路由器高级配置手册

Rev：3.0

上海艾泰科技有限公司
http://www.utt.com.cn

版 权 声 明

上海艾泰科技有限公司|总部地址：上海市漕河泾开发区松江高科技园莘砖公路 518 号 9 号楼 3 层（201612）

欲了解艾泰科技更多服务及解决方案，请访问 http://www.utt.com.cn

目　录

第 1 章 导读.....1
1.1 手册说明.....1
1.2 界面风格.....1
1.3 基本约定.....2
1.4 出厂配置.....3
1.5 关键特性.....3
1.6 规格.....4
1.7 联系我们.....4

第 2 章 硬件安装.....5
2.1 面板介绍.....5
2.2 安装注意事项.....6
2.3 安装准备.....6
2.4 硬件安装.....7
2.5 硬件连接.....8

第 3 章 登录设备.....9
3.1 配置正确的网络设置.....9
3.2 登录设备.....10
3.3 Web 页面介绍.....11

第 4 章 配置向导.....13

第 5 章 系统监控.....14
5.1 系统状态.....14
5.2 流量监控.....15

第 6 章 网络配置.....16
6.1 外网配置.....16
6.2 内网配置.....23
6.3 DHCP 服务.....24
6.4 端口映射.....31
6.5 路由配置.....38
6.6 动态域名.....42
6.7 交换配置.....44

第 7 章 用户管理.....46
7.1 组织成员.....46
7.2 用户状态.....49

7.3 用户认证.....50
7.4 黑名单.....57

第 8 章 行为管理.....59
8.1 行为管理.....59
8.2 域名过滤.....61
8.3 白名单.....64
8.4 电子通告.....65

第 9 章 流量管理.....67
9.1 应用优先.....67
9.2 流量管理.....68

第 10 章 防火墙.....71
10.1 访问控制.....71
10.2 连接控制.....77
10.3 攻击防护.....78

第 11 章 VPN 配置.....79
11.1 IPsec.....79
11.2 PPTP/L2TP.....93

第 12 章 系统对象.....107
12.1 时间计划.....107
12.2 地址组.....108

第 13 章 系统配置.....110
13.1 网管策略.....110
13.2 时钟管理.....114
13.3 系统维护.....115
13.4 网络工具.....118
13.5 系统日志.....120
13.6 计划任务.....122

第 1 章 导读

提示：

为了达到最好的使用效果，建议将 Windows Internet Explorer 浏览器升级到 10.0 以上版本。

1.1 手册说明

本手册描述应用于艾泰科技 ReOS_SE 3.0 软件平台产品的特性和功能，提供基于 WEB 界面的配置方法及其步骤，各型号的路由器功能模块有所不同，具体功能以产品为准。用户应保证所使用的软件版本与本手册所描述对象一致。由于产品版本升级或其它原因，本手册内容会不定期更新。

1.2 界面风格

WEB 管理界面遵循浏览器的习惯用法，如下所示：

单选框：选中代表只选用此项功能。

复选框：选中代表此选项所述功能被选中。

新增 按钮：单击则执行该按钮的动作。

文本框：输入相关参数值。

下拉列表框：通过下拉框可以找到供选择的选项。

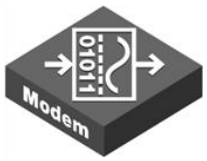
列表框：通过列表框可以找到供选择的选项。

1.3 基本约定

1.3.1 图标约定

路由器

交换机



Modem

服务器

终端

无线主机

无线接入点（AP）

PDA

AP 集中控制器（AC）

1.3.2 符号约定

注意:

用户需引起重视，注意内容中包含在原文中没有的帮助信息。.

提示:

在提示内容中可以找到解决问题的方法。

警告:

用户需引起注意，警告内容中包含危险性操作内容。

1.4 出厂配置

接口的出厂配置如下表所示。

接口类型	IP 地址/子网掩码
LAN 口	192.168.1.1/255.255.255.0
WAN 口	动态 IP 接入

系统管理员的出厂用户名为 admin，出厂密码为 admin（区分大小写）。

1.5 关键特性

- 支持 DSL、FTTX+LAN 和 Cable Modem 等多种接入方式
- 支持流量负载均衡以及线路备份
- 支持智能带宽管理功能
- 支持精细化限速
- 支持 DHCP 服务器功能
- 支持 DMZ
- 支持 PPPoE 服务器功能，提供固定 IP 分配、账号计费等功能
- 支持日常事务通告、账号到期通告功能
- 支持 WEB 认证功能
- 支持对用户的上网行为管理，提供丰富的管控策略
- 支持上网行为审计功能
- 支持 URL、MAC 地址、关键字过滤等防火墙策略
- 支持 QQ、MSN 白名单
- 支持内/外网攻击防御
- 支持端口镜像
- 支持地址组、时间段管理
- 支持 VPN 功能

- 支持动态域名（3322.org、花生壳、dyndns.org、no-ip.com、uttcare.com）
- 支持 HTTP 远程管理
- 支持 WEB 升级方式
- 支持 WEB 配置文件备份与导入

提示:

艾泰科技宽带网关所支持的功能根据各产品型号的不同而有所差异。各产品之间的功能、性能差异数据可从附赠的产品速查表中获取，或致电艾泰科技客户服务部进行咨询。

1.6 规格

- 符合 IEEE802.3Ethernet 以及 IEEE802.3u Fast Ethernet 标准。
- 支持 TCP/IP、DHCP、ICMP、NAT、PPPoE、静态路由等协议。
- 各个物理端口均支持自动协商功能、支持 MDI/MDI-X 正反线自适应。
- 提供状态指示灯。
- 工作环境：温度：0-40℃ 高度：0-4000m

  相对湿度：10-90%，不结露

1.7 联系我们

如果您在安装或使用过程中有任何疑问，请通过以下方式联系我们。

客服热线：4006-120-780

艾泰讨论区：http://www.utt.com.cn/discuzx/forum.php

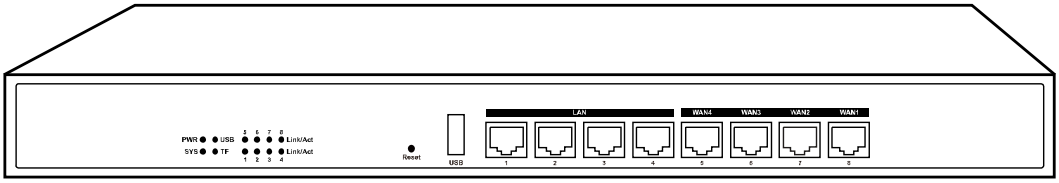
E-mail 支持：support@utt.com.cn

第 2 章 硬件安装

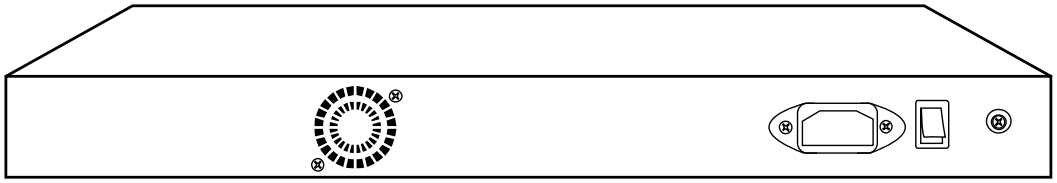
2.1 面板介绍

如下产品图片仅供参考，产品以实物为准。

前面板示意图：



后面板示意图：



指示灯说明:

指示灯	描述	功能
PWR LED	电源指示灯	电源工作正常时常亮。
SYS LED	系统状态指示灯	以每秒 2 次的频率闪烁，系统负担较大时，闪烁频率降低；有故障时常亮或常灭。
Link/Act LED	端口状态指示灯	当有设备正常连接到某端口后，该端口对应指示灯常亮，该端口有流量时闪烁。
USB LED	USB 接口状态指示灯	U 盘连接正常时常亮。
TF LED	TF 卡接口状态指示灯	TF 卡连接正常时常亮。

接口、按钮说明:

接口/按钮	说明	备注
LAN 网口	集成多个交换式以太网口。 部分产品仅提供一个 LAN 端口。	LAN/WAN 都为 RJ-45 端口，支持正反线自适应。

WAN 网口	WAN 口数量由产品型号决定。	
USB 接口	用于插入 U 盘。	
TF 卡插槽	用于插入内存卡。	
Console	符合 RS232 标准的异步通信串口。	部分产品支持 Console 口。
Reset 按钮	在忘记管理员口令时可通过此按钮将设备恢复到出厂时的配置。操作方法为：在设备带电运行过程中，按住 Reset 按钮 5 秒钟以上，再松开此按钮。操作完成后设备将恢复到出厂时的配置，并自动重启。 **提示：**上述操作会删除设备原来的所有配置，请谨慎使用。	

2.2 安装注意事项

1. 使用原装电源适配器或电源线。
2. 避免摆放重物在路由器上。
3. 雷雨天气请将路由器电源及所有连线拆除，以免遭雷击破坏。
4. 在储存、运输和运行环境中，请注意防水。
5. 尽量将路由器安装在远离强功率无线电、雷达发射台的地方。
6. 安装过程中电源保持关闭状态，同时佩戴防静电手腕。
7. 清洁路由器之前，应先将路由器电源插头拔出，勿用湿润面料擦拭或液体清洗。
8. 定期除尘，保持室内空气清洁，以免过多灰尘落在路由器表面产生静电吸附，使金属接点接触不良。
9. 确保机架和路由器接地良好。

2.3 安装准备

1. 已向当地运营商（ISP，如中国电信、中国联通等）申请宽带服务。
2. 相关设备准备：
   （1） 调制解调器（直接接入以太网时不需要此物件）。
   （2） 集线器或交换机。
   （3） 已安装以太网卡、Internet 协议（TCP/IP）的 PC。
   （4） 电源插座。

3. 工具及线缆准备：十字螺丝刀、网线。

2.4 硬件安装

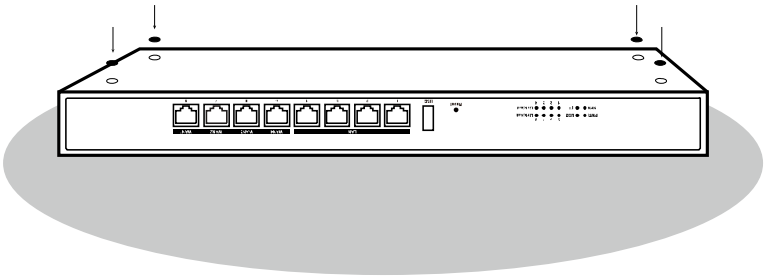
在安装设备前，请确认宽带服务正常。如果无法正常访问，请先联系运营商（ISP）解决该问题。成功访问网络后，请遵循以下步骤安装设备。安装时需拔除电源插头。

1. 安装在工作台上

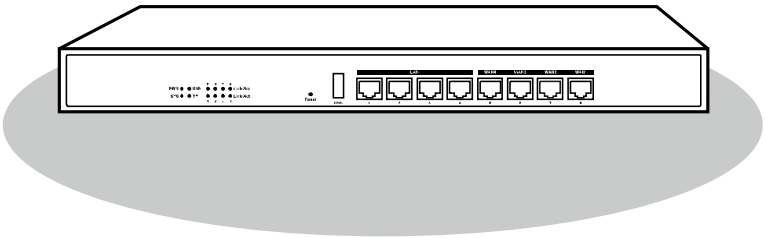
将设备放置在平稳的工作台上，安装步骤如下（部份产品脚垫已粘于主机上）：

（1） 将设备底部朝上放置在足够大、平稳且接地良好的工作台上。

（2） 揭去脚垫的胶面保护纸，把 4 个脚垫分别粘贴在机壳底部的 4 个圆型凹槽内。



（3） 把设备翻转过来，平稳地放置在工作台上。

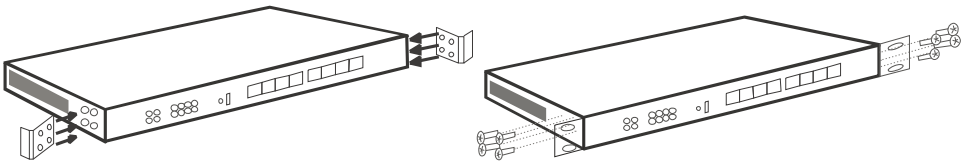


2. 安装在标准机架上

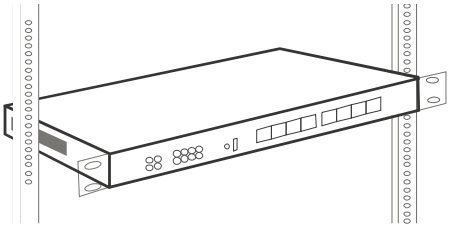
将设备安装在 19 英寸标准机架上，安装步骤如下：

（1） 检查机架的接地与稳定性。

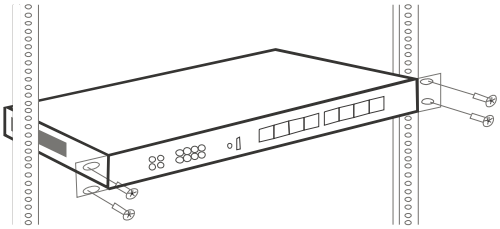
（2） 将配件中的两个 L 型支架分别安装在设备面板的两侧 ,并用配件中的螺丝固定。



（3） 将设备安放在机架内适当的位置，由托架支撑。

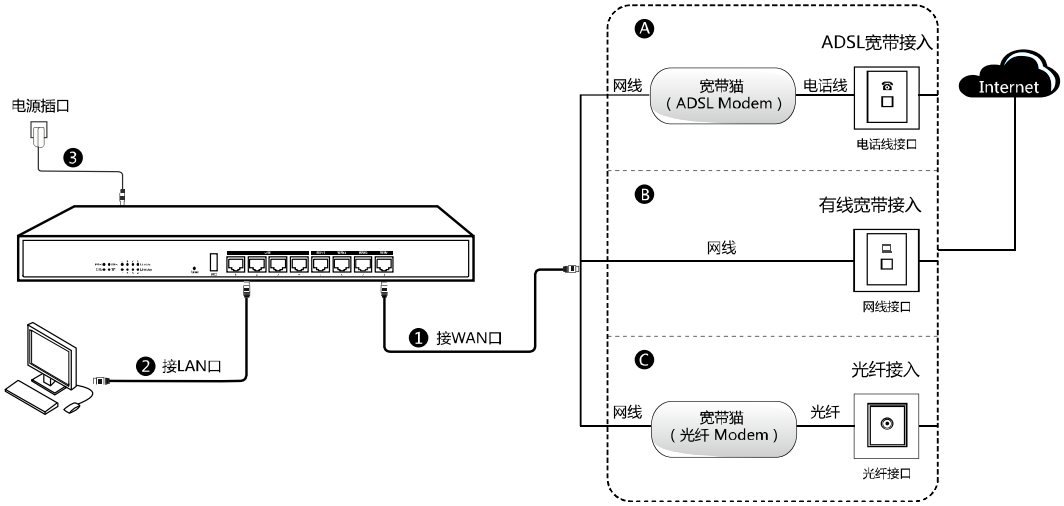


（4） 用螺钉将 L 型支架固定在机架两端固定的导槽上。



2.5 硬件连接

请依次按如下 1、2、3 顺序进行硬件连接，并根据实际情况选择相应的接入方式，如果是 ADSL 宽带接入请选择 A，如果是有线宽带接入请选择 B，如果是光纤接入请选择 C。



提示：

以上网络连接示意图仅供参考，请根据实际情况和需求配置适合的网络构架。

第 3 章 登录设备

本章介绍如何为内网计算机配置正确的网络设置、如何登录设备以及如何使用快捷图标快速链接到艾泰官网获取产品信息。

3.1 配置正确的网络设置

在通过 WEB 界面登录到设备之前，您必须对内网计算机进行正确的网络设置。

首先将计算机连接到设备的 LAN 口，接下来设置计算机的 IP 地址。

第一步，设置计算机的 TCP/IP 协议，如果已经正确设置，请跳过此步。有以下两种方法：

1. 设置计算机的 IP 地址为 192.168.1.2-192.168.1.254 中的任意一个地址，子网掩码为 255.255.255.0，默认网关为 192.168.1.1（设备的 LAN 口 IP 地址），DNS 服务器为当地运营商提供的地址。
2. 设置计算机的 TCP/IP 协议为“自动获取 IP 地址”。设置好后，路由器内置的 DHCP 服务器将自动为计算机分配 IP 地址。

第二步，在计算机上使用 Ping 命令检查其是否与路由器连通。在桌面上单击“开始>运行”，输入“cmd”，点击“确定”，打开命令窗口。输入“ping 192.168.1.1”。

下面列举在 Windows XP 环境中执行 Ping 命令的两种结果：

如果屏幕显示如下，表示计算机已经成功和路由器建立连接。

```
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

如果屏幕显示如下，表示计算机和路由器连接失败。

```
Pinging 192.168.1.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.1.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

连接失败时，请做以下检查：

1. 硬件连接：设备面板上与该 LAN 口对应的指示灯和计算机网卡灯必须亮。
2. 计算机 TCP/IP 属性的配置：如果路由器 LAN 口 IP 地址为 192.168.1.1，那么计算机的 IP 地址必须为 192.168.1.2-192.168.1.254 中的任意一个空闲地址。

3.2 登录设备

计算机使用 MS Windows、Macintosh、Unix 或者 Linux 操作系统时，都可以通过浏览器（Internet Explorer 或 Firefox 等）对路由器进行配置。

1. 打开浏览器，在地址栏里输入设备 LAN 口的 IP 地址，如 http://192.168.1.1。
2. 连接建立后，将会看到如下图所示的登录界面。在该登录界面输入用户名和密码。首次使用时需以系统管理员的身份登录，用户名、密码的出厂值均为 admin、admin，区分大小写。注意默认情况下输入 10 次错误密码，用户将被锁定 10 分钟。

3. 点击“登录”按钮，进入操作页面。
4. 如果需要重新输入所有登录信息，单击“重填”按钮，则清空输入的用户名、密码。

5. 退出当前登录，单击页面右上角的“注销”，重新返回到登录页面。

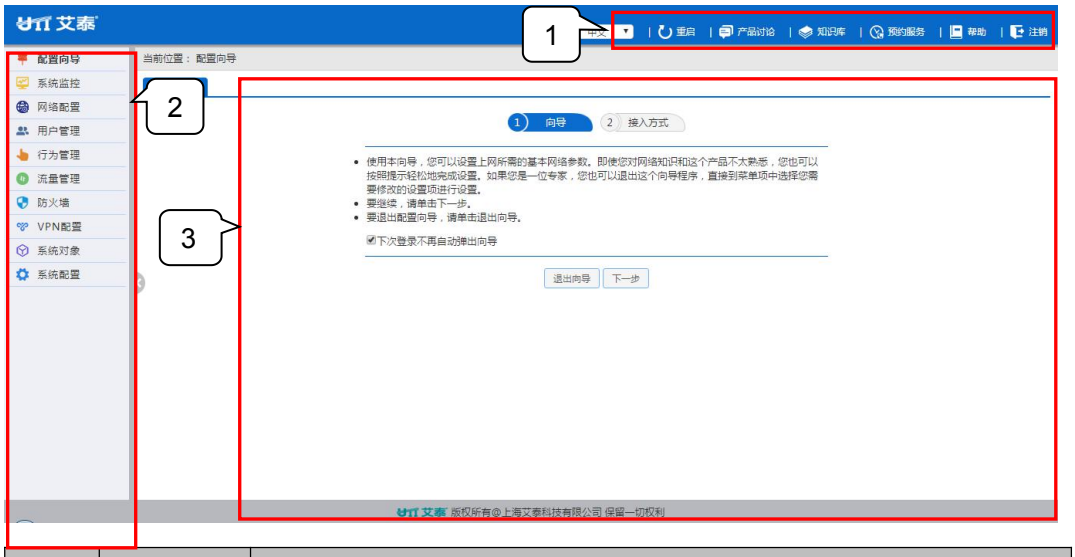
6. 用户登录成功后，在固定时间内未进行任何操作（缺省超时时间为 10 分钟），系统自动注销当前登录。再次输入用户名和密码后，重新返回到登录页面。

3.3 Web 页面介绍

介绍 Web 界面的主要构成部分与作用。

3.3.1 页面区域表

Web 界面的页面布局，主要包含以下几个区域：



序列	名称	说明
1	操作按钮	用户可以通过此区域，实现快速切换系统语言、获取帮助和退出登录系统的功能。
2	菜单导航	以导航树的模式显示各页签下的具体功能分类。点击节点，即可进入相应功能的配置页面。
3	操作区	用户可在此区域进行具体的功能配置，或者查看功能状态。

3.3.2 操作按钮

操作按钮位于界面的右上方，提供以下功能：

按钮	功能
语言栏	选择系统显示语言。
重启	单击重启路由器。
产品讨论	链接到艾泰科技官方网站的讨论区，参与产品的讨论。
知识库	链接到艾泰科技官方网站的知识库，查找相关技术资料。

预约服务	链接到艾泰科技官方网站预约服务页面，提前预约某一个工作时段的客户服务。
帮助	单击“帮助”后，将以网页形式打开当前操作区对应的联机帮助信息。
注销	单击“注销”，将安全退出本次登录。如果希望重新进入 Web 界面，需要再次输入用户名和密码。

3.3.3 操作区

操作区是 Web 界面的主要组成部分。

通过菜单导航与操作区之间的“  ”可以隐藏或显示菜单导航，以在必要的时候给操作区提供足够的显示空间。

第 4 章 配置向导

首次登录 Web 界面需要对系统进行初始化配置，便于基本通信。配置向导按步骤指导您配置上网所需基本参数，使内网用户通过设备快速连接因特网。

单击“下一步”，进入“接入方式”配置页面。根据运营商提供的上网参数确定上网连接方式。

选项	描述
动态接入	点击“保存”按钮完成 WAN 口网络接入配置。 使用动态接入方式，设备从运营商 DHCP 服务器处获取 IP 地址。每次拨通运营商的主机后，路由器自动获得一个动态的 IP 地址。任意两次连接所获取的 IP 地址很可能不同，但是在每次连接时间内 IP 地址保持不变。
固定接入	输入申请宽带时运营商提供的 IP 地址、子网掩码、网关地址、DNS 服务器地址后，点击“保存”按钮完成 WAN 口网络接入配置。
PPPoE 接入	输入申请宽带时运营商提供的用户名和密码后，点击“保存”按钮完成 WAN 口网络接入配置。 PPPoE 是基于以太网的点对点协议。该协议具有用户认证及通知 IP 地址的功能，是在以太网络中转播 PPP 帧信息的技术，适用于 ADSL 方式。

提示:

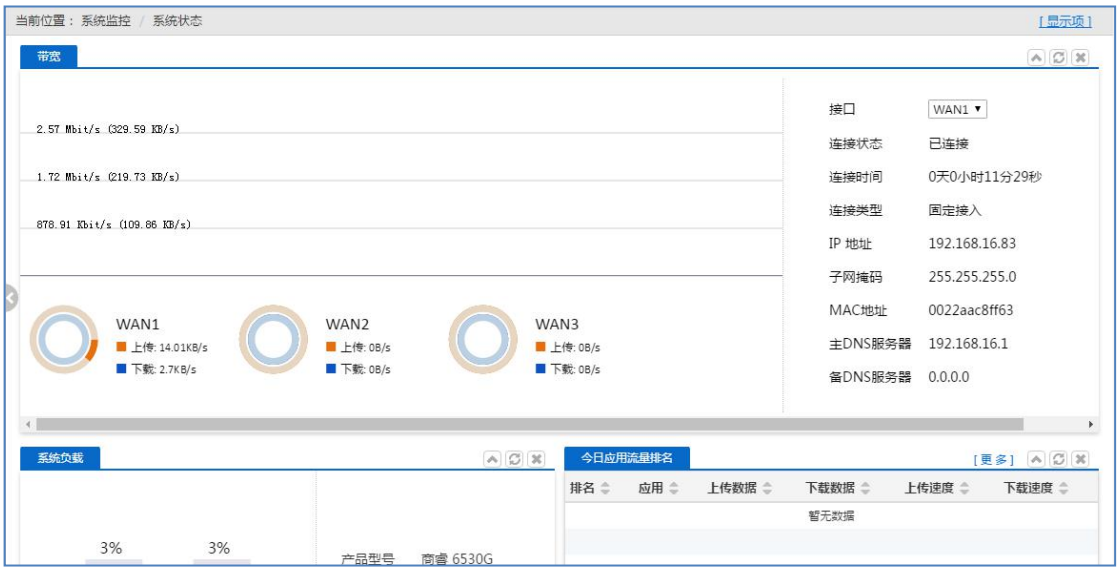
配置完 WAN 口线路的连接方式，可在“网络配置 > 外网配置”页面查看连接状态。

第 5 章 系统监控

5.1 系统状态

查看系统状态信息，了解路由器的当前运行情况，保证路由器工作正常。用户可定制显示在该页面的内容。

进入页面的方法：“系统监控 > 系统状态”。



系统状态页面用图表形式显示如下内容：

- 带宽：显示路由器各接口的状态信息，包括接口的实时上传下载流量、连接状态等。
- 系统负载：显示系统资源使用情况和系统信息。当系统资源占用超过 50%后用红色突出显示。
- 今日应用流量排名：只有开启流量监控功能才会产生应用流量排名统计信息。
- 今日用户网络流量排名：显示今日（从 0 点到 24 点）的网络流量使用排名情况。
- VPN 状态：显示当前已经建立的 VPN 隧道的实时状态。

提示:

不同型号、不同配置的路由器的状态显示存在差异，请以路由器的实际情况为准。

定制显示内容

路由器提供多种状态窗口，方便您了解路由器的当前运行情况。定制显示的窗口的操作步骤如下：

1. 单击页面右上角的[显示项]。
2. 勾选需要显示的状态窗口。

5.2 流量监控

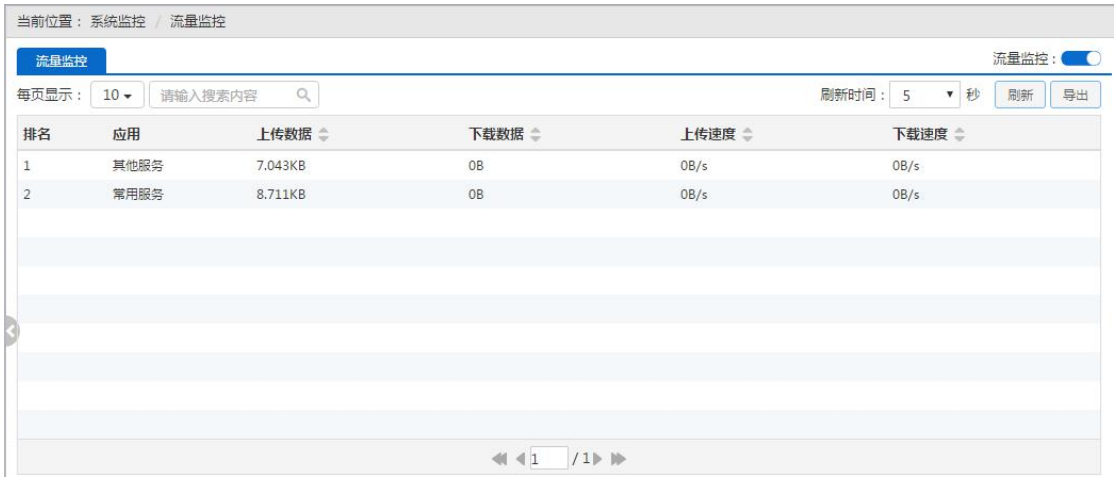
通过流量监控了解今日各应用分类的流量使用情况。系统已将各应用进行分类归纳，按照如下步骤查看各应用分类情况。

1. 选择“行为管理 > 行为管理”页面。
2. 点击“新增”按钮并在跳转后的页面中单击“应用服务”文本框。
3. 在弹出的应用列表中查看详细应用分类情况。

提示:

只有开启流量监控功能才会产生应用流量统计信息。

进入页面的方法：“系统监控 > 流量监控”。



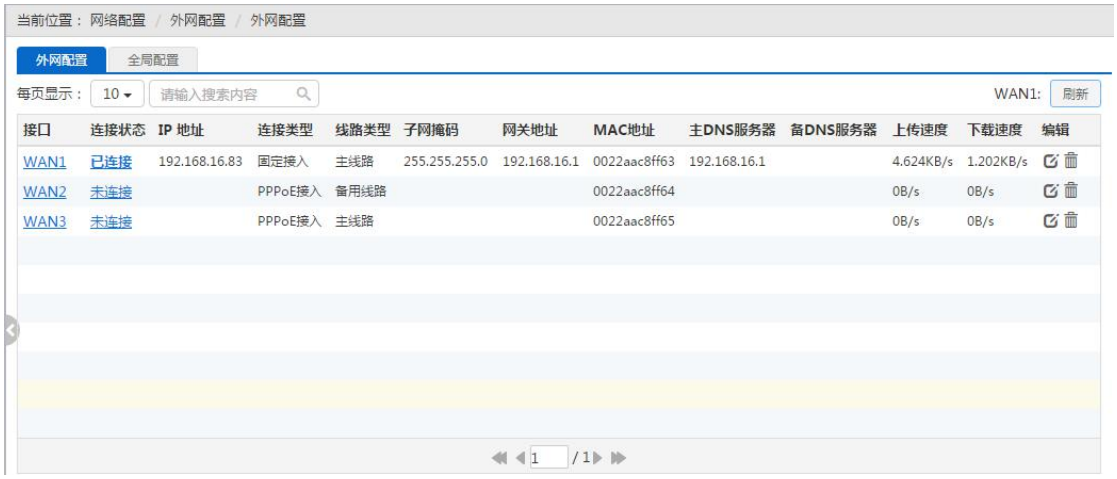
第 6 章 网络配置

6.1 外网配置

在本页面配置各 WAN 口的线路信息，也可以查看线路的连接状态。

6.1.1 外网配置

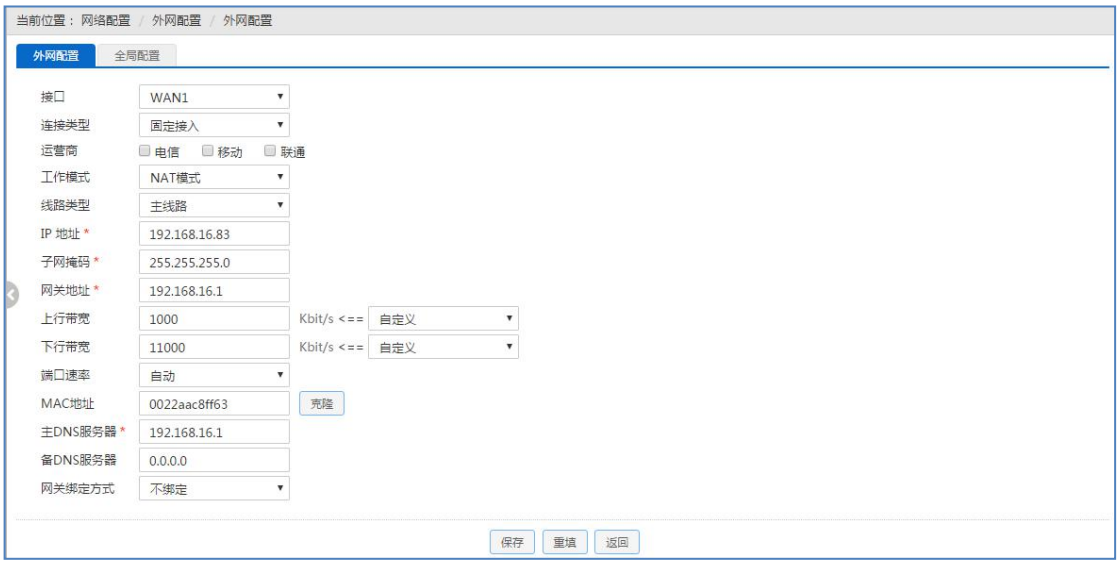
配置 WAN 口与外网的连接方式。进入页面的方法：“网络配置 > 外网配置 > 外网配置”。



单击各 WAN 接口相应的 编辑按钮，配置外网连接方式。路由器支持三种连接方式：固定接入、动态接入和 PPPoE 接入。根据线路的连接类型不同，需要配置的参数也不同。如下根据三种连接方式分别介绍配置参数。

1. 固定接入

路由器长期使用固定 IP 地址接入外网，一般是特殊的服务器才使用固定 IP 地址接入网络。



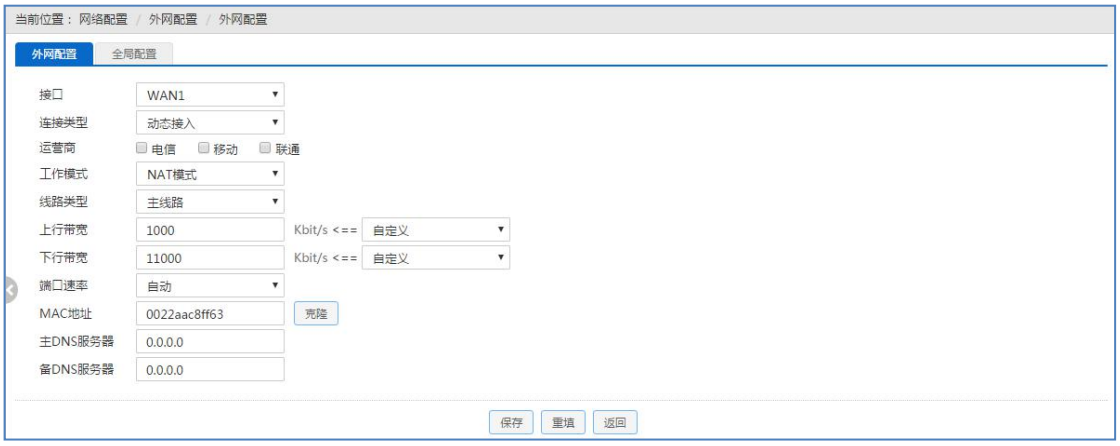
页面参数配置介绍：

选项	描述
接口	选择配置的接口。
连接类型	选择“固定接入”。
运营商	选择该接口的运营商策略，提供三个选项供选择：电信、移动、联通。当有多条线路连接外网时，系统将根据用户的选择生成相对应的路由，可以方便地实现电信流量走电信线路，联通流量走联通线路。
工作模式	选择上网方式。提供两个选项供选择：路由模式和 NAT 模式。 若无法确认上网方式，请选择“NAT 模式”。
线路类型	选择此接口代表的线路类型，提供两个选项供选择：主线路，备份线路。系统默认开启智能负载均衡模式，当有线路出现故障时，不同的线路类型，流量的走向也不同，详情参阅章节：智能负载均衡。
IP 地址	输入运营商提供的 IP 地址。
子网掩码	输入运营商提供的子网掩码。
网关地址	输入运营商提供的网关地址。
上、下行带宽	配置该线路允许通过的最大上、下行带宽。建议配置为运营商分配的带宽，即申请带宽时，运营商提供的上、下行带宽。只有正确配置上、下行带宽，“应用优先”、“保障带宽”等功能才能正常运行。
端口速率	配置该接口的双工模式及速率。一般情况下不需要修改，如有兼容性问题或使用的设备不支持自动协商功能，可以在这里设置以太网协商的类型。
MAC 地址	相应接口的 MAC 地址。一般不建议修改接口的 MAC 地址。但在某些情况下，运营商将设备的 MAC 做了绑定，这样造成新的网络设备无法拨号成功，此时需要将设备的 MAC 地址修改为原网络设备的 MAC 地址。

主 DNS 服务器	输入运营商提供的 DNS 服务器地址。
备 DNS 服务器	输入运营商提供的备用 DNS 服务器地址。
网关绑定方式	绑定上层网关地址的方式，提供的选项为：不绑定、手工绑定。选择“手动绑定”时可点击“获取”按钮获取上层网关 MAC，也可自己手动输入上层网关 MAC。注意：当绑定错误的网关 MAC 时，上网功能会异常。

2. 动态接入

通过运营商 DHCP 服务器动态分配的 IP 地址实现上网。



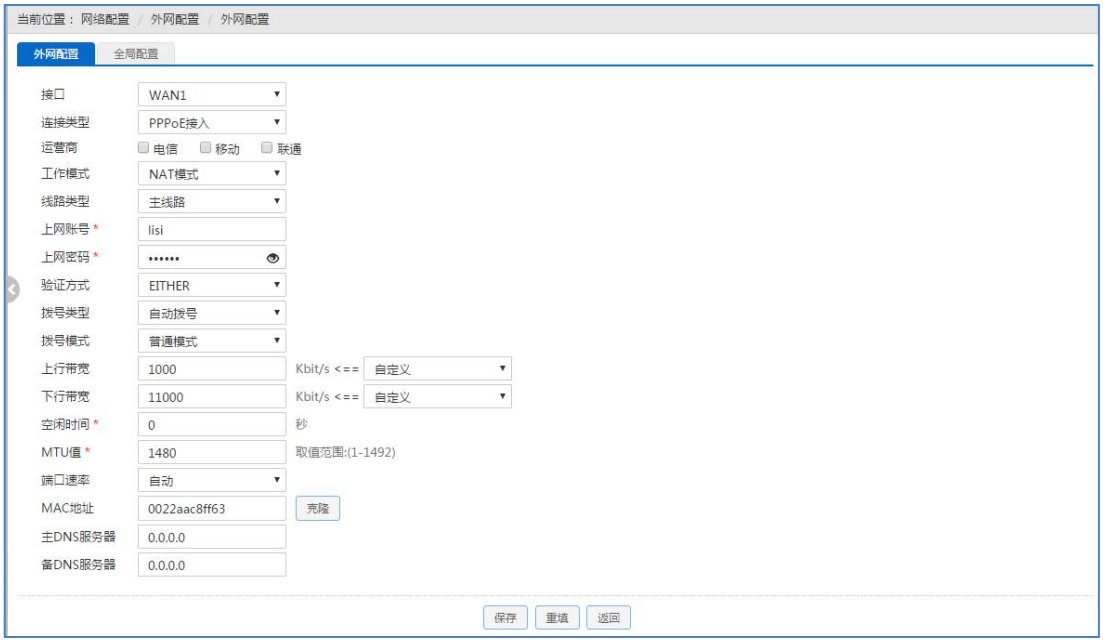
页面参数配置介绍：

选项	描述
接口	选择配置的接口。
连接类型	选择“动态接入”。 使用动态 IP 接入方式，设备从运营商 DHCP 服务器处获取 IP 地址。每次拨通运营商的主机后，路由器自动获得一个动态的 IP 地址。任意两次连接所获取的 IP 地址很可能不同，但是在每次连接时间内 IP 地址保持不变。
运营商	选择该接口的运营商策略，提供三个选项供选择：电信、移动、联通。当有多条线路连接外网时，系统将根据用户的选择生成相对应的路由，可以方便地实现电信流量走电信线路，联通流量走联通线路。
工作模式	选择上网方式。提供两个选项供选择：路由模式和 NAT 模式。若无法确认上网方式，请选择“NAT 模式”。
线路类型	选择此接口代表的线路类型，提供两个选项供选择：主线路，备份线路。系统默认开启智能负载均衡模式，当有线路出现故障时，不同的线路类型，流量的走向也不同，详情参阅章节：智能负载均衡。
上、下行带宽	配置该线路允许通过的最大上、下行带宽。建议配置为运营商分配的带宽，即申请带宽时，运营商提供的上、下行带宽。只有正确配置上、下行带宽，“应用优先”、“保障带宽”等功能才能正常运行。
端口速率	配置该接口的双工模式及速率。一般情况下不需要修改，如有兼容性

	问题或使用的设备不支持自动协商功能，可以在这里设置以太网协商的类型。
MAC 地址	相应接口的 MAC 地址。一般不建议修改接口的 MAC 地址。但在某些情况下，运营商将设备的 MAC 做了绑定，这样造成新的网络设备无法拨号成功，此时需要将设备的 MAC 地址修改为原网络设备的 MAC 地址。
主、备DNS服务器	输入 DNS 服务器地址，优先级高于上层设备下发的 DNS 服务器地址。

3. PPPoE 接入

PPPoE 全称 Point to Point Protocol over Ethernet，是基于以太网的点对点协议。该协议具有用户认证及通知 IP 地址的功能，是在以太网络中转播 PPP 帧信息的技术，适用于 ADSL 方式。



页面参数配置介绍：

选项	描述
接口	选择配置的接口。
连接类型	选择“PPPoE 接入”。
运营商	选择该接口的运营商策略，提供三个选项供选择：电信、移动、联通。当有多条线路连接外网时，系统将根据用户的选择生成相对应的路由，可以方便地实现电信流量走电信线路，联通流量走联通线路。
工作模式	选择上网方式。提供两个选项供选择：路由模式和 NAT 模式。若无法确认上网方式，请选择“NAT 模式”。

线路类型	选择此接口代表的线路类型，提供两个选项供选择：主线路，备份线路。系统默认开启智能负载均衡模式，当有线路出现故障时，不同的线路类型，流量的走向也不同，详情参阅章节：智能负载均衡。
上网账号	在运营商办理业务时，运营商提供的用户名。
上网密码	在运营商办理业务时，运营商提供的密码。
验证方式	ISP 验证用户名及密码的方式，默认为 EITHER。多数地区为 PAP 方式，也有少数地区采用 CHAP 方式，NONE 表示不进行用户名和密码验证，EITHER 表示自动和对方设备协商采用哪种验证方式。
拨号类型	通常选择“自动拨号”，当上网方式为按流量或按时计费时，可选择手动拨号或按需拨号。 • 自动拨号：启用路由器或者上一次拨号断线后，系统自动拨号连接。 • 手动拨号：点击在“网络配置 > 外网配置 > 外网配置”页面的各线路的“连接状态”，页面的右上方显示“拨号”、“挂断”等按钮，点击按钮进行手动拨号或挂断。 • 按需拨号：当内网访问 Internet 产生流量时，设备自动进行连接。
拨号模式	选择 PPPoE 拨号的模式。默认为普通模式。在使用正确的用户名和密码的前提下，如果拨号不成功，可以尝试使用其它模式。
上、下行带宽	配置该线路允许通过的最大上、下行带宽。建议配置为运营商分配的带宽，即申请带宽时，运营商提供的上、下行带宽。只有正确配置上、下行带宽，“应用优先”、“保障带宽”等功能才能正常运行。
空闲时间	无访问流量后自动断线前等待的时长，0 代表不自动断线。
MTU 值	最大传输单元。在传送数据单元时，设备将自动与对端设备协商最佳的传送数据单元大小，除非特别应用，不要修改此参数。
端口速率	配置该接口的双工模式及速率。一般情况下不需要修改，如有兼容性问题或使用的设备不支持自动协商功能，可以在这里设置以太网协商的类型。
MAC 地址	相应接口的 MAC 地址。一般不建议修改接口的 MAC 地址。但在某些情况下，运营商将设备的 MAC 做了绑定，这样造成新的网络设备无法拨号成功，此时需要将设备的 MAC 地址修改为原网络设备的 MAC 地址。
主、备DNS服务器	输入 DNS 服务器地址 ,优先级高于上层设备下发的 DNS 服务器地址。

智能负载均衡

设备提供了 2 种线路类型：主线路和备份线路。所有线路默认都是主线路，用户可以根据需要将某些线路划分到备份线路组中。

在所有线路均作为主线路使用时，智能负载均衡模式的工作原理如下：

1. 当所有线路都正常时，内网主机将同时使用所有线路上网。
2. 若某条线路出现故障 ,则立即屏蔽该线路 ,原先通过该线路的流量将分配到其他线路上。
3. 一旦故障线路恢复正常，设备会自动启用该线路，流量自动重新分配。

当部分线路为主线路，部分线路为备份线路时，智能负载均衡模式的工作原理如下：

1. 只要主线路正常，内网主机仅使用主线路上网。
2. 若主线路出现故障，则自动切换到使用备份线路上网。
3. 一旦故障主线路恢复正常，则立即切换回主线路。

提示:

当某条线路中断进行线路切换时，某些用户应用（比如部分网络游戏）可能会意外中断，这是由于 TCP/IP 协议的机制决定的。

6.1.2 全局配置

身份绑定

在多线路会话负载均衡的情况下，同一应用的 NAT 会话可能分布在不同的线路上，这样就会导致像网银、QQ 等应用由于身份变化而不能正常使用，身份绑定功能通过将这些来自同一用户的同一应用的会话绑定在一条线路上解决了这个问题。举个例子来说，内网某个用户在登录网上银行时，如果第一条会话被分配到 WAN2 口连接线路上，此后此用户所有的网银会话都会走 WAN2 口出去，直到此用户退出登录。

线路检测

要保证线路出现故障时网络不中断，要求设备能够实时监控线路状态。为此，我们为设备设计了灵活的自动检测机制，并提供多种线路检测方法供用户选择，以满足实际应用的需要。

为方便理解，先介绍几个相关参数。

检测间隔：发送检测包的时间间隔，一次发送一个检测包，缺省值为 0 秒。特别地，该值为 0 时，表示不进行线路检测。

检测次数：每个检测周期内，发送检测包的次数。

目标 IP 地址：检测的对象，设备将向预先指定的检测目标发送检测包以检测线路是否正常。

下面将分别介绍在线路正常和线路故障这两种情况下，设备的线路检测机制。

某条线路故障时，检测机制为：设备每隔指定的检测间隔向该线路的检测目标发送一个检测包，如果在某个检测周期内，发送的所有检测包都没有回应，就认为该线路出现故障，并立即屏蔽该线路。例如，缺省情况下，若某个检测周期内，发送的 3 个检测包都没有回应，就认为该线路出现故障。

某条线路正常时，检测机制为：设备每隔指定的检测间隔向该线路的检测目标发送一个检测包，如果在某个检测周期内，发送的检测包中有一半及以上数量的检测包有回应时，就认为该线路已经正常，并恢复启用该线路。例如，缺省情况下，若某个检测周期内，有 2 个检测包有回应，就认为该线路恢复正常。

设备允许用户预先为内网中的某些主机指定上网线路，它是通过设置线路的“内部起始 IP 地址”和“内部结束 IP 地址”来实现的，IP 地址属于两个地址范围内的主机将优先使用指定线路。对于已指定上网线路的主机来说，当指定线路正常时，它们只能通过该线路上网；但是，当指定线路有故障时，它们会使用其他的正常线路上网。

配置均衡模式和线路检测机制

进入页面的方法：“网络配置 > 外网配置 > 全局设置”。

页面参数配置介绍：

选项		描述
均衡模式	身份绑定	开启或关闭身份绑定功能。
线路检测	检测间隔	配置发送检测线路数据包的时间间隔，一次发送一个检测包，缺省值为 0 秒，表示不进行线路检测。
	检测次数	配置检测线路周期内发送检测数据包的次数 ,每次发送一个检测包，缺省值为 10，取值范围为 3-1000。

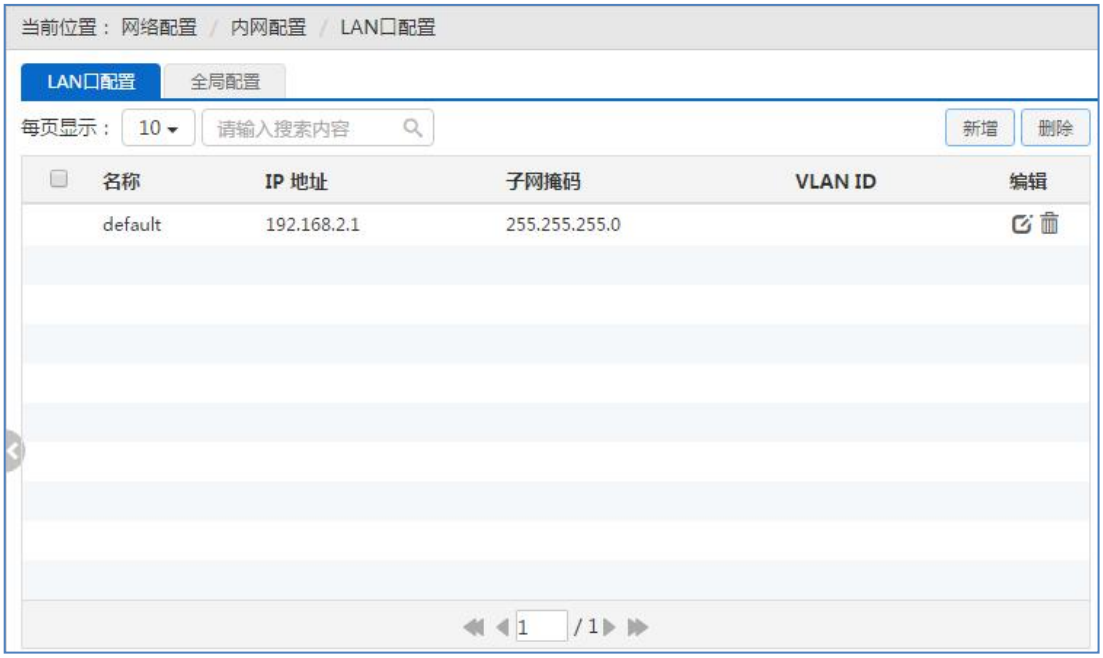
	带宽选择	ISP 提供的带宽。
	检测目标	配置欲检测的目标 IP 地址。检测的对象，设备将向预先指定的检测目标发送检测数据包以检测线路是否正常。

6.2 内网配置

设备默认 LAN 口的 IP 地址为 192.168.1.1，支持新增、修改、删除 LAN 口的 IP 地址以适应当前网络环境。

6.2.1 LAN 口配置

进入页面的方法：“网络配置 > 内网配置 > LAN 口配置”。



单击“新增”按钮，配置 LAN 口 IP 地址。

页面参数配置介绍：

选项	描述
名称	配置接口的名称。
IP 地址	配置接口的 IP 地址。
子网掩码	配置接口的子网掩码。
VLAN ID	配置接口 VLAN ID，路由器通过 VLAN ID 识别接入者身份，从而对接入者分类作流量限制、安全认证等策略。此功能必须配合支持 802.Q vlan 的设备使用，例如管理型交换机、艾泰 AP 等。

注意：修改过原有 LAN 口 IP 地址后，必须使用新的 IP 地址重新登录设备，且登录主机的 IP 要和其在同一网段。

6.2.2 全局设置

配置接口的 MAC 地址与接口模式。

进入页面的方法：“网络配置 > 内网配置 > 全局配置”。

页面参数配置介绍：

选项	描述
MAC 地址	LAN 口的 MAC 地址。建议不要随意修改 LAN 口的 MAC 地址。
接口模式	配置该接口的双工模式及速率。提供的选项为：Auto、10M 半双工、10M 全双工、100M 半双工、100M 全双工、1000M 全双工。一般情况下不需要修改，如有兼容性问题或使用的设备不支持自动协商功能，可以在这里设置以太网协商的类型。

6.3 DHCP 服务

DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）是一个局域网的网络协议，用来给内部网络自动分配 IP 地址，对网络管理员来说，是对所有计算机作中央管理的手段。有 DHCP 服务器与 DHCP 客户端之区别， DHCP 服务器控制一段 IP 地址范围，当客户端连接到服务器时可以自动获得服务器分配的 IP 地址和子网掩码等信息。每次客户端连接服务器时所获得的 IP 地址可能不同。当一客户端下线后，DHCP 服务器会收回已分配的 IP 地址并分配给其它上线的客户端。这样可以有效节约 IP 地址，既保证了网络通信，

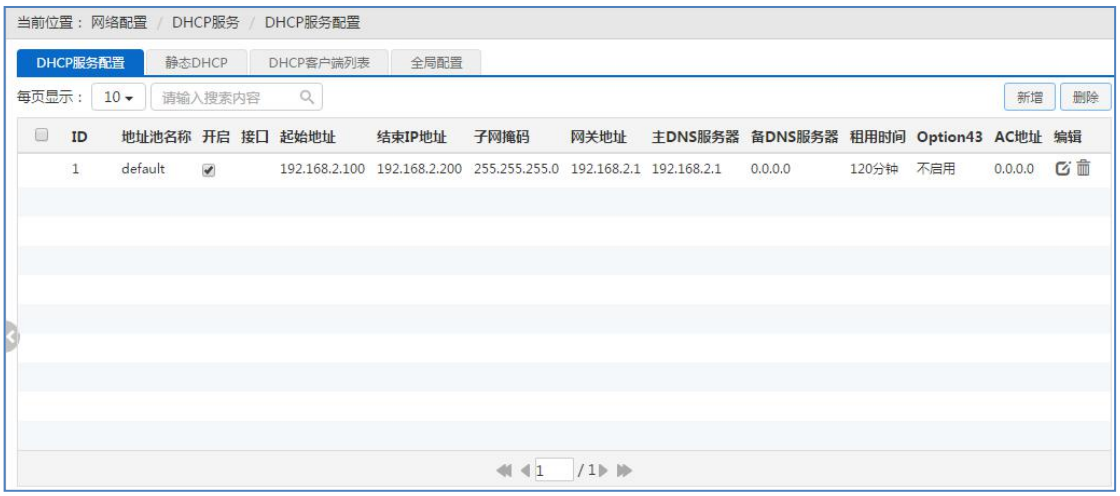
又提高 IP 地址的使用率。

6.3.1 DHCP 服务配置

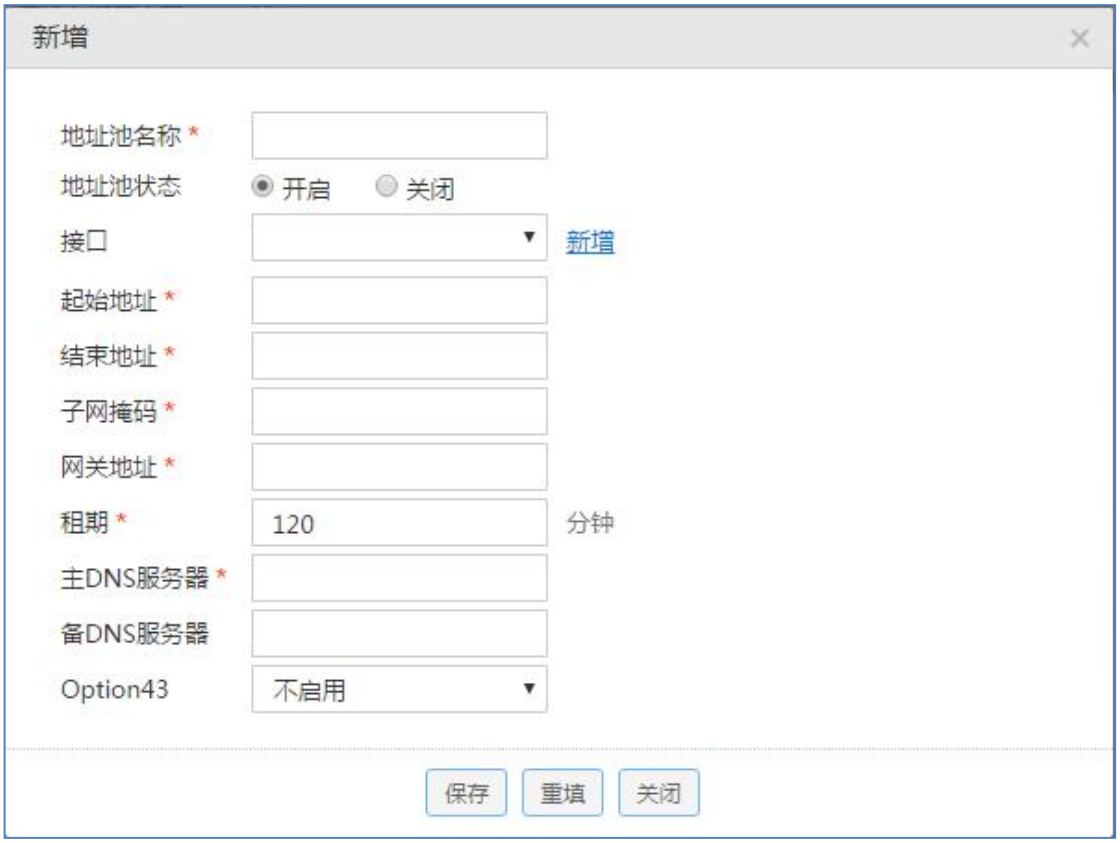
设备默认将 default 地址池中的地址下发给客户端，管理员可通过创建新的地址池，让不同属性（如属于不同部门）的客户端获取不同网段的 IP 地址。

为方便用户对 DHCP 服务器配置的操作，提供新建、修改、删除、查询 DHCP 服务器功能。在本页面，可指定在 VLAN 接口及 LAN 口上启用 DHCP 服务器功能，分配不同网段的 IP 地址。

进入页面的方法：“网络配置 > DHCP 服务 > DHCP 服务配置”。



单击“新增”按钮，配置 DHCP 服务器地址。



页面参数配置介绍：

选项	描述
地址池名称	配置 DHCP 服务器名称。
地址池状态	启用或关闭地址池。
接口	配置 DHCP 服务器的 VLAN 接口。携带此接口所属 VLAN ID 身份识别符的接入者，将从该地址池获取地址。
起始地址、结束地址	配置 DHCP 地址池的起始 IP 地址、结束 IP 地址，起始 IP 地址与结束 IP 地址一起定义 DHCP 服务器的地址范围，注意必须保持和设备 LAN 口 IP 地址在同一网段。
子网掩码	配置 DHCP 服务器给内网计算机自动分配的子网掩码。
网关地址	下发给 DHCP 客户端的网关地址，一般为设备 LAN 口 IP 地址。
租期	内网计算机使用 DHCP 服务器分配的 IP 地址的时长。
主 DNS 服务器	DHCP 服务器给内网计算机自动分配的主 DNS 服务器 IP 地址。
备 DNS 服务器	DHCP 服务器给内网计算机自动分配的备用 DNS 服务器 IP 地址。

Option43	通过修改 dhcp 协议报文里的 option 43 可变长字段（携带有 AC 的 IP 地址），让 AP 解析 option 43 携带的 AC 地址，从而发现 AC。配置方式包含不启用、HEX 定长、ASCII 不定长、自定义四个选项。 ● HEX 定长：填写 AC 地址，将 AC 地址解析成十六进制编码数字组成。 ● ASCII 不定长：不定长编码，将 AC 地址解析成一组字符。 ● 自定义：如果配置非法，将导致 DHCP 服务器异常或 option43 配置不生效。

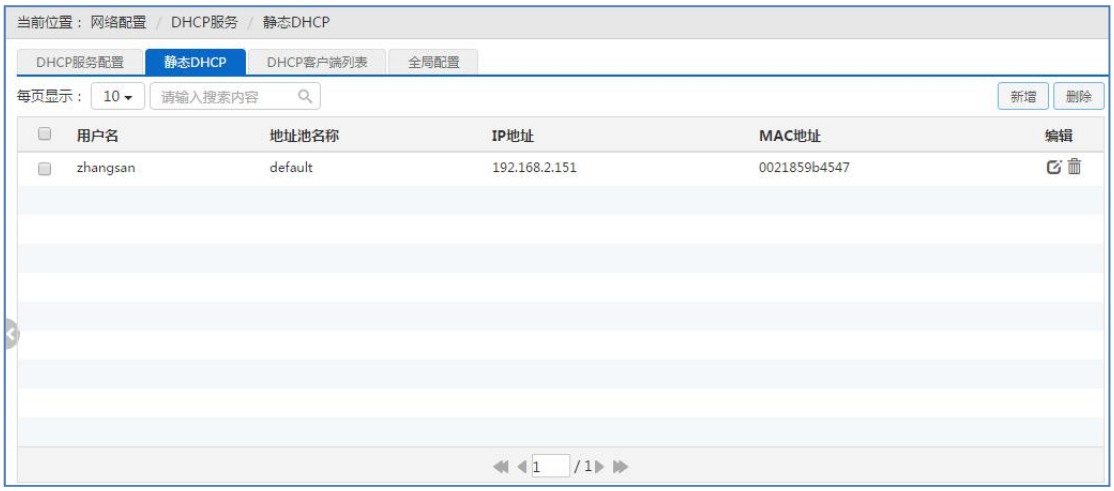
提示:

如果要使用设备的 DHCP 服务器功能，内网计算机的 TCP/IP 协议可设置为“自动获得 IP 地址”。

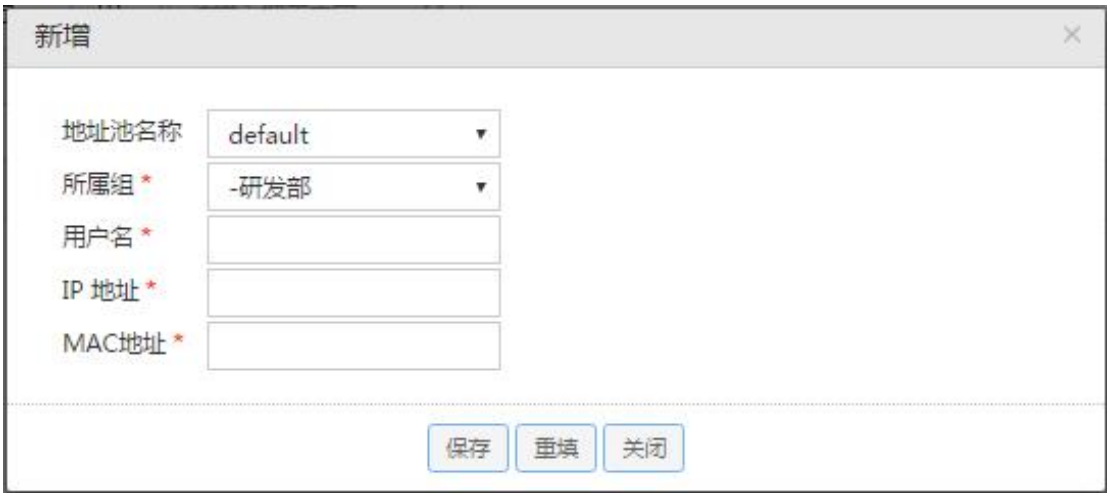
6.3.2 静态 DHCP

使用 DHCP 服务器为内网计算机配置 TCP/IP 属性是非常方便的，但会造成计算机在不同时间段被分配到不同 IP 地址。静态 DHCP 功能可以使内网计算机的 MAC 地址与 IP 地址绑定，当计算机向 DHCP 服务器（设备）申请地址时，设备根据计算机的 MAC 地址寻找对应的 IP 地址并分配给计算机，使计算机在任何时段都能使用不变的 IP 地址。

进入页面的方法：“网络配置 > DHCP 服务 > 静态 DHCP”。



单击“新增”按钮，配置静态 DHCP 条例。



页面参数配置介绍：

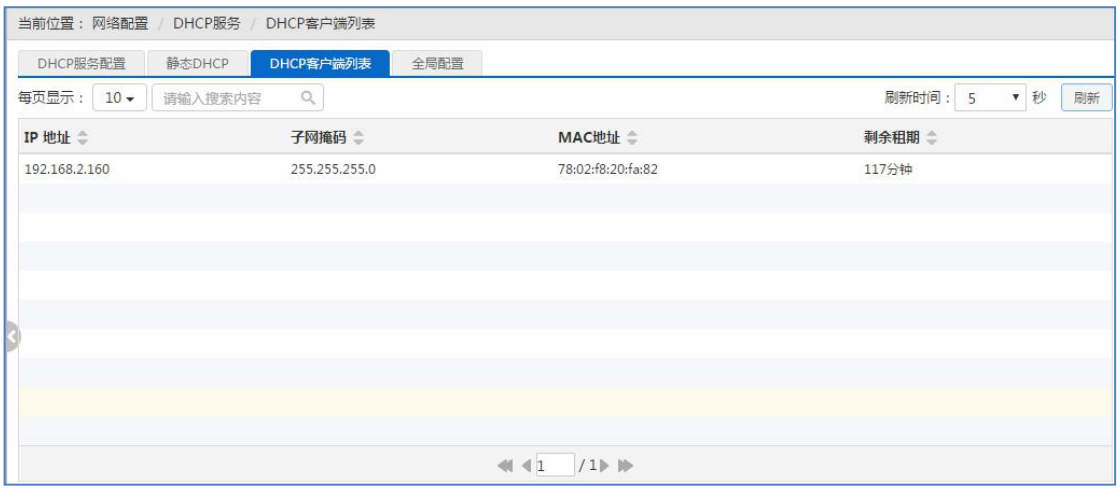
选项	描述
地址池名称	选择预留 IP 地址的所属地址池。
所属组	选择预绑定 IP 地址的计算机所属用户组。不可为空。在“用户管理>组织成员”中设置用户组及成员。
用户名	配置预绑定计算机的名称，不可重复。
IP 地址	配置预留的 IP 地址，必须是上面所设置的地址池中的合法 IP 地址。
MAC 地址	配置使用预留 IP 地址的设备 MAC 地址。

提示:

设置成功后，设备将为指定计算机固定分配预设的 IP 地址。

6.3.3 DHCP 客户端列表

查看已分配给内网计算机的 IP 地址及用户信息，包含 IP 地址、子网掩码、MAC 地址、剩余租期等。进入页面的方法：“网络配置 > DHCP 服务 > DHCP 客户端列表”。



6.3.4 全局配置

DNS 代理

开启 DNS 代理功能，可以简化局域网的配置。在路由器能正常访问 Internet 的情况下，局域网的计算机只需将 DNS 服务器配置为路由器的 LAN 口地址（局域网接在 LAN 口时）或将服务器地址获取方式设置为“自动获得 DNS 服务器地址”就可以正常访问网络。当 ISP 更改了 DNS 服务器或用户更改了所连接的 ISP 时，只需在路由器上重新配置 DNS 服务器，而无需为局域网中的每台计算机分别重新设置 DNS 服务器，局域网用户就可以正常使用 DNS 服务。

进入页面的方法：“网络配置 > DHCP 服务 > 全局配置”。

6.3.5 DHCP 配置实例

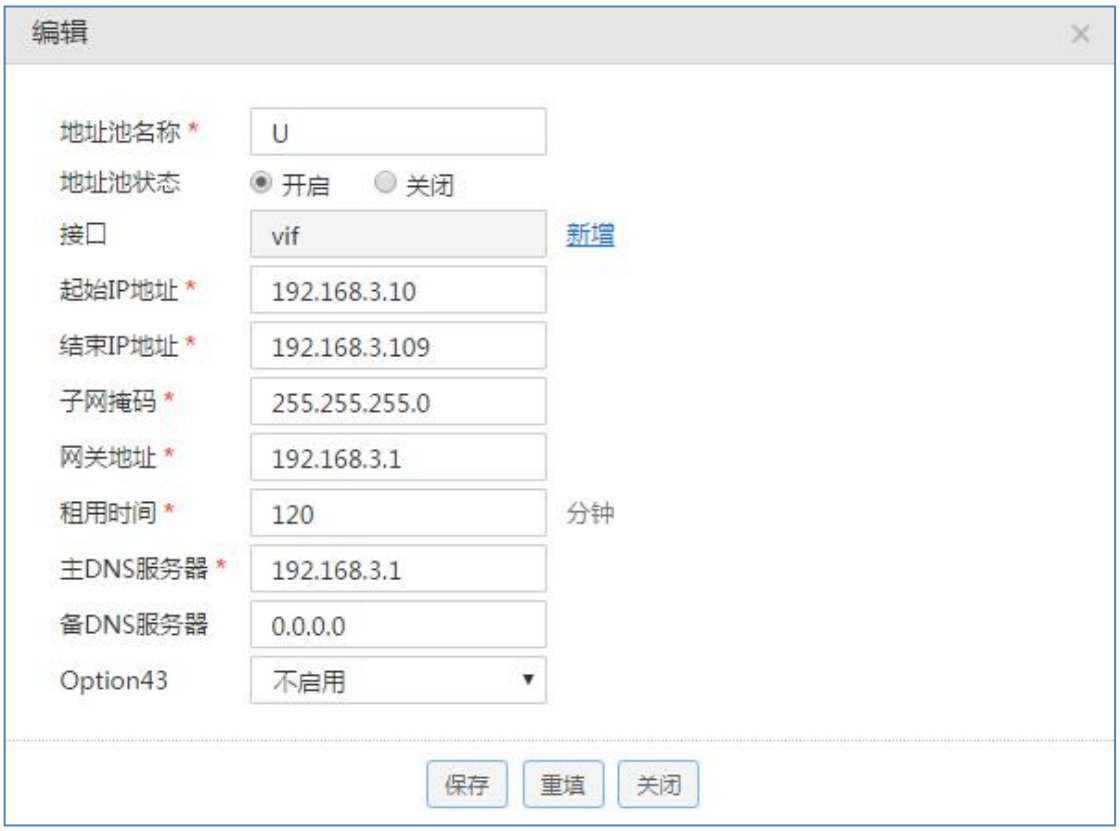
1. 应用需求

本实例中，要求设备开启 DHCP 功能，起始地址为 192.168.3.10，共可分配 100 个地址；其中 MAC 地址为 00:21:85:9B:45:46 的主机分配 192.168.3.15 的固定 IP 地址，MAC 地址为 00:1f:3c:0f:07:f4 分配 192.168.3.10 的固定 IP 地址。

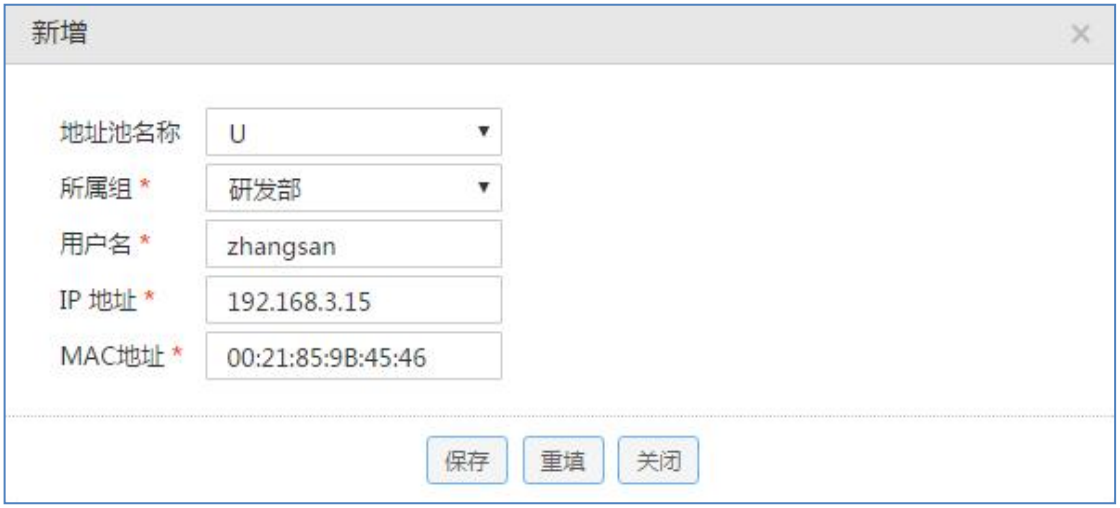
2. 配置步骤

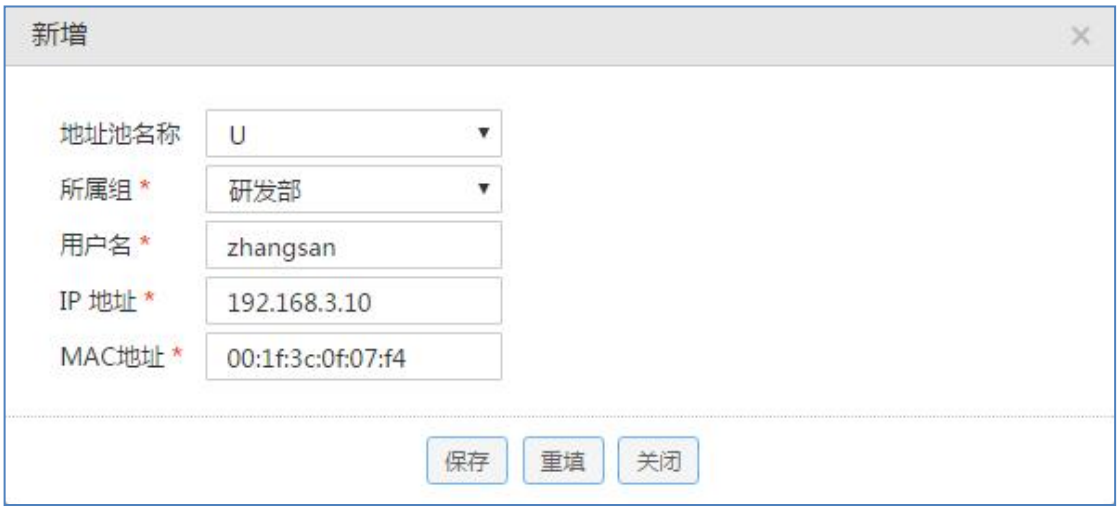
第一步，进入“网络配置 >DHCP 服务>DHCP 服务配置”页面。

第二步，点击“新增”按钮，配置相关 DHCP 服务器参数，配置完后点击“保存”。



第三步，进入“网络配置 >DHCP 服务>静态 DHCP”页面，点击“新增”按钮，配置需求中的两条静态 DHCP 实例。





至此配置完成，可以在“静态 DHCP”页面中查看这 2 个静态 DHCP 条目的相关信息。如果发现配置错误，可以直接单击对应条目的“编辑”按钮，进入静态 DHCP 配置页面中进行修改。

6.4 端口映射

6.4.1 NAT 规则

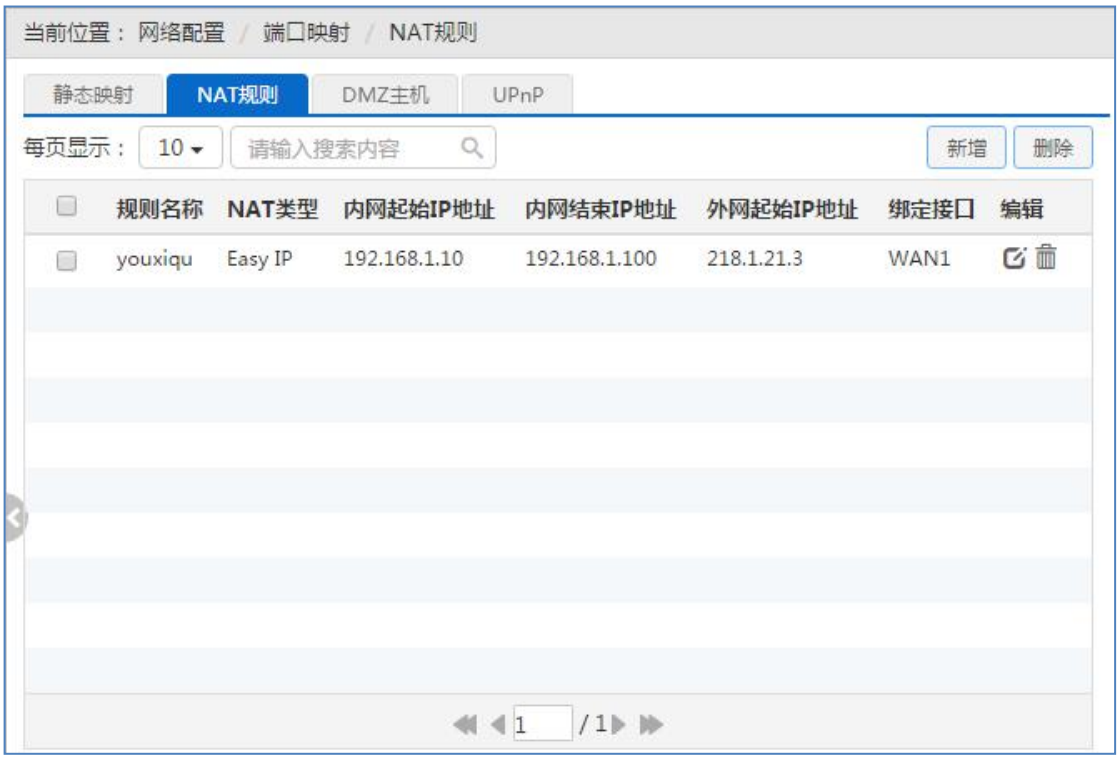
NAT： NAT（网络地址转换）是一种将一个 IP 地址域（如 Intranet）映射到另一个 IP 地址域（如 Internet）的技术。NAT 的出现是为了解决 IP 地址日益短缺的问题，NAT 允许专用网络在内部使用任意范围的 IP 地址，而对于公用的 Internet 则表现为有限的公网 IP 地址范围。由于内部网络能有效地与外界隔离开，所以 NAT 也可以对网络的安全性提供一些保证。

NAT 地址空间：为了正确进行 NAT 操作，任何 NAT 设备都必须维护两个地址空间，一个是内网主机在内部使用的私有 IP 地址，设备中用“内部 IP 地址”表示；另一个是用于外部的公网 IP 地址，设备中用“外部 IP 地址”表示。

NAT 类型：设备提供两种 NAT 类型，分别是 Easy IP 和 One2One。每个具体的 NAT 配置称为“NAT 规则”，配置 NAT 规则时必须指定其出口 IP 地址及线路。当有多个合法的公网地址时，每种类型的 NAT 规则均可配置多个。实际应用中，常常需要混合使用不同类型的 NAT 规则。

- EasyIP：即网络地址端口转换，多个内部 IP 地址映射到同一个外部 IP 地址。它可为每个内部连接动态分配一个与单一外部地址有关的端口，并维护这些内部连接到外部端口的映射，从而实现多个用户同时使用一个公网地址与外部 Internet 进行通信。
- One2One：即静态地址转换，内部 IP 地址与外部 IP 地址进行一对一的映射。此方式下，端口号不会改变。它通常用来配置外网访问内网的服务器：内网服务器依旧使用私有地址，对外提供为其分配的公网 IP 地址给外部网络用户访问。

进入页面的方法：“网络配置 > 端口映射 > NAT 规则”。



单击“新增”按钮，配置 NAT 规则。根据 NAT 类型不同，配置的参数不同。

页面参数配置介绍：

1. Easy IP 映射配置

选项	描述
规则名称	配置 NAT 规则的名称，自定义，可输入中文、数字和字母，不能重复。
绑定接口	配置 NAT 规则绑定的接口。
NAT 类型	Easy IP：表示内部 IP 地址映射到同一个外部 IP 地址。

内网起始 IP 地址、内网结束 IP 地址	配置内网中优先使用该 NAT 规则上网的计算机的地址范围。
外部 IP 地址	配置在该 NAT 规则中，内部 IP 地址所映射的外部 IP 地址。

2. One2One 映射配置

选项	描述
规则名称	配置 NAT 规则的名称。
绑定接口	配置 NAT 规则绑定的接口。
NAT 类型	One2One：内部 IP 地址与外部 IP 地址进行一对一的映射。
内网起始 IP 地址、内网结束 IP 地址	配置内网中优先使用该 NAT 规则上网的计算机的地址范围。
外部起始 IP 地址	配置在该 NAT 规则中，内部起始 IP 地址所映射的外部起始 IP 地址。

提示:

One2One 映射规则中的“外部起始 IP 地址”必须设置，实际映射的外部 IP 地址从设置值开始依次增加。例如，如果内部起始 IP 地址设为 192.168.1.50，内部结束 IP 地址设为 192.168.1.52，外部起始地址设为 200.200.202.50，则 192.168.1.50、192.168.1.51、192.168.1.52 依次映射成 200.200.202.50、200.200.202.51、200.200.202.52。

6.4.2 静态映射和 DMZ 主机

某些情况下，需要将一台内网计算机完全暴露给 Internet，以实现双向通信，这时候就需要将该计算机设置成 DMZ 主机。当有外部用户访问该 DMZ 主机所映射的公网地址时，设备会直接把数据包转发到该 DMZ 主机上。

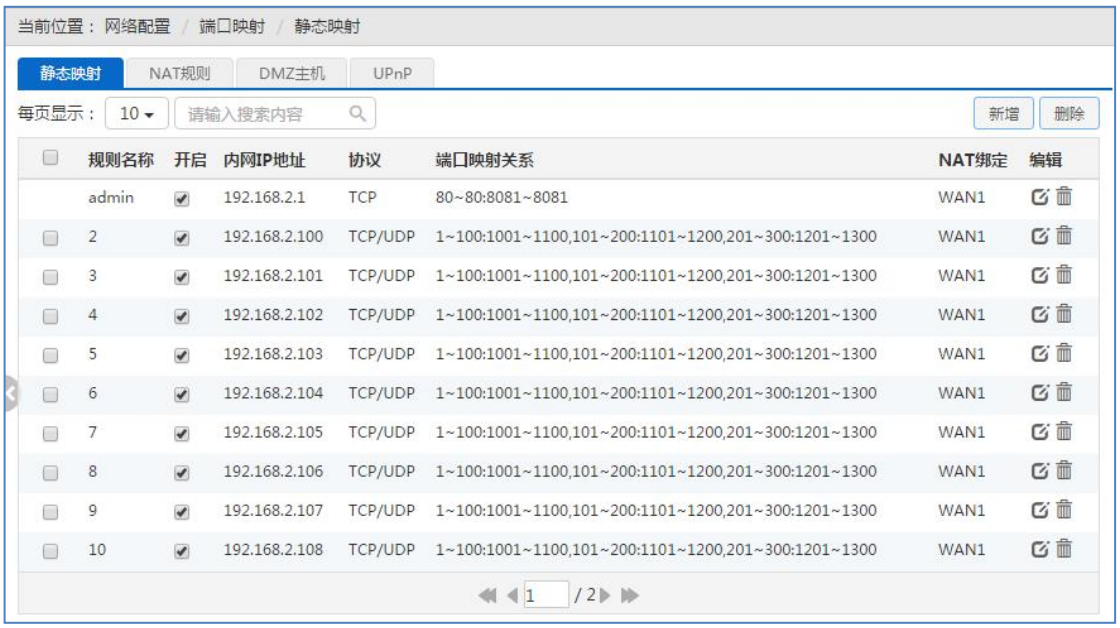
通过静态映射功能，可建立 <外部 IP 地址+外部端口> 与 <内部 IP 地址+内部端口> 一对一的映射关系，这样，所有对设备某指定端口的服务请求都会被转发到匹配的内网服务器上，从而，外网中的计算机就可以访问这台服务器提供的服务了。

提示:

1. 被设置为 DMZ 主机的计算机将失去设备的防火墙保护功能。
2. 静态映射的优先级高于 DMZ 主机。当设备收到一个来自外部网络的请求时，它将首先根据外部访问请求的 IP 地址及端口号，检查是否有匹配的静态映射，如果有的话，就把请求消息发送到该静态映射匹配的内网计算机上。如果没有匹配的静态映射，才会检查是否有匹配的 DMZ 主机。

配置静态映射规则

进入页面的方法：单击“网络配置 > 端口映射 > 静态映射”。



单击“新增”按钮，配置静态映射规则。

页面参数配置介绍：

选项	描述
状态	开启或关闭静态映射功能。
规则名称	配置此条规则的名称，自定义，由数字和字母组成，不能重复。
绑定接口	选择静态映射规则绑定的WAN口。
内网地址	配置作为服务器的内网计算机的 IP 地址。
协议	数据包的协议类型，可供选择的有：TCP、UDP 和 TCP/UDP；当用户无法确认该应用所使用的协议为 TCP 或 UDP 时，可选择 TCP/UDP。
端口	内部端口：内网服务器所开服务的连续端口。

	外部端口：设备提供给 Internet 的连续服务端口。

提示:

1. 点击  “添加”按钮，可以添加最多 10 个不连续的协议及端口段。
2. 系统某些功能启用后，列表会显示一些 NAT 静态映射条目（如在“系统配置 > 网管策略 > 远程管理”页面启用远程管理后，会在该列表启用一条名为 admin 的静态映射），在本页面无法编辑或删除它们。

配置 DMZ 主机

进入页面的方法：单击“网络配置 > 端口映射 > DMZ 主机”。

页面参数配置介绍：

选项	描述
DMZ 状态	开启或关闭 DMZ 主机功能。
全局 DMZ 主机	配置被用作 DMZ 主机的内网计算机的 IP 地址。设置成功后，外网主机可通过路由器的各 WAN 访问内网主机。
WAN 口 DMZ 主机	通过路由器的指定 WAN 口可以访问到的内网计算机（被用作 DMZ 主机）的 IP 地址。设置成功后，外网主机可通过路由器的指定 WAN 访问内网主机。

提示:

被设置为 DMZ 主机的计算机将失去设备的防火墙保护功能。

6.4.3 UPNP

开启 UPNP 功能，系统将自动动态建立<外部 IP 地址+外部端口>与<内部 IP 地址+内部端口>一对一的映射关系，这样，所有对设备某端口的服务请求都会被转发到匹配的内网服务

器上，从而，外网中的计算机就可以访问这台服务器提供的服务了。开启此功能，将增加内网服务器暴露在公网的风险。建议在不使用该功能时，不要启用 UPnP 功能。

进入页面的方法：单击“网络配置 > 端口映射 > UPnP”。

6.4.4 NAT 和 DMZ 配置实例

本小节介绍 NAT 和 DMZ 配置的具体实例。包括：静态映射实例、NAT 规则类型为 EasyIP、One2One 的实例。

1. 静态映射配置实例

内网计算机 192.168.1.99 开设了 TCP80 端口的服务，希望外部通过 WAN1 口 80 端口访问这个服务，具体配置如下图所示。

2. EasyIP 配置实例

某网吧使用单线路上网，ISP 为该线路分配了 8 个地址：218.1.21.0/29 ~218.1.21.7/29，其中 218.1.21.1/29 是该线路的网关地址，218.1.21.2/29 是该设备 WAN1 口的 IP 地址。注意 218.1.21.0/29、218.1.21.7/29 分别为相关子网的子网号和广播地址，不可使用。

现游戏 B 区（IP 地址范围：192.168.1.10/24~192.168.1.100/24）希望以 218.1.21.3/29 作为 NAT 映射地址通过 WAN 口上网。

配置步骤：

第一步，进入“网络配置> 端口映射 > NAT 规则”页面，点击“新增”按钮。

第二步，进入 NAT 规则配置页面，在规则名中填入“youxiqu”。

第三步，选择 NAT 类型为“EasyIP”。

第四步，在“外部 IP 地址”中填入“218.1.21.3”；在“内部起始 IP 地址”和“内部结束 IP 地址”中分别填入“192.168.1.10”和“192.168.1.100”。

第五步，选择该规则绑定的接口为 WAN1 口。

第六步，点击“保存”，该条 NAT 规则配置成功。

提示:

在配置 Easy IP 时，当外部 IP 地址与绑定的接口的 IP 地址不在同一网段时，必须在上层路由器上配置一条到外部 IP 地址所在网段的路由或者是到外部 IP 地址的 32 位的主机路由，下一跳设置为绑定的接口的 IP 地址。

3. One2One 配置实例

需求

某企业申请了一条电信的线路，固定 IP 接入方式，带宽为 6M。电信给它分配了 8 个地址：202.1.1.128/29～202.1.1.135/29。其中，202.1.1.129/29 是该线路的网关地址，202.1.1.130/29 是设备 WAN1 口的 IP 地址。注意：202.1.1.128/29、202.1.1.1.135/29 分别为相关子网的子网号和广播地址，不可使用。

该企业希望内部的人员上网通过 NAT 后使用 202.1.1.130/29 共享上网，另外有四台服务器做一对一 NAT（One2One）使用 202.1.1.131/29～202.1.1.134/29 对外提供服务。内部网络的地址是 192.168.1.0/24，4 台服务器的内部地址是 192.168.1.200/24～192.168.1.203/24。

分析

由于该线路是采用固定 IP 接入方式上网，首先需要在“网络配置 > 外网配置”页面中配置固定接入上网默认线路。上网默认线路正确配置后，将自动生成与默认线路对应的系统保留

NAT 规则，NAT 功能也自动启用。

而该企业使用提供四台内部服务器供外部访问，因此还需为它们设置一个类型为 One2One 的 NAT 规则。

配置步骤：

第一步，进入“网络配置> 端口映射 > NAT 规则”页面，点击“新增”按钮。

第二步，进入 NAT 规则配置页面，在规则名中填入“fuwuqi”。

第三步，选择 NAT 类型为“One2One”。

第四步，在“外部起始 IP 地址”中填入 202.1.1.131；在“内部起始 IP 地址”和“内部结束 IP 地址”中分别填入 192.168.1.200 和 192.168.1.203。

第五步，选择该规则绑定的接口为 WAN1 口。

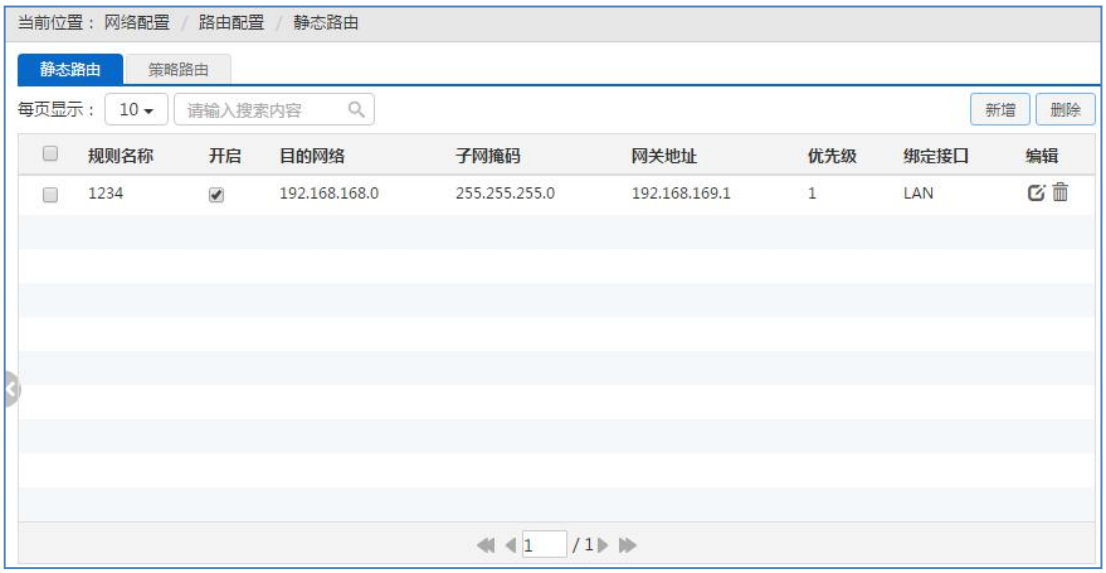
第六步，单击“保存”按钮，该条 NAT 规则添加成功。

6.5 路由配置

6.5.1 静态路由

静态路由是由网络管理员手工配置的路由，使数据包按照预定的路径传送到指定目的网络。静态路由不会随网络结构的改变而改变，因此，当网络结构发生变化或出现网络故障时，需要手工修改路由表中相关的静态路由信息。正确设置和使用静态路由可以改进网络的性能，还可以实现特别的要求，例如实现流量控制、为重要的应用保证带宽等。

进入页面的方法：单击“网络配置 > 路由配置 > 静态路由”。



单击“新增”按钮，配置静态路由。

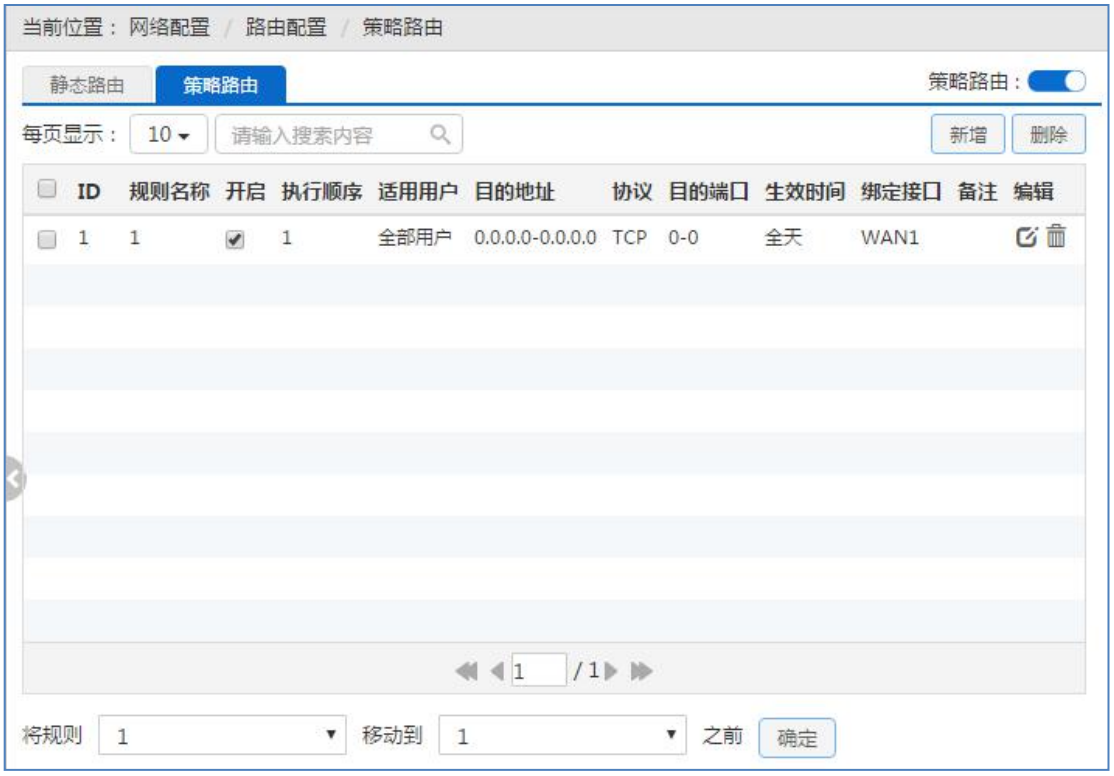
页面参数配置介绍：

选项	描述
状态	开启或关闭此条静态路由规则。
规则名称	配置此条规则的名称。
目的网络	配置此静态路由的目的网络号。
子网掩码	配置目的网络的子网掩码。
网关地址	下一跳路由器入口的 IP 地址，设备通过接口和网关定义一条跳到下一个路由器的线路。通常情况下，接口地址和网关须在同一网段。
绑定接口	配置数据包的转发接口，与该静态路由匹配的数据包将从指定接口转发。根据型号的不同选项不同。

6.5.2 策略路由

在本页面定义策略路由，数据包按照源 IP 地址（适用用户）、协议、目的地址以及目的端口进行路由。

进入页面的方法：单击“网络配置 > 路由配置 > 策略路由”。



单击“新增”按钮，配置策略路由。

页面参数配置介绍：

选项	描述
状态	开启或关闭此条策略路由规则。
规则名称	配置此条规则的名称。
备注	配置此条规则的描述信息。
执行顺序	配置此策略路由规则的优先级，值越小优先级越高。
绑定接口	配置策略路由绑定的物理接口，满足策略路由条件的数据包将从绑定接口转发出去。
适用用户	配置此策略路由的数据包的源 IP 地址（适用用户），默认为内网所有用户。可按以下两种方式配置： ● IP 地址：配置适用于此策略路由的源起始 IP 地址和源结束 IP 地址。当只添加一个 IP 地址时，则设置起始 IP 地址与结束 IP 地址为同一个 IP 地址。 ● 组织架构：在组织架构中选择适用于此策略的用户。
目的地址	设置此策略路由的数据包的目的地址，可按以下两种方式配置： ● IP 地址：配置适用于此策略路由的目的起始 IP 地址和目的结束 IP 地址。当只添加一个 IP 地址时，则设置起始 IP 地址与结束 IP 地址为同一个 IP 地址。 ● 地址组：在地址组中选择适用于此策略的用户。
自定义 IP 协议	配置走此策略路由的数据包的目的地址和协议类型。 ● 协议：选择的协议类型并配置相应的外部端口和内部端口号。 ● 应用服务：走此策略路由的数据包的类型。

	• 外部端口：添加连续的端口。范围 1~65535，对应的协议有 TCP 和 UDP（当选择的协议为 ICMP、AH、all 时不用配置端口范围)。
生效时间	配置策略路由生效的时间段，时间段也可以是不连续的时间点。默认是全天。

提示:

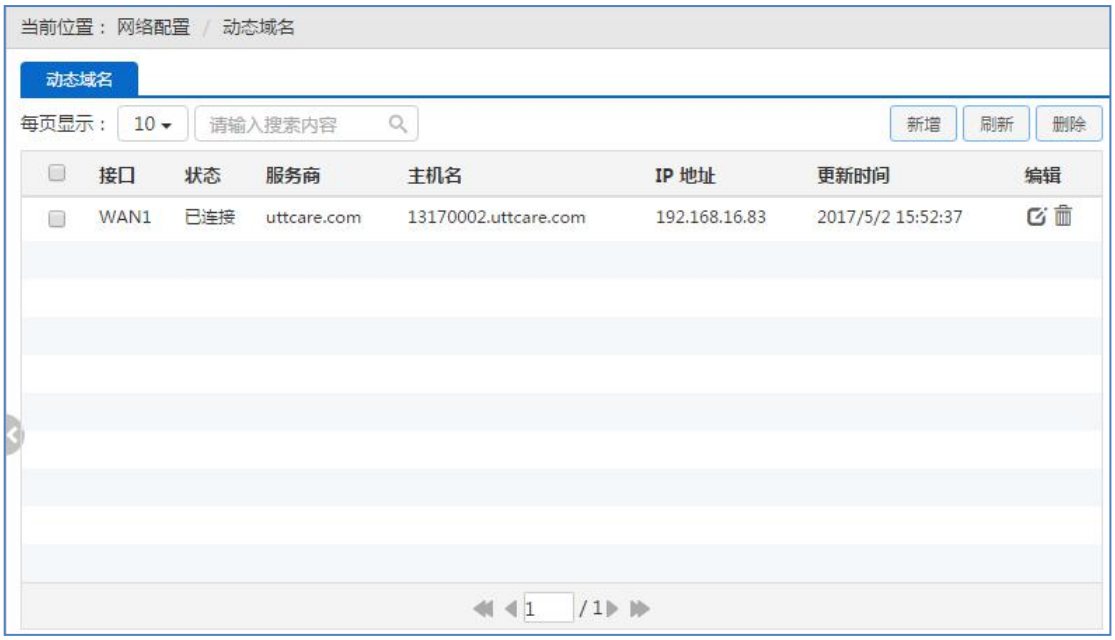
1. 当数据包与定义的适用用户、协议、目的地址、目的端口全部匹配后，将从指定的接口转发出去，找不到匹配策略路由的数据包将走正常的路由。
2. 策略路由的执行顺序：LAN 口静态路由>策略路由>WAN 口静态路由。

6.6 动态域名

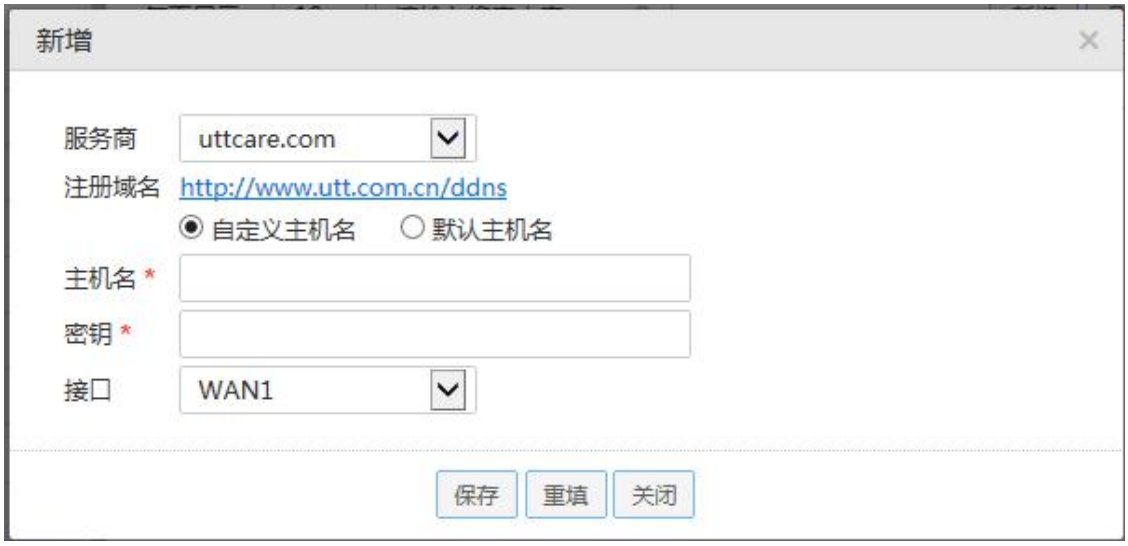
动态域名解析服务（DDNS）是将一个固定的域名解析成动态变化的 IP 地址（如 ADSL 拨号上网）的一种服务。需向 DDNS 服务提供商申请这项服务，DDNS 的具体服务由各服务商根据实际情况提供。各 DDNS 服务提供商保留随时变更、中断或终止部分或全部网络服务的权利。目前，DDNS 服务是免费的，DDNS 服务提供商在提供网络服务时，可能会对使用 DDNS 服务收取一定的费用。在此情况下，艾泰科技会尽可能及时通知，如拒绝支付该费用，则不能使用相关的服务。在免费阶段，艾泰科技不担保 DDNS 服务一定能满足要求，也不担保网络服务不会中断，对网络服务的及时性、安全性、准确性也都不作担保。

路由器长期对外提供特殊服务，需要对外公布一个固定的地址，以方便用户访问，而 WAN 口的接入方式却为动态接入或 PPPoE 接入，此时，可以使用动态域名功能。

进入页面的方法：单击“网络配置 > 动态域名”。



单击“新增”按钮，配置动态域名。



页面参数配置介绍：

选项	描述
服务商	选择相应的服务商。提供的服务商有：3322.org、花生壳、dydns.org、no-ip 和 uttcare.com。
注册域名	单击域名 ,在配置 DDNS 服务之前需到相关网站上申请二级域名及用户名和密码。
主机名	填写已申请的主机名，花生壳可不填写，输入用户名和密码后会自动获取。
用户名	填写注册 3322.org、dyndns.com 或花生壳时使用的用户名。
密码	填写注册 3322.org、dyndns.com、uttcare.com 或花生壳时使用的密码。
接口	选择 DDNS 服务绑定的接口。

提示:

1. WAN 口地址必须为公网地址才能将路由器的地址映射到域名。
2. 采用动态接入方式时，若需要从 WAN 口访问设备，需配合 DDNS 功能使用。

验证动态域名，可以在内网计算机的 DOS 状态下，使用 Ping 命令（例如：ping 1160612013.uttcare.com）检查 DDNS 是否更新成功。看到正确解析出 IP 地址（例如：200.200.202.192）,证明域名解析正确。注意：一般情况下，设备在使用 NAT 后，从 Internet 上将不能 ping 通设备的 IP 地址，只能解析出该域名对应的 IP 地址。

提示:

1. ISP（例如中国电信）分配给 WAN 口连接线路的 IP 地址是公网地址的时候才能保证该域名能被 Internet 的用户访问。

2. DDNS 功能可以帮助动态 IP 使用 VPN 和服务器映射。

6.7 交换配置

6.7.1 端口镜像

端口镜像工作的原理是将被监控端口的流量复制到监控端口 ,实时提供各个被监控端口的传输状况的详细资料，以便网络管理人员进行流量监控、性能分析和故障诊断。

进入页面的方法：“网络配置 > 交换配置 > 端口镜像”。

页面参数配置介绍：

选项	描述
状态	开启或关闭端口镜像功能。
监控端口	配置监控端口。
被监控端口	配置被监控端口。

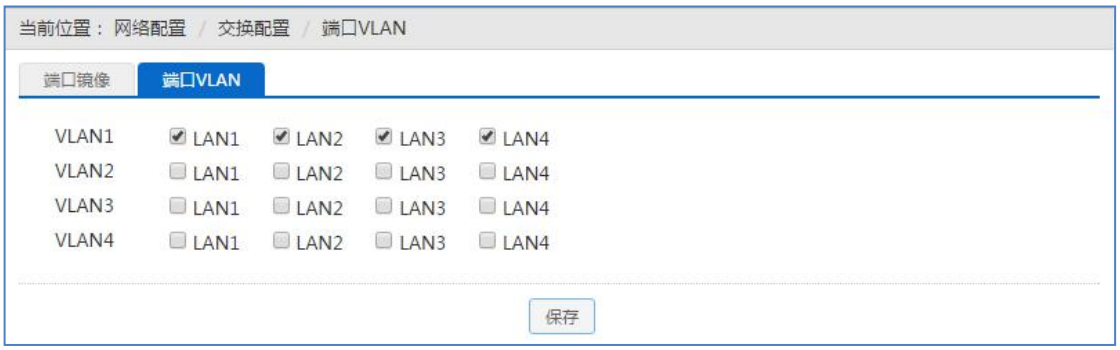
提示:

1. 因产品型号差异，部分设备不支持端口镜像功能。只有存在两个及两个以上 LAN 口时，端口镜像功能才生效。
2. 被监控端口不能与监控端口是同一个端口。

6.7.2 端口 VLAN

VLAN，即虚拟局域网，可以将网络逻辑地分割成多个不同的广播域。一个 VLAN 组成一个逻辑广播域。同一个 VLAN 中的成员共享广播，可相互通信。不同 VLAN 之间实现物理隔离，一个 VLAN 内部的单播、广播和多播包都不会转发到其他 VLAN 中，从而有助于控制流量、简化网络管理、加强网络安全性。

进入页面的方法：“网络配置 > 交换配置 > 端口 VLAN”。



配置 VLAN 端口。一个端口可以属于多个 VLAN 中。

提示:

1. 默认情况下，所有端口默认属于 VLAN1 中。
2. 一个 VLAN 可以包含多个端口，一个端口也可以属于多个 VLAN。

端口 VLAN 配置实例

需求

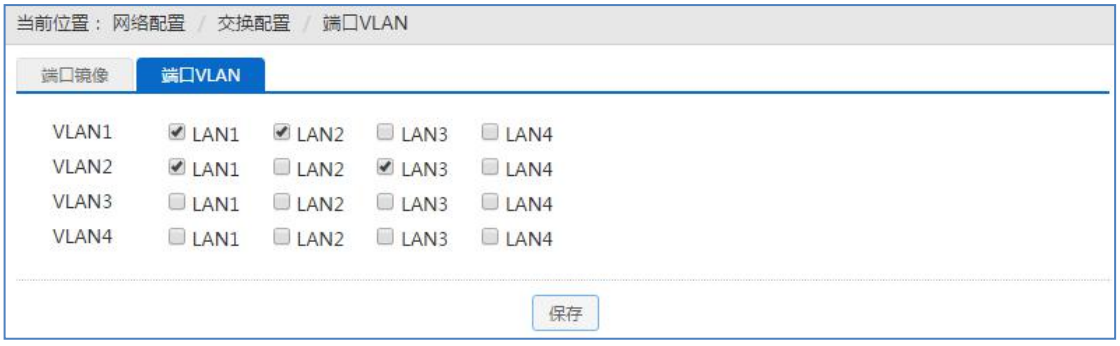
设备 LAN1 口下的主机能与 LAN2 口、LAN3 口下的主机进行通信，但 LAN2 口和 LAN3 口下的主机不能互访。

分析

LAN1 口与 LAN2 口属于 VLAN1，LAN1 口又与 LAN3 口属于 VLAN2，固 LAN1 口下的主机能与 LAN2 口、LAN3 口下的主机进行通信。又 LAN2 口与 LAN3 口不在同一 VLAN，固 LAN2 口与 LAN3 口下的主机彼此不能互访。

配置步骤

配置 VLAN 1 成员端口为：1、2；配置 VLAN 2 成员端口为 1、3。



第 7 章 用户管理

根据公司组织架构按组划分网络组织，便于网络管理员配置和维护内网用户。

7.1 组织成员

组织成员中包含内网所有按组划分的用户。成员按组划分有助于网络安全、流量控制、上网策略等功能按组名或人名做策略。管理员可对各组用户成员做新增、修改、删除等维护操作，例如管理员维护公司组织结构及其相应成员。

1. 组织架构

页面左侧为当前所有用户组的树型结构，有两个根组，可在 Root 组下新建子组；右侧是左侧组织架构中已定义的组所包含的所有直属用户和子组。未在 Root 组中定义的用户接入内网中，将分配至临时用户组中。

2. 用户

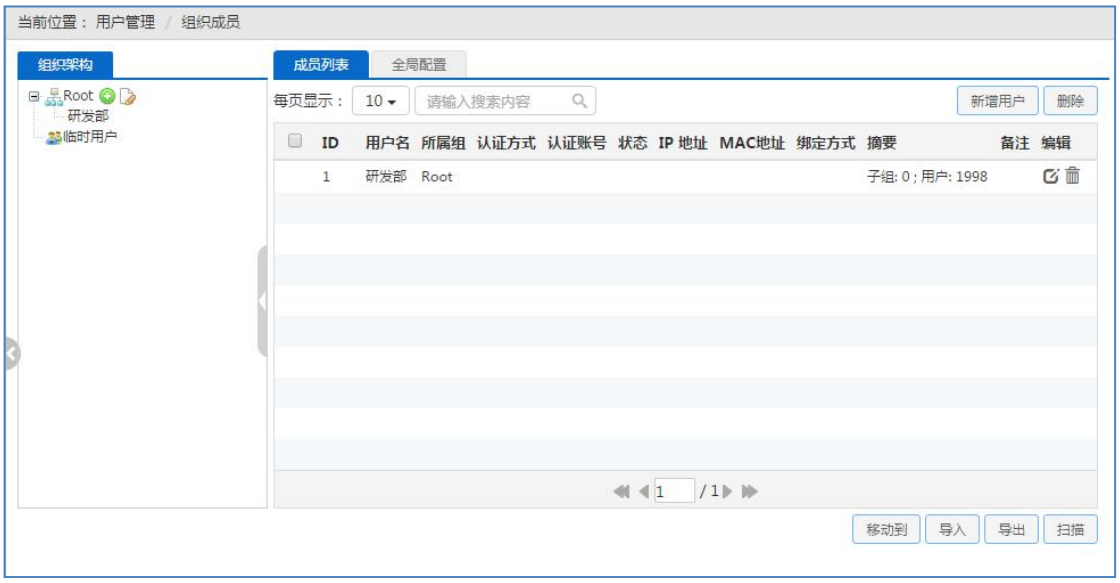
要实现网络安全管理，首先必须解决用户的身份识别问题，然后才能进行必要的业务授权工作。设备使用绑定的 IP/MAC 地址对作为用户唯一的身份识别标识，可以保护设备和网络不受 ARP 欺骗的攻击。在组织架构页面右侧添加用户，包含两种用户类型，普通用户和认证用户。

普通用户：分三种类型的用户，IP 绑定用户、MAC 绑定用户和 IP/MAC 绑定用户。

- IP/MAC 绑定 :将 MAC 地址与 IP 地址绑定到某用户名下，便于系统识别接入者身份。只有 IP 和 MAC 地址都匹配的用户才能接入网络，若只有 IP 匹配或 MAC 匹配，将被识别为网络欺骗，从而禁止上网。
- IP 绑定：通过 IP 识别接入者身份。
- MAC 绑定：通过 MAC 地址，识别接入者身份。不适用三层交换组网环境。

认证用户：分两种类型的用户，PPPoE 认证用户和 WEB 认证用户。认证用户通过对应的认证方式即可接入网络。您也可以通过设置认证用户的绑定方式进一步限定用户范围，从而保证用户的合法性和系统的安全性。

进入页面的方法：“用户管理 > 组织成员”。



配置根组/子组名称

1. 在组织架构页面，单击根组/子组名称。
2. 单击编辑按钮修改根组/子组名称。
3. 单击添加按钮新增子组。
4. 单击删除按钮删除子组。
5. 单击“保存”按钮完成配置。

新增普通用户

进入页面的方法：“用户管理 > 组织成员 > 成员管理”。

1. 在组织架构页面，单击“新增用户”按钮，弹出新增用户对话框。

2. 输入用户信息并单击“保存”按钮完成配置。

选项	描述
用户名	配置用户名称。
所属组	配置用户所属组。
用户类型	选择“普通用户”。
绑定方式	在“IP 绑定”、“MAC 绑定”或“IP+MAC 绑定”中选择一个绑定条件。并在文本框中输入相关 IP 地址或 MAC 地址。

新增认证用户

进入页面的方法：“用户管理 > 组织成员 > 成员管理”。

1. 在组织架构页面，单击“新增用户”按钮，弹出新增用户对话框。

2. 输入用户信息并单击“保存”按钮完成配置。

选项	描述
用户名	配置用户名称。
所属组	配置用户所属组。
用户类型	选择“认证用户”。
认证方式	有 WEB 认证与 PPPOE 认证两项供选择，认证方式不同，后续配置的选项也不同。
认证账号/认证密码	认证用户请求接入内网时使用的登录账号和密码。
并发数	配置认证账号同时可被多少用户登录使用。
绑定方式	在“无绑定”、”自动绑定”、“IP 绑定”、“MAC 绑定”或“IP+MAC 绑定”中选择一个绑定条件。当绑定方式为“IP 绑定”、“MAC 绑定”或“IP+MAC 绑定”时，需要设定绑定的 IP 地址或 MAC 地址。

账号计费	开启或关闭对登录账号的计费功能。当开启计费功能后，可设置计费方式。
用户状态	开启或冻结此用户。

全局配置

配置允许访问外网的用户。

进入页面的方法："用户管理 > 组织成员 > 全局配置"。

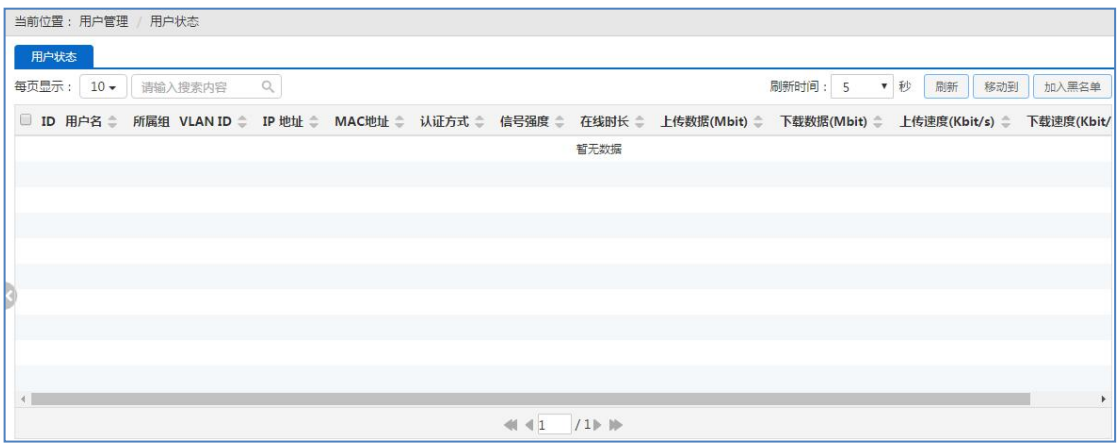
页面参数配置介绍：

选项	描述
仅 IP/MAC 绑定用户能上网	启用此功能后，非 IP/MAC 绑定用户无法访问网络。
仅 MAC 绑定用户能上网	启用此功能后，非 MAC 绑定用户无法访问网络。

7.2 用户状态

查看或编辑局域网中在线用户信息，包括在线用户的用户名、所属组、VLAN ID、IP 地址、MAC 地址、认证方式、在线时长、上传下载数据等，也可将用户加入黑名单中，禁止黑名单用户接入局域网。

进入页面的方法：单击"用户管理 > 用户状态"。



7.3 用户认证

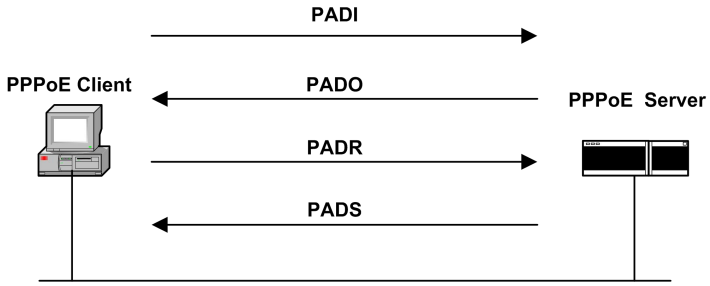
配置用户认证方法，当开启用户认证功能时，只有通过认证的用户才可接入局域网中。系统提供三种认证方式：PPPoE 认证、WEB 认证、远程认证。

7.3.1 PPPoE 认证

PPPoE（Point-to-Point Protocol over Ethernet），即以太网上的点对点协议，它可以使以太网上的主机通过一个简单接入设备连到 Internet 上。PPPoE 协议采用 Client/Server（客户端/服务器）方式，它将 PPP 报文封装在以太网帧内，在以太网上提供点对点的连接。PPPoE 拨号连接包括 Discovery（发现）和 Session（PPP 会话）两个阶段。下面将分别介绍这两个阶段。

1. **Discovery 阶段**

此阶段用来建立连接，当一个用户主机想开始一个 PPPoE 会话时，首先必须进行发现阶段以识别 PPPoE Server 的以太网 MAC 地址，并建立一个 PPPoE 会话标识（Session ID）。



如上图所示， Discovery 阶段由四个步骤组成，下面将介绍它的基本工作流程。

- PADI：如果要建立一条 PPPoE 连接，首先 PPPoE 客户端就要以广播的方式发送一个 PADI（PPPoE Active Discovery Initiation）数据包，PADI 数据包包括客户端请求的服务。
- PADO：当 PPPoE 服务器收到一个 PADI 包之后，它会判断自己是否能够提供服务，如果能够提供服务的话，就会向客户端发送 PADO（PPPoE Active Discovery Offer）数据包来进行回应。PADO 数据包包括 PPPoE 服务器名称和与 PADI 数据包中相同的服务名。如果 PPPoE 服务器不能为 PADI 提供服务，则不允许用 PADO 数据包响应。
- PADR：由于 PADI 是以广播的形式发送出去的，PPPoE 客户端可能收到不止一个 PADO 数据包，它将审查所有接收到的 PADO 数据包并根据其中的服务器名或所提供的服务选择一个 PPPoE 服务器，并向选中的服务器发送 PADR（PPPoE Active Discovery Request）数据包。PADR 数据包包括客户端所请求的服务。
- PADS：当 PPPoE 服务器收到客户端发送的 PADR 包时，它就准备开始一个 PPPoE 会话，它为 PPPoE 会话创建一个唯一的 PPPoE 会话 ID，并向客户端发送 PADS（PPPoE

Active Discovery Session- confirmation）包作为响应。

当发现阶段正常结束后，通信的两端都获得会话标识（Session ID）和对方的 MAC 地址，它们一起唯一定义一个 PPPoE 会话。

2. **PPP 会话阶段**

当 PPPoE 进入 PPP 会话阶段后，客户端和服务器将进行标准的 PPP 协商，PPP 协商通过后，数据通过 PPP 封装发送。PPP 报文作为 PPPoE 帧的净荷被封装在以太网帧内，发送到 PPPoE 链路的对端。Session ID 必须是 Discovery 阶段确定的 ID，且在会话过程中保持不变，MAC 地址必须是对端的 MAC 地址。

在会话阶段的任意时刻，PPPoE 服务器和客户端都可向对方发送 PADT（PPPoE Active Discovery Terminate）包通知对方结束本会话。当收到 PADT 以后，就不允许再使用该会话发送 PPP 流量了。在发送或接收到 PADT 数据包后，即使是常规的 PPP 结束数据包也不允许发送。一般情况下，PPP 通信双方使用 PPP 协议自身来结束 PPPoE 会话，但在无法使用 PPP 时可以使用 PADT 来结束会话。

PPPoE 配置

配置 PPPoE 认证功能。当开启 PPPoE 认证功能后，所有用户均需要通过 PPPoE 认证才可接入内网。

进入页面的方法："用户管理 > 用户认证 > 认证配置"。

单击"配置"按钮，配置 PPPoE 认证参数。

页面参数配置介绍：

选项	描述
强制 PPPoE 认证	启用/禁用设备的 PPPoE 服务器功能。启用强制 PPPoE 认证表示只允许内网 PPPoE 认证通过的用户访问因特网。
例外地址组	在设备开启强制 PPPoE 认证后，该地址组的用户可以不通过拨号认证也能与因特网通信，地址组需要在“系统对象 > 地址组”页面配置。
起始 IP 地址	PPPoE 服务器给内网计算机自动分配的起始 IP 地址。
总地址数	PPPoE 服务器给内网计算机自动分配的从起始 IP 地址开始的连续 IP 地址的个数。
主 DNS 服务器/备 DNS 服务器	PPPoE 服务器给内网计算机自动分配的主/备用 DNS 服务器的 IP 地址。
密码验证方式	PPPoE 验证用户名和密码的方式，设备提供 PAP、CHAP 以及 AUTO 三种验证方式，默认值为 AUTO，表示系统自动选择 PAP 或 CHAP 对拨入用户进行身份验证，一般情况下不需要设置。
系统最大会话数	同时上网的 PPPoE 接入终端个数的上限。
允许用户修改拨号密码	允许或禁止内网 PPPoE 拨号用户自助修改拨号密码。当 PPPoE 客户端拨号成功后，登录自助服务页面修改密码，自助服务页面地址为：http://192.168.1.1/noAuth/poeUsers.asp（该地址为设备 LAN 口 IP 地址）。
账号到期通告	开启或关闭账号到期通知用户的功能。

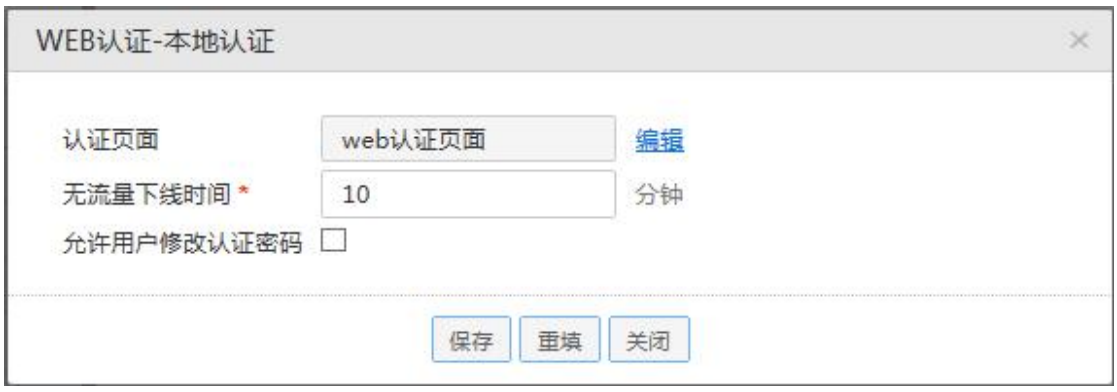
账号到期提前通告时间	配置提前几天通知用户账号将到期。例如：设置为 10 时，表示从账号到期前 10 天开始，当用户拨号成功，第一次访问网站时会收到设备发送的到期通告。 **提示：**内网拨号用户账号过期后，仍能够拨号成功，能够访问设备，但不能访问因特网；同时访问网站时会收到设备发送的到期通告。
账号通告页面	配置账号到期通告页面使用的模板。

7.3.2 WEB 认证

启用 WEB 认证，用户在电脑、手机等设备上通过认证后才可访问因特网。

进入页面的方法：“用户管理 > 用户认证 > 认证配置”。

单击“配置”按钮，配置 WEB 认证参数。



页面参数配置介绍：

选项	描述
认证页面	配置认证页面的模板。
无流量下线时间	配置用户通过认证后，多久未产生流量后被踢下线。
允许用户修改认证密码	启用或禁止内网用户自助修改认证密码。

提示:

WEB 认证用户修改认证密码步骤：

1. 用户打开浏览器，使用用户名、密码进行认证。
2. 认证成功后，在打开的认证成功的对话框中，点击“修改密码”。
3. 在密码修改页面输入用户名、旧密码、新密码、确认密码。
4. 点击“提交”，显示“操作成功”即密码修改成功。
5. 用户每天只能自助修改 5 次密码。
6. 管理员可以通过在“行为管理 >电子通告”页面配置日常事务通告通知用户如何修改 WEB 认证密码。

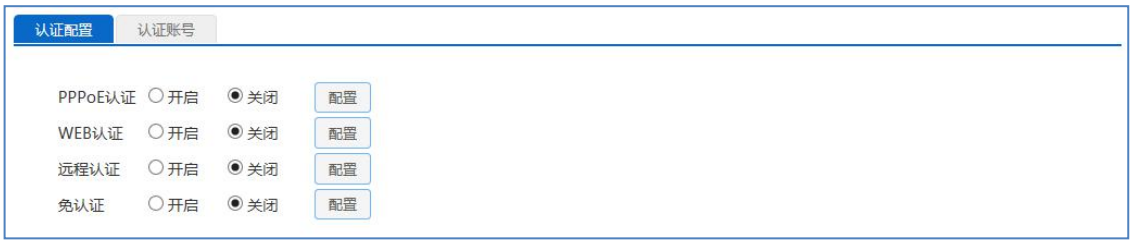
WEB 认证用户如何安全下线：

1. 用户打开浏览器，使用用户名、密码进行认证。
2. 认证成功后，在打开的认证成功的对话框中，点击“安全下线”。

7.3.3 远程认证

远程认证用于验证内网用户是否有权限访问因特网。启用该功能后，设备将用户的认证信息存储到远程云服务器上，当用户访问英特网时，远程服务器会自动生成用户所需的认证信息。内网用户只需要使用艾泰科技支持远程认证的任意设备，就可以在任何地点认证，并访问英特网，且云服务器端提供定制认证模板功能，支持微信认证、手机认证、一键认证、固定帐号认证四种认证方式，有利于商家定制广告，达到免费推销产品效果。

进入页面的方法：“用户管理 > 用户认证 > 认证配置”。



单击“配置”按钮，配置远程认证参数。

页面参数配置介绍：

选项	描述
序列号	设备的唯一序列号。
激活码	和序列号相对应，且唯一。可以使用序列号和激活码注册艾泰 WiFi 营销系统账号。
无流量下线时间	配置用户通过认证后，多久未产生流量后被踢下线。
域名名称	配置免认证的域名或 IP，若设置用户在未通过认证前也可以访问 http://www.utt.com.cn，则可将该域名添加到域名白名单中。
白名单列表	显示域名白名单列表。

7.3.4 免认证

配置免认证用户，免认证用户可以无需认证即可访问英特网。

进入页面的方法：“用户管理 > 用户认证 > 认证配置”。

单击“配置”按钮，配置远程认证参数。

页面参数配置介绍：

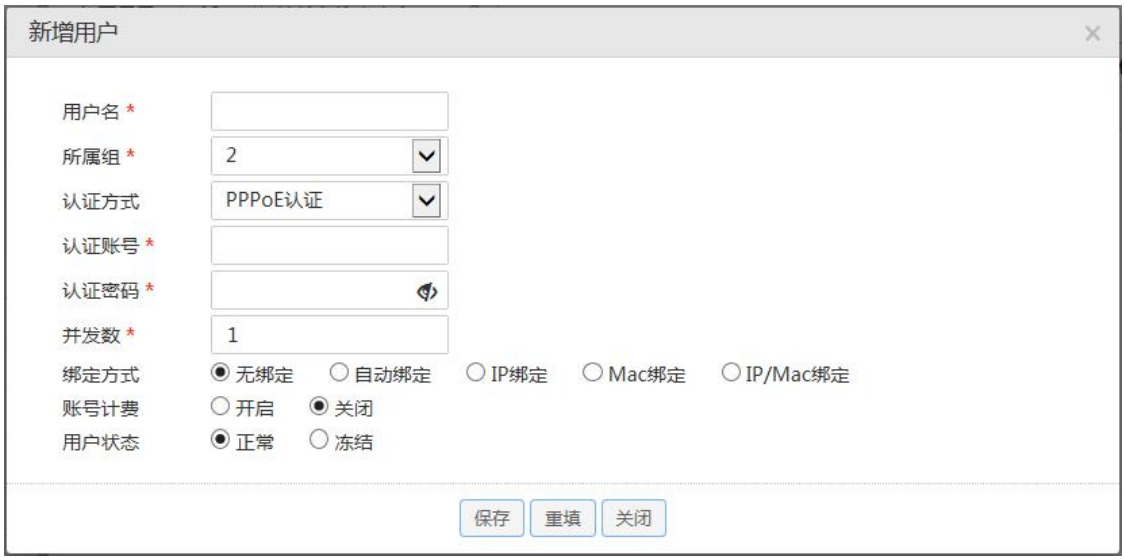
选项	描述
全部用户	接入内网的所有用户无需认证即可访问因特网。
组织架构	在组织架构中选择免认证用户，指定的用户无需认证即可访问因特网。
IP 地址	通过 IP 地址设计免认证用户，指定的 IP 地址用户无需认证即可访问因特网。

7.3.5 认证账号

当启用 PPPoE 认证或 WEB 认证时，用户访问因特网需要使用指定的登录帐号和密码才可通过认证。系统提供新增、删除、修改、查看、导入、导出认证账号功能。

进入页面的方法：“用户管理 > 用户认证 > 认证账号”。

单击“新增”按钮，配置认证账号参数。



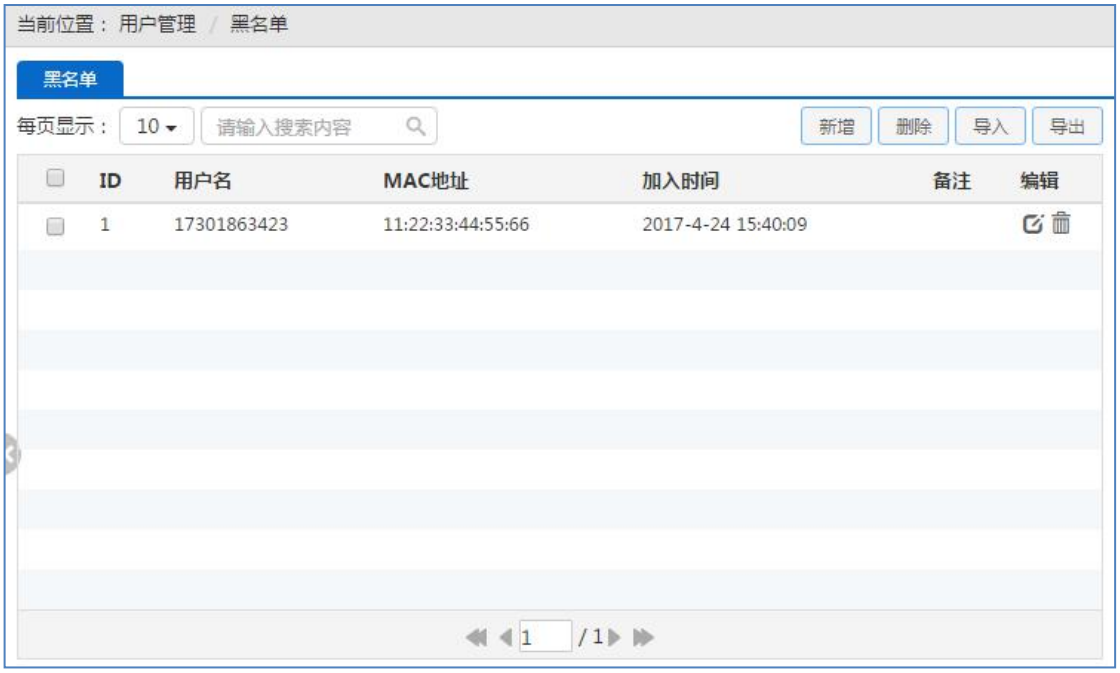
页面参数配置介绍：

选项	描述
用户名	配置 WEB 认证用户的用户名称。
所属组	配置用户所属组。
认证方式	配置认证用户的认证方式，为“PPPoE 认证”或“WEB 认证”。
认证账号	配置认证时使用的认证用户名。
认证密码	配置认证时使用的认证密码。
并发数	配置同时使用同一认证用户的终端数量。
绑定方式	✧ 仅适用于 PPPoE 认证。 在“无绑定”、“自动绑定”、“IP 绑定”、“MAC 绑定”或“IP/MAC 绑定”中选择一个绑定条件，并在文本框中输入相关 IP 地址或 MAC 地址。
账号计费	开启或关闭计费模式。
计费方式	配置费用的计算方式。
账号开通日期	配置账号的开通日期。
账号停用日期	配置账号的停用日期。
用户状态	✧ 仅适用于 PPPoE 认证。 开启或冻结此用户。

7.4 黑名单

查看与管理 MAC 黑名单用户。黑名单用户无法接入网络中。有效管理黑名单可以提高网络安全性和网络速率。例如将恶意攻击路由器的用户加入黑名单，可以提高网络安全。

进入页面的方法：“用户管理 > 黑名单”。



单击“新增”按钮，配置黑名单用户。

页面参数配置介绍：

选项	描述
用户名	配置被加入黑名单用户的名称。
MAC 地址	配置被加入黑名单用户的 MAC 地址。
备注	配置此规则的描述性信息。

第 8 章 行为管理

8.1 行为管理

制定上网行为管理规则，对内网特殊用户在指定时间内的上网行为作策略禁止操作。如果功能不生效，请更新策略库。

进入页面的方法：“行为管理 > 行为管理”。

页面右上方是行为管理功能的全局开关，只有打开此开关，配置的行为管理规则才会生效。

单击“新增”按钮，配置上网行为管理规则。

页面参数配置介绍：

选项	描述
开启	开启或关闭此行为管理规则。
规则名称	配置上网行为管理规则的名称。
备注	配置描述性信息。
适用用户	配置上网行为管理规则生效的用户。默认为全部用户，也可以通过组织架构选择指定的用户，或通过 IP 地址指定用户。
应用服务	配置哪些应用将被受限禁止访问。当选择的应用无法被禁止时，请至“系统配置 > 系统维护 > 应用特征库”更新策略。
生效时间	配置该上网行为管理规则生效的时间。

用户管理配置实例

需求

某公司为控制员工的上网行为，针对其实际需求，规定在工作时间中禁止 QQ、MSN 等聊天软件、禁止股票和游戏软件，禁止访问购物网站。在其余时间则开放所有业务。

其中管理层用户（地址为 192.168.1.5 和 192.168.1.9），上网行为不受任何限制。

销售部和客服部员工 ,地址分别为 192.168.1.50~192.168.1.69 和 192.168.1.70 ~192.168.1.92，由于工作需要，需使用聊天软件与客户进行沟通。

研发部（地址为 192.168.1.100~192.168.1.129）禁止聊天软件的使用。

该公司的工作时间为：周一～周五，9 点～18 点。

分析

由上，可以根据将该公司的上网行为管理需求，配置 2 条上网行为管理策略。

1. 为销售部和客服部员工配置上网行为管理策略，禁止除聊天软件以外的其他功能。
2. 为研发部员工配置上网行为管理策略，只禁止聊天软件的使用。

配置步骤

1. 进入“行为管理>行为管理”页面，点击“新增”按钮，进入行为管理配置页面。
2. 配置销售部、客服部的行为管理策略：

选项	选项值
开启	开启行为管理规则。
规则名称	IM
备注	禁止视频游戏股票。

适用用户	选用 IP 地址指定用户。IP 开始地址：192.168.1.50，IP 结束地址 192.168.1.92。
应用服务	勾选视频网站浏览、WEB 视频、P2P 下载、流媒体、网络游戏、股票行情、股票交易。
生效时间	周一至周五、9:00~18:00。

3. 配置研发部的行为管理策略：

选项	选项值
开启	开启行为管理规则。
规则名称	yanfa
备注	禁止聊天软件功能。
适用用户	选用 IP 地址指定用户。起始 IP 地址：192.168.1.100，结束 IP 地址：192.168.1.129。
应用服务	勾选即时通讯。
生效时间	周一至周五、9:00~18:00。

4. 查看配置列表

8.2 域名过滤

制定域名过滤规则，对内网部分用户在指定时间内的访问特殊域名行为作策略允许或禁止操作，还可配置网页通告模板内容提示用户这是正常现象。

进入页面的方法：“行为管理 > 域名过滤”。

页面参数配置介绍：

选项	描述
状态	开启或关闭域名过滤功能。
规则名称	配置域名过滤规则的名称。
备注	配置描述性信息。
适用用户	配置域名过滤规则生效的用户。默认为全部用户，也可以通过组织架构选择指定的用户，或通过 IP 地址指定用户。
生效时间	配置域名过滤规则生效的时间。
动作	勾选“允许”允许用户访问指定域名，勾选“禁止”禁止用户访问指定域名。
过虑域名	配置需要过滤的域名。
域名列表	显示被过滤的域名列表。
终端接入提醒	开启或关闭终端接入提醒功能。当开启终端接入提醒功能时，若用户被禁止访问某个网站时，希望给用户一个提示，表示此网站被禁止而非网络问题，配置域名过滤通知。
接入提醒方式	选择客户端接入指定域名时的提醒方式：“发布通告”或“重定向”。 ● 若选择“发布通告”方式，在“通告页面”中配置提示模板。当用户访问域名列表中的网站时，系统将用网页提示形式告知用户，显示内容为通告模板内容。 ● 若选择“重定向”方式，在“重定向 IP”中配置 IP 地址，当用户访问域名列表中的网站时，网页将跳转到指定的重定向 IP。

提示:

1. 域名过滤功能是全字匹配的，当内网用户在浏览器里输入的域名与域名列表中显示的域名全字匹配时，若动作是禁止，将无法访问此域名对应的网页。
2. 可以在域名名称中输入通配符“*”来实现对多个域名的过滤，例如在域名列表中输入域名名称“*.163.com”，在动作中选择“禁止”，内网用户将不能访问以“.163.com”结尾的所有网页。

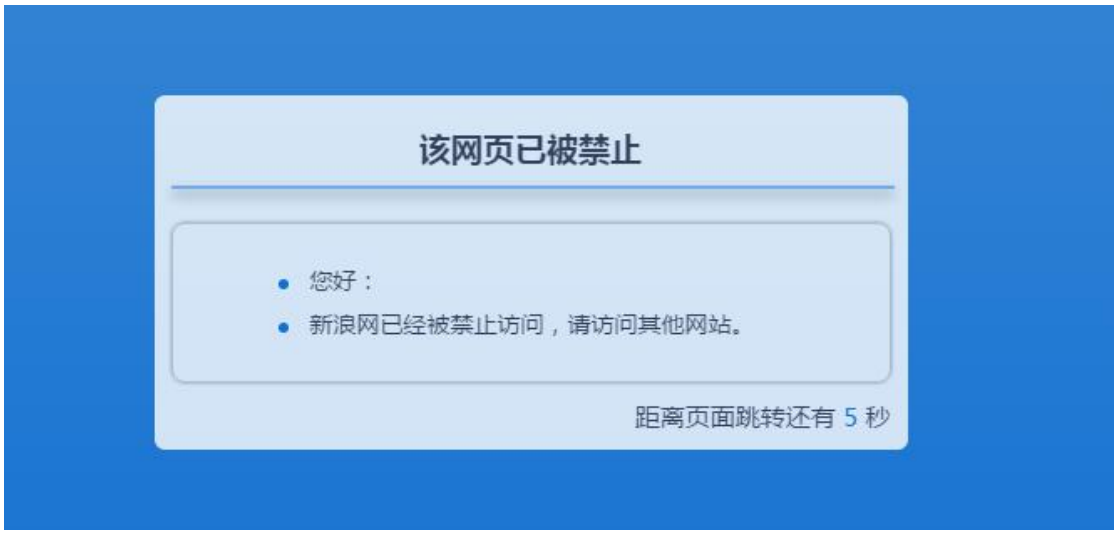
配置通告页面模板

点击“通告页面”后面的“编辑”按钮，配置通告页面模板。

选项	描述
页面名称	对此通告模板的页面的命名。
备注	对此通告模板的描述性信息。
通告标题	用户接收通告信息的标题。
跳转 URL	当访问域名列表中的域名时，将自动跳转到的域名地址。
跳转时间	当访问域名列表中的域名时，停留在通告页面的时间，超时将自动跳转到“跳转 URL”文本框中设置的网址。值为空时表示不跳转，为 0 时表示立即跳转。
跳转内容	推送的通告信息的详细内容。

点击“预览“按钮预览通告页面的显示效果，例如：

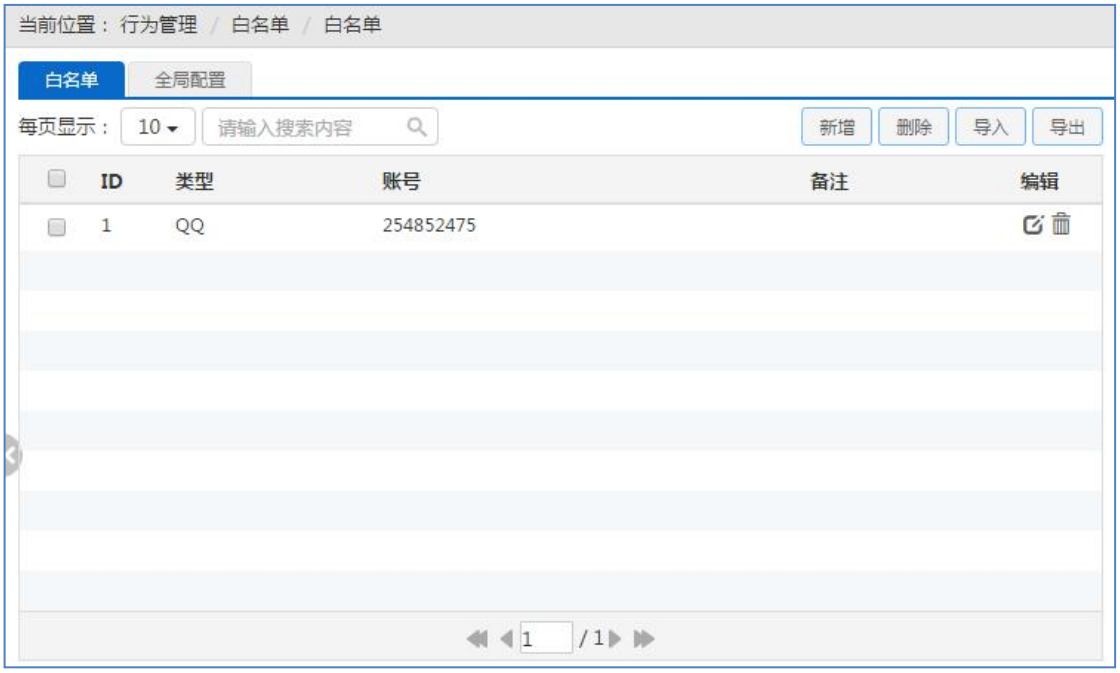
如上图的配置显示效果如下：



8.3 白名单

配置 QQ 与阿里旺旺白名单。在“行为管理”页面禁止 QQ 与阿里旺旺应用后，QQ 与阿里旺旺白名单用户仍可以正常登录。系统提供新增、修改、删除、导入、导出白名单功能。

进入页面的方法：“行为管理 > 白名单”。



点击“全局设置”按钮，开启或关闭 QQ 白名单、400/800 企业 QQ 白名单、阿里旺旺白名单功能。

单击“新增”按钮，配置白名单账号。

页面参数配置介绍：

选项	描述
白名单类型	勾选“QQ“单选框配置 QQ 白名单，勾选“阿里旺旺“单选框配置阿里旺旺白名单。
账号	配置白名单账号。注：该版本支持的最大的 QQ 号码为 4294967295。
备注	配置描述性信息。

8.4 电子通告

配置日常事务电子通告模板。用户打开网页时，日常事务以 Web 页面的形式发送给用户。用户收到通告后，在浏览器地址栏再次输入相应地址即可正常访问网站。

进入页面的方法：“行为管理 > 电子通告”。

页面参数配置介绍：

选项	描述
规则名称	配置此日常事务电子通告的名称。
状态	开启或关闭日常事务电子通告功能。

备注	配置描述性信息。
通告页面	配置日常事务电子通告显示页面。
适用用户	配置此日常事务电子通告生效的用户。默认为全部用户，也可以通过组织架构选择指定的用户，或通过 IP 地址指定用户。
生效时间	配置此日常事务电子通告生效的时间。可以引用时间计划组（在“系统对象 > 时间计划”中配置），也可以自定义时间段。

第 9 章 流量管理

9.1 应用优先

在多个应用程序同时请求交换数据包时，定义转发应用数据包的优先级。

提示:

为保障应用优先功能正确运行，请先配置好 WAN 口带宽的上行带宽和下行带宽，如何配置参阅：外网配置。

进入页面的方法：“流量管理 > 应用优先”。

页面右上方是应用优先功能的全局开关，只有打开此开关，配置的应用优先规则才会生效。

系统内置两套模板供使用：“办公优先”和“娱乐优先”。使用“办公优先”模板，系统将优先处理并转发社交即时通讯、办公软件、移动应用等类型的数据包；使用“娱乐优先”模板，系统将优先处理并转发网络游戏、视频网站、旅游、网站购物、股票交易等类型的数据包。

若使用系统预设置的模板，在“使用场景”下拉框中选择模板，并点击“确定”按钮即可。若需自定义应用优先规则，单击“新增”按钮，配置应用优先规则。

页面参数配置介绍：

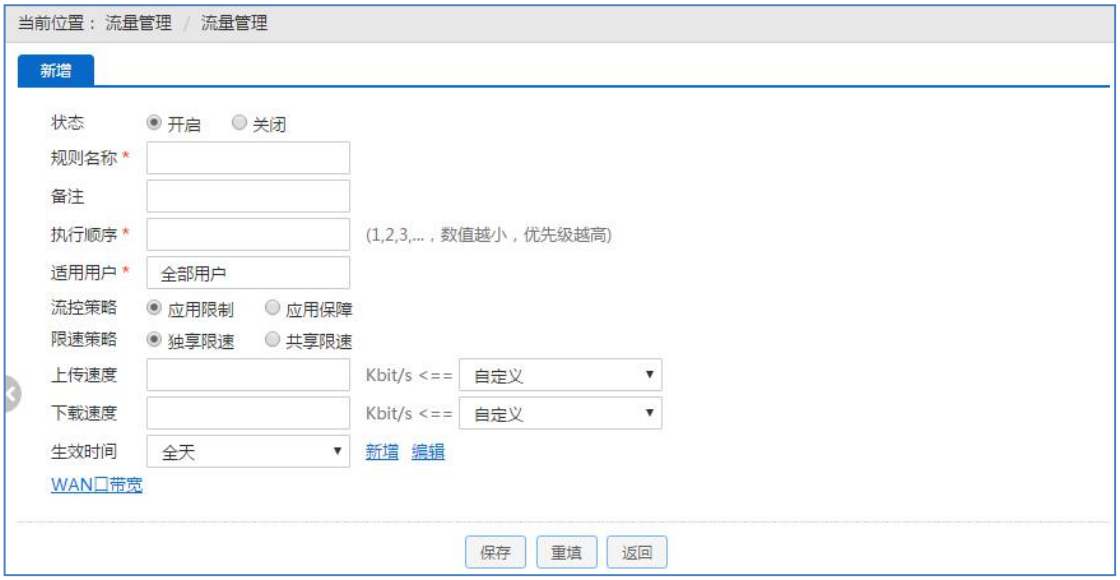
选项	描述
状态	开启或关闭应用优先功能。
规则名称	配置此规则的名称，不可与其他规则的名称重复。
备注	配置描述性信息。
执行顺序	配置规则的执行顺序，数值越小，执行越早，决定规则的属性取值。
优先级	配置此规则中应用数据包转发的优先级别，数值越小，优先级越高。系统优先转发优先级高的应用数据包。
适用用户	配置此规则生效的用户，默认为全部用户，也可以通过组织架构选择指定的用户，或通过 IP 地址指定用户。
应用服务	配置此规则生效的应用。
生效时间	配置此规则生效的时间。

9.2 流量管理

用户可以通过流量管理功能限制内网用户的上传、下载速率大小，从而实现带宽的合理分配与利用。

进入页面的方法：“流量管理 > 流量管理”。

单击“新增”按钮，配置流量管理规则。



页面参数配置介绍：

选项	描述
状态	开启或关闭流量管理功能。
规则名称	配置此规则的名称，不可与其他规则的名称重复。
备注	配置描述性信息。
执行顺序	配置规则的执行顺序，数值越小，执行越早，决定规则的属性取值。
适用用户	此流量控制规则生效的用户，默认为全部用户，也可以通过组织架构选择指定的用户，或通过 IP 地址指定用户。

流控策略	配置此流量控制规则的策略：应用保障或应用限制。 ● 应用限制：限制用户的最大上传、下载速率。 ● 应用保障：保障用户的最低上传、下载速率。为确保应用的带宽保障生效，请先配置好 WAN 口带宽的上行带宽和下行带宽。
限速策略	可供选项有“独享”和“共享”；独享表示此范围内的每一个 IP 地址使用此带宽；共享表示此范围内的 IP 地址共享此带宽。
上传速率	此范围内 IP 地址的最大上传速率。
下载速率	此范围内 IP 地址的最大下载速率。
生效时间	该条流量控制规则生效的时间。

第 10 章　防火墙

10.1　访问控制

灵活地运用访问控制功能，不仅能够为不同的用户设置不同的 Internet 访问权限，还可以控制用户不同时段的 Internet 访问权限。在实际应用中，可根据各个机构的管理规则，在设备上配置相应的访问控制策略。例如对于学校用户，可通过配置访问控制策略设置学生不能访问游戏网站。而对于家庭用户，可配置只在指定的时间内允许孩子上网。对于企业用户，可配置财务部门的机器不能被互联网访问等。

在设备中配置访问控制策略，可以监测流经设备的每个数据包。默认情况下，设备中没有配置任何访问控制策略，设备将转发接收到的所有合法的数据包。如果配置了访问控制策略，当数据包到达设备后，它会取出此数据包的源 MAC 地址、源地址、目的地址、协议、端口号或数据包中的内容进行分析，并按照策略表中的顺序从上至下进行匹配，查看是否有匹配的策略，并执行匹配到的第一个策略所定义的动作：转发或丢弃。并且不再继续比较其余的策略。

可以通过设置“过滤类型”指定访问控制策略的过滤类型，设备提供四种过滤类型：IP 过滤、URL 过滤、关键字过滤以及 DNS 过滤。

1.　IP 过滤

IP 过滤指对数据包的包头信息过滤，例如源地址和目的 IP 地址。如果 IP 头中的协议字段封装协议为 TCP 或 UDP，则再根据 TCP 头信息（源端口和目的端口）或 UDP 头信息（源端口和目的端口）执行过滤。

过滤类型为 IP 过滤时，可供设置的过滤条件包括：源地址（适用用户）、目的 IP 地址、协议、源端口、目的端口、动作和生效时间等。

2.　URL 过滤

URL 过滤指对 URL 网址过滤，根据 URL 中的关键字进行过滤，不仅可以控制内网用户对站点的访问，还可以控制用户对网页的访问。

过滤类型为 URL 过滤时，可供设置的过滤条件包括：源地址（适用用户）、过滤内容（指 URL 地址）、动作和生效时间等。

3.　关键字过滤

关键字过滤指对 HTML 页面（网页）中的关键字过滤，它的意思是如果你在某个网页里发

表了包含了定义的关键字（如色情、反动、赌博等）的言论，将会提交不成功。

过滤类型为关键字过滤时，可供设置的过滤条件有：源地址（适用用户）、过滤内容（指网页中的关键字）和生效时间等。

4. DNS 过滤

DNS 过滤指对域名进行过滤，根据域名名称中的关键字进行 DNS 过滤。

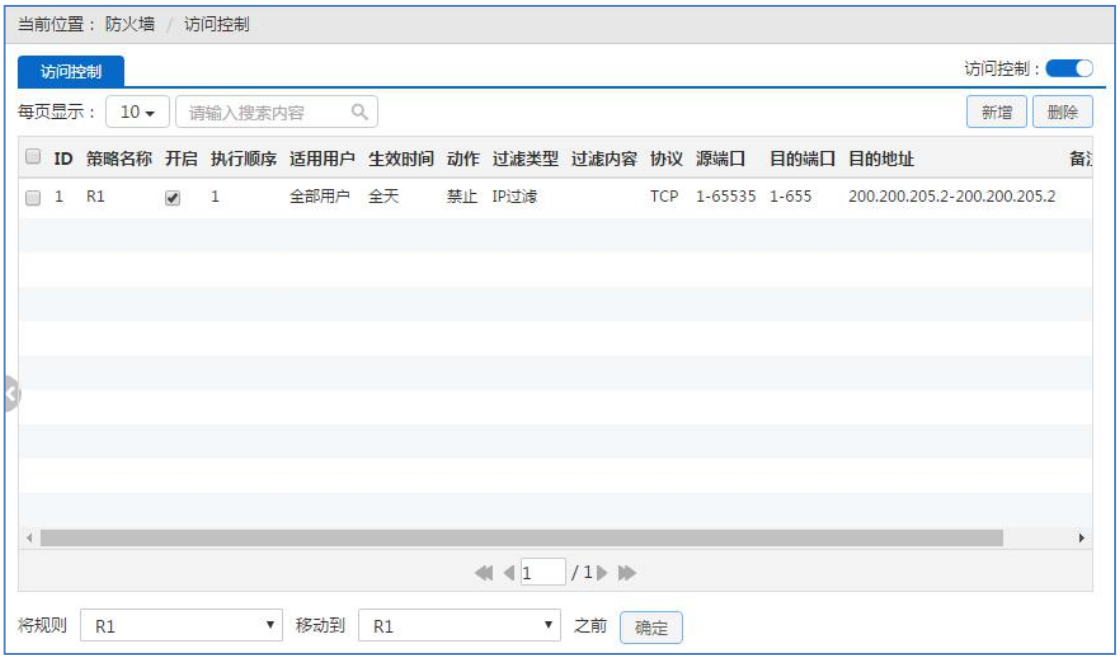
过滤类型为 DNS 过滤时，可供设置的过滤条件包括：源地址（适用用户）、过滤内容（指需要过滤的域名名称）、动作、生效时段。

提示：DNS 过滤是通过 UDP 53 端口实现过滤，URL 过滤是通过 TCP 80 端口实现过滤。

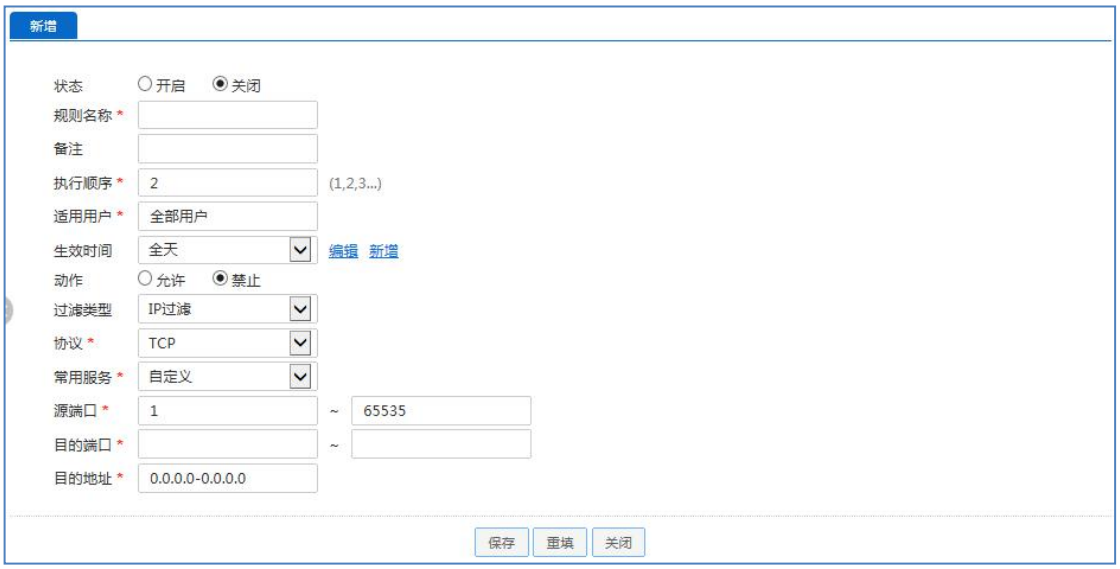
访问控制策略的动作包括转发和丢弃，对应的“动作”分别为“允许”或“禁止”。当需要处理的数据包与某条已定义的访问控制策略相匹配时，如果该策略的“动作”是“允许”，那么设备将转发该数据包。如果该策略的“动作”是“禁止”，那么设备将丢弃该数据包。

需要注意的是，关键字过滤由于其特殊的应用性，并不提供“动作”的选择，而是默认“禁止”。

进入页面的方法：“防火墙 > 访问控制”。



点击“新增”按钮，配置访问控制规则。不同的过滤类型，配置的参数不同。



1. IP 过滤

选项	描述
状态	开启或关闭访问控制功能。
规则名称	配置此规则的名称，不可与其他规则的名称重复。
备注	配置描述信息。
执行顺序	配置该访问控制规则执行的顺序级别，取值范围 1-65535，数值越小，执行越早，决定规则的属性取值。
适用用户	配置该访问控制规则适用的用户范围，默认为全部用户，也可以通过组织架构选择指定的用户，或通过 IP 地址指定用户。
生效时间	配置该访问控制规则的生效时间范围，默认为“全天”。
动作	配置该访问控制规则的执行动作，选项为“允许”或“禁止”。 允许：允许与该访问控制规则匹配的数据包通过，即设备将转发该数据包。 禁止：禁止与该访问控制规则匹配的数据包通过，即设备将丢弃该数据包。
过滤类型	选择“IP 过滤”。
协议	该访问控制策略的协议类型。
常用服务	定义该访问控制规则适用的服务。 选择某个常用服务后，系统自动将该端口号填充到“源端口”和“目的端口”。 特别地，若选择“所有”，则“源端口”和“目的端口”分别填充为 1 和 65535。
源端口	配置该访问控制规则的源起始端口和结束端口，通过它们可以指定一段范围的源端口。如果只定义一个源端口，则将它们设置为同一个值。取值范围均为 1～65535。
目的端口	配置该访问控制规则的目的起始端口和结束端口，通过它们可以指定一段范围的目的端口。如果只定义一个目的端口，则将它们设置成同一个值，取值范围均为 1～65535。
目的地址	配置该访问控制规则的目的起始 IP 地址和结束 IP 地址，通过它们可以指定一

	段范围的目的 IP 地址。如果只定义一个目的 IP 地址，则将它们设置成同一个值。

2. URL 过滤

选项	描述
状态	开启或关闭访问控制功能。
规则名称	配置此规则的名称，不可与其他规则的名称重复。
备注	该访问控制规则的描述信息。
执行顺序	配置该访问控制规则执行的顺序级别，取值范围 1-65535，数值越小，执行越早，决定规则的属性取值。
适用用户	配置该访问控制规则适用的用户范围，默认为全部用户，也可以通过组织架构选择指定的用户，或通过 IP 地址指定用户。
生效时间	配置该访问控制规则的生效时间范围，默认为“全天”。
动作	配置该访问控制规则的执行动作，选项为“允许”或“禁止”。 允许：允许与该访问控制规则匹配的数据包通过，即设备将转发该数据包。 禁止：禁止与该访问控制规则匹配的数据包通过，即设备将丢弃该数据包。
过滤类型	选择“URL 过滤”。
过滤内容	该访问控制策略需过滤的 URL 地址。

URL 过滤是根据 URL 的关键字进行过滤的，当访问的网页的 URL 中含有与“过滤内容”完全匹配的字段时，就认为是匹配该策略的。这里可输入一个完整的域名，这时，该域名开头的所有网页都被匹配。也可输入域名的子字符串，这时，URL 中包含该子字符串的所有网页都被匹配，从而实现对某个站点的所有网页的过滤。

例 1，如果输入 www.sina.com.cn，那么以 www.sina.com.cn 开头的所有网页都将匹配该策略，如 www.sina.com.cn/index.jsp，但是 book.sina.com.cn 开头的网页却不被匹配。

例 2，如果输入 www.utt.com.cn/bbs/，则以 www.utt.com.cn/bbs/ 开头的所有网页都将匹配该策略，从而控制对 utt 这个站点中 bbs 页面的访问。

例 3，如果输入 sina.com，那么所有出现 sina.com 和 sina.com.cn 的网页都被匹配，相当于整个 sina 站点都被匹配，当然，此时以 book.sina.com.cn 开头的网页将被匹配。

提示:

1. URL 地址中，英文字符不区分大小写。输入 URL 时，请不要包含 http://。
2. URL 过滤不能控制用户使用网页浏览器访问的其它服务。例如，URL 过滤不能控制对 ftp://ftp.utt.com.cn 的访问。在这种情况下，需通过配置 IP 过滤类型的访问控制策略来禁止或允许 FTP 连接。

3. 关键字过滤

选项	描述
状态	开启或关闭访问控制功能。
规则名称	配置此规则的名称，不可与其他规则的名称重复。
备注	该访问控制规则的描述信息。
执行顺序	配置该访问控制规则执行的顺序级别，取值范围 1-65535，数值越小，执行越早，决定规则的属性取值。
适用用户	配置该访问控制规则适用的用户范围，默认为全部用户，也可以通过组织架构选择指定的用户，或通过 IP 地址指定用户。
生效时间	配置该访问控制规则的生效时间范围，默认为“全天”。
动作	配置该访问控制规则的执行动作，选项为“允许”或“禁止”。 允许：允许与该访问控制规则匹配的数据包通过，即设备将转发该数据包。 禁止：禁止与该访问控制规则匹配的数据包通过，即设备将丢弃该数据包。
过滤类型	选择“关键字过滤”。
过滤内容	该访问控制策略需过滤的关键字，指网页上的关键字。

4. DNS 过滤

选项	描述
状态	开启或关闭访问控制功能。
规则名称	配置此规则的名称，不可与其他规则的名称重复。
备注	该访问控制规则的描述信息。
执行顺序	配置该访问控制规则执行的顺序级别，取值范围 1-65535，数值越小，执行越早，决定规则的属性取值。
适用用户	配置该访问控制规则适用的用户范围，默认为全部用户，也可以通过组织架构选择指定的用户，或通过 IP 地址指定用户。
生效时间	配置该访问控制规则的生效时间范围，默认为“全天”。
动作	配置该访问控制规则的执行动作，选项为“允许”或“禁止”。 允许：允许与该访问控制规则匹配的数据包通过，即设备将转发该数据包。 禁止：禁止与该访问控制规则匹配的数据包通过，即设备将丢弃该数据包。
过滤类型	选择“DNS 过滤”。
过滤内容	设置要过滤的域名名称。 在过滤内容中输入通配符“ * ”可实现对多个域名的过滤，例如在过滤内容中输入域名名称“*.163.*”，动作选择“禁止”，则内网用户将不能访问域名中有“.163.”的所有网页。

访问控制实例

本节介绍两个访问控制实例。

实例一

某企业内网要求在工作时间段（周一至周五，9:00~18:00）只允许 IP 地址为 192.168.1.9-192.168.1.20 的用户使用 WEB 业务。

分析

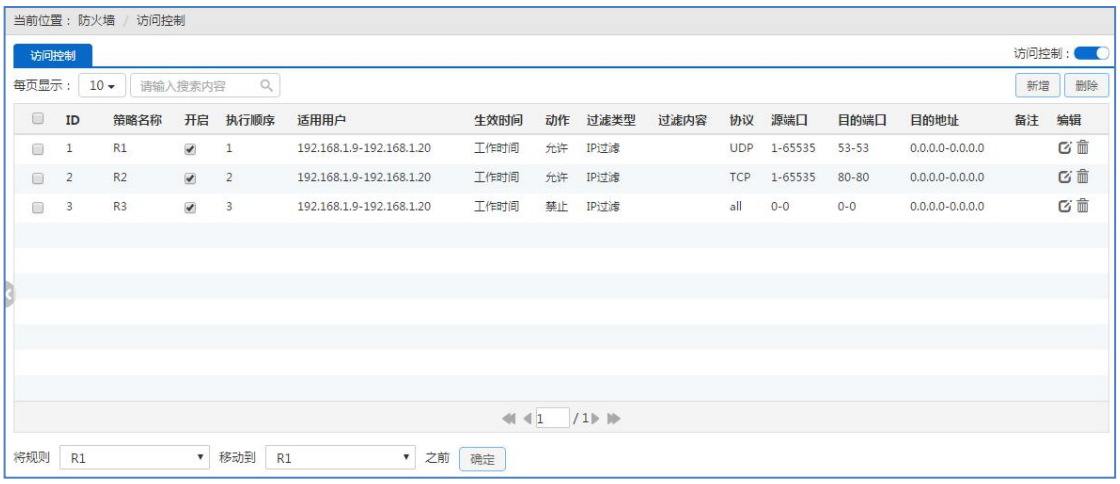
自定义策略 1：允许 192.168.1.9-192.168.1.20 的 DNS 应用。

自定义策略 2：允许 192.168.1.9-192.168.1.20 的 WEB 应用。

自定义策略 3：禁止 192.168.1.9-192.168.1.20 其他所有应用。

需要注意的是，(策略 3) 在禁止所有服务时，也会禁止 DNS 服务，为使该地址段得得用户网络访问正常，应该将策略 3 配置在最后。

访问控制策略列表：



实例二

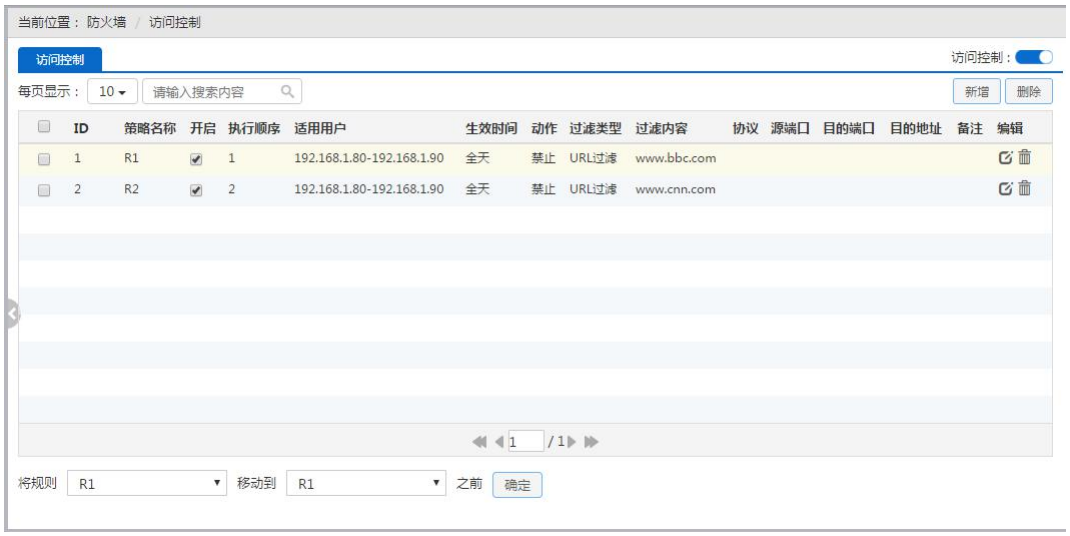
某企业网要禁止 IP 地址为 192.168.1.80~192.168.1.90 的用户访问网站 www.bbc.com（IP 地址为 29.58.246.93）和网站 www.cnn.com（IP 地址为 157.166.255.18），允许该组其他所有上网业务。

分析

配置策略 1，禁止 192.168.1.80~192.168.1.90 段用户访问 www.bbc.com。

配置策略 2，禁止 192.168.1.80~192.168.1.90 段用户访问 www.cnn.com。

访问控制策略列表：



10.2 连接控制

定义设备允许内网每台主机建立的最大总连接数、最大 TCP 连接数、最大 UDP 连接数、最大 ICMP 连接数。

进入页面的方法：“防火墙 > 连接控制”。

页面参数配置介绍：

选项	描述
状态	开启或关闭连接数控制功能。
总连接数	允许内网每台主机建立的最大总连接数。
TCP 连接数	允许内网每台主机建立的最大 TCP 连接数。
UDP 连接数	允许内网每台主机建立的最大 UDP 连接数。
ICMP 连接数	允许内网每台主机建立的最大 ICMP 连接数。

提示:

1. 当连接数设置为 0 时，表示对内网每台主机的连接数不进行限制。

2. 当内网应用(比如网络游戏)连接速度变慢时,可以适当提高“总连接数”以及“UDP连接数”(或者“TCP 连接数”)。注意,上述连接数设置过高可能会导致设备减弱甚至丧失防止 DDoS 攻击的能力。
3. 一般情况下,最大会话数不能设置得太小,建议:“TCP 连接数”不小于 90、“UDP连接数”不小于 50、“ICMP 连接数”不小于 9。如果它们的值太小,将导致局域网用户不能上网或上网异常。

10.3 攻击防护

配置安全防护功能。

进入页面的方法:“防火墙 > 攻击防护”。

页面参数配置介绍:

选项		描述
内网防护	启用 DDoS 攻击防御	启用后能有效防御内网常见的 DDOS 攻击。
	启用 IP 欺骗防御	启用后能有效防御内网的 IP 欺骗现象。
	启用 UDP FLOOD 防御	启用后能有效防御内网 UDP FLOOD 攻击。
	启用ICMP FLOOD防御	启用后能有效防御内网 ICMP FLOOD 攻击。
	启用 SYN FLOOD 防御	启用后能有效防御内网 SYN FLOOD 攻击。
	启用 ARP 欺骗防御	启用后,设备的 LAN 口每隔一定的时间(默认为 100 毫秒)发送 ARP 广播包,能有效防御 ARP 欺骗。
	启用端口扫描防御	启用后能有效防御内网端口扫描。
外网防护	拒绝外部 Ping	设备的 WAN 口不响应来自外网的 ping 请求。

第 11 章　VPN 配置

VPN（Vitual Private Network），虚拟专用网指的是依靠 ISP（Internet Service Provider 因特网服务提供商）和其它 NSP（Network Service Provider 网络服务提供商），在公用网络（如 Internet）中建立专用的网络连接的技术，此网络连接采用专有的隧道协议，实现了数据的加密和完整性的校验、用户的身份认证，从而保证信息在传输过程中不被偷窃、篡改、复制等，类似于在公共网络中建立了一个专线网络一样，只不过这个专线网络是逻辑上的而不是物理上的，所以称为虚拟专用网。由于使用 Internet 进行传输相对于租用专线来说，费用极为低廉，所以 VPN 的出现使企业通过 Internet 既安全又经济的传输私有的机密信息成为可能。

11.1　IPsec

随着安全标准与网络协议的不断发展，各种 VPN 技术层出不穷，IPSec VPN 则是当前应用最广泛的 VPN 安全技术之一。IPSec 是创建和维持 IP 网络安全通信的一套开放标准、协议，它提供两种安全机制：加密和认证。加密机制保证了数据的机密性，认证机制保证了数据是来自原始的发送者并且在传输过程中没有被破坏和篡改。

IPSec 能提供以下服务：

- 数据机密性：IPSec 发送方在通过网络传输包前对包进行加密。
- 数据完整性：IPSec 接收方对发送方发来的包进行认证，以确保数据在传输过程中没有被篡改。
- 数据源认证：IPSec 在接收端可以认证发送 IPSec 报文的发送端是否合法，以确保数据的真实性。
- 抗重播：IPSec 接收方可检测并拒绝接收重复的报文。

11.1.1 缩略语与专业名词

IPSec（IP Security Protocol），IP 网络安全协议：IPSec 是 IETF 制定的一系列协议，以保证在 Internet 上传送数据的安全保密性能，通信方之间在 IP 层通过加密与数据源验证来保证数据包在 Internet 上传输时的机密性、完整性和真实性。

IKE（Internet Key Exchange），因特网密钥交换：IKE 用于通信双方协商和建立安全联盟、交换密钥。IKE 定义了通信双方进行身份验证、协商加密算法以及生成共享密钥的方法。

DES（Data Encryption Standard），数据加密标准：DES 是 IPSec 使用的一种数据加密

算法，用于对数据包进行加密。

3DES（Triple Data Encryption Standard），三倍数据加密标准：3DES 是 IPSec 使用的一种数据加密算法，用于对数据包进行比 DES 强度更高的加密。

AES（Advanced Encryption Standard），高级加密标准：AES 是 IPSec 使用的一种数据加密算法。与 DES 和 3DES 相比，AES 更加高效、安全。

DH（Diffie-Hellman Group），一种密钥交换算法：通信的双方各自生成一对公/私钥，只需和对方交换公钥，经过计算就可得到一组用来保护通信的密钥，这就避免了直接在通信中传输密钥的风险，提高了整个 IPSec 系统的安全性。DH 有一个重要的属性：group（组件），共有 5 种基本 group，常用的 group 有：模数为 924 位的 MODP 组（group2）、模数为 1536 位的 MODP 组（group5）。

MD5（Message Digest 5），消息摘要版本 5：从任意长度信息和 16 字节密钥生成 98 位散列（也称作数字签名或信息整理）的算法。所生成的散列（如同输入的指印）用于验证内容和来源的真实性和完整性。

SHA-1（Secure Hash Alogrithm1），安全散列算法 1：从任意长度信息和 20 字节密钥生成 160 位散列的算法。通常认为它比 MD5 更安全，因为它生成的散列更大。

SA（Security Association），安全联盟：在两个设备之间建立一个 IPSec VPN 隧道并通过其进行安全通信之前，它们必须就通信期间需要使用的安全参数达成一致，即建立一个 SA。SA 将指定需要使用的认证与加密算法、在通话期间使用的密钥和安全联盟本身需要维持的时间，SA 是单向的。

SPI（Security Parameter Index），安全参数索引：SPI 实际上是一个长度为 32 位的数据实体，用于独一无二地标识出接收端上的一个 SA。

AH（Authentication Header），认证包头：属于 IPSec 的一种协议。该协议用于为 IP 数据包提供数据完整性、数据包源地址验证服务。与 ESP 协议相比，AH 不提供对通信数据加密服务。

ESP（Encapsulating Security Payload），封装安全负荷：属于 IPSec 的一种协议。它用于确保 IP 数据包的机密性（对第三方不可见）、数据的完整性以及对数据源地址的验证，同时还具有抗重播的特性。

PSK（Pre-Shared Key），预共享密钥：IKE 身份验证方法之一，它要求每个 IKE 对等方使用一个预定义和共享的密钥来对 IKE 交换执行身份验证。

第一阶段和第二阶段：采用互联网密钥交换协议（IKE）建立 IPSec 通道安全联盟（SA），需要进行两个阶段的协商。在第一阶段，参与者相互验证身份并协商建立一个用来协商随后 IPSec SA 的安全通道。在第二阶段，参与者协商并建立用于加密和认证用户数据的 IPSec SA。

Main Mode and Aggressive Mode，主模式和野蛮模式：IKE 自动协商通道的第一阶段，可以在主模式和野蛮模式这两种模式下进行。主模式下，发起方和响应方之间进行三次双向信息交换，总共六条信息。野蛮模式下，发起方和响应方获取相同的对象，但仅进行两次交换，总共有三条消息。

DPD（Dead Peer Detect）：周期对端检测：使用 DPD，能够定期检测 SA 对方是否正常，网络连接是否正常。

IPSec NAT-T(NAT-Traversal),IPSec NAT 穿透技术 :该技术实现了 IPSec 协议穿透 NAT 设备。

11.1.2 安全联盟

在两个设备之间建立一个 IPSec VPN 隧道并通过其进行安全通信之前，它们必须就通信期间需要使用的安全参数达成一致，即建立一个安全联盟 SA。SA 是由一对指定的安全参数索引（SPI）、目标 IP 地址以及使用的安全协议组成。

通过 SA，IPSec 隧道可以提供以下安全功能：

- 机密性（通过加密）
- 内容完整性（通过数据认证）
- 发送方认证和认可（通过身份认证）

一、安全联盟建立

安全联盟（SA）是 IPSec 隧道双方用于确保隧道安全的有关方法和参数的单向协议。对于 IPSec 双向通信，至少必须有两个 SA，一个用来接收来自对端的数据，一个用来发送数据给对方。

建立 SA，需要进行两个阶段的协商：

- 在第一阶段，通信双方协商如何保护以后的通信，建立一个已通过身份认证和安全保护的通道（即 IKE SA），此通道将用于保护后面的 IPSec SA 的协商过程。
- 在第二阶段，通信双方为 IPSec 协商加密算法、密钥、生存周期以及认证身份，建立用于加密和认证用户数据的通道（即 IPSec SA）。

1. **第一阶段**

第一阶段可以使用野蛮模式（Aggressive Mode）或主模式（Main Mode），不管使用哪种模式，双方均将交换对方可以接受的安全提议，例如：

- 加密算法（DES、3DES 和 AES98/192/256）和认证算法（MD5 和 SHA-1）
- Diffie-Hellman 组（请参阅本节的“Diffie-Hellman 交换”）

- 预共享密钥

当隧道的两端都同意接受所提出的至少一组第一阶段安全参数，并处理相关参数时，一个成功的第一阶段协商将结束。设备作为发起方时，目前最多同时支持 8 种第一阶段协商的提议，允许用户定义一系列安全参数。作为响应方时，可接受任何组合形式的第一阶段协商的提议。

➢ **主模式和野蛮模式（Main Mode / Aggressive Mode）**

第一阶段可能发生在野蛮模式或主模式下，这两种模式如下所述：

主模式：发起方和响应方之间进行三个双向信息交换（总共六条信息）以完成以下功能：

- 第一次交换，（信息 1 和 2）：提出并接受加密和认证算法。
- 第二次交换，（信息 3 和 4）：执行 Diffie-Hellman 交换，发起方和响应方各提供一个当前数（随机生成的号码）。
- 第三次交换，（信息 5 和 6）：发送并验证其身份。

在第三次交换信息时传输的信息由在前两次交换中建立的加密算法保护。因此，在明文中没有传输参与者的身份，从而提供了最大限度的保护。

野蛮模式：发起方和响应方获取相同的对象，但仅进行两次交换，总共有三条消息：

- 第一条消息：发起方建议 SA，发起 Diffie-Hellman 交换，发送一个当前数及其 IKE 身份。
- 第二条消息：响应方接受 SA，认证发起方，发送一个当前数及其 IKE 身份，以及发送响应方的证书（如果使用证书）。
- 第三条消息：发起方认证响应方，确认交换。

由于参与者的身份是在明文中交换的（在前两条消息中），故野蛮模式不提供身份保护。

提示:

当 IPSec 隧道的连接方式为对方动态连接到本地、动态连接到网关时，必须使用野蛮模式进行协商。

➢ **Diffie-Hellman 交换**

Diffie-Hellman 交换也称“DH 交换”，它允许双方生成一个共享密钥。该技术的优点在于它允许通信双方在非安全媒体上创建密钥，而不必把预共享密钥通过网络传输。共有五种基本 DH 组（设备支持组 2 和 组 5），在各组计算中所使用主要模数的大小都不同，如下所述：

- DH 组 2：924 位模数
- DH 组 5：1536 位模数

模数越大，就认为生成的密钥越安全。但是，模数越大，密钥生成过程就越长。

提示:

由于每个 DH 组的模数大小都不同，因此 IPSec 隧道通信双方必须使用相同的组。

2. **第二阶段**

当通信双方建立了一个已认证的安全通道后，将继续执行第二阶段，在此阶段中，将协商 IPSec SA 以保护要通过 IPSec 隧道传输的用户数据。

与第一阶段的过程相似，通信双方交换提议以确定要在 SA 中使用的安全参数。第二阶段提议还包括一个安全协议（目前设备支持 ESP）和所选的加密和认证算法。

不管在第一阶段中使用何种模式，第二阶段总是在“快速”模式中运行，并且包括三条消息的交换。

二、安全联盟的维护

一旦 SA 建立完毕，IPSec 双方还必须维护 SA，确保 SA 是安全有效的，IPSec 通过以下方法实现 SA 的有效性检测：

1. SA 生存时间

在建立 SA 的协商过程中，双方会协商该 SA 的生存时间，当生存时间达到预先设定的值时，需要重新协商以建立新的 SA。周期性的重新协商，相当于定期更改密码。

WEB UI 方式下，在“VPN 配置>IPSec”的“高级选项”中，可配置“生存时间”和“最大流量”。

由于频繁重建 SA 需要消耗大量的系统资源（主要是 DH 交换和当前数生成），会降低数据传输效率。因此 SA 的生存时间通常设置的比较长（典型的是 1 小时到 1 天），在有效期内，由于双方不能互相检测对方（类似 PING 的功能），通信的双方只能“假设”对方是正常工作的，万一有一方发生了不可预见的问题或连接双方的网络有故障，通信的另一方并不知道此时双方的连接线路中断，还会继续向早已经不存在的另一方发送数据，造成虚假连接（SA 正常，发出正常，但无法完成双向通信），因此需要一种有效的方法来检测参与 IPSec SA 的双方都完全正常，他们之间的网络连接也完全正常。这种检测方法的开销要比重新协商 IPSec SA 更小，因此可以用更高的密度进行检测。这种技术就是 IPSec“DPD”，DPD 作为 SA 协商的一种补充而存在。

2. DPD（Dead Peer Detect）

IPSec DPD 定期检测 SA 对方是否还存在，在 SA 的生存时间和最大流量范围内，定期检测对方网络是否可达，程序是否正常，以便发现网络变化导致的通信故障或避免与一个已经不存在的“火星人”主机保持 SA，这个检测周期通常为 20 秒或 1 分钟左右，双方通过发送“心

跳”包来检测对方是否正常，连续丢失多个心跳包后，IPSec DPD 会强制重新发起 SA 协商。

WEB UI 方式下，在“VPN 配置>IPSec”的“高级选项”中，可通过选中“DPD”选项来启用 DPD 功能，可通过配置“心跳”来确定检测周期。

11.1.3 IPSec NAT 穿透

由于历史的原因，部署 NAT 模式下的 IPSec VPN 网络的问题之一在于无法定位网络地址转换（NAT）之后的 IPSec 对话方。Internet 服务提供商和小型办公/家庭办公（SOHO）网络通常使用 NAT 共享单个公共 IP 地址。虽然 NAT 有助于节省剩余的 IP 地址空间，但是它们也给诸如 IPSec 之类的端对端协议带来了问题。

在 NAT 对 IPSec 造成中断的众多原因中，主要的一个原因就是，对于“封装安全性协议（ESP）”来说，NAT 设备不能识别端口转换的 Layer 4（第 4 层）包头的位置（因为它已被加密）。对于“认证包头（AH）”协议来说，NAT 设备能修改端口号，但不能修改认证检查，于是对整个 IPSec 封包的认证检查就会失败。

一种称为 IPSec NAT 穿透（NAT-T）的新技术正在由 Internet 工程任务组的 IPSec 网络工作组标准化。

在 IPSec 协商过程中，可根据以下两个条件自动确定支持 IPSec NAT-T 的对话双方：

- 发起 IPSec 对话的一方（通常是一个客户端计算机）和响应 IPSec 对话的一方（通常是一个服务器）是否都能执行 IPSec NAT-T。
- 它们之间的路径中是否存在任何 NAT。

如果这两个条件同时为真，那么双方将使用 IPSec NAT-T 来通过 NAT 发送受 IPSec 保护的流量。如果其中一方不支持 IPSec NAT-T，则执行常规的 IPSec 协商（在前两个消息之后）和 IPSec 保护。如果双方都支持 IPSec NAT-T，但是它们之间不存在 NAT，则执行常规的 IPSec 保护。

提示:

IPSec NAT-T 是仅为 ESP 流量定义的，AH 流量无法穿过 NAT 设备。

设备可以应用 NAT 穿透（NAT-T）功能。NAT-T 在第一阶段交换过程中，沿着数据路径检测发现存在一个或多个 NAT 设备后，将添加一层 UDP 封装（通常使用 UDP4500 端口），从而通过 NAT 设备。

WEB UI 方式下，在“VPN 配置>IPSec”的“高级选项”中，可通过选中“NAT 穿透”选项来启用 NAT 穿透功能。

11.1.4 IPSec 隧道列表

查看相关的 IPSec 隧道信息，如 SA 状态、远端网关地址、远端内网地址、本地绑定的接口等。

进入页面的方法：“VPN 配置 > IPSec”。

提示:

当 IPSec 的连接方式为“对方动态连接到本地”时，拨号按钮无效。

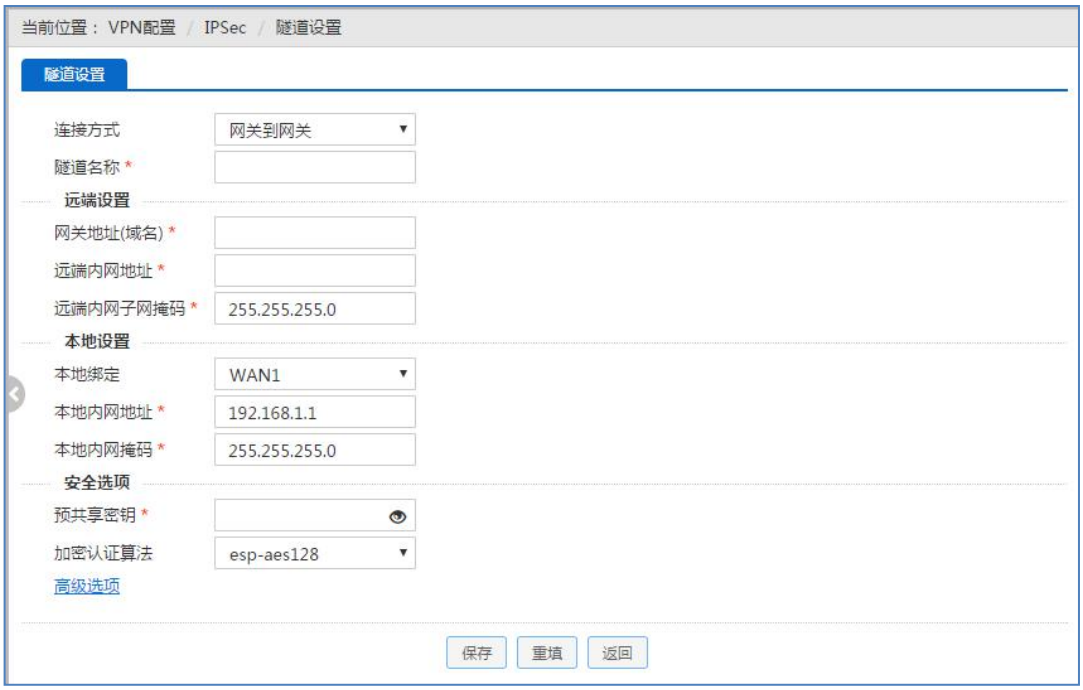
11.1.5 IPSec 配置

IPSec 支持的三种连接方式，分别为：网关到网关、动态连接到网关、对方动态连接到本地。下面分别介绍着三种连接方式配置参数的含义。

当 IPSec 隧道一端是动态 IP 接入(未申请 DDNS)时，隧道两端需使用“动态连接到网关”、“对方动态连接到本地”的连接方式。其中动态 IP 接入的一端选用“动态连接到网关”接入方式，作为发起方，另一端则选用“对方动态连接到本地”接入方式，做为响应方。

点击“VPN 配置 > IPSec”页面的“新增”按钮，配置 IPSec。IPSec 的连接方式不同，配置的参数不同。

1. 网关到网关

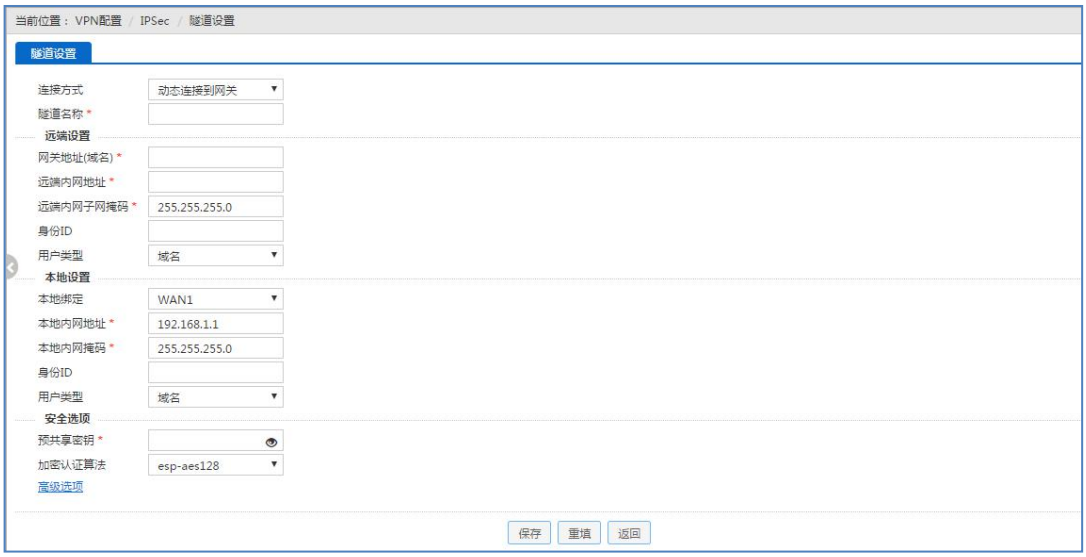


页面参数配置介绍：

选项			描述	
连接方式			选择“网关到网关”。	
隧道名称			配置隧道的名称。	
远端设置	网关地址（域名）		IPSec 隧道远端网关的地址（或域名），设置为域名时，需要在设备上设置 DNS 服务器，此时设备会定期解析该域名，如果 IP 地址发生变化，设备将重新协商 IPSec 隧道。	
	远端内网地址		IPSec 隧道远端受保护的内网的任一 IP 地址，如果远端是移动单机用户，则填写该设备的 IP 地址。	
	远端内网子网掩码		IPSec 隧道远端受保护的内网的子网掩码，如果远端是移动单机用户，则填写 255.255.255.255。	
本地设置	本地绑定		选择本地接口的类型，接口可以是以太网口或 PPPoE 拨号接口。如果将 IPSec 隧道配置为绑定到该接口上，那么所有经过该接口的数据包将通过 IPSec 检查，以确定是否对该数据包进行加密和解密操作。	
	本地内网地址		本地受保护的内网的任一 IP 地址。	
	本地内网掩码		本地受保护内网的子网掩码。	
安全选项	预共享密钥		协商所用的预共享密钥，最长为 98 个字符。	
	加密认证算法		可供第二阶段协商使用的首选加密认证算法。	
	高级选项	第一阶段	协商模式	设置第一阶段的协商模式，可选项有主模式和野蛮模式。当连接方式选择网关到网关时，请选择主模式。当连接方式为动态连接到网关、对方动态连接到本地时，请选择野蛮模式。
			生存时间	设置 IKE SA 的生存时间，至少 600 秒，当剩余时间为

			（秒）	540 秒时，将重新协商 IKE SA。
			加密认证算法 1~4	设置第一阶段协商使用的加密认证算法，可以选择四组，每组为不同的加密算法、认证算法及 DH 组的组合。
		第二阶段	加密认证算法 1~4	设置第二阶段协商使用的加密认证算法，可选三组，加上在基本参数配置中已配置的一组，共四组。
			生存时间（秒）	设置 IPSec SA 的生存时间，至少 600 秒，当剩余时间为 540 秒时，SA 将过期，重新协商 IPSec SA。
		其他	抗重播	设置是否启用抗重播。启用后，网关将支持抗重播功能，从而可以拒绝接收过的数据包或数据包拷贝 ,以保护自己不被攻击。
			DPD	设置是否启用 DPD。启用后，在 SA 的生存时间内，设备定期发送心跳包检测对方网络是否可达，程序是否正常，如果连续丢失多个心跳包，则 IPSec DPD 会强制重新发起 SA 协商。
			NAT 穿透	启用或取消 NAT 穿透功能。
			心跳（秒）	设置发送心跳包的时间间隔。配置该值后，网关会每隔单位时间（“心跳”）向对端发送探测消息，来确定对端是否还存活。
			端口	设置 NAT 穿透时 UDP 封装包的端口号。
			维持（秒）	启用 NAT 穿透功能后，设备将每隔单位时间（“维持”）向 NAT 设备发送一个数据包以维持 NAT 映射，这样就不需要更改 NAT 映射，直到第一阶段和第二阶段的 SA 过期。

2. 动态连接到网关



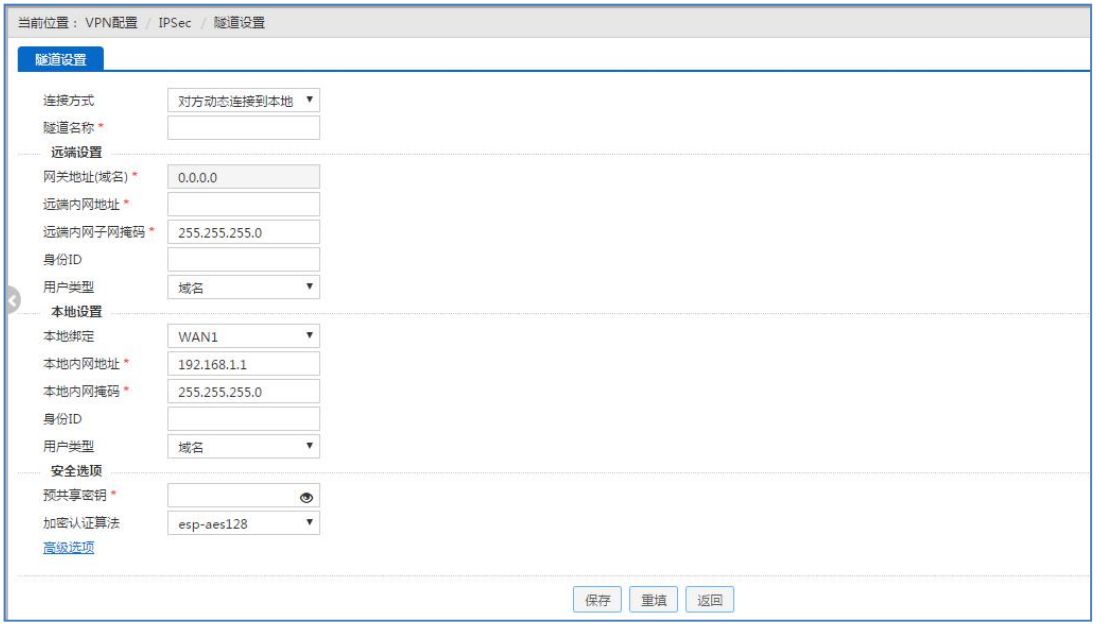
页面参数介绍：

“动态连接到网关”连接方式的部分参数配置同“网关到网关”连接方式，这里不再一一介绍。

选项		描述
连接方式		选择“动态连接到网关”。在这种情况下，在建立 IPSec 隧道时本设备只能作为发起方，且 IPSec 隧道两端都应该选择野蛮模式进行第一阶段的 IKE 协商。
远端设置	身份 ID	设置用于认证远端的身份 ID。
	用户类型	远端身份 ID 的类型，有 Email 地址、 域名及 IP 地址三个选项。
本地设置	身份 ID	本地发送给远端认证的身份 ID。
	用户类型	本地身份 ID 的类型，有 Email 地址、域名及 IP 地址三个选项。

3. 对方动态连接到本地

“对方动态连接到本地”连接方式的参数配置同“动态连接到网关”。选择“对方动态连接到本地”时，远端的网关地址（域名）无需配置。在这种情况下，在建立 IPSec 隧道时本设备只能作为响应方，且 IPSec 隧道两端都应该选择野蛮模式进行第一阶段的 IKE 协商。



11.1.6 IPSec 配置实例

11.1.6.1 网关到网关

1. 需求

在本方案中，某公司总部在上海。在北京有一个分公司希望可以实现两地局域网内部资源的相互访问。本方案使用 IPSec 协议建立 VPN 隧道，两地的 VPN 网关都使用艾泰路由器，地址如下：

上海网关：

内网网段：192.168.1.0/24。

LAN 口 IP 地址：192.168.1.1/24。

WAN1 口域名：200.200.202.126/24。

北京网关：

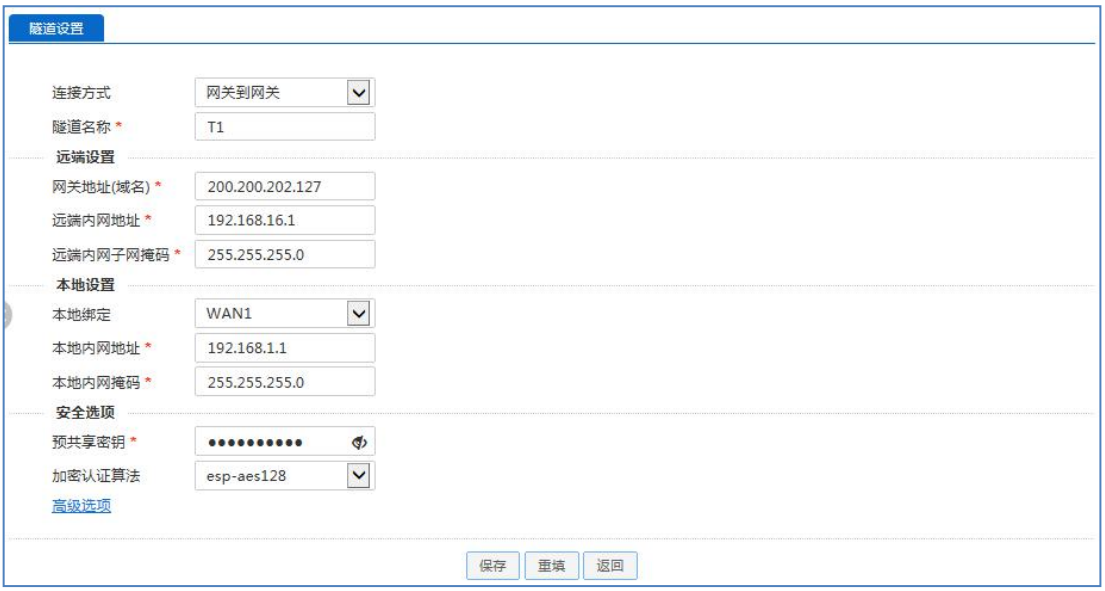
内网网段：192.168.16.0/24。

LAN 口 IP 地址：192.168.16.1/24。

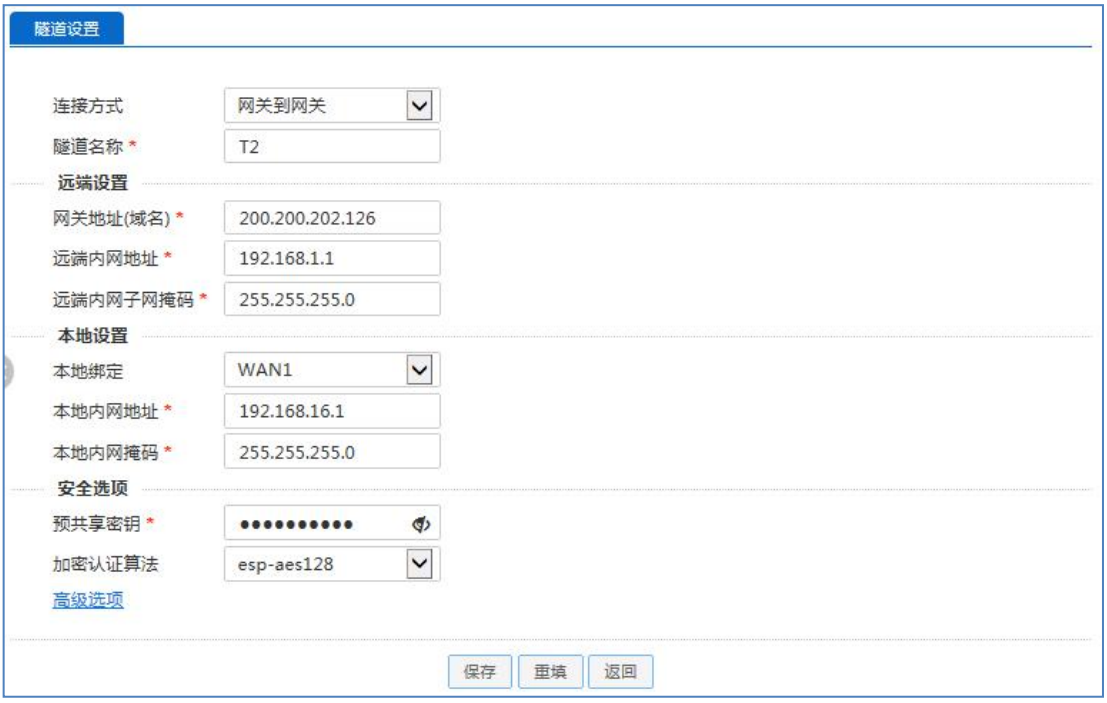
WAN1 口 IP 地址：200.200.202.127/24。

2. 配置

首先：配置上海网关。远端网关地址设置为北京网关的 WAN 口 IP 地址 200.200.202.127，远端内网地址为北京网关的 LAN 口 IP 地址 192.168.1.1，本地绑定在 WAN1 口，设置第一阶段的预共享密钥为 testing，第二阶段的加密认证算法为 esp-ase-128。



其次，配置北京网关。远端网关地址设置为上海网关的 WAN 口 IP 地址 200.200.202.126，远端内网地址为上海网关的 LAN 口 IP 地址 192.168.16.1，本地绑定在 WAN1 口，设置第一阶段的预共享密钥为 testing，第二阶段的加密认证算法为 esp-ase-128。



最后，查看连接状态。分别进入相应页面，查看其 IPSec 实例连接信息。如下图所示可以查看 IPSec 实例的会话状态、远端网关、远端内网、本地绑定接口等信息。

11.1.6.2 一方动态

1. 需求

在本方案中，某公司总部在上海。在北京有一个分公司希望可以实现两地局域网内部资源的相互访问。本方案使用 IPSec 协议建立 VPN 隧道，两地的 VPN 网关都使用艾泰路由器，地址如下：

上海网关：

内网网段：192.168.1.0/24。

LAN 口 IP 地址：192.168.1.1/24。

WAN1 口域名：200.200.202.126/24。

北京网关：

内网网段：192.168.16.0/24。

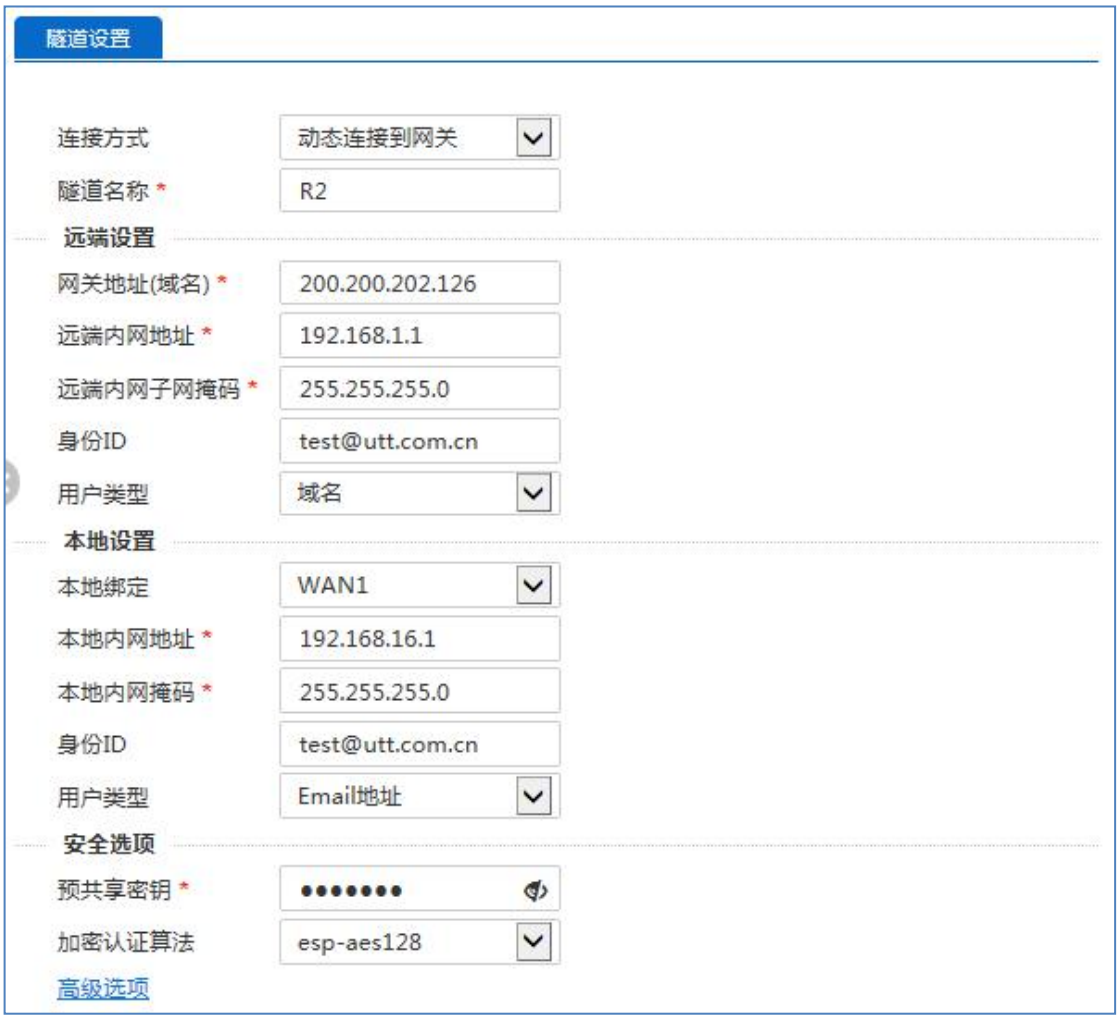
LAN 口 IP 地址：192.168.16.1/24。

WAN1 口 IP 地址：动态获取。

2. 配置

首先，配置上海网关。设置连接方式为对方动态连接到本地，北京网关动态连接到上海网关。同时设置北京网关相关信息，如内网地址、身份 ID。本地绑定在 WAN1 口，设置第一阶段的预共享密钥为 testing，第二阶段的加密认证算法为 esp-ase-128。

其次，配置北京网关。设置北京网关的连接方式为动态连接到网关。同时设置上海网关相关信息，如网关地址、内网地址、身份 ID。本地绑定在 WAN1 口，设置第一阶段的预共享密钥为 testing，第二阶段的加密认证算法为 esp-ase-128。



最后，查看连接状态。分别进入相应页面，查看其 IPSec 实例连接信息。如下图所示可以查看 IPSec 实例的会话状态、远端网关、远端内网、本地绑定接口等信息。

11.2 PPTP/L2TP

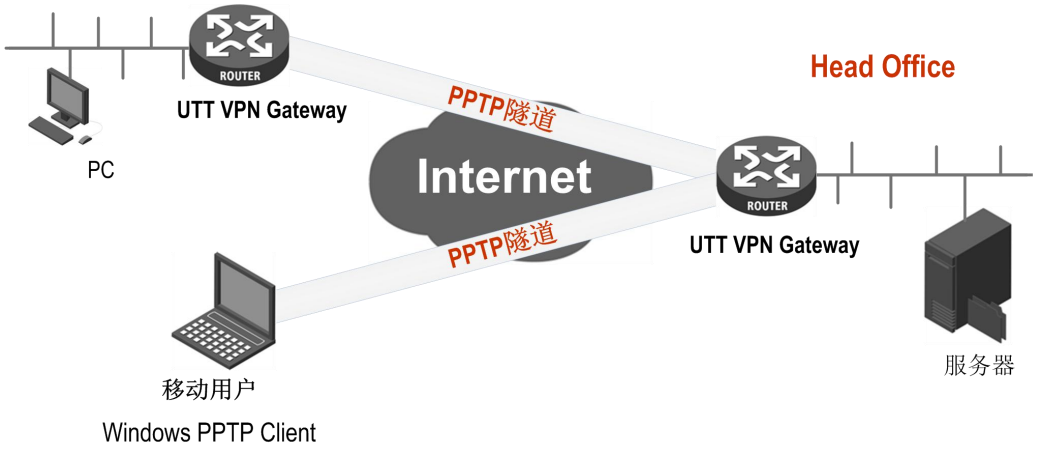
11.2.1 PPTP 介绍

PPTP（Point-to-Point Tunneling Protocol），点到点隧道协议：PPTP 是一种虚拟专用网络协议，属于第二层的协议。PPTP 将 PPP（Point-to-Point Protocol）帧封装在 IP 数据报中，通过 IP 网络如 Internet 或企业专用 Intranet 等发送。

PPTP 协议的基本功能是在 IP 网络中传送采用 PPP 封装的用户数据包。PPTP 客户端负责

接收用户的原始数据，并将之封装到 PPP 数据包，然后在 PPTP 客户端和服务器之间建立 PPTP 隧道传送该 PPP 数据包。

典型的应用通常是 PPTP 客户端部署在远程分支机构或移动办公用户的个人电脑软件中，他们用来发起 PPTP 隧道。PPTP 服务器部署在企业中心或办公室，用来接收来自 PPTP 客户端的呼叫，当建立起 PPTP 隧道连接后，PPTP 服务器接收来自 PPTP 客户端的 PPP 数据包，并还原出用户的数据包，然后把还原后的数据包发送到最终用户的电脑设备上。



11.2.2 PPTP 隧道列表

查看相关的 PPTP 隧道信息，如用户类型、远端网关 IP 地址、会话状态、会话时间等。

进入页面的方法：“VPN 配置 > PPTP/L2TP”。

提示:

1. “建立”、“挂断”按钮的操作只对 PPTP 客户端生效。
2. 为保证 VPN 网关启用 NAT 后，PPTP 隧道正常连接，PPTP 配置完成之后，系统会自动生成一条 TCP 1723 端口的 NAT 静态映射（可在“网络配置> 端口映射 > 静态映射”页面中查看，名称为“pptp”）。请不要编辑、删除它们，否则可能造成

PPTP 隧道无法连接和无法传输数据。

11.2.3 PPTP 配置

点击“VPN 配置 > PPTP/L2TP > 隧道列表”页面的“新增”按钮，配置 PPTP 服务端或客户端参数。

配置 PPTP 服务端

路由器作为 PPTP 服务器，在 PPTP 服务器上配置 PPTP 用户账号供用户建立 PPTP 隧道使用。

页面参数配置介绍：

选项	描述
工作模式	选择“服务端（拨入）”。
协议类型	选择“PPTP”。
隧道名称	自定义该条隧道的名称，不能重复。
用户类型	选择用户类型，可选项为“LAN 到 LAN”或“移动用户”。 • 移动用户：拨入的 VPN 用户是个人用户，往往由单个计算机拨入，实现 PPTP 隧道远端计算机与本地局域网的通信。 • LAN 到 LAN：拨入的 PPTP 用户是一个网段的用户，往往是通过一个路由器拨入，实现 PPTP 隧道两端局域网的通信。
用户名、密码	自定义客户端拨号时使用的用户名和密码。
远端内网地址	✧ 仅适用于“LAN 到 LAN”用户。 配置 PPTP 隧道对端局域网所使用的 IP 地址（一般可以填 VPN 隧道对端设备的 LAN 口 IP 地址）。
远端内网子网掩	✧ 仅适用于“LAN 到 LAN”用户。

码	配置 PPTP 隧道对端局域网所使用的子网掩码。
固定 IP 地址	配置 PPTP 服务器分配给客户端的 IP 地址 ,该地址必须从属于 PPTP 服务器地址池中。
硬件特征码	✧ 仅适用于“移动用户”。 配置 PPTP 移动用户的 MAC 地址。

配置 PPTP 客户端

路由器作为 PPTP 隧道的客户端，发起建立 PPTP 隧道。

页面参数配置介绍：

选项	描述
工作模式	选择“客户端（拨出）”。
协议类型	选择“PPTP”。
NAT 模式	启用 NAT 后，PPTP 客户端会对此 PPTP 隧道连接进行 NAT，即将局域网用户的 IP 地址转化为对端 PPTP 服务器分配的 IP 地址，这样局域网用户将使用 PPTP 服务器分配的 IP 地址连接到隧道对端的局域网，隧道对端设备无需设置到本地的路由。
隧道加密	开启或关闭隧道加密。若启用隧道加密 ,将采用 MPPE 加密技术加密，在“密码验证方式”下拉框中只能选择“MS-CHAPV2”密码验证方式。
隧道名称	该条隧道的名称，与设备中已有的实例名不能重复。
隧道服务器地址	远端 VPN 网关 WAN 口的 IP 地址或者域名（一般填 PPTP 隧道对端设备的 WAN 口 IP 地址或者域名）。
用户名、密码	该条隧道拨号时使用的用户名、密码。

密码验证方式	设置建立 PPTP VPN 的密码验证方式 ,选项有 MS-CHAPV2、PAP、CHAP、ANY（自动和对端设备协商密码验证方式）。密码验证方式要确保与服务端的一致。
远端内网地址	远端内网的 IP 地址，可填写远端 VPN 网关的 LAN 口 IP 地址。
远端内网子网掩码	远端内网的子网掩码。
MTU	最大传输单元。在传送数据单元时，设备将自动与对端设备协商最佳的传送数据单元大小，除非特别应用，不要修改此参数。

PPTP 全局配置

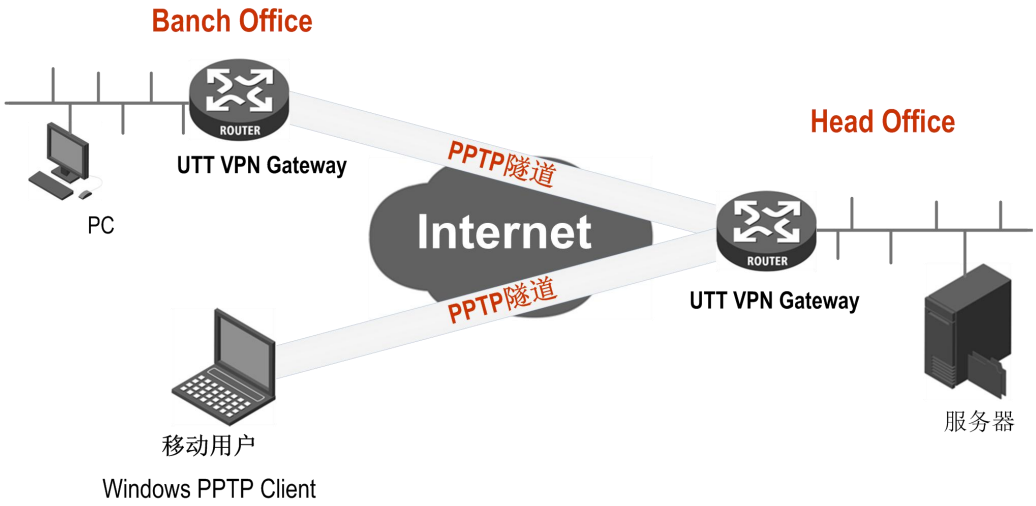
点击“PPTP 服务器全局配置”标签卡，配置参数。

页面参数配置介绍：

选项	描述
状态	开启或关闭 PPTP 功能。
隧道加密	开启或关闭隧道加密。若启用隧道加密，将采用 MPPE 加密技术加密，在“密码验证方式”下拉框中只能选择“MS-CHAPV2”密码验证方式。
密码验证方式	建立 PPTP VPN 的密码验证方式，选项有 ANY（自动和对端设备协商密码验证方式）、PAP、CHAP、MS-CHAPV2。
地址池起始地址	PPTP 服务器分配给 PPTP 客户端的起始 IP 地址，要确保该地址所属网段与局域网中的任何一个网段不重复。
最大连接数	地址池包含的 IP 地址总数量。
服务端 IP 地址	隧道服务端的虚接口 IP 地址，该地址不包含在地址池中，请确认该地址与所配置的地址池在同一网段。

主、备 DNS 服务器	配置主、备 DNS 服务器的 IP 地址。 当设备被配置为 PPTP 服务端时，可以为 PPTP 客户端分配 DNS 地址，其用于客户端连上服务端之后可以通过服务端线路分配的 DNS 地址浏览网页，可解决用户拨通 VPN 后可以访问服务器内部网却无法打开网页的问题。
MTU（字节）	最大传输单元。在传送数据单元时，设备将自动与对端设备协商最佳的传送数据单元大小，除非特别应用，不要修改此参数。

11.2.4 PPTP 配置实例



在本方案中，某公司总部在上海。在北京有一个分公司希望可以实现两地局域网内部资源的相互访问。该公司还有一些出差和远程办公的移动用户希望在远程访问总公司局域网内部资源。

本方案使用 PPTP 协议建立 VPN 隧道，两地的 VPN 网关都使用艾泰路由器，移动用户使用 Windows 操作系统内置的 PPTP 客户端软件，地址如下：

上海网关（PPTP 服务端）：

内网网段：192.168.16.0/24。

LAN 口 IP 地址：192.168.16.1/24。

WAN 口域名：200.200.203.250/24。

北京网关（PPTP 客户端）：

内网网段：192.168.1.0/24。

LAN 口 IP 地址：192.168.1.1/24。

WAN 口 IP 地址：200.200.203.238/24。

移动客户端（PPTP 客户端）：

使用 Windows 操作系统通过 PPTP 拨号建立 PPTP 隧道连接。

配置步骤如下：

首先，配置上海 VPN 网关。

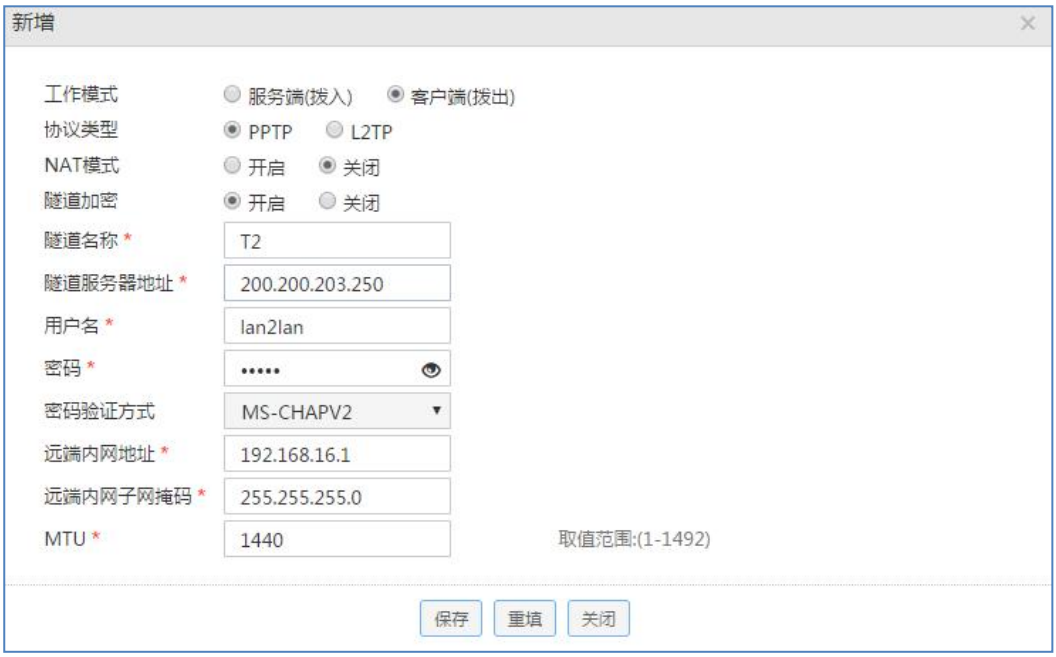
1. 在“VPN 配置 > PPTP/L2TP > PPTP 服务器全局配置”页面，配置上海 VPN 网关。

2. 在“VPN 配置 > PPTP/L2TP > 隧道列表”页面，单击“新增”按钮，为北京分部创建一个账号。用户类型为：LAN 到 LAN。用户名为：lan2lan。密码为：93456。远端内网内网地址为：192.168.1.1。远端内网子网掩码为 255.255.255.0。

3. 为移动用户创建一个账号，用户类型为：移动用户。用户名为：pptpyd。密码为：93456。并且为该移动用户分配 192.168.55.41 的固定 IP 地址。

然后，配置北京 VPN 网关

1. 配置 PPTP 客户端。配置如下图所示，用户名为：lan2lan。密码为：93456。远端内网网络地址为：192.168.16.1。远端子网掩码为：255.255.255.0，隧道服务器地址为：200.200.203.250。



2. 配置移动用户

按照以下步骤配置 Windows XP 计算机，使得它能够连接到 PPTP 服务器。

第一步　创建 PPTP 拨号连接：

（1）　进入 Windows XP 的“开始>设置>控制面板”，选择“切换到分类视图”。

（2）　选择“网络和 Internet 连接”。

（3）　选择“建立一个您的工作位置的网络连接”。

（4） 选择“虚拟专用网络连接（V）”，单击“下一步”。

（5） 为连接输入一个名字为 Banch2，单击“下一步”。

（6） 选择“不拨此初始连接”，单击“下一步”。

（7） 输入准备连接的 PPTP 服务器的 IP 地址 200.200.203.250，单击“下一步”。

（8） 单击”完成”。

（9） 双击”Banch2”连接，在 Banch2 连接窗口，单击”属性”。

（10） 选择”安全”属性页面，选择”高级（自定义设置）”，单击”设置”。

（11） 在”数据加密”中选择”可选加密（没有加密也可以连接）”。

（12） 在允许这些协议选中”不加密的密码（PAP）”、”质询握手身份验证协议（CHAP）”、“Microsoft CHAP（MS-CHAP）”、“Microsoft CHAP 版本（MS-CHAP v2）”，单击“确定”。

（13） 选择“网络”属性页面，在 VPN 类型选择“PPTP VPN”。

（14） 确认“Internet 协议（TCP/IP）”被选中。

（15） 单击“确定”，保存所做的修改。

第二步 使用 PPTP 隧道连接到设备 PPTP 服务器：

（1） 确认计算机已经连接到 Internet（可能是拨号连接或者是固定 IP 接入）。

（2） 启动第一步中创建的 Banch2 拨号连接。

（3） 输入的 pptp 用户名 pptpyd 和密码 93456。

（4） 单击“连接”。

（5） 连接成功后，在 MS-DOS 方式下输入 ipconfig，可以看到一个在 PPTP 服务器地址池中的地址，就是 PPTP 服务器分配给本机的 IP 地址。

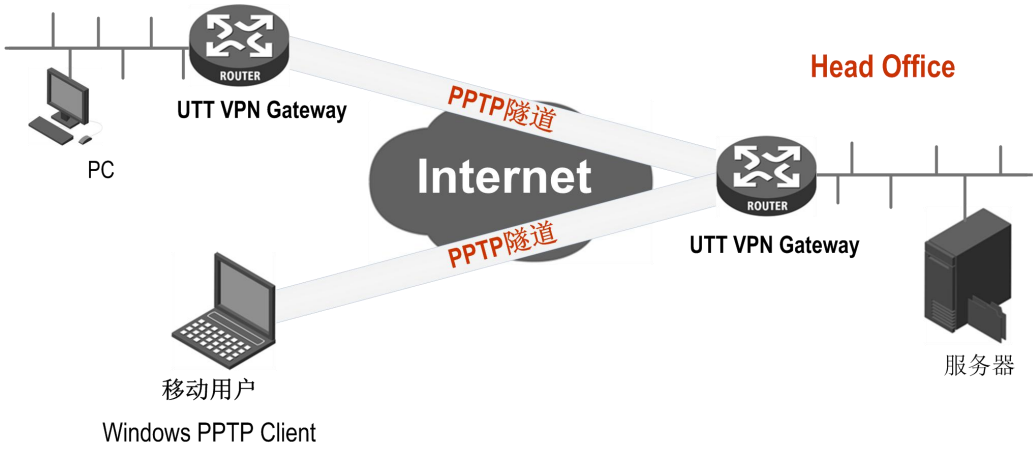
最后，查看连接信息

分别进入相应页面，查看其 PPTP 实例连接信息。如下图所示可以查看 PPTP 实例的用户名、业务类型、会话状态、使用时间、远端内网 IP 地址/掩码等信息。

11.2.5 L2TP 介绍

L2TP（Layer Two Tunneling Protocol），第二层隧道协议：L2TP 是一种虚拟专用网络协议，已成为 IETF 有关二层隧道协议的工业标准。路由器可以工作在 L2TP 客户端和/L2TP 服务器两种模式下。

典型的应用通常是 L2TP 客户端部署在远程分支机构或移动办公用户的个人电脑软件中，他们用来发起 L2TP 隧道。L2TP 服务器部署在企业中心或办公室，用来接收来自 L2TP 客户端的呼叫，当建立起 L2TP 隧道连接后，L2TP 服务器接收来自 L2TP 客户端的 L2TP 数据包，并还原出用户的数据包，然后把还原后的数据包发送到最终用户的电脑设备上。



11.2.6 L2TP 隧道列表

查看相关的 L2TP 隧道信息，如用户名、业务类型、远端内网 IP 地址、会话状态、已建立连接的时间等。

进入页面的方法：“VPN 配置 > PPTP/L2TP”。

提示:

为保证 VPN 网关启用 NAT 后，L2TP 隧道正常连接，L2TP 配置完成之后，系统会自动生成一条 UDP1701 端口 NAT 静态映射（可在“网络配置> 端口映射 >静态映射”页面中查看，名称为“l2tp”）。请不要编辑、删除它们，否则可能造成 L2TP 隧道无法连接和无法传输数据。

11.2.7 L2TP 配置

点击“VPN 配置 > PPTP/L2TP > 隧道列表”页面的“新增”按钮，配置 L2TP 服务端或客户端参数。

配置 L2TP 服务端

路由器作为 L2TP 服务器 ,在 L2TP 服务器上配置 L2TP 用户账号供用户建立 L2TP 隧道使用。

页面参数配置介绍：

选项	描述
工作模式	选择“服务端（拨入）”。
协议类型	选择“L2TP”。
隧道名称	自定义该条隧道的名称，不能重复。
用户类型	选择用户类型，可选项为“LAN 到 LAN”或“移动用户”。 • 移动用户：拨入的 VPN 用户是个人用户，往往由单个计算机拨入，实现 L2TP 隧道远端计算机与本地局域网的通信。 • LAN 到 LAN：拨入的 L2TP 用户是一个网段的用户，往往是通过一个路由器拨入，实现 L2TP 隧道两端局域网的通信。
用户名、密码	自定义客户端拨号时使用的用户名、密码。
远端内网地址	✧ 仅适用于“LAN 到 LAN”用户。 配置 L2TP 隧道对端局域网所使用的 IP 地址（一般可以填 VPN 隧道对端设备的 LAN 口 IP 地址）。
远端内网子网掩码	✧ 仅适用于“LAN 到 LAN”用户。 配置 L2TP 隧道对端局域网所使用的子网掩码。

配置 L2TP 客户端

路由器作为 L2TP 隧道的客户端，发起建立 L2TP 隧道。

页面参数配置介绍：

选项	描述
工作模式	选择“客户端（拨出）”。
协议类型	选择“L2TP”。
隧道名称	该条隧道的名称，与设备中已有的实例名不能重复。
隧道服务器地址	L2TP 服务器的 IP 地址或者域名（一般填 L2TP 隧道对端设备的 WAN

	口 IP 地址或者域名）
用户名、密码	该条隧道拨号时使用的用户名、密码。
密码验证方式	本地客户端将使用 L2TP 协议和对端服务器协商创建 L2TP 隧道时需要验证密码的方式。
远端内网地址	L2TP 隧道对端局域网所使用的 IP 地址段，可填写 L2TP 隧道对端设备的 LAN 口 IP 地址。
远端内网子网掩码	L2TP 隧道对端局域网所使用的子网掩码。

提示:

当 L2TP 隧道两端设备建立连接时，会各用一个虚接口来连接对方。一般情况下， L2TP 服务器会从地址池分配一个 IP 地址作为两个虚接口的路由地址；但是某些 L2TP 服务器并没有配置地址池，此时需要为隧道两端设备的虚接口配置 IP 地址来作为各自的路由地址，即配置对端虚接口 IP 地址、本地虚接口 IP 地址及虚接口子网掩码这三个参数。注意，L2TP 隧道两端设备的虚接口使用同一个子网掩码。

L2TP 全局配置

点击“L2TP 服务器全局配置”标签卡，配置参数。

页面参数配置介绍：

选项	描述
状态	开启或关闭 L2TP 功能。默认为关闭。
密码验证方式	配置建立 L2TP VPN 的密码验证方式，选项有 EITHER（自动和对端设备协商密码验证方式）、PAP、CHAP、NONE。

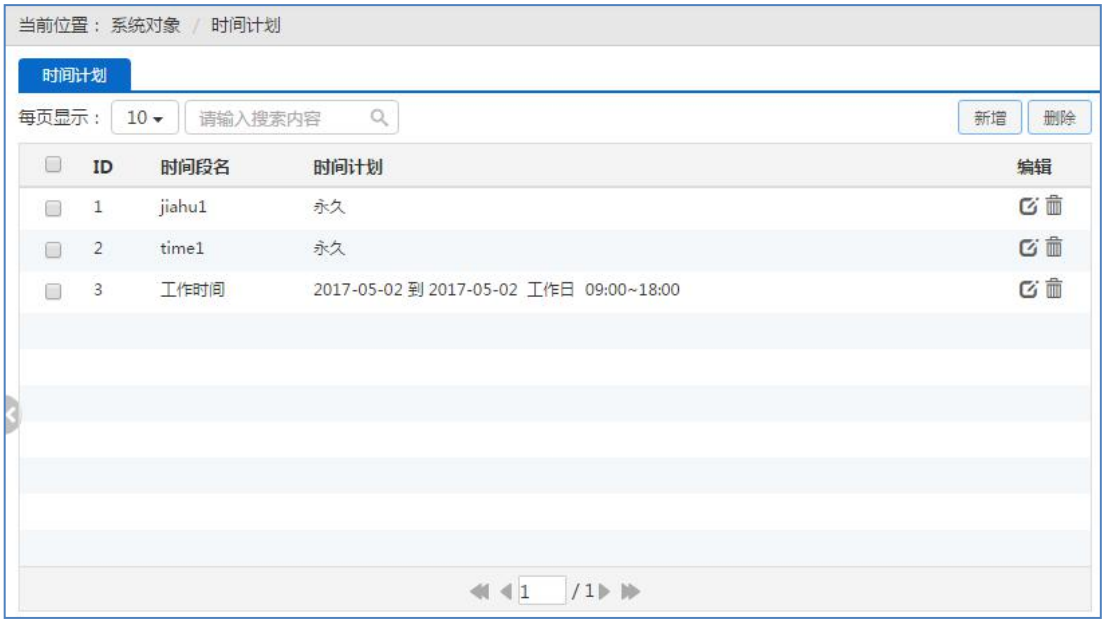
地址池起始地址	配置 L2TP 服务器为 L2TP 客户端分配的起始 IP 地址 ,要确保该地址所属网段与局域网中的任何一个网段不重复。
最大连接数	配置隧道地址池包含的 IP 地址总数量。
服务端 IP 地址	隧道服务端的虚接口 IP 地址，该地址不包含在地址池中，请确认该地址与所配置的地址池在同一网段。
主、备 DNS 服务器	配置主 DNS 服务器的 IP 地址。 当设备被配置为 L2TP 服务端时，可以为 L2TP 客户端分配 DNS 地址，其用于客户端连上服务端之后可以通过服务端线路分配的 DNS 地址浏览网页，可解决用户拨通 VPN 后可以访问服务器内部网却无法打开网页的问题。

第 12 章　系统对象

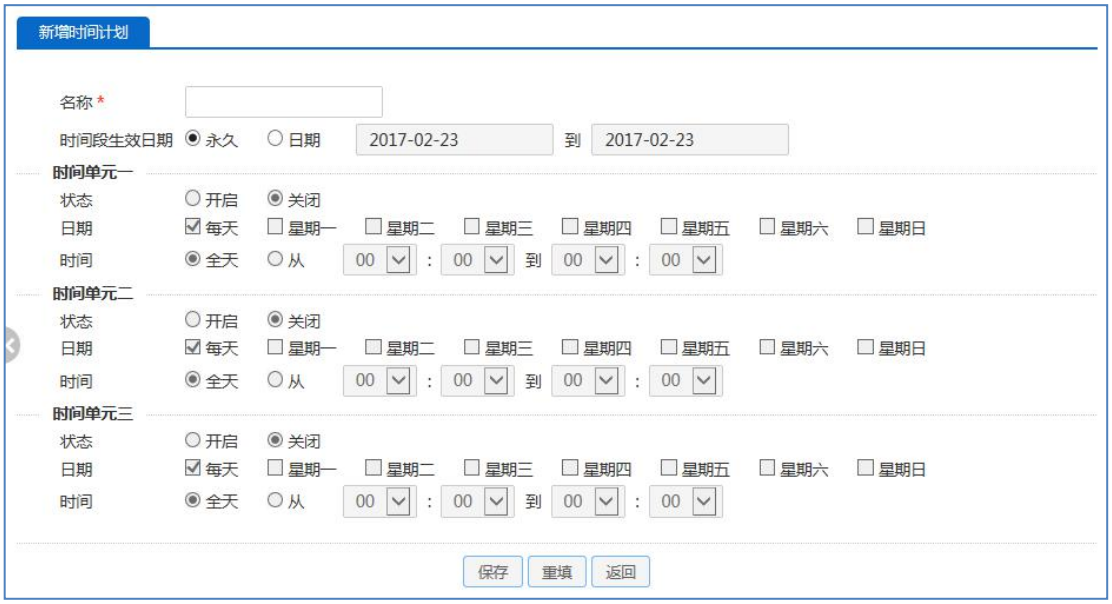
12.1　时间计划

制定时间计划，将多个不连续的时间段组成一个时间组，以方便对用户进行组管理。

进入页面的方法：“系统对象 > 时间计划”。



点击“新增”按钮配置时间计划。



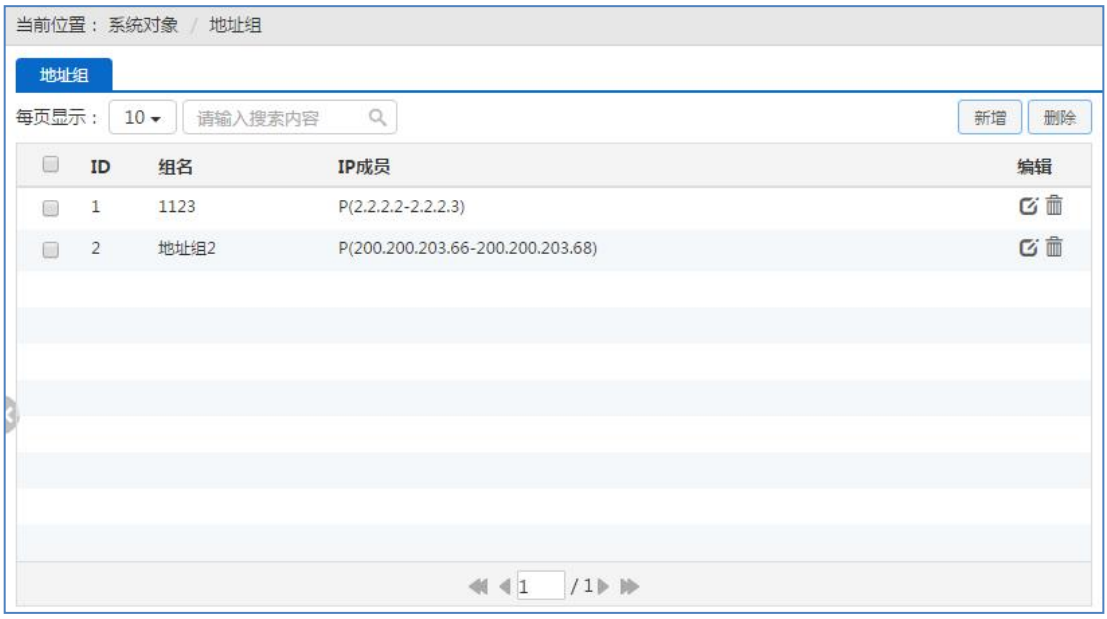
页面参数配置介绍：

选项	描述
名称	输入一个名称来标识一个组。
时间段生效日期	配置时间计划的生效日期。
时间单元	配置时间计划生效的时间段。

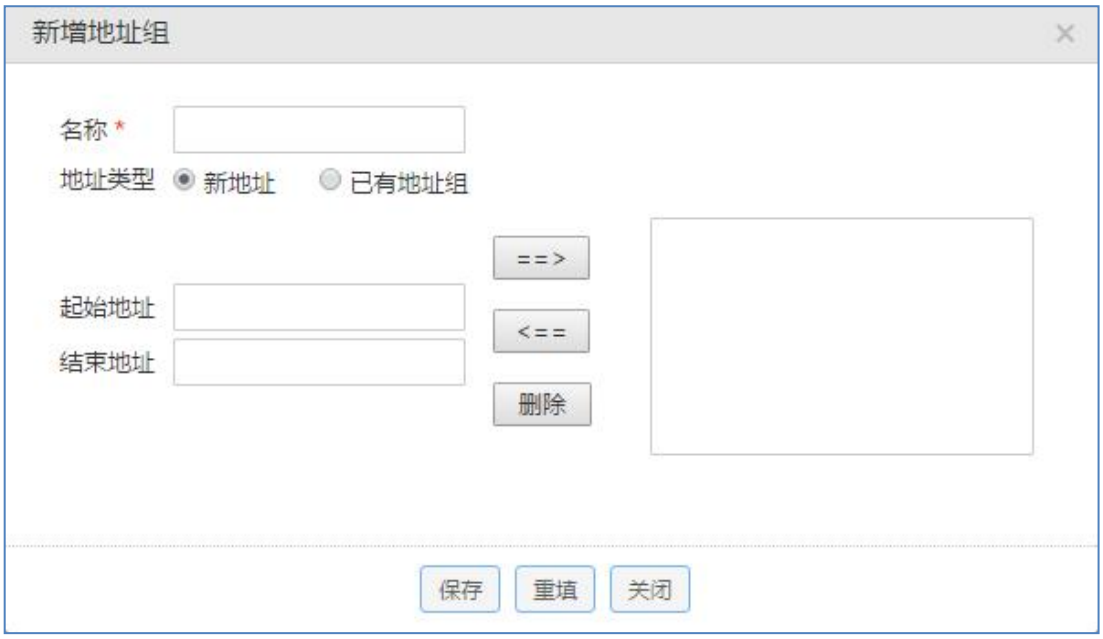
12.2 地址组

配置 IP 地址组，将多个不连续的 IP 段组成一个地址组，便于其他程序引用。地址组可以多层叠加。

进入页面的方法：“系统对象 > 地址组”。



点击“新增”按钮配置地址组。



页面参数配置介绍：

选项	描述
名称	指定一个名称来标识一个组。
地址类型	配置该组可以包含的地址或子组。 勾选“新地址”单选框配置地址池起始 IP 和地址池结束 IP，并单击 ==> 将地址段加入地址组中。注意：起始 IP 必须不大于结束 IP，且不能与已有的地址池范围重叠，当前一个地址池最多可以包含 1024 个 IP 地址。 勾选“已有地址组” 单选框，从左边已有地址组中选择一个地址组，并单击 ==> 将地址子组加入地址组中。

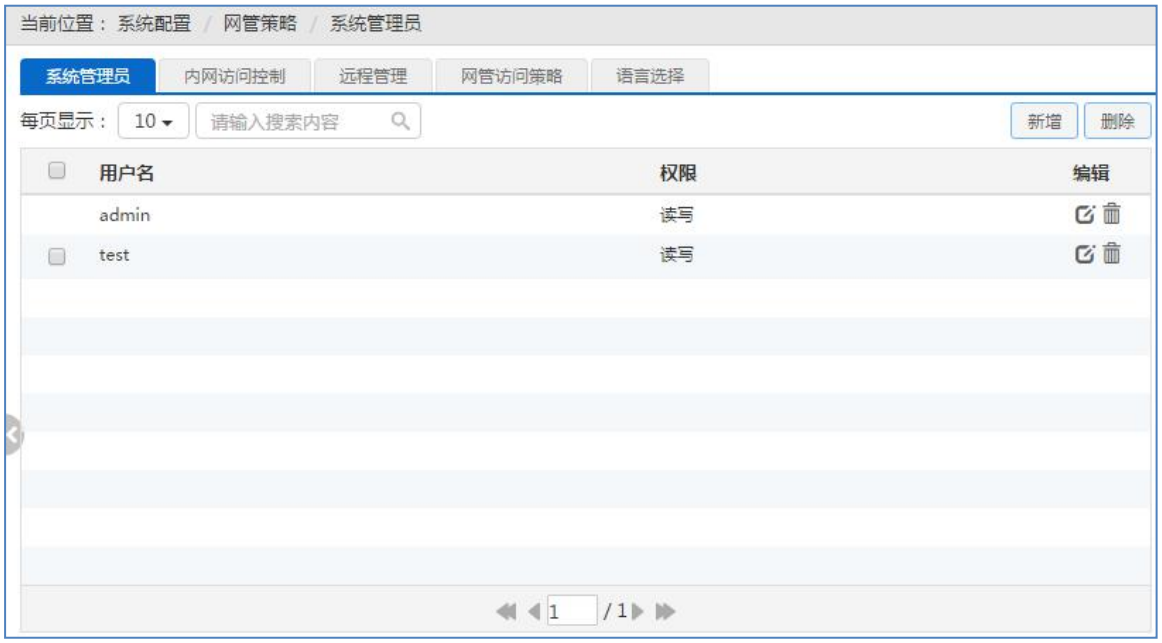
第 13 章　系统配置

13.1　网管策略

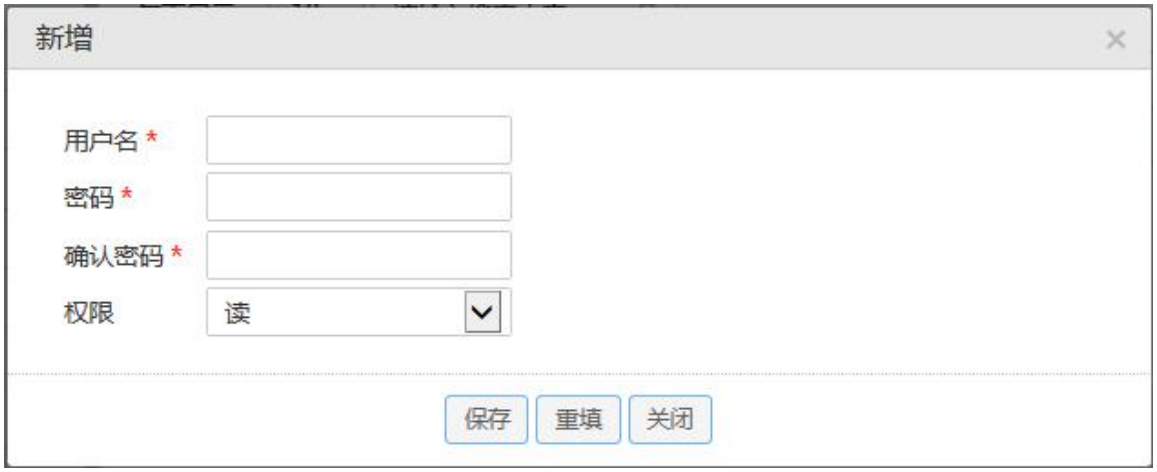
13.1.1 系统管理员

配置不同读写权限的系统管理员。系统管理员可以登录 Web 管理界面配置和维护系统。

进入页面的方法：“系统配置 > 网管策略 > 系统管理员”。



点击“新增”按钮，配置管理员账号。



页面参数配置介绍：

选项	描述
用户名	配置登录路由器的的用户名。
密码	配置登录路由器使用的密码。
确认密码	再次输入登录路由器使用的密码。
权限	配置此帐号的读写权限：读或读写。

注意:

出厂的用户名和密码均为 admin。更改用户名及密码并保存生效后，后续登录时请使用新用户名及新密码。

13.1.2 内网访问控制

为了安全管理网络，可以限制指定用户访问路由器。

进入页面的方法：“系统配置 > 网管策略 > 内网访问控制”。

页面参数配置介绍：

选项	描述
内网访问控制	开启或关闭内网访问控制功能。
选择用户	配置内网中可以访问路由器的用户。默认为全部用户，也可以通过组织架构选择指定的用户，或通过 IP 地址指定用户。

13.1.3 远程管理

开启此功能便于管理员从因特网远程维护与管理路由器。

进入页面的方法：“系统配置 > 网管策略 > 远程管理”。

页面参数配置介绍：

选项	描述
状态	开启或关闭远程管理功能。
端口	配置远程管理端口（默认值为 8081）。开启远程管理功能后，如要从 Internet 通过 WEB 管理设备必须用“IP 地址：端口”（例如 http://218.21.31.3：8081）的方式才能登录设备。若配置了动态域名，也可使用“域名：端口”（例如 13170002.uttcare.com：8081）的方式登录设备。 注意：若把端口修改成 80，在“网络配置 >端口映射 > 静态映射”页面中增加一条 TCP80 端口的映射，此时如需要再次增加内网 WEB 服务器的映射，就会引起冲突。

提示:

1. 设备的 Internet 地址可以从“网络配置 > 外网配置”页面中获知。
2. 如果 WAN1 采用 PPPoE 拨号，其 IP 地址是动态的，可在“网络配置 > 动态域名”中配置 DDNS 功能。
3. 为安全起见，如非必要，请不要启用远程管理功能；在寻求艾泰科技客服工程师服务之前，请事先打开远程管理功能。

应用举例：

某企业路由器地址为为 200.200.210.20，为方便远程管理，希望管理员能对路由器进行远程管理。

可以通过开启远程管理功能实现此需求。在服务端设置远端访问路由器的端口（例如为 8000），并启用远程管理功能，如下图所示：

远程管理员在远程端的浏览器地址栏中输入路由器地址（http://200.200.210.20:8000）登录路由器 Web 界面。

13.1.4 网管访问策略

设置 WEB 登录设备的访问策略。

进入页面的方法："系统配置 > 网管策略 > 网管访问策略"。

页面参数配置介绍：

选项	描述
网管模式	HTTP：信息是明文形式传输，登录速度快。 HTTPS：信息以具有安全性的 ssl 加密传输协议传输，登录更安全。
内网登录端口	配置登录路由器 WEB 管理界面时使用的端口号。
WEB UI 超时	在 WEB 管理界面未进行操作的时间，超时界面将被锁定，再次输入用户名及密码即可正常操作。
管理员最大错误登录次数	管理员登录 WEB 管理界面时允许输错用户名或密码的次数。
管理员超出登录次数惩罚时间	管理员登录 WEB 管理界面时输错用户名或密码的次数超过设定值，帐号将被锁定，帐号锁定期间无法登录设备。在此处设置帐号锁定时间。

13.1.5 语言选择

选择 WEB 管理界面的语言。

进入页面的方法：“系统配置 > 网管策略 > 语言选择”。

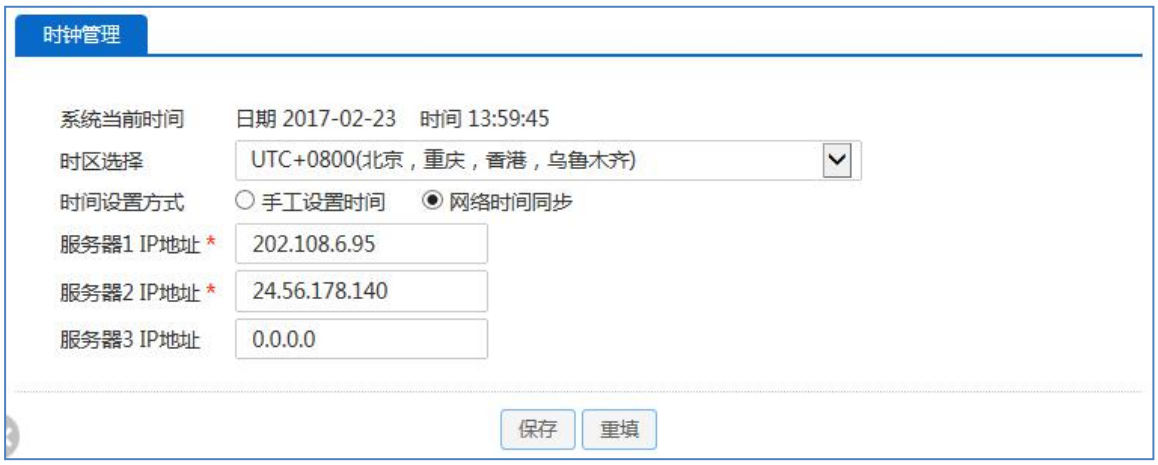
选择语言并点击“保存“按钮，配置立即生效。

13.2 时钟管理

为了保证设备各种涉及到时间的功能正常工作，需要准确地设定设备的时钟，使其与当地标准时间同步。

设备提供“手工设置时间”和“网络时间同步”两种设置系统时间的方式，一般建议选择“网络时间同步”功能，路由器将从互联网上获取标准的时间。若网络时间同步有异常，建议更新 NTP 服务器地址。

进入页面的方法：“系统配置 > 时钟管理”。



页面参数配置介绍：

选项	描述
系统当前时间	显示设备当前的日期和时间信息。
时区选择	选择设备所在地的国际时区，只有选择了正确的时区，网络时间同步功能才能运行正常。

时间设置方式	选择“手工设置时间”手动输入当前的日期和时间；选择“网络时间同步”同步网络时间。
服务器 1~3 IP 地址	时间获取方式采用“网络时间同步”功能后，需设置正确的 ntp 服务器。当设备连接到 Internet 之后，会自动和所设置 NTP 服务器同步时间。系统缺省预设两个 NTP 服务器地址为 202.108.6.95、24.56.178.140，一般情况下不需要修改。若需了解更多 NTP 知识及服务器，可访问 http://www.ntp.org。

提示:

设备的时钟建议设置为网络时间同步，只有系统的时间配置正确，如防火墙等和时间有关系的配置才会正常生效！

13.3 系统维护

13.3.1 系统升级

查看当前系统运行版本信息或升级软件版本。

进入页面的方法：“系统配置 > 系统维护 > 系统升级”。

页面参数配置介绍：

选项	描述
硬件版本	显示设备的硬件版本信息。
软件版本	显示设备的软件版本信息。若系统检测到更新版本，点击“一键升级”按钮升级软件。

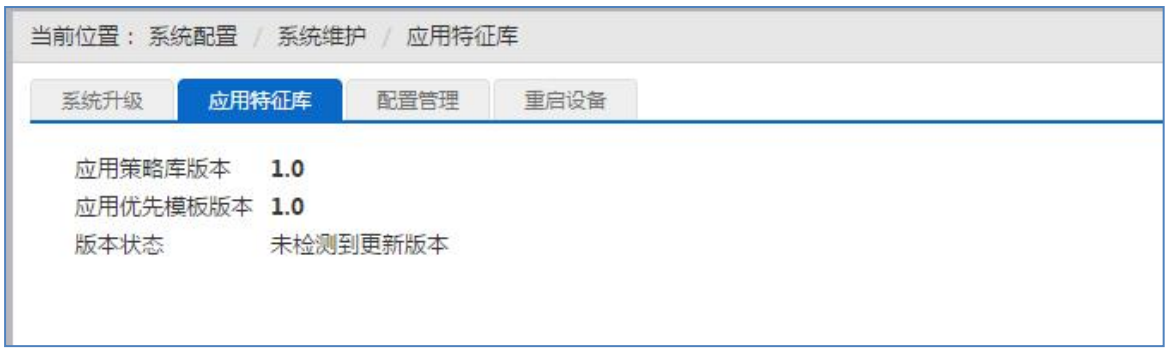
手动升级	手动升级软件版本，需先从上海艾泰科技有限公司官方网站下载最新的软件版本到本地计算机。
升级后重启	软件升级后，系统自动重启。

提示:

1. 请选择合适型号的最新软件；下载的软件适用的硬件版本必须和当前产品的硬件版本一致。
2. 建议升级之前，先到“系统配置 > 系统维护 >配置管理”备份系统当前配置。
3. 强烈建议在设备负载比较轻（用户比较少）的情况下升级。
4. 升级过程不能关闭设备电源，否则将会导致不可预期的错误甚至不可恢复的硬件损坏。
5. 升级完成后软件会自动重启并生效。

13.3.2 应用特征库

显示应用特征库版本信息，目前支持识别两千多种应用，艾泰将持续不断更新应用特征库。当应用无法被识别时，建议更新应用特征库。



13.3.3 配置管理

进入页面的方法：“系统配置 > 系统维护 > 配置管理”。

导出配置

点击“导出”按钮，路由器会将目前所有已保存配置导出为文件。建议在修改配置或升级软件前备份当前的配置信息。

导入配置

单击“选择文件”按钮，选择保存在本地 PC 上的配置文件；或者在文件路径输入框中填写完整的配置文件路径，然后点击“导入”按钮，将路由器恢复到以前备份的配置状态。如果已勾选“导入前恢复出厂设置”复选框，则点击“导入”按钮后，设备将先恢复到出厂配置再加载当前上传的配置文件。

提示:

1. 在加载配置过程中请不要关闭设备电源，以避免不可预期的错误。
2. 导入的配置文件版本与路由器当前配置版本差距过大，将有可能导致路由器现有配置信息丢失，如果有重要的配置信息，请谨慎操作。

恢复出厂配置

点击“恢复出厂配置”按钮，将设备恢复到出厂时的默认值。建议在网络配置错误、组网环境变更等情况时使用此功能。

恢复设备出厂配置将删除所有自定义的配置。强烈建议在恢复出厂配置之前，先备份其配置文件。执行本操作后，设备重启。

13.3.4 重启设备

进入页面的方法：“系统配置 > 系统维护 > 重启设备”。

点击“重启”按钮重启设备。

提示:

重启时，所有的用户将断开与路由器的连接。

13.4 网络工具

13.4.1 Ping

Ping (Packet Internet Grope)，即因特网包探索器，一般用于检测网络通不通。Ping 发送一个 ICMP 回声请求消息给目的地并报告是否收到所希望的 ICMP 回声应答。

进入页面的方法：“系统配置 > 网络工具 > Ping”。

页面参数配置介绍：

选项	描述
IP/域名	配置检测的目的 IP 地址或域名 ,如果设置为域名 ,需要首先配置本机 DNS。点击“Ping”按钮后，路由器将发送 Ping 包检测目的地址是否可以到达，并将检测结果显示在测试结果的方框中。
报文长度	配置 Ping 数据包大小。
Ping 次数	配置 ping 次数。
测试结果	显示 ping 结果。

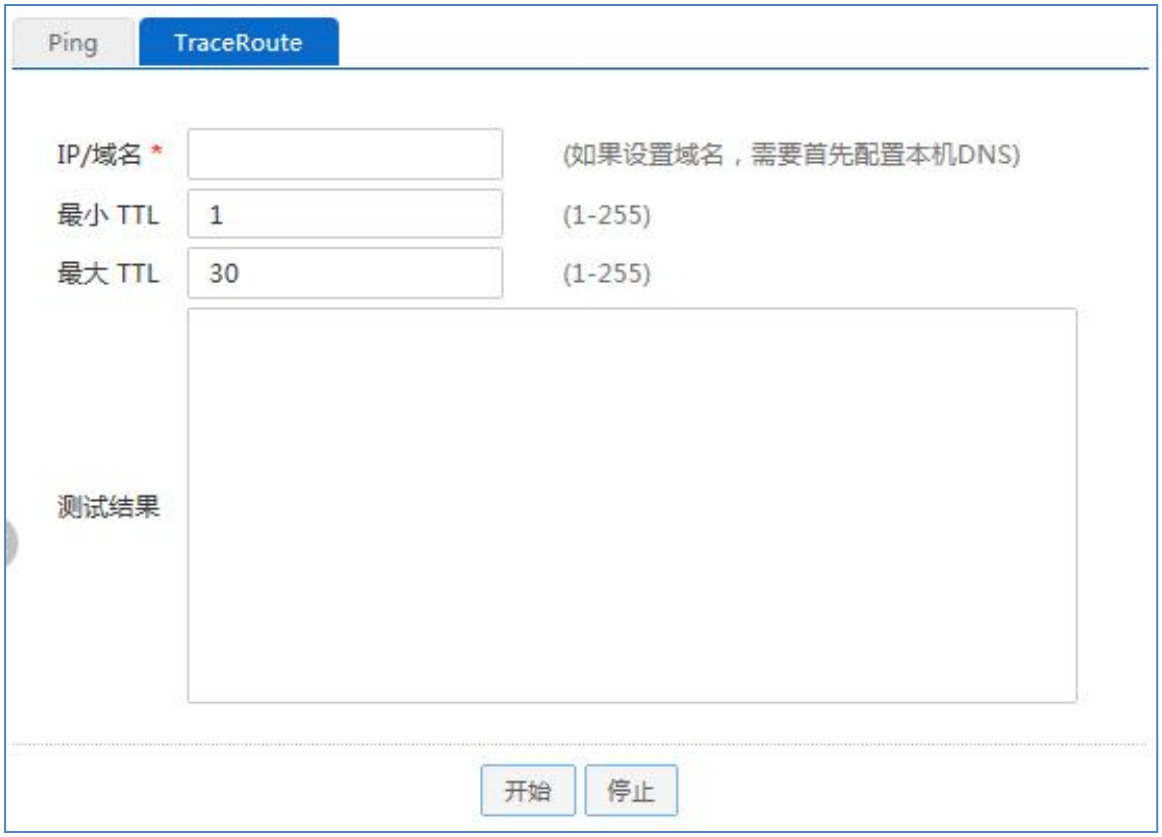
注意:

Ping 的目的地址必须允许响应 Ping 请求。

13.4.2 TraceRoute

Tracert 命令用来诊断当前路由器的网络连接状态。

进入页面的方法：“系统配置 > 网络工具 > TraceRoute”。



页面参数配置介绍：

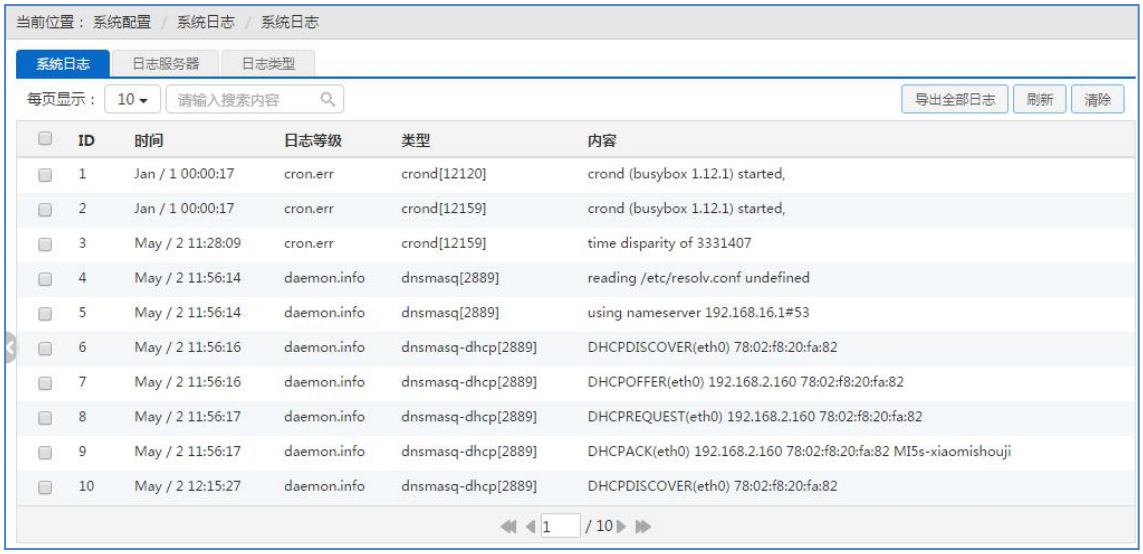
选项	描述
IP/域名	设置目的地址 IP 地址或域名，如果输入地址无效将提示重新输入。如果设置为域名，需要首先配置本机 DNS。点击“开始”按钮后，路由器将发送 tracert 包检测经过哪些路由到达目的地址，并将检测结果显示在测试结果的方框中。
最小 TTL	设置路由跟踪的最小 TTL 值。
最大 TTL	设置路由跟踪的最大 TTL 值。
测试结果	显示 TraceRoute 结果。

13.5 系统日志

查看并管理系统日志记录信息。用户根据需求，查看特定的日志信息，并对日志进行简单的管理，如设置显示日志的类别，删除日志信息等。

13.5.1 系统日志

进入页面的方法：“系统配置 > 系统日志 > 系统日志”。



13.5.2 日志服务器

设备断电后，系统日志会同步删除。建议配置 syslog 服务器保存系统日志。

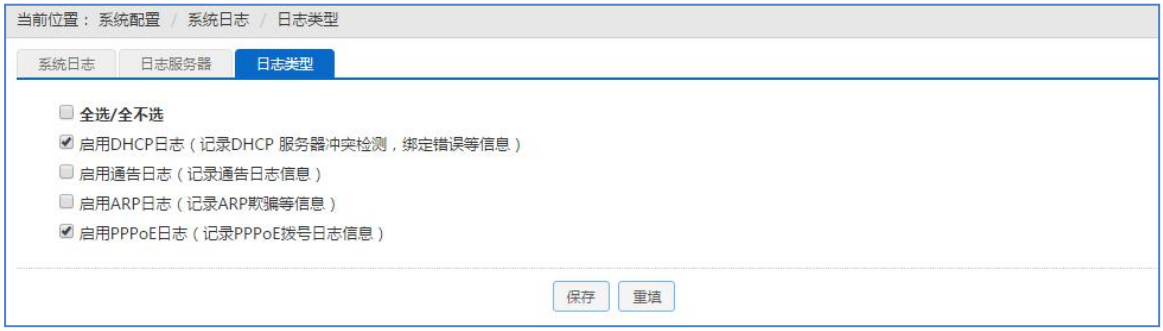
进入页面的方法：“系统配置 > 系统日志 > 日志服务器”。

页面参数配置介绍：

选项	描述
启用 syslog 服务	开启或关闭 syslog 服务功能后。该功能会将设备运行的大量日志记录信息发送给 syslog 服务器，便于管理员分析系统的状况、监视系统的活动。
syslog 服务器的地址（域名）	配置 syslog 服务器的地址，可以是 IP 地址或域名。
syslog 服务器端口	设置 syslog 服务器所开放的服务端口。
syslog 消息类型	设置发送 syslog 的消息类型。
Syslog 消息发送间隔	设置日志信息发送时间间隔。

13.5.3 日志类型

配置日志记录信息类别。进入页面的方法：“系统配置 > 系统日志 > 日志类型”。



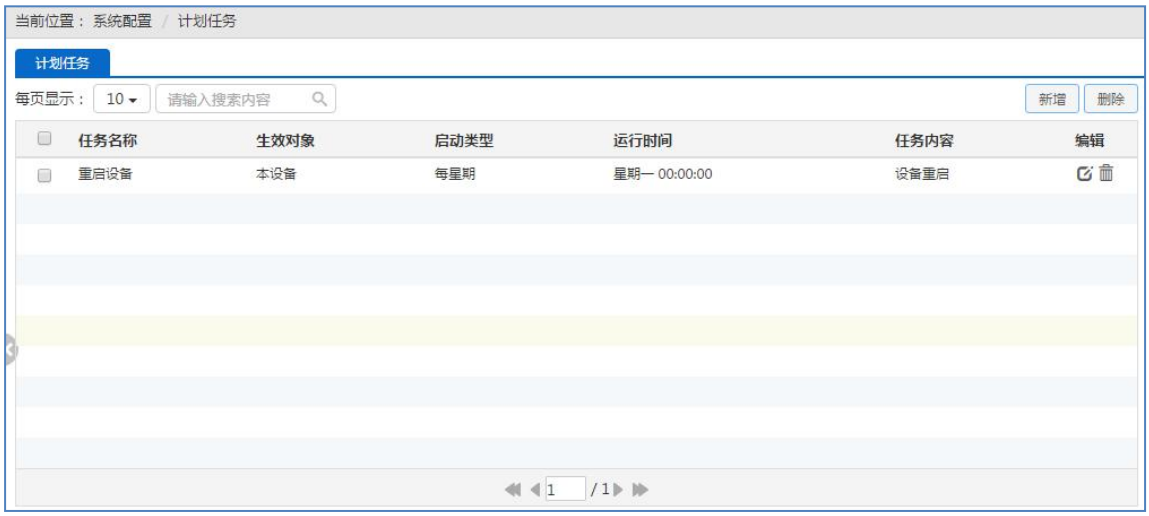
页面参数配置介绍：

选项	描述
启用 DHCP 日志	记录 DHCP 服务器冲突检测，以及 DHCP 分配地址冲突等信息。
启用通告日志	记录通告日志信息。
启用 ARP 日志	记录 ARP 欺骗等信息。
启用 PPPoE 日志	记录 PPPoE 拨号日志信息。

13.6 计划任务

配置周期性任务供路由器自动执行，例如在空闲时间重启设备，有利于释放缓存，回收资源，提高效率。

进入页面的方法：“系统配置 > 计划任务”。



点击“新增”按钮，配置计划任务。

页面参数配置介绍：

选项	描述
任务名称	配置任务名。
任务间隔	选择时间周期，可选项有：每星期、每天、每小时、每分钟。
运行时间	配置计划任务执行的具体时间。
任务内容	配置任务内容，如重启设备等。