在“本端受保护端口”配置项处，输入本端受保护端口。仅当受保护协议选择为 TCP 或 UDP 时支持配置。

由本端受保护网段内主机的受保护端口发送的报文将被设备进行 IPsec 隧道封装处理。

d. 在“对端受保护网段/掩码”配置项处，输入对端受保护网段。

e. 在“对端受保护端口”配置项处，输入对端受保护端口。仅当受保护协议选择为 TCP 或 UDP 时支持配置。

由对端受保护网段内主机的受保护端口发送的报文才可以被设备进行 IPsec 隧道解封装处理。

f. 可以通过多次执行步骤（9）添加多条保护流。

IKE 配置

如您需要改变设备的缺省 IKE 配置，可按如下方式进行配置。

(9) 按上述方式完成 IPsec 基本配置。

(10) 点击<显示高级配置>链接，进入高级配置页面。

(11) 单击“IKE 配置”页签，进入 IKE 配置页面。

(12) 在“协商模式”配置项处，选择 IKE 协商模式：

- 主模式：协商步骤多，身份验证位于密钥交互过程之后进行，适用于对身份保护要求较高的场合。
- 野蛮模式：协商步骤少，身份验证与密钥交互同时进行，适用于对身份保护要求不高的场合。

若设备公网 IP 地址是动态分配的，建议您选择 IKE 协商模式为野蛮模式。

(13) 在“本端身份类型”配置项处，配置用于 IKE 认证的本端设备身份类型和身份标识。身份类型可选择 IP 地址、FQDN 名称或 user FQDN 名称。需要注意的是，此项必须与对端设备上执行步骤（6）配置的对端身份类型和身份标识一致。

如果您执行步骤（4）选择的 IKE 协商模式为主模式，您需要将本端设备身份类型配置为 IP 地址。

(14) 在“对端身份类型”配置项处，配置用于 IKE 认证的对端设备身份类型和身份标识。身份类型可选择 IP 地址、FQDN 名称或 user FQDN 名称。需要注意的是，此项必须与对端设备上执行步骤（5）配置的本端身份类型和身份标识一致。

(15) 在“对等体存活检测（DPD）”配置项处，选择是否开启对等体存活检测功能。该功能可用于检测对端是否存活，设备将拆除对端失活的 IPsec 隧道。建议您开启此功能，使设备能够及时获悉 IPsec 隧道的可用情况。

(16) 在“算法组合”配置项处，选择 IKE 协议交互所需的加密和认证算法。您可选择推荐的算法组合亦可自定义认证算法、加密算法和 PFS 算法。

IPsec 隧道的两端所配置的认证算法、加密算法和 PFS 算法必须一致。

(17) 在“SA 生存时间”配置项处，输入 IKE 重新协商的时间间隔，超过所配时间将触发 IKE 相关参数的重新协商。

IPsec 高级配置

如您需要改变设备的缺省 IPsec 高级配置，可按如下方式进行配置。

(18) 按上述方式完成 IPsec 基本配置。

(19) 单击“IPsec 配置”页签，进入 IPsec 配置页面。

(20) 在“算法组合”配置项处，选择 IPsec 协议交互使用的安全协议以及相应的加密和认证算法。您可选择推荐的算法组合亦可自定义安全协议、认证算法、加密算法、封装模式和 PFS 算法。

若 IPsec 本端受保护网段与对端受保护网段均为私网网段，建议您选择封装模式为隧道模式。

IPsec 隧道的两端所配置的安全协议、认证算法、加密算法、封装模式和 PFS 算法必须一致。

(21) 在“基于时间的 SA 生存时间”配置项处，输入触发 IPsec 重新协商的时间间隔，超过所配时间将触发 IPsec 相关参数的重新协商。

(22) 在“基于流量的 SA 生存时间”配置项处，输入触发 IPsec 重新协商的流量大小，超过所配流量将触发 IPsec 相关参数的重新协商。

(23) 点击<返回基本配置>按钮，返回添加 IPsec 策略页面。

(24) 点击<确定>按钮，完成配置。

3配置 IPsec 中心节点

1. 配置需求

“中心—分支”方式组网环境中的中心节点设备需要主动建立 IPsec 隧道与分支节点通信。

2. 配置步骤

IPsec 基本配置

(1) 单击导航树中[虚拟专网/IPsec VPN]菜单项，进入 IPsec VPN 配置页面。

(2) 单击“IPsec 策略”页签，进入 IPsec 策略配置页面。

(3) 点击<添加>按钮，进入添加 IPsec 策略页面。

(4) 在“名称”配置项处，输入 IPsec 策略的名称。

(5) 在“接口”配置项处，选择应用 IPsec 策略的接口。请注意，此接口需要与分支节点设备路由可达。

(6) 在“组网方式”配置项处，选择中心节点。

(7) 在“预共享密钥”配置项处，输入与对端设备相同的预共享密钥。该密钥需要提前进行协商和通告。

IKE 配置

如您需要改变设备的缺省 IKE 配置，可按如下方式进行配置。

(8) 按上述方式完成 IPsec 基本配置。

(9) 点击<显示高级配置>链接，进入高级配置页面。

(10) 单击“IKE 配置”页签，进入 IKE 配置页面。

(11) 在“协商模式”配置项处，选择 IKE 协商模式：

- 主模式：协商步骤多，身份验证位于密钥交互过程之后进行，适用于对身份保护要求较高的场合。
- 野蛮模式：协商步骤少，身份验证与密钥交互同时进行，适用于对身份保护要求不高的场合。

若设备公网 IP 地址是动态分配的，建议您选择 IKE 协商模式为野蛮模式。

(12) 在“本端身份类型”配置项处，配置用于 IKE 认证的本端设备身份类型和身份标识。身份类型可选择 IP 地址、FQDN 名称或 user FQDN 名称。需要注意的是，此项必须与分支节点设备上配置的对端身份类型和身份标识一致。

如果您执行步骤（4）选择的 IKE 协商模式为主模式，您需要将本端设备身份类型配置为 IP 地址。

(13) 在“对等体存活检测（DPD）”配置项处，选择是否开启对等体存活检测功能。该功能可用于检测对端是否存活，设备将拆除对端失活的 IPsec 隧道。建议您开启此功能，使设备能够及时获悉 IPsec 隧道的可用情况。

(14) 在“算法组合”配置项处，选择 IKE 协议交互所需的加密和认证算法。您可选择推荐的算法组合亦可自定义认证算法、加密算法和 PFS 算法。

IPsec 隧道的两端所配置的认证算法、加密算法和 PFS 算法必须一致。

(15) 在“SA 生存时间”配置项处，输入 IKE 重新协商的时间间隔，超过所配时间将触发 IKE 相关参数的重新协商。

IPsec 高级配置

如您需要改变设备的缺省 IPsec 高级配置，可按如下方式进行配置。

(16) 按上述方式完成 IPsec 基本配置。

(17) 单击“IPsec 配置”页签，进入 IPsec 配置页面。

(18) 在“算法组合”配置项处，选择 IPsec 协议交互使用的安全协议以及相应的加密和认证算法。您可选择推荐的算法组合亦可自定义安全协议、认证算法、加密算法、封装模式和 PFS 算法。

若 IPsec 本端受保护网段与对端受保护网段均为私网网段，建议您选择封装模式为隧道模式。

IPsec 隧道的两端所配置的安全协议、认证算法、加密算法、封装模式和 PFS 算法必须一致。

(19) 在“基于时间的 SA 生存时间”配置项处，输入触发 IPsec 重新协商的时间间隔，超过所配时间将触发 IPsec 相关参数的重新协商。

(20) 在“基于流量的 SA 生存时间”配置项处，输入触发 IPsec 重新协商的流量大小，超过所配流量将触发 IPsec 相关参数的重新协商。

(21) 点击<返回基本配置>按钮，返回添加 IPsec 策略页面。

(22) 点击<确定>按钮，完成配置。

L2TP服务器端

本章节介绍 L2TP 服务器端的相关内容，包括：

1简介

本功能主要用于配置 L2TP 服务器端基本参数，开启 L2TP 服务。

如果您希望为企业驻外机构和出差人员等远端用户，提供一种安全且经济的方式，让他们能够与企业内部网络通信，访问企业内部网络资源，那么您可以通过配置 L2TP 服务器端来实现上述需求。

L2TP 服务器端是具有 PPP 和 L2TP 协议处理能力的设备，通常位于企业内部网络的边缘。

2配置步骤

(1) 单击导航树中[虚拟专网/L2TP 服务器端]菜单项，进入 L2TP 服务器端页面。

(2) 单击“L2TP 配置”页签，进入 L2TP 配置页面。

(3) 在“L2TP 服务器端”配置项处，选择“开启”，开启 L2TP 服务。

(4) 点击<添加>按钮，进入新建 L2TP 组页面。

(5) 在“L2TP 配置”下，设置 L2TP 隧道参数：

- 根据需要决定是否勾选“对端隧道名称”，如勾选，则在配置项处输入 L2TP 客户端的隧道名称。
- 在“本端隧道名称”配置项处，输入 L2TP 服务器端的隧道名称。
- 在“隧道验证”配置项处，根据实际需要选择“启用”或“禁用”。
  - 如选择“启用”，则需在“隧道验证密码”配置项处，输入验证密码。该方式更加安全，但需要 L2TP 服务器端和 L2TP 客户端都启用隧道验证，且密码一致。
  - 如选择“禁用”，则表示 L2TP 服务器端和 L2TP 客户端在建立隧道时无需验证。

(6) 在“PPP 认证配置”下的“PPP 认证方式”配置项处，根据需要选择认证方式为“None”、“PAP”或“CHAP”。

- 如选择“None”，则表示对用户免认证。该方式，安全性最低，请谨慎使用。
- 如选择“PAP”，则表示采用两次握手机制对用户进行认证。该方式，安全性中。
- 如选择“CHAP”，则表示采用三次握手机制对用户进行认证。该方式，安全性最高。

(7) 在“PPP 地址配置”下，设置 PPP 地址参数：

- 在“虚拟模板接口地址”配置项处，输入虚拟模板接口的 IP 地址，使 L2TP 服务器端具有为 L2TP 客户端或用户分配 IP 地址的能力。
- 在“子网掩码”配置项处，输入虚拟模板接口 IP 地址的子网掩码。
- 在“用户地址池”配置项处，输入用于分配给 L2TP 客户端或用户的 IP 地址。

(8) 在“LNS 用户管理”下根据提示添加指定接入的 PPP 用户。

(9) 单击<显示高级设置>按钮，展开高级配置页面。

(10) 在“高级配置”下，设置高级配置参数：

- 在“Hello 报文间隔”配置项处，输入保活报文的时间间隔。
- 在“AVP 数据隐藏”配置项处，根据实际需要选择“启用”或“禁用”。

- 如选择“启用”，则表示利用隧道验证密码对 AVP 数据（例如隧道协商参数、会话协商参数和用户认证信息）进行加密传输，增强数据传输的安全性。
- 如选择“禁用”，则表示不对 AVP 数据进行加密传输。

○ 在“流量控制”配置项处，根据实际需要选择“启用”或“禁用”。

- 如选择“启用”，则表示在 L2TP 数据报文的接收与发送过程中，基于报文中携带的序列号来检测是存在否丢包，并根据序列号对乱序报文进行排序，提高 L2TP 数据报文传输的正确性和可靠性。在 L2TP 服务器端和 L2TP 客户端中的任意一端启用流量控制，该功能即可生效。
- 如选择“禁用”，则表示不对报文进行检测及排序。

○ 在“强制本端 CHAP 认证”配置项处，根据实际需要选择“启用”或“禁用”。

- 如选择“启用”，则表示在 L2TP 客户端对用户进行验证后，再由 L2TP 服务器端采用 CHAP 方式对用户进行二次认证，增强安全性。启用强制 CHAP 认证时，PPP 认证方式必须选择为“CHAP”。
- 如选择“禁用”，则表示不在 L2TP 服务器端对用户进行强制 CHAP 验证。对于不支持进行第二次 CHAP 认证的用户，建议禁用本功能。

○ 在“强制 LCP 重协商”配置项处，根据实际需要选择“启用”或“禁用”。

- 如选择“启用”，则表示在 L2TP 客户端对用户进行验证后，再由 L2TP 服务器端采用 LCP 重协商方式对用户进行二次 LCP 协商及认证，增强安全性。如果同时启用了强制 LCP 重协商和强制 CHAP 认证，则仅强制 LCP 重协商生效。
- 如选择“禁用”，则表示不在 L2TP 服务器端与用户进行强制 LCP 重协商。对于不支持 LCP 协商的用户，建议禁用本功能。

(11) 点击<确定>按钮，完成配置。

L2TP客户端

本章节介绍 L2TP 客户端的相关内容，包括：

1简介

本功能主要用于配置 L2TP 客户端基本参数，开启 L2TP 服务。

如果您希望为企业驻外机构，提供一种安全且经济的方式，让他们能够与企业内部网络通信，访问企业内部网络资源，那么您可以通过配置 L2TP 服务器端来实现上述需求。

L2TP 客户端是具有 PPP 和 L2TP 协议处理能力的设备，通常位于企业驻外机构网络的出口。

2配置步骤

(1) 单击导航树中[虚拟专网/L2TP 客户端]菜单项，进入 L2TP 客户端页面。

(2) 单击“L2TP 配置”页签，进入 L2TP 配置页面。

(3) 在“L2TP 客户端”配置项处，选择“开启”，开启 L2TP 服务。

(4) 点击<添加>按钮，进入新建 L2TP 组页面。

(5) 在“L2TP 配置”下，设置 L2TP 隧道参数：
- 在“本端隧道名称”配置项处，输入 L2TP 客户端的隧道名称。
- 在“隧道验证”配置项处，根据实际需要选择“启用”或“禁用”。
  - 如选择“启用”，则需在“隧道验证密码”配置项处，输入验证密码。该方式更加安全，但需要 L2TP 服务器端和 L2TP 客户端都启用隧道验证，且密码一致。
  - 如选择“禁用”，则表示 L2TP 服务器端和 L2TP 客户端在建立隧道时无需验证。

(6) 在“PPP 认证配置”下的“PPP 认证方式”配置项处，，根据需要选择认证方式为“None”、“PAP”或“CHAP”。
- 如选择“None”，则表示对用户免认证。该方式，安全性最低，请谨慎使用。
- 如选择“PAP”，则表示采用两次握手机制对用户进行认证。该方式，安全性中。
- 如选择“CHAP”，则表示采用三次握手机制对用户进行认证。该方式，安全性最高。

(7) 在“L2TP 服务器端配置”下的“L2TP 服务器端地址”配置项处，输入 L2TP 服务器端的 IP 地址。

(8) 在“高级配置”下，设置高级配置参数：
- 在“Hello 报文间隔”配置项处，输入保活报文的时间间隔。
- 在“AVP 数据隐藏”配置项处，根据实际需要选择“启用”或“禁用”。
  - 如选择“启用”，则表示利用隧道验证密码对 AVP 数据（例如隧道协商参数、会话协商参数和用户认证信息）进行加密传输，增强数据传输的安全性。
  - 如选择“禁用”，则表示不对 AVP 数据进行加密传输。
- 在“流量控制”配置项处，根据实际需要选择“启用”或“禁用”。
  - 如选择“启用”，则表示在 L2TP 数据报文的接收与发送过程中，基于报文中携带的序列号来检测是存在否丢包，并根据序列号对乱序报文进行排序，提高 L2TP 数据报文传输的正确性和可靠性。在 L2TP 服务器端和 L2TP 客户端中的任意一端启用流量控制，该功能即可生效。
  - 如选择“禁用”，则表示不对报文进行检测及排序。

(9) 点击<确定>按钮，完成配置。

认证管理

用户管理

本章节介绍用户管理的相关内容，包括：

1简介

如果您需要对通过设备访问外部网络的用户进行身份认证（例如 Portal 认证、PPPoE 认证），则需要通过本功能配置相应的用户账户，来维护用户的身份信息和与其相关的网络服务信息（例如用户名、密码、可用的服务、有效期等）。通过身份认证的用户将可以获得访问外部网络的权限。

2添加上网用户账户

1. 配置准备

如果待添加的用户账户需要与某个 MAC 地址绑定，请提前收集该客户端网卡的 MAC 地址。

2. 配置步骤

(1) 单击导航树中[认证管理/用户管理]菜单项，进入用户管理配置页面。

(2) 单击“用户设置”页签，进入用户配置页面。

(3) 点击<添加>按钮，进入添加用户页面。

(4) 在“用户名”配置项处，输入账户名称。

(5) 在“状态”配置项处，选择“可用”或“禁用”。

- 如果需要该账户在配置完成后立即生效，请选择“可用”。
- 如果暂时不需要该账户生效，请选择“禁用”。

(6) 在“密码”配置项处，输入用户密码。如果不设置用户密码，则该用户进行身份认证时，不需要提供密码。为提高用户帐户的安全性，建议您设置用户密码。

(7) 在“可用服务”配置项处，选择该账户可使用的接入认证方式。

(8) 在“MAC 地址”配置项处，选择该账户是否需要与某个客户端的 MAC 地址绑定。

- 如果选择“绑定“，请同时输入要绑定的 MAC 地址，输入格式例如：00-e0-fc-00-58-29，用户进行身份认证时，设备会检查该用户客户端的 MAC 地址与此处绑定的 MAC 地址是否一致，如果不一致则用户认证失败。
- 如果您不希望该账户仅能由指定 MAC 地址的客户端设备使用，请选择“不绑定”。

(9) 在“最大用户数”配置项处，输入允许同时使用该账户在线的用户数目。如果不设置该值，则表示不限制使用该账户在线的用户数。

(10) 在“有效日期”配置项处，选择该账户的有效期。如果指定了有效期，则用户只能在有效期内使用账户进行认证。

(11) 在“描述”配置项处，可输入相应的描述信息以便记忆和管理用户。

(12) 点击<确定>按钮，完成配置。

3删除上网用户账户

1. 注意事项

删除用户账户并不会导致正在使用该账户的在线用户下线，仅会导致新用户无法使用该账户上线。

2. 配置步骤

(1) 单击导航树中[认证管理/用户管理]菜单项，进入用户管理配置页面。

(2) 在用户行的“操作”区域，点击删除按钮，删除该用户账户。

(3) 在弹出的“确认提示”对话框中，点击<是>按钮，完成删除操作。

PPPoE服务器

本章节介绍 PPPoE 服务器的相关内容，包括：

1简介

如果您希望对用户提供 PPPoE 宽带拨号服务，以实现对拨号用户的地址分配管理和认证管理，那么您可以通过配置 PPPoE 服务器来满足上述需求。

2注意事项

本节配置完成后，设备仅作为 PPPoE 服务器为拨号用户提供地址分配和认证管理服务。如果您希望为拨号用户提供上网服务，以便用户可以访问互联网，除完成本节配置外，还需要完成外网的设置。外网的具体设置步骤具体请参见[快速设置]或[网络设置/外网配置]菜单项中的配置。

3配置步骤

(1) 单击导航树中[认证管理/PPPoE 服务器]菜单项，进入 PPPoE 服务器配置页面。

(2) 点击<添加>按钮，进入新建 PPPoE 服务器页面。

(3) 在“应用于”配置项处，选择设备用于提供 PPPoE 拨号服务的接口。

(4) 在“虚拟模板接口地址”配置项处，输入虚拟模板接口的 IP 地址，使 PPPoE 服务器具有为用户分配 IP 地址的能力。

(5) 在“子网掩码”配置项处，输入虚拟模板接口 IP 地址的子网掩码。

(6) 在“用户地址池”配置项处，输入用于分配给 PPPoE 拨号用户的 IP 地址。

(7) 在“DNS1”配置项处，输入用于分配给 PPPoE 拨号用户的主 DNS 服务器 IPv4 地址。

(8) 在“DNS2”配置项处，输入用于分配给 PPPoE 拨号用户的从 DNS 服务器 IPv4 地址。

(9) 在“当前服务器可接入的终端数”配置项处，输入允许拨号上网的最大用户数。

(10) 点击<确定>按钮，启动 PPPoE 服务。

Portal认证

本章节介绍 Portal 认证配置的相关内容，包括：

- 简介
- 配置 Web 网页 Portal 认证页面信息
- 配置微信客户端 Portal 认证页面信息
- 配置免认证 MAC 地址
- 配置免认证 IP 地址/域名

1简介

Portal 是互联网接入的一种认证方式，通过对用户进行身份认证，以达到对用户访问进行控制的目的。

- Web 网页认证应用场景下，用户无需安装客户端软件，直接通过 Web 页面接受用户输入的用户名和密码，设备对用户进行身份认证，用户通过 Portal 认证后，可以访问互联网资源。
- 微信客户端认证应用场景下，用户关注微信公众号进行认证，在微信公众号中点击上网链接即可进行认证，用户通过 Portal 认证后，可以访问互联网资源。

您可以为不需要通过 Portal 认证即可访问网络资源的用户设置免认证规则，免认证规则的匹配项包括 MAC 地址、IP 地址或主机名。

2配置 Web 网页 Portal 认证页面信息

1. 配置准备

为设备连接 Portal 用户终端的接口配置 IP 地址。

将需要导入的背景图片文件保存到本地。该图片的分辨率为 1440×900，大小为 255K，名称为 background-logon.jpg。

2. 配置步骤

(1) 单击导航树中[认证管理/Portal 认证]菜单项，进入 Portal 认证配置页面。

(2) 单击“认证设置”页签，进入认证设置页面。

(3) 选择“Web 网页认证”。

(4) 勾选“启用 Web 认证服务”，使用 Portal 认证功能，必须开启 Web 认证服务。

- 在“会话超时时间”配置项处，输入 Portal 会话的超时时间。

  如果用户在线时长超过该值，设备会强制该用户下线。
- 在“认证服务接口”配置项处，选择需要开启 Portal 功能的接口。

  该接口必须已配置 IP 地址。

(5) 在“窗口标题”配置项处，输入窗口标题的内容，例如“欢迎登录 Portal 认证页面”。

(6) 在“窗口提示信息”配置项处，输入窗口提示信息，例如“*XXX* 公司”。

(7) 在“导入背景图片”配置项处，点击<选择文件>按钮，选择要导入的图片文件。

(8) 点击<确定>按钮，完成配置。

(9) 点击<预览>按钮，可以预览已配置完成的 Portal 认证页面。

3配置微信客户端 Portal 认证页面信息

1. 配置准备

为设备连接 Portal 用户终端的接口配置 IP 地址。

将需要导入的背景图片文件保存到本地。该图片的分辨率为 422×251，大小为 47K，名称为 guanzhu.jpg。

2. 配置步骤

(1) 单击导航树中[认证管理/Portal 认证]菜单项，进入 Portal 认证配置页面。

(2) 单击“认证设置”页签，进入认证设置页面。

(3) 选择“微信客户端认证”。

(4) 勾选“启用 Web 认证服务”，使用 Portal 认证功能，必须开启 Web 认证服务。

- 在“会话超时时间”配置项处，输入 Portal 会话的超时时间。
  如果用户在线时长超过该值，设备会强制该用户下线。
- 在“认证服务接口”配置项处，选择需要开启 Portal 功能的接口。
  该接口必须已配置 IP 地址。

(5) 在“窗口标题”配置项处，输入窗口标题的内容，例如“欢迎登录 Portal 认证页面”。

(6) 在“窗口提示信息”配置项处，输入窗口提示信息，例如“*XXX* 公司”。
在“导入背景图片”配置项处，点击<选择文件>按钮，选择要导入的图片文件。

(7) 在“微信 DNS”配置项处，输入微信公众号上面设置的设备的域名。
输入设备的域名时，只能输入字母、数字、“-”、“_”和“.”，且不能以“.”开头。

(8) 点击<确定>按钮，完成配置。

(9) 点击<预览>按钮，可以预览已配置完成的 Portal 认证页面。

4配置免认证 MAC 地址

(1) 单击导航树中[认证管理/Portal 认证]菜单项，进入 Portal 认证配置页面。

(2) 单击“免认证 MAC 地址”页签，进入免认证 MAC 地址配置页面。

(3) 点击<添加>按钮，进入添加免认证 MAC 地址页面。

(4) 在“MAC 地址”配置项处，输入免认证 MAC 地址。

(5) 在“描述”配置项处，输入与本配置相关的描述。

(6) 点击<确定>按钮，完成配置。

5配置免认证 IP 地址/域名

(1) 单击导航树中[认证管理/Portal 认证]菜单项，进入 Portal 认证配置页面。

(2) 单击“免认证 IP 地址/域名”页签，进入免认证 IP 地址/域名配置页面。

(3) 点击<添加>按钮，进入添加免认证地址页面。

(4) 在“地址添加方式”配置项处，选择免认证地址的类型。

- 选择“源地址”或“目的地址”，请继续在“IP 地址”配置项处，输入免认证的 IP 地址及掩码。

- 选择“域名”，请继续在“域名”配置项处，输入域名。

(5) 在“描述”配置项处，输入与本配置相关的描述。

(6) 点击<确定>按钮，完成配置。

高级选项

静态路由

本章节介绍静态路由的相关内容，包括：

1简介

静态路由是在路由器中通过手工方式设置的固定路由条目。当您的网络结构比较简单且比较稳定时，通过配置静态路由就可以实现网络互通。例如，当您知道网络的出接口，以及网关的 IP 地址时，设置静态路由即可实现正常通信。

当去往同一目的地存在多条静态路由时，如果您希望优先选用某条静态路由，可以调整静态路由的优先级。优先级的值越小，对应的静态路由的优先级越高。

2注意事项

当静态路由中下一跳对应的接口失效时，本地的静态路由条目不会被删除，这种情况下需要您检查网络环境，然后修改静态路由的配置。

3配置步骤

(1) 单击导航树中[高级选项/静态路由]菜单项，进入静态路由配置页面。

(2) 点击<添加>按钮，进入添加 IPv4 静态路由页面。

(3) 在“目的 IP 地址”配置项处，输入设备要访问的目的网络的 IP 地址。

(4) 在“掩码长度”配置项处，输入目的网络的掩码长度。

(5) 在“下一跳”下，设置去往目的网络的出接口和下一跳参数：

- 选择出接口。选择 Null0 接口作为出接口时，设备会丢弃发送到指定目的网络的报文。当存在针对某个目的网络的攻击报文，或将报文发送到某个目的网络时产生环路，可以通过指定去往该目的网络的出接口为 Null0 接口，来避免攻击和环路。
- 设置下一跳 IP 地址。

(6) 在“路由优先级”下，输入静态路由的优先级。

(7) 在“描述”下，输入静态路由的描述信息。

(8) 点击<确定>按钮，完成静态路由的添加。

策略路由

本章节介绍策略路由的相关内容，包括：

1简介

与单纯按照 IP 报文的目的地址查找路由表进行转发不同，策略路由是一种依据用户制定的策略进行路由转发的机制。策略路由可以对于满足一定条件（源地址和目的地址等）的报文，执行指定的操作（设置报文的下一跳、出接口、缺省下一跳和缺省出接口等）。策略路由的匹配条件比普通路由更丰富，当需要按照报文的某些特征（如报文源地址和目的地址等）转发到不同的网络中时，可以配置策略路由功能。

2配置步骤

(1) 单击导航树中[高级选项/策略路由]菜单项，进入策略路由配置页面。

(2) 选择应用策略路由的接口。

(3) 点击<添加>按钮，进入“新增策略路由列表”页面。

(4) 在“匹配规则”下，设置策略路由的匹配规则参数：

- 选择匹配的协议类型，如果选择了“协议号”，则需要输入具体的协议编号，如 HTTP 的协议号为 80。
- 如果协议类型指定为“TCP”或“UDP”，则需要设置匹配报文的源端口和目的端口。
- 在“源 IP 地址段”和“目的 IP 地址段”配置项处，设置匹配报文的源 IP 地址范围和目的 IP 地址范围。输入地址段时，起始地址和结束地址间需要用短横线连接，如“1.1.1.1-1.1.1.2”，如果只指定一个地址，则起始地址和结束地址需要相同。
- 设置匹配规则的生效时间。如果策略需要全天生效，则设置为 00:00-23:59。

(5) 在“出接口”或“下一跳”配置项处，配置匹配规则的报文通过指定出接口转发或转发到指定的下一跳。

(6) 配置策略的描述信息，当某些策略用于特殊用途时，管理员可以配置描述信息，方便后续查询使用。

(7) 点击<确定>按钮，完成配置。

动态DNS

本章节介绍动态 DNS 的相关内容，包括：

1简介

如果您通过设备的 WAN 接口来提供 Web、Mail 或者 FTP 等服务，且希望在设备 WAN 接口的 IP 发生变化的情况下（如宽带拨号方式下），用户仍然能够通过固定的域名访问设备提供的服务，那么需要在设备上的提供 Web、Mail 或者 FTP 等服务的 WAN 接口上配置 DDNS（Dynamic Domain Name System，动态域名系统）服务。

使用 DDNS 服务之前，需要提前在 DDNS 服务器（即 DDNS 服务提供商，如花生壳网站）上注册。之后，当设备 WAN 接口的 IP 地址变化时，设备会自动通知 DDNS 服务器更新记录的 IP 地址和固定域名的映射关系。

2注意事项

设备向 DDNS 服务器申请域名时，请保证 WAN 接口地址为公网 IP 地址。

3配置准备

请提前在动态域名服务提供商（如花生壳网站）处注册账户，设置密码。

4配置步骤

(1) 单击导航树中[高级选项/动态 DNS]菜单项，进入动态 DNS 配置页面。

(2) 点击<添加>按钮，进入“新建动态 DNS 策略”页面。

(3) 在“WAN 接口”配置项处，选择设备上的提供 Web、Mail 或者 FTP 等服务的 WAN 接口。

(4) 在“域名”配置项处，输入设备的域名。

(5) 在“服务器配置”下，设置 DDNS 服务器参数：

- 选择服务提供商，如花生壳等。
- 设置服务器地址。如果服务器地址与缺省情况不同，勾选“修改服务器地址”后进行修改。
- 设置设备向服务器发送更新请求的时间间隔。如果配置时间间隔为 0，设备只在 WAN 接口 IP 地址发生变化或者接口连接由 down 变为 up 时发送更新请求。

(6) 在“账户配置”下，输入在服务提供商处注册的用户名和密码。

(7) 点击<确定>按钮，启动动态 DNS 服务。

SNMP

本章节介绍 SNMP 的相关内容，包括：

1简介

SNMP（Simple Network Management Protocol，简单网络管理协议）是互联网中的一种网络管理标准协议，广泛用于实现管理设备对被管理设备的访问和管理。

如果您希望通过网管软件（比如 iMC、MIB Browser 等）实现对设备的管理，或者设备发生紧急事件（比如接口 Up 或者 Down、CPU 利用率高、内存耗尽等）时能自动通过告警信息告知网管软件，则需要配置 SNMP。

设备支持 SNMPv1、SNMPv2c 和 SNMPv3 三种版本。SNMPv3 比 SNMPv1 和 SNMPv2c 更安全。

- SNMPv1 和 SNMPv2c 使用口令认证。

- SNMPv3 采用用户名认证，并且必须配置认证密码和加密密码。其中：
  - 用户名和认证密码用于对网管软件进行身份认证，以免非法网管软件访问设备。
  - 加密密码用于对网管软件和设备之间传输的报文进行加密，以免报文被窃听。

2配置准备

确定 SNMP 版本号，网管软件和设备必须配置相同的 SNMP 版本号。

3配置 SNMPv1 和 SNMPv2c

1. 注意事项

网管软件和设备必须配置相同的 SNMP 口令。SNMP 口令包括只读口令和读写口令，二者至少配置一项。

- 如果您仅需读取设备上参数的值，则只需配置只读口令。
- 如果您既需要读取设备上参数的值、又需要设置参数的值，则需配置读写口令。

2. 配置步骤

(1) 单击导航树中[高级选项/SNMP]菜单项，进入 SNMP 配置页面。

(2) 选择“开启”SNMP。

(3) 选择“SNMPv1 和 SNMPv2c”版本。

(4) 在“SNMP 口令”配置项处，输入口令。

(5) 在“SNMP 信任主机 IPv4 地址”配置项处，输入网管软件的地址。只有指定地址的网管软件可以管理设备。如果不配置该参数，则拥有口令的网管软件均可以管理设备。

(6) 在“Trap 接收主机 IPv4 地址/域名”配置项处，输入接收告警信息的主机的 IPv4 地址或域名，通常为网管软件的 IP 地址。

(7) 在“联系信息”配置项处，输入设备管理员的联系方式。

(8) 在“设备位置”配置项处，输入设备所处的地理位置，方便快速定位设备。

(9) 点击<确定>按钮，完成配置。

4配置 SNMPv3

1. 注意事项

网管软件和设备必须配置相同的用户名、认证密码和加密密码。

2. 配置步骤

(1) 单击导航树中[高级选项/SNMP]菜单项，进入 SNMP 配置页面。

(2) 选择“开启”SNMP。

(3) 选择“SNMPv3”版本。

(4) 在“用户名”配置项处，输入用户名。

(5) 在“认证密码”配置项处，输入认证密码。

(6) 在“加密密码”配置项处，输入加密密码。

(7) 在“SNMP 信任主机 IPv4 地址”配置项处，输入网管软件的地址。只有指定地址的网管软件可以管理设备。如果不配置该参数，则用户名、认证密码和加密密码正确的网管软件均可以管理设备。

(8) 在“Trap 接收主机 IPv4 地址/域名”配置项处，输入接收告警信息的主机的 IPv4 地址或域名，通常为网管软件的 IP 地址。

(9) 在“联系信息”配置项处，输入设备管理员的联系方式。

(10) 在“设备位置”配置项处，输入设备所处的地理位置，方便快速定位设备。

(11) 点击<确定>按钮，完成配置。

CWMP

本章节介绍 CWMP 的相关内容，包括：

1简介

CWMP（CPE WAN Management Protocol，CPE 广域网管理协议）通过 ACS（Auto-Configuration Server，自动配置服务器）对 CPE（Customer Premises Equipment，用户侧设备）进行远程集中管理，解决了 CPE 设备管理困难的问题，并节约了维护成本。

2配置准备

需要准备安装了 iMC BIMS 功能的 iMC 服务器作为 ACS 服务器或者其他支持 ACS 功能的服务器，并完成 ACS 服务器的配置。

3配置步骤

(1) 单击导航树中[高级选项/CWMP]菜单项，进入 CWMP 页面。

(2) 选择开启 CWMP。

(3) 在“ACS”配置项处，输入 ACS 的 URL 地址、用户名和密码。

CPE 向 ACS 发起的连接请求中携带 ACS 的用户名和密码。只有该用户名和密码与 ACS 本地配置的用户名和密码一致时，ACS 才会接受 CPE 的连接请求。

(4) 在“CPE”配置项处，配置 CPE 相关参数：

- CPE 的用户名和密码。为了防止被恶意控制，当 ACS 向 CPE 发送管理指令时，携带 CPE 的用户名和密码，只有该用户名和密码与 CPE 上配置的一致时，ACS 才能控制 CPE。
- 是否发送 Inform 报文，及 Inform 报文的发送时间间隔。

  CPE 通过向 ACS 发送 Inform 报文发起连接请求，Inform 报文中携带 CPE 和 ACS 的用户名、密码等信息。

  如果希望设备可以周期性地自动连接 ACS，则需要开启 Inform 报文发送功能。
- CPE 上用于连接 ACS 的接口。

(5) 点击<确定>按钮，完成配置。

系统工具

管理账户

本章节介绍管理账户的相关内容，包括：

1简介

可以通过本页面对登录设备的管理员账户信息进行管理和维护，包括添加管理账户以及修改或删除管理账户。

2添加管理账户

(1) 单击导航树中[系统工具/管理账户]菜单项，进入管理账户配置页面。

(2) 点击<添加>按钮，进入添加管理员页面。

(3) 在“用户名”配置项处，输入管理员名称。

(4) 在“密码”配置项处，输入管理员密码。如果不设置管理员密码，则管理员登录设备时，不需要提供密码。为提高管理员帐户的安全性，建议您设置管理员密码。

(5) 在“确认密码”配置项处，请再次输入您设置的密码，并确保与之一致。

(6) 在“角色”配置项处，选择该账户登录时的角色。

- 如果该账户需要具有最高管理权限，请选择“Administrator”
- 如果该账户仅拥有普通的查看权限，无配置权限，请选择“Operator”。

(7) 在“可用服务”配置项处，点击复选框选择允许该管理员账户使用的网络服务。

- Console：表示管理员可通过 Console 口登录设备。
- Telnet：表示管理员可通过 Telnet 方式登录设备。使用该服务的管理员需要使用 Telnet 客户端来访问设备，设备将作为 Telnet 服务器为其提供服务。
- FTP：表示管理员可通过 FTP 访问设备文件系统资源。使用该服务的管理员需要使用 FTP 客户端来访问设备，设备将作为 FTP 服务器为其提供服务。
- WEB：表示管理员可通过 Web 页面登录设备。
- SSH：表示管理员可通过 SSH 方式登录设备，该方式比 Telnet 方式更安全。使用该服务的管理员需要使用 SSH 客户端来访问设备，设备将作为 SSH 服务器为其提供服务。

(8) 在“同时在线最大用户数”配置项处，输入允许同时使用该账户在线的用户数目。如果不设置该值，则表示不限制使用该账户在线的用户数。需要注意的是，使用 FTP 服务的管理员不受此配置限制。

(9) 在“FTP 目录”配置项处，输入管理员通过 FTP 方式访问设备时的工作路径，例如 flash:/dpi。建议您首先通过[系统工具/系统升级]菜单项的“文件管理”页面查看系统中已有的文件路径，以确保此处输入的工作路径准确。

(10) 点击<确定>按钮，完成配置。

3修改管理账户

(1) 单击导航树中[系统工具/管理账户]菜单项，进入管理账户配置页面。
(2) 在用户行的“操作”区域，点击编辑按钮，进入修改管理员配置页面。
(3) 可在“密码”配置项处，输入新密码。重置了管理员账户的密码后，该管理员下次登录设备时还需要修改密码。
(4) 如果您修改了密码，请在“确认密码”配置项处，再次输入新密码，并确保与之一致。
(5) 可在“角色”配置项处，选择该账户的新角色，并删除不需要的角色。
    - 如果该账户需要具有最高管理权限，请选择“Administrator”
    - 如果该账户仅拥有普通的查看权限，无配置权限，请选择“Operator”。
(6) 可在“可用服务”配置项处，点击复选框选择允许该管理员账户使用的网络服务。
    - Console：表示管理员可通过 Console 口登录设备。
    - Telnet：表示管理员可通过 Telnet 方式登录设备。使用该服务的管理员需要使用 Telnet 客户端来访问设备，设备将作为 Telnet 服务器为其提供服务。
    - FTP：表示管理员可通过 FTP 访问设备文件系统资源。使用该服务的管理员需要使用 FTP 客户端来访问设备，设备将作为 FTP 服务器为其提供服务。
    - WEB：表示管理员可通过 Web 页面登录设备。
(7) SSH：表示管理员可通过 SSH 方式登录设备，该方式比 Telnet 方式更安全。使用该服务的管理员需要使用 SSH 客户端来访问设备，设备将作为 SSH 服务器为其提供服务。
(8) 可在“同时在线最大用户数”配置项处，输入允许同时使用该账户在线的用户数目。如果不设置该值，则表示不限制使用该账户在线的用户数。需要注意的是，使用 FTP 服务的管理员不受此配置限制。
(9) 可在“FTP 目录”配置项处，输入管理员通过 FTP 方式访问设备时的工作路径，例如 flash:/dpi。建议您首先通过[系统工具/系统升级]菜单项的“文件管理”页面查看系统中已有的文件路径，以确保此处输入的工作路径准确。
(10) 点击<确定>按钮，完成配置。

4删除管理账户

(1) 单击导航树中[系统工具/管理账户]菜单项，进入管理账户配置页面。
(2) 在用户行的“操作”区域，点击删除按钮，删除该管理员账户。
(3) 在弹出的“确认提示”对话框中，点击<是>按钮，完成删除操作。

配置管理

本章节介绍配置管理的相关内容，包括：

1简介

本功能主要用于对设备的配置文件进行管理。配置文件是指用来保存设备配置的文件。

通过本功能可以：

- 查看当前配置：如果希望查看设备的当前配置，例如设备版本号、接口 IP 地址等，则需通过单击导航树中[系统工具/配置管理]菜单项，点击“查看当前配置”页签查看设备的当前配置。
- 恢复出厂配置：如果设备没有配置文件或者配置文件损坏时，希望设备能够正常启动运行，则需通过本功能将设备上的配置恢复到出厂状态。
- 保存当前配置：对设备进行配置后，如果希望设备重启后配置能继续生效，则需通过本功能保存设备当前所有配置。
- 从备份文件恢复：设备配置错误后，如果希望设备恢复到正确配置运行状态，则需通过本功能恢复设备配置。
- 导出当前配置：如果希望将当前配置文件导出作为备份配置文件，则需通过本功能将当前配置文件导出保存到指定路径。

2恢复出厂配置

(1) 单击导航树中[系统工具/配置管理]菜单项，进入配置管理页面。

(2) 单击“恢复出厂配置”页签，进入恢复出厂配置页面。

(3) 点击<重置>按钮，在确认提示框中选择“是”选项，完成恢复出厂配置并强制重启设备。

3保存当前配置

(1) 单击导航树中[系统工具/配置管理]菜单项，进入配置管理页面。

(2) 单击“备份恢复配置”页签，进入备份恢复配置页面。

(3) 点击<保存当前配置>按钮，进入保存当前配置页面。

(4) 选择当前配置的保存方式：

- 如果选择“保存到下次启动配置文件”，将当前配置保存到存储介质的根目录下，并将该文件设置为设备下次启动使用的配置文件。
- 如果选择“保存到指定配置文件”，则可以需输入自定义的配置文件名称。

(5) 点击<确定>按钮，完成保存当前配置。

4从备份文件恢复

(1) 单击导航树中[系统工具/配置管理]菜单项，进入配置管理页面。

(2) 单击“备份恢复配置”页签，进入备份恢复配置页面。

(3) 点击<从备份文件恢复>按钮，进入从备份文件恢复页面。

(4) 点击“浏览”按钮选择特定路径下的备份配置文件。

(5) 点击<确定>按钮，完成当前配置。

- 如果勾选“立即执行导入后的配置文件”，点击<确定>按钮，系统会立即使用导入的配置替换当前运行的配置，无需重启设备。

- 如果不勾选“立即执行导入后的配置文件”，点击<确定>按钮后，需手动重启设备，才可以恢复配置。

5导出当前配置

(1) 单击导航树中[系统工具/配置管理]菜单项，进入配置管理页面。

(2) 单击“备份恢复配置”页签，进入备份恢复配置页面。

(3) 点击<导出当前配置>按钮，选择保存路径，即可将当前配置保存到本地 PC。

系统日志

本章节介绍系统日志的相关内容，包括：

1简介

设备在运行过程中会生成系统日志。日志中记录了管理员在设备上进行的配置、设备的状态变化以及设备内部发生的重要事件等，为用户进行设备维护和故障诊断提供参考。

用户可以将日志发送到日志服务器集中管理，也可以直接在 Web 页面查看日志。

日志划分为如表 10-1 所示的八个级别，各级别的严重性依照数值从 0～7 依次降低。了解日志级别，能章节您迅速筛选出重点日志。

表1 日志级别列表

数值	信息级别	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

2将系统日志发往日志服务器

1. 配置准备

请确保设备和日志服务器能互相 ping 通，日志服务器才能收到设备发送的日志。

2. 配置步骤

(1) 单击导航树中[系统工具/系统日志]菜单项，进入系统日志配置页面。

(2) 选择“发送到日志服务器”，输入日志服务器的 IP 地址或者域名地址。

(3) 点击<应用>按钮，完成配置。

3通过 Web 页面查看系统日志

(1) 单击导航树中[系统工具/系统日志]菜单项，进入系统日志配置页面。设备会逐条显示日志的生成时间、级别以及详细信息。

(2) 点击<导出>按钮，可以将设备上已有的日志信息导出到登录 PC 上。

系统设置

本章节介绍系统设置的相关内容，包括：

1简介

通过本功能可以设置设备信息和系统时间。

设备信息包括设备名称、设备位置和设备管理员的联系方式，方便管理员管理和定位设备。

系统时间包括日期、时间和时区等。为了便于管理设备，并保证本设备与其它网络设备协同工作，您需要为设备配置准确的系统时间。

系统时间的获取方式有两种：

- 手工设置日期和时间。该方式下，用户手工指定的日期和时间即为当前的系统时间。后续，设备使用内部时钟信号计时。如果设备重启，系统时间将恢复到出厂时间。
- 自动同步网络日期和时间。该方式下，设备使用从 NTP 服务器获取的时间作为当前的系统时间，并周期性地同步 NTP 服务器的时间，以便和 NTP 服务器的系统时间保持一致。即便本设备重启，设备也会迅速重新同步 NTP 服务器的系统时间。如果您管理的网络中有 NTP 服务器，推荐使用该方式，该方式获取的时间比手工配置的时间更精准。

2配置设备信息

(1) 单击导航树中[系统工具/系统设置]菜单项，进入系统设置配置页面。

(2) 单击“设备信息”页签，进入设备信息配置页面。

(3) 在“设备名称”配置项处，输入设备名称，例如以“设备型号.IP 地址”为设备名称。

(4) 在“设备位置”配置项处，输入设备所处的地理位置，方便快速定位设备。

(5) 在“联系方式”配置项处，输入设备管理员的联系方式。

(6) 点击<应用>按钮，完成配置。

3手工设置日期和时间

1. 注意事项

如果设备重启，系统时间将恢复到出厂时间。

2. 配置准备

了解设备所处的时区。全球分为 24 个时区，请将设备的时区配置为设备所在地理区域的时区。例如，设备在中国，请选择“北京,重庆,香港特别行政区,乌鲁木齐(GMT+08:00)”；如果设备位于美国，请选择“中部时间(美国和加拿大)(GMT-06:00)”。

3. 配置步骤

(1) 单击导航树中[系统工具/系统设置]菜单项，进入系统设置配置页面。

(2) 单击“日期/时间”页签，进入系统时间配置页面。

(3) 选择“手工设置日期和时间”。

(4) 将系统时间配置为设备所在地理区域的当前时间。

a. 选择年月日。

b. 选择时分秒。界面中供选择的分钟和秒钟数值为 3 的倍数（00、03、06、09、……、57），您可以通过向上或者向下的箭头来进行微调。例如要配置分钟数为 20，则先选中 18，再点击两次向上的箭头即可得到 20。

(5) 将时区配置为设备所在地理区域的时区。

(6) 点击<应用>按钮，完成配置。

4自动同步网络日期和时间

1. 注意事项

设备和 NTP 服务器上配置的时区必须相同，否则，会导致设备的系统时间和 NTP 服务器的系统时间不一致。

2. 配置准备

了解设备所处的时区。全球分为 24 个时区，请将设备的时区配置为设备所在地理区域的时区。例如，设备在中国，请选择“北京,重庆,香港特别行政区,乌鲁木齐(GMT+08:00)”；如果设备位于美国，请选择“中部时间(美国和加拿大)(GMT-06:00)”。

3. 配置步骤

(1) 单击导航树中[系统工具/系统设置]菜单项，进入系统设置配置页面。

(2) 单击“日期/时间”页签，进入系统时间配置页面。

(3) 选择“自动同步网络日期和时间”。

(4) 在“NTP 服务器 1”配置项处，输入 NTP 服务器 1 的 IP 地址。

(5) 在“NTP 服务器 2”配置项处，输入 NTP 服务器 2 的 IP 地址。设备会自动从 NTP 服务器 1 和 NTP 服务器 2 中择优选取一台服务器的系统时间作为设备的系统时间。如果这台优选的服务器故障，则自动使用另一台 NTP 服务器的系统时间作为设备的系统时间。如果 NTP 服务器均故障，设备将使用内部时钟信号继续计时，待 NTP 服务器恢复后，再同步 NTP 服务器的时间。

(6) 将时区配置为设备所在地理区域的时区。

(7) 点击<应用>按钮，完成配置。

远程管理

本章节介绍远程管理的相关内容，包括：

1简介

远程管理功能既可以用来检测网络的连通性，又可以为用户提供登录设备、管理设备的方式。远程管理功能包括：

- Ping：通过 ping 功能，可以检测网络的连通性，及时了解网络状况。
- Telnet：是一种实现远程登录服务的协议。用户可以在 PC 上通过 Telnet 方式登录设备，对设备进行远程管理。
- HTTP/HTTPS：是基于 HTTP、HTTPS 超文本传输协议的两种 Web 登录方式。HTTPS 登录方式的安全性能高于 HTTP 登录方式。用户可以在 PC 上使用 HTTP/HTTPS 协议登录设备的 Web 界面，通过 Web 界面直观地配置和管理设备。
- SSH（Secure Shell，安全外壳）：用来在不安全的网络环境中，通过加密机制和认证机制，实现安全的远程访问以及文件传输。如果希望用户更安全地访问设备，则可以使用 SSH 服务。设备作为 SSH 服务器，提供如下几种服务：
  - Stelnet：即安全的 Telnet。Stelnet 实现的功能与 Telnet 相同，但访问方式更加安全可靠。
  - SFTP：即安全的 FTP。可提供安全可靠的网络文件传输服务，使得用户可以安全登录到设备上进行文件管理操作，且能保证文件传输的安全性。
  - SCP：即 Secure Copy。可提供安全的文件复制功能。

2配置 Ping

(1) 单击导航树中[系统工具/远程管理]菜单项，进入远程管理页面。
(2) 单击 Ping 页签。
(3) 勾选一个发送 Ping 报文的接口。
(4) 单击<应用>按钮。

3配置 Telnet

(1) 单击导航树中[系统工具/远程管理]菜单项，进入远程管理配置页面。
(2) 单击“Telnet”页签，进入 Telnet 配置页面。
(3) 在“Telnet 服务”配置项处，单击按钮，使得按钮状态为“ON”，开启 Telnet 服务。
(4) 在“IPv4 端口”或“IPv6 端口”配置项处，输入 Telnet 服务使用的端口号。
请根据组网需求选择 IP 协议对应的端口类型：

- 如果用户通过 IPv4 网络 Telnet 登录设备时，使用的端口号需要与本配置项指定的端口号相同。
- 如果用户通过 IPv6 网络 Telnet 登录设备时，使用的端口号需要与本配置项指定的端口号相同。

(5) 在“管理员 IP”列表下可配置一个或者多个 IPv4 地址用于远程管理设备。在“Telnet”列表下勾选“允许远程登录”选择框，则可通过“接口”列表对应接口的 IP 地址远程登录设备。

(6) 点击<应用>按钮，完成配置。

4配置 SSH

(1) 单击导航树中[系统工具/远程管理]菜单项，进入远程管理配置页面。

(2) 单击“SSH”页签，进入 SSH 配置页面。

(3) 根据需要执行以下任意一个或多个操作，开启相应的 SSH 服务。

- 单击“Stelnet 服务”后的按钮，使其置为“ON”状态，开启 Stelnet 服务。
- 单击“SFTP 服务”后的按钮，使其置为“ON”状态，开启 SFTP 服务。
- 单击“SCP”服务后的按钮，使其置为“ON”状态，开启 SCP 服务。

5配置 HTTP/HTTPS

(1) 单击导航树中[系统工具/远程管理]菜单项，进入远程管理配置页面。

(2) 单击“HTTP/HTTPS”页签，进入 HTTP/HTTPS 配置页面。

(3) 在“HTTP 登录端口”配置项处输入 HTTP 方式登录设备对应的端口号，建议使用 10000 以上的端口号。

(4) 在“HTTPS 登录端口”配置项处输入 HTTP 方式登录设备对应的端口号，建议使用 10000 以上的端口号。

(5) 在“例外 IP”配置项处，可以添加一个或多个 IPv4 地址，表示与“允许远程登录”选择框选项相反操作。

- 如果添加了 IPv4 地址，并在“HTTP/HTTPS”列表下勾选“允许远程登录”选择框，表示禁止通过该接口的 IP 地址以 HTTP/HTTPS 方式登录设备。
- 如果添加了 IPv4 地址，并在“HTTP/HTTPS”列表下不勾选“允许远程登录”选择框，表示允许通过该接口的 IP 地址以 HTTP/HTTPS 方式登录设备。
- 如果不添加 IPv4 地址，并在“HTTP/HTTPS”列表下勾选“允许远程登录”选择框，表示允许通过该接口的所有 IP 地址以 HTTP/HTTPS 方式登录设备。

添加的 IPv4 地址必须是对应“接口”列表下接口的 IP 地址。

(6) 点击<应用>按钮，完成配置。

系统升级

章节介绍系统升级相关内容，包括：

- 下载

1简介

本功能主要用来对设备版本进行升级以及对设备上的文件进行管理。如果希望完善当前软件版本漏洞或者更新应用功能，则需通过版本升级功能来实现。文件管理支持以下三种操作：

- 上传：本地的文件上传至设备。例如，对设备进行系统升级前，需要将 IPE 文件上传到设备。
- 删除：删除设备上的文件。上传文件到设备时，如果内存空间不足以存储要上传的文件，则需要删除某些非重要文件，释放存储空间。
- 下载：将设备上保存的文件下载到本地。用户可以根据自己需求将设备上的文件下载到本地，以便备份或者数据分析。

2上传

(1) 单击导航树中[系统工具/系统升级]菜单项，进入系统升级页面。
(2) 单击“文件管理”页签，进入文件管理配置页面。
(3) 点击<上传>按钮，进入上传页面。
(4) 点击<浏览>按钮，选择特定路径下保存的文件。
(5) 点击<确定>按钮，完成文件上传。

3删除

1. 注意事项

不能删除版本文件，否则会导致设备运行出错。

2. 配置步骤

(1) 单击导航树中[系统工具/系统升级]菜单项，进入系统升级页面。
(2) 单击“文件管理”页签，进入文件管理配置页面。
(3) 在文件名列表中勾选要删除的文件。
(4) 点击<删除>按钮，完成文件删除。

4下载

(1) 单击导航树中[系统工具/系统升级]菜单项，进入系统升级页面。
(2) 单击“文件管理”页签，进入文件管理配置页面。
(3) 在文件名列表中勾选要下载的文件。
(4) 点击<下载>按钮，选择保存路径即可实现文件下载。

License管理

本章节介绍 License 管理的相关内容，包括：

- 简介
- 注意事项
- 查看哪些特性需要 License

1简介

用户需要为设备购买授权码、申请激活文件、安装 License，才能使用设备上基于 License 的特性。哪些特性需要安装 License 可通过“License 和特性”页签来查看。

2注意事项

对于一台设备，请不要多个用户同时进行 License 操作，以免操作失败。

3查看哪些特性需要 License

(1) 单击导航树中[系统工具/License 管理]菜单项，进入 License 管理配置页面。

(2) 单击“License 和特性”页签，进入 License 和特性显示页面。

(3) 了解特性的授权情况。

- “特性名称”列：表示设备支持的、需安装 License 才能正常使用的特性。
- “是否授权”列：取值为“Y”时，表示已安装了 License；取值为“N”时，表示未安装 License。
- “状态”列：表示 License 的状态。取值为“Formal”时表示当前已经为该特性安装了正式 License，License 处于有效状态；取值为“Trial”时表示当前已经为该特性安装了临时 License，License 处于有效状态；取值为“-”时表示当前无有效 License，用户如需使用该特性，请安装对应的 License。

4压缩 License 存储区

1. 功能简介

过期后的 License 会一直占用 License 存储区。如果 License 存储区空间耗尽，会导致新的 License 安装失败。此时，需要压缩 License 存储区来释放空间。

2. 注意事项

压缩 License 可能会导致 DID 变化。因此，在压缩 License 存储区前，请确保使用旧 DID 申请的 License 已经安装完毕。否则，License 存储区压缩后，使用旧 DID 申请的 License 将无法继续安装。

3. 配置步骤

(1) 单击导航树中[系统工具/License 管理]菜单项，进入 License 管理配置页面。

(2) 单击“压缩”页签，进入压缩 License 存储区配置页面。

(3) 确认设备还可安装的激活文件的个数。“设备还可安装的激活文件的个数”=“可安装激活文件个数”-“已安装激活文件的个数”。

(4) 如果您当前需要安装的激活文件的个数大于“设备还可安装的激活文件的个数”，请点击<压缩>按钮，完成配置。否则，不需要压缩 License 存储区。

5申请 License 激活文件

请登录 H3C License 管理平台（网址为 http://www.h3c.com/cn/License），获取 License 激活文件，具体方法请参见《H3C 交换机及路由器产品 通用 License 使用指南》。

6安装 License

(1) 单击导航树中[系统工具/License 管理]菜单项，进入 License 管理配置页面。

(2) 单击“License 配置”页签，进入 License 配置页面。

(3) 点击<添加>按钮，进入添加 License 页面。

(4) 选择激活文件。

(5) 点击<确定>按钮，完成配置。