网关路由器

操作手册

关于本产品

本手册描述的产品仅供中国大陆地区销售和使用。本产品只能在购买地所在国家或地区享受售后服务及维保方案。

关于本手册

本手册仅作为相关产品的指导说明，可能与实际产品存在差异，请以实物为准。因产品版本升级或其他需要，海康威视可能对本手册进行更新，如您需要最新版手册，请您登录海康威视官网查阅（www.hikvision.com）。

海康威视建议您在专业人员的指导下使用本手册。

商标声明

- HIKVISION 海康威视 为海康威视的注册商标。
- 本手册涉及的其他商标由其所有人各自拥有。

责任声明

- 在法律允许的最大范围内，本手册以及所描述的产品（包含其硬件、软件、固件等）均“按照现状”提供，可能存在瑕疵或错误。海康威视不提供任何形式的明示或默示保证，包括但不限于适销性、质量满意度、适合特定目的等保证；亦不对使用本手册或使用海康威视产品导致的任何特殊、附带、偶然或间接的损害进行赔偿，包括但不限于商业利润损失、系统故障、数据或文档丢失产生的损失。
- 您知悉互联网的开放性特点，您将产品接入互联网可能存在网络攻击、黑客攻击、病毒感染等风险，海康威视不对因此造成的产品工作异常、信息泄露等问题承担责任，但海康威视将及时为您提供产品相关技术支持。
- 使用本产品时，请您严格遵循适用的法律法规，避免侵犯第三方权利，包括但不限于公开权、知识产权、数据权利或其他隐私权。您亦不得将本产品用于大规模杀伤性武器、生化武器、核爆炸或任何不安全的核能利用或侵犯人权的用途。
- 如本手册内容与适用的法律相冲突，则以法律规定为准。

前　言

本节内容的目的是确保用户通过本手册能够正确使用产品，以避免操作中的危险或财产损失。在使用此产品之前，请认真阅读产品手册并妥善保存以备日后参考。

概述

本说明书适用于以下型号的 HIKVISION 网关路由器：DS-3WS256-E、DS-3WS256-S，文中若无特殊说明，产品图片以 DS-3WS256-E 为例。

符号约定

对于文档中出现的符号，说明如下所示。

符号	说明
 说明	说明类文字，表示对正文的补充和解释。
 注意	注意类文字，表示提醒用户一些重要的操作或者防范潜在的伤害和财产损失危险。
 警告	警告类文字，表示有潜在风险，如果不加避免，有可能造成伤害事故、设备损坏或业务中断。

安全使用注意事项

 警告

- 设备安装使用过程中，必须严格遵守国家和使用地区的各项电气安全规定。
- 在接线、拆装等操作时请一定要将设备电源断开，切勿带电操作。

 注意

- 设备接入互联网可能面临网络安全问题，请您加强个人信息及数据安全的保护。当您发现设备可能存在网络安全隐患时，请及时与我们联系。
- 请您理解，您有责任合理配置所有的密码及其他相关产品安全设置，并妥善保管好您的用户名和密码。

文档版本 01 (2020-07-20)

第一次正式发布。

目 录

第1章 快速上网

1.1 登录路由器管理页面

如果您是首次使用路由器或已将路由器恢复出厂设置，请参考相关路由器的安装手册。否则，请参考下文。

步骤1 用网线将管理电脑接到路由器 LAN 口（或路由器 LAN 口连接的交换机）；

步骤2 设置电脑的本地连接为“自动获得 IP 地址，自动获得 DNS 服务器地址”；

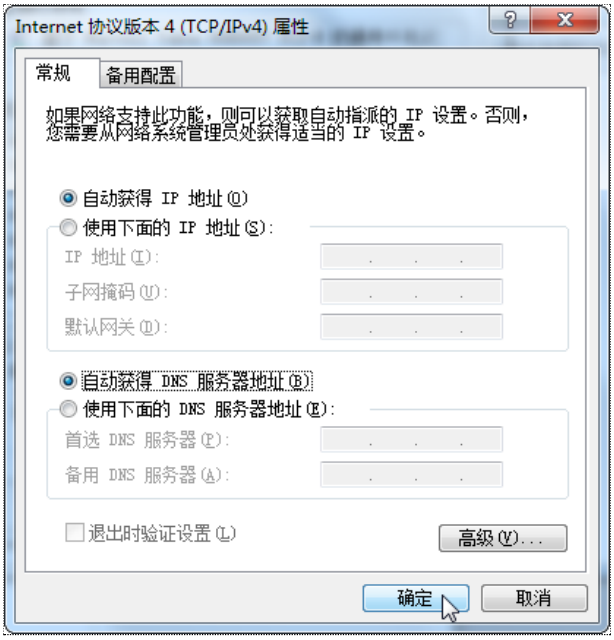


图1-1 本地连接

步骤3 打开电脑上的浏览器（如 IE），访问路由器的管理地址（默认为“192.168.0.252”），进入路由器的登录页面；

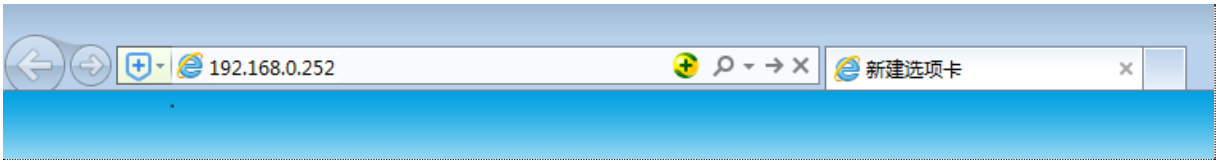


图1-2 浏览器

步骤4 设置登录密码，点击 登录 。

图1-3 登录页面

说明

若未出现上述页面，请查看附录 A-常见问题解答的问 1。

成功登录到路由器的管理页面，您可以设置路由器。

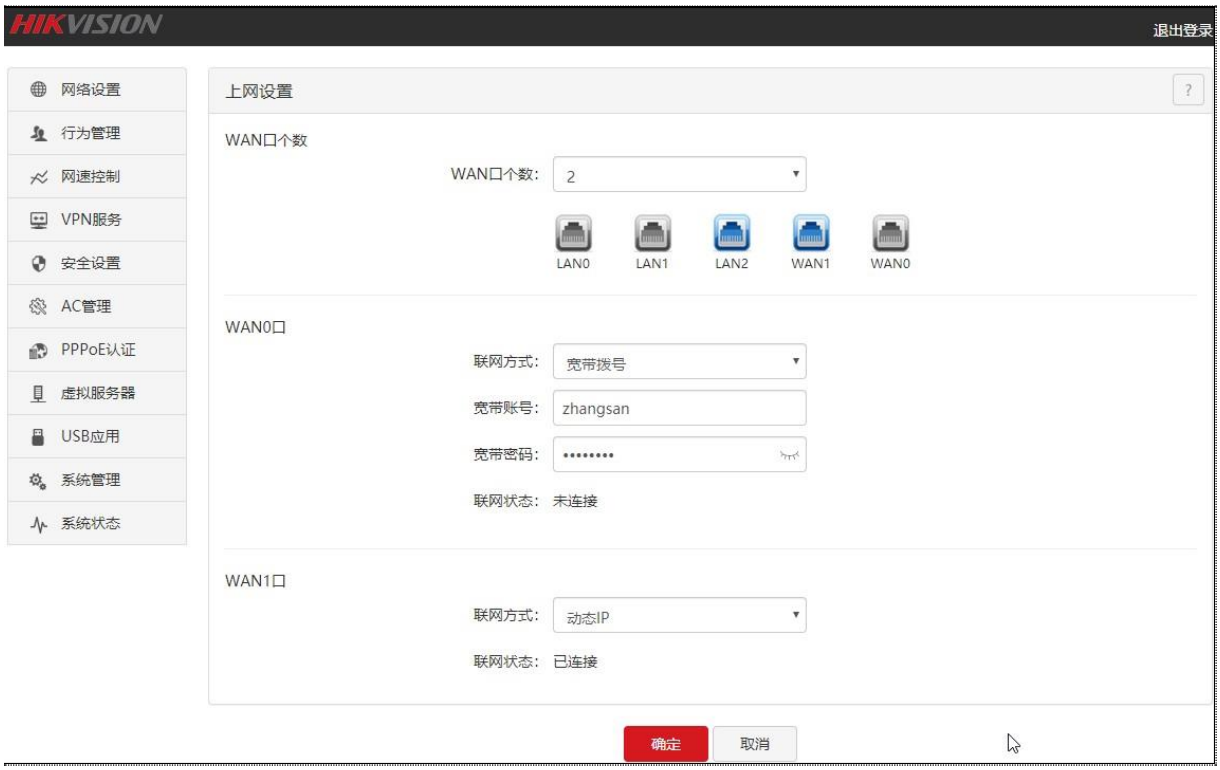


图1-4 路由器的管理页面

1.2 设置路由器

进行上网设置，实现局域网内的多台计算机共享您办理的宽带服务上网。可以先根据下表说明或咨询您的 ISP，确定路由器的联网方式，再进行上网设置。

表1-1 上网方式参数说明

联网方式	特征
宽带拨号	ISP 提供了宽带账号和宽带密码。
动态 IP	ISP 未提供任何上网信息，或说明了联网方式为“动态 IP”。
静态 IP	ISP 提供了一组固定 IP 地址信息，如 IP 地址，子网掩码、默认网关、DNS 等。

注意

- 路由器默认提供了 2 个 WAN 口，下文以 WAN0 设置为例，WAN1 口的设置与 WAN0 方法类似。
- 路由器 WAN0 默认的联网方式为宽带拨号，WAN1 默认的联网方式为动态 IP。
- 各上网设置参数均由 ISP（互联网服务提供商）提供，如不清楚，请咨询您的 ISP。

1.2.1 宽带拨号

点击「网络设置」>「上网设置」，参照下图进行设置。

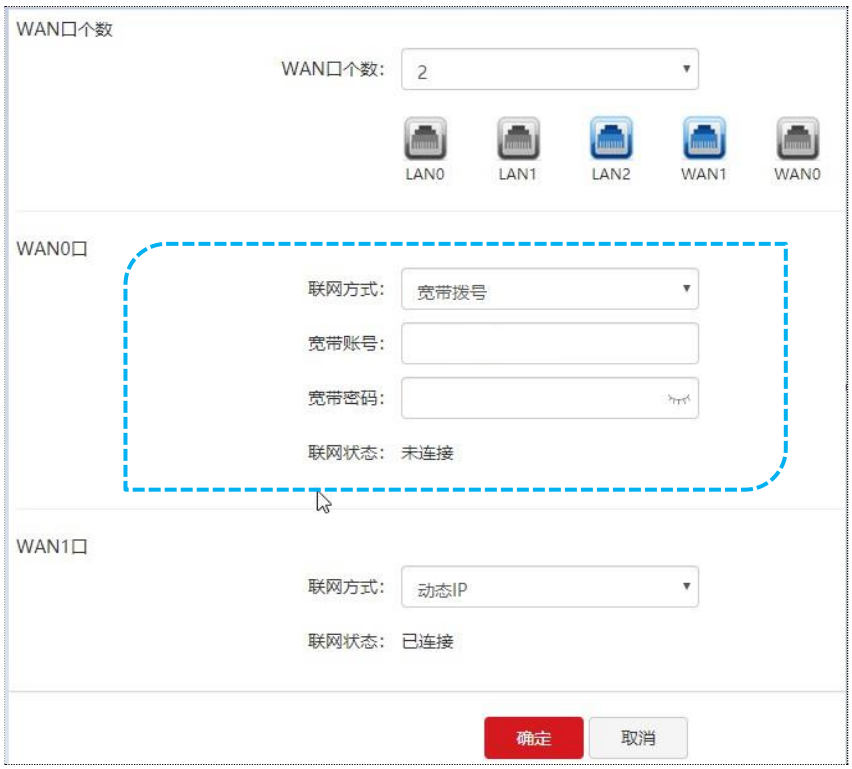


图1-5 宽带拨号

设置步骤：

步骤1 联网方式：选择“宽带拨号”；

步骤2 宽带账号：输入 ISP 提供的宽带账号；

步骤3 宽带密码：输入 ISP 提供的宽带密码；

步骤4 点击 确定 。

稍等片刻，当联网状态显示“认证成功”时，您可以尝试上网了。如果您仍然不能上网，可以进入「网络设置」>「WAN 口参数」页面，尝试修改 WAN 口参数解决问题。

1.2.2 动态 IP

点击「网络设置」>「上网设置」，参照下图进行设置。

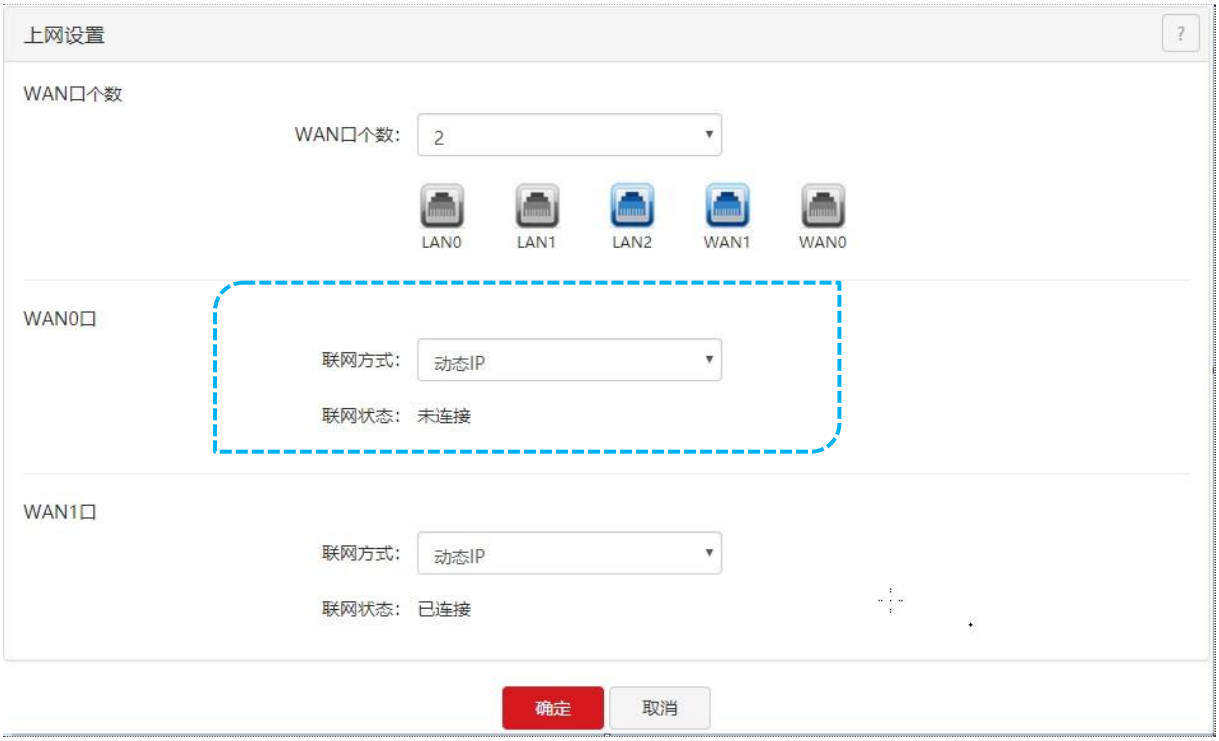


图1-6 动态 IP

设置步骤：

步骤1 联网方式：选择“动态 IP”；

步骤2 点击 确定 。

稍等片刻，当联网状态显示“已连接”时，您可以尝试上网了。如果您仍然不能上网，可以进入「网络设置」>「WAN 口参数」页面，尝试修改 WAN 口参数解决问题。

1.2.3 静态 IP

点击「网络设置」>「上网设置」，参照下图进行设置。

图1-7 静态 IP

设置步骤：

步骤1 联网方式：选择“静态 IP”；

步骤2 IP 地址、子网掩码、网关地址、主/次 DNS：输入 ISP 提供的固定 IP 地址相关信息；

步骤3 点击 确定 。

稍等片刻，当联网状态显示“已连接”时，您可以尝试上网了。如果您仍然不能上网，可以进入「网络设置」>「WAN 口参数」页面，尝试修改 WAN 口参数解决问题。

第2章 登录路由器

2.1 登录路由器管理页面

方法请参考**第一章 快速上网**的“1.1 登录路由器管理页面”。

2.2 退出登录

您登录到路由器的管理页面后，如果在 5 分钟内没有任何操作，系统将自动退出登录。此外，在管理页面上，单击右上角的 退出登录 ，也可以安全地退出管理页面。

图2-1 路由器的管理页面

2.2 管理页面布局介绍

管理页面共分为：一级导航栏、二级导航栏和配置区三部分。如下图所示。

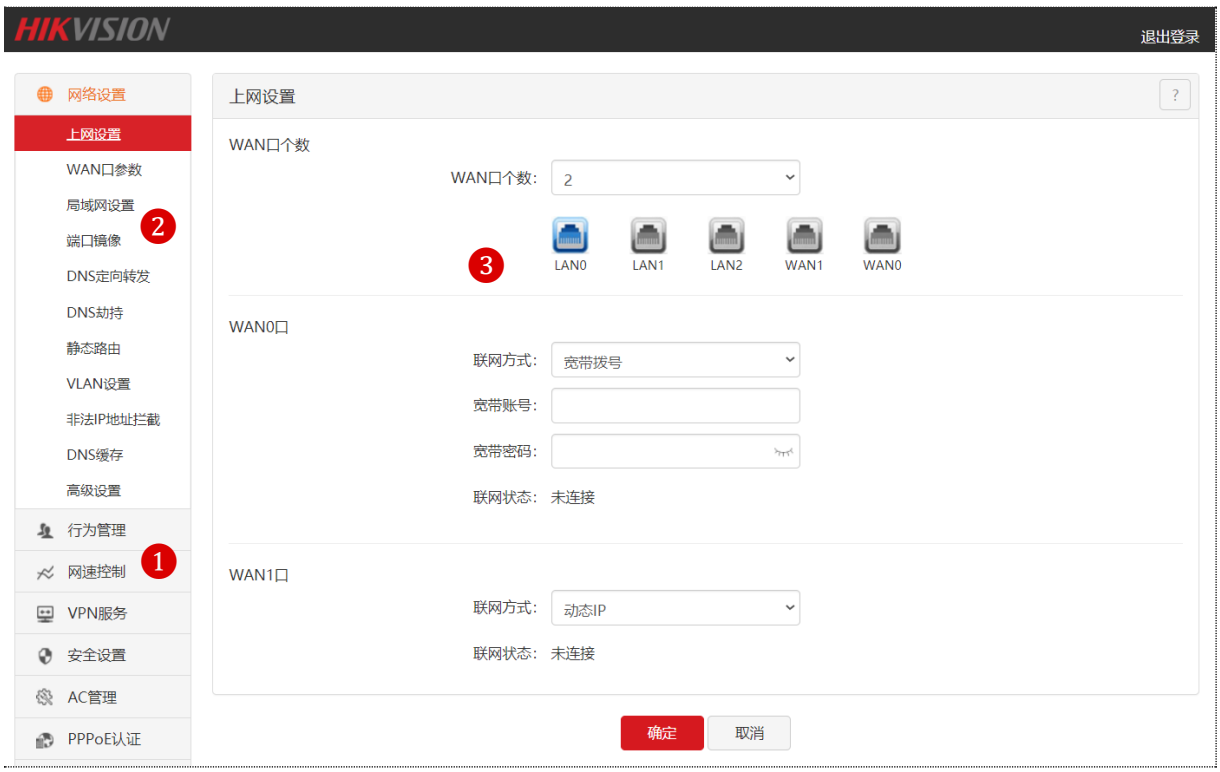


图2-2 管理页面布局

表2-1 参数说明

序号	名称	说明
1	一级导航栏	以导航树的形式组织路由器的功能菜单。用户在导航栏中可以方便地选择功能菜单，选择结果显示在配置区。
2	二级导航栏	
3	配置栏	用户进行配置或查看配置的区域。

2.3 管理页面常用按钮

以下是管理页面中常用按钮的功能介绍。

表2-2 常用按钮

常用元素	说明
确定	用于保存当前页面配置，并使配置生效。
取消	用于取消当前页面未保存的配置，并恢复到修改前的配置。
?	在配置区的右上角。点击可查看对应页面的设置帮助信息。

第3章 网络设置

路由器的「网络设置」模块包括：上网设置、WAN 口参数、局域网设置、端口镜像、DNS 定向转发、DNS 劫持、静态路由、VLAN 设置、非法 IP 地址拦截、DNS 缓存、高级设置。

3.1 上网设置

通过上网设置，可以实现局域网内的多台计算机共享您办理的宽带服务上网。点击「网络设置」>「上网设置」进入页面。

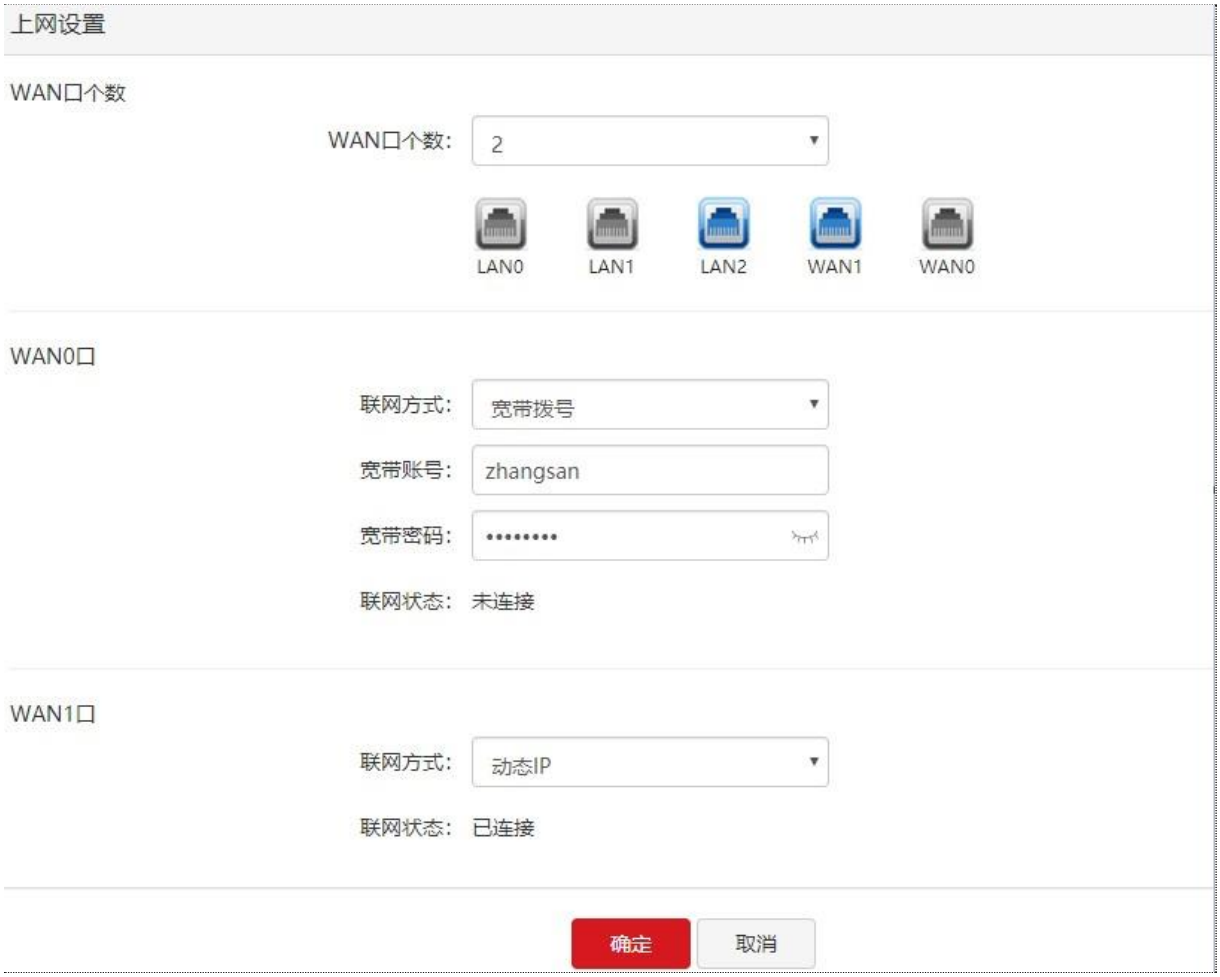
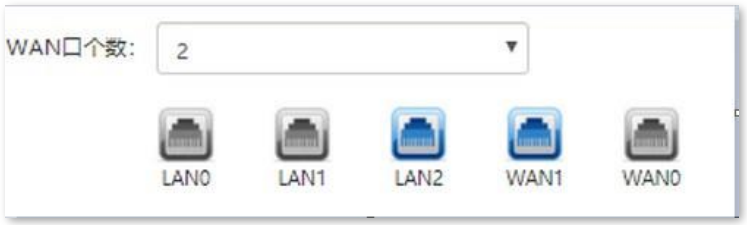


图3-1 上网设置

表3-1 上网设置参数说明

标题项	说明
WAN 口个数	路由器 WAN 口的个数，默认的 WAN 口个数为 2。可以根据需要修改 WAN 口个数，最多支持 4 个 WAN 口。 修改 WAN 口个数后，RJ45 口状态图也会随之改变。如下图。   ：表示接口连接正常。  ：表示接口未连接设备或连接异常。
联网方式	路由器的联网方式，支持宽带拨号、动态 IP、静态 IP。 ● 宽带拨号：ISP（互联网服务提供商）提供了宽带账号和密码。用户不使用路由器时，需要在在电脑上拨号上网。 ● 动态 IP：ISP 没有提供任何上网信息。用户不使用路由器时，电脑只需要接上宽带网线即可上网。 ● 静态 IP：用户在 ISP 办理宽带业务时，ISP 提供了固定的 IP 地址信息。用户不使用路由器时，需要在电脑上设置静态 IP 地址上网。
宽带账号	联网方式为“静态 IP”时才需设置。可以在办理宽带的业务单据上查到，如果没有，请咨询您的 ISP。 如果 ISP 没有提供两个 DNS 地址，“次 DNS”可以不填。
宽带密码	
IP 地址	
子网掩码	
网关地址	
主 DNS	
次 DNS	

标题项	说明
联网状态	显示路由器 WAN 口的连接状态。 ● 已连接：路由器 WAN 口已插网线，并已经获得 IP 地址信息。 ● 认证成功：路由器拨号成功，并已经获得 IP 地址信息。 ● 连接中...：路由器正在连接到上级网络设备。 ● 未连接：未连接或连接失败，请检查网线连接状态、上网信息设置或咨询相应的 ISP。 如果显示其他状态信息，请根据联网状态提示信息采取相应措施。

3.2 WAN 口参数

如果您已经正确完成上网设置，但接在路由器下的计算机还是不能联网，或者联网出现问题，可以尝试修改 WAN 口参数解决。

进入页面的方法：点击「网络设置」>「WAN 口参数」。

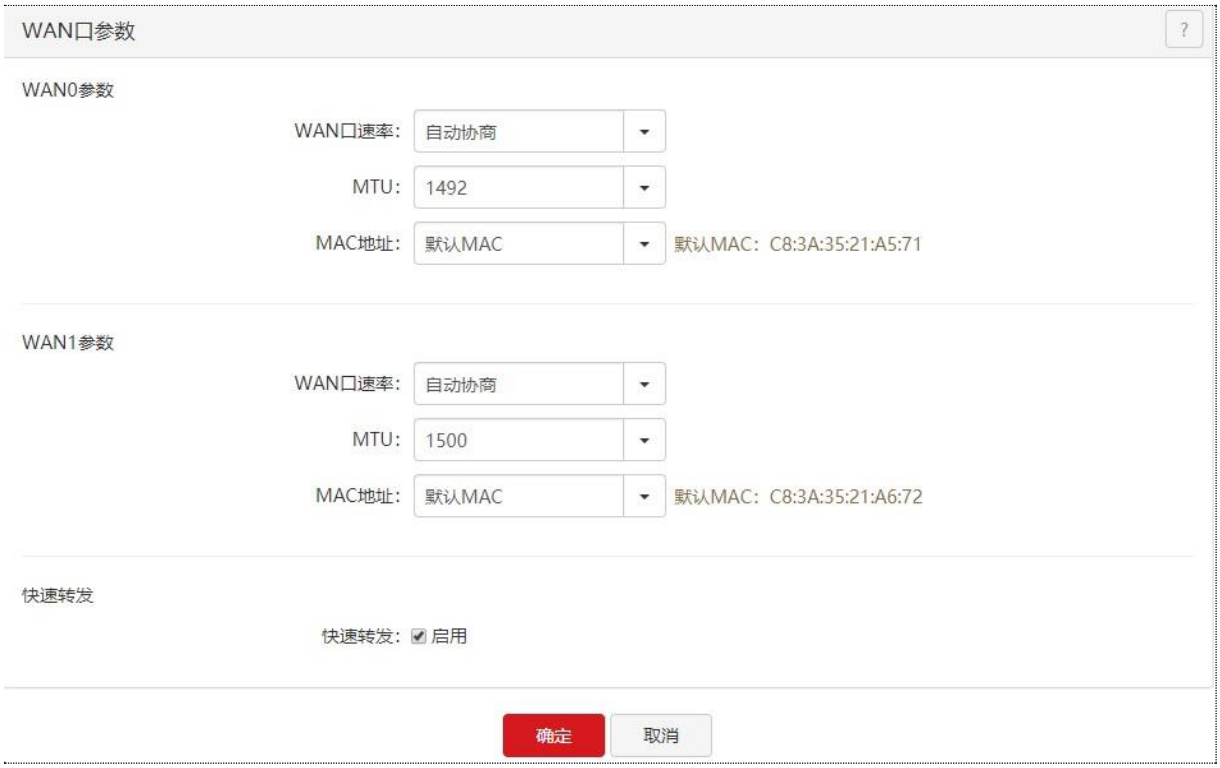


图3-2 WAN 口参数

3.2.2 WAN 口速率

如果路由器 WAN 口已正确连接网线，且网线工作正常，但对应 WAN 口的 Link 灯不亮；或者插上网线后 Link 灯要等待一会儿（5 秒以上）才亮。此时，可以将路由器的 WAN 口速率调为 10M 半双工或 10M 全双工尝试解决问题。

否则，建议 WAN 口速率保持默认设置“自动协商”。

3.2.3 MTU

MTU，即“最大传输单元”，是网络设备传输的最大数据包。联网方式为“宽带拨号”时，默认 MTU 值为 1492。联网方式为“动态 IP”或“静态 IP”时，默认 MTU 值为 1500。一般情况下，建议保持 MTU 值为默认设置，除非您遇到以下情况：

- 无法访问某些网站、或打不开安全网站（如网银、支付宝登录页面）。
- 无法收发邮件、无法访问 FTP 和 POP 等服务器等。

此时，可以尝试从最大值 1500 逐渐减少 MTU 值（建议修改范围 1400~1500），直到问题消失。

表3-2 MTU 参数说明

MTU 值	应用
1500	非宽带拨号、非 VPN 拨号环境下最常用的设置。
1492	用于宽带拨号拨号环境。
1472	使用 ping 的最大值 (大于此值的包会被分解)。
1468	用于一些 DHCP（动态 IP）环境。
1436	用于 VPN 或 PPTP 环境。

3.2.4 MAC 地址

当上网设置完毕后，如果路由器还是无法联网，有可能是 ISP 将上网账号信息与某一 MAC 地址（物理地址）绑定了。

此时，您可以尝试通过 MAC 地址克隆（方法 1 或方法 2）解决该问题。

注意

请克隆之前能正常上网的电脑 MAC 地址或能正常上网的路由器 WAN 口 MAC 地址。

方法 1:

步骤1 使用之前能正常上网的电脑连接路由器；

步骤2 登录路由器管理页面，点击「网络设置」>「WAN 口参数」页面，在对应 WAN 口的 MAC 地址选项框选择“克隆本机 MAC”；

步骤3 点击页面底端的 确定 。

图3-3 克隆本机 MAC 地址

方法 2:

步骤1 记录正确的 MAC 地址。

步骤2 登录路由器管理页面，点击「网络设置」>「WAN 口参数」页面，在对应 WAN 口的 MAC 地址选项框选择“手动输入”，然后填入正确的 MAC 地址（可能是“直连宽带网线时能成功联网的电脑的 MAC 地址”或“之前能正常上网的路由器的 WAN 口 MAC 地址”）。

步骤3 点击页面底端的 确定 。

图3-4 手动输入 MAC 地址

注意

如果需要将 MAC 地址恢复为出厂 MAC，请点击「网络设置」>「WAN 口参数」，在对应 WAN 口的 MAC 地址选项框选择“默认 MAC”，点击 确定 。

3.2.5 快速转发

路由器的“快速转发”功能，即快速 NAT 转发功能。NAT（Network Address Translation）是网络地址转换，本地地址的主机在和外界通信时，都要将 NAT 路由器上的本地地址转换成全球 IP 地址，才能和互联网通信。

启用“快速转发”功能后路由器 NAT 转发性能会提高。

3.3 局域网设置

点击「网络设置」>「局域网设置」进入页面，在这里，您可以设置路由器的 LAN 口 IP 地址等参数。

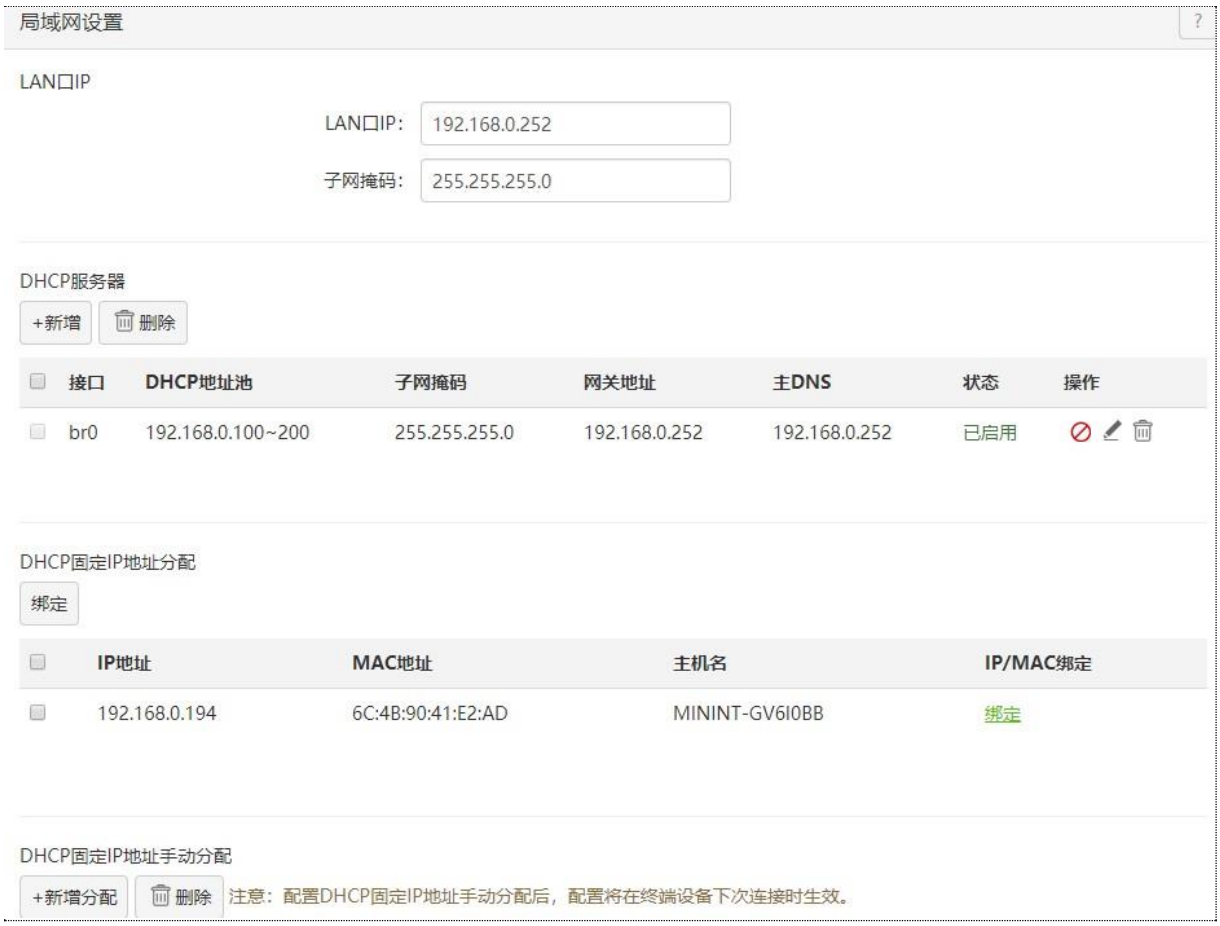


图3-5 局域网设置

3.3.2 LAN 口 IP

LAN 口 IP 是路由器对局域网的 IP 地址，也是路由器的管理 IP 地址。路由器默认的 LAN 口 IP 为 192.168.0.252，子网掩码为 255.255.255.0。

图3-6 LAN 口 IP

一般情况下，您无需修改 LAN 口设置，除非遇到 IP 地址冲突，如：路由器获得的 WAN 口 IP 和其 LAN 口 IP 处于同一网段；局域网内，有其它设备的 IP 地址也为 192.168.0.252。

修改 LAN 口 IP 后，系统出现如下提示。

图3-7 温馨提示

进度条走完后，系统将自动重新登录。如果没有，请确认电脑的本地连接 IP 地址设置为“自动获得”，并修复一下电脑的 IP 地址，之后使用新的 LAN 口 IP 地址重新尝试。

注意

如果新的 LAN 口 IP 与原 LAN 口 IP 不在同一网段，系统将自动匹配修改 DHCP 地址池，使其和新的 LAN 口 IP 在同一网段。

3.3.3 DHCP 服务器

DHCP 服务器能自动给局域网计算机分配 IP 地址、子网掩码、网关、DNS 等上网信息。如果关闭该功能，需要在局域网计算机上手动配置 IP 地址信息才能实现上网。如无特殊情况，请保持 DHCP 服务器为开启状态。

默认情况下，路由器已存在 1 个接口名称为“br0”的 DHCP 服务器。如下图所示。

图3-8 DHCP 服务器

表3-3 DHCP 服务器参数说明

标题项	说明
接口	已设置 DHCP 服务器的接口，默认存在接口为 br0 的 DHCP 服务器规则，接入未划分 VLAN 网络的用户会获取本 DHCP 服务器下发的 IP 地址。
DHCP 服务池	DHCP 服务器可分配的 IP 地址范围，br0 接口的起始 IP 地址默认为 192.168.0.100，结束 IP 地址默认为 192.168.0.200。 本路由器的“起始 IP 地址”和“结束 IP 地址”可以不在一个网段。
子网掩码	DHCP 服务器分配给局域网计算机的子网掩码，固定为该接口的子网掩码，不可编辑。
网关地址	DHCP 服务器分配给局域网计算机的默认网关 IP 地址，固定为该接口的 IP 地址，不可编辑。
主 DNS	DHCP 服务器分配给局域网计算机的首选 DNS 服务器 IP 地址。路由器支持 DNS 代理功能，故主 DNS 默认为路由器的 LAN 口 IP 地址。 一般情况下，建议保持默认设置。如需修改，为了使局域网计算机能够正常上网，请务必确保修改的主 DNS 是正确的 DNS 服务器或 DNS 代理的 IP 地址
次 DNS	DHCP 服务器分配给计算机的备用 DNS 服务器 IP 地址。不填表示 DHCP 服务器不分配此项。
租约时间	DHCP 服务器所分配给计算机的 IP 地址的有效时间。当地址到期后： ● 如果计算机仍连接在路由器上，计算机将自动续约，继续占用该 IP 地址。 ● 如果计算机未连接（关机、网线已拔掉、无线已断开等）到路由器，路由器将释放该 IP。以后若有其它计算机请求 IP 地址信息，路由器可将该 IP 分配给其它计算机。 ● 如无特殊需要，建议保持默认设置。

新增 DHCP 服务器

步骤1 添加 VLAN 接口；

1. 点击「网络设置」>「VLAN 设置」；
2. 点击 +新增 ；

图3-9 VLAN 设置

3. 在弹出的窗口设置 VLAN 规则；

4. 点击 确定 ；

图3-10 添加 VLAN 规则

返回“VLAN 设置”页面点击**重启设备**，路由器重启后生效。

步骤2 为接口设置 DHCP 服务器；

1. 点击「网络设置」>「局域网设置」，找到“DHCP 服务器”模块；

2. 点击 +新增 ；

图3-11 新增 DHCP 服务器

3. 在弹出的窗口设置 DHCP 服务器信息。

– 接口：点击下拉菜单，选择已在“VLAN”设置页面添加的 VLAN，如“caiwubu”。

- 起始/结束 IP 地址：设置 DHCP 服务器可分配给客户端的 IP 地址范围，IP 地址网段须和“网关地址”一致，如“192.168.5.2~192.168.5.100”。
- 主 DNS：可设置为“网关地址”或正确的 DNS 信息，如“192.168.5.1”。
- 点击 确定 。

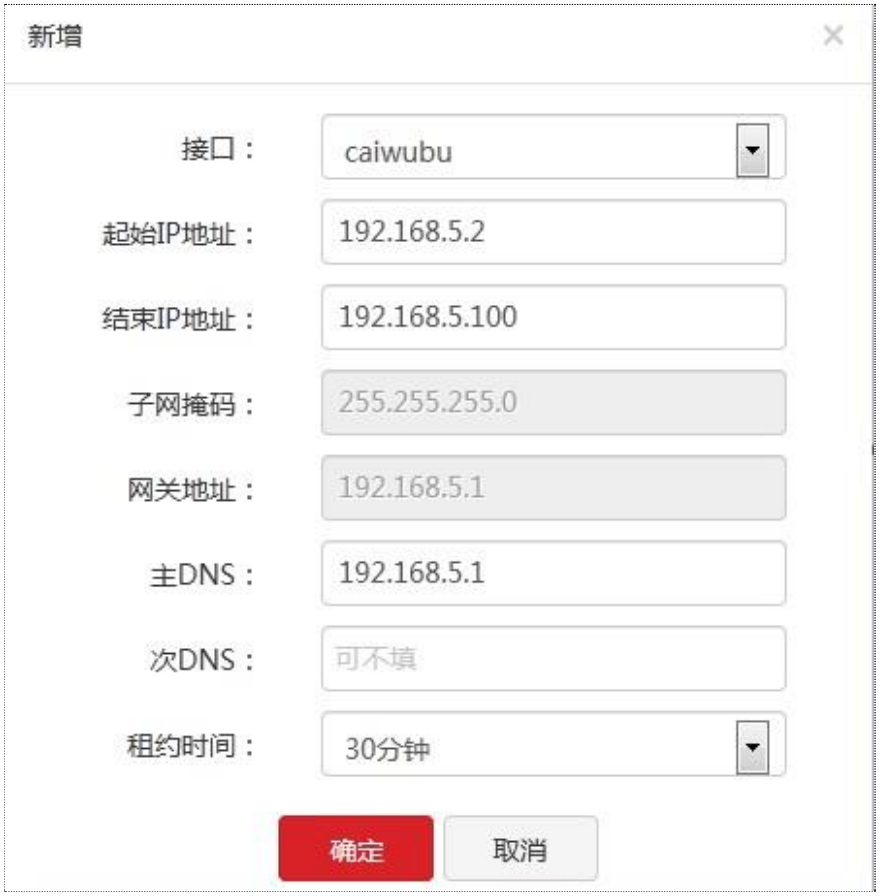


图3-12 设置 DHCP 服务器

添加成功。

图3-13 添加 DHCP 服务器成功

修改 DHCP 服务器

步骤1 点击「网络设置」>「局域网设置」，找到“DHCP 服务器”模块；

步骤2 找到要修改“DHCP 服务器”信息的接口，点击 ；

图3-14 修改 DHCP 服务器

步骤3 修改相关参数；

图3-15 编辑 DHCP 服务器

步骤4 点击 确定 。

删除 DHCP 服务器

步骤1 点击「网络设置」>「局域网设置」，找到“DHCP 服务器”模块；

步骤2 找到要删除“DHCP 服务器”的接口，点击 ；

图3-16 删除 DHCP 服务器

步骤3 在弹出的窗口点击 确定 。

图3-17 确认删除 DHCP 服务器

3.3.4 DHCP 固定 IP 地址分配

概述

“DHCP 固定 IP 地址分配”功能允许客户端始终获取同一 IP 地址，从而使路由器的“行为管理”、“网速控制”、“虚拟服务器”等功能正常生效。本功能仅在路由器“DHCP 服务器”功能启用时生效。

在“DHCP 固定 IP 地址分配”模块，可以查看从路由器 DHCP 服务器自动获取 IP 地址的客户端信息，并一键绑定客户端，使 DHCP 服务器始终给同一客户端分配固定的 IP 地址。

在“DHCP 固定 IP 地址手动分配”模块可以手动绑定客户，使 DHCP 服务器始终给同一客户端分配固定的 IP 地址。

情景 1：客户端当前已连接到路由器

客户端当前已连接到路由器时，推荐在“DHCP 固定 IP 地址分配”模块进行设置。

点击「网络设置」>「局域网设置」，找到“DHCP 固定 IP 地址分配”模块。

图3-18 DHCP 固定 IP 地址分配

表3-4 DHCP 固定 IP 地址分配参数说明

标题项	说明
绑定	将选中的客户端都进行 IP 地址、MAC 地址绑定。
IP 地址	客户端的 IP 地址。
MAC 地址	客户端的 MAC 地址。
主机名	客户端的名称。
IP/MAC 绑定	点击“绑定”即可一键绑定客户端 IP 地址、MAC 地址，使客户端始终获取同一 IP 地址。绑定成功后将显示“已绑定”。

- 绑定单个客户端的 IP 地址

步骤1 点击『网络设置』→『局域网设置』，找到“DHCP 固定 IP 地址分配”模块；

步骤2 在“DHCP 固定 IP 地址分配”列表，找到要分配固定 IP 地址的客户端，点击 绑定 。

图3-19 绑定单个客户端的 IP 地址

绑定成功，如下。

图3-20 成功绑定单个客户端的 IP 地址

- 同时绑定多个客户端的 IP 地址

步骤1 点击「网络设置」>「局域网设置」，找到“DHCP 固定 IP 地址分配”模块。

步骤2 在“DHCP 固定 IP 地址分配”列表，选择多个要分配固定 IP 地址的客户端；

步骤3 然后点击 绑定 。

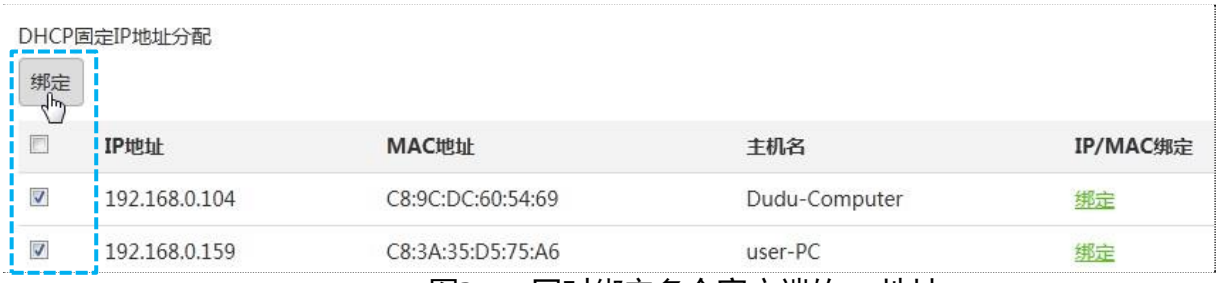


图3-21 同时绑定多个客户端的 IP 地址

绑定成功，如下。

图3-22 成功同时绑定多个客户端的 IP 地址

情景 2：客户端未连接到路由器

客户端未连接到路由器时，推荐在“DHCP 固定 IP 地址手动分配”模块进行设置。

点击「网络设置」>「局域网设置」，找到“DHCP 固定 IP 地址手动分配”模块。

图3-23 DHCP 固定 IP 地址手动分配

● 新增规则

步骤1 点击「网络设置」>「局域网设置」，找到“DHCP 固定 IP 地址手动分配”模块；

步骤2 点击 +新增分配 ；

图3-24 新增 DHCP 固定 IP 地址手动分配

步骤3 在【DHCP 固定 IP 地址手动分配】窗口进行各项参数设置；

步骤4 点击 确定 。

图3-25 设置 DHCP 固定 IP 地址手动分配参数

规则添加成功，如下。如果需要添加多个客户端，重复步骤 1~4 即可。

图3-26 成功添加 DHCP 固定 IP 地址手动分配

表3-5 DHCP 固定 IP 地址手动分配参数说明

标题项	说明
+新增分配	点击此按钮，新增一条规则。
删除	删除已选中的 IP 地址、MAC 地址绑定规则。
MAC 地址	客户端的 MAC 地址。
IP 地址	对应 MAC 地址的客户端绑定的 IP 地址。
备注	客户端 IP 地址、MAC 地址绑定规则的备注信息。
状态	IP 地址、MAC 地址绑定规则的状态。
操作	可对 IP 地址、MAC 地址绑定规则进行相关操作，包括：启用/禁用规则、编辑规则信息、删除规则。

● 修改规则

点击「网络设置」>「局域网设置」，找到“DHCP 固定 IP 地址手动分配”模块；

如果需要修改规则参数，请点击操作栏的；如果需要禁用/启用规则，请点击操作栏的 / 。

● 删除规则

点击「网络设置」>「局域网设置」，找到“DHCP 固定 IP 地址手动分配”模块；

如果需要删除某条规则，请点击操作栏的；如果需要同时删除多个规则，请选中要删除的多个规则，然后点击 删除 。

3.4 端口镜像

3.4.1 概述

路由器提供了端口镜像功能，可将路由器一个或多个端口（被镜像端口）的数据复制到指定的端口（镜像端口），在镜像端口一般接有数据监测设备，以便网络管理员实时进行流量监控、性能分析和故障诊断。端口镜像使用拓扑图如下。

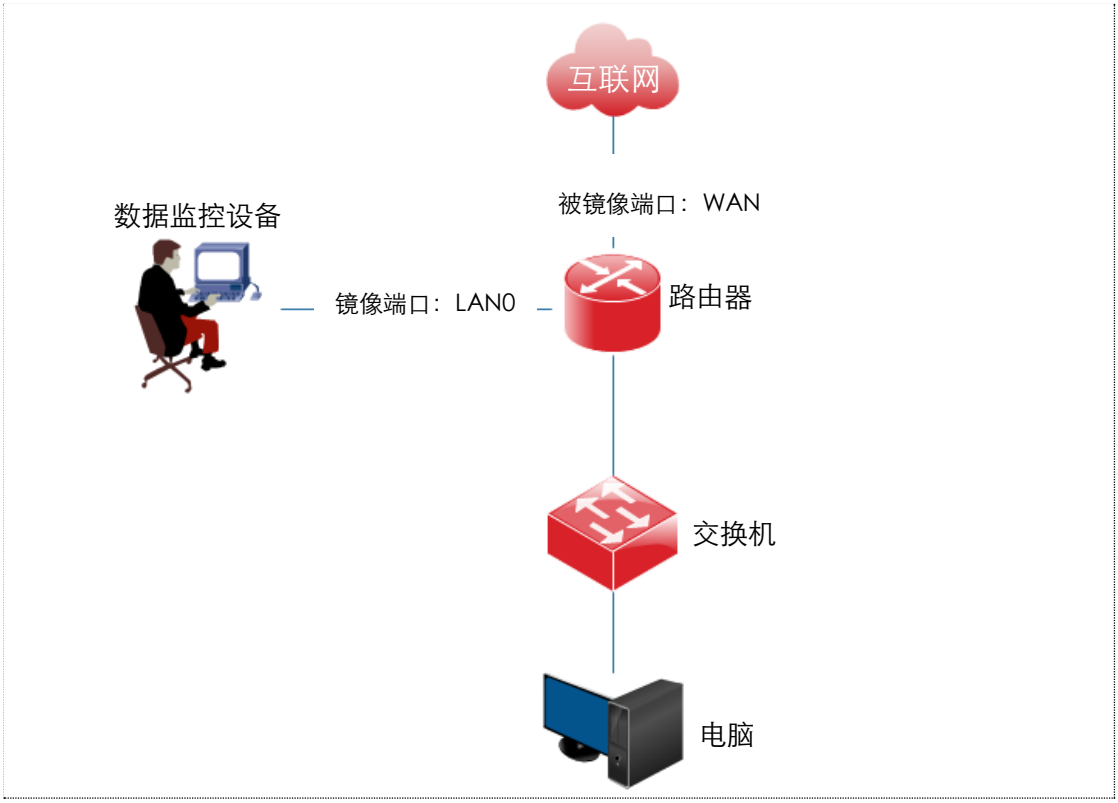


图3-27 端口镜像

3.4.2 配置端口镜像

步骤1 点击「网络设置」>「端口镜像」；

步骤2 选择“开启”端口镜像；

步骤3 选择“被镜像端口”；

步骤4 点击 确定 。

图3-28 配置端口镜像

表3-6 端口镜像参数说明

标题项	说明
端口镜像	开启/关闭路由器的端口镜像功能，默认为“关闭”。
镜像端口	即监控端口，该端口下的计算机要安装监控软件。镜像端口默认为 LAN0，暂不支持修改。
被镜像端口	选择被监控端口。开启端口镜像功能后，被镜像端口的报文会被复制到镜像端口。

3.4.3 端口镜像配置举例

组网需求

某企业使用网关路由器进行网络搭建，最近公司网络异常，经常上不了网，网络管理员需要捕获路由器 WAN 口、LAN 口的数据进行分析。

配置步骤

步骤1 点击「网络设置」>「端口镜像」，选择“开启”端口镜像功能；

步骤2 被镜像端口：勾选“LAN1、LAN2、WAN1、WAN0”；

步骤3 点击 确定 。

图3-29 端口镜像配置

验证配置

在监控电脑上运行监控软件，如 Wireshark，可以抓取到被镜像端口的数据包。

3.5 DNS 定向转发

3.5.1 概述

DNS 定向转发功能将指定的域名通过固定的 WAN 口转发到指定的 DNS 服务器进行 DNS 地址解析，提高访问速率。

点击「网络设置」>「DNS 定向转发」进入设置页面。

图3-30 DNS 定向转发

表3-7 DNS 定向转发参数说明

标题项	说明
域名	要进行性换发的域名地址。
DNS 地址	进行 DNS 解析服务的地址。
WAN 口选择	数据从路由器出去的接口，设置时，请根据需要选择相应 WAN 口。
状态	规则当前的状态。
操作	可对端口过滤规则进行如下操作： - 点击可以禁用该规则。 - 点击可以启用该规则。 - 点击可以修改该规则。 - 点击可以删除该规则。

3.5.2 添加 DNS 定向转发规则

步骤1 点击「网络设置」>「DNS 定向转发」；

步骤2 点击 +新增 。

图3-31 新增 DNS 定向转发规则

1. 域名：输入要进行解析转发的域名，如“baidu.com”；
2. DNS 地址：输入要进行 DNS 解析的服务器地址，如“14.215.177.38”；
3. WAN 口选择：选择对数据进行转发的 WAN 口，如“WAN0”口；
4. 点击 确定 。

图3-32 DNS 定向转发规则配置

3.5.3 修改 DNS 定向转发规则

步骤1 点击「网络设置」>「DNS 定向转发」；

步骤2 找到要修改的 DNS 定向转发规则，点击；

图3-33 修改 DNS 定向转发规则

步骤3 修改相关参数；

步骤4 点击 确定 。

图3-34 编辑 DNS 定向转发规则

3.5.4 删除 DNS 定向转发规则

步骤1 点击「网络设置」>「DNS 定向转发」；

步骤2 找到要删除的 DNS 定向转发规则，点击；

图3-35 删除 DNS 定向转发规则

步骤3 在弹出的窗口点击 确定 。

图3-36 确认删除 DNS 定向转发规则

3.5.5 导出导入 DNS 数据

路由器还支持导出/导入 DNS 数据功能。网络管理员可以将已配置好的 DNS 数据导出到本地电脑保存，当 DNS 数据丢失时，可以直接导入之前的用户数据，不用重新添加。

导出 DNS 数据

步骤1 点击「网络设置」>「DNS 定向转发」；

步骤2 点击 导出数据 ，按页面提示即可导出文件名为 “DNSForward.csv” 的文件。

导入 PPPoE 用户账号数据

步骤1 点击「网络设置」>「DNS 定向转发」；

步骤2 点击 浏览... ，加载之前导出的用户数据文件 “DNSForward.csv”，然后点击 导入数据 。

3.6 DNS 劫持

3.6.1 概述

启用 DNS 劫持后，可以设置域名与 IP 地址的对应规则。这样，当局域网用户访问规则中的域名时，直接解析为访问对应的 IP 地址

点击「网络设置」>「DNS 劫持」进入设置页面。

图3-37 DNS 劫持

表3-8 DNS 劫持参数说明

标题项	说明
域名	要解析为内网固定 IP 地址的域名。
DNS 地址	域名解析的 IP 地址，即用户访问指定域名时，都会解析到该 IP 地址。
状态	规则当前的状态。
操作	可对端口过滤规则进行如下操作： - 点击可以禁用该规则。 - 点击可以启用该规则。 - 点击可以修改该规则。 - 点击可以删除该规则。

3.6.2 添加 DNS 劫持规则

步骤1 点击「上网设置」>「DNS 劫持」，进入设置页面；

步骤2 点击 +新增 ；

图3-38 新增 DNS 劫持规则

1. 域名：到指定 IP 地址的域名，如“baidu.com”；
2. DNS 地址：输入该域名地址固定解析到的 IP 地址，如“14.215.177.38”；
3. 点击 确定 ；

图3-39 新增 DNS 劫持规则

3.6.3 修改 DNS 劫持规则

步骤1 点击「上网设置」>「DNS 劫持」，进入设置页面；

步骤2 找到要修改的 DNS 劫持规则，点击；

图3-40 修改 DNS 劫持规则

步骤3 修改相关参数；

步骤4 点击 确定 。

图3-41 编辑 DNS 劫持规则

3.6.4 删除 DNS 劫持规则

步骤1 点击「网络设置」>「DNS 劫持」；

步骤2 找到要删除的 DNS 劫持规则，点击；

图3-42 删除 DNS 劫持规则

步骤3 在弹出的窗口点击 确定 。

图3-43 确认删除 DNS 劫持规则

3.7 静态路由

3.7.1 概述

路由，是选择一条最佳路径把数据从源地址传送到目的地址的行为。静态路由则是手动配置的一种特殊路由，具有简单、高效、可靠等优点。合适的静态路由可以减少路由选择问题和路由选择数据流的过载，提高数据包的转发速度。

通过设置目标网段/掩码、网关 IP 地址和接口来确定一条静态路由，其中，目标网段/掩码用来确定一个目标网络或主机。静态路由设置完成后，所有目的地址为静态路由目的地址的数据均直接通过该静态路由接口转发至网关 IP。

注意

在大型复杂网络中完全使用静态路由时，如果网络发生故障或者拓扑发生变化，可能会出现路由不可达，并导致网络中断，此时必须由网络管理员手工修改静态路由的配置。

3.7.2 配置静态路由

进入页面的方法：点击「网络设置」>「静态路由」。

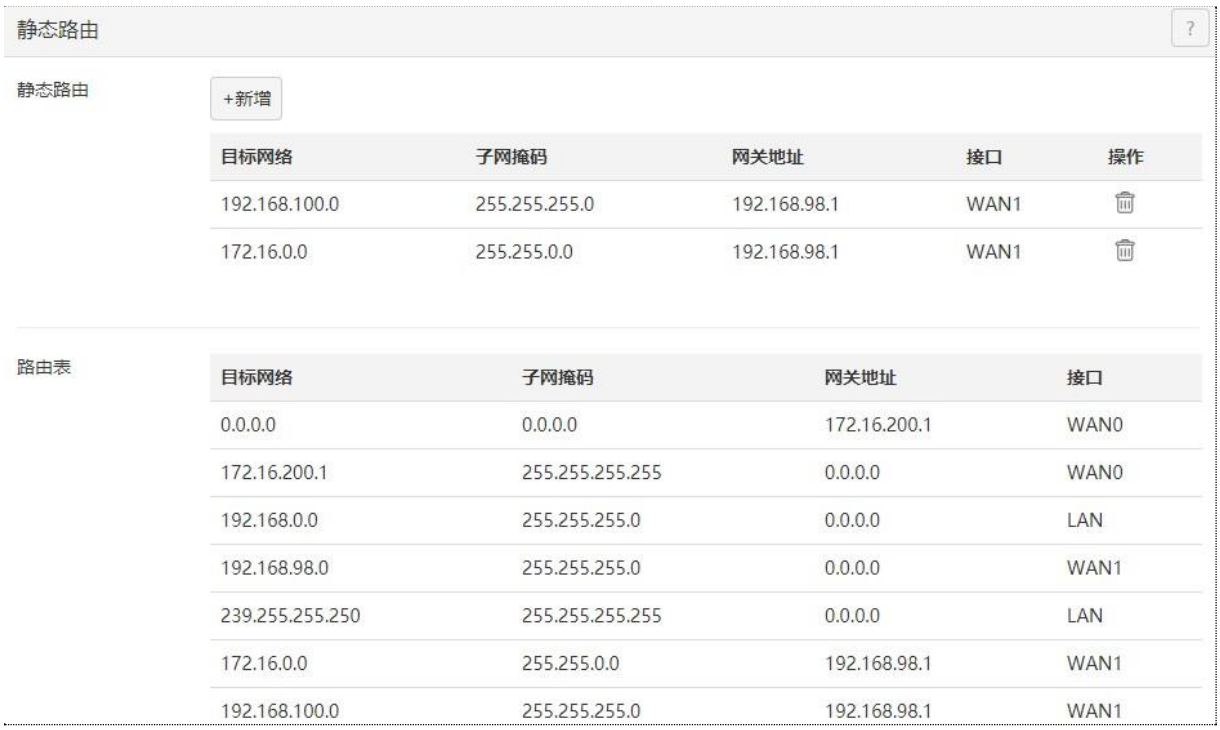


图3-44 静态路由

新增静态路由

步骤1 点击「网络设置」>「静态路由」；

步骤2 点击 +新增 ；

步骤3 在【新增】窗口进行各项参数设置；

步骤4 点击 确定 。

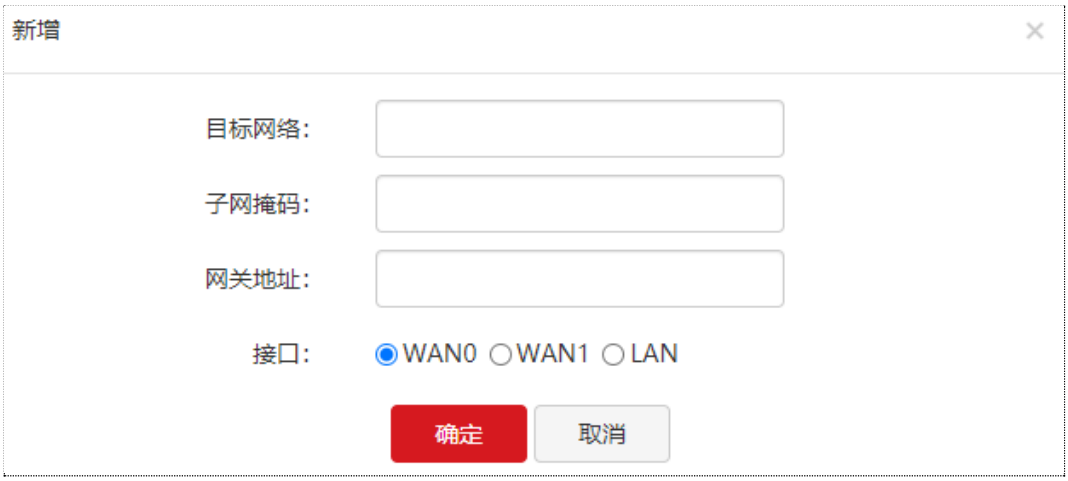


图3-45 新增静态路由

静态路由添加成功后，可以在「网络设置」>「静态路由」页面查看已添加的静态路由规则。配置好的静态路由也将显示在下方的路由表中，如下图示例。

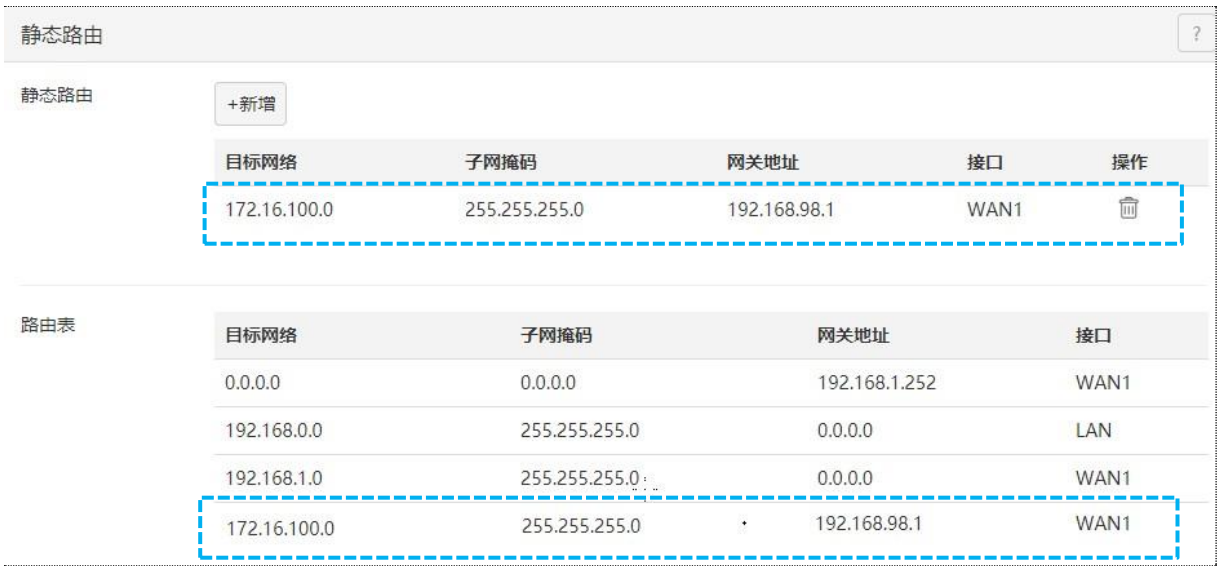


图3-46 成功添加静态路由

路由表中，目标网络/子网掩码都为“0.0.0.0”的路由为路由器的默认路由，当在路由表中找不到与数据包的目的地址精确匹配的路由时，路由器会选择默认路由来转发该数据包；网关为“0.0.0.0”的路由为直连路由，表示该目标网络是路由器该接口直连的网络。

注意

当静态路由规则和自定义的多 WAN 策略冲突时，静态路由优先生效。

表3-9 静态路由

标题项	说明
目标网络	目的网络的 IP 地址。
子网掩码	目的网络 IP 地址的子网掩码。
网关地址	数据包从路由器的接口出去后，下一跳陆游的入口 IP 地址。
接口	数据从路由器出去的接口，请根据需要选择相应 WAN 口。

修改静态路由

步骤1 点击「网络设置」>「静态路由」，找到“静态路由”模块；

步骤2 点击操作栏的 。

删除静态路由

步骤1 点击「网络设置」>「静态路由」，找到“静态路由”模块；

步骤2 点击操作栏的 。

3.7.3 静态路由配置举例

组网需求

某企业使用本网关路由器进行网络搭建。互联网、公司内网在不同的网络，其中，路由器的 WAN0 口通过宽带拨号接入互联网，WAN1 口通过动态 IP 接入公司内网。现要求：局域网的用户能同时访问互联网和公司内网。

假设外网 ISP 提供的宽带拨号的账号/密码均为 “zhangsan”。

注意

如果公司内网和互联网没有完全隔离，则路由器可能会将默认路由指向内网网关，导致路由出错。此时，请转到「网速控制」页面，修改 WAN1 口的速率，使其远小于 WAN0 的值。

如果发生上述情况，建议关闭路由器的智能限速功能；并使用自定义多 WAN 策略，将局域网中所有用户指定到 WAN0 口。否则可能导致网络异常。

网络拓扑

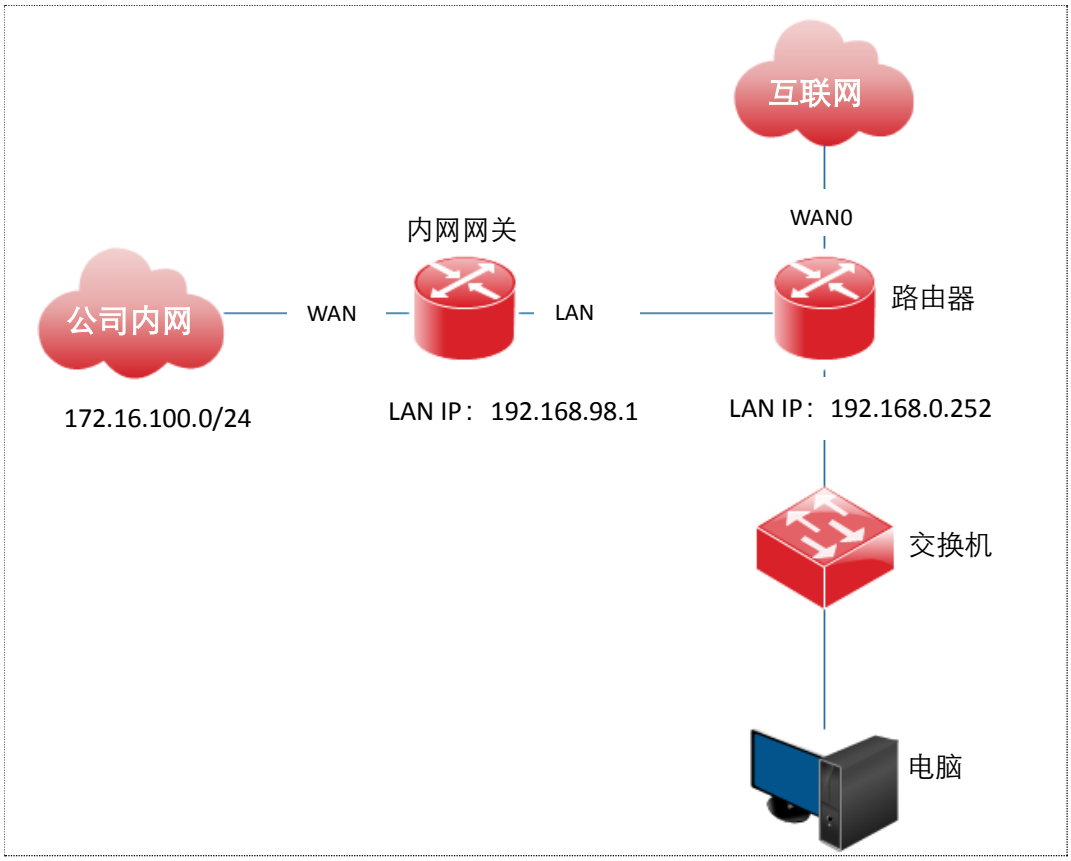


图3-47 静态路由配置

配置步骤

在路由器上进行上网设置，并配置静态路由，即可满足需求。

步骤1 上网设置；

点击「网络设置」>「上网设置」，进行上网设置，然后点击 确定 。

图3-48 上网设置

步骤2 配置静态路由。

点击「网络设置」>「静态路由」，点击 +新增 ，配置如下静态路由。

图3-49 配置静态路由

配置好的静态路由将显示在路由表中，如下图所示。

图3-50

验证配置

局域网中的电脑可以同时访问互联网和公司内网。

3.8 VLAN 设置

3.8.1 概述

传统的共享介质以太网和交换式以太网中，所有的用户都在一个广播域。随着网络内计算机数量的增多，广播包的数量也急剧增加，这大大增加了网络中所有设备之间的数据流量，进而影响了网络性能。随着网络不断扩充，还可能出现广播风暴，导致整个网络无法使用。

VLAN（Virtual Local Area Network，虚拟局域网），是一种将局域网内的设备在逻辑上而不是在物理上划分成不同网段，从而实现虚拟工作组的数据交换技术。它将一个局域网划分成多个逻辑的局域网—VLAN，VLAN 组内主机位于同一个广播域，它们在任何地理位置都可以像连接在同一个网段上一样正常通信；组间隔绝广播，不同 VLAN 内的主机不能直接通信，必须通过路由器或其它三层包转发设备转发。

VLAN 使用示意图如下：

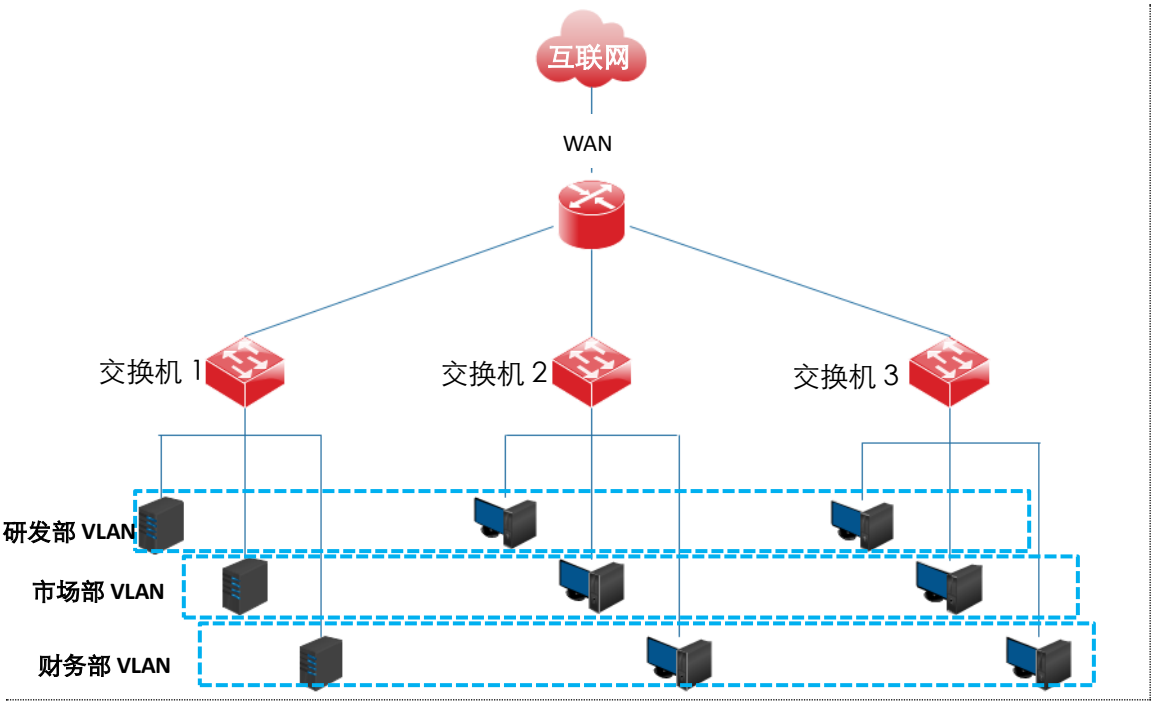


图3-51 VLAN

VLAN 有如下优点：

- 提高网络性能。将局域网内的广播包限制在一个 VLAN 内，节省了网络带宽，提高了网络处理能力。
- 减少设备投资。传统通过路由器来隔离广播风暴的方法加大了网络管理成本，VLAN 技术使成本控制成为可能。
- 简化网络管理。使用 VLAN 可以创建跨物理网络范围的虚拟工作组，当用户的物理位置在虚拟局域网范围内移动时，不需要更改网络配置即可正常访问网络。
- 确保网络安全。不同 VLAN 的主机不能直接相互通信，需要通过路由器或三层交换机等网络层设备对报文进行三层转发，这加强了企业网络中不同部门之间的安全性。

本路由器支持 IEEE 802.1Q VLAN，详细说明如下：

- IEEE 于 1999 年正式签发了 802.1Q 标准，用于规定 VLAN 的国际标准实现，使得不同厂商设备之间 VLAN 互通成为可能。
- 802.1Q 协议规定在以太网帧的目的 MAC 地址和源 MAC 地址之后封装一个 4 字节的 802.1Q VLAN 标记，用以标识 VLAN 的相关信息。如下图所示，标准以太网帧在目的 MAC 地址（DA）和源 MAC 地址（SA）后加入一个 802.1Q VLAN 标签（tag）就变成了带有 802.1Q 标签的以太网帧。

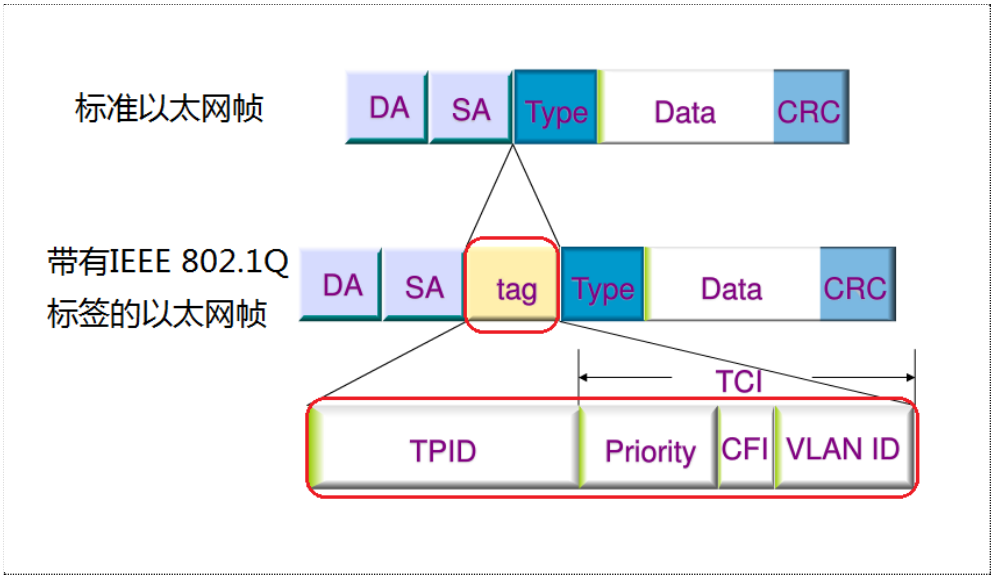


图3-52

表3-10 802.1Q 参数说明

字段	说明
TPID	用来标识该数据帧是带有 802.1Q VLAN Tag 的数据帧。该字段长度为两字节，即 16bit，IEEE 802.1Q 协议定义该值为 0x8100。
Priority	● 用来标识该数据帧的优先级，主要用于当交换机阻塞时，优先发送优先级高的数据包。 ● 该字段长度为 3bit，取值范围为<0~7>，7 为最高优先级，0 为最低优先级。
CFI	● 用来标识 MAC 地址是否以标准格式进行封装，该字段长度为 1bit。 ● 0 表示 MAC 地址以标准格式进行封装，1 表示以非标准格式封装。对于以太网交换机，默认为 0。
VLAN ID	虚拟局域网的标识，用来标识报文所属 802.1Q VLAN，该字段长度为 12bit，取值范围为<0~4095>，0 和 4095 通常不使用，所以 VID 取值范围一般为<1~4094>。

3.8.2 添加 VLAN

本路由器添加 VLAN 后，接口为 Trunk 口。

添加 VLAN 规则

步骤1 点击「网络设置」>「VLAN 设置」；

步骤2 点击 +新增 ；

图3-53 VLAN 设置

步骤3 在弹出的窗口设置 VLAN 规则；

步骤4 点击 确定 ；

图3-54 新增 VLAN

返回“VLAN 设置”页面点击**重启设备**，路由器重启后生效。

表3-11 VLAN 设置参数说明

标题项	说明
VLAN ID	设置 VLAN ID 值，范围：10~4094。
VLAN 名称	设置 VLAN 接口名称。
IP 地址	设置 VLAN（虚拟局域网）的 IP 地址。
子网掩码	设置 VLAN（虚拟局域网）的子网掩码。
接口	选择 VLAN 接口对应的物理接口。 1 个 VLAN 接口可以对应多个物理接口，1 个物理接口也可以对应多个 VLAN 接口。
备注	设置 VLAN 规则的备注信息。
状态	规则的启用状态，包括已启用或未启用。新增规则后，默认状态为“已启用”。 ● 已启用规则时，点击 ⊘ ，可以将规则状态改为“未启用”。 ● 未启用规则时，点击 ✓ ，可以将规则状态改为“已启用”。

配置 VLAN DHCP 服务器

添加 VLAN 规则后，需要为该 VLAN 设置 DHCP 服务器信息，否则在该 VLAN 下的客户端不能自动获取 IP 地址上网。

步骤1 点击「网络设置」>「局域网设置」，找到“DHCP 服务器”模块；

步骤2 点击 +新增 ；

图3-55 新增 DHCP 服务器

步骤3 在弹出的窗口设置 DHCP 服务器信息。

步骤4 接口：点击下拉菜单，选择已在“VLAN”设置页面添加的 VLAN，如“caiwubu”。

步骤5 起始/结束 IP 地址：设置 DHCP 服务器可分配给客户端的 IP 地址范围，IP 地址网段须和“网关地址”一致，如“192.168.5.2~192.168.5.100”。

步骤6 主 DNS：可设置为“网关地址”或正确的 DNS 信息，如“192.168.5.1”。

步骤7 点击 确定 。

图3-56 新增 DHCP 服务器

添加成功。

图3-57 成功添加 DHCP 服务器

3.8.3 修改 VLAN 规则

步骤1 点击「网络设置」>「VLAN 设置」；

步骤2 找到要修改的 VLAN 规则，点击；

图3-58 修改 VLAN 规则

步骤3 修改相关参数；

步骤4 点击 确定 。

图3-59 编辑 VLAN 规则

返回“VLAN 设置”页面点击重启设备，路由器重启后生效。

3.8.4 删除 VLAN 规则

步骤1 点击「网络设置」>「VLAN 设置」；

步骤2 找到要删除的 VLAN 规则，点击；

图3-60 删除 VLAN 规则

步骤3 在弹出的窗口点击 确定 。

图3-61 确认删除 VLAN 规则

返回“VLAN 设置”页面点击重启设备，路由器重启后生效。

3.8.5 VLAN 配置举例

组网需求

某企业使用网关路由器+AP 进行网络搭建。要给员工、管理人员、访客分别设置不同的上网权限。

- 员工可以通过有线、无线接入到网络上网。
- 管理人员可以通过有线、无线接入到网络上网。
- 访客只能通过无线接入到网络上网。

方案设计

结合路由器的 VLAN 功能、WEB 认证功能实现不同用户群上网。将员工划入 VLAN10、管理人员划入 VLAN20、访客划入 VLAN30。假设网络拓扑图如下：

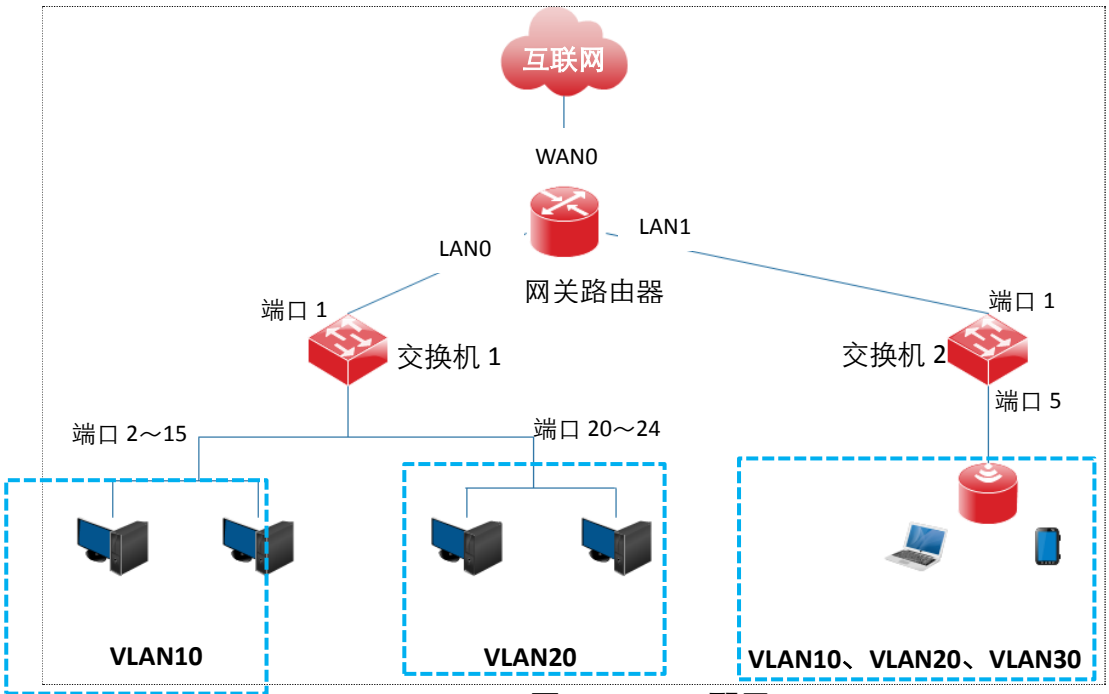


图3-62 VLAN 配置

配置步骤

一、设置路由器

为 LAN0、LAN1 分别设置 VLAN，并设置 DHCP 服务器。

步骤1 设置 VLAN；

1. 点击「网络设置」>「VLAN 设置」；
2. 点击 +新增 ；

图3-63 新增 VLAN

3. 在弹出的窗口设置 VLAN 规则；
4. VLAN ID：设置 VLAN ID 值，本例为“10”；
5. VLAN 名称：设置本条 VLAN 规则的名称，如“yuangong”；
6. IP 地址：设置 VLAN 接口 IP 地址，如“192.168.5.1”；
7. 子网掩码：设置 VLAN 接口的子网掩码，如“255.255.255.0”；
8. 接口：选择 VLAN 所属接口，本例为“LAN0、LAN1”；
9. 备注：设置本条 VLAN 规则的备注信息，如“员工”；
10. 点击 确定 。

图3-64 新增 VLAN

重复 1~10 添加 VLAN20、VLAN30。

返回“VLAN 设置”页面点击**重启设备**，根据页面提示操作，路由器重启后生效。

图3-65 重启设备

步骤2 为 VLAN 接口设置 DHCP 服务器信息；

1. 点击「网络设置」>「局域网设置」，找到“DHCP 服务器”模块；
2. 点击 +新增 ；

图3-66 新增 DHCP 服务器

3. 在弹出的窗口设置 DHCP 服务器信息；
4. 接口：点击下拉菜单，选择已在“VLAN”设置页面添加的 VLAN，如“yuangong”；
5. 起始/结束 IP 地址：设置 DHCP 服务器可分配给客户端的 IP 地址范围，IP 地址网段须和“网关地址”一致，如“192.168.5.2~192.168.5.100”；
6. 主 DNS：可设置为“网关地址”或正确的 DNS 信息，如“192.168.5.1”；

7. 点击 确定 。

图3-67 新增 DHCP 服务器

重复步骤 1~7 为 VLAN20、VLAN30 设置 DHCP 服务器信息。

添加成功，如下图示：

图3-68 成功添加 DHCP 服务器

步骤3 给 AP 下发策略；

1. 点击「AC 管理」>「无线配置」进入设置页面。
2. AC 管理：点击“开启”，启用该功能。
3. 状态：选择“开启”。
4. SSID：设置要下发给 AP 的无线网络名称，本例为“办公网络”。
5. 频段：选择“2.4G&5G”。
6. 最大用户数：设置可连接该 SSID 的最大用户数值，如“50”。

7. VLAN ID：设置 SSID 所属的 VLAN ID，本例为“10”。

8. 认证类型：设置 SSID 认证类型，如“WPA2-PSK”。

9. 密码：设置无线密码，如“12345678”。

10. 参考步骤 3~9 添加“管理网络”和“HIKVISION”的无线信息。

11. 点击 确定 。

图3-69 无线配置

步骤4 启用 AP QVLAN 功能。

1. 点击「AC 管理」>「高级配置」，找到“全局配置”模块。

2. VLAN：点击“开启”。

3. 点击 确定 。

图3-70 全局配置

二、设置交换机

在交换机上设置 802.1QVLAN。

表3-12 交换机 1 参数

端口	VLAN ID(允许通过的 VLAN)	端口链路类型	PVID
端口 1	10、20	Trunk	1
端口 2~15	10	Access	10
端口 20~24	20	Access	20

表3-13 交换机 2 参数

端口	VLAN ID(允许通过的 VLAN)	端口链路类型	PVID
端口 1	10、20、30	Trunk	1
端口 5	10、20、30	Trunk	1

因部署网络时所用交换机不尽相同，详细设置说明请参考相应说明书的用户手册。

验证配置

- 员工可以接在交换机 1 的端口 2~15 进行上网。
- 管理人员可以接在交换机 1 的端口 20~24 进行上网。
- 员工可以连接 SSID 为“办公网络”进行上网。

– 管理人员可以连接 SSID 为“管理网络”进行上网。

– 访客可以连接 SSID 为“HIKVISION”进行上网。

3.9 非法 IP 地址拦截

非法 IP 地址拦截，即路由器禁止客户端使用不正确的 IP 地址上网，本功能默认启用。

关闭“非法 IP 地址拦截”功能后，客户端配置任意 IP 地址、网关、DNS 都可以上网，用户无需理会电脑网卡 IP 地址配置。

点击「网络设置」>「非法 IP 地址拦截」，进入设置页面。

本功能默认开启，可根据实际需要点击开启或关闭，然后点击 确定 即可。

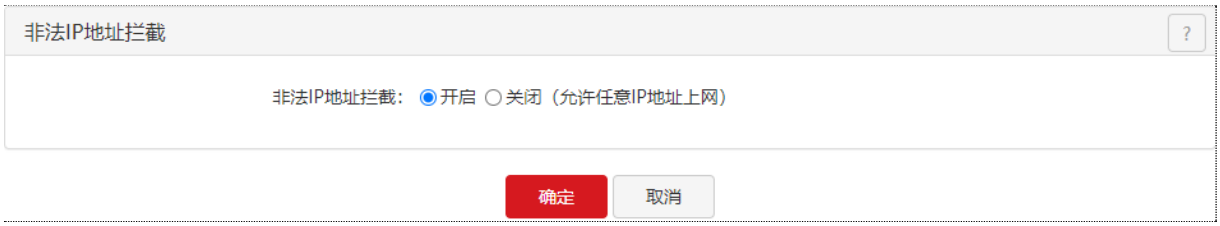


图3-71 非法 IP 地址拦截

3.10 DNS 缓存

在“DNS 缓存”页面，您可以开启/关闭 DNS 缓存功能，设置缓存容量条数。

路由器的 DNS 缓存功能使路由器可以记录用户访问网站的 DNS 解析信息。当用户访问的网站存在于缓存中时，将直接从路由器的 DNS 缓存列表中调用缓存的信息，不必再去询问 DNS 服务器，提高了访问速率。

点击「网络设置」>「DNS 缓存」，进入设置页面。

缓存容量默认为 1000 条，可根据需要修改。输入缓存容量值，然后点击 确定 即可。

图3-72 DNS 缓存

3.11 高级设置

在高级设备页面中，勾选启用之后，设备会接入萤石云平台，可以通过萤石云平台了解设备的信息。

步骤1 点击「网络设置」>「高级设置」，进入设置页面；

步骤2 选择“启用”；

图3-73 高级设置

表3-14 参数说明

标题项	说明
启用	勾选启用之后，设备会接入萤石云平台。启用之前，请确保设备已接入公网。
平台接入方式	目前只支持接入萤石云。
接入服务器 IP	萤石云平台的服务器 IP，用户也可自定义接入服务器的 IP。
连接状态	设备连接到萤石云平台的状态。
操作码	用户通过海康云管 App 设备时，设备定义的验证用户对该设备具有所有权的凭证。默认初始值为验证码。用户也可以自行设置 6~12 位大小写字母和数字组合的操作码。

第4章 行为管理

4.1 概述

路由器的「行为管理」模块包括：

IP 组和时间组、IP 地址过滤、MAC 地址过滤、端口过滤、网络应用过滤、网址分类过滤、多 WAN 策略。

4.1.1 功能介绍

- IP 组和时间组

  用于设置 IP 组和时间组。在使用路由器的 IP 地址过滤、MAC 地址过滤、端口过滤、网络应用过滤、网址分类过滤、单独限速等功能时，会引用时间组配置；在使用路由器的 IP 地址过滤、端口过滤、网络应用过滤、网址分类过滤、自定义多 WAN 策略等功能时，会引用 IP 组配置。

- IP 地址过滤

  通过 IP 地址黑白名单，限制可以通过路由器上网的用户。

  - 白名单：对应过滤规则“允许访问互联网”。

  - 黑名单：对应过滤规则“禁止访问互联网”。

- MAC 地址过滤

  通过 MAC 地址黑白名单，限制可以通过路由器上网的用户。

  - 白名单：对应过滤规则“允许访问互联网”。

  - 黑名单：对应过滤规则“禁止访问互联网”。

- 端口过滤

  - 互联网上众多服务所涉及的应用协议都有特定的端口号，从 0 到 1023 是常用服务的端口号，这些端口号一般固定分配给特定的服务。

  - 端口过滤通过禁止用户对互联网上指定端口的访问，以此来控制用户的互联网服务类型。

- 网络应用过滤

  使用本功能，可以禁止局域网的用户使用指定的应用，如聊天应用、视频影音、音乐盒子等，有效提升员工的工作效率。

- 网址分类过滤

  使用网址分类过滤，禁止局域网用户访问指定类别网址，可以规范局域网用户上网行为，提升员工工作效率。路由器的特征库默认添加了多个类别的网站，如果需要，用户可以自定义新增分类。

- 多 WAN 策略

  路由器默认启用 2 个 WAN，最多支持 4 个 WAN 口。当多个 WAN 口同时工作时，合理的设置多 WAN 策略可以大幅提升路由器的带宽利用率。路由器支持以下两种多 WAN 策略，用户可以根据需要自行选择。

  – 智能负载均衡：默认方式。路由器根据用户在「网速控制」页面设置的 WAN 口“带宽”，自动寻找流量最小的 WAN 口进行通信，完全不用人工干预，自动分配数据流量。

  – 自定义策略：由用户配置规则，将指定 IP 组的数据分配给特定的 WAN 口。

4.1.2 配置向导

- IP 地址过滤

表4-1 IP 地址过滤

配置任务	说明
设置时间组	设置 IP 地址过滤规则时，需要调用时间组。在「行为管理」>「IP 组和时间组」页面进行。
设置 IP 组	设置 IP 地址过滤规则时，需要调用 IP 组。在「行为管理」>「IP 组和时间组」页面进行。
设置 IP 地址过滤	在「行为管理」>「IP 地址过滤」页面进行。

- MAC 地址过滤

表4-2 MAC 地址过滤

配置任务	说明
设置时间组	设置 IP 地址过滤规则时，需要调用时间组。在「行为管理」>「IP 组和时间组」页面进行。
设置 MAC 地址过滤	在「行为管理」>「MAC 地址过滤」页面进行。

- 端口过滤/网络应用（除 QQ）过滤/网址分类过滤

表4-3 端口过滤/网络应用（除 QQ）过滤/网址分类过滤

配置任务	说明
设置时间组	设置 IP 地址过滤规则时，需要调用时间组。在「行为管理」>「IP 组和时间组」页面进行。
设置 IP 组	设置 IP 地址过滤规则时，需要调用 IP 组。在「行为管理」>「IP 组和时间组」页面进行。
设置端口过滤或网络应用（除 QQ）过滤或网址分类过滤	分别在「行为管理」模块下的「端口过滤」、「网络应用过滤」、「网址分类过滤」页面进行。

- 多 WAN 策略--自定义策略

表4-4 自定义多 WAN 策略

配置任务	说明
设置 IP 组	设置 IP 地址过滤规则时，需要调用 IP 组。在「行为管理」>「IP 组和时间组」页面进行。
自定义多 WAN 策略	在「行为管理」>「多 WAN 策略」页面进行。

- QQ 过滤

  直接在「行为管理」>「网络应用过滤」页面的“QQ 过滤”模块设置即可。

- 多 WAN 策略—智能负载均衡

  直接在「行为管理」>「多 WAN 策略」页面设置即可。

4.2 IP 组和时间组

进入页面的方法：点击「行为管理」>「IP 组和时间组」。进入页面后，默认显示如下。

图4-1 IP 组和时间组

4.2.2 时间组设置

新增时间组

步骤1 点击「行为管理」>「IP 组和时间组」，找到“时间组设置”模块；

步骤2 点击 新增 ；

步骤3 在【新增】窗口进行参数设置；

步骤4 点击 确定 。

图4-2 新增时间组

表4-5 时间组参数说明

标题项	说明
组名称	时间组的名称，注意不能和已有的时间组名称重复。
时间	本时间段的开始~结束时间。00:00~00:00，表示全天。
星期	时间段所包含的日期。

修改时间组

步骤1 点击「行为管理」>「IP 组和时间组」，找到“时间组设置”模块；

步骤2 点击操作栏的 。

注意

如果修改的时间组已经被引用，则修改后，将自动引用修改后的时间组。

删除时间组

步骤1 点击「行为管理」>「IP 组和时间组」，找到“时间组设置”模块；

步骤2 如果您要删除某条时间组设置，请点击操作栏的 ；如果您要同时删除多个时间组，请选中要删除的多个时间组，然后点击 删除 。

注意

使用中（已经被其他功能引用）的时间组不可删除。

4.2.3 IP 组设置

新增 IP 组

步骤1 点击「行为管理」>「IP 组和时间组」，找到“IP 组设置”模块；

步骤2 点击 新增 ；

步骤3 在【新增】窗口进行参数设置；

步骤4 点击 确定 。

图4-3 新增 IP 组

表4-6 新增 IP 组

标题项	说明
组名称	IP 组的名称，注意不能和已有的 IP 组名称重复。
IP 或 IP 段	本 IP 段的开始~结束 IP 地址。

修改 IP 组

步骤1 点击「行为管理」>「IP 组和时间组」，找到“IP 组设置”模块；

步骤2 点击操作栏的 。

注意

如果修改的 IP 组已经被引用，则修改后，将自动引用修改后的 IP 组。

删除 IP 组

步骤1 点击「行为管理」>「IP 组和时间组」，找到“IP 组设置”模块；

步骤2 如果您要删除某条 IP 组设置，请点击操作栏的 ；如果您要同时删除多个 IP 组，请选中要删除的多个 IP 组，然后点击 删除 。

注意

使用中（已经被其他功能引用）的 IP 组不可删除。

4.3 IP 地址过滤

进入页面的方法：点击「行为管理」>「IP 地址过滤」。进入页面后，默认显示如下。

图4-4 IP 地址过滤

4.3.2 配置 IP 地址过滤

开启 IP 地址过滤功能

步骤1 点击「行为管理」>「IP 地址过滤」；

步骤2 选择“开启”IP 地址过滤；

步骤3 点击 确定 。

图4-5 IP 地址过滤

开启 IP 地址过滤功能后，您就可以配置 IP 地址过滤规则了。

配置 IP 地址过滤规则

新增规则

步骤1 点击「行为管理」>「IP 地址过滤」；

步骤2 点击 +新增 ；

步骤3 在【新增】窗口配置各项参数；

步骤4 点击 确定 。

图4-6 新增 IP 地址过滤

表4-7 IP 地址过滤参数说明

标题项	说明
过滤规则	IP 地址过滤的过滤规则。 ● 允许访问互联网：即，白名单。使用此规则时，指定 IP 地址的用户在对应时间段内可以访问互联网，在其他时间段内不可以访问互联网。 ● 禁止访问互联网：即，黑名单。使用此规则时，指定 IP 地址的用户在对应时间段内禁止访问互联网，在其他时间段内可以访问互联网。
IP 组	选择引用的 IP 组，以指定规则对应的用户。IP 组应事先已在「行为管理」>「IP 组和时间组」页面配置好。
时间组	选择引用的时间组，以指定规则对应的生效时间。 时间组应事先已在「行为管理」>「IP 组和时间组」页面配置好。
备注	规则的备注信息。

规则添加完成后，您可以在「行为管理」>「IP 地址过滤」页面查看到已添加的 IP 地址过滤规则。如下图示例。

图4-7 成功新增 IP 地址过滤

表4-8 IP 地址过滤参数说明

标题项	说明
状态	规则的启用状态，包括已启用或未启用。新增规则后，默认状态为“已启用”。 已启用规则时，点击 ，可以将规则状态改为“未启用”；未启用规则时，点击 ，可以将规则状态改为“已启用”。
允许未启用规则和列表外的主机访问互联网	● 勾选时：列表中“未启用”规则的设备和列表外的设备均可以访问互联网。 ● 未勾选时：只有列表中的规则生效，列表中“未启用”规则的设备和列表外的设备均不能访问互联网。

修改规则

步骤1 点击「行为管理」>「IP 地址过滤」；

步骤2 点击操作栏的 。

删除规则

步骤1 点击「行为管理」>「IP 地址过滤」；

步骤2 如果您要删除某条 IP 地址过滤规则，请点击操作栏的 ；如果您要同时删除多个规则，请选中要删除的多个规则，然后点击 删除 。

4.3.3 IP 地址过滤配置举例

组网需求

某企业使用网关路由器进行网络搭建。要求：上班时间（周一到周五的 8:00~18:00），仅允许采购部门人员访问互联网，其他员工禁止访问互联网。

可以使用路由器的 IP 地址过滤功能实现上述需求。假设采购部门人员电脑的 IP 地址为 192.168.0.2~192.168.0.100。

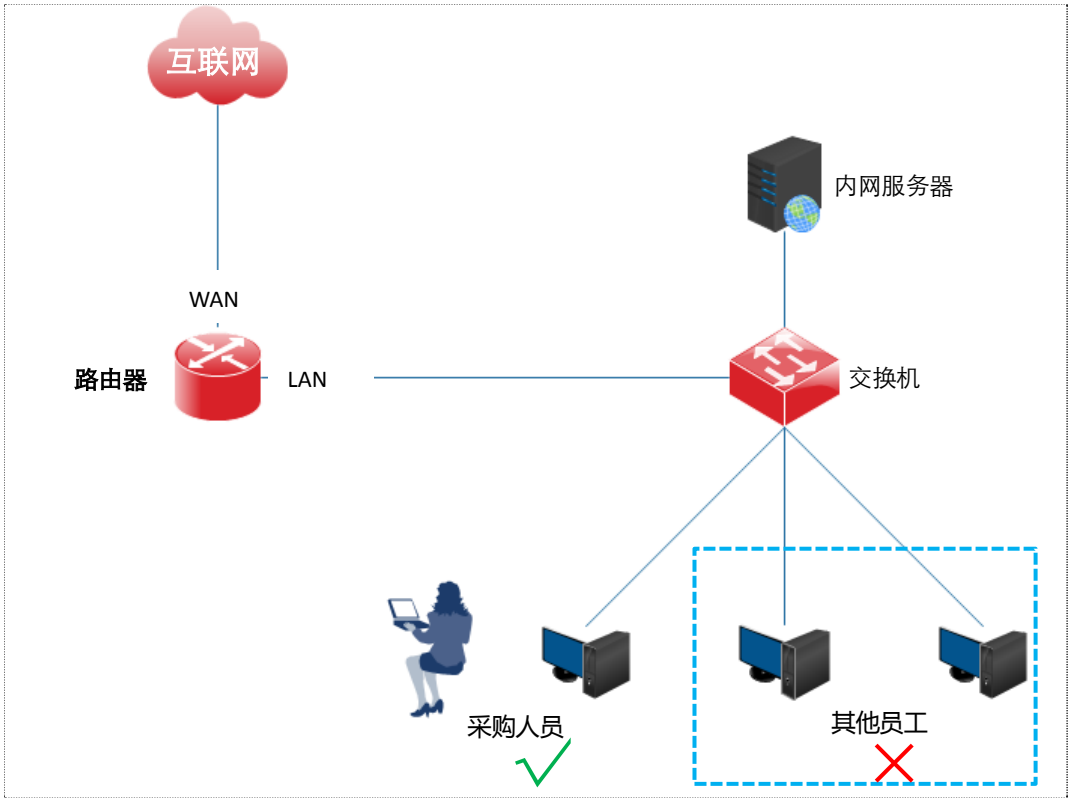


图4-8 IP 地址过滤配置

配置步骤

步骤1 点击「行为管理」>「IP 组和时间组」页面，配置如下时间组。

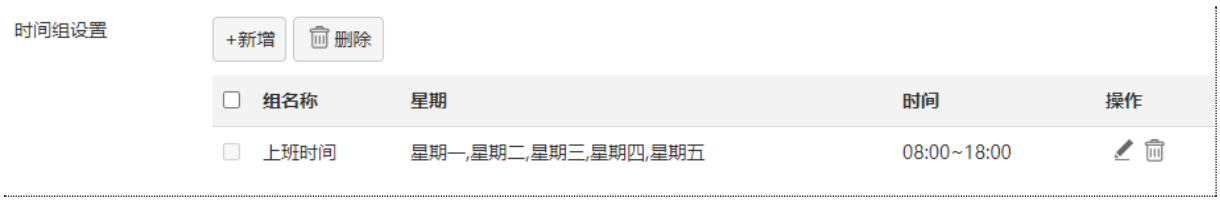


图4-9 时间组设置

步骤2 点击「行为管理」>「IP 组和时间组」页面，配置如下 IP 组。

图4-10 IP 组设置

步骤3 点击「行为管理」>「IP 地址过滤」，进行下述设置。

1. IP 地址过滤：选择“开启”；
2. 点击 确定 。

图4-11 开启 IP 地址过滤

步骤4 点击 +新增 ，配置 IP 地址过滤规则。

1. 在【新增】窗口配置各项参数；
2. 过滤规则：选择“允许访问互联网”。
3. IP 组：选择规则生效的 IP 组，本例为“采购部门”。
4. 时间组：选择规则生效的时间组，本例为“上班时间”。
5. 备注：设置本规则的备注，如“允许上网”。
6. 点击 确定 。

步骤5 取消勾选“允许未启用规则和列表外的主机访问互联网”；

步骤6 点击 确定 。

图4-12 禁用“允许未启用规则和列表外的主机访问互联网”

验证配置

在星期一~星期五的 8:00~18:00，局域网中，只有使用采购部门人员的电脑才能访问互联网，使用其他员工的电脑不能访问互联网。

4.4 MAC 地址过滤

进入页面的方法：点击「行为管理」>「MAC 地址过滤」。进入页面后，默认显示如下。

图4-13 MAC 地址过滤

4.4.2 配置 MAC 地址过滤

开启 MAC 地址过滤功能

步骤1 点击「行为管理」>「MAC 地址过滤」；

步骤2 选择“开启”MAC 地址过滤；

步骤3 点击 确定 。

图4-14 开启 MAC 地址过滤

开启 MAC 地址过滤功能后，您就可以配置 MAC 地址过滤规则了。

配置 MAC 地址过滤规则

新增规则

步骤1 点击「行为管理」>「MAC 地址过滤」；

步骤2 点击 +新增 ；

步骤3 在【新增】窗口配置各项参数；

步骤4 点击 确定 。

图4-15 新增 MAC 地址过滤

表4-9 MAC 地址过滤参数说明

标题项	说明
过滤规则	MAC 地址过滤的过滤规则。 ● 允许访问互联网：即，白名单。使用此规则时，指定 MAC 地址的用户在对应时间段内可以访问互联网，在其他时间段内不可以访问互联网。 ● 禁止访问互联网：即，黑名单。使用此规则时，指定 MAC 地址的用户在对应时间段内禁止访问互联网，在其他时间段内可以访问互联网。
时间组	选择引用的时间组，以指定规则对应的生效时间。 时间组应事先已在「行为管理」>「IP 组和时间组」页面配置好。
MAC 地址	规则对应的用户设备的 MAC 地址。
备注	规则的备注信息。

规则添加完成后，您可以在「行为管理」>「MAC 地址过滤」页面查看到已添加的 MAC 地址过滤规则。如下图示例。

图4-16 成功新增 MAC 地址过滤

表4-10 MAC 地址过滤参数说明

标题项	说明
状态	规则的启用状态，包括已启用或未启用。新增规则后，默认状态为“已启用”。 已启用规则时，点击 ，可以将规则状态改为“未启用”；未启用规则时，点击 ，可以将规则状态改为“已启用”。
允许未启用规则和列表外的主机访问互联网	● 勾选时：列表中“未启用”规则的设备和列表外的设备均可以访问互联网。 ● 未勾选时：只有列表中的规则生效，列表中“未启用”规则的设备和列表外的设备均不能访问互联网。

修改规则

步骤1 点击「行为管理」>「MAC 地址过滤」；

步骤2 点击操作栏的 。

删除规则

步骤1 点击「行为管理」>「MAC 地址过滤」；

步骤2 如果您要删除某条 MAC 地址过滤规则，请点击操作栏的 ；如果您要同时删除多个规则，请选中要删除的多个规则，然后点击 删除 。

4.4.3 MAC 地址过滤配置举例

组网需求

某企业使用网关路由器进行网络搭建。要求：上班时间（周一到周五的 8:00~18:00），仅允许某一采购人员访问互联网，其他员工禁止访问互联网。

可以使用路由器的 MAC 地址过滤功能实现上述需求。假设该采购人员电脑的物理地址为 CC:3A:61:71:1B:6E。

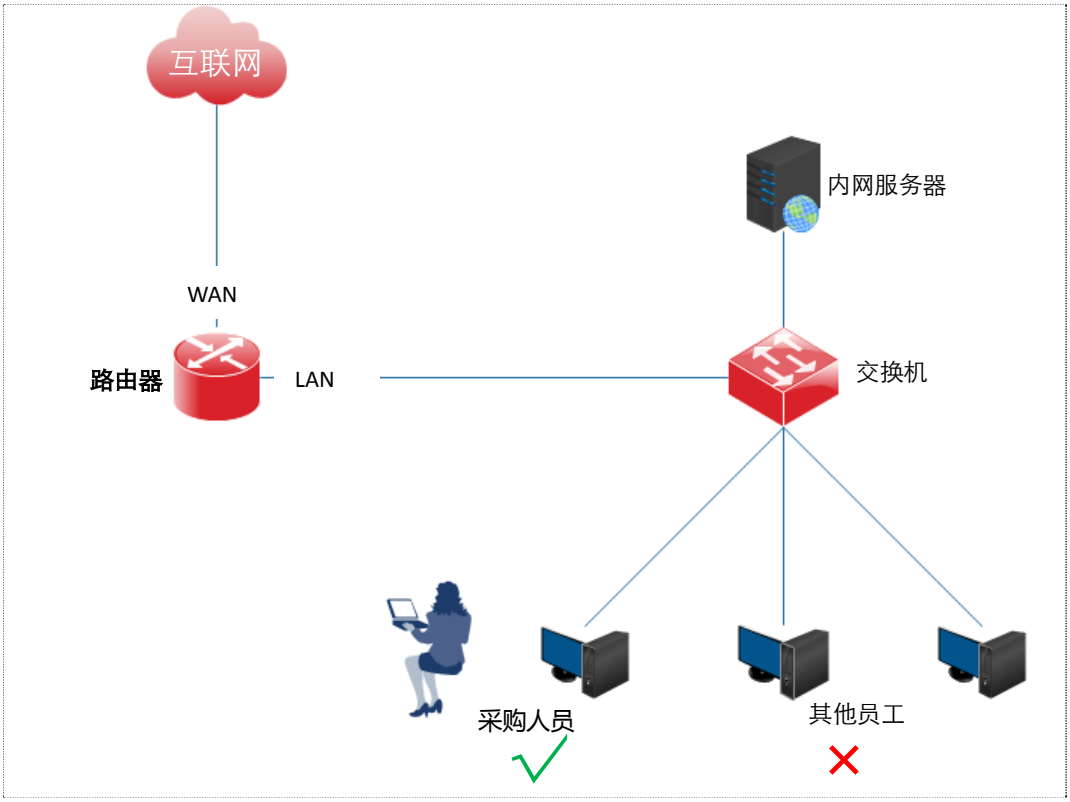


图4-17 MAC 地址配置过滤

配置步骤

步骤1 进入「行为管理」>「IP 组和时间组」页面，配置如下时间组。

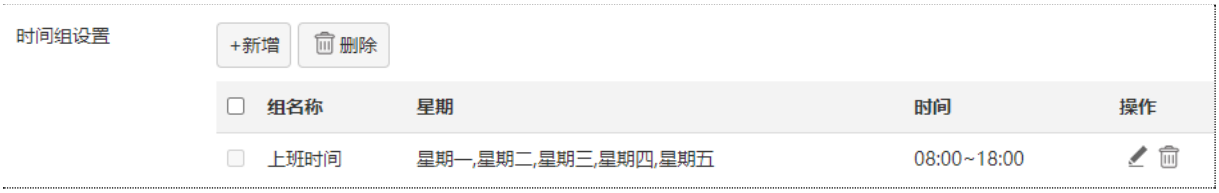


图4-18 配置时间组

步骤2 进入「行为管理」>「MAC 地址过滤」页面，开启 MAC 地址过滤功能。

1. MAC 地址过滤：选择“开启”；
2. 点击 确定 。

图4-19

步骤3 点击 +新增 ，在【新增】窗口配置 MAC 地址过滤规则参数。

1. 过滤规则：选择“允许访问互联网”。
2. 时间组：选择规则生效的时间组，本例为“上班时间”。
3. MAC 地址：输入采购人员电脑的物理地址，本例中为“CC:3A:61:71:1B:6E”。
4. 备注：设置本规则的备注，如“允许上网”。
5. 点击 确定 。

步骤4 取消勾选“允许未启用规则和列表外的主机访问互联网”；

步骤5 点击 确定 。

验证配置

在星期一~星期五的 8:00~18:00，局域网中，只有使用 MAC 地址为 CC:3A:61:71:1B:6E 的电脑的采购人员才能访问互联网，使用其他员工的电脑不能访问互联网。

4.5 端口过滤

进入页面的方法：点击「行为管理」>「端口过滤」。进入页面后，默认显示如下。

图4-20 端口过滤

4.5.2 配置端口过滤

开启端口过滤功能

步骤1 点击「行为管理」>「端口过滤」；

步骤2 选择“开启”端口过滤；

步骤3 点击 确定 。

图4-21 开启端口过滤

开启端口过滤功能后，您就可以配置端口过滤规则了。

配置端口过滤规则

新增规则

步骤1 点击「行为管理」>「端口过滤」；

步骤2 点击 +新增 ；

步骤3 在【新增】窗口配置各项参数；

步骤4 点击 确定 。

图4-22 新增端口过滤

表4-11 端口过滤参数说明

标题项	说明
IP 组	选择引用的 IP 组，以指定规则对应的用户。IP 组应事先已在「行为管理」>「IP 组和时间组」页面配置好。
时间组	选择引用的时间组，以指定规则对应的生效时间。 时间组应事先已在「行为管理」>「IP 组和时间组」页面配置好。
端口或端口段	禁止访问的服务使用的 TCP 或 UDP 端口号。
协议类型	禁止访问的服务使用的协议。“全部”表示 TCP 和 UDP。

规则添加成功后，您可以在「行为管理」>「端口过滤」页面查看到已添加的端口过滤规则。如下图示例。

图4-23 成功添加端口过滤

修改规则

步骤1 点击「行为管理」>「端口过滤」；

步骤2 如果要修改某条端口过滤规则，请点击操作栏的；如果要禁用/启用规则，请点击操作栏的 / 。

删除规则

步骤1 点击「行为管理」>「端口过滤」；

步骤2 如果要删除某条端口过滤规则，请点击对应操作栏的；如果要同时删除多个端口过滤规则，请选中要删除的多个规则，然后点击 删除 。

4.5.3 端口过滤配置举例

组网需求

某企业使用网关路由器进行网络搭建，现要禁止采购部门员工（其计算机 IP 地址为 192.168.0.2~192.168.0.100）在星期一到星期五的上班时间（8:00~18:00）浏览网页（浏览网页服务默认的端口号是 80）。

可以使用路由器的端口过滤功能实现上述需求。

配置步骤

步骤1 进入「行为管理」>「IP 组和时间组」页面，配置如下时间组；

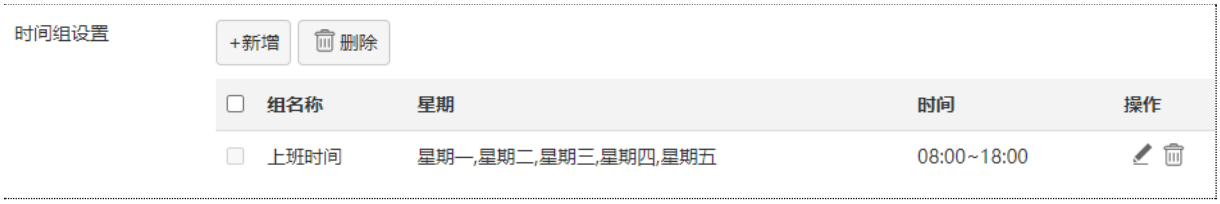


图4-24 时间组设置

步骤2 进入「行为管理」>「IP 组和时间组」页面，配置如下 IP 组；

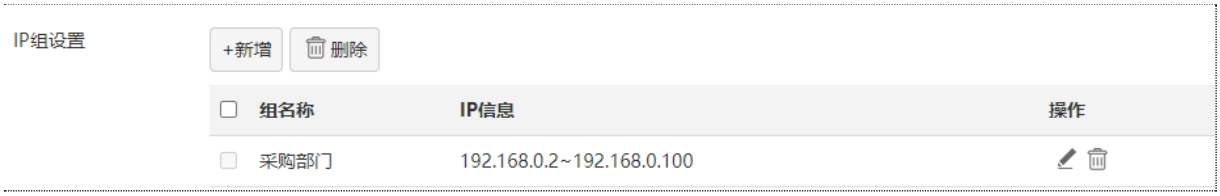


图4-25 IP 组设置

步骤3 进入「行为管理」>「端口过滤」页面，开启端口过滤功能；

1. 端口过滤：选择“开启”；
2. 点击 确定 。

图4-26 开启端口过滤

步骤4 点击 +新增 ，在【新增】窗口配置各项参数；

1. IP 组：选择规则生效的 IP 组，本例为“采购部门”；
2. 时间组：选择规则生效的时间组，本例为“上班时间”；
3. 端口或端口段：输入浏览网页服务使用的端口号“80”；
4. 协议：保持默认“全部”；
5. 点击 确定 。

图4-27 新增端口过滤

验证配置

在星期一~星期五的 8:00~18:00，局域网中，IP 地址为 192.168.0.2~192.168.0.100 的电脑不能浏览网页，其他电脑（IP 为 192.168.0.101~192.168.0.254）可以浏览网页。

4.6 网络应用过滤

进入页面的方法：点击「行为管理」>「网络应用过滤」。进入页面后，默认显示如下。

图4-28 网络应用过滤

网络应用过滤包括两部分功能：网络应用过滤、QQ 过滤。

4.6.1 配置网络应用过滤

开启网络应用过滤功能

步骤1 点击「行为管理」>「网络应用过滤」；

步骤2 选择“开启”网络应用过滤；

步骤3 点击 确定 。

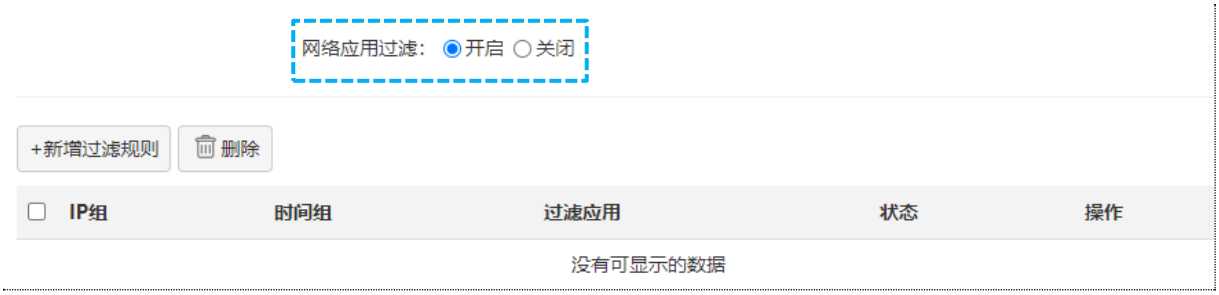


图4-29 开启网络应用过滤功能

开启网络应用过滤功能之后，您就可以配置网络应用过滤规则了。

配置网络应用过滤规则

新增规则

步骤1 点击「行为管理」>「网络应用过滤」；

步骤2 点击 +新增过滤规则 ；

步骤3 在【新增过滤规则】窗口配置各项参数；

步骤4 点击 确定 。

图4-30 新增网络过滤应用规则

表4-12 网络过滤规则参数说明

标题项	说明
IP 组	选择引用的 IP 组，以指定规则对应的用户。IP 组应事先已在「行为管理」>「IP 组和时间组」页面配置好。
时间组	选择引用的时间组，以指定规则对应的生效时间。 时间组应事先已在「行为管理」>「IP 组和时间组」页面配置好。
应用类别	选择要禁止的应用的类别。
请选择	选择要禁止的具体应用。

规则添加成功后，可以在「行为管理」>「网络应用过滤」页面查看到已添加的网络应用过滤规则。如下图示例。

图4-31 开启网络应用过滤

修改规则

步骤1 点击「行为管理」>「网络应用过滤」；

步骤2 如果要修改规则参数，请点击网络应用过滤规则列表里操作栏的；如果要禁用/启用规则，请点击操作栏的 / 。

删除规则

步骤1 点击「行为管理」>「网络应用过滤」；

步骤2 如果要删除某条规则，请点击网络应用过滤规则列表里操作栏的；如果要同时删除多个规则，请选中要删除的多个规则，然后点击 删除 。

4.6.2 配置 QQ 过滤

开启 QQ 过滤功能

步骤1 点击「行为管理」>「网络应用过滤」；

步骤2 选择“开启”QQ 过滤；

步骤3 点击 确定 。

图4-32 开启 QQ 过滤

开启 QQ 过滤功能后，路由器局域网的用户都不能使用 QQ 进行聊天，除非添加例外 QQ 号。只有例外 QQ 列表里的 QQ 号才能进行正常通讯。

配置例外 QQ 号

添加例外 QQ 号

步骤1 进入「行为管理」>「网络应用过滤」页面；

步骤2 点击 +新增例外 QQ 号 ；

步骤3 在【新增例外 QQ 号】窗口进行参数配置；

步骤4 点击 确定 。

图4-33 新增例外 QQ 号

表4-13 新增例外 QQ 号参数说明

标题项	说明
QQ 号	允许进行正常通讯的 QQ 号码。
备注	该例外 QQ 号的描述，如“zhangsan”。可不填。
操作	+ ：点击可以新增一条例外 QQ。 - ：点击可以删除本条例外 QQ 号。

例外 QQ 添加成功后，您可以在「行为管理」>「网络应用过滤」页面查看到已添加的例外 QQ 规则。如下图示例。

图4-34 成功添加例外 QQ 号

删除例外 QQ 号

步骤1 点击「行为管理」>「网络应用过滤」；

步骤2 如果要删除某个例外 QQ 号，请点击例外 QQ 列表里对应操作栏的 ；如果要同时删除多个例外 QQ 号，请选中要删除的多个规则，然后点击 删除 。

4.6.3 网络应用过滤+QQ 过滤配置举例

组网需求

某企业使用网关路由器进行网络搭建。要求采购部门（计算机 IP 地址为 192.168.0.2~192.168.0.100）在星期一到星期五的上班时间（8:00~18:00）不能：

使用这些应用：聊天、视频、音乐、金融、购物、社交、婚恋、手机游戏、网络游戏、对战平台。

使用 QQ，但允许某一员工使用 QQ 与客户沟通。假设该员工的 QQ 号为 12345678。

配置步骤

步骤1 进入「行为管理」>「IP 组和时间组」页面，配置如下时间组；

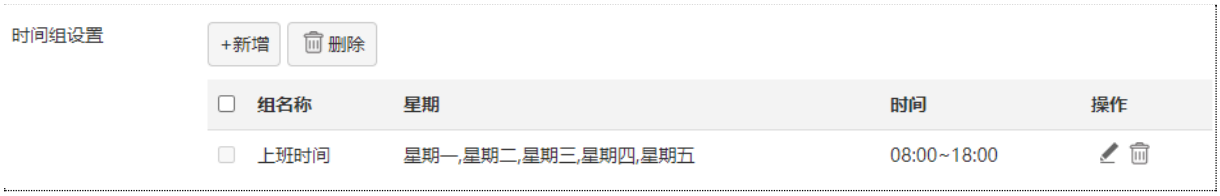


图4-35 配置时间组

步骤2 进入「行为管理」>「IP 组和时间组」页面，配置如下 IP 组；

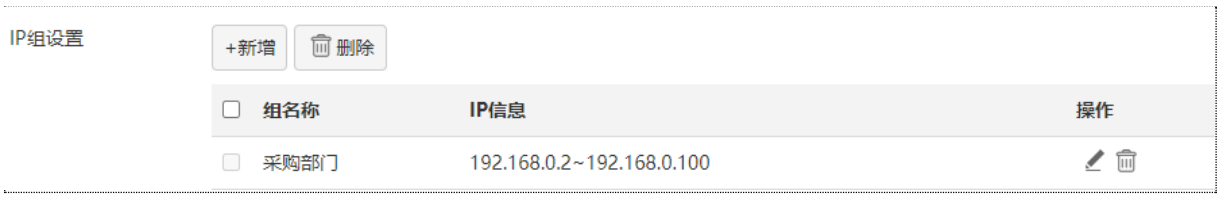


图4-36 配置 IP 组

步骤3 进入「行为管理」>「网络应用过滤」页面，开启网络应用过滤和 QQ 过滤功能；

1. 选择“开启”网络应用过滤和 QQ 过滤；
2. 点击页面底端的 确定 。

图4-37 开启网络应用过滤

步骤4 点击 +新增过滤规则 ，在【新增过滤规则】窗口配置各项参数；

1. IP 组：选择需要限制网络应用的 IP 组，本例为“采购部门”；
2. 时间组：选择规则生效的时间组，本例为“上班时间”；
3. 过滤应用：在“应用类别”栏选择聊天、视频、音乐、金融、购物、社交、婚恋、手机游戏、网络游戏、对战平台；
4. 点击 确定 。

图4-38 新增网络应用过滤规则

步骤5 点击 +新增例外 QQ 号 ，在【新增例外 QQ 号】窗口进行如下设置，然后点击 确定 。

图4-39 新增例外 QQ 号

验证配置

局域网中 192.168.0.2~192.168.0.100 的电脑在星期一到星期五的 8:00-18:00 不能使用聊天、视频、音乐、金融、购物、社交、婚恋、手机游戏、网络游戏、对战平台等应用，不能使用 QQ，只有 12345678 的 QQ 号可以正常使用。

4.7 网址分类过滤

进入页面的方法：点击「行为管理」>「网址分类过滤」。进入页面后，默认显示如下。

图4-40 网址分类过滤

4.7.2 配置网址分类过滤

开启网址分类过滤功能

步骤1 点击「行为管理」>「网址分类过滤」；

步骤2 选择“开启”网址分类过滤；

步骤3 点击 确定 。

图4-41 开启网址分类过滤

开启网址分类过滤功能后，您就可以配置网址分类过滤规则、自定义网址分类或查看某一类网址类型中包含的网址了。

配置网址分类规则

新增规则

步骤1 进入「行为管理」>「网址分类过滤」页面；

步骤2 点击 +新增 ；

步骤3 在【新增】窗口配置各项参数；

步骤4 点击 确定 。

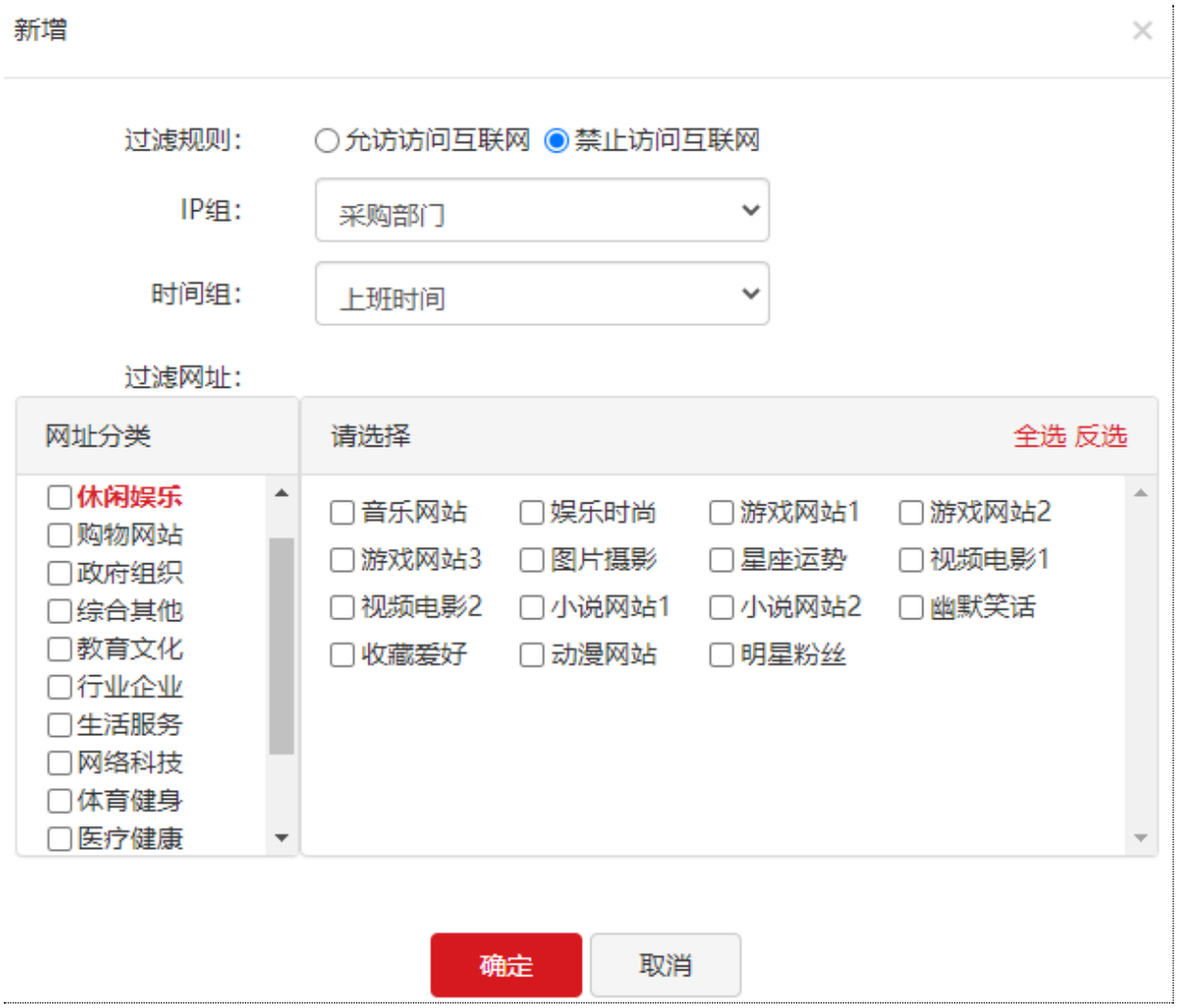


图4-42 新增网址分类过滤

表4-14 网址分类过滤参数说明

标题项	说明
过滤规则	网址分类过滤规则的类型。 ● 允许访问互联网（白名单）：允许 IP 组内的用户在对应时间段内访问指定的网站，不能访问其他网站；在其他时间段内可以访问所有网站。 ● 禁止访问互联网（黑名单）：禁止 IP 组内的用户在对应时间段内访问指定的网站，可以访问其他网站；在其他时间段内可以访问所有网站。
IP 组	选择引用的 IP 组，以指定规则对应的用户。IP 组应事先已在「行为管理」>「IP 组和时间组」页面配置好。
时间组	选择引用的时间组，以指定规则对应的生效时间。时间组应事先已在「行为管理」>「IP 组和时间组」页面配置好。
网址分类	选择要禁止的应用的网址类型。
请选择	选择要禁止的具体网址。

规则添加成功后，您可以在「行为管理」>「网址分类过滤」页面查看到已添加的网址分类过滤规则。如下图示例。

图4-43 成功添加网址分类过滤规则

修改规则

步骤1 点击「行为管理」>「网址分类过滤」；

步骤2 如果要修改某条网址分类过滤规则，请点击网址分类过滤列表里对应操作栏的 ；如果要禁用/启用规则，请点击操作栏的 / 。

删除规则

步骤1 点击「行为管理」>「网址分类过滤」；

步骤2 如果要删除某条网址分类过滤规则，请点击网址分类过滤列表里对应操作栏的 ；如果要同时删除多个网址分类过滤规则，请选中要删除的多个规则，然后点击 删除 。

自定义网址分类

如果系统自带的网址分类里未包含您需要过滤的网址，您还可以自定义网址分类。

新增网址分类

步骤1 点击「行为管理」>「网址分类过滤」，找到“网址分类管理”模块；

步骤2 点击 网址分类管理 ；

步骤3 在“网址分类管理”页面点击 +新增分类 ；

图4-44 网址分类管理

步骤4 在【新增分类】窗口配置各项参数；

步骤5 点击 确定 。

图4-45 新增网址分类

表4-15 新增分类参数说明

标题项	说明
组名称	设置新增分类的名称。
加入网址	该分类所包含的网址 URL 及其描述信息。 新增分类时，只需先输入一条 URL。如果有其他 URL 需加入此分类，请参考修改网址分类。

成功新增网址分类后，可以在“网址分类管理”页面查看到已添加的网址分类。如下图示例。

图4-46 成功添加网址分类

修改网址分类

您只能修改自定义的网址分类，不能修改系统自带的网址分类。

修改方法:

步骤1 点击「行为管理」>「网址分类过滤」；

步骤2 点击 网址分类管理 ；

步骤3 点击要修改的自定义网址分类；

步骤4 在出现的窗口修改。

图4-47 网址管理

说明

如果修改的网址分类已经被引用，则修改后，将自动引用修改后的网址分类。

删除网址分类

您只能删除自定义的网址分类，不能删除系统自带的网址分类。

删除方法：

步骤1 点击「行为管理」>「网址分类过滤」；

步骤2 点击 网址分类管理 ；

步骤3 将鼠标放在要删除的自定义网址分类上面；

步骤4 对应网址分类的右上角将出现图标，点击该图标即可。

说明

使用中的网址分类不可删除。

查看某一类网址类型中包含的网址

步骤1 点击「行为管理」>「网址分类过滤」；

步骤2 点击 网址分类管理 ；

步骤3 点击要查看的网址类型，如“音乐网站”，如下图示例。

图4-48 网址管理

4.7.3 网址分类过滤配置举例

组网需求

某企业使用网关路由器进行网络搭建。要求局域网中采购部（IP 地址范围为 192.168.0.2~192.168.0.100）的计算机在星期一到星期五的上班时间（8:00~18:00）只能访问网络科技网站，不能访问其他类型网站。

配置步骤

步骤1 配置时间组；

进入「行为管理」>「IP 组和时间组」页面，配置如下时间组。

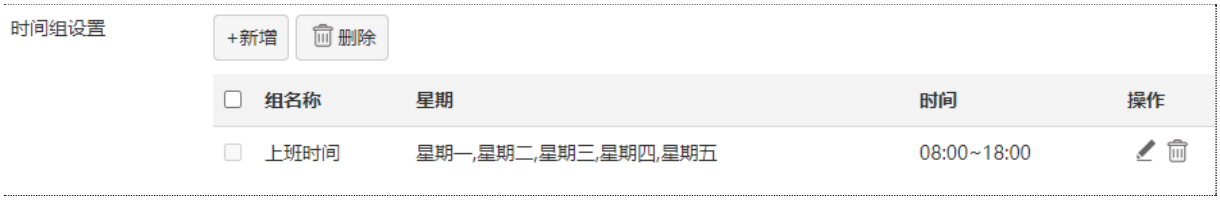


图4-49 时间组设置

步骤2 配置 IP 组；

进入「行为管理」>「IP 组和时间组」页面，配置如下 IP 组。

图4-50 IP 组设置

步骤3 开启网址分类过滤；

1. 点击「行为管理」>「网址分类过滤」；
2. 选择“开启”网址分类过滤；
3. 点击 确定 。

图4-51 开启网址分类过滤

步骤4 新增网址分类过滤规则。

1. 进入「行为管理」>「网址分类过滤」页面；
2. 点击 +新增 ；
3. 在【新增】窗口设置下述参数；
4. 过滤规则：选择“允许访问互联网”。
5. IP 组：选择要限制访问网址类型的计算机所属的 IP 组，本例为“采购部门。
6. 时间组：选择规则生效的时间组。
7. 过滤网址：选择要过滤的网址类型，本例为“网络科技”。
8. 点击 确定 。

图4-52 新增网址分类过滤

添加成功。

图4-53 成功添加网址分类过滤

验证配置

局域网中 192.168.0.2~192.168.0.100 的电脑在星期一到星期五的 8:00-18:00 只能访问路由器中“网络科技”包含的网站，不能访问其他网站。

4.8 多 WAN 策略

进入页面的方法：点击「行为管理」>「多 WAN 策略」。进入页面后，默认显示如下。

图4-54 多 WAN 策略

表4-16 多 WAN 策略参数说明

标题项	说明
多 WAN 策略	路由器 WAN 口的策略。 ● 智能负载均衡：系统自动寻找流量最小的 WAN 口通信，完全不用人工干预，自动分配流量。 ● 基于源 IP 与目的 IP 的负载均衡：在保持用户对同一目标的访问从同一 WAN 口出去的前提下，根据线路带宽，自动分配数据流量，提升带宽的利用率；选择此项可避免一些特殊应用服务因数据通过多个 WAN 转发出现异常，一般不建议开启。 ● 自定义策略：用户根据实际需要，针对特定的源地址指定对应的 WAN 口。
广域网线路侦测	开启后，路由器会定期检测 WAN 口与“侦测地址”的连通情况。 ● 侦测地址：需侦测的 IP 或域名。 ● 侦测间隔：侦测时间间隔，默认为 5 分钟侦测一次。

4.8.2 自定义多 WAN 策略

开启自定义多 WAN 策略功能

步骤1 点击「行为管理」>「多 WAN 策略」；

步骤2 选择“自定义策略”；

步骤3 点击 确定 。

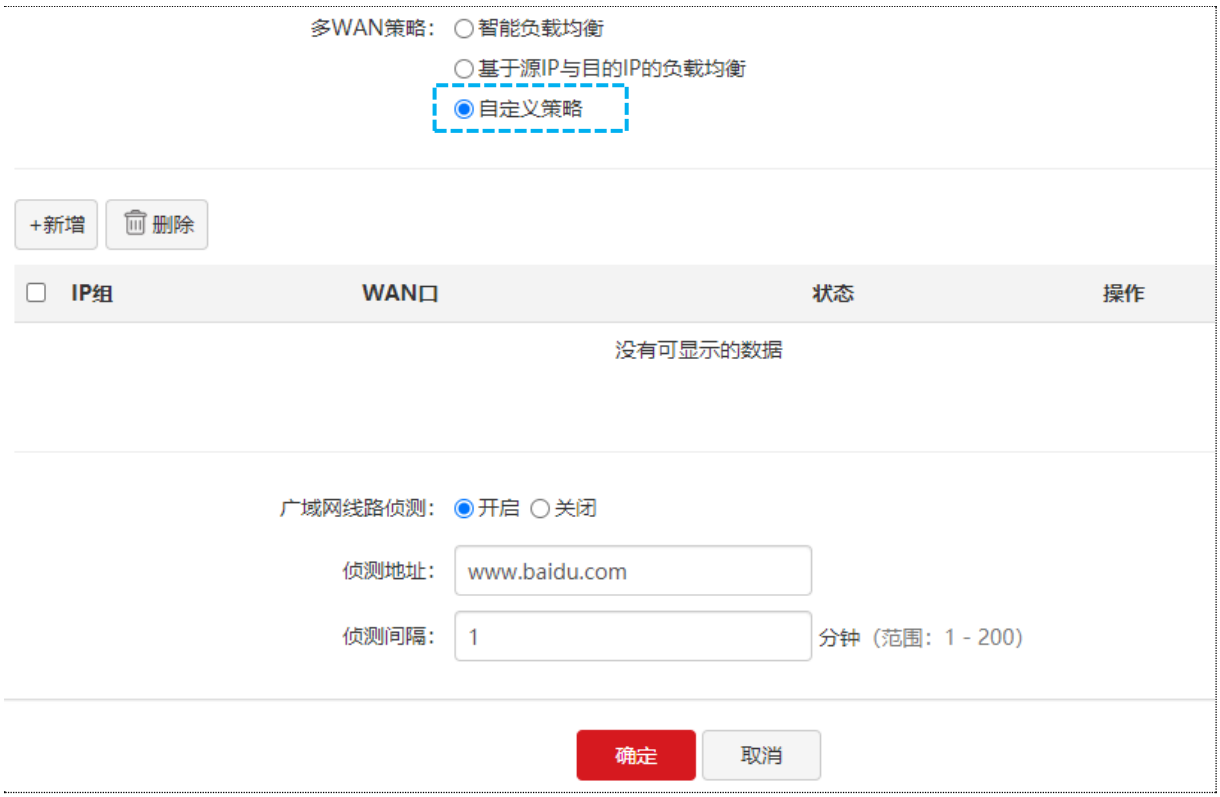


图4-55 自定义多 WAN 策略

开启自定义多 WAN 策略功能后，您就可以自定义多 WAN 策略规则了。

自定义多 WAN 策略规则

新增规则

步骤1 点击「行为管理」>「多 WAN 策略」；

步骤2 点击 +新增 ；

步骤3 在【新增】窗口进行参数配置；

步骤4 点击 确定 。

图4-56 新增多 WAN 策略

表4-17 多 WAN 策略参数说明

标题项	说明
IP 组	选择引用的 IP 组，以指定规则对应的用户。IP 组应事先在「行为管理」>「IP 组和时间组」页面配置。
指定 WAN 口	对应 IP 组数据流量使用的 WAN 口。

成功添加自定义多 WAN 策略规则后，可以在「行为管理」>「多 WAN 策略」页面查看到已添加的自定义策略规则。如下图示例。

图4-57 成功添加多 WAN 策略

修改规则

步骤1 点击「行为管理」>「多 WAN 策略」；

步骤2 如果要修改某条自定义多 WAN 策略规则，请点击对应操作栏的 ；如果要禁用/启用规则，请点击操作栏的 / 。

删除规则

步骤1 点击「行为管理」>「多 WAN 策略」；

步骤2 如果要删除某条自定义多 WAN 策略规则，请点击对应操作栏的 ；如果要同时删除多个规则，请选中要删除的多个规则，然后点击 删除 。

4.8.3 自定义多 WAN 策略配置举例

组网需求

某企业使用网关路由器进行网络搭建，为了满足企业网络需求，办理了两条宽带线路（中国电信和中国移动），并且已经成功访问互联网。为了实现负载均衡，现要求局域网中：

- IP 地址为 192.168.0.2~192.168.0.100 的计算机通过电信宽带访问互联网。

● IP 地址为 192.168.0.101~192.168.0.250 的计算机通过移动宽带访问互联网。

可以使用路由器的多 WAN 策略功能实现上述需求。

网络拓扑

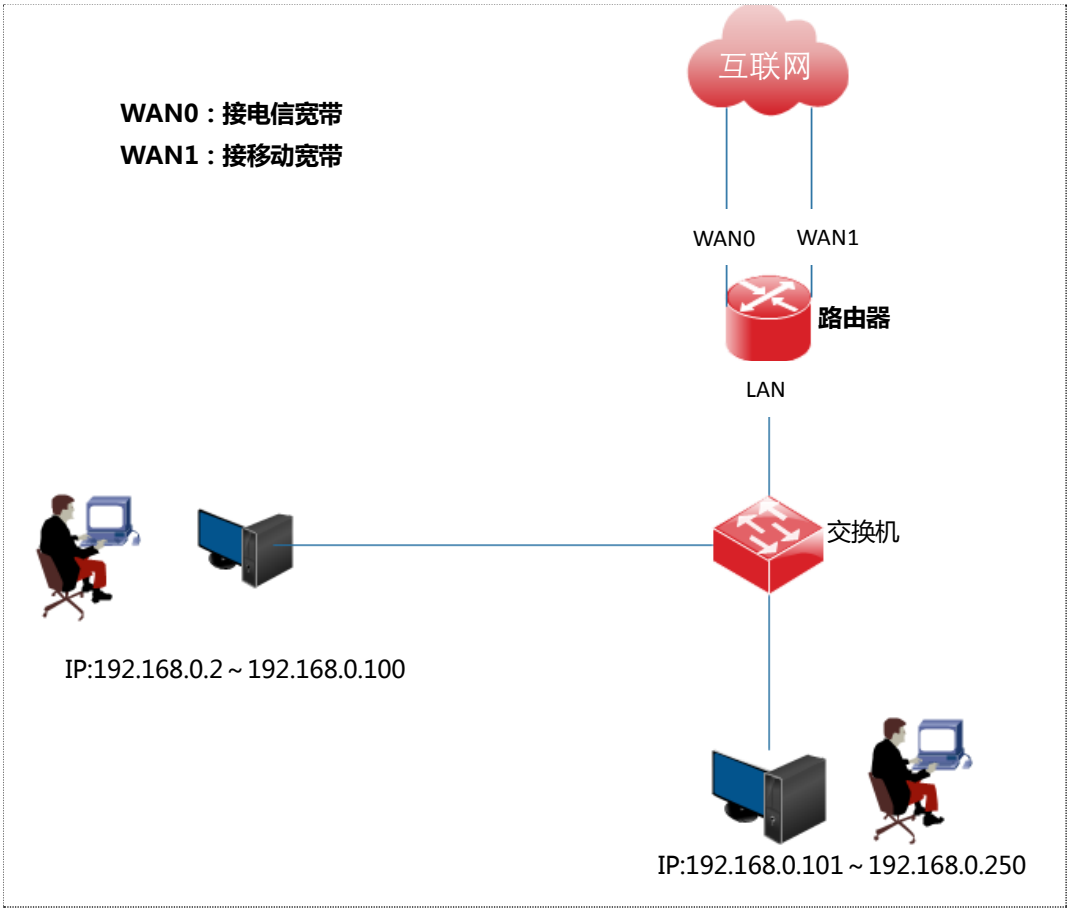
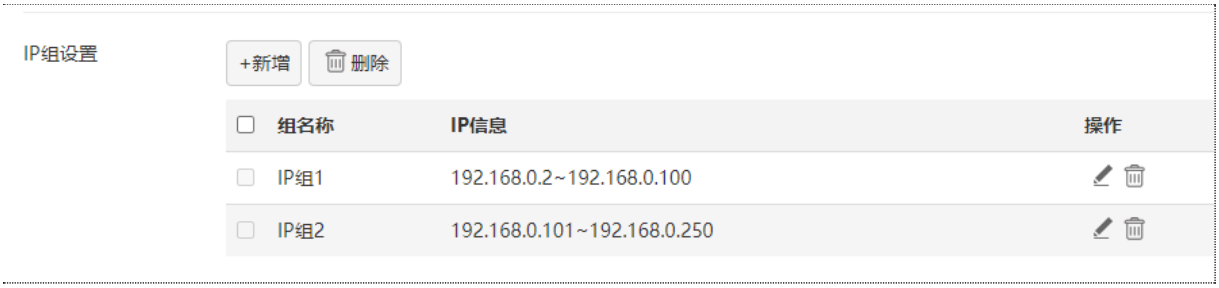


图4-58 自定义多 WAN 策略配置

配置步骤

步骤1 配置 IP 组；

进入「行为管理」>「IP 组和时间组」页面，配置如下 IP 组。



步骤2 自定义多 WAN 策略。

1. 开启自定义多 WAN 策略功能。
2. 点击「行为管理」>「多 WAN 策略」，选择“自定义策略”，点击 确定 。

图4-59 开启自定义多 WAN 策略

配置如下多 WAN 策略。

图4-60 成功添加多 WAN 策略

验证配置

局域网中 192.168.0.2~192.168.0.100 设备的数据将会走 WAN0 口；
192.168.0.101~192.168.0.250 设备的数据将会走 WAN1 口。

第5章 网速控制

5.1 概述

外网带宽总是有限的，因此，网络管理员需要对用户进行网速控制，使有限的带宽资源得到合理分配，以有效利用外网资源。

5.1.1 功能介绍

路由器支持以下两种网速控制方式。

- 智能限速

  路由器根据网络管理员在「网速控制」页面设置的“WAN 口带宽”，智能地给局域网用户分配带宽。

  使用智能限速时，网络管理员务必首先在「网速控制」页面的“带宽”正确输入其办理的宽带带宽，否则，智能限速功能可能会产生误差。

- 单独限速

  网络管理员根据实际环境需要，手动设置网速控制规则。设置“单独限速”时，可以设置 IP 组内的用户在一段时间内共享或独享所设置的上传/下载速率,指定单台并发连接数等。相比智能限速而言，单独限速更加灵活，但智能限速设置更加简单方便。

5.1.2 配置向导

- 智能限速

表5-1 智能限速参数说明

配置任务	说明
设置 WAN 口带宽	在「网速控制」页面进行配置。
启用智能限速	在「网速控制」页面，选择“智能限速”，然后点击 确定 。

- 单独限速

表5-2 单独限速参数说明

配置任务	说明
设置时间组	设置“单独限速”规则时，需要调用时间组。在「行为管理」>「IP 组和时间组」页面进行。
设置 IP 组	设置“单独限速”规则时，需要调用 IP 组。在「行为管理」>「IP 组和时间组」页面进行。
配置单独限速	在「网速控制」页面进行。

5.2 配置网速控制

进入页面的方法：点击「网速控制」。进入页面后，默认显示如下，可根据需要设置 WAN 口带宽。下文主要介绍单独限速。

图5-1 网速控制

5.2.2 开启智能限速功能

步骤1 点击「网速控制」；

步骤2 在“网速控制”模块选择“智能限速”；

步骤3 点击 确定 。

图5-2 开启智能限速功能

5.2.3 设置单独限速

新增规则

步骤1 点击「网速控制」；

步骤2 在“网速控制”模块选择“单独限速”；

步骤3 点击 +新增 ；

步骤4 在【新增】窗口配置各项参数；

步骤5 点击 确定 。

图5-3 新增规则

表5-3 网速控制参数说明

标题项	说明
IP 组	选择引用的 IP 组，以指定规则对应的用户。IP 组应事先已在「行为管理」>「IP 组和时间组」页面配置好
时间组	选择引用的时间组，以指定规则对应的生效时间。时间组应事先已在「行为管理」>「IP 组和时间组」页面配置好。
单台设备并发连接数	受控 IP 地址范围中，每台用户设备所能使用的最大连接数。若无特殊需求，建议设置为 300。
模式	设置网速控制的模式。 ● 共享：受控 IP 地址范围内的所有用户共享所设置的上传/下载速率。此模式下，每个受控用户所获得的带宽可能不一样。 ● 独享：受控 IP 地址范围内的每个用户独享所设置的上传/下载速率。此模式下，每个受控用户所获得的带宽都是一样的。
上传速率	限制的上传/下载速率
下载速率	

成功添加“单独限速”规则后，可以在「网速控制」页面查看到已添加的规则。如下图示例。

图5-4 成功添加单独限速

修改规则

1. 点击「网速控制」；
2. 如果要修改规则参数，请点击规则列表里操作栏的；如果要禁用/启用规则，请点击操作栏的 / 。

删除规则

步骤1 点击「网速控制」；

步骤2 如果要删除某条规则，请点击规则列表里操作栏的；如果要同时删除多个规则，请选中要删除的多个规则，然后点击 删除 。

5.2.4 配置未受控主机的流控参数

设置“单独限速”时，还可以指定“未受控主机”的流控参数。未受控主机，即，IP 地址不在流控规则列表里的用户设备或列表中未启用规则的设备。

如果不勾选“未受控主机默认为”，表示不限制未受控主机的带宽和最大并发连接数。

图5-5 未受控主机的留空参数

设置完成后，请点击 确定 保存。

5.3 单独限速配置举例

组网需求

某企业使用网关路由器进行网络搭建，要求：局域网中采购部（IP 地址为 192.168.0.2~192.168.0.100）的每个员工在星期一到星期五的上班时间（8:00~18:00）都能使用 1Mbps 的固定上下行带宽。对于局域网其他计算机，不限制使用带宽。

可以使用路由器的“单独限速”功能实现上述需求。假设每台用户设备的并发连接数为 300。

配置步骤

步骤1 配置时间组；

进入「行为管理」>「IP 组和时间组」页面，配置如下时间组。

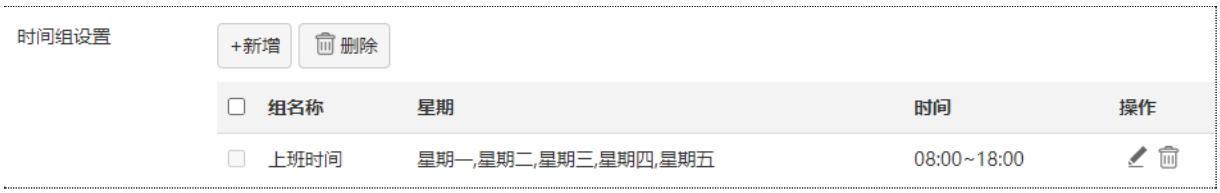


图5-6 配置时间组

步骤2 配置 IP 组；

进入「行为管理」>「IP 组和时间组」页面，配置如下 IP 组。

图5-7 配置 IP 组进入「行为管理」>「IP 组和时间组」页面，配置如下 IP 组；

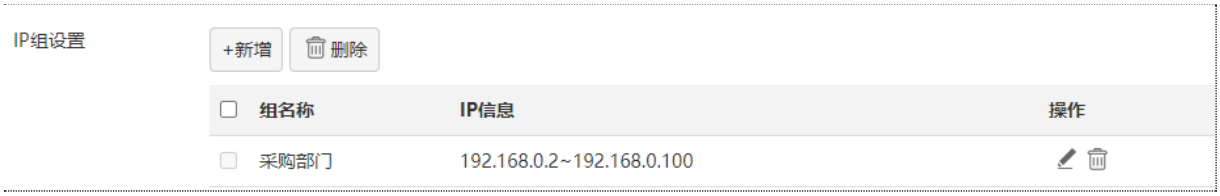


图5-8 IP 组设置

步骤3 启用“单独限速”功能；

点击「网速控制」，在“网速控制”模块选择“单独限速”，然后点击 确定 。

图5-9 单独限速

步骤4 设置“单独限速”规则。

1. 进入“网速控制”页面，点击 +新增 ；
2. 在【新增】窗口配置下述参数；
3. IP 组：点击下拉框，选择规则应用的 IP 组，本例为“采购部”。

4. 时间组：点击下拉框，选择规则应用的时间组，本例为“上班时间”。
5. 单台设备并发连接数：设置单个客户端并发连接数，本例为“300”。
6. 模式：选择“独享”。
7. 上传/下载速率：设置客户端的最大上传/下载速率，本例为“128KB/s”。
8. 点击 确定 。

图5-10 新增单独限速

配置验证

IP 地址为 192.168.0.2~192.168.0.100 的用户，在星期一到星期五的 8:00~18:00 的最大上传速率为 128KB/s，最大下载速率为 128KB/s。

第6章 VPN 服务

6.1 概述

路由器的「VPN 服务」模块包括：PPTP/L2TP 客户端、PPTP/L2TP 服务器、IPSec。

6.1.1 功能介绍

VPN（Virtual Private Network，虚拟专用网），是一个建立在公用网（通常是互联网）上的专用网络，这个专用网络只在逻辑上存在，并没有实际物理线路。使用 VPN 技术，可以让企业的分公司员工在方便共享对方或公司总部局域网资源的同时，保证这些资源不会暴露给互联网上的其他用户。

6.1.2 网络拓扑

VPN 典型网络拓扑图如下。

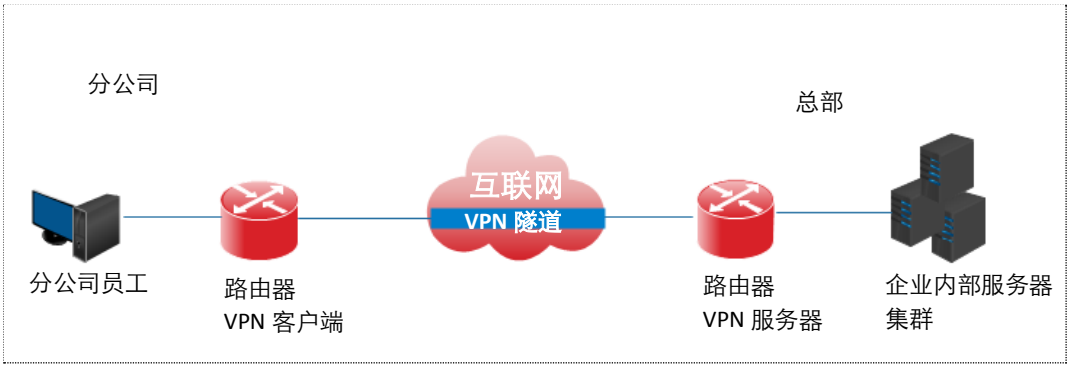


图6-1 VPN 服务

6.1.3 VPN 类型

路由器支持三种 VPN：PPTP、L2TP、IPSec。

- PPTP/L2TP

  PPTP（Point to Point Tunneling Protocol，点到点隧道协议）和 L2TP（Layer 2 Tunneling Protocol，第二层隧道协议）都是二层 VPN 隧道协议，使用 PPP（Point to Point Protocol，点到点协议）进行数据封装，并都为数据增添额外首部。

  本路由器既可作为 PPTP/L2TP 客户端，也可作为 PPTP/L2TP 服务器。

- IPSec

  IPSec（IP Security，IP 安全性）是一系列协议的集合，用来实现在互联网上安全、保密地传送数据。

6.1.4 IPSec 相关概念

- 封装模式

封装模式，即 IPSec 传输的数据的封装模式。IPSce 支持“隧道模式”和“传输模式”两种封装模式。

- 隧道（tunnel）模式：增加新的 IP 头，通常用于两个安全网关之间的通讯。用户的整个 IP 数据包被用来计算 AH 或 ESP 头，AH 或 ESP 头以及 ESP 加密的用户数据被封装在一个新的 IP 数据包中。
- 传输（transport）模式：不改变原有的 IP 头部，通常用于主机和主机之间的通信。只是传输层数据被用来计算 AH 或 ESP 头，AH 或 ESP 头以及 ESP 加密的用户数据被放置在原 IP 包头后面。

- 安全网关

  指具有 IPSec 功能的网关设备（安全加密路由器），安全网关之间可以利用 IPSec 对数据进行安全保护，保证数据不被偷窥和篡改。

- IPSec 对等体

  IPSec 的两个端点被称为 IPSec 对等体，要在两个对等体（安全网关）之间安全传输数据，首先要在两者之间建立安全联盟（Security Association，SA）。

- SA

  SA 是通信对等体间对某些要素的约定。如，使用哪种协议（AH、ESP 还是两者结合）、协议的封装模式（传输模式、隧道模式）、加密算法（DES、3DES、AES）、特定流中保护数据的共享密钥以及密钥的生命周期等。SA 具有以下特征：

  - 由{SPI，IP 目的地址，安全协议标识符}三元组唯一标识。
  - 它决定了对报文进行何种处理：协议、算法、密钥。
  - 每个 IPSec SA 都是单向的，并且是具有生命周期的。
  - SA 可以手工建立或由 IKE（Internet Key Exchange，互联网密钥交换）协商生成。

6.2 配置 VPN

6.2.1 PPTP/L2TP 客户端

路由器支持 PPTP/L2TP 客户端功能，可以连接到 PPTP/L2TP 服务器端。如：企业分支机构与企业总部之间需要实现简单安全的信息互访，可以在企业总部架设 PPTP/L2TP 服务器，再在分支机构出口路由器上使用 PPTP/L2TP 客户端进行连接。

开启 PPTP/L2TP 客户端：

步骤1 点击「VPN 服务」>「PPTP/L2TP 客户端」；

步骤2 PPTP/L2TP 客户端：选择“开启”；

步骤3 设置各项展开参数；

步骤4 点击 确定 。

图6-2 PPTP/L2TP 客户端

表6-1 PPTP/L2TP 客户端参数说明

标题项	说明
PPTP/L2TP 客户端	开启/关闭“PPTP/L2TP 客户端”。开启后，路由器作为 PPTP/L2TP VPN 客户端。
客户端类型	路由器充当的客户端类型，PPTP 或 L2TP。 ● PPTP：要连接的 VPN 服务器是 PPTP 服务器时，选择此项。 ● L2TP：要连接的 VPN 服务器是 L2TP 服务器时，选择此项。
WAN 口	选择路由器进行 VPN 拨号时使用的 WAN 口。
服务器 IP/域名	要拨入的 VPN 服务器的 IP 地址或域名，一般是对端 VPN 路由器上开启了“PPTP/L2TP 服务器”功能的 WAN 口的 IP 地址或域名。
用户名	输入 PPTP/L2TP 用户账号，即，VPN 服务器分配的用户名和密码
密码	
加密	根据 VPN 服务器配置选择是否启用 128 位数据加密。请保证和服务器配置保持一致，否则不能正常通信。只有 PPTP VPN 才支持此选项，L2TP VPN 不支持。
VPN 代理上网	开启后，局域网内的计算机通过 PPTP/L2TP 服务器端路由器上网。
服务器内网网段	PPTP/L2TP 服务器端局域网的网段。
状态	显示当前 VPN 客户端的连接状态。

6.2.2 PPTP/L2TP 服务器

路由器支持 PPTP/L2TP 服务器功能，可以接受 PPTP/L2TP 客户端拨入。如：企业分支机构与企业总部之间需要实现简单安全的信息互访，可以在企业总部架设 PPTP/L2TP 服务器，再在分支机构出口路由器上使用 PPTP/L2TP 客户端进行连接。

进入页面的方法：点击「VPN 服务」>「PPTP/L2TP 服务器」。进入页面后，默认显示如下。

图6-3 PPTP/L2TP 服务器

配置 PPTP/L2TP 服务器需要两步：开启 PPTP/L2TP 服务器、配置 PPTP/L2TP 用户账号。

开启 PPTP/L2TP 服务器

步骤1 点击「VPN 服务」>「PPTP/L2TP 服务器」，找到“PPTP/L2TP 服务器”模块；

步骤2 服务器状态：选择“开启”；

步骤3 设置其他各项参数；

步骤4 点击页面底端的 确定 。

图6-4 PPTP/L2TP 服务器

表6-2 PPTP/L2TP 服务器参数说明

标题项	说明
服务器状态	开启/关闭“PPTP/L2TP”服务器功能。开启后，路由器作为 PPTP/L2TP VPN 服务器。
服务器类型	路由器充当的服务器类型，PPTP 服务器或 L2TP 服务器。 ● PPTP 服务器：此时，VPN 客户端需要使用 PPTP 客户端进行连接。 ● L2TP 服务器：此时，VPN 客户端需要使用 L2TP 客户端进行连接。
WAN 口	指定 PPTP/L2TP 服务器与客户端建立 VPN 隧道的出口。该 WAN 口的 IP 地址或域名是 PPTP/L2TP 客户端的“服务器 IP 地址/域名”。
加密	只有 PPTP VPN 才支持此选项，L2TP VPN 不支持。是否启用 128 位数据加密。注意客户端设置需与服务器端保持一致，否则将不能正常通信。
IPSec 加密	只有 L2TP VPN 才支持此选项，PPTP VPN 不支持。是否启用 IPSec 加密，如果要进行 IPSec 加密，需要选择在“IPSec”页面已建立的 IPSce 规则。
地址池网段	PPTP/L2TP 客户端通过 VPN 拨进来以后，服务器给它分配的 IP 地址范围。
最大连接数	PPTP/L2TP 服务器最多支持同时拨入的 VPN 客户端数量。系统固定为 32 个。

配置 PPTP/L2TP 用户账号

配置 PPTP/L2TP 用户账号。开启 PPTP/L2TP 服务器时，VPN 用户需要使用该用户账号拨入路由器的 VPN。

新增用户

步骤1 点击「VPN 服务」>「PPTP/L2TP 服务器」，找到“PPTP/L2TP 用户”模块；

步骤2 点击 +新增 ；

步骤3 在【新增】窗口配置各项参数；

步骤4 点击 确定 。

图6-5 新增 PPTP/L2TP 用户

表6-3 PPTP/L2TP 用户参数说明

标题项	说明
用户名/密码	VPN 用户进行 PPTP/L2TP 拨号（VPN 连接）时需要输入的用户名/密码。
是否网段	VPN 客户端网络情况。 ● 是：VPN 客户端是一个网络时选择。此时，还需设置“网段”、“掩码”参数。 ● 否：VPN 客户端是一台计算机。
网段	输入客户端的内网网络号。客户端是一个网络时设置。
子网掩码	输入客户端的内网网络的子网掩码。客户端是一个网络时设置。
备注	该账号的描述信息。可不填。

成功添加 PPTP/L2TP 用户后，可以在「VPN 服务」>「PPTP/L2TP 服务器」页面查看已添加的 PPTP/L2TP 用户账号。如下图示例。

图6-6 成功添加 PPTP/L2TP 用户

修改用户

步骤1 点击「VPN 服务」>「PPTP/L2TP 服务器」，找到“PPTP/L2TP 用户”模块；

步骤2 点击操作栏的 。

删除用户

步骤1 点击「VPN 服务」>「PPTP/L2TP 服务器」，找到“PPTP/L2TP 用户”模块；

步骤2 如果要删除某个 PPTP/L2TP 用户账号，请点击操作栏的 ；如果要同时删除多个账号，请选中要删除的多个账号，然后点击 删除 。

6.2.3 IPSec

进入页面的方法：点击「VPN 服务」>「IPSec」。

进入页面后，默认显示如下。

图6-7 IPSec

新建 IPSec 连接

隧道模式

点击 +新增 可以添加 IPSec 隧道连接。

本路由器支持“隧道模式”和“传输模式”两种封装模式，默认为“隧道模式”，如下所示。


新增
IPSec: 开启 关闭
封装模式: 隧道模式
WAN口: WAN0
连接名称:
隧道协议: ESP
远端网关地址:
本地内网网段/掩码: 如：192.168.100.0/24
远端内网网段/掩码: 如：192.168.100.0/24
密钥协商方式: 自动协商
认证方式: 共享密钥模式
预共享密钥:
显示高级设置...
确定
取消

图6-8 新增 IPSec

表6-4 IPSec 参数说明

标题项	说明
IPSec	开启/关闭 IPSec 功能。
封装模式	选择 IPSec 数据的封装模式。 隧道模式通常用于两个安全网关之间的通讯；传输模式通常用于主机和主机、主机与网关之间的通信。
WAN 口	指定 IPSec 在本侧使用的接口，IPSec 对端设备的“远端网关地址”需填为此接口的 IP 地址。
连接名称	设置该 IPSec 连接的名称描述。
隧道协议	选择为 IPSec 提供安全服务的协议。 ● AH：Authentication Header，鉴别首部。该协议主要提供数据完整性校验功能，若数据报文在传输过程中被篡改，则接收方将在完整性验证时丢弃该报文。 ● ESP：Encapsulating Security Payload，封装安全性载荷。该协议可以对数据的完整性进行检查，还对数据进行加密，这样，即使报文在传输过程中被截获，截取方也难以获取到真实信息。 ● AH+ESP：同时使用上述两种协议。
远端网关地址	填写 IPSec 隧道对端网关的 IP 地址或域名。
本地内网网段/掩码	填写本路由器局域网的网段/掩码。如本路由器的 LAN 口 IP 为 192.168.0.252，子网掩码为 255.255.255.0，则本地内网网段/掩码可填为 192.168.0.0/24。
远端内网网段/掩码	填写 IPSec 隧道对端网关局域网的网段/掩码。若对端是移动单机用户，则此参数设置为“该设备的 IP 地址/32”。

标题项	说明
密钥协商方式	建立 IPSec 安全隧道的密钥协商方式。默认为“自动协商”。 ● 自动协商：通过 IKE 自动建立 SA，并进行动态维护、删除，降低了手工配置的复杂度，简化 IPSec 的使用、管理工作。自动建立的 SA 有生命周期，会定时更新，增强了安全性。 ● 手动设置：需要用户手动设置加密/认证算法及密钥来建立 SA。手动建立的 SA 没有生命周期限制，除非手工删除，否则永不过期，因此有安全隐患。该方式常用于调试阶段。

密钥协商方式--自动协商

自动协商时，为了保证信息的私密性，IPSec 通信双方需要使用彼此都知道的信息来对数据进行加密和解密，所以在通信建立之初双方需要协商安全性密钥，这一过程便由 IKE 完成。IKE 是 ISAKMP、Oakley、SKEME 这三个协议的混合体。

- ISAKMP：Internet Security Association and Key Management Protocol，互联网安全性关联和密钥管理协议，该协议为交换密钥和 SA 协商提供了一个框架。
- Oakley：密钥确定协议，该协议描述了密钥交换的具体机制。
- SKEME：安全密钥交换机制，该协议描述了与 Oakley 不同的另一种密钥交换机制。

IKE 协商过程分为两个阶段：

- **阶段 1：**通信双方将协商交换验证算法、加密算法等安全提议，并建立一个 ISAKMP SA，用于在阶段 2 中安全交换更多信息。
- **阶段 2：**使用阶段 1 中建立的 ISAKMP SA 为 IPSec 的安全性协议协商参数，创建 IPSec SA，用于对双方的通信数据进行保护。

密钥协商方式为“自动协商”时，如下图。

图6-9 自动协商

表6-5 自动协商参数说明

标题项	说明
认证方式	显示为“共享密钥”，表示 IPSec 双方事先通过某种方式协商好一个双方共享的密钥字符串。
预共享密钥	输入协商时所用的预共享密钥，需要保持与对端网关设备一致。最长为 128 字符。

点击**显示高级设置**可显示自动协商的高级参数。点击后，页面如下图示。

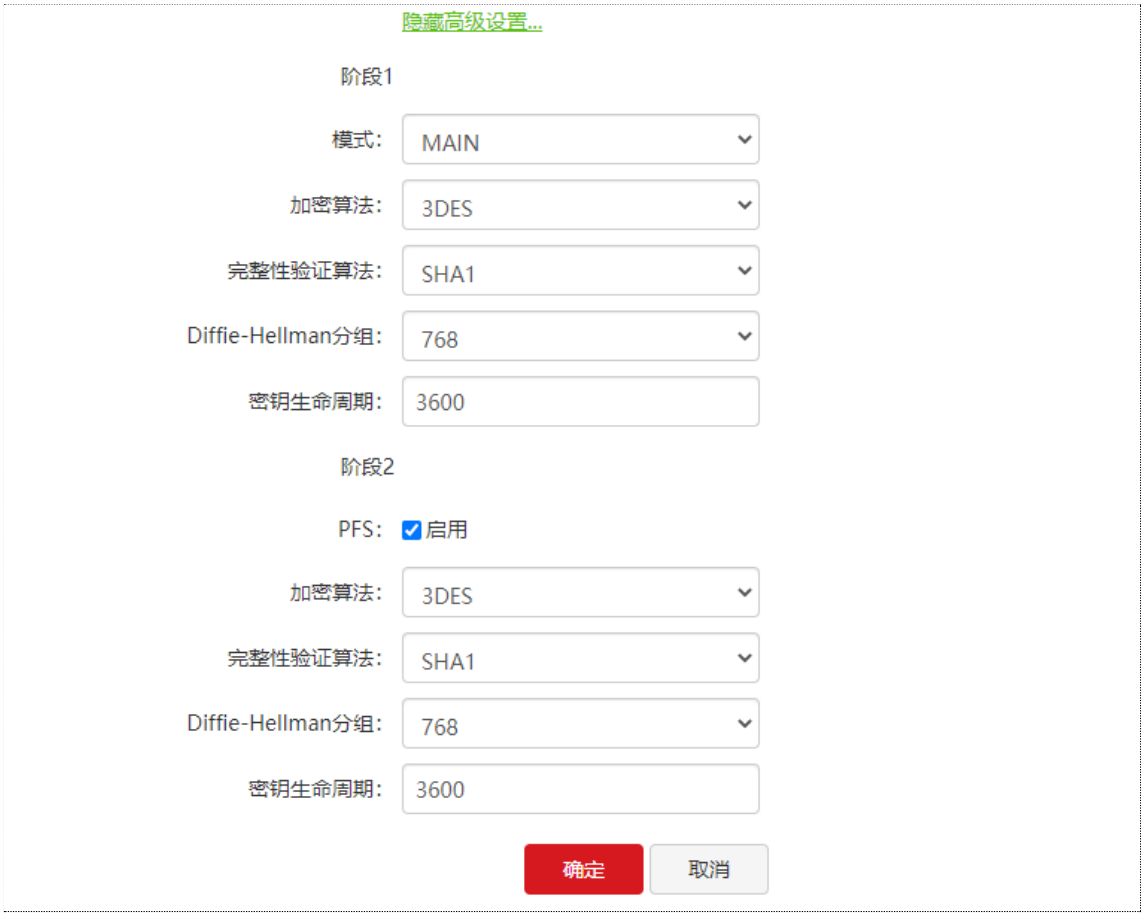


图6-10 高级设置

表6-6 高级设置参数说明

标题项	说明
模式	设置 IKE 阶段 1 的交换模式，该交换模式必须与对端设置相同。 ● MAIN：主模式，该模式双方交换报文多，提供身份保护，适用于对身份保护要求较高的场合。 ● AGGRESSIVE：野蛮模式，又称主动模式，该模式不提供身份保护，双方交换报文少，协商速度快，适用于对身份保护要求不高的场合。
加密算法	选择应用于 IKE 会话的加密算法。本路由器支持以下加密算法： ● DES（Data Encryption Standard，数据加密标准）：使用 56bit 的密钥对 64bit 数据进行加密，64bit 的最后 8 位用于奇偶校验。3DES 则为三重 DES，使用三个 56bit 的密钥进行加密。 ● AES（Advanced Encryption Standard，高级加密标准）：AES 128/192/256 表示使用长度为 128/192/256 bit 的密钥进行加密。
完整性验证算法	选择应用于 IKE 会话的验证算法。本路由器支持以下验证算法： ● MD5：Message Digest Algorithm，消息摘要算法。对一段消息产生 128bit 的消息摘要，防止消息被篡改。 ● SHA1：Secure Hash Algorithm，安全散列算法。对一段消息产生 160bit 的消息摘要，比 MD5 更难破解。
Diffie-Hellman 分组	选择 Diffie-Hellman 算法的组信息，用于产生加密 IKE 隧道的会话密钥。
密钥生命周期	设置 IPSec SA 的生存时间。

标题项	说明
PFS	● PFS（Perfect Forward Secrecy，完善的前向安全性）特性使得 IKE 阶段 2 协商生成一个新的密钥材料，该密钥材料与阶段 1 协商生成的密钥材料没有任何关联，这样即使 IKE1 阶段 1 的密钥被破解，阶段 2 的密钥仍然安全。 ● 如果没有使用 PFS，阶段 2 的密钥将根据阶段 1 生成的密钥材料来产生，一旦阶段 1 的密钥被破解，用于保护通信数据的阶段 2 密钥也岌岌可危，这将严重威胁到双方的通信安全。

密钥协商方式-手动设置

密钥协商方式为“手动设置”时，如下图（以隧道协议为“AH+ESP”时为例）。

图6-11 密钥协商方式-手动设置

表6-7 密钥协商方式-手动设置参数说明

标题项	说明
ESP 加密算法	当隧道协议选择“ESP”时需设置 ESP 加密算法。本路由器支持以下加密算法： ● DES：使用 56bit 的密钥对 64bit 数据进行加密，64bit 的最后 8 位用于奇偶校验。3DES 则为三重 DES，使用三个 56bit 的密钥进行加密。 ● AES：AES128/192/256 表示使用长度为 128/192/256bit 的密钥进行加密。
ESP 加密密钥	● 设置 ESP 加密密钥。IPSec 通信双方设置需保持一致。
ESP/AH 认证算法	当隧道协议选择“ESP”时，需设置 ESP 认证算法；当隧道协议选择“AH”时，需设置 AH 认证算法。本路由器支持以下验证算法： ● NONE：ESP 认证算法为空，此时，不需要设置 ESP 认证密钥。 ● MD5：对一段消息产生 128bit 的消息摘要，防止消息被篡改。 ● SHA1：对一段消息产生 160bit 的消息摘要，比 MD5 更难破解。
ESP/AH 认证密钥	当隧道协议选择“ESP”时，需设置 ESP 认证密钥；当隧道协议选择“AH”时，需设置 AH 认证密钥。 IPSec 通信双方设置需保持一致。
ESP/AH 外出 SPI	设置进入 SPI 参数。 SPI 与隧道对端网关地址、协议类型三个参数共同标识一个 IPSec 安全联盟，必须与通信对端的“外出 SPI”值相同。
ESP/AH 进入 SPI	设置进入 SPI 参数。 SPI 与隧道对端网关地址、协议类型三个参数共同标识一个 IPSec 安全联盟，必须与通信对端的“外出 SPI”值相同。

传输模式

点击 +新增 可以添加 IPSec 隧道连接。封装模式为“传输模式”的页面如下。


新增
IPSec: 开启 关闭
封装模式: 传输模式
WAN口: WAN0
连接名称:
加密算法: 3DES
完整性验证算法: SHA1
预共享密钥:
确定
取消

图6-12 传输模式

表6-8 传输模式参数说明

标题项	说明
IPSec	● 开启/关闭 IPSec 功能。
封装模式	选择 IPSec 数据的封装模式。 隧道模式通常用于两个安全网关之间的通讯；传输模式通常用于主机和主机、主机与网关之间的通信。
WAN 口	指定 IPSec 在本侧使用的接口，IPSec 对端设备的“远端网关地址”需填为此接口的 IP 地址。
连接名称	设置该 IPSec 连接的名称描述。
加密算法	选择应用于 IKE 会话的加密算法。本路由器支持以下加密算法： ● DES（Data Encryption Standard，数据加密标准）：使用 56bit 的密钥对 64bit 数据进行加密，64bit 的最后 8 位用于奇偶校验。3DES 则为三重 DES，使用三个 56bit 的密钥进行加密。 ● AES（Advanced Encryption Standard，高级加密标准）：AES 128/192/256 表示使用长度为 128/192/256 bit 的密钥进行加密。
完整性验证算法	选择应用于 IKE 会话的验证算法。本路由器支持以下验证算法： ● MD5：Message Digest Algorithm，消息摘要算法。对一段消息产生 128bit 的消息摘要，防止消息被篡改。 ● SHA1：Secure Hash Algorithm，安全散列算法。对一段消息产生 160bit 的消息摘要，比 MD5 更难破解。
预共享密钥	输入协商时所用的预共享密钥，需要保持与对端网关设备一致。最长为 128 字符。

6.3 VPN 配置举例

6.3.1 PPTP/L2TP VPN 配置举例

组网需求

某企业使用网关路由器进行网络搭建，并成功接入互联网。分公司员工需要经过互联网访问公司内部局域网资源，如，内部资料、办公 OA、ERP 系统、CRM 系统、项目管理系统等。

可以在路由器上设置 PPTP/L2TP VPN 服务，实现远端用户经互联网安全访问企业内部局域网的需求。本例以 PPTP VPN 为例说明，L2TP VPN 的设置方法类似。

网络拓扑

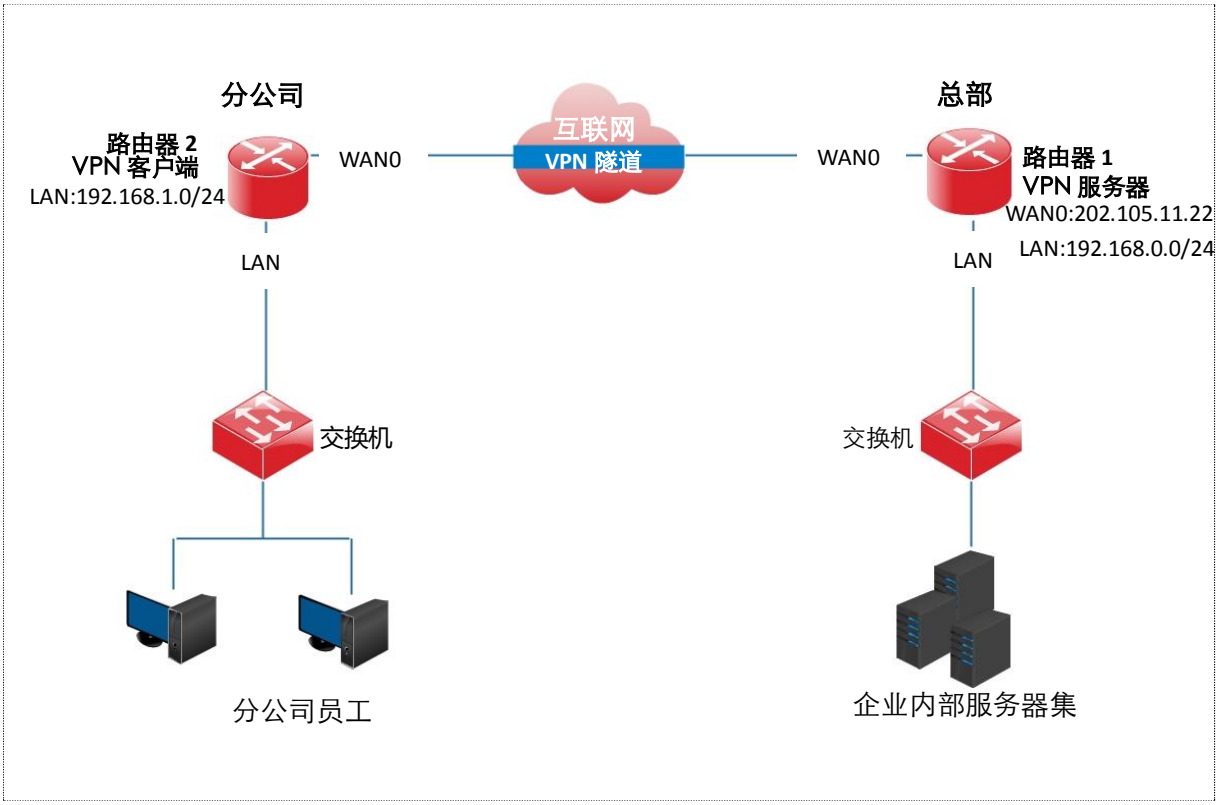


图6-13 PPTP/L2TP VPN 配置

配置步骤

配置路由器 1，使其作为 VPN 服务器；配置路由器 2，使其作为 VPN 客户端。

步骤1 配置路由器 1；

1. 开启 PPTP 服务器；

- 点击「VPN 服务」>「PPTP/L2TP 服务器」；

- 进行各项参数配置；

- 服务器状态：选择“开启”；

- 服务器类型：选择 VPN 服务器的类型，本例为“PPTP”；

- WAN 口：指定 VPN 服务器与客户端建立隧道的出口，本例为“WAN0”；

- 加密：是否启用数据加密，PPTP 客户端处配置必须与服务器端保持一致；

- 点击页面底端的 确定 。

图6-14 PPTP/L2TP 服务器

2. 配置 PPTP/L2TP 用户。

- 点击「VPN 服务」>「PPTP/L2TP 服务器」，找到“PPTP/L2TP 用户”模块；

- 点击 +新增 ；

- 在【新增】窗口配置下述参数；

- 用户名：输入 VPN 客户端进行 VPN 连接时所用的用户名，如“fengongsi1”；

- 密码：输入对应用户名的密码，如“fengongsi1”；

- 是否网段：选择“是”；

- 网段：输入 VPN 客户端局域网的网络号，本例为“192.168.1.0”；

- 掩码：输入“255.255.255.0”；

- 备注：输入该用户账号的描述信息，如“分公司 1”；

- 点击 确定 。

图6-15 新增 PPTP/L2TP 用户

添加完成，如下图示。

图6-16 成功添加 PPTP/L2TP 用户

步骤2 配置路由器 2。

1. 点击「VPN 服务」>「PPTP/L2TP 客户端」，配置如下参数；

- PPTP/L2TP 客户端：选择“开启”；

- 客户端类型：和 VPN 服务器侧保持一致，本例为“PPTP 客户端”；

- WAN 口：指定 VPN 客户端与服务器建立隧道的出口，本例为“WAN0”；

- 服务器 IP/域名：输入 VPN 服务器侧作为隧道出口的 WAN 口的 IP 地址，本例为“202.105.11.22”；

– 用户名/密码：输入 VPN 服务器分配的用户名和密码，本例中均为“fengongsi1”；

– 加密：选择“开启”，和 VPN 服务器侧配置保持一致；

– VPN 代理上网：选择“关闭”；

– 服务器内网网段：输入 VPN 服务器内网的网段，本例为“192.168.0.0”；

– 内网子网掩码：输入 VPN 服务器内网的子网掩码，本例为“255.255.255.0”。

2. 点击 确定 。

图6-17 新增 PPTP/L2TP 客户端

验证配置

当**路由器 2** 上「VPN 服务」>「PPTP/L2TP 客户端」页面的状态显示为“已连接”且已经获取 IP 地址时，VPN 连接成功。如下图示。

图6-18 成功添加 PPTP/L2TP 客户端

之后，分公司和总部的员工就可以通过互联网安全访问对方的局域网资源了。下文以分公司访问总部 FTP 服务器内容为例。公司总部的项目资料放在 FTP 服务器中，假设服务器信息如下：

- FTP 服务器 IP 地址：192.168.0.159
- 服务器端口：21
- 登录用户名/密码：admin

当分公司员工访问总部项目资料时，步骤如下：

步骤1 在电脑上访问“ftp: //服务器 IP 地址:服务端口号”，本例为 ftp://192.168.0.159:21；

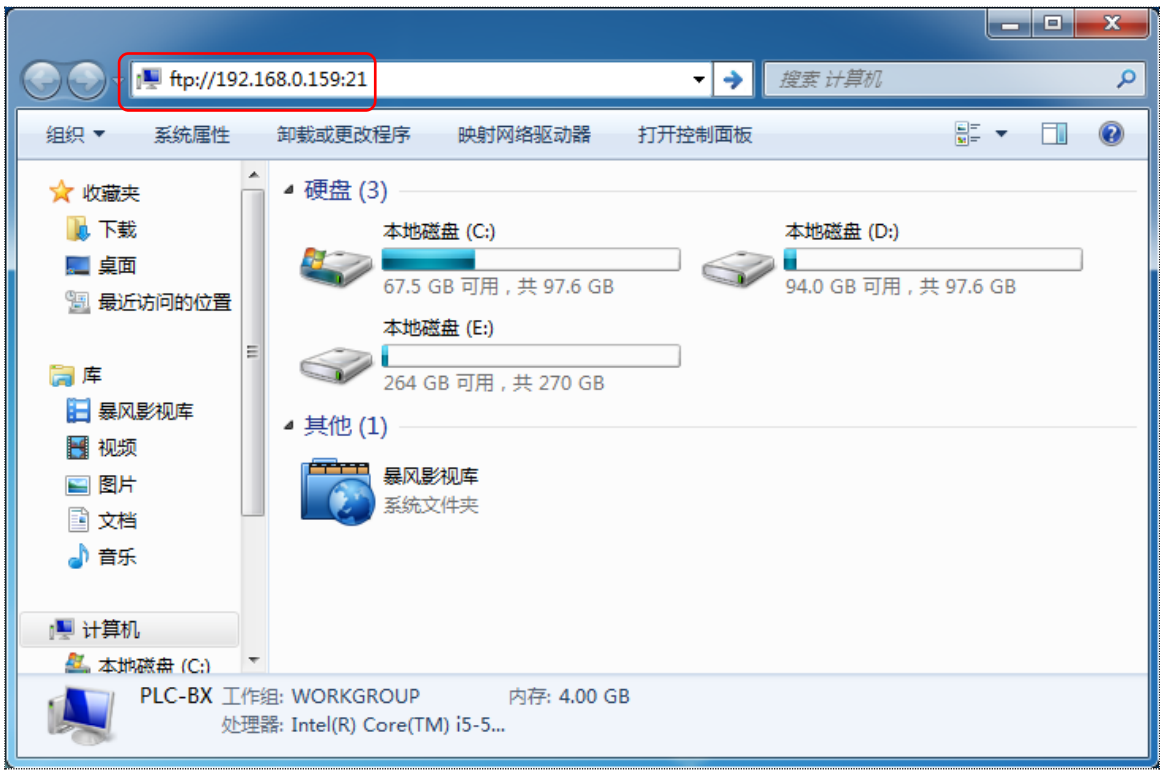


图6-19 ftp: //服务器 IP 地址:服务端口号

步骤2 在弹出的窗口输入登录用户名和密码，本例均为 admin；

步骤3 点击 登录 。

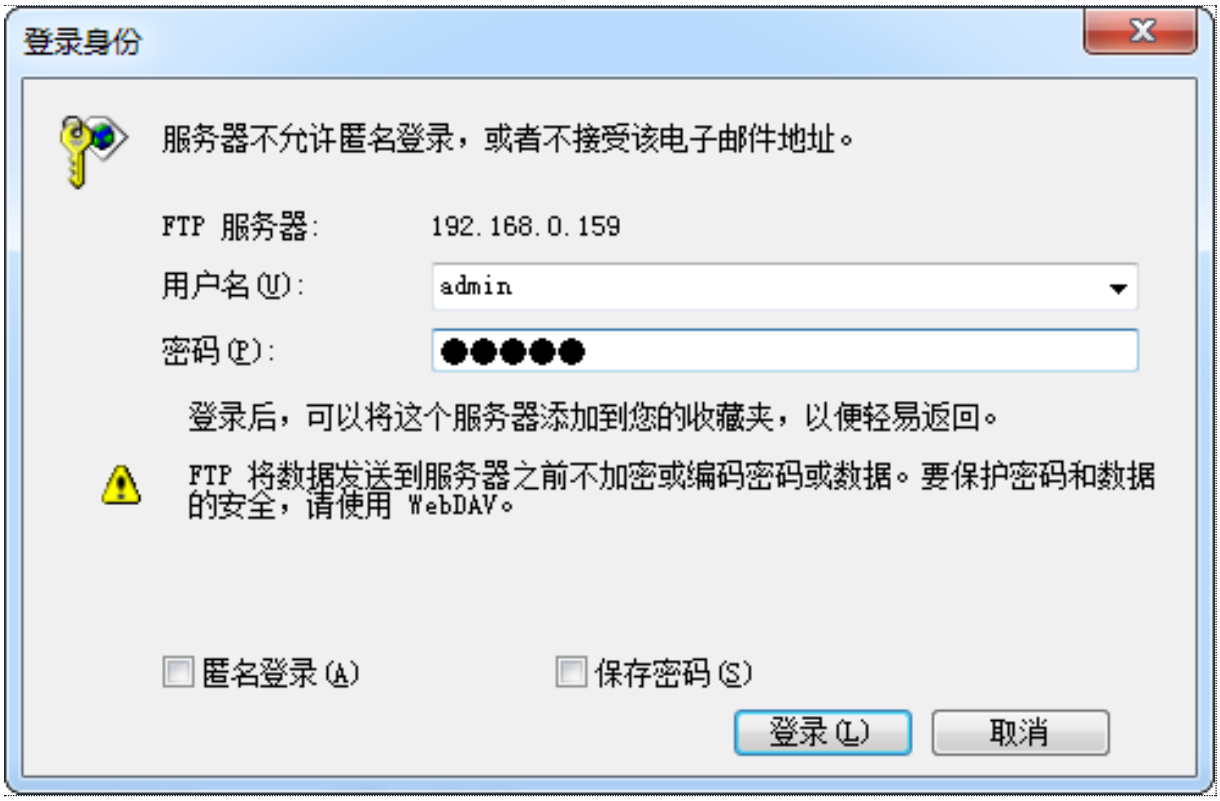


图6-20 登录身份

访问成功。

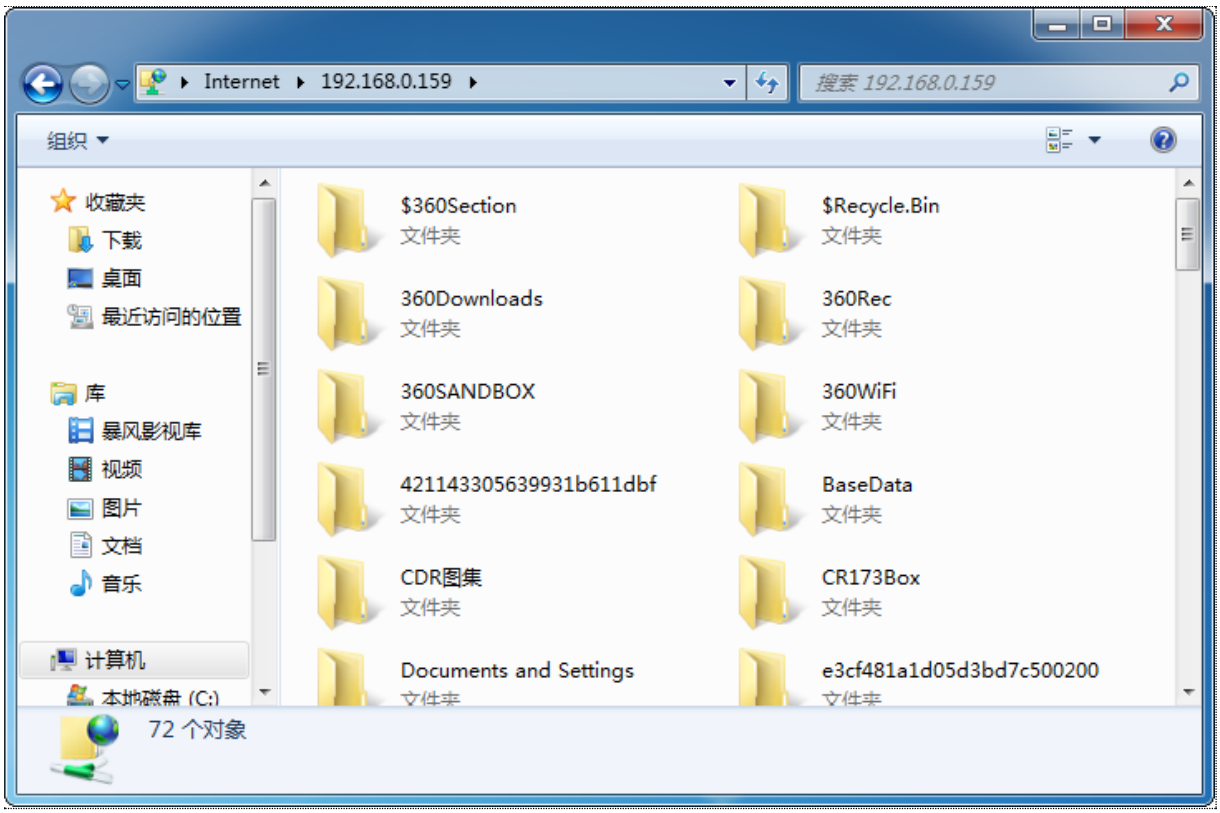


图6-21 成功访问 ftp 服务器

6.3.2 IPSec VPN 配置举例

组网需求

某企业使用网关路由器进行网络搭建，并成功接入互联网。分公司员工需要经过互联网访问公司内部局域网资源，如，内部资料、办公 OA、ERP 系统、CRM 系统、项目管理系统等。

可以在路由器上设置 IPSec VPN 服务，实现远端用户经互联网安全访问企业内部局域网的需求。

网络拓扑

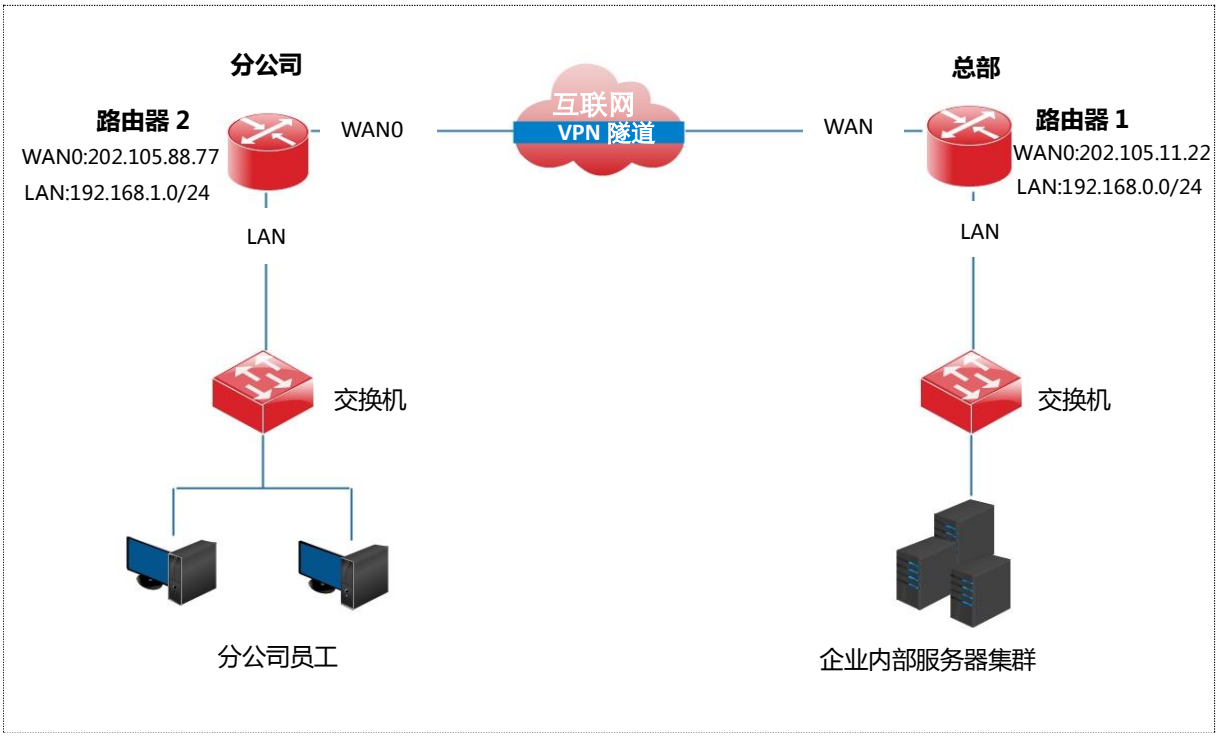


图6-22 IPsec VPN 配置

配置注意事项

- 配置过程中，如果需要设置 IPSec 连接的高级选项，请保持两台路由器的设置参数一致。
- 密钥协商方式为“手动设置”时，IPSec 两端的加密算法、加密密钥、认证算法需一致，路由器 1 的外出 SPI 与路由器 2 的进入 SPI 一致，路由器 1 的进入 SPI 与路由器 2 的外出 SPI 一致。

配置步骤

假设两台路由器的 IPSec 连接基本信息如下：

- 封装模式：隧道模式。
- 密钥协商方式：自动协商。
- 预共享密钥为：12345678。

步骤1 设置路由器 1；

1. 点击「VPN 服务」>「IPSec」；
2. 点击 新增 ；
3. 在【新增】窗口配置各项参数；
4. IPSec：点击“开启”。
5. 封装模式：选择“隧道模式”。
6. WAN 口：选择本条 IPSec 隧道绑定的 WAN 口，本例为“WAN0”。

7. 连接名称：为本条隧道设置一个名称，如“IPSec_1”。

8. 远端网关地址：输入对端路由器上 IPSec 隧道绑定的 WAN 口的 IP 地址，本例为“202.105.88.77”。

9. 本地内网网段/掩码：输入本路由器内网的网段/子网掩码，本例为“192.168.0.0/24”。

10. 远端内网网段/掩码：输入对端路由器内网的网段/子网掩码，本例为“192.168.1.0/24”。

11. 预共享密钥：本例为“12345678”。

12. 点击 确定 。

图6-23 新增 IPSec

添加完成，如下图示。

图6-24 成功添加 IPSec

步骤2 设置路由器 2；

点击「VPN 服务」>「IPSec」，点击 新增 进行配置。如下图示。

图6-25 新增 IPSec

验证配置

登录路由器的管理页面，转到「系统状态」>「用户列表」页面。当“IPSec 安全联盟”显示连接数量及对应连接信息时，设置成功。

之后，分公司和总部的员工就可以通过互联网安全访问对方的局域网资源了。

6.3.3 L2TP over IPSec VPN 配置举例

组网需求

某企业使用网关路由器进行网络搭建，并成功接入互联网。出差的员工需要访问公司内部局域网资源，如，内部资料、办公 OA、ERP 系统、CRM 系统、项目管理系统等。

可以在路由器上设置 L2TP VPN 服务，实现远端用户经互联网安全访问企业内部局域网的需求。

网络拓扑

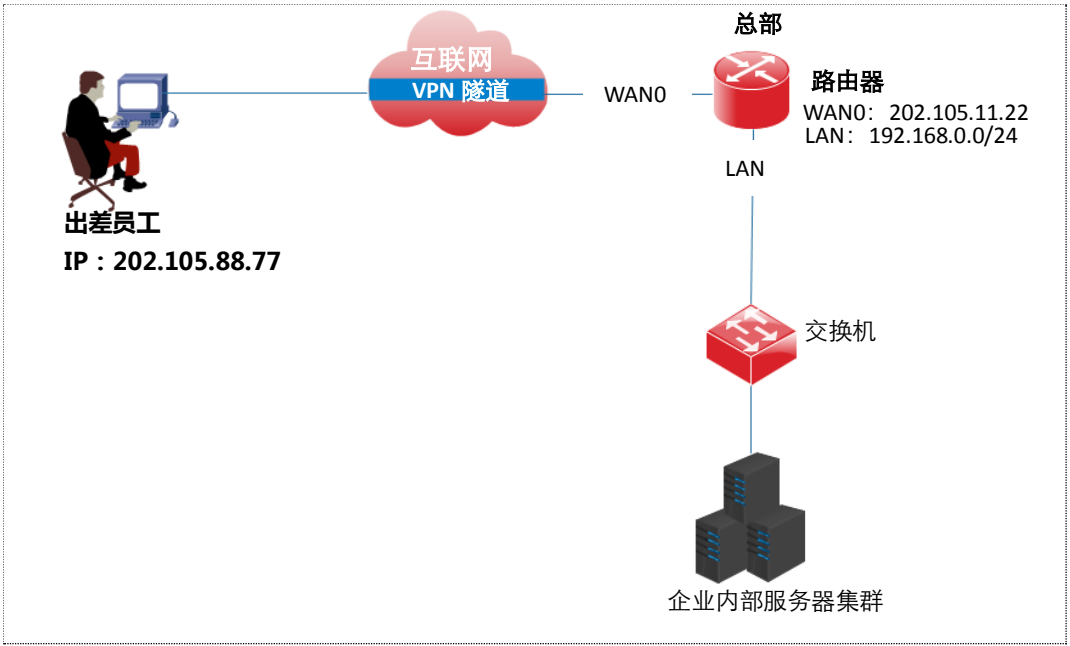


图6-26 L2TP over IPsec 配置

配置步骤

假设路由器的 IPSec 连接基本信息如下：

- 封装模式：传输模式。
- 密钥协商方式：自动协商。
- 预共享密钥为：87654321。

步骤1 建立 IPSec 连接

1. 点击「VPN 服务」>「IPSec」；
2. 点击 新增 ；
3. 在“新增”页面配置各项参数；
4. IPSec：点击“开启”；
5. 封装模式：选择“传输模式”；
6. WAN 口：选择本条 IPSec 连接绑定的 WAN 口，本例为“WAN0”；
7. 连接名称：为本条连接设置一个名称，如“公司总部”；
8. 预共享密钥：设置密码，用于出差员工建立 VPN 连接时输入，如“87654321”；
9. 点击 确定 。

图6-27 建立 IPSec 连接

添加成功。

图6-28 成功建立 IPSec 连接

步骤2 开启 L2TP 服务器

1. 点击「VPN 服务」>「PPTP/L2TP 服务器」；
2. 进行各项参数配置；
3. 服务器状态：选择“开启”；
4. 服务器类型：选择 VPN 服务器的类型，本例为“L2TP”；
5. WAN 口：指定 VPN 服务器与客户端建立隧道的出口，本例为“WAN0”；
6. IPSec 加密：选择已连接的 IPSec 隧道，本例为“公司总部”；
7. 点击页面底端的 确定 ；

图6-29 开启 L2TP 服务器

步骤3 添加 L2TP 用户

1. 点击「VPN 服务」>「PPTP/L2TP 服务器」，找到“PPTP/L2TP 用户”模块；
2. 点击 +新增 ；
3. 在【新增】窗口配置下述参数；
4. 用户名：输入 VPN 客户端进行 VPN 连接时所用的用户名，如“zhangsan”；
5. 密码：输入对应用户名的密码，如“zhangsan”；
6. 是否网段：选择“否”；
7. 备注：输入该用户账号的描述信息，如“张三”；
8. 点击 确定 。

图6-30 新增 L2TP 用户

添加完成，如下图示。

图6-31 成功添加 L2TP 用户

验证配置

出差员工进行 VPN 拨号

情景 1：在电脑上建立 VPN 与总部通信，请参考下文，以 Windows 7 为例说明。

步骤1 建立 VPN 连接；

1. 点击桌面右下角图标，选择“打开网络和共享中心”。

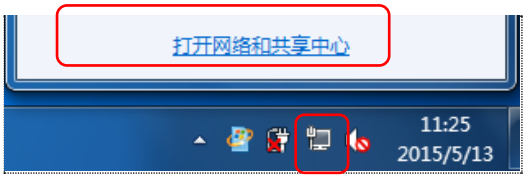


图6-32 打开网络和共享中心

2. 点击“设置新的连接或网络”。

图6-33 设置新的连接或网络

3. 点击“连接到工作区”，点击“下一步”。

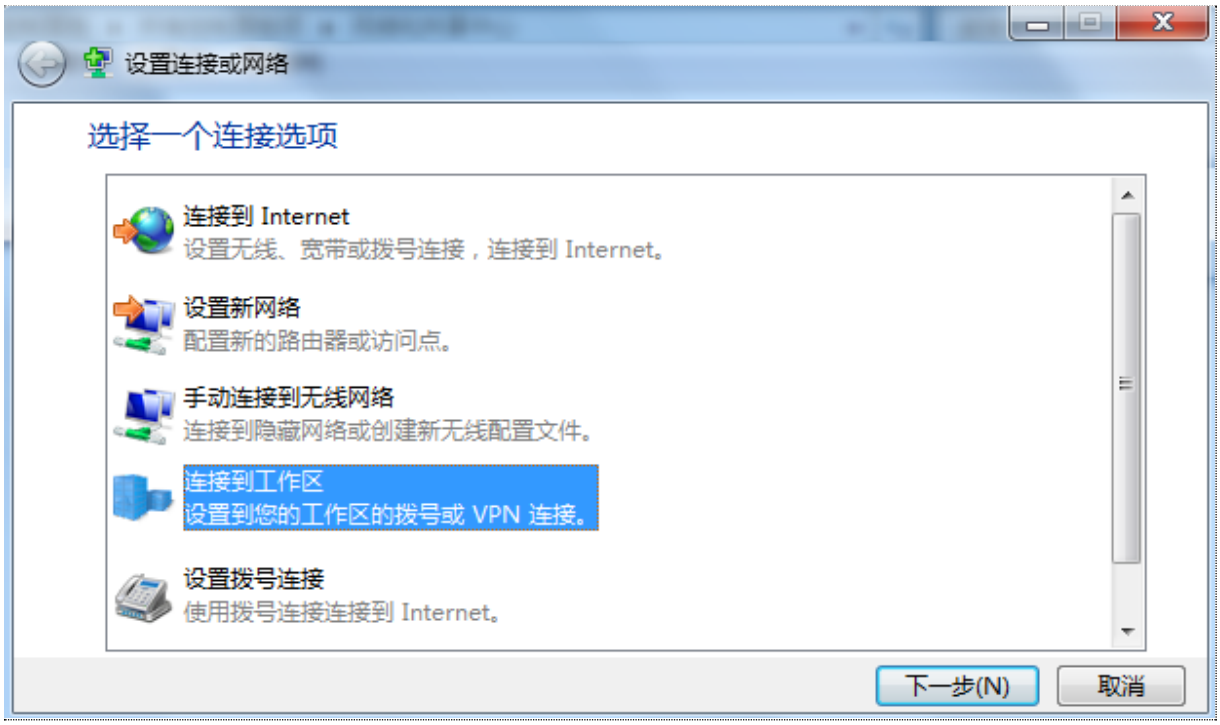


图6-34 连接到工作区

图6-35

4. 点击“使用我的 Internet 连接（VPN）”。如果弹出其他对话框，请根据提示操作。

图6-36 使用我的 Internet 连接（VPN）

5. 在 Internet 地址框输入 L2TP 服务器的 IP 地址，本例为“113.88.112.220”，点击“下一步”。

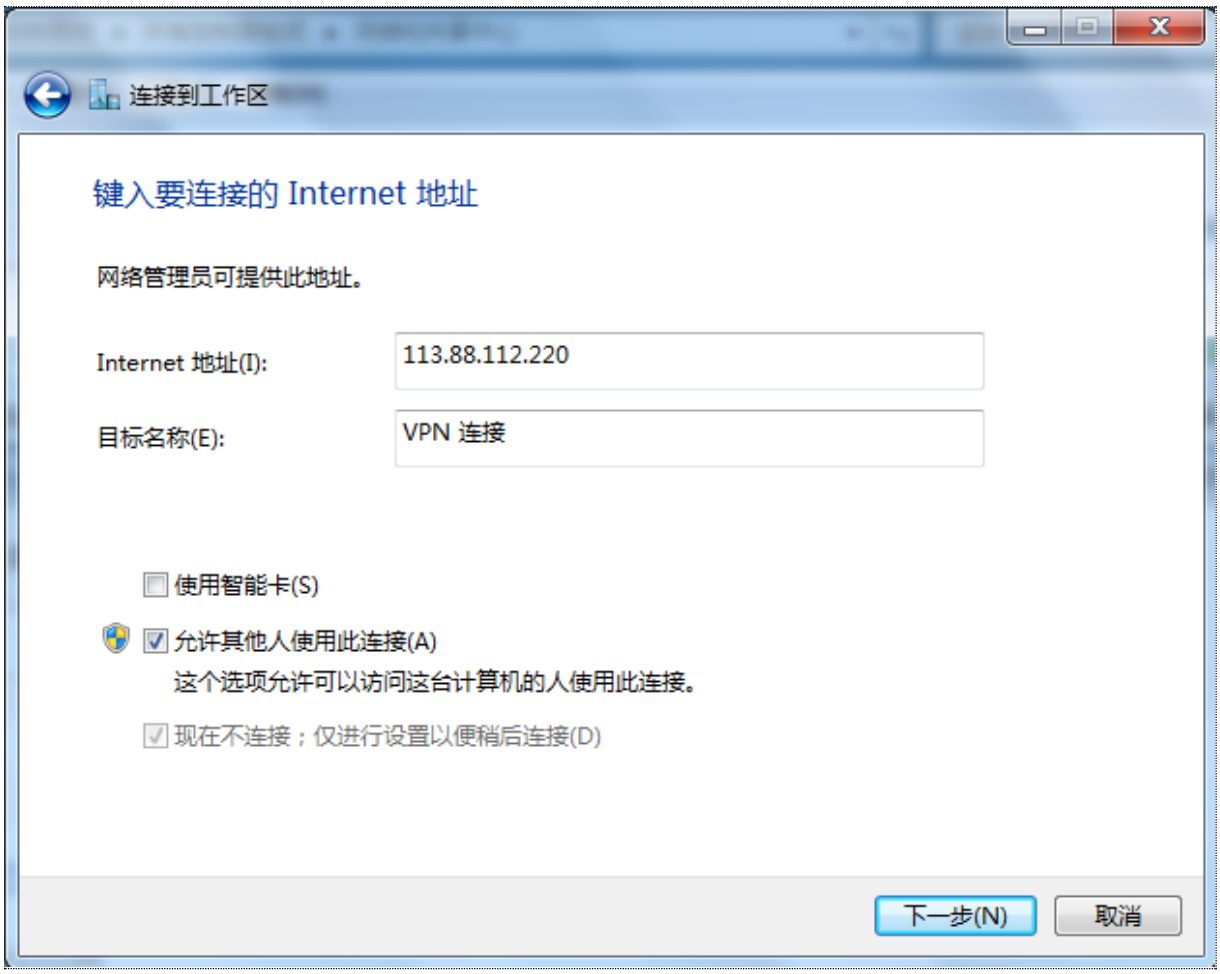


图6-37 键入要连接的 Internet 地址

6. 输入 L2TP 服务器允许拨入的用户名及其密码，本例均为“zhangsan”。点击“创建”。

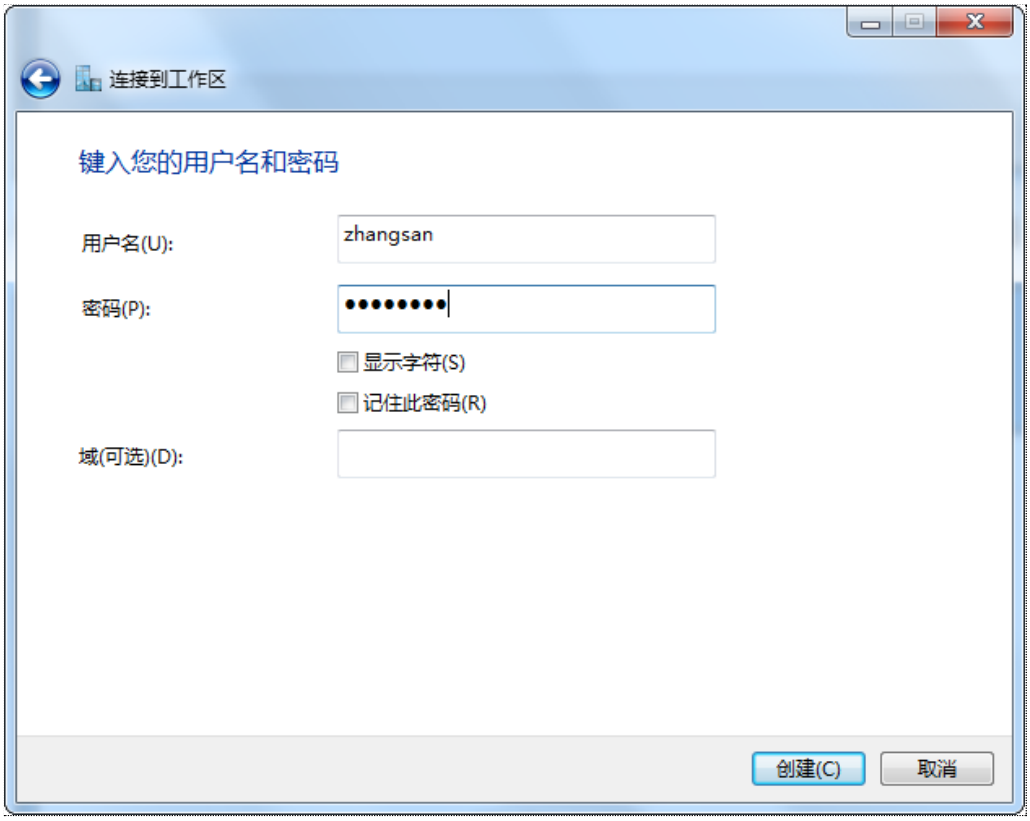


图6-38 键入您的用户和密码

稍等片刻，建立成功。

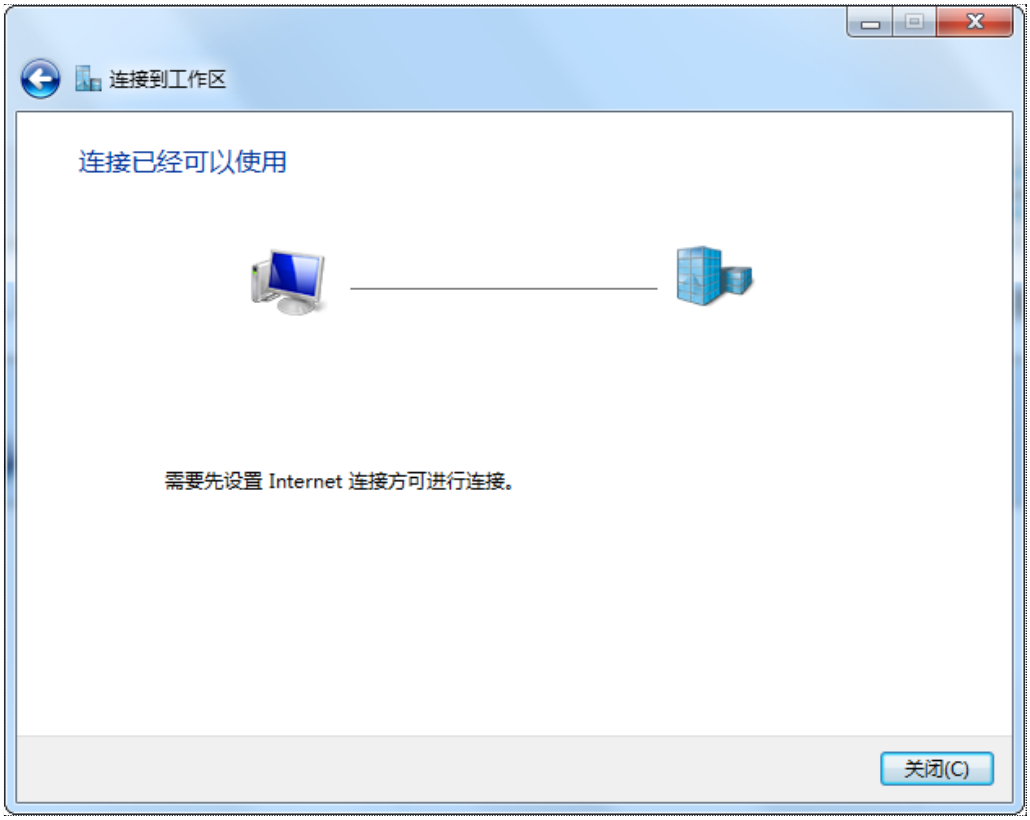


图6-39 成功连接到工作区

步骤2 设置“VPN 连接”的相关参数；

1. 点击桌面右下角图标，选择“打开网络和共享中心”，点击左侧栏“更改适配器设置”，右键点击“VPN 连接”，选择“属性”。

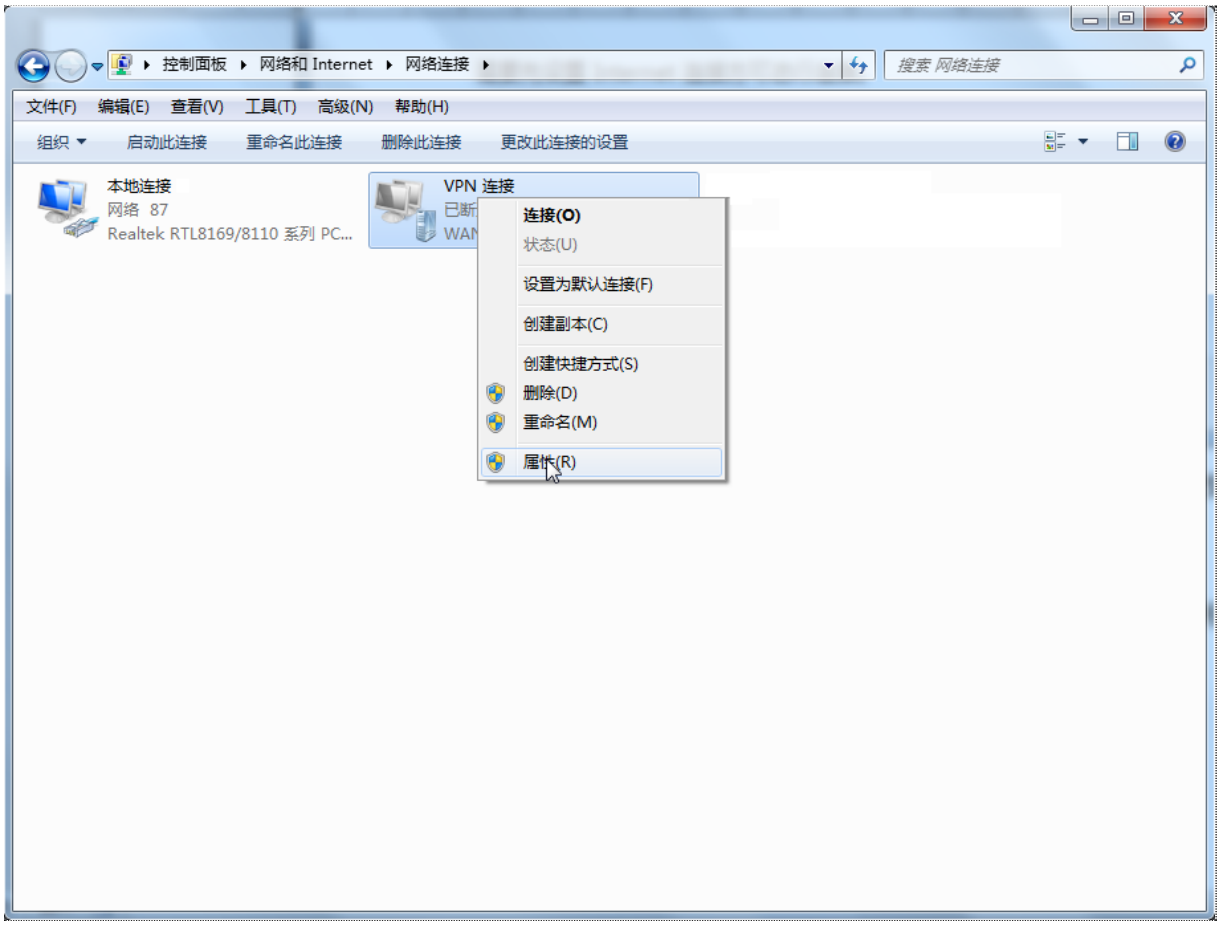


图6-40 VPN 连接

2. 点击“安全”，在“VPN 类型”选项，选择“使用 IPsec 的第 2 层隧道协议（L2TP/IPSec）”，点击“高级设置”。

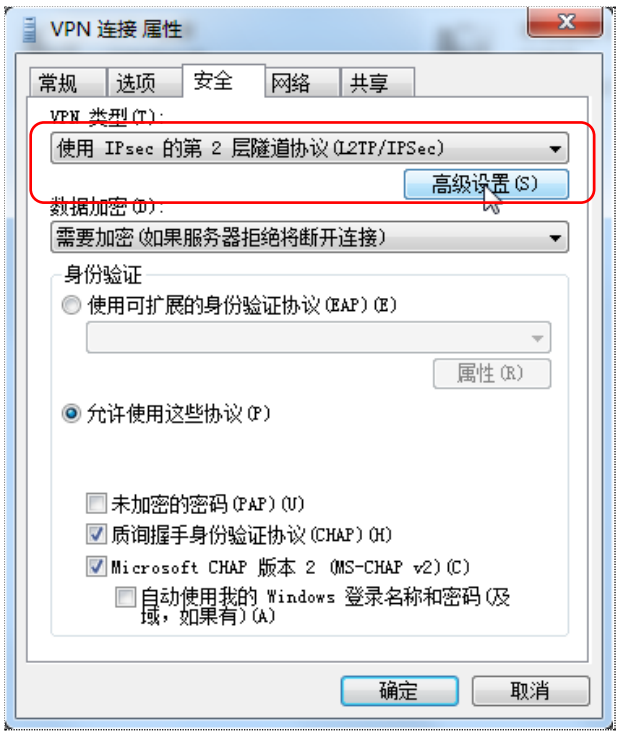


图6-41 VPN 连接属性

3. 点击“使用预共享的密钥作为身份验证”，在“密钥”选框输入 IPSec 隧道设置的预共享密钥，本例为“87654321”。
4. 点击“确定”。

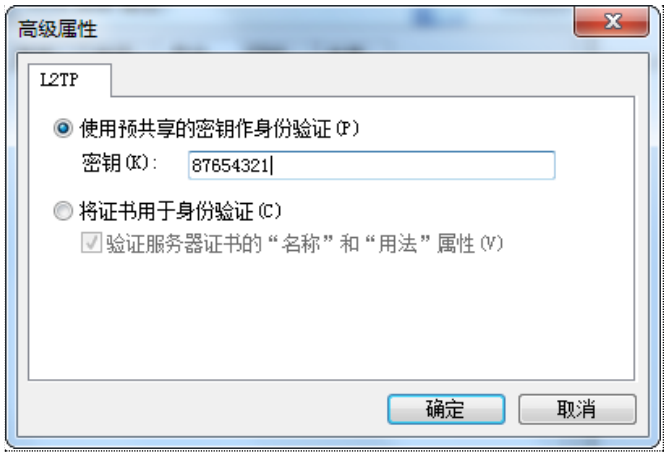


图6-42 高级属性

5. 返回“VPN 连接 属性”对话框，勾选“未加密的密码（PAP）”，点击“确定”。

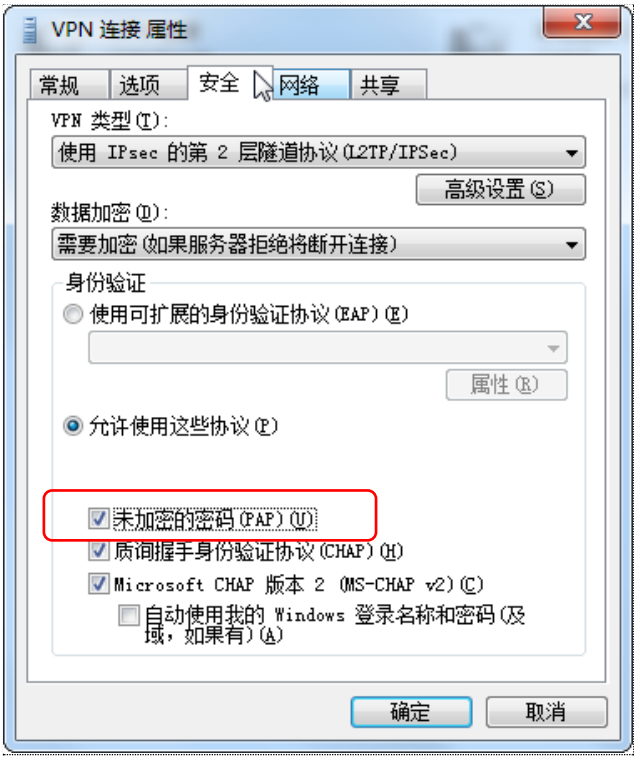


图6-43 VON 连接属性

步骤3 VPN 拨号。

1. 进入“网络连接”页面，右键点击“VPN 连接”，选择“连接”。

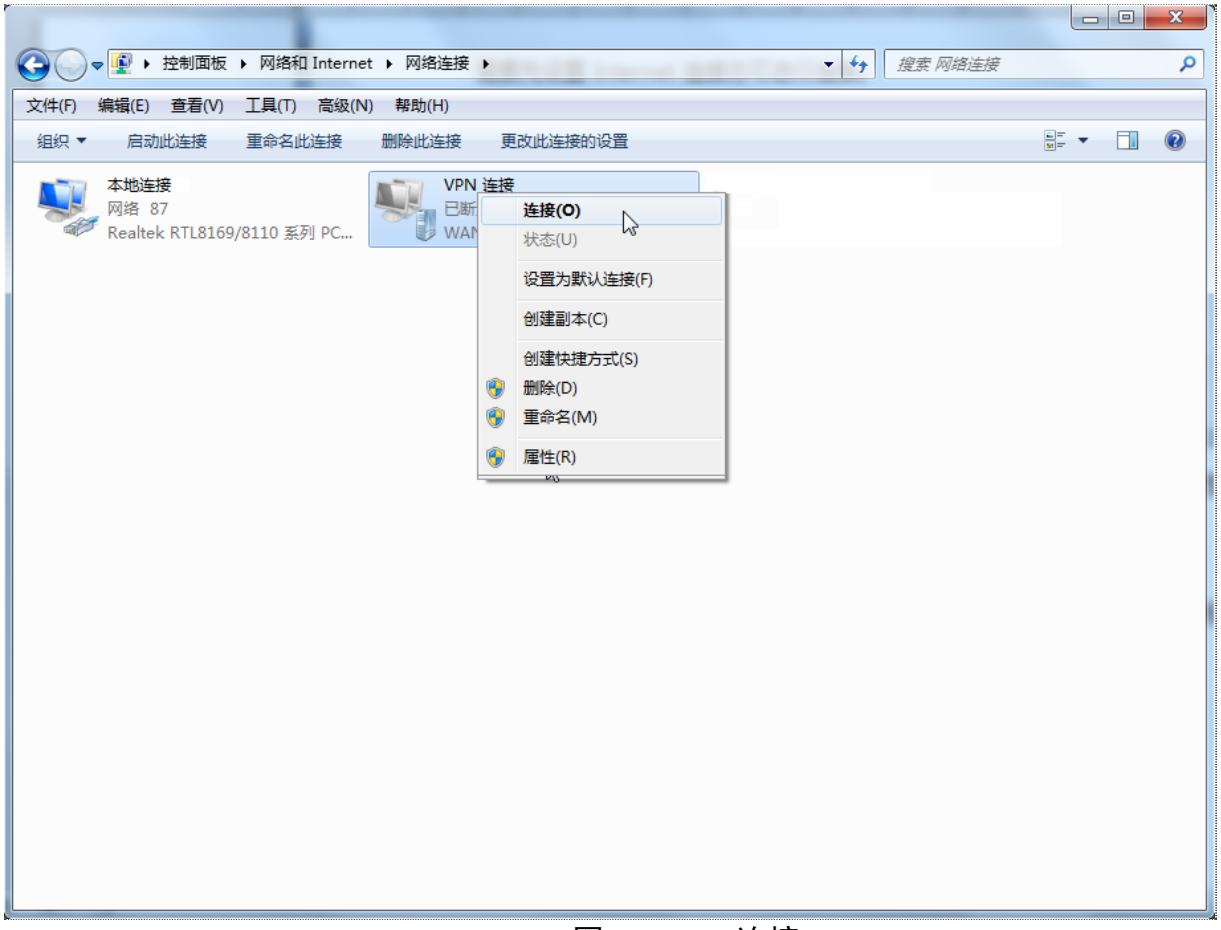


图6-44 VPN 连接

2. 用户名/密码：输入 L2TP 服务器允许拨入的用户名及其密码，本例均为“zhangsan”。

3. 点击“连接”。

图6-45 连接 VPN 连接

稍等片刻，拨号成功。即可根据总部提供的账号信息进行访问。

图6-46 成功连接 VPN 连接

情景 2：使用移动设备建立 VPN 连接访问公司总部时，请参考下文，以 iOS 系统为例说明。

步骤1 在手机界面上找到并点击“设置”图标；

步骤2 点击“VPN”；

图6-47 VPN

步骤3 点击“添加 VPN 配置...”；

图6-48 添加 VPN 配置

步骤4 设置 VPN 相关参数；

- 类型：点击选择“L2TP”。

– 描述：设置此 VPN 连接的名称，如“总部”。

– 服务器：输入 L2TP 服务器的 IP 地址，本例为“113.88.112.220”。

– 帐户/密码：输入 L2TP 服务器允许拨入的用户及其密码，本例均为“zhangsan”。

– 密钥：输入 IPSec 隧道设置的预共享密钥，本例为“87654321”。

– 点击“完成”。

图6-49 添加 VPN 配置

步骤5 点击 。

图6-50 开启 VPN 连接

稍等片刻，当“状态”变为“已连接  ”时，拨号成功。

图6-51 成功连接 VPN 连接

出差员工访问总部

下文以访问总部 Web 服务器内容为例。公司总部的项目资料放在 Web 服务器中，假设服务器信息如下：

- Web 服务器 IP 地址：192.168.0.159
- 服务器端口：80

访问步骤：

在电脑上打开浏览器，访问“http: //服务器 IP 地址:服务端口号”，本例为 htttp://192.168.0.159:80。

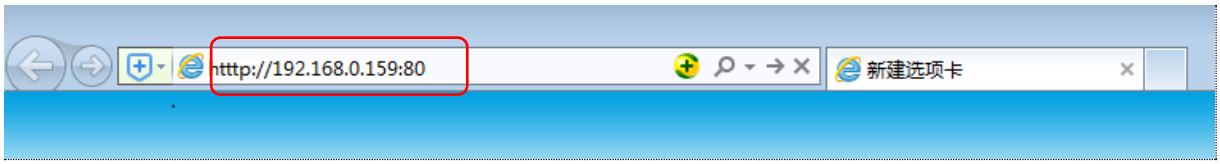


图6-52 访问 http: //服务器 IP 地址:服务端口号

如下图，访问成功。

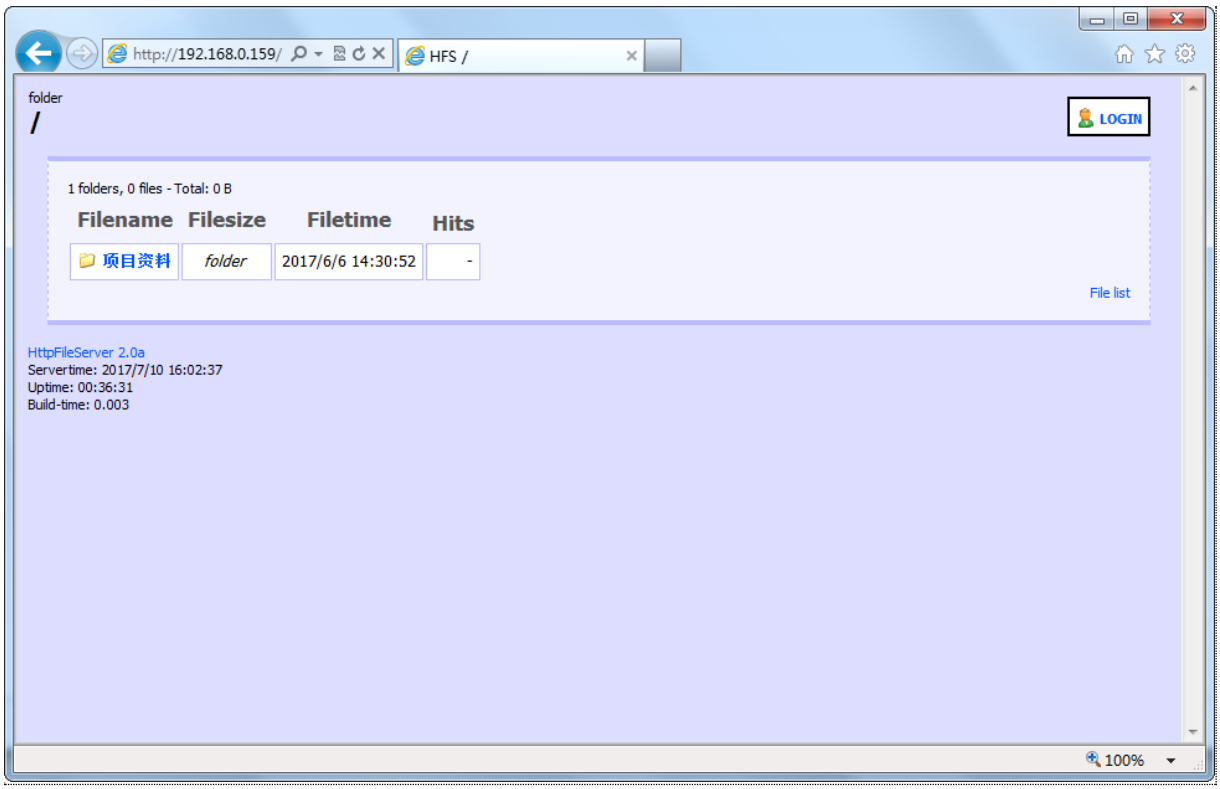


图6-53 成功访问服务器 IP 地址

注意

如果要使用移动端（智能手机、平板电脑等）访问 FTP 服务器，移动端需要成功安装 FTP 客户端才能访问。

第7章 安全设置

7.1 概述

路由器的「安全设置」模块包括：IP-MAC 访问控制、攻击防御。

- IP-MAC 访问控制

  使用 IP-MAC 访问控制功能，可以绑定局域网内计算机的 IP 地址与 MAC 地址。当开启 IP-MAC 访问控制功能后，只有在路由器的“已添加列表”中的用户才能访问互联网，其他用户禁止访问互联网。IP-MAC 访问控制可以有效防止局域网 IP 地址被非法盗用，进而增强网络安全性。

  路由器支持手动添加和动态添加两种方式。

  - 手动添加：由网络管理员手动添加 IP-MAC 访问控制列表。此方式需要网络管理员事先了解局域网每台计算机的 MAC 地址，并明确每个 IP 与 MAC 的对应关系。

  - 动态添加：局域网用户连上路由器后，路由器「安全设置」>「IP-MAC 访问控制」页面的“动态添加”模块将显示用户的 IP-MAC 对应关系，网络管理员只需在该页面点击 添加 ，即可完成 IP-MAC 绑定操作。

- 攻击防御

  路由器支持的攻击防御类型有：ARP 攻击防御、DDOS 防御、IP 攻击防御、防 WAN 口 Ping。

  - ARP 攻击防御：路由器可以抵御局域网的 ARP 欺骗、ARP 广播等攻击。

  - DDOS 防御：DDOS 攻击，即分布式拒绝服务（Distributed Denial of Service）攻击。利用 DDOS 攻击，攻击者可以消耗目标系统资源，使该目标系统无法提供正常服务。路由器可以防止的 DDOS 攻击类型包括：ICMP flood、UDP flood、SYN flood 攻击。

  - IP 攻击防御：路由器可以按照要求拦截具有一些特殊 IP 选项的数据包，这些 IP 选项包括：IP Timestamp Option、IP Security Option、IP Stream Option、IP Record Route Option、IP Loose Source Route Option 及非法 IP 选项等。

– 防 WAN 口 Ping：广域网计算机 Ping 路由器 WAN 口 IP 时，路由器可以自动忽略该 Ping 请求，防止暴露自己，同时防范外部的 Ping 攻击。

启用对应的攻击防御后，如果发生攻击，路由器可以将攻击信息如攻击时间、类型、次数，攻击者 IP、MAC 等记录在「系统状态」>「防攻击日志」页面的防攻击日志中，助力网络管理员进行网络安全管理。

7.2 IP-MAC 访问控制

进入页面的方法：点击「安全设置」>「IP-MAC 访问控制」。进入页面后，默认显示如下。

图7-1 IP-MAC 访问控制

7.2.2 开启 IP-MAC 访问控制功能

步骤1 点击「安全设置」>「IP-MAC 访问控制」；

步骤2 IP-MAC 访问控制：选择“开启”；

步骤3 点击 确定 。

图7-2 开启 IP-MAC 访问控制

表7-1 IP-MAC 访问控制参数说明

标题项		说明
IP-MAC 访问控制		开启/关闭 IP-MAC 访问控制。默认为“关闭”。 开启 IP-MAC 访问控制后，只有 IP-MAC 在“已添加列表”中，且 IP 与 MAC 的匹配的用户才能上网。
已添加列表	+新增	点击此按钮可手动添加要绑定的 IP 地址和 MAC 地址。
	删除	点击此按钮可将选中的已绑定的 IP-MAC 解绑。
	IP 地址	显示绑定的 IP 地址及其对应 MAC 地址。
	MAC 地址	
	备注	显示对应 IP-MAC 访问控制规则的描述信息。若添加规则时未设置备注信息，将显示空白。
	操作	点击 可修改规则；点击 可删除（解绑）规则。
动态添加	添加	连接到路由器的局域网计算机信息将会显示在动态列表中。点击此按钮可将已选中的规则添加到“已添加列表”。
	全部添加	点击此按钮可将动态列表中的所有规则添加到“已添加列表”。
	IP 地址	显示连接到路由器的局域网计算机的 IP 地址及其对应的 MAC 地址。
	MAC 地址	
	操作	点击规则后的 添加 ，即可将该规则快速添加到“已添加列表”。

开启 IP-MAC 访问控制功能后，您就可以配置 IP-MAC 访问控制规则了。

7.2.3 配置 IP-MAC 访问控制规则

手动添加

步骤1 点击「安全设置」>「IP-MAC 访问控制」，找到“已添加列表”模块；

步骤2 点击 +新增 ；

步骤3 在弹出的页面进行配置；

步骤4 配置完成后，点击 确定 。

图7-3 配置 IP-MAC 访问控制规则

成功添加“IP-MAC 访问控制”规则后，可以在「安全设置」>「IP-MAC 访问控制」页面看到已添加的 IP-MAC 访问控制规则。

图7-4 成功添加 IP-MAC 访问控制

如果需要修改 IP-MAC 访问控制规则，请点击对应操作栏的；如果需要删除规则，请点击对应操作栏的；如果需要同时删除多个规则，请选中要删除的多个规则，然后点击 删除 。

自动添加

点击「安全设置」>「IP-MAC 访问控制」，找到“动态添加”模块进行设置。

7.3 攻击防御

进入页面的方法：点击「安全设置」>「攻击防御」。进入页面后，默认显示如下。

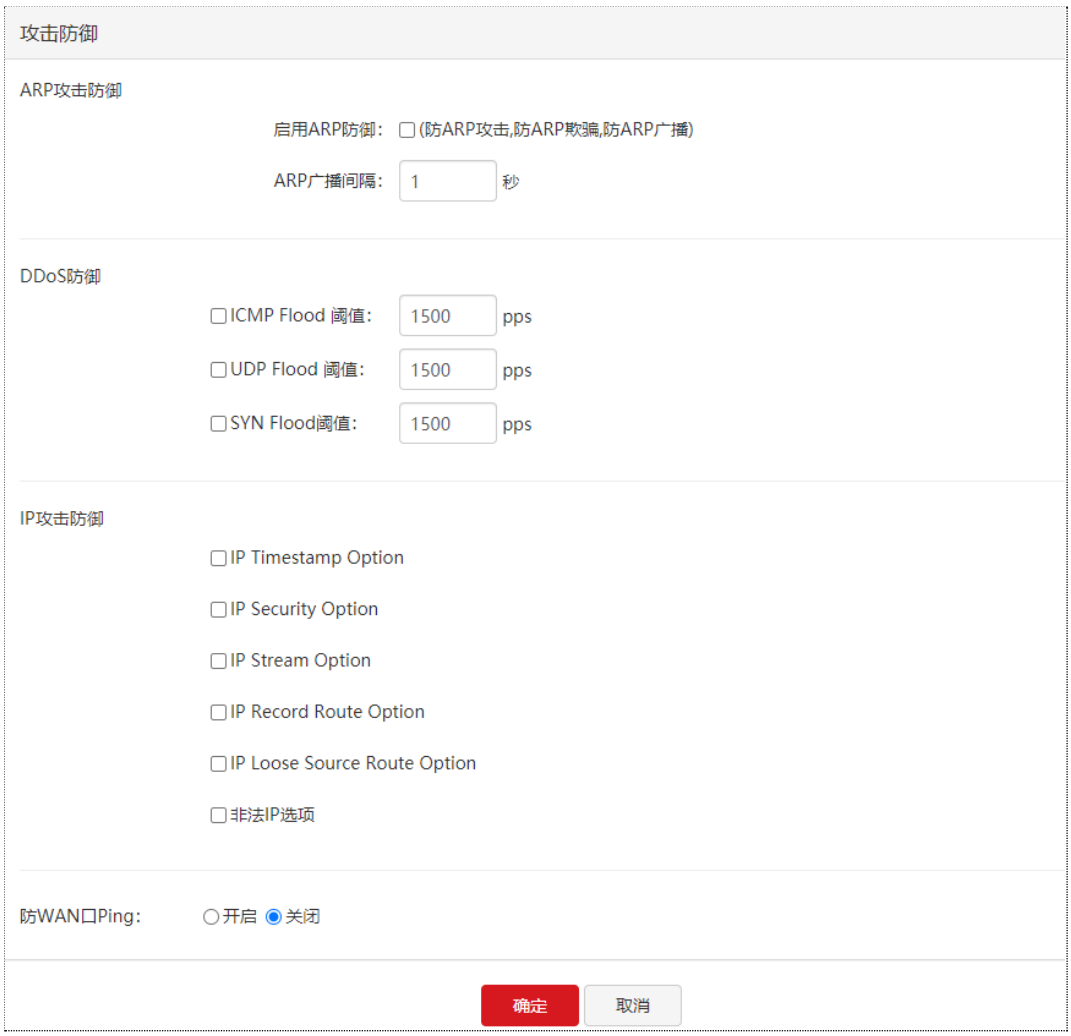


图7-5 攻击防御

启用攻击防御后，网络管理员可以在「系统状态」>「防攻击日志」页面查看攻击信息。

说明

某些时候，符合以上特征的数据包并不是攻击数据包，比如在进行网络测试时。所以请视情况开启攻击防御功能。

表7-2 攻击防御参数说明

标题项		说明
ARP 攻击防御	启用 APR 防御	开启/关闭 ARP 防御（包括防 ARP 攻击、防 ARP 欺骗、防 ARP 广播等）功能。
	ARP 广播间隔	开启/关闭 ARP 防御（包括防 ARP 攻击、防 ARP 欺骗、防 ARP 广播等）功能。
DDOS 防御	ICMP Flood 阈值	一秒钟内，如果路由器收到超过此阈值的 ICMP 请求包，则认为路由器正受到 ICMP Flood 攻击。
	UDP Flood 阈值	一秒钟内，如果路由器某一端口收到超过此阈值的 UDP 包，则认为路由器该端口正受到 UDP Flood 攻击。
	SYN Flood 阈值	一秒钟内，如果路由器某一端口收到超过此阈值的 TCP SYN 包，则认为路由器该端口正受到 SYN Flood 攻击。
IP 攻击防御	IP Timestamp Option	启用后，路由器将拦截带有 Internet Timestamp 选项的 IP 包。
	IP Security Option	启用后，路由器将拦截带有 Security 选项的 IP 包。
	IP Stream Option	启用后，路由器将拦截带有 Stream ID 选项的 IP 包。
	IP Record Route Option	启用后，路由器将拦截带有 Record Route 选项的 IP 包。
	IP Loose Source Route Option	启用后，路由器将拦截带有 Loose Source Route 选项的 IP 包。
	非法 IP 选项	启用后，路由器将检查 IP 包的完整性、正确性，如果不符合，则拦截。
防 WAN 口 Ping		开启/关闭路由器的防 WAN 口 Ping 功能。默认“关闭”。 开启防 WAN 口 Ping 功能后，广域网的设备不能 Ping 通路由器的 WAN 口 IP 地址。

第8章 AC 管理

8.1 概述

路由器的「AC 管理」模块包括：无线配置、高级配置、AP 管理、用户状态。

路由器作为无线控制器管理 AP 时，网络拓扑图如下：

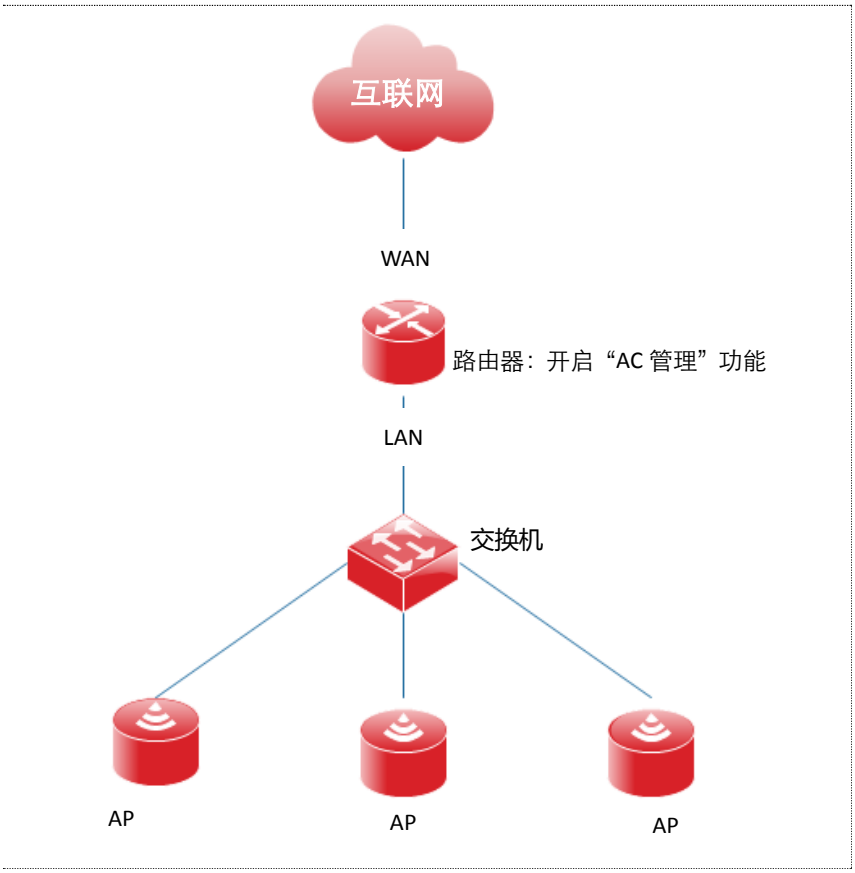


图8-1 AC 管理

- 无线配置

  在“无线配置”模块，您可以开启/关闭路由器的 AC 管理功能。开启 AC 管理功能后，您还可以在这里集中配置局域网中 AP 的 SSID 相关参数，如 SSID、启用状态、隐藏 SSID 状态、频段、最大用户数、VLAN ID、认证类型密码等。

- 高级配置

  开启 AC 管理功能后，您可以在“高级配置”模块对局域网中 AP 集中进行射频配置、全局配置。

- AP 管理

  开启 AC 管理功能后，您可以在“AP 管理”模块查看路由器管理上的局域网 AP 信息，另外，还可以对 AP 进行批量重启、升级、复位等操作。

- 用户状态

开启 AC 管理功能后，如果您需要了解连接到网络中“管理 AP”的无线用户信息，可以进入“用户状态”模块查看。“管理 AP”，指正在被路由器管理的 AP。

8.2 无线配置

进入页面的方法：点击「AC 管理」>「无线配置」。进入页面后，默认显示如下。

图8-2 无线配置

8.2.1 开启 AC 管理功能

步骤1 点击「AC 管理」>「无线配置」；

步骤2 选择“开启”。

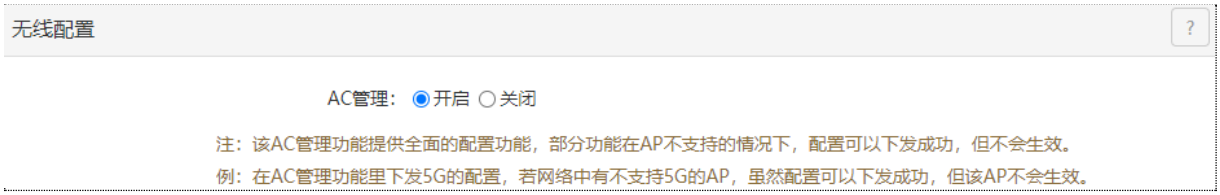


图8-3 开启 AC 管理

开启“AC 管理”功能后，路由器可以对局域网中的 AP 进行集中管理，您可以进入「AC 管理」>「AP 管理」页面查看已被路由器管理的 AP。

8.2.2 下发无线策略到 AP

在「AC 管理」>「无线配置」页面，可以集中配置“管理 AP”的 SSID 相关参数。

配置方法：配置各项参数，然后点击 确定 。

说明

AC 管理提供全面的 AP 配置功能，部分功能在 AP 不支持的情况下，配置可以下发成功，但不会生效。如：通过 AC 管理功能下发 5G 的配置，若网络中有不支持 5G 的 AP，虽然配置可以下发成功，但该 AP 不会生效。


无线配置
AC管理： 开启 关闭
注：该AC管理功能提供全面的配置功能，部分功能在AP不支持的情况下，配置可以下发成功，但不会生效。
例：在AC管理功能里下发5G的配置，若网络中有不支持5G的AP，虽然配置可以下发成功，但该AP不会生效。
序号 状态 SSID 隐藏SSID 频段 最大用户数 VLAN ID 认证类型 密码 高级
1 开启 HIKVISIO 关闭 2.4G 48 1000 不加密
2 关闭 HIKVISIO 关闭 2.4G 48 1000 不加密
3 关闭 HIKVISIO 关闭 2.4G 48 1000 不加密
4 关闭 HIKVISIO 关闭 2.4G 48 1000 不加密
5 关闭 HIKVISIO 关闭 2.4G 48 1000 不加密
6 关闭 HIKVISIO 关闭 2.4G 48 1000 不加密
7 关闭 HIKVISIO 关闭 2.4G 48 1000 不加密
8 关闭 HIKVISIO 关闭 2.4G 48 1000 不加密
确定
取消

图8-4 AC 管理

表8-1 AC 管理参数说明

标题项	说明
序号	无线策略的序号。1~4 分别对应 AP 2.4G 或 5G 频段的第 1~4 个 SSID，5~8 分别对应 AP 2.4G 频段的第 5~8 个 SSID。 前 4 条策略支持配置 2.4G、5G、2.4G&5G 频段的 SSID 相关参数，后 4 条策略仅支持配置 2.4G 频段的 SSID 相关参数。
状态	无线策略的启用状态，也是对应 SSID 的开启/关闭状态。默认启用无线策略 1，关闭其他无线策略。 关闭无线策略 1 会导致 AP 的无线功能关闭，因此，不建议关闭无线策略 1。AP 的无线功能关闭后，可以到「AC 管理」>「高级配置」页面开启。
SSID	无线策略使用的 SSID。
隐藏 SSID	开启/关闭 SSID 的“隐藏 SSID”功能。 ● 开启：AP 将不广播对应 SSID，该 SSID 不会显示在客户端的可用网络列表中。客户端连接该 SSID 时，需要正确地手动输入该 SSID 才能连接。 ● 关闭：AP 广播对应 SSID，该 SSID 能被周围的无线设备搜索到。
频段	选择 SSID 的工作频段。 ● 2.4G：无线策略下发到 AP 的 2.4G 频段。 ● 5G：无线策略下发到 AP 的 5G 频段。 ● 2.4G&5G：AP 的 2.4G 和 5G 频段都会下发该无线策略。 如果无线策略 1 的频段选择为单频，如 2.4G（或 5G），则点击 确定 后，AP 将关闭另一频段如 5G（或 2.4G）的无线功能。 关闭 AP 某频段的无线功能后，可以到「AC 管理」>「高级配置」页面重新开启。
最大用户数	该 SSID 最多允许同时接入的无线客户端个数。默认为 48。
VLAN ID	SSID 所在的 802.1Q VLAN。默认 VLAN ID 为 1000。 如果要使用 AP 的 QVLAN 功能，还需要到路由器「AC 管理」>「高级配置」页面的“全局配置”模块，开启 VLAN。
认证类型	SSID 的无线认证类型。 ● 不加密：不加密无线网络，允许任意客户端接入。为保障网络安全，不建议选择此项。 ● WPA-PSK：SSID 采用 WPA-PSK 认证方式（AES 加密规则）。 ● WPA2-PSK：SSID 采用 WPA2-PSK 认证方式（AES 加密规则）

标题项	说明
密码	WPA-PSK 或 WPA2-PSK 的预共享密码，也是用户连接 SSID 时需要输入的无线密码。
高级	点击 可开启/关闭“客户端隔离”功能。 ● 开启：连接到本 SSID 的无线客户端之间不能相互通信。 ● 关闭：连接到本 SSID 的无线客户端之间可以相互通信。

8.3 高级配置

进入页面的方法：点击「AC 管理」>「高级配置」。在这里，可以对 AP 进行射频配置、全局配置。

完成参数设置后，请点击页面底端的 确定 ，将配置下发到 AP。

8.3.1 射频配置

在“射频配置”模块，可以配置 AP 的射频相关参数，如频段、无线开关、信道等。

点击「AC 管理」>「高级配置」进入设置页面。

图8-5 射频配置

表8-2 射频配置参数说明

标题项	说明
频段	选择要设置射频参数的频段：2.4G 或 5G。
国家	选择当前所在的国家。 下发配置到 AP 时，会将当前所有配置下发到 AP，包括 2.4G 和 5G。
无线开关	开启/关闭对应频段的无线功能。
网络模式	选择无线网络模式。2.4G 包括 11b、11g、11b/g、11b/g/n；5G 包括 11a、11ac、11a/n。 ● 11b：AP 使用 11b 模式，此时，仅允许 802.11b 客户端连接到 AP。 ● 11g：AP 使用 11g 模式，此时，仅允许 802.11g 客户端连接到 AP。 ● 11b/g：AP 使用 11b/g 模式，此时，允许 802.11b、802.11g 客户端连接到 AP。 ● 11b/g/n：AP 使用 11b/g/n 模式，此时，工作在 2.4G 频段的 802.11b、802.11g、802.11n 客户端均可连接到 AP。 ● 11a：AP 使用 11a 模式，此时，仅允许 802.11a 客户端连接到 AP。 ● 11ac：AP 使用 11ac 模式，此时，允许 802.11ac 客户端连接到 AP。 11a/n：AP 使用 11a/n 模式，此时，工作在 5G 频段的 802.11a 和 802.11n 客户端均可连接至 AP。
带宽	选择无线带宽。 ● 20：AP 限制只能使用 20MHz 的信道带宽。 ● 40：AP 优先使用 40MHz 的信道带宽，如果环境恶劣，将自动改为使用 20MHz 的信道带宽。 ● 80：仅适用 5G，AP 根据周围环境，自动调整信道带宽为 20MHz、40MHz 或 80MHz。 自动：仅适用于 2.4G，AP 根据周围环境，自动调整信道带宽为 20MHz 或 40MHz。
信道	选择无线工作信道。信道的可选择范围由当前选择的“国家”和“频段”（2.4G 或 5G）决定。

标题项	说明
功率	设置 AP 的发射功率。 若 AP 不支持设置的功率，则配置下发后，以 AP 支持的最大范围为准生效。即，当功率超过 AP 的上限功率时，只使用 AP 的最大功率；当功率小于 AP 的下限功率时，只使用 AP 的最小功率。
SSID 隔离	开启/关闭 SSID 隔离功能。开启后，连接到 AP 对应频段不同 SSID 的无线客户端之间不能互相通信。
空口调度	开启/关闭空口调度功能。 空口调度可以保证每个客户端的数据传输时间相等，如果低速率终端在单位时间内没有传输完数据，也要等到下次继续传输。解决了某些低速率客户端占用无线空口太多资源问题，提升 AP 的整体效率，有效保障了带机量和吞吐量。
更多配置...	配置射频高级参数，详细可参考下文参数说明 2。

在“射频配置”模块，点击更多配置...，将展开射频配置高级参数。

图8-6 射频配置

修改参数后，点击本页面的 确定，即可将配置下发到 AP。

表8-3 射频配置参数说明 2

标题项	说明
RSSI 阈值	AP 可接受的无线客户端信号强度，信号强度低于此值的客户端将无法接入该 AP。正确设置 RSSI 可以确保客户端主动连接到信号比较强的 AP。
穿墙能力	仅 2.4G 有效，请根据实际应用场景，选择“穿墙能力”特性。 ● 强覆盖：常用于 AP 部署密度较低的场景，如办公室、仓库、医院等，使用此模式可以增加 AP 的覆盖范围。 ● 高密度：常用于 AP 部署密度较高的场景，如会场、展厅、宴会厅、体育场馆、高校教室、候机厅等，使用此模式可以有效减少 AP 相互之间的干扰。
部署模式	仅 2.4G 有效，请根据实际应用场景，选择“穿墙能力”特性。 ● 强覆盖：常用于 AP 部署密度较低的场景，如办公室、仓库、医院等，使用此模式可以增加 AP 的覆盖范围。 ● 高密度：常用于 AP 部署密度较高的场景，如会场、展厅、宴会厅、体育场馆、高校教室、候机厅等，使用此模式可以有效减少 AP 相互之间的干扰。
部署模式	仅 2.4G 有效，请根据实际应用场景，选择“部署模式”特性。 ● 强覆盖：常用于 AP 部署密度较低的场景，此模式可以尽可能地确保客户端成功接入 AP。 ● 高密度：常用于 AP 部署密度较高的场景，此模式可以确保客户端连接到信号好的 AP。 ● 默认：介于“强覆盖”和“高密度”之间。
WMM	即“无线多媒体”。 开启 WMM 后，音视频数据优先转发。如果要提高 AP 对于无线多媒体数据（如观看在线视频）的传输性能，建议开启。
APSD	APSD（Automatic Power Save Delivery），即“自动省电模式”，是 WiFi 联盟的 WMM 省电认证协议。开启“APSD”能降低 AP 的电能消耗。默认关闭。

标题项	说明
客户端老化时间	客户端连接到 AP 的 WiFi 后，如果在该时间段内与 AP 没有数据通信，AP 将主动断开该客户端；如果在该时间段内与 AP 有数据通信，则停止老化计时。

8.3.2 全局配置

在 “全局配置”模块，可以配置 AP 的全局参数，如 VLAN 启用状态、管理 VLAN ID、LED 状态、端口驱动能力等。点击「AC 管理」>「高级配置」进入设置页面。

图8-7 全局配置

表8-4 全局配置参数说明

标题项	说明
VLAN	开启/关闭 AP 的 QVLAN 功能。开启后，本页配置的“管理 VLAN ID”和「AC 管理」>「无线配置」页面配置的“VLAN ID”将生效。默认为“关闭”。
管理 VLAN ID	AP 的管理 VLAN ID，默认为“1”。 更改管理 VLAN ID 并成功下发到 AP 后，路由器或管理电脑需要重新连接到新的管理 VLAN，才能管理 AP。
LED 状态	开启/关闭 AP 的 LED 指示灯显示功能。 开启：开启 AP 的指示灯显示功能，可根据指示灯判断 AP 的工作状态。默认为“开启”。 关闭：关闭 AP 的所有指示灯。
端口驱动能力	AP 的以太网口驱动距离。 ● 标准：速率高，驱动距离较短。一般情况下，建议选择此模式。 ● 增强：驱动距离远，但速率较低，一般协商为 10Mbps。 除非连接 AP 以太网口与对端设备的网线超过 100 米时，才建议尝试改为“增强”以提高网线驱动距离。此时，必须确保对端端口工作模式为自协商，否则可能导致 AP 以太网口无法正常收发数据
更多配置...	配置全局高级参数，详细可参考下文参数说明 2。

在“全局配置”模块，点击更多配置...，将展开全局配置高级参数。

图8-8 更多配置

修改参数后，点击本页面的 确定 ，即可将配置下发到 AP。

表8-5 更多配置参数说明

标题项	说明
PVID	AP Trunk 口默认所属的 VLAN ID。AP 开启 VLAN 功能时，此参数才有效。
Trunk 口	选择作为 AP Trunk 口的有线 LAN 口。Trunk 口允许所有 VLAN 通过。 启用 802.1Q VLAN 功能时，至少要选择一个 LAN 口作为 Trunk 口。如果网络中有的 AP 只有一个 LAN 口，请选择 LAN 0 为 Trunk 口，否则可能会导致配置失败。
自动维护设置	开启/关闭 AP 的“自动维护”功能。开启时，需设置“维护类型”、“时间”等参数。默认为“关闭”。 开启“自动维护”可以预防长时间地运行 AP 导致 WLAN 出现性能降低、不稳定等现象。但维护时 AP 会重启，从而导致无线断线，因此建议将“维护时间”设置在无线业务相对空闲的时间。
维护类型	选择 AP 的自动维护类型。 ● 定时维护：AP 在指定日期的指定时间点自动维护。 ● 循环维护：AP 每隔一个“间隔时间”便自动维护。
维护时间设置	指定“定时维护”的维护时间。
间隔时间	指定“循环维护”的维护间隔。

8.4 AP 管理

进入页面的方法：点击「AC 管理」>「AP 管理」进入页面。在这里，可以查看/导出“管理 AP”信息，批量重启/复位/升级在线 AP，批量删除离线 AP 信息，单独修改某一 AP 的配置信息等。

图8-9 AP 管理

8.4.1 导出

使用导出功能，可以将 AP 列表信息以 Excel 的格式导出并保存到本地电脑。

操作步骤：

步骤1 点击「AC 管理」>「AP 管理」；

步骤2 点击 导出 ，之后按页面提示操作。

8.4.2 重启

使用重启功能，可以同时将多个 AP 重新启动。

操作步骤：

步骤1 点击「AC 管理」>「AP 管理」，选择需要重新启动的 AP；

步骤2 点击 重启 ，之后按页面提示操作。

图8-10 重启

重启时，AP 将离线一段时间，重启完成后，AP 将自动上线。AP 从离线到重新上线的过程可能需要 1~2 分钟，请耐心等待。您可以点击 刷新 查看此过程。

8.4.3 升级

使用升级功能，可以同时升级多个 AP 的软件版本。

注意

AP 升级过程中，为了避免损坏 AP 导致其无法使用，请切勿关闭路由器和 AP 的电源。

升级 AP 前，需要先下载对应型号的 AP 软件到本地电脑。然后，再按以下步骤进行操作：

步骤1 进入路由器的「AC 管理」>「AP 管理」页面，选择需要进行软件升级的 AP；

步骤2 点击 升级 ，之后按页面提示操作。

图8-11 升级

8.4.4 复位

使用复位功能，可以同时将多个 AP 恢复出厂设置。

操作步骤：

步骤1 点击「AC 管理」>「AP 管理」，选择需要复位的 AP；

步骤2 点击 复位 ，之后按页面提示操作。

图8-12 复位

8.4.5 删除

使用删除功能，可以同时删除多个处于离线状态的 AP。

操作步骤：

步骤1 点击「AC 管理」>「AP 管理」，选择需要同时删除的离线 AP；

步骤2 点击 删除 ，之后按页面提示操作。

图8-13 删除

注意

在线 AP 不能删除。

8.4.6 修改

使用修改功能，可以单独修改某一 AP 的配置信息，如备注、无线开关、国家、信道、功率等参数。

操作步骤：

步骤1 在「AC 管理」>「AP 管理」页面，找到需要修改的 AP，然后点击对应操作栏的 ；

图8-14 修改

步骤2 根据需要修改 AP 的配置，完成后点击 确定 。

图8-15 AP 详细设置

8.5 用户状态

进入页面的方法：点击「AC 管理」>「用户状态」。在这里，可以查看连接到“管理 AP”的无线用户信息。

图8-16 用户状态

表8-6 用户状态参数说明

标题项	说明
频段	2.4G、5G、2.4G+5G。选中某频段后，页面将仅显示对应频段的用户信息。
备注	用户连接的 AP 的备注信息。
AP 型号	用户连接的 AP 的产品型号。
SSID	用户连接的 SSID。
频段	用户连接的 SSID 所在的频段。
用户 IP	用户设备获得的 IP 地址。
用户 MAC	用户设备的 MAC 地址。
下载总流量	用户下载数据的总量。
信号强度	接收的信号强度（RSSI），即 AP 接收到的用户终端的无线信号强度。
上网时长	客户端接入网络的时长。
状态	客户端当前与 AP 的连接状态。

8.5.1 导出用户信息

步骤1 点击「AC 管理」>「用户状态」；

步骤2 点击 导出 ，之后按页面提示操作。

8.5.2 刷新用户信息

步骤1 点击「AC 管理」>「用户状态」；

步骤2 点击 刷新 。

第9章 PPPoE 认证

9.1 概述

路由器支持 PPPoE 认证。您可参考以下说明选择要启用的认证方式。

如果局域网中有线和无线连接的计算机都要进行认证上网，选择“PPPoE 认证”。

9.1.1 功能介绍

默认情况下，路由器接入互联网后，连接到路由器局域网的计算机就可以访问互联网了。开启 PPPoE 认证功能后，路由器下的计算机访问网络前，需要先进行宽带拨号，连接成功后才能上网。

路由器还支持账号到期提醒功能。网络管理员可以设置路由器，使其在用户账号到期前 7 天之内及到期后提醒用户，从而简化网络管理工作，并提高网管工作效率。另外，还可以配置不需要认证主机、用户流控策略。

9.1.2 配置向导

路由器的 PPPoE 认证配置步骤如下表所示。

表9-1 配置向导

配置任务	说明
基本设置	开启 PPPoE 认证，并设置相关认证参数。在「PPPoE 认证」>「基本设置」页面进行。
用户管理	配置宽带连接账号。用户需要使用该账号进行宽带拨号，才能访问互联网。 在「PPPoE 认证」>「用户管理」页面进行。

9.2 配置 PPPoE 认证

9.2.1 基本设置

进入页面的方法：点击「PPPoE 认证」>「基本设置」。在这里，可以设置 PPPoE 服务器、账号到期提醒、不需要认证的主机、用户流控策略。

配置 PPPoE 服务器

开启/关闭 PPPoE 认证功能，设置 PPPoE 服务器相关参数。

图9-1 PPPoE 服务器

表9-2 PPPoE 服务器参数说明

标题项	说明
PPPoE 认证	开启/关闭路由器的 PPPoE 认证功能。开启 PPPoE 认证功能后，路由器的其他认证功能自动关闭。
服务器 IP 地址	设置 PPPoE 服务器的 IP 地址。建议保持默认设置，如必须修改时，通常建议也将此 IP 设在私网 IP 段。私网 IP 如下。 ● A 类：10.0.0.1～10.255.255.254 ● B 类：172.16.0.1～172.31.255.254 ● C 类：192.168.0.1～192.168.255.254
PPPoE 用户起始/结束 IP	设置用户宽带拨号成功后，PPPoE 服务器可以分配给用户的 IP 地址的范围。PPPoE 用户起始/结束 IP 必须与服务器 IP 地址在同一个网段。
主/次 DNS 服务器	路由器分配给 PPPoE 用户的域名服务器地址，一般与路由器 WAN 口设置的主/次 DNS 地址相同。

配置用户流控策略

路由器支持用户流控策略配置，可以有效控制 PPPoE 用户的网络带宽，防止某些用户抢占过多带宽，导致其它用户网速过慢甚至不可用。默认的用户流控策略如下。

图9-2 用户流控策略

表9-3 用户流控策略参数说明

标题项	说明
策略名称	流控策略名称，暂不支持修改。 启用 PPPoE 认证功能后，路由器原“流量控制”功能将由 PPPoE“用户流控策略”代替。
上行/下行速率	对应策略的上行/下行速率。这些策略将会关联到 PPPoE 用户账号，使用流控策略关联账号认证上网的用户的最大上行/下行速率为此速率。
操作	点击可修改上行/下行速率，默认为 1024KB/s。1Mbps=128KB/s=1024kb/s，1B=8b 如果修改的流控策略已经被 PPPoE 账号引用，则修改后，该 PPPoE 账号将自动引用修改后的流控策略。

配置账号到期提醒

路由器支持账号到期提醒功能，网络管理员还可以自定义到期前多少天进行提醒，以及到期前/已到期的提醒页面显示效果。

图9-3 账号到期提醒

表9-4 账号到期提醒参数说明

标题项	说明
到期前提醒时间	设置账号到期前多少天进行提醒。默认为账号到期前 7 天提醒。
上行/下行速率	对应策略的上行/下行速率。这些策略将会关联到 PPPoE 用户账号，使用流控策略关联账号认证上网的用户的最大上行/下行速率为此速率。
账号到期前提醒页面	设置账号到期前提醒的页面信息。点击 配置页面 可以修改页面提醒信息，如下图示。  完成设置后，您可以点击 预览页面 预览效果。
账号已到期提醒页面	设置账号已到期提醒的页面信息。点击 配置页面 可以修改页面提醒信息，如下图示。  完成设置后，您可以点击 预览页面 预览效果。

配置不需要认证的主机

新增不需要认证的主机

步骤1 点击「PPPoE 认证」>「基本设置」，找到“不需要认证的主机”模块；

步骤2 点击 +新增 ；

步骤3 在【新增】窗口配置各项参数；

步骤4 点击 确定 。

图9-4 新增不需要认证的主机

表9-5 新增不需要认证主机的参数说明

标题项	说明
MAC 地址	不需要认证即可上网的计算机的网卡物理地址。。
备注	该计算机的描述信息。可不填。
操作	+ ：点击可以新增一条不受限制主机。 - ：点击可以删除本条不受限制主机。

成功添加“不需要认证的主机”后，您可以在「PPPoE 认证」>「基本设置」页面查看到已添加的不需要认证主机。如下图示例。

图9-5 成功添加不需要认证的主机

修改不需要认证的主机

步骤1 点击「PPPoE 认证」>「基本设置」，找到“不需要认证的主机”模块；

步骤2 点击操作栏的 。

删除不需要认证的主机

步骤1 点击「PPPoE 认证」>「基本设置」，找到“不需要认证的主机”模块；

步骤2 如果要删除某一个不需要认证主机，请点击操作栏的 。如果要同时删除多个不需要认证主机，请选中要删除的多个规则，然后点击 删除 。

9.2.2 用户管理

在这里，您可以设置 PPPoE 认证账号信息。开启 PPPoE 认证功能时，用户需要使用此处设置的用户名、密码进行宽带拨号上网。

进入页面的方法：点击「PPPoE 认证」>「用户管理」。进入页面后，默认显示如下。

图9-6 用户管理

新增账号

步骤1 点击「PPPoE 认证」>「用户管理」；

步骤2 点击 +新增 ；

步骤3 在【新增】进行各项参数配置；

步骤4 点击 确定 。

图9-7 新增用户管理

表9-6 新增 PPPoE 账号参数说明

标题项	说明
用户名	用户进行 PPPoE 认证（宽带连接）时需要输入的用户名/密码。
密码	
流控策略	选择该账号对应的用户流控策略。流控策略可以在「PPPoE 认证」>「基本设置」页面的“用户流控策略”模块进行配置。
并发连接数	可以对 PPPOE 账号进行连接数限制，范围为 0-4000，0 表示不做限制。
备注	该账号的描述信息。可不填。
到期时间	该账号的到期时间。过了到期时间后，该账号仍然可以拨号成功，但不能上网。
状态	该账号的启用/禁用状态。

账号添加成功后，可以在「PPPoE 认证」>「用户管理」页面查看到已添加的 PPPoE 账号。如下图示例。

图9-8 成功添加 PpoE 账号

修改 PPPoE 认证账号

步骤1 点击「PPPoE 认证」>「用户管理」；

步骤2 如果要修改 PPPoE 账号，请点击对应操作栏的，如果要禁用/启用该账号，请点击操作栏的 / 。

删除 PPPoE 认证账号

步骤1 点击「PPPoE 认证」>「用户管理」；

步骤2 如果要删除某条 PPPoE 账号，请点击对应操作栏的；如果要同时删除多个账号，请选中要删除的多个账号，然后点击 删除 。

导出/导入 PPPoE 用户账号数据

路由器还支持导出/导入 PPPoE 用户数据功能。网络管理员可以将已配置好的 PPPoE 用户数据导出到本地电脑保存，当 PPPoE 用户数据丢失时，可以直接导入之前的用户数据，不用重新添加。

导出 PPPoE 用户账号数据：

步骤1 点击「PPPoE 认证」>「用户管理」；

步骤2 点击 导出数据 ，按页面提示即可导出文件名为“pppoe_user.cfg”的文件。

导入 PPPoE 用户账号数据：

步骤1 点击「PPPoE 认证」>「用户管理」；

步骤2 点击 浏览... ，加载之前导出的用户数据文件“pppoe_user.cfg”，然后点击 导入数据 。

9.3 PPPoE 认证配置举例

组网需求

某小区宽带服务商使用网关路由器为某栋出租屋提供网络服务：租客上网时，需要先进行 PPPoE 拨号（宽带连接）；该楼管理员要上网时，无需认证，自动获取 IP 地址即可。

可通过路由器的 PPPoE 认证功能实现上述需求，具体如下：启用 PPPoE 服务器，并添加账号和密码（分配给租客），然后将管理员电脑设置为“不需要认证的主机”。

网络拓扑

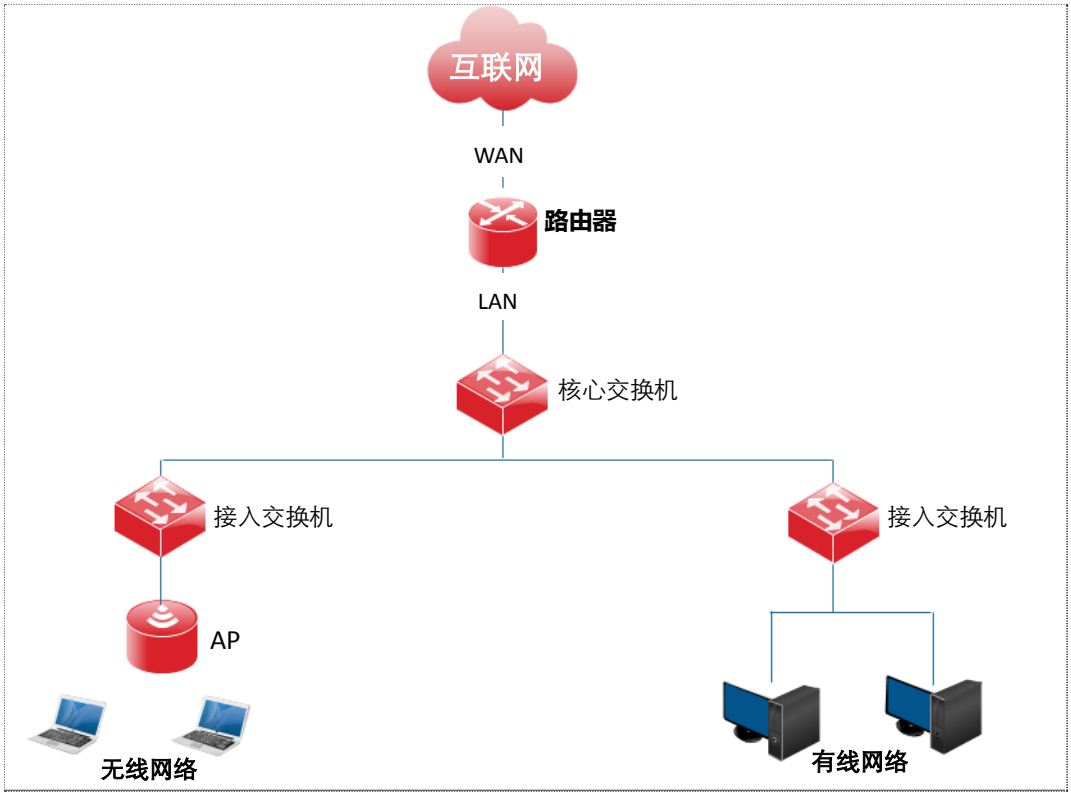


图9-9 PPPoE 认证配置

配置步骤

说明

配置步骤中，其他未提到的参数，请保持默认设置即可。

步骤1 进行 PPPoE 认证基本配置；

进入「PPPoE 认证」>「基本设置」页面进行以下设置。

1. 开启 PPPoE 认证功能，并设置账号到期提醒时间。

- PPPoE 认证：选择“开启”。

- 点击页面底端的 确定 。

图9-10 开启 PPPoE 认证

2. 配置账号到期提醒页面。

在“账号到期提醒”模块进行下述设置。

– 到期前提醒时间：选择账号到期前多少天进行提醒，如“3 天”。

– 账号到期前提醒页面：点击 配置页面 ，设置“公告标题”和“公告内容”，点击 确定 ；

图9-11 账号到期前提醒页面

– 账号已到期提醒页面：点击 配置页面 ，设置“公告标题”和“公告内容”，点击 确定 。

图9-12 账号已到期提醒页面

3. 新增不需要认证主机。

- 在“不需要认证主机”模块，点击 +新增 ；
- 在【新增】窗口进行下述参数设置；
- MAC 地址：输入上网时不需要认证的用户的电脑 MAC，本例为“44:37:E6:12:34:56”。
- 备注：输入该用户电脑 MAC 的描述，如“网络管理员”。
- 点击 确定 。

图9-13 新增不需要认证主机

4. 配置用户流控策略。

在“用户流控策略”模块点击 修改上行/下行速率，如某租客办理的网络带宽为 4Mbps，则修改如下。

图9-14 编辑流控策略

步骤2 添加 PPPoE 认证账号。

1. 点击「PPPoE 认证」>「用户号管理」；
2. 点击 +新增 ；
3. 在【新增】窗口配置下述参数；

- 用户名：输入 PPPoE 认证用户名，如“zhangsan”。
- 密码：输入 PPPoE 认证用户名对应的密码，如“zhangsan”。
- 备注：输入该用户的描述，如“张三”。也可以不填。
- 流控策略：根据该用户办理的宽带带宽，选择流控策略。
- 到期时间：该用户所办理的宽带的到期时间，如“2017 年 12 月 31 日”。
- 状态：选择“启用”。

4. 点击 确定 。

图9-15 新增 PPPoE 认证账号

如果有多个租客要办理宽带，请参考上述步骤添加多个账号即可。

验证配置

管理员访问网络时无需认证。租客访问网络时，需要先在电脑上进行宽带连接，步骤如下（以 Window 7 为例说明）。

步骤1 点击桌面左下角的开始图标；

步骤2 点击**控制面板>网络和 Internet>网络和共享中心>设置新的连接或网络**；

图9-16 设置新的连接或网络

步骤3 选择**连接到 Internet**，然后点击 下一步 ；

图9-17 连接到 Internet

步骤4 点击宽带（PPPoE）（R）；

图9-18 宽带（PPPoE）（R）

步骤5 填写 **PPPoE 认证用户名**和**密码**，本例中用户名为 zhangsan，密码为 zhangsan，勾选**记住此密码（R）**，点击 连接 。

图9-19 连接到 Internet

稍等片刻，拨号成功，可以上网了。

以后每次开机后，点击电脑桌面右下角的网络图标，然后点击**宽带连接**，拨号成功后即可正常上网。

第10章 虚拟服务器

10.1 概述

路由器的「虚拟服务器」模块包括：端口映射、UPnP、DMZ 主机、DDNS。

- 端口映射

  默认情况下，广域网中的用户不能主动访问局域网内的计算机。端口映射开放了一个服务端口，并以 IP 地址和内网端口来指定其对应的局域网服务器，之后，路由器将广域网中对此服务端口的请求定位到该局域网服务器上，这样，广域网中的用户就能够访问局域网计算机，局域网也能避免受到侵袭。

- UPnP

  UPnP（Universal Plug and Play），通用即插即用。UPnP 协议可以自动识别局域网计算机上支持 UPnP 的应用程序，并在路由器上为这些程序自动打开端口，实现自动端口映射功能。特别是在一些 P2P 应用上，如迅雷、BitComet、AnyChat 等，使用 UPnP 可以有效提高速率。

- DMZ 主机

  将局域网中某台计算机设置为 DMZ 主机后，该计算机与互联网通信时将不受限制。如某些视频会议和在线游戏，可将正在进行这些应用的计算机设置为 DMZ 主机，使视频会议和在线游戏更加顺畅。

- DDNS

  DDNS（Dynamic Domain Name Server），动态域名服务。当服务运行时，路由器上的 DDNS 客户端将其当前的 WAN 口 IP 地址传送给 DDNS 服务器，服务器再更新数据库中域名与 IP 地址的映射关系，实现动态域名解析。

  使用 DDNS 功能，可以让路由器动态变化的 WAN 口 IP 地址（公网 IP）始终被映射到一个固定的域名上。DDNS 功能一般与其他功能如端口映射、DMZ 主机、远端 WEB 管理等结合使用，这样，用户在进行诸如远程访问局域网服务器、远程访问路由器管理页面等应用时，无需再关注路由器的 WAN 口 IP 变化，直接使用对应的域名即可，更加方便易用。

10.2 端口映射

进入页面的方法：点击「虚拟服务器」>「端口映射」。进入页面后，默认显示如下。

图10-1 端口映射

10.2.1 配置端口映射

新增规则

步骤1 点击「虚拟服务器」>「端口映射」；

步骤2 点击 +新增 ；

步骤3 在【新增】窗口进行参数设置；

步骤4 点击 确定 。

图10-2 新增端口映射

表10-1 端口映射参数说明

标题项	说明
内网主机 IP	局域网内建立服务器的计算机的 IP 地址。
内部端口	局域网内服务器的服务端口。
外部端口	路由器开放给广域网用户访问的端口。
协议	相应服务的协议类型。“全部”表示 TCP 和 UDP。设置时，如果不确定服务的协议类型，可以选择“全部”。
接口	内网服务映射的 WAN 口，也是广域网用户访问局域网服务器时使用的 WAN 口。

规则添加成功后，可以在「虚拟服务器」>「端口映射」页面查看到已添加的端口映射规则。如下图示例。

图10-3 成功添加端口映射

修改规则

步骤1 点击「虚拟服务器」>「端口映射」；

步骤2 如果要修改端口映射规则参数，请点击操作栏的；如果要禁用/启用规则，请点击操作栏的 / 。

删除规则

步骤1 点击「虚拟服务器」>「端口映射」；

步骤2 如果要删除某条端口映射规则，请点击对应操作栏的；如果要同时删除多个端口映射规则，请选中要删除的多个规则，然后点击删除。

10.2.2 端口映射配置举例

组网需求

某企业使用网关路由器进行网络搭建，路由器已接入互联网，可以为局域网用户提供上网服务。该企业内部有一个 Web 服务器，需要开放给广域网用户，好让企业员工即使不在公司，也能访问企业内部网络。

可以使用路由器的端口映射功能实现上述需求。假设路由器开放给广域网用户访问的端口为 80。

网络拓扑

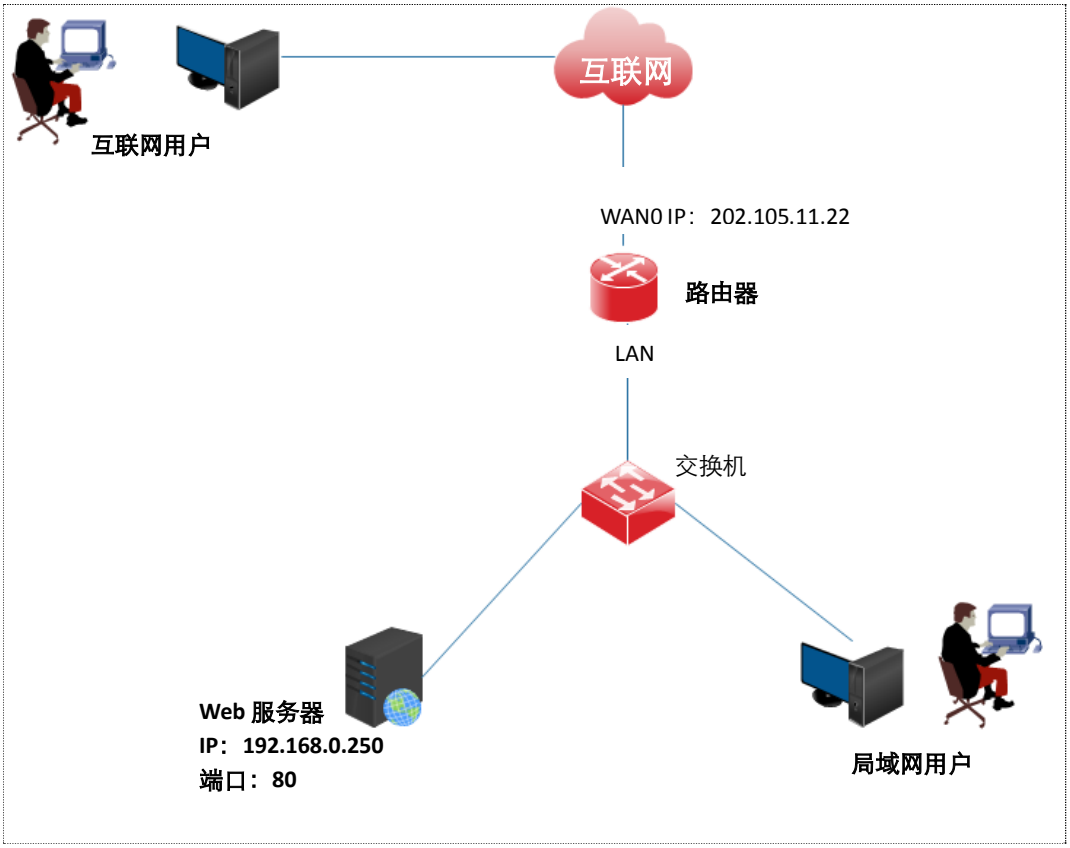


图10-4 端口映射配置

配置步骤

步骤1 点击「虚拟服务器」>「端口映射」，点击 +新增 ；

步骤2 配置端口映射规则。

1. 内网主机 IP：输入 Web 服务器的 IP 地址，本例为“192.168.0.250”。
2. 内网端口：输入 Web 服务器使用的端口，本例为“80~80”。

3. 外网端口：输入路由器开放给广域网用户访问的端口，本例为“80~80”。

4. 协议：Web 服务器使用的协议为“TCP”，如果您不清楚，可以选择“全部”。

5. 接口：选择内网服务映射的 WAN 口，本例为“WAN0”。

步骤3 点击 确定 。

图10-5 新增端口映射

添加完成，如下图示。

图10-6 成功添加端口映射

验证配置

互联网用户使用“内网服务应用层协议名称://对应 WAN 口 IP:外网端口”可以成功访问企业内部 Web 服务器。在本例中，访问地址为“http://202.105.11.22:80”。

如果对应 WAN 口开启了 DDNS，还可使用“内网服务应用层协议名称://对应 WAN 口域名:外网端口”访问。

说明

配置完成后，如果互联网用户仍然无法访问局域网 Web 服务器，请依次尝试以下方法解决。

- 确保路由器 WAN 口获取的是公网 IP 地址，您填写的内网端口段是正确的相应服务端口。
- 可能是局域网服务器上的系统防火墙、杀毒软件、安全卫士阻止了互联网用户访问，请关闭这些程序后再尝试。
- 手动配置局域网服务器 IP，避免因为 IP 的自动变化而导致服务中断。

10.3 UPnP

路由器默认关闭了 UPnP 功能。

开启 UPnP：

步骤1 点击「虚拟服务器」>「UPnP」；

步骤2 选择“开启”UPnP；

步骤3 点击 确定 。

图10-7 UPnP

开启 UPnP 功能后，当局域网中运行支持 UPnP 的程序（如迅雷等）时，就可以在 UPnP 页面看到的应用程序发出请求时提供的端口转换信息。如下图示例。

图10-8 开启 UPnP

10.4 DMZ 主机

进入页面的方法：点击「虚拟服务器」>「DMZ 主机」。进入页面后，默认显示如下。

注意

- 当把计算机设置成 DMZ 主机后，该计算机相当于完全暴露于外网，路由器的防火墙对该计算机不再起作用。
- 黑客可能会利用 DMZ 主机对本地网络进行攻击，请不要轻易使用 DMZ 主机功能。

图10-9 DMZ 主机

10.4.1 配置 DMZ 主机

步骤1 点击「虚拟服务器」>「DMZ 主机」；

步骤2 在对应的 WAN 口选择“开启”，然后输入局域网内需要设置为 DMZ 主机的计算机的 IP 地址；

步骤3 点击 确定 。

10.4.2 DMZ 主机配置举例

组网需求

某企业使用网关路由器进行网络搭建，路由器已接入互联网，可以为局域网用户提供上网服务。该企业内部有一个 Web 服务器，需要开放给广域网用户，好让企业员工即使不在公司，也能访问企业内部网络。

可以使用路由器的 DMZ 功能实现上述需求。

网络拓扑

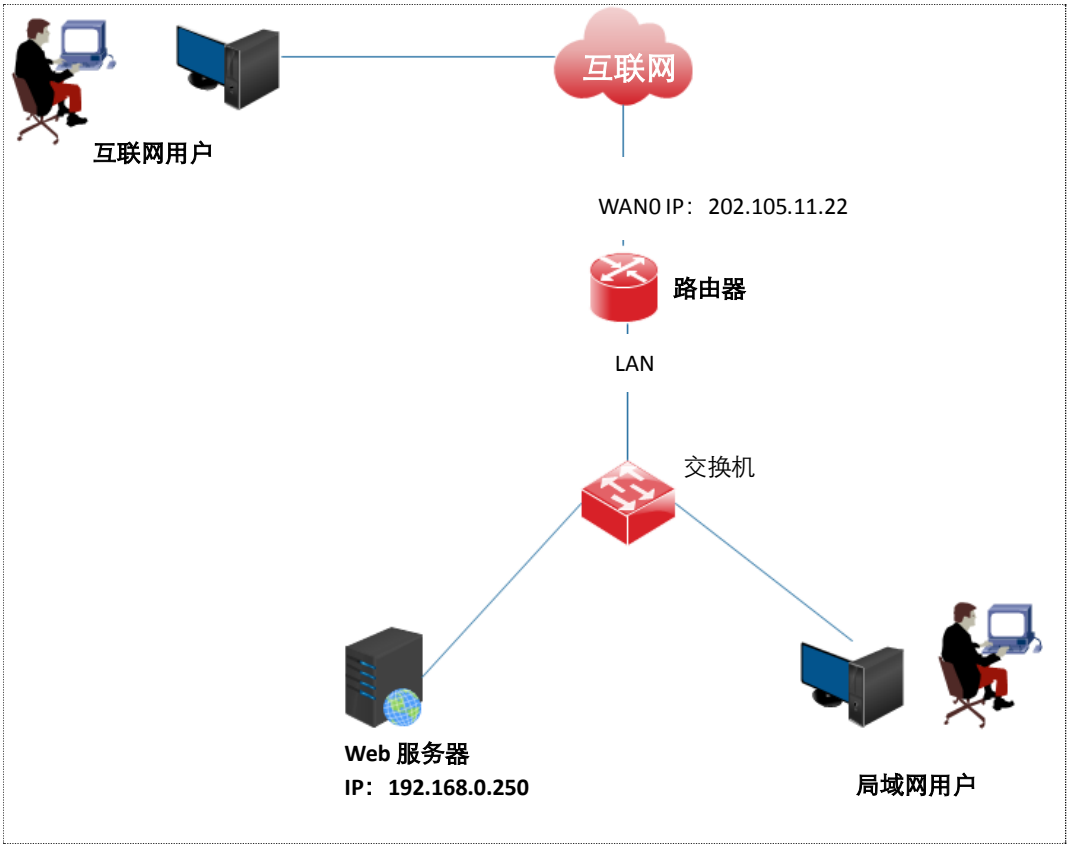


图10-10 DMZ 主机配置

配置步骤

步骤1 点击「虚拟服务器」>「DMZ 主机」；

步骤2 设置 WAN0 口；

步骤3 DMZ 主机：选择“开启”；

步骤4 主机 IP 地址：输入局域网中 Web 服务器的 IP 地址，本例为“192.168.0.250”；

步骤5 点击 确定 。

图10-11 配置 DMZ 主机

验证配置

互联网用户使用“内网服务应用层协议名称://对应 WAN 口 IP”可以成功访问企业内部 Web 服务器。在本例中，访问地址为“http://202.105.11.22”。

如果对应 WAN 口开启了 DDNS，还可使用“内网服务应用层协议名称://对应 WAN 口域名”访问。

说明

配置完成后，如果互联网用户仍然无法访问局域网 Web 服务器，请依次尝试以下方法解决。

- 确保路由器 WAN 口获取的是公网 IP 地址。
- 可能是局域网服务器上的系统防火墙、杀毒软件、安全卫士阻止了互联网用户访问，请关闭这些程序后再尝试。
- 手动配置局域网服务器 IP，避免因为 IP 的自动变化而导致服务中断。

10.5 DDNS

进入页面的方法：点击「虚拟服务器」>「DDNS」。进入页面后，默认显示如下。

图10-12 DDNS

10.5.1 配置 DDNS

步骤1 点击「虚拟服务器」>「DDNS」，找到对应 WAN 口模块；

步骤2 DDNS 状态：选择“开启”；

步骤3 设置各 DDNS 参数；

步骤4 点击 确定 。

图10-13 配置 DDNS

表10-2 DDNS 参数说明

标题项	说明
DDNS 状态	开启/关闭 DDNS 功能。
DDNS 供应商	DDNS 的服务提供商。路由器支持的 DDNS 服务提供商有： 3322.org、88ip.cn、oray.com（花生壳）、gnway.com（金万维）。
服务类型	仅对 oray.com 有效，该 DDNS 账号的类型。
用户名	登录 DDNS 服务的用户名，即在“DDNS 供应商”网站上注册的登录用户名。
密码	登录 DDNS 服务的密码，即在“DDNS 供应商”网站上注册的登录用户名对应的登录密码。
域名信息	从 DDNS 服务器获取的域名信息。除了 oray.com 外，设置其他 DDNS 提供商时，需要手动输入在其网站上申请的域名。
联网状态	显示 DDNS 服务的运行状态。

10.5.2 DDNS 配置举例

组网需求

某企业使用网关路由器进行网络搭建，路由器已接入互联网，可以为局域网用户提供上网服务。该企业内部有一个 Web 服务器，需要开放给广域网用户，好让企业员工即使不在公司，也能访问企业内部网络。

网络管理员使用路由器的端口映射功能实现上述需求（假设路由器开放给广域网用户访问的端口为 80）。另外，为避免路由器 WAN 口 IP 动态变化导致广域网用户不能正常访问，管理员还开启了路由器的 DDNS 功能，使广域网用户可以每次都能使用同一域名访问。

网络拓扑

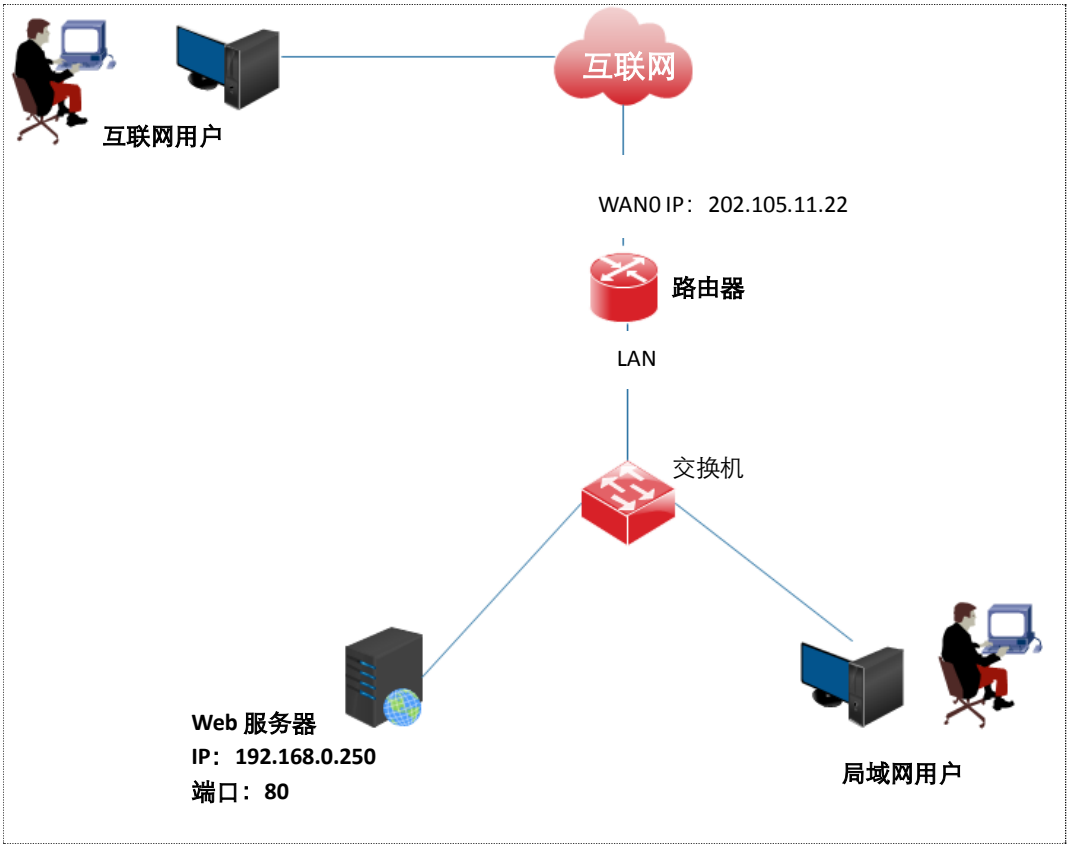


图10-14 DDNS 配置

配置步骤

步骤1 配置端口映射

在「虚拟服务器」>「端口映射」页面，配置如下规则。若有需要，可参考端口映射新增规则。

图10-15 配置端口映射

步骤2 配置 DDNS

1. 注册域名。

登陆到 DDNS 供应商网站进行注册。假设您到 3322.org 网站注册的用户名为 hikvision，密码为 123456，申请到的域名为 hikvision.3322.org。

2. 设置 DDNS。

登录到路由器的管理页面，设置对应 WAN 口。本例为“WAN0”。

- DDNS 状态：选择“开启”；
- DDNS 供应商：选择您申请域名的 DDNS 供应商，本例为“3322.org”；
- 用户名：输入您在 DDNS 供应商网站注册的用户名，本例为“hikvision”；
- 密码：输入您在 DDNS 供应商网站注册的用户名对应的密码，本例为“123456”；
- 域名信息：输入您从 DDNS 供应商网站申请的域名，本例为“hikvision.3322.org”；

说明

如果您使用的 DDNS 供应商为“oray.com”，即“花生壳”，则无需输入域名信息。

3. 点击 确定 。

图10-16 配置 DDNS

完成设置后，刷新一下页面，稍等片刻。当 WAN0 口“联网状态”显示为**已连接**时，连接成功。

验证配置

广域网用户使用“内网服务应用层协议名称://对应 WAN 口域名:外网端口”可以成功访问企业内部 Web 服务器。在本例中，访问地址为“http://hikvision.3322.org:80”。

说明

配置完成后，如果互联网用户仍然无法访问局域网 Web 服务器，请依次尝试以下方法解决。

- 确保路由器 WAN 口获取的是公网 IP 地址，您填写的内网端口段是正确的相应服务端口。
- 可能是局域网服务器上的系统防火墙、杀毒软件、安全卫士阻止了互联网用户访问，请关闭这些程序后再尝试。
- 手动配置局域网服务器 IP，避免因为 IP 的自动变化而导致服务中断。

第11章 USB 应用

11.1 概述

路由器提供了一个 USB 接口，支持 USB 文件共享。

路由器能自动识别插上其 USB 接口的 USB 存储设备，并在管理页面显示该 USB 设备的磁盘使用率等信息。网络中的用户可以共享访问 USB 存储设备上的文件，路由器支持文件访问权限管理。

11.2 USB 文件共享

进入页面的方法：点击「USB 应用」>「USB 文件共享」。

图11-1 USB 文件共享

路由器插上 U 盘后，可以自动识别 U 盘信息，如下图示例。

图11-2 基本设置

表11-1 基本设置参数说明

标题项	说明
Sda1	路由器插上 USB 存储设备后，显示该设备的磁盘使用率。
安全弹出	需要拔除 USB 存储设备时，为了避免 USB 设备丢失数据，请先点击 安全弹出 ，再拔下该 USB 设备。
本地访问	路由器 LAN 侧（局域网）用户访问 USB 存储设备文件的地址。 ● ftp://192.168.0.252:21：点击此链接即可访问，也可将此链接复制到电脑浏览器进行访问。 ● \\192.168.0.252：需要将此地址复制到电脑的“开始”>“运行”菜单中，才能访问。 **说明** 192.168.0.252 为路由器的当前 LAN 口 IP 地址，如果路由器的 LAN 口 IP 地址改变，则本地访问地址也会相应改变。
允许互联网访问	启用/禁用互联网访问功能。 ● 启用：用户可以通过互联网访问 USB 存储设备上的文件。启用时，将显示互联网访问地址。 ● 禁用：用户不能通过互联网访问 USB 存储设备上的文件。默认为“禁用”。
互联网访问	启用“允许互联网访问”时，显示路由器 WAN 侧用户访问 USB 存储设备文件的地址。
用户名/密码	用户访问 USB 存储设备时需输入的用户名/密码。
权限	用户访问 USB 存储设备时输入的账号的权限。 ● 读写：用户可以查看、修改 USB 存储设备上的文件。账号默认用户名和密码均为“admin”。 ● 只读：用户只能查看 USB 存储设备上的文件，不能对文件进行修改。账号默认用户名和密码均为“guest”。

11.3 用户共享 USB 存储设备资源

组网需求

某企业使用网关路由器进行网络搭建，在路由器的 USB 接口接了一个移动存储设备作为服务器，公司员工在局域网或互联网都可以登录到该服务器去查找、下载资料。

假设读写账户的用户名/密码为“xxadmin”，只读账户的用户名/密码均为“xxguest。

网络拓扑

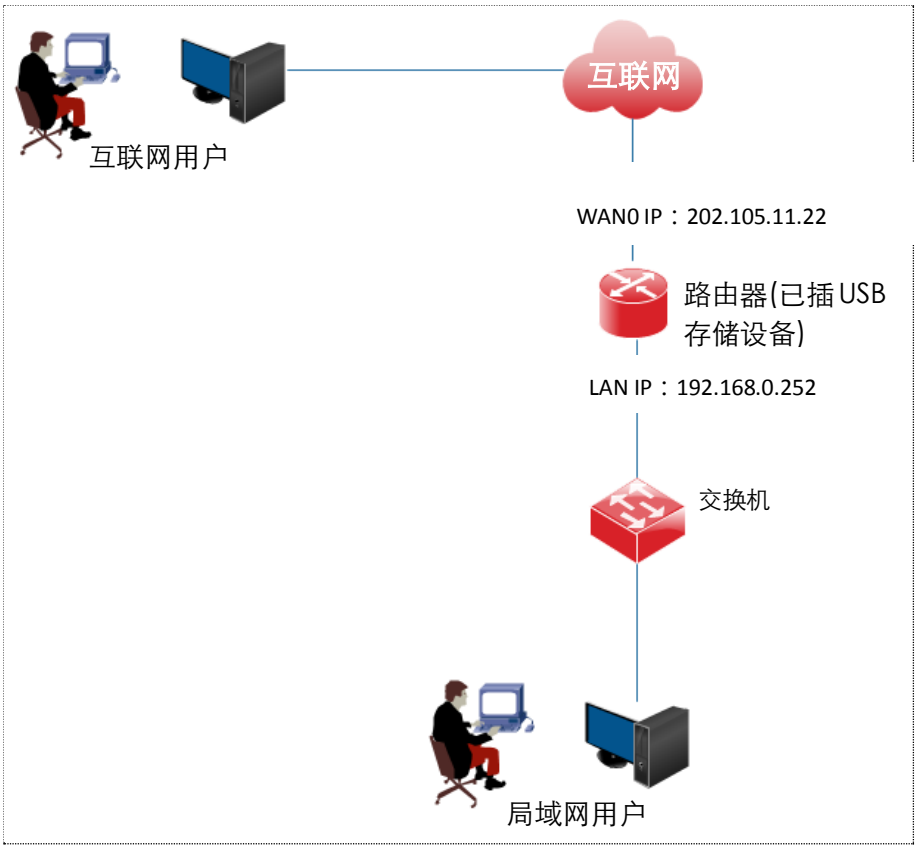


图11-3 用户共享 USB 存储设备

配置步骤

步骤1 点击「USB 应用」>「USB 文件共享」；

步骤2 允许互联网访问：选择“启用”；

步骤3 将读写用户名/密码均改为“xxadmin”，只读用户名改为“xxguest”；

步骤4 点击页面底端 确定 。

图11-4 基本设置

验证配置

局域网用户访问服务器：

方法 1：在电脑浏览器里访问网址 ftp://192.168.0.252:21。

方法 2：在电脑左下角访问\\192.168.0.252。以 Windows 10 为例，操作步骤为：在电脑左下角“搜索 Web 和 Windows” 

处输入\\192.168.0.252，回车。

访问时会出现下述页面，输入相应权限的用户名/密码，点击 确定 即可。

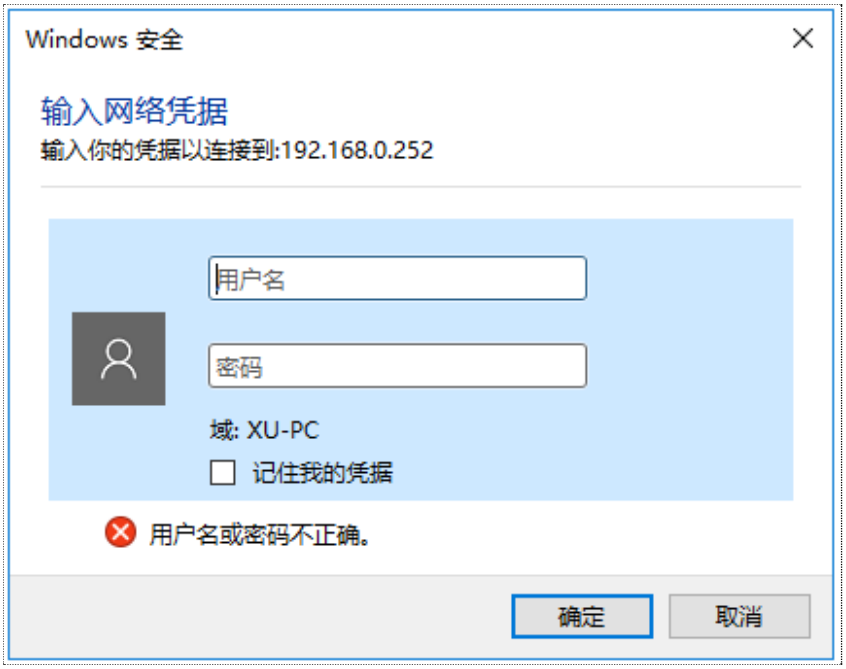


图11-5 局域网用户访问路由器

互联网用户访问服务器:

在电脑浏览器里访问网址 ftp://202.105.11.22:21，出现用户名/密码认证页面，输入相应权限的用户名/密码即可。

第12章 系统管理

路由器的「系统管理」模块包括：

登录密码、重启、配置备份/恢复、软件升级、策略升级、恢复出厂设置、系统时间、排障工具。

12.1 登录密码

在“登录密码”页面，您可以修改路由器的登录密码。首次使用路由器时，需要设置登录密码。

点击「系统管理」>「登录密码」进入页面。

图12-1 登录密码

12.1.2 修改登录密码

步骤1 点击「系统管理」>「登录密码」；

步骤2 旧密码：输入当前路由器的登录密码；

步骤3 新密码：设置新的登录密码；

步骤4 确认密码：再一次输入新的登录密码；

步骤5 点击 确定 。

页面将会跳转到登录页面，此时输入刚才设置的密码，然后点击 登录 ，即可登录到路由器的管理页面。

12.2 重启

在“重启”页面，您可以重新启动路由器。当您设置的某项参数不能正常生效时，可以尝试手动重启路由器解决。另外，您还可以设置周期性定时地自动重启路由器，预防路

由器长时间运行导致其出现性能下降、不稳定等现象。点击「系统管理」>「重启」进入页面。

图12-2 重启

12.2.1 手动重启路由器

点击「系统管理」>「重启」，点击 重启 ，然后根据页面提示操作。

12.2.2 定时重启路由器

步骤1 点击「系统管理」>「重启」，选择“开启”定时重启；

步骤2 重启时间：选择路由器自动重启的时间点，如“3:00”；

步骤3 重复：设置路由器自动重启的日期，如指定“星期四”；

步骤4 点击 确定 。

图12-3 开启定时重启

之后，每个星期四的凌晨 3 点，路由器将自动重启。

说明

自动重启时间以路由器的系统时间为准，为避免重启时间出错，请确保您已正确设置了路由器的系统时间。

12.3 配置备份/恢复

使用配置备份功能，可以将路由器当前的配置信息保存到本地电脑；使用配置恢复功能，可以将路由器配置还原到之前备份的配置。

如，当您对路由器进行了大量的配置，使其在运行时拥有较好的状态/性能，或更符合对应环境的需求，此时建议对该配置进行备份；当您对路由器进行了升级操作、恢复出厂设置等操作后，可以恢复路由器原有的配置文件。

点击「系统管理」>「配置备份/恢复」进入页面。

图12-4 配备备份/恢复

12.3.1 配置备份

步骤1 点击「系统管理」>「配置备份/恢复」；

步骤2 点击 备份 ，之后按电脑提示选择备份文件的存储路径。

12.3.2 配置恢复

步骤1 点击「系统管理」>「配置备份/恢复」；

步骤2 点击 浏览 ，选择并加载之前备份的配置文件；

步骤3 点击 恢复 ，之后按路由器管理页面提示操作。

12.4 软件升级

通过软件升级，可以使路由器获得更多新增功能或更稳定的性能。本路由器支持“本地升级”。

本地升级：您需要先访问 HIKVISION 官方网站 www.hikvision.com/cn 下载升级软件到本地电脑，然后再进行升级。

进入页面的方法：点击「系统管理」>「软件升级」。

图12-5 软件升级

下文详述本地升级的步骤。

注意

为了确保升级正确，避免路由器损坏，请在升级之前，务必确认软件的正确性；升级过程中，请勿断开路由器电源。

步骤1 登陆 HIKVISION 官方网站 www.hikvision.com/cn，下载最新的升级软件并存放到本地电脑；

步骤2 进入路由器的「系统管理」>「软件升级」页面；

步骤3 升级类型：选择“本地升级”；

步骤4 点击 浏览 ，找到并载入相应目录下的升级软件；

步骤5 点击 升级 。

将出现进度条，等待进度条走完即可。进度条走完后，您可重新登录路由器，进入「系统状态」>「系统信息」页面，在“系统信息”模块查看路由器当前的软件版本号。

注意

为了更好的体验高版本软件的稳定性及增值功能，路由器升级完成后，建议将路由器恢复出厂设置，然后重新配置路由器。

12.5 策略升级

使用策略升级功能，您可以更新路由器行为管理模块的应用特征库和 URL 特征库，而不对路由器系统软件进行更新。本路由器支持“本地升级”。

本地升级：您需要先访问 HIKVISION 官方网站 www.hikvision.com/cn 下载策略升级软件到本地电脑，然后再进行升级。

进入页面的方法：点击「系统管理」>「策略升级」。

图12-6 策略升级

策略升级步骤：

步骤1 登录 HIKVISION 官方网站 www.hikvision.com/cn，下载最新的策略文件并存放到本地电脑；

步骤2 进入路由器的「系统管理」>「策略升级」页面；

步骤3 点击 浏览 ，找到并载入相应目录下的策略文件；

步骤4 点击 升级 。

将出现进度条，请等待进度条走完即可。进度条走完后，您可重新登录路由器，进入「系统管理」>「策略升级」页面，查看路由器当前的策略版本号。

12.6 恢复出厂设置

当局域网计算机不能访问互联网，但又找不到问题所在时；或您需要登录路由器的管理页面，但是却忘记登录密码时，可以将路由器恢复出厂设置后重新设置。路由器支持“软件恢复出厂设置”和“硬件恢复出厂设置”两种恢复出厂设置方式。

恢复出厂设置后，路由器的登录 IP 地址为 192.168.0.252。

注意

- 恢复出厂设置意味着路由器的所有设置将会丢失，您需要重新设置路由器才能上网。若不是万不得已，不建议将路由器恢复出厂设置。
- 为避免损坏路由器，恢复出厂设置过程中，请确保路由器供电正常。

12.6.1 软件恢复出厂设置

步骤1 点击「系统管理」>「恢复出厂设置」；

步骤2 点击 恢复出厂设置 。

图12-7 恢复出厂设置

12.6.2 硬件恢复出厂设置

使用此方式时，您无需进入路由器管理页面就可以将路由器恢复出厂设置。

操作方法：

步骤1 路由器通电情况下，用尖状物按住机身前面板上的 **Reset** 按钮 8 秒后放开；

步骤2 等待约 1 分钟。

12.7 系统时间

在“系统时间”页面，您可以设置路由器的系统时间。

为了保证路由器上行为管理等涉及时间的功能正常生效，需要确保路由器的系统时间准确。路由器支持“与网络时间同步”和“手动设置”两种时间设置方式，默认为“与网络时间同步”。

点击「系统管理」>「系统时间」进入页面。

图12-8 系统时间

12.7.1 与网络时间同步

系统时间自动同步互联网上的时间服务器。使用此方式时，只要路由器成功连接至互联网就能自动校准其系统时间，即路由器重启后，也能自行校准，无需网络管理员重新设置。

表12-1 网络时间同步参数说明

标题项	说明
同步时间周期	路由器向互联网上的时间服务器校对系统时间的时间间隔。
选择时区	选择路由器当前所在地区的标准时区。

设置完成后，您可以进入「系统状态」>「系统信息」页面，查看路由器的系统时间是否校对正确。

12.7.2 手动设置

网络管理员手动设置路由器的系统时间。如果使用此方式，则路由器每次重启后，您都需要重新设置路由器的系统时间。选择“手动设置”时，页面展开的相关参数如下图所示。

图12-9 系统时间

表12-2 系统时间参数说明

标题项	说明
日期/时间	可以直接在此处输入正确的时间。
与电脑同步	可以点击 与电脑同步 ，可将正在管理路由器的电脑的时间同步到路由器。

设置完成后，您可以进入「系统状态」>「系统信息」页面，查看路由器的系统时间是否校对正确。

12.8 排障工具

12.8.1 概述

在“排障工具”页面您可以检测网络通信情况。点击「系统管理」>「排障工具」，进入设置页面。

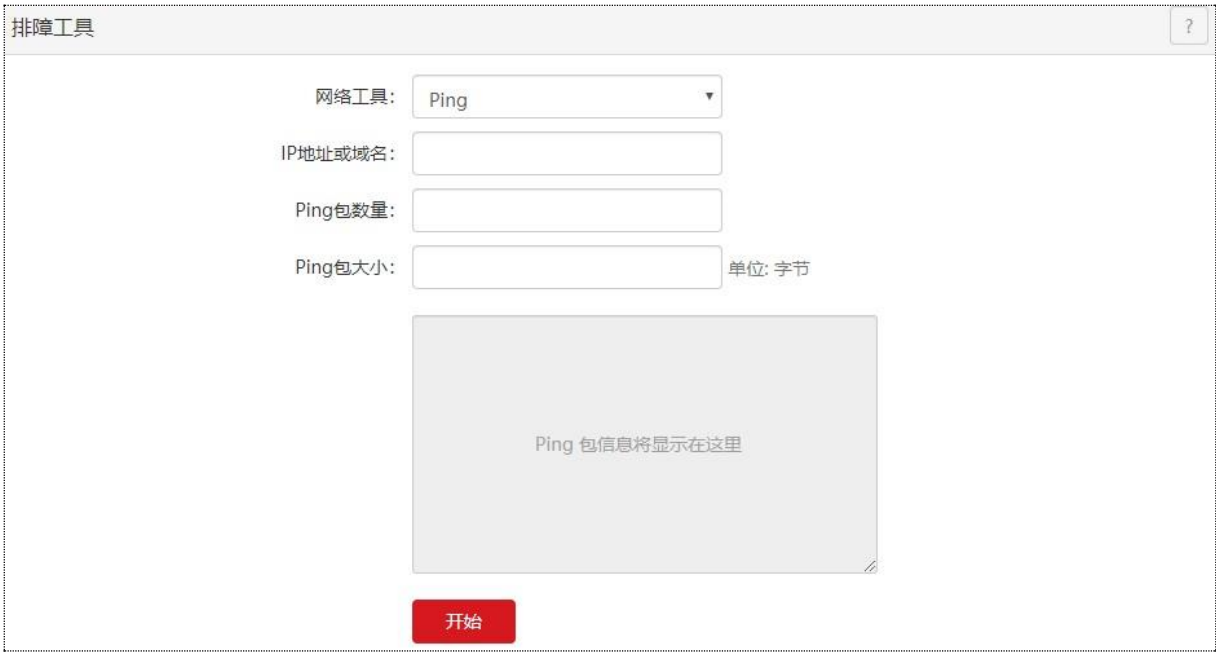


图12-10 排障工具

表12-3 排障工具参数说明

标题项	说明
Ping	常用的故障诊断与排除命令。它由一组 ICMP 回应请求报文组成，如果网络正常运行将返回一组回应应答报文。
Traceroute	路由跟踪实用程序，用于确定 IP 数据访问目标所采取的路径。

12.8.2 Ping 检测步骤

Ping 功能可以检测网络的连通性。假设要检测路由器与百度的连通性，可参考下文设置。

步骤1 进入「系统管理」>「排障工具」页面；

步骤2 点击下拉菜单，选择“Ping”；

步骤3 IP 地址或域名：输入要检测的 IP 地址或域名，本例为“www.baidu.com”；

步骤4 Ping 包个数：设置进行 Ping 包的个数，如“5”；

步骤5 数据包大小：设置 Ping 包的大小，如“100”；

步骤6 点击 开始 。

图12-11 网络工具 Ping

稍等片刻，结果将会显示在页面下方。

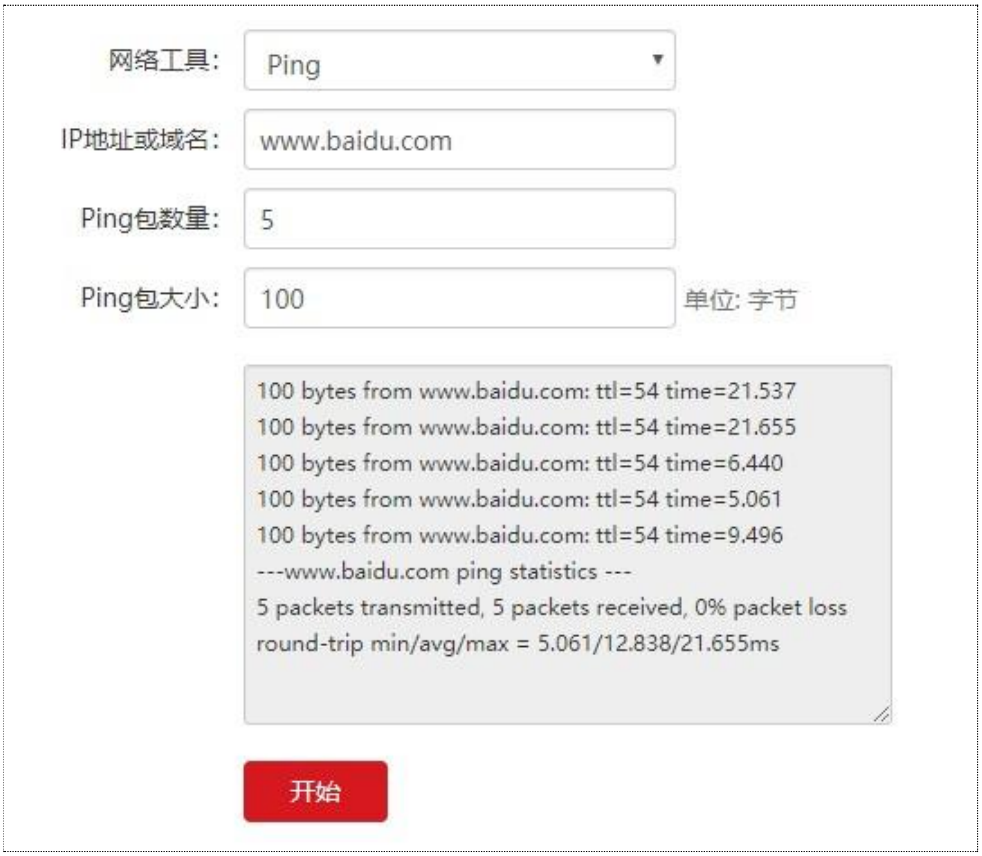


图12-12 Ping 结果

12.8.3 Traceroute 检测步骤

Traceroute 功能用于检测到目的 IP 地址或域名过程中的每一跳地址。假设要检测路由器到百度的路径，可设置如下。

步骤1 点击「系统管理」>「排障工具」；

步骤2 点击下拉菜单，选择“Traceroute”；

步骤3 目标 IP 或域名：输入要检测的 IP 地址或域名，本例为“www.baidu.com”；

步骤4 点击 开始 。

图12-13 网络工具 Traceroute

稍等片刻，结果将显示在页面下方。路径的记录按序列号从 1 开始，每个纪录是一跳，每跳表示一个网关。

图12-14 Traceroute 结果

第13章 系统状态

路由器的「系统状态」模块包括：系统信息、用户列表、流量统计、防攻击日志、系统日志、设备信息。

13.1 系统信息

在这里，您可以了解路由器的端口信息、系统信息、LAN 口信息、WAN 口信息。点击「系统状态」>「系统信息」进入页面。

13.1.1 端口信息

在“端口信息”模块，您可以查看路由器接口的连接状态以及当前所充当的角色（WAN 口或 LAN 口）。

图13-1 端口信息

13.1.2 系统信息

在“系统信息”模块，您可以查看路由器的设备名称、系统时间、运行时间、软件版本号、CPU 使用率及内存使用率。

图13-2 系统信息

13.1.3 LAN 口信息

在“LAN 口信息”模块，可以查看路由器的 LAN 口 MAC 地址和 IP 地址。

图13-3 LAN 口信息

13.1.4 WAN 口信息

在“WAN 口信息”模块，可以查看路由器当前所有的 WAN 口信息，包括：网线连接状态、IP 地址信息以及对应 WAN 口的连接状态等。

图13-4 WAN 口信息

13.2 用户列表

点击「系统状态」>「用户列表」进入页面。在这里，您可以查看路由器的各种用户列表信息，包括：DHCP 用户、VPN 用户、PPPoE 在线用户和 IPSec 安全联盟。

13.2.1 DHCP 用户

在这里，您可以查看局域网中从路由器的 DHCP 服务器获取 IP 地址信息的计算机数量及详细信息。「系统状态」>「用户列表」页面默认显示的就是 DHCP 用户信息。

图13-5 DHCP 用户

表13-1 DHCP 用户参数说明

标题项	说明
IP 地址	客户端从路由器 DHCP 服务器获取的 IP 地址。
MAC 地址	客户端的 MAC 地址。
在线时长	客户端的在线时长。
剩余租期	客户端 IP 地址的剩余租期。

13.2.2 VPN 用户

如果您已经在路由器上开启了 PPTP/L2TP 服务器功能，现需要了解拨入路由器 PPTP/L2TP 服务器的客户端数量及详细信息，请进入「系统状态」>「用户列表」页面后，点击 “VPN 用户”。

图13-6 VPN 用户

表13-2 VPN 用户参数说明

标题项	说明
用户名	VPN 客户端拨入 VPN 服务器使用的账号信息。
备注	对应账号的描述说明。
拨入 IP	VPN 客户端的 IP 地址。 如果 VPN 客户端是路由器，则显示路由器上绑定 VPN 功能的 WAN 口 IP 地址。
分配 IP	本路由器上的 VPN 服务器分配给 VPN 客户端的 IP 地址信息。

13.2.3 PPPoE 在线用户

如果您已经在路由器上开启了 PPPoE 认证功能，现需要了解拨入路由器 PPPoE 服务器的客户端数量及详细信息，请进入「系统状态」>「用户列表」页面后，点击“PPPoE 在线用户”。

图13-7 PPPoE 在线用户

表13-3 PPPoE 在线用户参数说明

标题项	说明
账号	客户端进行 PPPoE 认证（宽带连接）时使用的账号信息。
备注	对应账号的描述说明。
IP 地址	客户端从本路由器上的 PPPoE 服务器获取的 IP 地址。
上传/下载速率	客户端当前的上传/下载速率。

13.2.4 IPSec 安全联盟

如果您在路由器上新增了 IPSec 隧道，现需要了解 IPSec 安全联盟数及 IPSec 隧道的连接情况，请进入「系统状态」>「用户列表」页面后，点击“IPSec 安全联盟”。

图13-8 IPSec 安全联盟

表13-4 IPSec 安全联盟参数说明

标题项	说明
名称	IPSec 连接的名称。
SPI	SPI 参数值。 IPSec 连接的“外出 SPI”值与通信对端的“进入 SPI”值相同，“进入 SPI”值与通信对端的“外出 SPI”值相同。
方向	IPSec 连接数据的进出方向。
隧道两端	IPSec 连接数据在互联网上的传输方向。
数据流	IPSec 连接数据在局域网上的传输方向。
安全协议	IPSec 连接使用的安全协议。
AH 验证算法	IPSec 连接使用的 AH 验证算法。
ESP 验证算法	IPSec 连接使用的 ESP 验证算法。
ESP 加密算法	IPSec 连接使用的 ESP 加密算法。

13.3 流量统计

在这里，您可以查看路由器 WAN 口上/下行流量动态图，还可以了解局域网某个用户的上/下行速率，以及连接数。

进入页面的方法：点击「系统状态」>「流量统计」。

图13-9 流量统计

13.4 防攻击日志

路由器开启攻击防御中的功能后，如果发生攻击，路由器会将攻击情况显示在防攻击日志里。根据防攻击日志，网络管理员可以快速地定位攻击者，采取针对措施。进入页面的方法：点击「系统状态」>「防攻击日志」。

图13-10 防攻击日志

13.5 系统日志

路由器的系统日志记录了系统的启动、PPPoE 拨号、时间同步、设备登录、WAN 口连接等情况，如遇到网络故障，可以利用路由器的系统日志信息进行问题排查。

进入页面的方法：点击「系统状态」>「系统日志」。

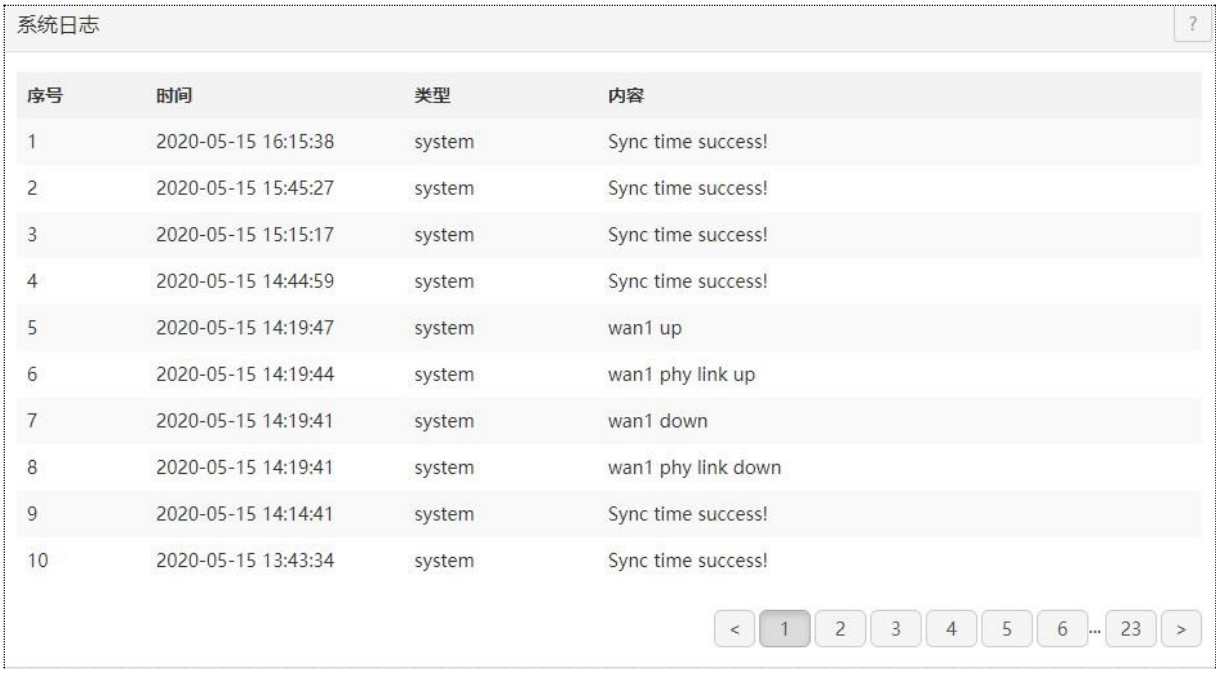


图13-11 系统日志

日志记录时间以路由器的系统时间为准，如果要让日志记录时间准确，请先确保路由器的系统时间准确。可以到「系统管理」>「系统时间」页面校准路由器的系统时间。

说明

- 路由器重启后，之前的日志信息将丢失。
- 断电后重新通电、软件升级、备份/恢复设置、恢复出厂设置等操作都会导致路由器重启。

13.6 设备信息

路由器的设备信息记录了路由器的设备名称，设备型号，设备 SN，固件版本号，设备 MAC 地址，设备二维码等情况。

进入页面的方法：点击「系统状态」>「设备信息」。

图13-12 设备信息

表13-5 设备信息参数说明

标题项	说明
设备名称	设备的名称。
设备型号	设备的型号。
设备 SN	设备的序列号。
固件版本号	设备的固件版本号。
设备 MAC 地址	设备的 MAC 地址。
设备二维码	设备的二维码，用于连接萤石云。

附录A 常见问题解答

问 1：输入 192.168.0.252 登录不了路由器的管理页面，怎么办?

答：请分别从以下几个方面检查：

- 请确保网线连接正确，且网线无松动现象。
- 确认电脑 IP 地址为 192.168.0.X（X 为 2~254，除开 252）。
- 清空浏览器的缓存或更换别的浏览器进行尝试。
- 关闭电脑的防火墙或更换别的电脑进行尝试。
- 确认局域网内没有其它的设备的 IP 地址也为 192.168.0.252。
- 若经过上述操作仍无法登录，请将路由器恢复出厂设置再重新登录。

问 2：想进入路由器的管理页面，但忘记了登录用户名和密码怎么办?

答：请将路由器恢复出厂设置再重新设置密码登录。

问 3：不能登录路由器管理页面的情况下，怎么将路由器恢复出厂设置?

答：在路由器启动完成的状态下，使用尖状物按住路由器 Reset 按钮 8 秒后放开，等待约 1 分钟即可。路由器恢复出厂设置后，需要重新配置参数。

问 4：连接路由器后，电脑出现“IP 地址与网络上的其他系统有冲突”提示信息，怎么办?

答：请参考以下方法解决。

- 确保局域网没有其他 DHCP 服务器或其它 DHCP 服务器已关闭。
- 确保局域网内的电脑没有占用路由器的 LAN 口 IP 地址，路由器出厂默认的 LAN 口 IP 是 192.168.0.252。
- 请确保局域网内为电脑静态设置的 IP 没有其它电脑使用。

附录B 产品规格

表B-1 产品规格

产品型号	DS-3WS256-E
带机量	300 台终端
可管理 AP 数	256 台
ARM	双核 1.4GHz
内存	4GB
FLASH	1GB
网络接口	5 个 10/100/1000Mbps 自适应 RJ45 端口
其它接口	1 个 USB 接口
指示灯	1 个 PWR 灯，1 个 SYS 灯，1 个 USB 灯，每个 RJ45 端口带有 1 个 Link 灯、1 个 Act 灯
按钮	1 个 Reset 按钮
工作环境	工作温度：0℃ ~ 40℃ 工作湿度：（10 ~ 90）%RH，无凝结
存储环境	存储温度：-40℃ ~ 70℃ 存储湿度：（5 ~ 90）%RH，无凝结
电源输入	100-240V AC，50/60Hz
外形尺寸（L*W*H）	440 mm*285mm*44mm

限制物质或元素标识表

《电器电子产品有害物质限制使用管理办法》限制物质或元素标识表

部分名称	《电器电子产品有害物质限制使用管理办法》限制物质或元素					
	铅(Pb)	汞(Hg)	镉(Cd)	六价铬(CrⅥ)	多溴联苯(PBB)	多溴二苯醚(PBDE)
金属部件	×	O	O	O	O	O
塑料部件	O	O	O	O	O	O
玻璃部件	×	O	O	O	O	O
线路板	×	O	O	O	O	O
电源（如果有）	×	O	O	O	O	O
附件	×	O	O	O	O	O
本表格依据 SJ/T 11364-2014 的规定编制。						
O 表示该有害物质在该部件所有均质材料中的含量均在 GB/T 26572-2011 规定的限量要求下。						
×表示该有害物质至少在该部件某一均质材料中的含量超出 GB/T 26572-2011 规定的限量要求，且目前业界没有成熟的替代方案，符合欧盟 RoHS 指令环保要求。						

本产品超过使用期限或者经过维修无法正常工作后，不应随意丢弃，请交由有废电器电子产品处理资格的企业处理，正确的方法请查阅国家或当地有关废弃电器电子产品处理的规定。

产品质量合格证
Qualification Card
PASS

保修服务

感谢您选用本产品，为了您能够充分享有完善的售后服务支持，请您在购买后认真阅读本产品保修卡的说明并妥善保存。
我们将按照海康威视产品标准保修承诺为您提供售后服务，售后服务政策明细请查看海康威视官网。部分信息摘录如下:
1. 保修期自产品首次购买之日起算，购买日以购买产品的发票日期为准。如无有效发票，则保修期将自产品出厂日推算。产品发票日期晚于产品实际交付日的，保修期自产品实际交付日起算。保修期限参考售后服务政策中的《海康威视产品标准保修期》执行。
2. 不保修范围(仅摘录部分,具体请见售后服务政策):
①超出规定的保修期限的;
②因误用、意外、改装、不适当的物理或操作环境、自然灾害、电涌及不当维护或保管导致的故障或损坏;
③第三方产品、软件、服务或行为导致的故障或损坏;
④产品使用过程中发生的正常脱色、磨损和消耗;
⑤产品可以不间断或无错误地正常运行;
⑥数据丢失或损坏;
⑦消耗零部件，除非是因材料或工艺缺陷而发生的故障;
⑧不能出示产品有效保修凭证和有效原始购物发票或收据，产品原序列号标签有涂改、替换、撕毁的现象、产品没有序列号或保修凭证上的产品型号或编号与产品实物不相符合的;
⑨未按随附的说明、操作手册使用产品，或者产品未用于预定功能或环境，海康威视经证实后确定您违反操作手册的任何其他情况。
3. 海康威视不对销售商或任何第三方对您的额外承诺负责，您应向这些第三方要求兑现。
用户名称：_____
详细地址：_____
电话：_____
产品型号（Model）：_____
产品编号（S/N）：_____
购买日期：___ 年__ 月__ 日
销售商：_____
电话：_____

注意:
1. 凭此卡享受保修期内的免费保修及保修期外的优惠性服务。
2. 本保修卡仅适用于本保修卡内产品，由销售单位盖章后方有效。
3. 特殊项目的产品保修条款以具体购销合同为准。

杭州海康威视数字技术股份有限公司
HANGZHOU HIKVISION DIGITAL TECHNOLOGY CO., LTD.
www.hikvision.com
服务热线：400-800-5998