用户手册

思科 **Wireless-N 3G** 无线 **VPN** 路由器

CVR328W

OL-32780-01

目 录

1

简介

本章介绍思科 3G 无线 VPN 路由器的基本特性，安装方法以及如何登录基于 web 的设备管理器设置相关参数。包括以下内容：

- 产品概述
- 设备特性
- 安装
- 连接
- 使用设备管理器
- 常用的配置任务

产品概述

思科 3G 无线 VPN 路由器专为中小型企业互联网接入设计，高度集成了路由、交换、安全防护、无线、 3G、 VPN 组网、 QoS 和流量控制等功能。它配置简单，操作方便，使用灵活且安全可靠，完全可以满足中小型企业用户对互联网接入和 VPN 组网需求。

本路由器具有以下优势：

- **可靠的互联网接入 —** 提供双千兆以太网口，可以同时接入互联网，即可为企业增加带宽，又可相互备份。路由器还可以通过 3G USB 上网卡拨号接入 3G 无线网络，作为应急备份。在有线网络中断服务的情况下， 3G USB 上网卡自动拨号接入互联网，在最短时间内恢复网络连接和 VPN 隧道的建立，最大程度减少有线网络中断对企业业务的影响。而当有线网络恢复服务时， 3G USB 上网卡则可自动断开 3G 网络连接，减少企业 3G 上网费用。
- **快速灵活的业务扩展 —** 随着企业业务的不断扩展，企业内部引入的网络设备种类会愈来愈多，包括千兆的网络设备、 802.11N 无线移动终端和其他 USB 设备。路由器的端口类型丰富，硬件集成度高，能够随着企业 IT 网络的扩展而灵活调整。路由器支持 802.11N 的无线接入，传输速率更快，覆盖范围更广。其第二个千兆以太网口可下联千兆口交换机，扩展接入更多的网络设备，并全面

提升网络性能。路由器具有两个 USB 2.0 接口，第一个 USB 接口用作接驳 3G USB 上网卡，支持 CDMA ECDO 和 WCDMA 无线网络接入，第二个 USB 接口用于未来其他 USB 设备的扩展接入，目前可支持存储系统日志到 USB 存储设备。

- **安全的虚拟专网连接 —** 企业员工出差时需要随时随地通过互联网访问公司内部网络。路由器的 VPN 远程拨号功能，可以通过 VPN 隧道加密技术，实现员工对企业内部网络的安全接入。企业分支机构和商业连锁网点，也需要通过互联网，利用 VPN 隧道加密技术，建立与公司总部网络的 VPN 虚拟专网。路由器支持多种 VPN 组网方案，可通过公网动态 IP 和 NAT 内网 IP 与企业总部 VPN 设备进行 VPN 组网。路由器还支持 VPN 隧道冗余保护机制，可充分保障企业分支机构到总部的 VPN 隧道的高可用性，最大程度地减少 VPN 隧道意外中断对企业业务的影响。

- **高效的远程集中网管 —** 对于企业分支机构或商业网点的大规模 VPN 组网，由于网点数量较多，地域分散较广，而且网点人员缺乏相应的网络设备操作技能，路由器的远程网管功能显得尤为重要。路由器可支持远程集中式网络管理，允许企业 IT 管理员通过部署在企业总部的专用网管平台，远程对全国各地分支机构的设备进行自动批量部署，上传或下载配置文件和升级固件版本，并可实时监控路由器的上线情况及 VPN 隧道的连接状态。

- **值得信赖的安全防护 —** 互联网的接入安全对于企业运营非常重要。路由器具有多重安全防护功能，可以充分保障企业内网的网络安全。例如，通过状态数据包检测 (SPI) 防火墙和应用程序过滤功能，可将未经授权的数据包进行过滤和拦截；通过访问控制 （ACL）功能，可有效防止未经授权用户的非法接入；通过 WLAN 的 RADIUS 身份验证功能，可杜绝外部 WLAN 用户的恶意蹭网；通过 MAC 地址过滤功能，可阻止非法终端设备接入企业内网；通过防 DoS 攻击功能，可避免服务资源的过度占用和网络拥塞；通过防 ARP 攻击功能，可防止企业网络被恶意欺骗和仿冒攻击。

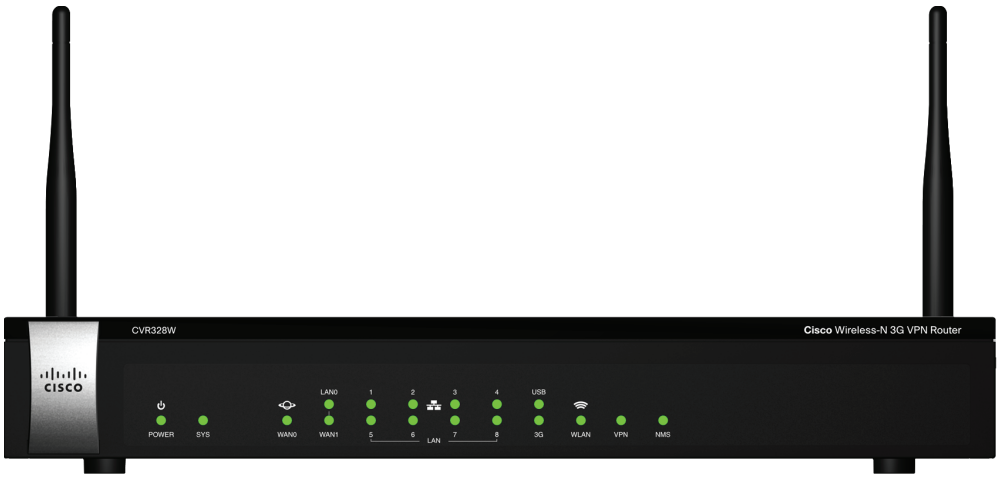
- **规范上网行为 —** 不规范的上网行为，不仅降低了企业的生产效率，而且会给企业网络带来安全隐患；而使用 P2P 下载或流媒体视频业务，也会严重消耗企业网络的带宽资源。因此，路由器支持黑白名单功能，可以限制对某些外部网址的访问；通过文件下载过滤功能，可以阻拦对某些特殊类型的文件下载；通过端口限速功能，可保障网络资源的合理分配，减少网络拥塞。

设备特性

在开始使用路由器之前，请预先了解路由器前面板所有指示灯和后面板所有接口的功能和状态说明。

前面板

路由器前面板提供各种指示灯，用于显示设备重要特性的工作状态。

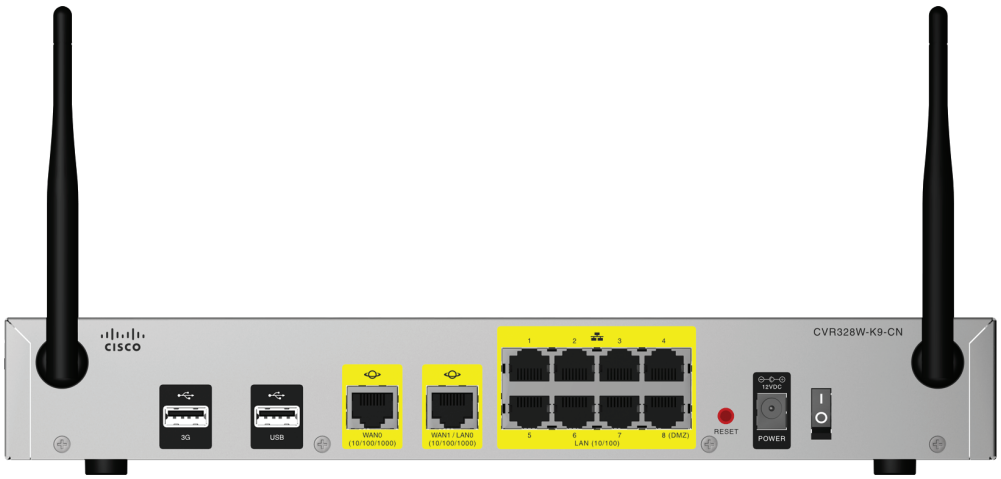


指示灯	说明
电源 **(POWER)**	▪ 绿灯常亮：表示电源接通且工作正常。 ▪ 关闭：表示电源关闭或出现电源故障。
系统 **(SYS)**	▪ 绿灯常亮：表示设备已经成功接入互联网并获得 IP 地址。 ▪ 绿灯闪烁：表示设备正在尝试接入互联网，或设备接入互联网不成功，或设备正处于固件升级状态中。 ▪ 红灯常亮：表示设备出现系统故障。 ▪ 红灯闪烁：表示系统过于繁忙，如 CPU 或内存利用率超过上限。 ▪ 关闭：表示没有配置网络连接。
WAN0	▪ 绿灯常亮：表示设备已经成功接入互联网但没有数据流。 ▪ 绿灯闪烁：表示设备已经成功接入互联网且有数据流。 ▪ 关闭：表示链路没有连通。

指示灯	说明
WAN1	如后面板 WAN1/LAN0 端口被设为一个 WAN 接口 （WAN1）： ▪ 绿灯常亮：表示设备已经成功接入互联网但没有数据流。 ▪ 绿灯闪烁：表示设备已经成功接入互联网且有数据流。 ▪ 关闭：表示链路没有连通。
LAN0	如后面板 WAN1/LAN0 端口被设为一个 LAN 接口 （LAN0）： ▪ 绿灯常亮：表示链路已经接通但没有数据流。 ▪ 绿灯闪烁：表示链路已经接通且有数据流。 ▪ 关闭：表示链路没有连通。
LAN1-8	▪ 绿灯常亮：表示链路已经接通但没有数据流。 ▪ 绿灯闪烁：表示链路已经接通且有数据流。 ▪ 关闭：表示链路没有连通。
USB	▪ 绿灯常亮：表示端口有 USB 设备插入但无读写操作。 ▪ 绿灯闪烁：表示端口有 USB 设备插入且有读写操作。 ▪ 关闭：表示端口没有 USB 设备插入。
3G	▪ 绿灯常亮：表示 3G 无线连接已建立但没有数据流。 ▪ 绿灯闪烁：表示 3G 无线连接已建立且有数据流。 ▪ 关闭：表示 3G 无线连接未建立。
无线 **(WLAN)**	▪ 绿灯常亮：表示无线网络已开启但没有数据流。 ▪ 绿灯闪烁：表示无线网络已开启且有数据流。 ▪ 关闭：表示无线网络关闭。
VPN	▪ 绿灯常亮：表示 VPN 连接已建立。 ▪ 绿灯闪烁 (每 2 秒闪烁一次)：表示设备正在试图建立一条 VPN 连接，或某一建立 VPN 连接的尝试失败。即便设备已建立多条 VPN 连接，当某一新建 VPN 连接尝试失败时，VPN 指示灯将显示绿色并定时闪烁。 ▪ 关闭：表示设备没有 VPN 连接。
网管 **(NMS)**	▪ 绿灯常亮：表示设备与上级网管系统已建立连接但没有操作。 ▪ 绿灯闪烁：表示设备与上级网管系统已建立连接且有操作。 ▪ 关闭：表示设备与上级网管系统未建立连接。

后面板

路由器后面板提供各种接口，用于连接设备电源和各种网络设备。



接口	说明
3G 接口	插入 3G USB 设备，用于接入 3G 无线网络。如需获取路由器兼容的移动宽带 USB 调制解调器的详细信息，请访问 www.cisco.com/go/cn/cvr328w 并参阅 《*思科 CVR328W Wireless-N 3G 无线 VPN 路由器兼容的移动宽带 USB 调制解调器*》一文的介绍。
USB 接口	插入 USB 存储设备，用于存储系统日志。
WAN0 接口	用于连接设备到互联网。
WAN1/LAN0 接口	▪ 如该端口被设为一个 WAN 接口 (WAN1)，用于连接设备到互联网。 ▪ 如该端口被设为一个 LAN 接口 (LAN0)，用于连接局域网设备到路由器。
LAN1-8 接口	用于连接局域网设备到路由器。
重置按钮 **(RESET)**	使用回形针或笔尖长按重置按钮可重启设备或恢复设备出厂设置： ▪ **重启设备 —** 长按该按钮至少 1 秒但不超过 5 秒。 ▪ **恢复设备出厂设置 —** 长按该按钮超过 5 秒。设备将自动重启并恢复到出厂设置。您之前所做的任何配置信息都将丢失。
电源接口 **(POWER)**	接通设备电源。电源接口必须连接到提供 12 V/3 A 交流电的电源适配器上。
电源开关	打开或关闭设备电源。

出厂默认配置

首次登录基于 web 的设备管理器时，可使用以下出厂默认配置：

参数	出厂默认配置
用户名	**cisco**
密码	**cisco**
路由器 IP 地址	**192.168.1.1**
DHCP 地址范围	192.168.1.100 - 192.168.1.200

注 如需恢复设备出厂默认设置，可使用回形针或笔尖长按后面板的重置按钮 **(RESET)** 超过 5 秒。设备将自动重启并恢复到出厂设置。您之前所做的任何配置信息都将丢失。

安装

您可以将路由器放置到桌面上或固定在墙壁上。

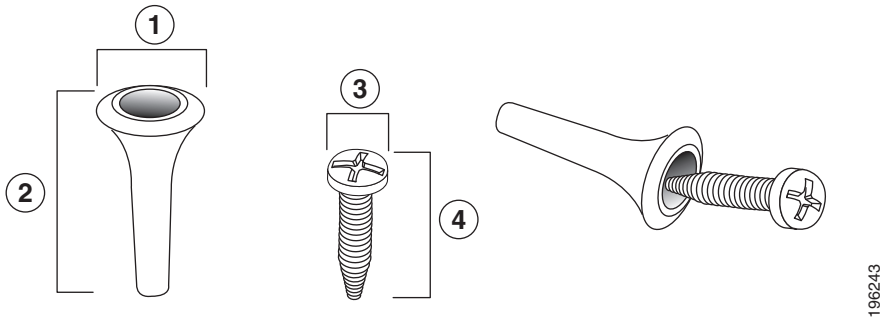
安放提示

- **环境温度 —** 为防止设备过热，请勿在环境温度 104 华氏度（40 摄氏度）的环境下运行设备。
- **通风 —** 请确保设备周围通风良好。
- **机械负载 —** 请确保设备放置平稳，以免出现任何对设备造成损坏的情况。

壁挂式安装

路由器未提供壁挂式安装套件。您需要自行准备安装套件将其固定在墙壁上。壁挂式安装路由器时，应使其端口朝上或朝下。请勿使路由器端口朝向侧面，因为这会导致挤压端口部件。

推荐的壁挂式安装套件规格如下：



1 8 毫米 /0.31 英寸 2 25 毫米 /0.98 英寸 3 6.5 毫米 /0.26 英寸 4 17.9 毫米 /0.7 英寸

警告 壁挂不当可能会损坏设备或造成人身伤害。对于因壁挂不牢固而造成的损坏，思科不承担任何责任。

步骤 1 确定路由器的安装位置。确保墙面光滑、平整、干燥且固定。

步骤 2 在墙面上钻两个间隔为 150 毫米 （5.9 英寸）的定位孔。

步骤 3 分别向每一个定位孔中插入一个墙锚和螺丝钉，将其固定到墙上。在墙面和螺丝钉头基部之间至少留出 3 毫米 （0.1 英寸）的距离。

步骤 4 将路由器底部的安装插槽套在螺钉上，然后向下滑动直至螺钉稳定地卡入安装插槽。

连接

路由器默认开启无线接入功能。您可以通过有线方式或无线网络连接至路由器。在您首次建立无线连接时，可使用路由器设备底部的标签上提供默认的无线网络名称 (SSID) 和密钥等信息。

步骤 1 关闭包括路由器、用来配置路由器的主机、调制解调器和其他网络设备在内所有设备的电源。

步骤 2 将以太网线的一端连接至调制解调器的以太网端口，另一端连接至路由器后面板的 WAN0 端口。

步骤 3 将以太网线的一端连接至主机或其他网络设备的以太网端口，另一端连接至路由器后面板的 LAN 端口。

注 如希望将主机通过无线方式连接至路由器，请跳过此步骤。

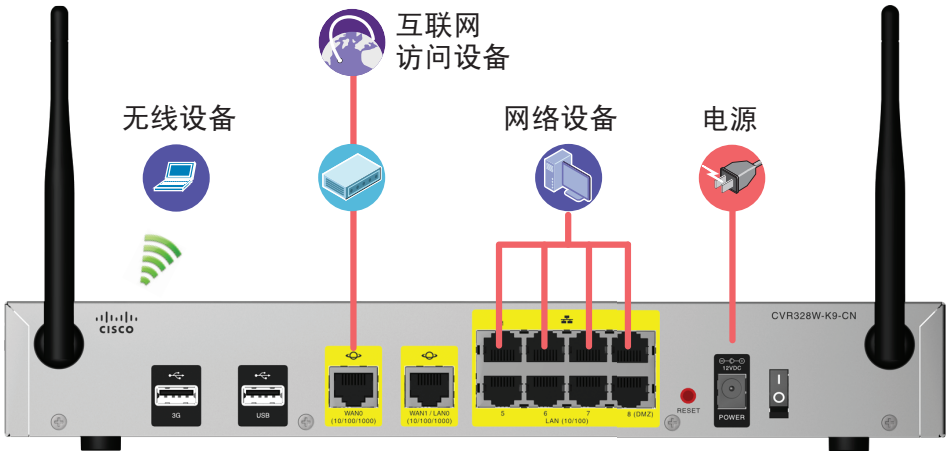
步骤 4 将电源适配器的一端插入到路由器的电源插孔中，另一端插入电源插座中。请确保路由器后面板的电源开关处于关闭状态。

步骤 5 开启所有连接设备的电源。

步骤 6 打开路由器后面板的电源开关，启动设备。

步骤 7 首次通过无线方式连接至路由器时，可使用设备底部标签上的密钥信息将您的主机连接至路由器默认的无线网络接入点。

至此，您已成功连接至路由器并可以开始访问互联网。



使用设备管理器

通过基于 web 的设备管理器，用户可查看路由器的基本信息和运行状态，设置系统参数，升级固件版本，重启设备或恢复出厂配置等。

配置前准备

请确保用来连接路由器的主机安装有 Microsoft Internet Explorer 6.0 （或更高版本）或 Mozilla Firefox 3.0 （或更高版本）。

注 为保证最佳显示效果，请确保您所使用的主机的屏幕分辨率设置不低于 1024 x 768。

访问基于 **Web** 的设备管理器

请按照以下步骤登录基于 web 的设备管理器并使用快速向导完成初始化设置：

步骤 **1** 将一台主机连接到路由器后面板的任意 LAN 接口。启动这台主机后，它将成为路由器的 DHCP 客户端，并自动获取一个在 192.168.1.xxx 范围内的 IP 地址。

步骤 **2** 打开浏览器，在地址栏中输入路由器的 IP 地址，并按回车键。

注 路由器默认的 IP 地址为 **192.168.1.1**。如果该地址被修改，请使用修改后的 IP 地址访问设备管理器。

步骤 **3** 在弹出的登录页面输入用户名和密码。路由器默认的用户名和密码均为 **cisco**。用户名和密码均区分大小写。

步骤 **4** 单击 “ **登录** ”。打开 “ 更改密码 ” 页面。

出于安全考虑，请立即修改默认的管理员密码以防止未经授权的访问。

步骤 **5** 输入旧管理员密码。

步骤 **6** 输入新管理员密码。默认情况下，新密码应包含至少三种字符类型 （字符类型包括大写字母、小写字母、数字和特殊字符），且密码长度不少于 8 个字符。

注 勾选 “ 禁用密码强度检测 ” 选项，新密码无需满足最小的密码强度规则。不建议勾选此选项。

步骤 **7** 单击 “ 确定 ”。密码修改成功并返回到登录界面。

步骤 **8** 如需对路由器进行初始化设置，请使用新密码重新登录，然后单击 “ **快速向导** ” 菜单，并按照页面提示完成相应的配置。详细信息请参考 “ 快速向导配置 ”。

使用帮助文件

路由器提供了详细的帮助文档以帮助用户了解路由器的具体功能和详细的配置信息。如需使用帮助文档，请单击设备管理器右上方的“**帮助**”。在打开的帮助文档窗口中，您将看到与您正在浏览的页面所相关的信息，帮助您快速获取所需要的信息。

常用的配置任务

在开始使用路由器之前，我们建议您完成以下配置任务：

修改管理员密码

为防止未经授权的访问，建议您首次登录之后立即修改管理员账号的默认密码。您也可打开“用户管理”页面修改管理员账号的密码。

修改管理员账号密码的步骤：

步骤 **1** 选择“系统管理”>“用户管理”。打开“用户管理”页面。

步骤 **2** 在“用户列表”栏，勾选要修改密码的系统管理员。

步骤 **3** 单击“修改密码”。打开“修改密码”对话框。

步骤 **4** 输入以下信息：

- 原始密码 — 输入当前管理员密码。
- 新密码 — 输入一个新密码。如果您启用了密码复杂度设置，新密码应满足密码复杂度的要求。默认情况下，密码包含至少三种字符类型（字符类型包括大写字母、小写字母、数字和特殊字符），且密码长度不少于 8 个字符。
- 确认密码 — 再次输入新设的密码。

步骤 **5** 单击“确定”。

升级固件版本

首次成功登录路由器之后，请检查系统使用的固件版本。建议在执行配置任务之前，手动将其升级到最新的固件版本。

注 意 在固件升级过程中，请不要断开设备电源，拔出连接的以太网电缆，或以其它任何方式打断或干扰固件升级过程。否则将造成固件升级失败，并无法正常启动路由器。固件升级过程可能需要几分钟的时间。

升级系统固件版本的步骤：

步骤 1 选择“系统管理”>“软件升级”。打开“软件升级”页面。

步骤 2 在“下载最新固件”部分，单击“下载”可从指定的网站上下载最新版本的固件。

步骤 3 在“请选择升级文件”部分，单击“浏览”，选择已下载的固件文件。

步骤 4 单击“升级”，开始升级设备的固件版本。

升级系统固件时，新的固件版本将替换系统默认的备份固件版本并自动重启。固件升级成功后，新的固件版本将作为主用固件版本为系统所使用，而之前使用的主用固件版本此时将成为备份固件版本。

备份配置文件

建议您经常备份路由器的配置文件，用于今后恢复系统配置。

备份系统配置文件的步骤：

步骤 1 选择“系统管理”>“配置维护”。打开“配置维护”页面。

步骤 2 单击“导出配置文件”。

步骤 3 选择配置文件的保存路径，单击“确定”。

2

快速向导配置

“ 快速向导 ” 帮助您快速设置上网所需的基本网络参数。即使您对网络知识和本产品不太熟悉，您也可以按照提示轻松地完成设置。

本章包括以下内容：

启动快速向导

步骤 1 单击左侧的 “ 快速向导 ” 菜单，打开快速向导。

步骤 2 如果您是一位专家，您也可以退出这个向导程序，直接选择相应的菜单项进行设置。如需继续，请单击 “ 下一步 ”，进入 “ 宽带连接配置 ” 页面。如需退出快速向导，请单击 “ 退出 ”。

宽带连接配置

“ 宽带连接配置 ” 页面允许您使用您的网络服务提供商所提供的相关信息设置 WAN 连接参数。

路由器支持以下几种常用的上网方式，请您根据自身情况进行选择。

- PPPoE

- DHCP
- Static IP
- L2TP

设置 WAN 连接参数的步骤：

步骤 1 从“**WAN** 端口”下拉框中选择连接到互联网的 WAN 接口，如 WAN0 和 WAN1（当后面板的 WAN1/LAN0 接口被设定为 WAN1 接口时才会显示）。

步骤 2 从“连接模式”下拉框中选择接入互联网的方法并配置相应的参数。下表给出了不同连接方式的配置说明：

连接方式	参数配置
DHCP	如果您的网络服务提供商使用动态主机配置协议（Dynamic Host Control Protocol）分配用户的 IP 地址（即用户每一次登录都会得到一个新分配的 IP 地址），选择此选项并输入以下信息： ▪ 启用**DNS**服务器— 选择启用或禁用DNS服务器功能。DNS 服务器可将主机名解析到 IP 地址映射。 ▪ 首选**DNS**服务器— 如启用DNS服务器功能，输入主用 DNS 服务器的 IP 地址。 ▪ 备用**DNS**服务器— 如启用DNS服务器功能，输入备用 DNS 服务器的 IP 地址。当首选 DNS 服务器无法连接时，连接到此备用 DNS 服务器。

连接方式	参数配置
Static IP	如果您的网络服务提供商分配给用户的是静态 IP 地址，请选择此选项。 您需要设定以下参数： ▪ **IP** 地址 — 网络服务提供商提供的静态 IP 地址。 ▪ 子网掩码 — WAN 接口的子网掩码。 ▪ 缺省网关 — WAN 接口的默认网关地址。 ▪ 首选 **DNS** 服务器 — 您的网络服务提供商将至少提供一个 DNS 服务器以便将主机名解析到 IP 地址映射。输入主用 DNS 服务器的 IP 地址。 ▪ 备用 **DNS** 服务器 — 输入备用 DNS 服务器的 IP 地址。当首选 DNS 服务器无法连接时，连接到此备用 DNS 服务器。

连接方式	参数配置
PPPoE	如果您的网络服务提供商提供上网账号及口令进行拨号上网，请选择此选项并设定以下参数： ▪ 上网账号 — 输入网络服务提供商提供的上网账号。 ▪ 上网口令 — 输入网络服务提供商提供的上网密码。 ▪ 服务名称 — 输入服务名称。 ▪ 启用**DNS**服务器— 选择启用或禁用DNS服务器功能。DNS 服务器可将主机名解析到 IP 地址映射。 ▪ 备用**DNS**服务器— 如启用DNS服务器功能，输入主用 DNS 服务器的 IP 地址。 ▪ 备用**DNS**服务器— 如启用DNS服务器功能，输入备用 DNS 服务器的 IP 地址。当首选 DNS 服务器无法连接时，连接到此备用 DNS 服务器。 ▪ 在线方式 — 选择以下任意一种在线方式： - 按需连接 — 如果您的网络服务提供商按连接时长收费，建议您选择此选项。当路由器空闲一定时间后自动终止 PPPoE 会话。您需要设置最大空闲时间，默认为 300 秒。 - 一直在线 — 如果您希望始终保持网络连接，请选择此项。当互联网连接中断时，路由器将自动重新建立链接。您可以设定当互联网连接中断多少秒后，自动重新建立链接，默认为 30 秒。

连接方式	参数配置
L2TP	如果您的网络服务商使用 L2TP 协议提供接入互联网的服务，请选择此选项。 您需要设定以下参数： ▪ 自动获取 **IP**— 启用或禁用自动从网络服务提供商获取 IP 地址。 ▪ **L2TP** 服务器地址 — 输入网络服务提供商提供的 L2TP 服务器 IP 地址。 ▪ 用户名 — 输入连接 L2TP 服务器的用户名。 ▪ 密码 — 输入连接 L2TP 服务器的密码。 ▪ 启用 **DNS** 服务器— 选择启用或禁用 DNS 服务器功能。DNS 服务器可将主机名解析到 IP 地址映射。 ▪ 首选 **DNS** 服务器— 如启用 DNS 服务器功能，输入主用 DNS 服务器的 IP 地址。 ▪ 备用 **DNS** 服务器— 如启用 DNS 服务器功能，输入备用 DNS 服务器的 IP 地址。当首选 DNS 服务器无法连接时，连接到此备用 DNS 服务器。 ▪ 在线方式 — 选择以下任意一种在线方式： - 按需连接 — 如果您的网络服务提供商按连接时长收费，建议您选择此选项。当路由器空闲一定时间后自动终止连接。您需要设置最大空闲时间，默认为 300 秒。 - 一直在线 — 如果您希望始终保持网络连接，请选择此项。当互联网连接中断时，路由器将自动重新建立链接。您可以设定当互联网连接中断多少秒后，自动重新建立链接，默认为 30 秒。

步骤 **3** 在 “ 启用 **VLAN**” 部分，当网络服务提供商使用 VLAN ID 来标识不同上网用户时，选择 “ 启用 ” 并输入 WAN 接口相应的 VLAN ID 以及 802.1p 优先级等信息。

- **VLAN ID**— 输入用来标识不同上网用户的 VLAN ID。
- **802.1p** 优先级 — 设定 802.1p 优先级。

步骤 4 在 “**MTU**” 部分，设定网络中可传输的最大数据包的长度。如果您所在的网路服务提供商没有特殊要求，建议您选择 “Auto”。如果 您所在的网络服务提供商自定义 MTU 设置，请选择 “Manual” 并手动输入相应的 MTU 值。

步骤 5 在 “**MAC Clone**” 部分，启用或禁用 MAC 地址克隆功能。 MAC 地址克隆可以在路由器上复制其它设备的 MAC 地址。

- **MAC Clone** 地址 — 如启用 MAC Clone 功能，输入需要克隆的网卡 MAC 地址。或单击 **Clone Your PC's MAC** 按钮，直接将当前计算机的网卡 MAC 地址克隆到路由器的 WAN 端口。

步骤 6 如需继续，请单击 “ 下一步 ”，进入 “ 局域网配置 ” 页面。如需返回先前配置页面，请单击 “ 上一步 ”。如需退出快速向导，请单击 “ 退出 ”。

局域网配置

“ 局域网配置 ” 页面可设置路由器默认的局域网参数。

步骤 1 设定以下参数：

- **VLAN**— 从下拉框中选择一个 VLAN 接口。关于 VLAN 接口设置的详细信息，请参考 “ 设置 **LAN** 接口参数 ” 一节的说明。
- **IP** 地址 — 设置路由器默认的 IP 地址。
- 子网掩码 — 设置路由器默认的子网掩码。
- **DHCP** 服务器 — 启用或禁用 DHCP 服务器功能。启用此功能，对接入子网的用户自动配置 IP 地址。禁用此功能，不对接入子网的用户自动配置 IP 地址。
- 起始 **IP** 地址 — 如启用 DHCP 服务器功能，输入 DHCP 地址池的起始地址。
- 结束 **IP** 地址 — 如启用 DHCP 服务器功能，输入 DHCP 地址池的结束地址。
- 租用时间 — 输入 DHCP 服务器配置给接入子网用户 IP 地址的租约时间，为子网用户可使用 DHCP 服务器配置的 IP 地址的时间。当租约时间到达上限时，子网用户须重新请求 DHCP 服务器分配 IP 地址。如果不做任何修改，系统默认为 1 天。

步骤 2 如需继续，请单击 “ 下一步 ”，进入 “ 无线路由配置 ” 页面。如需返回先前配置页面，请单击 “ 上一步 ”。如需退出设置向导，请单击 “ 退出 ”。

无线路由配置

“ 无线路由配置 ” 页面可设置路由器的无线网络的基本参数和安全认证选项。

步骤 1 设定以下参数：

- 当前 **SSID—** 选择一个无线接入点进行配置。
- **SSID** 名称 **—** 输入所选无线接入点的名称。
- 启用当前 **SSID—** 启用或禁用此无线接入点。
- 安全模式 **—** 选择无线网络的安全认证模式。下表给出了各无线安全认证模式的详细配置说明：

认证模式	参数配置
已禁用	表示此 SSID 不使用任何无线网络安全认证，无线网络用户可以直接接入此 SSID。
WEP	使用 Wired Equivalent Privacy （WEP）进行无线网络安全认证。无线网络用户需使用相同无线安全设置才能接入此 SSID。 ▪ 认证类型 **—** 选择“开放系统”或“共享密钥”进行认证。默认为 “ 开放系统 ”。 ▪ 密钥长度 **—** 设定密钥长度。可选密钥长度选项包括 64 位（5 ASCII 字符 或 10 Hex 字符）和 128 位 （13 ASCII 字符 或 26 Hex 字符）。密钥长度越长则安全等级越高。 ▪ 短语 **—** 输入短语后按下“生成密钥”按钮，系统将自动生成“密钥 1”、“ 密钥 2”、“ 密钥 3” 和 “ 密钥 4”。用户可视需求选择使用哪一个密钥。短语最大可支持 16 位字符。 ▪ 当前密钥 **—** 选择进行无线网络安全认证的密钥。 ▪ 密钥 **1**、**2**、**3**、**4—** 可分别手动设置 “ 密钥 1”、“ 密钥 2”、“ 密钥 3” 和 “ 密钥 4” 。选择密钥长度 64 位时，需填入 5 位 ASCII 字符 或 10 位 Hex 字符。选择密钥长度 128 位时，需填入 13 位 ASCII 字符 或 26 位 Hex 字符。合法的 Hex 字符包括 0-9 以及 A-F。

认证模式	参数配置
WPA-Personal	使用 WiFi Protected Access （WPA）进行无线网络安全认证。安全等级较 WEP 标准高。无线网络用户需使用相同无线安全设置才能接入此 SSID。 ▪ **WPA** 预共享密钥 — 输入安全密钥。密钥长度范围为 8-63 字符。 ▪ 显示密钥 — 以明文的形式显示输入的安全密钥。 ▪ **WPA**群组更新密钥间隔时间— 输入群组密钥的更新时间。单位为秒。默认值为 3600 秒。 ▪ **WPA**加密— 选择AES或TKIP+AES作为加密算法。默认为TKIP+AES。
WPA2-Personal	使用 WiFi Protected Access 2 （WPA2）进行无线网络安全认证。安全等级较 WEP 标准高。无线网络用户需使用相同的无线安全设置才能接入此 SSID。 ▪ **WPA** 预共享密钥 — 输入安全密钥。密钥长度范围为 8-63 字符。 ▪ 显示密钥 — 以明文的形式显示输入的安全密钥。 ▪ **WPA**群组更新密钥间隔时间— 输入群组密钥的更新时间。单位为秒。默认值为 3600 秒。 ▪ **WPA**加密— 选择AES或TKIP+AES作为加密算法。默认为AES。

认证模式	参数配置
WPA-Enterprise	使用 WiFi Protected Access （WPA）进行无线网络安全认证，并配合 RADIUS 服务器认证无线网络用户。选择此功能需要配置并连接一台 RADIUS 服务器至路由器。无线网络用户需使用相同的无线安全设置才能接入此 SSID。 ▪ **WPA**群组更新密钥间隔时间— 输入群组密钥的更新时间。单位为秒。默认值为 3600 秒。 ▪ **WPA**加密— 选择AES或TKIP+AES作为加密算法。默认为TKIP+AES。 ▪ **RADIUS** 服务器地址 — 输入 RADIUS 服务器的 IP 地址。 ▪ **RADIUS** 服务器端口 — 输入 RADIUS 服务器使用的端口号。默认为 1812。 ▪ **RADIUS** 服务器密钥— 输入RADIUS服务器与路由器所使用的共享密钥。 ▪ 显示密钥 — 以明文的形式显示输入的共享密钥。
WPA2-Enterprise	使用 WiFi Protected Access 2 （WPA2）无线网络安全认证，并配合 RADIUS 服务器进行无线网络用户认证。选择此功能需要配置并连接一台 RADIUS 服务器至路由器。无线网络用户需使用相同的无线安全设置才能接入此 SSID。 ▪ **WPA**群组更新密钥间隔时间— 输入群组密钥的更新时间。单位为秒，默认为 3600 秒。 ▪ **WPA**加密— 选择AES或TKIP+AES作为加密算法。默认为AES。 ▪ **RADIUS** 服务器地址 — 输入 RADIUS 服务器的 IP 地址。 ▪ **RADIUS** 服务器端口 — 输入 RADIUS 服务器使用的端口号。默认为 1812。 ▪ **RADIUS** 服务器密钥— 输入RADIUS服务器与路由器所使用的共享密钥。 ▪ 显示密钥 — 以明文的形式显示输入的共享密钥。

步骤 **2** 如需继续，请单击“下一步”，进入“完成快速配置向导”页面。如需返回先前配置页面，请单击“上一步”。如需退出快速向导，请单击“退出”。

完成快速向导配置

“ 完成快速安装向导 ” 页面显示您之前所设定的 WAN 连接参数、局域网参数和无线网络参数设置。

如无问题请单击 “ 完成 ” 保存快速向导设置。如需返回先前配置页面，请单击 “ 上一步 ”。如需退出快速向导，请单击 “ 退出 ”。

3

查看设备状态

本章介绍如何查看路由器的系统信息和实时工作状态，包括以下内容：

- 设备信息
- **WAN** 连接信息
- **3G** 无线连接信息
- **LAN** 接口信息
- 无线网络信息
- **MAC** 地址
- **DHCP** 客户端信息
- 业务信息
- 网络进程信息
- 刷新周期

选择 “ 设备概览 ” 菜单，打开 “ 设备概览 ” 页面。

设备信息

“ 设备信息 ” 栏显示以下信息：

- 产品名称 — 显示产品名称。
- 设备型号 — 显示设备型号。
- **VID**— 显示设备版本 ID
- 设备标识号 — 显示设备序列号。
- 硬件版本 — 显示系统当前使用的硬件版本。
- 当前固件版本 — 显示系统当前使用的固件版本。

- 备份固件版本 — 显示系统的备份固件版本。
- 设备运行时间 — 显示系统已经运行了多长时间。
- **CPU** 利用率 — 显示系统当前的 CPU 使用率。
- 内存利用率 — 显示系统当前的内存使用率。

WAN 连接信息

“WAN 连接信息 ” 栏显示以下信息：

- **WAN** 端口 — 显示物理 WAN 接口名称。
- 端口状态 — 显示物理 WAN 接口当前是否连接到互联网。
- **WAN** 连接名称 — 显示所有 WAN 连接名称，包括通过物理 WAN 接口及其 WAN 子接口创建的 WAN 连接。
- **IP** 地址 — 显示相应的物理 WAN 接口或 WAN 子接口所获得的 IP 地址。

3G 无线连接信息

“3G 无线连接信息 ” 栏显示以下信息：

- **3G** 无线网络信息 — 显示路由器是否连接到 3G 无线网络。
- **3G Modem** 状态 — 显示路由器是否检测到 3G USB 调制解调器。3G USB 调制解调器应插入到路由器后面板的 3G USB 接口。
- **UIM** 卡状态 — 显示路由器是否检测到 3G 无线上网卡。3G 无线上网卡应插入到 3G USB 调制解调器。
- 信号强度 — 显示 3G 无线网络的信号强度。

如需查看 3G 无线上网卡的详细信息：

步骤 1 单击 “ 详细信息 ”，显示以下信息：

- **3G Modem** 信息 — 显示 3G USB 调制解调器的连接状态、设备型号、生产厂商、入网许可证编号、设备序列号、硬件版本、固件版本以及 PRL 版本等信息。

- **UIM** 卡信息 — 显示 UIM 卡的连接状态、 IMSI 编码以及供电电压等信息。
- **3G** 网络信息 — 显示 3G 无线网络运营商的名称、当前的工作状态、总流量、数据传输速率、总连接时间以及信号强度等信息。

步骤 2 单击 “ 返回 ”，返回到 “ 设备概览 ” 页面。

LAN 接口信息

“LAN 接口信息 ” 栏显示所有 LAN 接口的连接状态，包括：

- **LANx**— 显示 LAN 接口的名称。
- 状态 — 显示 LAN 接口的连接状态。

无线网络信息

“ 无线网络信息 ” 栏显示路由器上所有 4 个无线网络接入点的状态信息，包括：

- **SSID** （无线网络名称） — 显示无线网络接入点的名称。
- 服务状态 — 显示此无线网络接入点是否启用。
- 连接的设备数 — 显示连接到此无线网络接入点的无线客户端的数量。

MAC 地址

“**MAC**” 栏显示路由器上所有接口的 MAC 地址信息，包括：

- **Interface** （接口） — 显示所有的 WAN 接口， LAN 接口以及无线网络接口。
- **MAC** 地址 — 显示对应接口的 MAC 地址信息。

DHCP 客户端信息

“DHCP 客户端 ” 栏显示路由器上设定的所有 DHCP 服务器。

如需查看相应的 DHCP 客户端的详细信息：

步骤 1 点击 “ 详细信息 ” 并选择要查看的 DHCP 服务器，显示以下信息：

- 主机名称 — 显示连接主机的名称。
- **IP** 地址 — 显示连接主机的 IP 地址。
- **MAC** 地址 — 显示连接主机的 MAC 地址。
- 租用时间 — 显示连接主机的 IP 地址的租用到期时间。
- 接口 — 显示主机连接到路由器的方式和对应接口。

步骤 2 单击 “ 返回 ”，返回到 “ 设备概览 ” 页面。

业务信息

“ 业务信息 ” 栏显示路由器上运行的重要应用或服务的工作状态，包括：

- 服务名称 — 显示服务名称，如 IPsec VPN。
- 当前状态 — 显示 IPsec VPN 服务当前是否启用。

网络进程信息

“ 网络进程 ” 栏显示路由器的网络进程信息，点击 “ 详细信息 ” 可查看路由器当前所有活跃的互联网连接的详细信息，包括：

- 协议 — 显示当前连接或服务所使用的服务类型，如 TCP、 UDP 或 raw。
- 接收队列 — 显示当前连接或服务所接收的字节数。
- 发送队列 — 显示当前连接或服务所发送的字节数。
- 本地地址 — 显示当前连接或服务所使用的本地 IP 地址。

- 外部地址 — 显示当前连接或服务的远程受用 IP 地址。
- 状态 — 显示协议类型为 TCP 的连接或服务的状态。如当前连接或服务所使用的协议类型为 UDP 或 raw，此栏为空。

刷新周期

“ 刷新周期 ” 栏可设定页面自动刷新的频率。可选择的刷新周期包括：10 秒、 30 秒、 1 分钟、 5 分钟、 10 分钟。

如需手动刷新页面数据，选择 “ 手动刷新 ” 并单击 “ 刷新 ”。

4

端口配置

本章介绍如何配置路由器的 WAN 连接、局域网、无线网络以及 3G 接口等功能，包括以下内容：

- **WAN** 配置
- 设置 **LAN**
- **WLAN** 配置
- **3G** 接口配置

WAN 配置

默认情况下，路由器被设置为从网络服务提供商处自动获取 IP 地址。根据您的网络服务提供商的具体要求，您也可以修改路由器的 WAN 接口设置以确保正常的网络连接。

-
-

查看 WAN 接口信息

如需查看 WAN 接口信息，选择 “ 端口配置 ”>“**WAN**”>“**WAN** 接口配置 ” 菜单。打开 “WAN 接口配置 ” 页面。

“**Internet** 接口参数 ” 栏显示路由器当前所有的 WAN 连接的详细信息，包括：

选项	描述
接口	显示物理 WAN 接口的编号。

选项	描述
连接名称	显示 WAN 连接名称，包括通过物理 WAN 接口和相应的 WAN 子接口创建的 WAN 连接。 路由器支持 WAN 子接口功能。一个物理 WAN 接口可以分成多个逻辑接口，每一个逻辑接口叫子接口。用户可在 WAN0 和 WAN1 两个物理接口上添加不超过 8 个 WAN 子接口。
连接模式	显示连接到互联网的方式。详细信息请参考 “ 宽带连接配置 ”。
IP 地址	显示 WAN 接口的 IP 地址。
DNS	显示 WAN 接口的 DNS 服务器 IP 地址。
状态	显示 WAN 接口的连接状态。

设置 **WAN** 接口

路由器后面板的 WAN1/LAN0 接口默认被设为一个物理 WAN 接口，使得路由器可同时建立两条 WAN 连接以确保网络连接的安全或合理分配网络带宽到不同 WAN 接口。

用户可以在物理 WAN 接口上添加多个子接口。每一个 WAN 子接口均可创建一条 Internet 连接。当物理 WAN 接口创建了多条 WAN 连接时，必须指定物理 WAN 接口的默认路由接口。最多可以在两个物理 WAN 接口上创建不超过 8 个 WAN 子接口。

设置 WAN 接口配置的步骤：

步骤 **1** 选择 “ 端口配置 ”>“**WAN**”>“**WAN** 接口配置 ” 菜单。打开 “WAN 接口配置 ” 页面。

步骤 **2** 如需添加一条 WAN 子接口，单击 “ 添加子接口 ”。打开 “ 新建 WAN 连接 ” 页面。

步骤 **3** 在 “ 连接模式 ” 栏，选择路由模式或桥接模式。通过物理 WAN 接口的 Internet 连接模式始终为路由模式。

步骤 **4** 如您选择路由模式，请选择合适的 Internet 连接类型并设定相关参数。如您不知道选择哪种 Internet 连接类型，请联系您的网络服务提供商获取上网所需的相关信息。

- **DHCP—** 如果您的网络服务提供商使用动态主机配置协议 （Dynamic Host Control Protocol）分配用户的 IP 地址 （即用户每一次登录都会得到一个新分配的 IP 地址），选择此选项。
  - 启用 DNS 服务器 — 选择启用或禁用 DNS 服务器功能。DNS 服务器可将主机名解析到 IP 地址映射。

- 首选 DNS 服务器 — 如启用 DNS 服务器，输入主 DNS 服务器的 IP 地址。
- 备用DNS服务器 — 如启用DNS服务器，输入用来备份的DNS服务器的IP地址。当首选 DNS 服务器无法连接时，连接到此备用 DNS 服务器。

- **Static—** 如果您的网络服务提供商分配给用户的是静态 IP 地址，请选择此选项并设定以下参数：
  - IP 地址 — 输入网络服务提供商提供的静态 IP 地址。
  - 子网掩码 — 输入 WAN 接口的子网掩码。
  - 缺省网关 — 输入 WAN 接口的默认网关地址。
  - 首选DNS服务器 — 您的网络服务提供商将至少提供一个DNS服务器的IP地址以便将主机名解析到 IP 地址映射。输入主 DNS 服务器的 IP 地址。
  - 备用DNS服务器 — 输入用来备份的DNS服务器的IP地址。当首选DNS服务器无法连接时，连接到此备用 DNS 服务器。
- **PPPoE—** 如果您的网络服务提供商提供上网帐号及口令，请选择此选项并设定以下参数：
  - 用户名 — 输入网络服务提供商提供的上网账号。
  - 密码 — 输入网络服务提供商提供的上网密码。
  - 服务名称 — 输入服务名称。
  - 启用DNS服务器 — 选择是否启用或禁用DNS服务器功能。DNS服务器功能可将主机名解析到 IP 地址映射。
  - 首选DNS服务器 — 如您启用DNS服务器功能，输入主用DNS服务器的IP地址。
  - 备用DNS服务器 — 输入用来备份的DNS服务器的IP地址。当首选DNS服务器无法连接时，连接到此备用 DNS 服务器。
  - 在线方式 — 选择以下任意一种在线方式：

    按需连接 — 如果您所在的网络服务提供商按连接时长收费，建议您选择此选项。当路由器空闲一定时间后自动终止 PPPoE 会话。您需要设置最大空闲时间，默认为 300 秒。

    一直在线 — 如果您希望始终保持网络连接，请选择此项。如果 Internet 连接中断，将自动重新建立链接。您可以设定当 Internet 连接中断多少秒后，自动重新建立链接，默认为 30 秒。
- **L2TP—** 如果您的网络服务商使用 L2TP 协议提供接入互联网的服务，请选择此选项并设定以下参数：

- 自动获取 IP （DHCP） — 启用此功能自动从网络服务器提供商处获得 IP 地址，禁用此功能需手动输入 IP 地址、子网掩码和缺省网关等信息。
- L2TP 服务器地址 — 输入网络服务提供商提供的 L2TP 服务器 IP 地址。
- 用户名 — 输入连接 L2TP 服务器的用户名。
- 密码 — 输入连接 L2TP 服务器的密码。
- 启用 DNS 服务器 — 选择是否启用或禁用 DNS 服务器功能。DNS 服务器功能可将主机名解析到 IP 地址映射。
- 首选 DNS 服务器 — 如您启用 DNS 服务器功能，输入主用 DNS 服务器的 IP 地址。
- 备用 DNS 服务器 — 输入用来备份的 DNS 服务器的 IP 地址。当首选 DNS 服务器无法连接时，连接到此备用 DNS 服务器。
- 在线方式 — 选择以下任意一种在线方式：

  按需连接 — 如果您所在的网络服务提供商按连接时长收费，建议您选择此选项。当路由器空闲一定时间后终止连接。您需要设置最大空闲时间，默认为 300 秒。

  一直在线 — 如果您希望始终保持网络连接，请选择此项。如果 Internet 连接中断，将自动重新建立链接。您可以设定当 Internet 连接中断多少秒后，自动重新建立链接，默认为 30 秒。

- 启用 **NAT**— 启用或禁用 NAT 功能。如果此 WAN 连接是管理专用，则应禁用 NAT。
- 启用 **VLAN**— 当您的网络服务提供商使用 VLAN ID 标识不同上网用户时，启用此功能。如您启用此功能，需输入相应的 VLAN ID 以及 802.1p 优先级信息。
- **MTU**— 设定网络中可传输的最大数据包的长度。如果您所在的网络服务提供商没有特殊要求，建议您选择 “**Auto**”。如您所在的网络服务提供商自定义 MTU 设置，请选择 “**Manual**” 并手动输入相应的 MTU 值。
- 服务类别绑定 — 选择 WAN 连接的服务类别，其中：
  - Management— 表示此连接仅用作管理通道。
  - Internet— 表示此连接仅用作上网通道。
  - Management_Internet— 表示此连接仅用作管理和上网信道。
  - VoIP— 表示此连接仅用作 VoIP 通道。
  - IPTV— 表示此连接仅用作 IPTV 通道。

- 其他 — 表示此连接用作其他用途。

- **MAC Clone—** 启用或禁用 MAC 地址克隆功能。MAC 地址克隆可以在路由器上复制其它设备的 MAC 地址。
  - **MAC Clone** 地址 **:** 如启用 MAC Clone 功能，输入需要克隆的网卡 MAC 地址。或单击 **Clone Your PC's MAC** 按钮，直接将当前计算机的网卡 MAC 地址克隆到路由器的 WAN 端口。

步骤 **5** 如您选择桥接模式，设置以下参数：

- 启用 **NAT—** 选择启用或禁用 NAT 功能。如果此 WAN 连接是管理专用，则应禁用 NAT。
- 启用 **VLAN—** 当您的网络服务提供商使用 VLAN ID 标识不同上网用户时，启用此功能。如您启用此功能，输入相应的 VLAN ID 和 802.1p 优先级。
- **MTU—** 设定网络中可传输的最大数据包的长度。如果您所在的网络服务提供商没有特殊要求，建议您选择 “**Auto**”。如您所在的网络服务提供商自定义 MTU 设置，请选择 “**Manual**” 并手动输入相应的 MTU 值。
- 绑定端口 — 设定 WAN 接口桥接指向的端口。
- **MAC Clone—** 启用或禁用 MAC 地址克隆功能。MAC 地址克隆可以在路由器上复制其它设备的 MAC 地址。
  - **MAC Clone** 地址 **:** 如启用 MAC Clone 功能，输入需要克隆的网卡 MAC 地址。或单击 **Clone Your PC's MAC** 按钮，直接将当前计算机的网卡 MAC 地址克隆到路由器的 WAN 端口。
- 单击 “ 确定 ”，保存您的配置信息并返回到 “WAN 接口配置 ” 页面。

设置 **WAN** 接口的默认路由

如果物理 WAN 接口上配置了多条 WAN 连接 （添加了 1 个或多个 WAN 子接口），您必须指定此物理 WAN 接口的默认路由接口。

设置物理 WAN 接口的默认路由接口的步骤：

步骤 **1** 选择 “ 端口配置 ”>“**WAN**”>“**WAN** 接口配置 ” 菜单。打开 “WAN 接口配置 ” 页面。

步骤 **2** 在 “**WAN** 接口默认路由 ” 栏，分别设置 WAN0 和 WAN1 物理接口默认的路由接口。

步骤 **3** 单击 “ 确定 ”。

Multi-WAN 配置

路由器支持 Multi-WAN 功能，可通过 Internet 连接备份来确保恒定的 Internet 连接，或者在不同 WAN 连接之间建立负载均衡以使带宽效率最大化。

注 意　在配置多 WAN 功能之前，建议您首先在 “WAN1/LAN0 配置 ” 页面将 WAN1/LAN0 接口设置为 WAN1 接口。

设置 Multi-WAN 功能的步骤：

步骤 1　选择 “ 端口配置 ”>“**WAN**”>“**Multi-WAN** 配置 ” 菜单。打开 “Multi-WAN 配置 ” 页面。

步骤 2　在 “**Multi-WAN** 配置 ” 栏设定以下参数：

- **WAN Failover**— 选择启用或禁用 WAN Failover 功能。启用此功能，当主用 WAN 连接断开时，系统自动切换到备用 WAN 连接。当主 WAN 连接恢复后，从备用 WAN 连接自动切回到主用 WAN 连接。
- 连接查询间隔 — 输入检测 Internet 连接的超时时间间隔。默认为 60 秒。
- **Ping** 超时时间 — 输入等待响应 ping 请求的超时时间。默认为 5 秒。
- **Ping** 检测次数 — 输入重复发送 ping 请求的最大次数。当对端无响应时，重新发送 ping 请求指令。默认为 1。
- 连接查询成功几次后恢复连接— 设置多少次成功响应后恢复WAN连接。验证后恢复到高优先级的 WAN 连接。

步骤 3　在 “ 网络服务检测 ” 栏，分别指定用来检测主用 WAN 连接和备用 WAN 连接状态的 IP 地址。

- 网关 — 选择此选项，使用默认的网关地址检测网络服务连接状态。
- 自定义 — 选择此选项，手动输入一个 IP 地址检测网络服务连接状态。

步骤 4　在 “**WAN** 接口 ” 栏，您可以指定不同 WAN 接口的优先级。

- 接口 — 显示 WAN 接口的名称。
- 状态 — 显示 WAN 接口的连接状态。
- 优先级 — 设定 WAN 接口的优先级别。

步骤 5　在 “**WAN** 接口信息 ” 栏，可查看 WAN 接口的详细信息，包括：

- 接口 — 显示 WAN 接口的名称。

- **IP** 地址 — 显示 WAN 接口的 IP 地址。
- 网络掩码 — 显示 WAN 接口的子网掩码。
- 网关 — 显示 WAN 接口的网关地址。

步骤 6 在 “ 负载均衡 ” 栏，选择启用或禁用负载均衡功能。

步骤 7 如果启用负载均衡功能，需在 “ 负载均衡配置 ” 栏为每个 WAN 接口设置负载均衡权重值。有效值为 0-99。“0” 表示此接口不参加负载均衡。

步骤 8 在 “ 健康检查 ” 部分，选择启用或禁用健康检查功能。启用健康检查功能，可以帮助用户监测多个 WAN 接口的流量状态。

- 如启用健康检查功能，需输入健康检查时间间隔，以及在多少个健康检查失败后关闭相应接口，并在经过多少次成功的健康检查后重新启用该接口。

步骤 9 在 “ 健康检查设置 ” 部分，选择相应接口需要进行健康检查的站点。默认情况下健康检查站点为对应的默认网关，也可以自定义需要监测的主机 IP 地址。

步骤 10 单击 “ 确定 ”。

WAN1/LAN0 配置

用户可以将后面板的 WAN1/LAN0 接口设置为一个扩展的 LAN 接口 （LAN0）或者一个 WAN 接口 （WAN1）。

设置 WAN1 或 LAN0 接口的步骤：

步骤 1 选择 “ 端口配置 ”>“**WAN**”>“**WAN1/LAN0** 配置 ” 菜单。打开 “WAN1/LAN0 配置 ” 页面。

步骤 2 选择端口类型：

- **WAN1**— 选择此选项，该端口被设为一个 WAN 接口 （WAN1）。
- **LAN0**— 选择此选项，该端口被设为一个 LAN 接口 （LAN0）。

步骤 3 单击 “ 确认 ”。

注 意 修改 WAN1/LAN0 接口的类型将重启设备。如果将此接口从 WAN1 接口切换到 LAN0 接口，设备将复位到出厂默认设置，所有先前的设置将被删除并且重新启动。

USB 设备更新

路由器支持不同类型的 USB 设备。在 “ 动态载入 **USB** 调制解调器列表 ” 下，动态显示 USB 设备的变化。

新增 USB 设备的步骤：

步骤 1 选择 “ 端口配置 ”>“**WAN**”>“**USB** 设备更新 ” 菜单。打开 “**USB** 设备更新 ” 页面。

步骤 2 单击 “ 浏览 ”，在本地主机上选择需要新增的 USB 设备驱动文件。单击 “ 导入 ” 完成 USB 设备更新。

设置 LAN

VLAN （Virtual Local Area Network，虚拟局域网）是功能上相关联或者拥有诸多共性的一组网络终端的集合。与基于物理位置的局域网不同，VLAN 可以不考虑设备以及用户的物理位置而组成新的工作组。

设置 LAN 接口参数

“LAN 配置 ” 页面可设定 LAN 接口的相关参数。

设置 LAN 接口参数的步骤：

步骤 1 选择 “ 端口配置 ”>“**LAN**”>“**LAN** 配置 ” 菜单。打开 “LAN 配置 ” 页面。

步骤 2 在 “**LAN** 配置 ” 栏，设定以下参数：

- **VLAN**— 从下拉框中选择一个 VLAN 进行设定。默认为 VLAN1。您可以在 “VLAN 配置 ” 页面添加新的 VLAN 并将物理端口映射到 VLAN 上。
- **IP** 地址 — 输入 VLAN 接口的 IP 地址。
- 子网掩码 — 输入 VLAN 接口的子网掩码。
- **DHCP** 服务 — 启用或禁用 DHCP 服务器功能。启用此功能，对接入子网的用户自动配置 IP 地址。您需要手动设置自动分配地址池的范围。禁用此功能，不对接入子网的用户自动配置 IP 地址。
- 起始 **IP** 地址 — 输入 DHCP 地址池的起始 IP 地址。
- 结束 **IP** 地址 — 输入 DHCP 地址池的终止 IP 地址。

- 网关地址 — 输入默认的网关地址。
- **DNS** 代理 — 选择启用或禁用 DNS 代理服务器功能。
- **DNS** 服务器 **1**— 输入首选 DNS 服务器的 IP 地址。
- **DNS** 服务器 **2**— 输入备选 DNS 服务器的 IP 地址。
- 地址保留 — 选择启用或禁用地址保留功能。启用此功能时，手动添加需要预留的 DHCP 地址。
- 手动添加主机 — 如果您启用地址保留功能，设定以下参数：
  - 主机名称 — 输入主机名称用于识别该主机。
  - **IP** 地址 — 输入需要预留的 IP 地址。
  - 主机 **MAC** 地址 — 输入主机的物理 MAC 地址。

  输入完以上信息之后，单击 “ 添加 ” 将其保存到 “ 预留的地址 ” 列表。

步骤 **3** 单击 “ 确定 ”。

设置 VLAN

“VLAN 配置 ” 页面可自定义新的 VLAN，并设置物理 LAN 接口到 VLAN 的映射关系。

设置 VLAN 的步骤：

步骤 **1** 选择 “ 端口配置 ”>“**LAN**”>“**VLAN** 配置 ” 菜单。打开 “VLAN 配置 ” 页面。

步骤 **2** 如需添加一个新 VLAN，选择 “ 添加 ”。在 “**VLAN ID**” 栏输入新 VLAN 的 VLAN ID（VLAN1 和 VLAN2 为系统预留的 VLAN ID），并设置物理 LAN 接口到 VLAN 的映射关系。 LAN 接口映射到 VLAN 上可将相应物理 LAN 接口的所有数据流都关联到此 VLAN。

步骤 **3** 单击 “ 确定 ”。

步骤 **4** 如需删除一个 VLAN，选择 “ 删除 ” 并从 “ 选择 **VLAN**” 下拉框中选择要删除的 VLAN ID，然后单击 “ 确定 ”。 VLAN1 和 VLAN2 为系统预留的 VLAN，不能被删除。

WLAN 配置

路由器默认开启无线接入功能。您可以设定路由器无线网络的基本参数，也可以分别设置每个虚拟无线网络 （SSID）的无线安全配置等。

WLAN 基本参数设置

设置 WLAN 基本参数的步骤：

步骤 1 选择 “ 端口配置 ”>“**WLAN** 配置 ”。打开 “WLAN 配置 ” 页面。

步骤 2 在 “**WLAN** 基本参数设置 ” 栏，设定以下参数：

- **WLAN** 功能 — 启用或禁用 WLAN 功能。默认为启用。
- 工作模式 — 从下拉框中选择无线网络的工作模式：
  - **802.11b/g/n** 混合 — 如您的无线网络存在 802.11n、802.11b 与 802.11g 装置，选择此模式。此项是默认的无线网络工作模式 （建议启用此项）。
  - **802.11b/g** 混合 — 如您的无线网络仅存在 802.11b 与 802.11g 装置，选择此模式。
  - **802.11b**— 如您的无线网络仅存在 802.11b 装置，选择此模式。
  - **802.11g**— 如您的无线网络仅存在 802.11g 装置，选择此模式。
  - **802.11n**— 如您的无线网络仅存在 802.11n 装置，选择此模式。
- 信道带宽 — 从下拉框中选择无线网络的工作频段：
  - **20 MHz**— 使用 20 MHz 工作频段。
  - **20/40 MHz**— 自动选择 20 MHz 或 40 MHz 工作频段。
- 工作信道 — 从下拉框中选择无线网络的工作信道。默认为自动选择工作信道。当信道带宽被设为 20 MHz 时，可选择 1-13 中的任意信道。当信道带宽被设为 40 MHz 时，可选择 3-11 当中的任意信道 （默认为使用第 11 信道）。
- **Wi-Fi** 功率 — 选择高、中或低发射功率。默认为高发射功率。
- 无线用户隔离 — 勾选此选项，启用 SSID 下无线终端之间的二层隔离。取消此选项，禁用 SSID 下无线终端之间的二层隔离。
- 无线 **QoS**— 选择启用或禁用无线 WiFi MultiMedia （WMM）功能。

步骤 **3** 单击 “ 确认 ”。

SSID 参数设置

路由器支持 4 个虚拟无线网络 （即 4 个 SSID），默认开启一个 SSID。您可以修改每个 SSID 的基本参数和无线安全设置。

设置 SSID 参数的步骤：

步骤 **1** 选择 “ 端口配置 ”>“**WLAN** 配置 ”。打开 “WLAN 配置 ” 页面。

“**SSID** 配置 ” 栏显示每个 SSID 的基本信息，包括：

- **SSID—** 显示 SSID 的名称。
- 安全模式 — 显示 SSID 当前采用的数据加密方式。
- 状态 — 显示 SSID 当前是否启用。

步骤 **2** 如需启用一个 SSID，选择相应的 SSID 并单击 “ 启用 ”。

步骤 **3** 如需禁用一个 SSID，选择相应的 SSID 并单击 “ 禁用 ”。

步骤 **4** 如需编辑某一 SSID 的参数，单击 “ 编辑 ”。打开 “ 编辑 SSID 配置 ” 页面。

步骤 **5** 设定以下参数：

- **SSID** 名称 — 输入唯一的 SSID 名称，以便无线网络客户端识别此无线接入点。
- 隐藏无线网络 — 勾选此选项，禁用 SSID 广播功能。无线网络客户端必须要知道 SSID 名称才能接入，而无法通过网络名称扫描发现该 SSID。取消勾选此功能，允许广播该 SSID。配置网络时可能需要启用此功能，但要确保在结束配置时停用此功能。启用此选项，其他人可以用地址轻易获取 SSID 信息，并可不经授权对网络进行访问。
- 允许远程管理 — 勾选此选项，允许通过此无线网络接口远程管理路由器。
- 限制用户数量 — 启用此功能，设置此无线网络接口允许的最大无线连接数。设置范围为 1-30 。禁用此功能，不限制接入此无线网络的用户数量。
- 安全模式 — 选择安全认证模式并设置相关参数。下表给出了各安全认证模式的配置说明：

认证模式	参数配置
禁用	表示此 SSID 不使用任何无线网络安全认证，无线网络用户可以直接接入此 SSID。
WEP	使用 Wired Equivalent Privacy （WEP）无线网络安全认证。无线网络用户需使用相同的无线安全配置才能接入此 SSID。 ▪ 认证类型— 从下拉框中选择“开放系统”或“共享密钥 ”。 ▪ 密钥长度 — 设定密钥长度。可选密钥长度选项包括 64 位 （5 ASCII 字符 或 10 Hex 字符）和 128 位 （13 ASCII 字符 或 26 Hex 字符）。密钥长度越长则安全等级越高。用户可视需求选择 64 位还是 128 位。 ▪ 短语 — 输入短语后按下 “ 生成密钥 ” 按钮，设备将自动生成 “ 密钥 1”、 “ 密钥 2”、 “ 密钥 3” 和 “ 密钥 4”。用户可视需求选择使用哪一个密钥。短语最大可支持 16 位字符。 ▪ 当前密钥 — 选择使用哪一个密钥进行无线网络安全认证。 ▪ 密钥 **1**、 **2**、 **3**、 **4**— 您也可以手动设置 “ 密钥 1”、 “ 密钥 2”、 “ 密钥 3” 和 “ 密钥 4” 。选择密钥长度 64 位时，需输入 5 个 ASCII 字符 或 10 个 Hex 字符。选择密钥长度 128 位时，需输入 13 个 ASCII 字符或 26 个 Hex 字符。合法的 Hex 字符包括 0-9、 A-F。

认证模式	参数配置
WPA-Personal	使用 WiFi Protected Access （WPA）无线网络安全认证。安全等级较 WEP 标准高。无线网络用户需使用相同的无线安全配置才能接入此 SSID。 ▪ **WPA** 预共享密钥 — 输入安全密钥。密钥长度范围为 8-63 字符。 ▪ 显示密钥 — 以明文形式显示输入的安全密钥。 ▪ **WPA** 群组更新密钥间隔时间 — 输入群组密钥的更新时间。单位为秒，默认值为 3600 秒。 ▪ 加密算法 — 选择 AES 或 TKIP+AES 作为加密算法。默认值为 TKIP+AES。
WPA2- Personal	使用 WiFi Protected Access 2 （WPA2）无线网络安全认证。安全等级较 WEP 标准高。无线网络用户需使用相同的无线安全配置才能接入此 SSID。 ▪ **WPA** 预共享密钥 — 输入安全密钥。密钥长度范围为 8-63 字符。 ▪ 显示密钥 — 以明文形式显示输入的安全密钥。 ▪ **WPA** 群组更新密钥间隔时间 — 输入群组密钥的更新时间。单位为秒，默认值为 3600 秒。 ▪ 加密算法 — 选择 AES 或 TKIP+AES 作为加密算法。默认值为 AES。

认证模式	参数配置
WPA-Enterprise	使用 WiFi Protected Access （WPA）无线网络安全认证，配合 RADIUS 服务器进行无线网络用户认证。选择此功能需要配置并连接一台 RADIUS 服务器至路由器。无线网络用户需使用相同的无线安全配置才能接入此 SSID。 ▪ **WPA** 群组更新密钥间隔时间 — 输入群组密钥的更新时间。单位为秒，默认值为 3600 秒。 ▪ 加密算法 — 选择 AES 或 TKIP+AES 作为加密算法。默认值为 TKIP+AES。 ▪ **RADIUS** 服务器地址 — 输入 RADIUS 服务器的 IP 地址。 ▪ **RADIUS** 服务器端口 — 输入 RADIUS 服务器使用的端口号，默认值为 1812。 ▪ **RADIUS** 服务器密钥 — 输入 RADIUS 服务器与路由器所使用的共享密钥。 ▪ 显示密钥 — 以明文形式显示输入的共享密钥。
WPA2-Enterprise	使用 WiFi Protected Access 2 （WPA2）无线网络安全认证，配合 RADIUS 服务器进行无线网络用户认证。选择此功能需要配置并连接一台 RADIUS 服务器至路由器。无线网络用户需使用相同的无线安全配置才能接入此 SSID。 ▪ **WPA** 群组更新密钥间隔时间 — 输入群组密钥的更新时间。单位为秒，默认值为 3600 秒。 ▪ 加密算法 — 选择 AES 或 TKIP+AES 作为加密算法。默认值为 AES。 ▪ **RADIUS** 服务器地址 — 输入 RADIUS 服务器的 IP 地址。 ▪ **RADIUS** 服务器端口 — 输入 RADIUS 服务器使用的端口号，默认值为 1812。 ▪ **RADIUS** 服务器密钥 — 输入 RADIUS 服务器与路由器所使用的共享密钥。 ▪ 显示密钥 — 以明文形式显示输入的共享密钥。

步骤 6 单击 “ 确认 ”。

3G 接口配置

路由器支持 3G 无线接入功能。如需接入到 3G 无线网络，您需要将 3G USB 设备插入路由器后面板的 3G 接口，并设置相应的 3G 接口参数。

设置 3G 接口参数的步骤：

步骤 1 选择 “ 端口配置 ”>“**3G** 接口配置 ”。打开 “3G 接口配置 ” 页面。

步骤 2 设定以下参数：

- 当前**3G**无线网络— 显示提供3G网络接入服务的服务提供商或显示为“未连接”。
- 参数设置模式 — 选择手动或自动设置 3G 拨号参数。选择自动方式，路由器将自动检测 3G 无线上网卡的参数。选择手动方式，您需要手动设置 3G 无线上网卡的参数，包括：
  - **APN**— 输入 3G 网络服务提供商所提供的 APN。
  - 用户名 — 输入 3G 网络服务提供商提供的用户名。
  - 密码 — 输入 3G 网络服务提供商提供的密码。
  - 拨号字符串 — 输入 3G 网络服务提供商提供的拨号串号码。
- 连接方式 — 选择手动或自动拨号。
- 在线方式 — 当连接方式设为自动时，选择以下任意一种在线方式：
  - 一直在线 — 定期检查 3G 无线上网接口状态，断线时会自动重连。可设定断线多少秒之后进行自动重连。默认为 30 秒。
  - 按需连接 — 当空闲一段时间后，如无数据流发送至互联网时会自动断线，当有数据流发送至互联网时则再自动拨号连接。输入最大空闲时间 （单位为秒），默认为 5 秒。
- 手动拨号 — 当连接方式设为手动时，单击 “ 手动连接 ” 手动进行拨号连接。如需断开拨号连接，单击 “ 断开连接 ”。

- 服务类型 — 当您的网络服务提供商同时提供 3G 无线网络和 4G 无线网络的接入服务时，您可以选择接入到哪种无线网络。选择 “ 自动 ” 自动选择接入的无线网络类型，选择 “**3G Only**” 仅接入到 3G 无线网络，或选择 “**4G Only**” 仅接入到 4G 无线网络。

  注 请首先检查您使用的 3G USB 设备可接入的无线网络类型以及相应的计费方法，然后选择恰当的拨号网络以节约费用或提供较快的网速。

- 状态 — 显示当前路由器是否接入 3G 无线网络。

步骤 **3** 单击 “ 确认 ”。

5

网络配置

本章介绍如何配置路由器的其他网络参数。包括以下内容：

- **DDNS** 配置
- 端口转发
- 端口触发
- **DMZ** 配置
- **UPnP**
- 端口镜像
- 路由配置
- **IGMP** 配置

DDNS 配置

“DDNS 配置 ” 页面可设置路由器的动态域名解析服务功能。动态域名解析服务，简称 DDNS （Dynamic Domain Name Server），是将用户的动态 IP 地址映射到一个固定的域名解析服务上，用户每次连接网络的时候，客户端程序就会通过信息将该主机的动态 IP 地址传送给位于服务商主机上的服务器程序，服务器程序负责提供 DNS 服务并实现动态域名解析。就是说 DDNS 捕获用户每次变化的 IP 地址，然后将其与域名相对应，这样域名就可以始终解析到非固定 IP 的服务器上。互联网用户通过本地的域名服务器获得网站域名的 IP 地址，从而可以访问网站的服务。

在设置 DDNS 服务之前，您必须向 DDNS 服务提供商 （如 DynDNS.com）申请一个动态域名账号。路由器支持 DynDNS.org， TZO， ORAY 和 No-IP 服务。

设置 DDNS 服务的步骤：

步骤 **1** 选择 “ 网络配置 ”>“**DDNS** 配置 ” 菜单。打开 “DDNS 配置 ” 页面。

步骤 **2** 如需添加一个 DDNS 服务，单击 “ 添加 ”。

步骤 3 设定以下参数：

- **DDNS** 服务 — 选择 DDNS 服务提供商，如 DynDNS.org，TZO，ORAY 或 No-IP。
- 域名 — 输入 DDNS 域名地址。
- 用户名 — 输入 DDNS 账户的用户名。
- 密码 — 输入 DDNS 账户的密码。

步骤 4 单击 “ 确定 ”。

端口转发

端口转发功能允许您在网络上建立公共服务，如 web 服务、FTP 服务、email 服务或其他使用一个或多个端口号的特殊 Internet 应用程序 （如视频会议），转发到本地网络时正在使用的端口号不会改变。这一特性可使 Internet 用户通过使用 WAN 端口 IP 地址和预先定义的端口号来访问该服务器。当用户通过 Internet 向 WAN 端口 IP 地址发送此类请求时，将这些请求转发到局域网上的正确服务器。

设置单端口转发

设置单端口转发规则的步骤：

步骤 1 选择 “ 网络配置 ”>“ 端口转发 ”>“ 单端口转发 ” 菜单。打开 “ 单端口转发 ” 页面。

步骤 2 如需添加一条单端口转发规则，设定以下参数：

- 接口 — 选择 WAN 接口或 3G 网络接口。
- 协议 — 选择相应的网络协议，如 TCP 或 UDP。
- 外部端口 — 系统预设了部分服务类型选项，如 Finger、FTP、NNTP、POP3、SMTP、 Telnet 和 HTTP。选择 “ 其他 ” 可手动输入服务器所使用的外部端口号。选择其它服务类型时会自动使用各服务的缺省端口号。
- 内部 **IP** 地址 — 输入内部服务器的 IP 地址。
- 内部端口 — 系统预设了部分服务类型选项，如 Finger、FTP、NNTP、POP3、SMTP、 Telnet 和 HTTP。选择 “ 其他 ” 可手动输入服务器所使用的内部端口号。选择其它服务类型时会自动使用各服务的缺省端口号。

- 状态 — 选择启用或禁用此单端口转发规则。

步骤 3 单击 “ 添加 ”。

设置多端口转发

设置多端口转发规则的步骤：

步骤 1 选择 “ 网络配置 ”>“ 端口转发 ”>“ 多端口转发 ” 菜单。打开 “ 多端口转发 ” 页面。

步骤 2 如需添加一条多端口转发规则，设定以下参数：

- 接口 — 选择 WAN 接口或 3G 网络接口。
- 协议 — 选择相应的网络协议，如 TCP 或 UDP。
- 起始 - 结束端口 — 输入端口转发的起始端口号和结束端口号。
- 内部 **IP** 地址 — 输入内部服务器的 IP 地址。
- 状态 — 选择启用或禁用此多端口转发规则。

步骤 3 单击 “ 添加 ”，添加多端口转发规则。

端口触发

端口触发功能用于外发端口与输入端口不相同的特殊互联网应用程序。启用此功能时，路由器将监视特定端口号的外发数据。路由器会记住发送传输请求数据的 PC（LAN 侧）的 IP 地址，所以当被请求数据经路由器 （从 WAN 侧）返回时，数据借助于 IP 地址和端口映像规则被转发到正确的 PC。

设置端口触发规则的步骤：

步骤 1 选择 “ 网络配置 ”>“ 端口触发 ” 菜单。打开 “ 端口触发 ” 页面。

步骤 2 如需添加一条端口触发规则，设定以下参数：

- **WAN** 接口 — 选择欲绑定此端口触发规则的 WAN 接口。
- **LAN** 接口 — 选择欲绑定此端口触发规则的 LAN 接口。
- 协议 — 选择协议类型，如 TCP 或 UDP。

- 触发范围 — 输入端口触发所使用的端口范围。
- 转发范围 — 输入端口转发所使用的端口范围。
- 状态 — 启用或禁用此端口触发规则。

步骤 **3** 单击 “ 添加 ”，添加端口触发规则。

DMZ 配置

路由器支持软件 DMZ 和硬件 DMZ 功能。软件 DMZ 功能通过创建 NAT 规则允许私有 IP 网络连接到互联网。 NAT 规则通过将内网的私有地址翻译成一个合法的、可路由的公共网络所使用的外部 IP 地址，从而将一个私有 IP 地址替换一个公共 IP 地址。硬件 DMZ 功能将 LAN8 端口用于 DMZ 目的，以供公众查阅客户的网络和其他服务器从互联网访问。

软件 DMZ

软件 DMZ 功能通过创建 NAT 规则允许私有 IP 网络连接到互联网。 NAT 规则通过将内网的私有地址翻译成一个合法的、可路由的公共网络所使用的外部 IP 地址，从而将一个私有 IP 地址替换一个公共 IP 地址。

设置软件 DMZ 功能的步骤：

步骤 **1** 选择 “ 网络配置 ”>“**DMZ**”>“ 软件 **DMZ**” 菜单。打开 “ 软件 DMZ” 页面。

步骤 **2** 如需创建一条软件 DMZ 规则，设定以下参数：

- **DMZ** 状态 — 启用或禁用此软件 DMZ 规则。
- 外网 **IP** 地址 — 输入外网 IP 地址。
- 内网 **IP** 地址 — 输入内网服务器的 IP 地址。
- 绑定接口 — 选择软件 DMZ 规则所使用的网络接口。

步骤 **3** 单击 “ 添加 ”，添加软件 DMZ 规则。

硬件 DMZ

硬件 DMZ 功能将物理 LAN8 端口用于 DMZ 目的，以供公众查阅客户的网络和其他服务器从互联网访问。

注 此功能只支持 WAN 接口通过静态 IP 或 DHCP 模式接入互联网。硬件 DMZ 可以应用于 VPN 连接。

设置硬件 DMZ 功能的步骤：

步骤 1 选择 “ 网络配置 ”>“**DMZ**”>“ 硬件 **DMZ**” 菜单。打开 “ 硬件 DMZ” 页面。

步骤 2 启用或禁用硬件 DMZ 功能。启用此功能将路由器的 LAN8 端口设为一个 DMZ 端口。

步骤 3 如需添加一条硬件 DMZ 规则，单击 “ 添加 ”。

步骤 4 设定以下参数：

- 状态 — 启用或禁用此硬件 DMZ 规则。
- 公共 **IP**— 输入此 DMZ 规则对于互联网上的 IP 地址。
- **WAN** 接口 — 输入此 DMZ 规则所采用的 WAN 接口。

步骤 5 单击 “ 确定 ”。

UPnP

UPnP （Universal Plug and Play，通用即插即用）是一种类似于 CDP 的网络发现协议。您可以启用或禁用路由器的 UPnP 功能。

启用或禁用 UPnP 功能的步骤：

步骤 1 选择 “ 网络配置 ”>“**UPnP**” 菜单。打开 “UPnP” 页面。

步骤 2 启用或禁用 UPnP 功能。启用 UPnP 可使得路由器支持自动发现 （Auto-Discovery）功能。局域网中支持 UPnP 的终端设备可发现路由器。

步骤 3 单击 “ 确定 ”。

端口镜像

端口镜像可以通过指定一个或两个端口当成监控或分析的端口，接收来自被监控或分析的端口的报文。被监控或分析的端口称为被分析端口，拿来做监控或分析的端口称为镜像端口。

设置端口镜像功能的步骤：

步骤 1 选择 “ 网络配置 ”>“ 端口镜像 ” 菜单。打开 “ 端口镜像 ” 页面。

步骤 2 在 “ 端口镜像 ” 栏，选择启用或禁用端口镜像功能。

步骤 3 如启用端口镜像功能，分别设置 TX 和 RX 两个方向的镜像端口和分析端口：

- **TX/RX—** TX 表示数据发送方向， RX 表示数据接收方向。
- 镜像目的端口 — 选择监控其他端口传输流量的端口。
- 镜像源端口 — 选择被监控的端口。镜像目的端口不能同时被设为分析端口。

步骤 4 单击 “ 确定 ”。

路由配置

路由器允许用户在路由表中输入静态路由或使用路由协议建立动态路由表。

基本路由配置

“ 基本路由 ” 页面可设置路由器的工作模式，启用或禁用 VLAN 间路由功能以及设置静态路由规则。

路由模式设置

根据您的网络服务提供商的要求，您可以将路由器设为工作在路由模式或网关模式下。默认为网关模式。

设置路由模式的步骤：

步骤 1 选择 “ 网络配置 ”>“ 路由配置 ”>“ 基本路由 ” 菜单。打开 “ 基本路由 ” 页面。

步骤 2 在 “ 路由模式 ” 区域，选择路由器的工作模式：

- 网关模式 — 选择此选项 （建议），路由器工作在网关模式。如果您使用路由器控制进出互联网的网络连接，请使用网关模式。
- 路由模式 — 选择此选项，路由器工作在路由模式。

步骤 3 单击 “ 确定 ”。

VLAN 间路由设置

VLAN 间路由功能有助于控制广播域的大小。然而，当一个终端站需要在一个 VLAN 通信终端站的另一个 VLAN， VLAN 间路由沟通是必需的。

启用或禁用 VLAN 间路由功能的步骤：

步骤 1 选择 “ 网络配置 ”>“ 路由配置 ”>“ 基本路由 ” 菜单。打开 “ 基本路由 ” 页面。

步骤 2 在 “**VLAN** 间路由 ” 栏，启用或关闭 VLAN 间路由功能。

步骤 3 单击 “ 确定 ”。

静态路由设置

静态路由预先设定了数据包的转发路径，包括必须经过的主机或网络。静态路由的优点在于不需要消耗 CPU 资源与对端路由器交换路由信息。

设置静态路由的步骤：

步骤 1 选择 “ 网络配置 ”>“ 路由配置 ”>“ 基本路由 ” 菜单。打开 “ 基本路由 ” 页面。

步骤 2 在 “ 静态路由 ” 区域，单击 “ 添加 ” 添加静态路由规则并指定数据包抵达目标节点的路径。打开 “ 添加策略路由 ” 页面。

步骤 3 设定以下参数：

- 目的地址 — 输入目的网络或终端的 IP 地址。
- 子网掩码 — 输入目的网络或终端的子网掩码。
- 下一跳地址 — 输入下一跳的网关地址。

步骤 4 单击 “ 确定 ”。

策略路由配置

设置策略路由功能的步骤：

步骤 1 选择 “ 网络配置 ”>“ 路由配置 ”>“ 策略路由 ” 菜单。打开 “ 策略路由 ” 页面。

步骤 2 如需添加一条策略路由，单击 “ 添加 ”。

步骤 3 在打开的页面中设定以下参数：

- 策略路由规则名称 — 输入策略路由规则的名称。
- 接口 — 选择策略路由欲绑定的接口。
- 源 **IP** 地址 — 输入源节点的 IP 地址。
- 子网掩码 — 输入源网络的子网掩码。
- 目的 **IP** 地址 — 输入目的节点的 IP 地址。
- 子网掩码 — 输入目标网络的子网掩码。
- 端口 — 选择策略路由发送数据包的接口。
  - 选择 “ 任意 ” 任意选择路由端口。
  - 选择 “ 单一 ” 手动输入端口号。
  - 选择 “ 范围 ” 手动输入端口范围。
- 协议：选择此策略路由的协议类型 （如 TCP 或 UDP）。
- **DSCP**— 输入 DSCP （Differentiated Services Code Point）值。
- 下一跳 — 选择以下任意选项：
  - **IPSec** 通道 — 选择 IPsec VPN 连接作为下一跳。
  - 接口 — 从下拉框中选择一个 WAN 接口作为下一跳接口。
  - 如果接口关闭禁用此规则 — 勾选此选项，当所选下一跳接口关闭时禁用此规则。

步骤 4 单击 “ 确定 ”，保存您的配置信息并返回到 “ 策略路由 ” 页面。

动态路由 **RIP** 设置

动态路由，又称 RIP （Routing Information Protocol）是 IGP （Interior Gateway Protocol）的一种，在内部网络中使用。 RIP 允许路由器之间自动交换路由信息并动态调整路由表以适应网络变化。

动态路由功能使得路由器可以自适应物理上的网络拓扑变化并与其它路由器交换路由表信息。路由器通过计算起始点与目标点之间最优化 （跳数最少）的路径选择数据包如何路由。默认情况下，路由器禁用 RIP 功能。

设置动态路由功能的步骤：

步骤 **1** 选择 “ 网络配置 ”>“ 路由配置 ”>“**RIP**” 菜单。打开 “RIP” 页面。

步骤 **2** 在 “**RIP** 基本配置 ” 栏，设置以下参数：

- **RIP** 状态 — 启用或停用 RIP。默认为禁用。
- **RIP** 版本 — 选择 RIP 版本。路由器支持版本 1 （RIPv1）、版本 2 （RIPv2）和 RIPv1/v2。
- **RIP** 计时器 — 分别设置 RIP 的更新时间、超时时间以及 Flush 时间。单位为秒。
- **RIP** 通告 — 选择通过接口或 RIP 网络交换路由信息。

步骤 **3** 如果通过接口交换路由信息 （“**RIP** 通告 ” 被设为 “ 接口 ”），在 “**RIP** 接口成员 ” 栏勾选 “ 启用 RIP”，应用 RIP 到相应的接口。

步骤 **4** 单击 “ 编辑 ”，可编辑相应接口的 RIP 设置信息：

- **RIP**— 显示此接口是否启用或禁用 RIP。
- 无源接口 — 设置接口如何接收RIP数据包。勾选“启用”启用无源模式到该接口，所有接收的数据包正常处理， RIP 守护进程不发送多播或单播 RIP 数据包；勾选 “ 禁用 ” 禁用此功能。
- 认证 — 选择以下任意 RIP 认证方法：
  - 无 — 不进行认证。
  - 简单的密码验证 — 使用简单的密码进行认证。
  - **MD5** 认证 — 采用 MD5 进行认证。

步骤 **5** 单击 “ 确定 ”。

步骤 **6** 如果通过 RIP 网络交换路由信息 （“**RIP** 通告 ” 被设为 “ 网络 ”），在 “**RIP** 网络 ” 栏手动添加 RIP 网络。单击 “ 添加 ”，输入 RIP 网络的 IP 地址。

步骤 7 单击 “ 确定 ”。

查看路由表信息

如需查看路由表信息，选择 “ 网络配置 ”>“ 路由配置 ”>“ 路由表 ” 菜单。打开 “ 路由表 ” 页面。

路由表中显示以下信息：

- 目的地局域网 **IP** 地址 — 路由指向的主机或网络的 IP 地址。
- 子网掩码 — 目的网络的子网掩码。
- 网关 — 目的主机或网络可到达的网关地址。
- 接口 — 此路由所采用的路由器接口。

IGMP 配置

“IGMP” 页面可启用 IGMP （Internet Group Management Protocol）功能，使得路由器支持 IPTV 的组播功能。

设置 IGMP 功能的步骤：

步骤 1 选择 “ 网络配置 ”>“**IGMP**” 菜单。打开 “IGMP” 页面。

步骤 2 设定以下参数：

- **IGMP** 版本 — 选择 IGMPv1 或 IGMPv2。
- **IGMP Proxy**— 启用或禁用 IGMP Proxy 功能。
- **IGMP Snooping**— 启用或禁用 IGMP Snooping 功能。支持群播路由的路由器，会对其连接接口 （VLAN）下面的所有端口进行 Flooding 的传播。为了避免 Flooding 浪费网络频宽，使用 IGMP Snoopng 可撷取 IGMP 报文，来取得连接接口下的哪些端口需要群播资料，路由器可针对需要的端口来发送群播报文，而不是对接口下的所有端口进行发送，因此可有效提高效能。

步骤 3 单击 “ 确定 ”。

6

VPN 配置

路由器支持 IPsec VPN 功能以建立网关到网关或客户端到网关的 VPN 隧道。通过 VPN 隧道，路由器可以与一台启用 IPsec VPN 功能的远程路由器或安装有 VPN 客户端软件的远程用户建立安全的 VPN 连接。例如，您可以将一个分支机构的路由器连接到公司总部的 VPN 路由器，使得分支机构的员工可以通过 VPN 隧道安全地远程访问公司的内网资源。

本章介绍如何配置路由器的 IPsec VPN 功能，使得远程用户建立安全的 VPN 隧道远程访问公司网络和相关服务。包括以下内容：

- 查看 **IPSec VPN** 状态
- 设置 **IPsec VPN** 连接

查看 IPSec VPN 状态

“IPsec VPN” 页面显示路由器所有 IPsec VPN 策略的详细信息及其连接状态。

查看 IPsec VPN 策略信息和连接状态的步骤：

步骤 1 选择 “**VPN** 配置 ”>“**IPsec VPN**” 菜单。打开 “IPsec VPN” 页面。

“**IPsec** 连接策略 ” 栏显示所有的 IPsec VPN 策略及其连接状态，包括以下信息：

- 策略名称 — IPsec VPN 策略的名称。
- 状态 — IPsec VPN 策略是否已启用。
- 接口 — IPsec VPN 策略所采用的通信接口。
- 连接类型 — IPsec VPN 策略的组网模式，其中：
  - 站点到站点 **VPN**— 表示两台 VPN 设备之间建立安全的 VPN 隧道。
  - **PC**到站点**VPN**— 表示远程用户通过使用第三方VPN软件客户端连接到VPN网关。

- 对端网关地址 / 主机名 — 显示远程网关 IP 地址或主机名称。
  - 如果连接类型为站点到站点 VPN，则表示对端网关的 IP 地址或主机名称。
  - 如果连接类型为PC到站点VPN，则表示接入到设备的PC客户端的IP地址或主机名称。如有多台 PC 客户端接入，则显示多个 PC 客户端的 IP 地址并用逗号隔开。
- 本端网关地址 — 显示本地网关的 IP 地址。
- 认证方式 — 显示安全认证的方式。
- 连接状态 — 显示 VPN 连接当前是否建立。

步骤 2 如需编辑 IPsec VPN 策略，选择相应的条目并单击 “ 编辑 ”。详见 “ 设置 **IPsec VPN** 连接 ”。

步骤 3 如需删除某— IPsec VPN 策略，选择相应的条目并单击 “ 删除 ”。

设置 IPsec VPN 连接

单个 IPsec VPN 策略可用于建立两个节点之间的安全 VPN 隧道。路由器最多允许创建 50 条 VPN 连接通道。

创建站点到站点 VPN

站点到站点 VPN 可在两台 VPN 设备之间建立安全的 VPN 隧道，如在公司总部和远程办公分支机构的两台路由器之间建立 VPN 连接。

创建站点到站点 VPN 连接的步骤：

步骤 1 选择 “**VPN** 配置 ”>“**IPsec VPN**” 菜单。打开 “IPsec VPN” 页面。

步骤 2 单击 “ 添加 ”。

步骤 3 在 “**IPsec VPN** 策略 ” 区域，设定以下参数：

- 启用 — 启用或禁用该 IPsec VPN 策略。
- 策略编号 — 选择 IPsec VPN 策略的编号。
- **IPsec VPN** 策略名称 — 输入 IPsec VPN 策略的名称以便于识别。

步骤 4 在 “ 网关信息 ” 区域，设定以下参数：

- **VPN Failover**— 选择启用或禁用 VPN Failover 功能。启用 VPN Failover 功能，路由器将自动选择 VPN 隧道的通信接口。禁用此功能需手动设定 VPN 隧道的通信接口。
- 接口 — 如果禁用 VPN Failover 功能，选择 IPsec VPN 策略所采用的通信接口。
- 组网模式 — 选择 “ 站点到站点 ”。
- **VPN** 容灾 — 启用或禁用 VPN 容灾功能（缺省为禁用）。VPN 容灾功能可用于当主用 VPN 连接断开时，自动切换到备用 VPN 连接。
  - 主选 — 输入主选对端网关的 IP 地址或主机名称。
  - 备选 — 输入备选对端网关的 IP 地址或主机名称。
  - 恢复主用后切回 — 选择启用或禁用此功能。启用此功能时，当与主选对端网关的 VPN 连接重新建立后，会自动切回使用主用 VPN 连接。禁用此功能时，维持使用现在设备上所建立的对端网关 IPsec 隧道。缺省为启用。
- 本端网关地址 — 显示本端网关的 IP 地址，通常为本地网关的 WAN 接口地址。
- 本端网关 **ID**— 选择 “ 自动 ” 自动获取本地网关的 IP 地址或域名，或选择 “ 手动 ” 手动输入本地网关的 IP 地址或域名。
- 对端网关 **ID**— 选择 “ 自动 ” 自动获取主用远程网关的 IP 地址或域名，或选择 “ 手动 ” 手动输入主用远程网关的 IP 地址或域名。
- 备选对端网关地址 — 选择 “ 自动 ” 自动获取备用远程网关的 IP 地址或域名，或选择 “ 手动 ” 手动输入备用远程网关的 IP 地址或域名。
- 认证方式 — IPsec VPN 连接使用密钥进行认证，请在 “ 预共享密钥 ” 处输入进行认证的安全密钥。密钥长度范围为 1-128 个字符长度。
- 显示密钥 — 勾选以明文形式显示预共享密钥。

步骤 5 在 “ 流量筛选 ” 区域，选择 VPN 流量的筛选方式：

- 路由 — 根据路由信息进行筛选。选择此选项，输入被 IPsec 保护的目的地址和掩码。
- 基于流量 — 根据流量特征进行筛选。选择此选项，分别输入源地址 / 通配符以及目的地址 / 通配符。

步骤 6 在 “ 新增感兴趣流配置 ” 区域，对于站点到站点的 IPsec VPN 流量配置，在一条 VPN 策略下可以定义多达 49 条感兴趣的流量。

- 本地网络 — 在 “ 地址 ” 栏输入本地网络地址，并在 “ 子网掩码 ” 栏输入子网掩码。

- 目的网络 — 在“地址”栏输入目的网络地址，并在“子网掩码”栏输入子网掩码。
- 单击“添加”按钮后下面窗口就会显示已经添加成功的通道。也可以选择窗口中的一个或多个通道，修改本地网络或目的网络的地址和子网掩码信息。

步骤 7 单击“**VPN** 高级配置”，设置 IPSec VPN 策略的高级参数。

- 第一阶段 — 设定以下参数：
  - 交换模式 — 选择“**Main Mode**”或“**Aggressive Mode**”。Main 模式具备较高安全等级，但是频繁的密钥交换造成较慢的连接速率。 Aggressive 模式使用较少的密钥交换程序，具备较快的连接速率，但是安全等级较 Main 模式低。
  - 认证算法 — 选择 SHA1 或 MD5 作为认证算法。缺省值为 SHA1。
  - 加密算法 — 选择 DES、3DES、AES-128、AES-192 或 AES-256 作为加密算法。缺省值为 AES-256。
  - **DH Group**— 选择 Diffie-Hellman Group1 或 Diffie-Hellman Group2。缺省为 DH Group1。
  - **SA** 生存周期 — 设定安全协商的生存周期，单位为秒。设定范围为 60-604800 秒，默认为 86400 秒。
- 第二阶段 — 设定以下参数：
  - **ESP** 认证算法 — 选择 SHA1 或 MD5 作为第二阶段 ESP 认证算法。缺省为 SHA1。
  - **ESP** 加密算法 — 选择 DES、3DES、AES-128、AES-192 或 AES-256 作为第二阶段的 ESP 加密算法。缺省为 AES-256。
  - **PFS**— 启用或禁用 PFS 功能 （缺省为禁用）。
  - **SA**生存周期— 分别设定“基于时间的生存周期”和“基于流量的生存周期”。其中“基于时间的生存周期”的设置范围为 180-604800 秒，缺省为 3600 秒，而“基于流量的生存周期”的设置范围为 2560-4294967295 千字节，缺省为 1843200 千字节。
  - **DPD**— 启用或关闭 DPD （Dead Peer Detection）功能 （缺省为禁用）。如启用 DPD 功能，分别输入 DPD Delay 周期和 DPD 超时时间。

步骤 8 单击“确定”。

创建 PC 到站点 VPN

PC 到站点 VPN 策略允许远程用户使用第三方 VPN 客户端软件连接到本地 VPN 网关。路由器可支持 TheGreenBow 和 Shrewsoft 两款 VPN 客户端软件。

创建 PC 到站点 VPN 连接策略的步骤：

步骤 1 选择 “**VPN** 配置 ”>“**IPsec VPN**” 菜单。打开 “IPsec VPN” 页面。

步骤 2 单击 “ 添加 ”。

步骤 3 在 “**IPsec VPN** 策略 ” 区域，设定以下参数：

- 启用 — 启用或禁用该 IPsec VPN 策略。
- 策略编号 — 选择 IPsec VPN 策略的编号。
- **IPsec VPN** 策略名称 — 输入 IPsec VPN 策略的名称以便于识别。

步骤 4 在 “ 网关信息 ” 区域，设定以下参数：

- **VPN Failover**— 选择启用或禁用 VPN Failover 功能。启用 VPN Failover 功能，路由器将自动选择 VPN 隧道的通信接口。禁用此功能需手动设定 VPN 隧道的通信接口。
- 接口 — 如果禁用 VPN Failover 功能，选择 IPsec VPN 策略所采用的通信接口。
- 组网模式 — 选择 “PC 到站点 ” 作为 VPN 组网方式。
- 本端网关地址 — 显示本端网关的 IP 地址。
- 本端网关 **ID**— 选择 “ 自动 ” 自动获取本地网关的 IP 地址或域名，或选择 “ 手动 ” 手动输入本地网关的 IP 地址或域名。
- 对端网关 **ID**— 选择 “ 自动 ” 自动获取主用远程网关的 IP 地址或域名，或选择 “ 手动 ” 手动输入主用远程网关的 IP 地址或域名。
- 备选对端网关地址 — 选择 “ 自动 ” 自动获取备用远程网关的 IP 地址或域名，或选择 “ 手动 ” 手动输入备用远程网关的 IP 地址或域名。
- 认证方式 — IPsec VPN 连接使用密钥进行认证，请在 “ 预共享密钥 ” 处输入进行认证的安全密钥。密钥长度范围为 1-128 个字符长度。
- 显示密钥 — 勾选以明文形式显示预共享密钥。

步骤 5 单击 “**VPN** 高级配置 ”，设置 IPSec VPN 策略的高级参数。

- 第一阶段 — 设定以下参数：

- 交换模式 — 选择 “**Main Mode**” 或 “**Aggressive Mode**”。Main 模式具备较高安全等级，但是频繁的密钥交换造成较慢的连接速率。 Aggressive 模式使用较少的密钥交换程序，具备较快的连接速率，但是安全等级较 Main 模式低。
- 认证算法 — 选择 SHA1 或 MD5 作为认证算法。缺省值为 SHA1。
- 加密算法 — 选择 DES、3DES、AES-128、AES-192 或 AES-256 作为加密算法。缺省值为 AES-256。
- **DH Group**— 选择 Diffie-Hellman Group1 或 Diffie-Hellman Group2。缺省为 DH Group1。
- **SA** 生存周期 — 设定安全协商的生存周期，单位为秒。设定范围为 60-604800 秒，默认为 86400 秒。

▪ 第二阶段 — 设定以下参数：

- **ESP** 认证算法 — 选择 SHA1 或 MD5 作为第二阶段 ESP 认证算法。缺省为 SHA1。
- **ESP** 加密算法 — 选择 DES、3DES、AES-128、AES-192 或 AES-256 作为第二阶段的 ESP 加密算法。缺省为 AES-256。
- **PFS**— 启用或禁用 PFS 功能 （缺省为禁用）。
- **SA**生存周期— 分别设定“基于时间的生存周期”和“基于流量的生存周期”。其中 “ 基于时间的生存周期 ” 的设置范围为 180-604800 秒，缺省为 3600 秒，而 “ 基于流量的生存周期 ” 的设置范围为 2560-4294967295 千字节，缺省为 1843200 千字节。
- **DPD**— 启用或关闭 DPD 功能。缺省为禁用。如您启用 DPD 功能，分别输入 DPD Delay 周期和 DPD 超时时间。

步骤 **6** 单击 “ 确定 ”。

7

QoS 配置

本章介绍如何设置服务质量 （Quality of Service， QoS）功能，包括以下内容：

- 接口带宽配置
- 流量限制策略
- 会话数限制

接口带宽配置

“ 接口带宽配置 ” 页面可限制 WAN 接口的上行带宽。从 WAN 接口出去的总流量不得超出此设定值。

限制 WAN 接口上行带宽的步骤：

步骤 **1** 选择 “**QoS** 配置 ”>“ 接口带宽配置 ” 菜单。打开 “ 接口带宽配置 ” 页面。

步骤 **2** 勾选 “ 启用 ”，限制相应接口的上行带宽。

步骤 **3** 单击 “ 确定 ”。

步骤 **4** 如需修改某一接口的上行带宽上限以及指定不同接口队列的保证速率和最大速率，单击 “ 修改 ” 并设定以下参数：

- 限速速率 — 输入该端口允许的最大上行速率。
- 接口队列配置 — 分别设置每一个接口队列必须保证的上行速率以及允许的最大上行速率：
  - 严格优先队列 — 输入严格优先队列必须保证的上行速率。在满足严格优先队列的上行速率之外，您可以将剩余的带宽分配到其他队列。
  - 保证速率 — 输入其他各队列的保证带宽。
  - 最大速率 — 输入其他各队列允许的最大带宽。

步骤 5 单击 “ 确定 ”，保存您的配置信息并返回到之前的配置界面。

流量限制策略

流量限制策略可标记不同类型流量的优先级，从而达到流量控制的目的。“ 流量限制策略 ” 页面可添加、删除或编辑流量限制策略配置。路由器最多可以可添加 25 条流量限制策略。

设置流量控制策略的步骤：

步骤 1 选择 “**QoS** 配置 ”>“ 流量限制策略 ” 菜单。打开 “ 流量限制策略 ” 页面。

此页面显示系统所有的流量限制策略信息，包括策略名称、应用队列、类型、配置信息等。

步骤 2 如需添加一条流量限制策略，单击 “ 添加 ”。

步骤 3 设定以下参数：

- 策略名称 — 输入流量限制策略名称。
- 策略类型 — 选择基于何种类型进行流量限制。您可以基于指定的目的端口、MAC 地址、物理端口、 VLAN 或 IP 地址进行流量控制。
  - 目的端口 — 基于目的端口进行流量控制。选择此项，分别在 “ 应用协议 ”、“LAN 接口 ” 和 “ 目的端口 ” 三个字段中设定相应的应用协议、目的端口和 LAN 接口等信息。路由器预设了部分常用的应用协议，且预设的应用协议带入了指定的目的端口。您也可以手动指定应用协议类型并设定端口范围。
  - **MAC** 地址 — 基于 MAC 地址进行流量控制。选择此项，分别在 “MAC 地址 ” 和 “LAN 接口 ” 字段中设定相应的 MAC 地址和 LAN 接口。
  - 物理端口 — 基于物理端口进行流量控制。选择此项，分别在 “ 物理端口 ” 和 “LAN 接口 ” 下拉框中选择相应的物理端口和 LAN 接口。
  - **VLAN**— 基于 VLAN 进行流量控制。选择此项，从 “VLAN” 下拉框中选择此策略所限制的 VLAN。
  - **IP** 地址 — 基于主机 IP 地址进行流量控制。选择此项，分别在 “ 起始地址 ”、“ 结束地址 ” 和 “LAN 接口 ” 字段内设定此策略所限制的主机 IP 地址范围和 LAN 接口。
- 应用队列 — 选择此流量限制策略所使用的接口队列。

- 标记功能 — 启用或关闭标记流量优先级功能。
- 标记值 — 如果启用此功能，选择采用何种方法标记流量的优先级，并设定相应的优先级值：
  - **CoS**— 选择此选项，通过 CoS（Class of Service，服务等级）值分配流量优先级。输入匹配的 CoS 值。范围为 0 - 7。
  - **DHCP**— 选择此选项，通过 DSCP（Differentiated Services Code Point，差分服务代码点）值分配流量优先级。输入匹配的 DSCP 值。范围为 0-63。

步骤 **4** 单击 “ 确定 ”，保存您的配置信息并返回到 “ 流量限制策略 ” 页面。

会话数限制

“ 会话数限制 ” 页面可分别设置基于 IP 地址或基于物理端口的最大会话数，并限制整个系统允许的最大会话总数。

设置会话数限制功能的步骤：

步骤 **1** 选择 “**QoS** 配置 ”>“ 会话数限制 ” 菜单。打开 “ 会话数限制 ” 页面。

步骤 **2** 启用或禁用会话数限制功能。

步骤 **3** 如启用此功能，设定以下参数：

- 基于 **IP** 地址限制 — 选择此选项，输入每 IP 允许的最大会话数和欲限制的 IP 地址范围。
- 基于物理端口限制 — 选择此选项，输入每物理端口允许的最大会话数以及选取欲限制的物理端口。
- 最大会话数 — 输入整个系统允许的最大会话总数。当系统会话总数达到此限制值后，即不允许任何 IP 地址或物理端口建立新会话。

步骤 **4** 单击 “ 确定 ”。

8

安全配置

本章介绍如何设置路由器的安全功能以保护您的网络，包括以下内容：

- 防火墙
- 防火墙
- 网站过滤
- 访问控制
- **MAC** 地址过滤
- 防 **ARP** 攻击
- **ALG**

防火墙

“ 基本防火墙 ” 页面可启用或禁用防火墙功能并设置其他安全选项。

设置路由器防火墙功能的步骤：

步骤 **1** 选择 “ 安全配置 ” > “ 基本防火墙 ”。打开 “ 基本防火墙 ” 页面。

步骤 **2** 在 “ 防火墙配置 ” 栏，选择启用或禁用防火墙功能。不推荐禁用防火墙功能，建议您启用该功能。

步骤 **3** 在 “ 禁止 **Proxy**” 栏，勾选此选项可禁止 HTTP 代理。HTTP 代理允许您的主机通过代理访问其它主机或网络，在这个过程中可能会绕开某些安全规则。例如：安全规则已设置阻止访问某一特定 IP 地址，但是通过代理仍然可以将这一访问请求发出，导致安全规则失效。

步骤 **4** 在 “ 禁止 **Java**” 栏，勾选此选项可禁止加载 Java applets。Java applets 是嵌入 web 网页的小程序，用于实现页面的动态功能。一个恶意 Java applet 会危害您的主机。

步骤 **5** 在 “ 禁止 **Cookies**” 栏，勾选此选项可禁止使用 cookies。 cookies 一般用于储存网站的登录信息，也有网站使用 cookies 储存用户轨迹信息与浏览习惯。勾选此选项将过滤由网站创建的 cookies。

注 许多网站要求必须使用 cookies 才能正确访问。禁止 cookies 可能会导致这些网站访问异常。

步骤 **6** 在 “ 禁止 **ActiveX**” 栏，勾选此选项可禁止加载 ActiveX。与 Java applets 相似，ActiveX 在用户使用浏览器时会加载到网页。一个恶意 ActiveX 会危害您的主机。

步骤 **7** 在 “ 禁止 **Ping**” 栏，勾选此项可禁止来自 WAN 端口的 ping 请求。 ping 命令可以测试网络连接情况和检测主机，同时回应 ping 命令也会耗费本机资源。所以禁止 ping 命令可以预防某端口发来的恶意攻击。

步骤 **8** 在 “ 过滤端口 ” 栏，输入用来过滤 HTTP 流量的端口。防火墙只监视和控制通过该端口的网络访问流量。

步骤 **9** 单击 “ 确定 ”。

DoS 攻击防护

“DoS 攻击防护 ” 页面可启用或禁用常见的 DoS 攻击防护功能。

设置 DoS 攻击防护功能的步骤：

步骤 **1** 选择 “ 安全配置 ” > “**DoS** 攻击防护 ”。打开 “DoS 攻击防护 ” 页面。

步骤 **2** 在 “**DoS** 攻击防护 ” 栏，选择启用或禁用 DoS 攻击防护功能。

步骤 **3** 路由器支持三种 DoS 攻击防护，包括 SYN Flood、 UDP Flood 和 ICMP Flood。勾选 “ 启用 ” 可启用相应的 DoS 攻击防护，并设定其触发阈值数。阈值设置范围为 400-60000 攻击次数 / 秒，缺省为 1000。

步骤 **4** 单击 “ 确定 ”。

网站过滤

路由器支持根据黑名单或白名单进行网站过滤。

设置网站过滤功能的步骤：

步骤 1 选择“安全配置”>“网站过滤”。打开“网站过滤”页面。

步骤 2 选择过滤类型：

- 黑名单 — 选择此选项，所有符合过滤规则的网站将被拒绝访问，而不在过滤规则列表中的网站将被允许访问。
- 白名单 — 选择此选项，所有符合过滤规则的网站将被允许访问，而不在过滤规则列表中的网站将被拒绝访问。

步骤 3 路由器根据 URL、关键字或文件类型进行网站访问过滤。如需添加一条网站过滤规则，设定以下参数：

- **URL/** 关键字 — 输入欲过滤的 URL 地址或关键字。
- 文件类型 — 选择欲过滤的文件类型。

步骤 4 单击“添加”，添加此网站过滤规则。

步骤 5 如需删除已创建的网站过滤规则，选择要删除的过滤规则然后单击“删除”。

步骤 6 如需将设置的网站过滤规则导出到本地，单击“导出”。

步骤 7 在“导入网站过滤规则”栏，如需从本地批量导入网站过滤规则，单击“浏览”，从本地 PC 选择导入文件，然后单击“导入”。

访问控制

“访问控制”页面可设置访问控制类型和定义访问控制策略。访问控制策略用于定义访问控制的流量类型，而访问控制类型用于定义路由器如何控制符合条件的流量。白名单表示所有符合访问控制策略条件的流量允许通过，而其他 LAN 到 WAN 的流量将被拒绝；黑名单表示所有符合访问控制策略条件的流量被拒绝通过，而其他 LAN 到 WAN 的流量被允许通过。

设置访问控制功能的步骤：

步骤 **1** 选择“安全配置”>“访问控制”。打开“访问控制”页面。

步骤 **2** 在“设置控制类型”部分，选择访问控制的类型。路由器支持黑名单和白名单两种访问控制类型，其中：

- 白名单— 表示所有符合访问控制策略条件的流量允许通过，而其他LAN到WAN的流量将被拒绝。
- 黑名单 — 表示所有符合访问控制策略条件的流量被拒绝通过，而其他 LAN 到 WAN 的流量被允许通过。

步骤 **3** 在“访问控制策略”区域，可设置访问控制策略。访问控制策略可以根据时间段、协议类型、物理端口以及来源地址和目的地址筛选要控制的流量类型。单击“添加”，添加一条访问控制策略。打开“访问控制策略配置”页面。

步骤 **4** 设定以下参数：

- 起止时间 — 输入访问控制策略生效的起止时间。
- 星期 — 勾选访问控制策略每周生效的具体日期。
- 协议 — 选择要控制的流量协议类型。选择 TCP/UDP、TCP 或 UDP 等选项时，需输入相应的端口号。选择“全部流量”或其他协议类型，无需定义端口号。
- 源物理端口 — 选择流量通过的物理端口。选择“任意”表示无论客户端连接到哪个物理端口或无线网络接入点。
- 源 **IP** 地址 — 设定流量的来源类型。
  - 任何 **IP** 地址 — 表示不限制流量的来源类型。
  - 单个 **IP** 地址 — 表示控制来自特定源 IP 地址的流量。
  - **IP** 地址段 — 表示控制来自特定源 IP 网段的流量。
- 目的 **IP** 地址 — 设定流量的目的类型。
  - 任何 **IP** 地址 — 表示控制访问所有目的 IP 地址的流量。

- 单个 **IP** 地址 — 表示控制访问特定的目的 IP 地址的流量。
- **IP** 地址段 — 表示控制访问特定目的子网的流量。

▪ 目的端口 — 输入流量的目的端口或端口范围。

▪ 状态 — 选择启用或禁用此访问控制策略。

步骤 **5** 单击 “ 确定 ”。返回到 “ 访问控制 ” 页面。

MAC 地址过滤

MAC 地址过滤功能基于物理 MAC 地址允许或拒绝特定主机访问网络。 “MAC 地址过滤 ” 页面可定义过滤类型以及 MAC 地址过滤规则。

设置 MAC 地址过滤的步骤：

步骤 **1** 选择 “ 安全配置 ” > “**MAC** 地址过滤 ”。打开 “MAC 地址过滤 ” 页面。

步骤 **2** 选择过滤类型：

▪ 禁止访问网络 — 符合 MAC 地址列表的拒绝通过。

▪ 允许访问网络 — 符合 MAC 地址列表的允许通过。

步骤 **3** 在 “**MAC** 地址过滤策略 ” 栏，可查看和设置 MAC 地址过滤规则。如需添加一条 MAC 地址过滤规则，单击 “ 添加 ”。您最多可添加 20 条 MAC 地址过滤规则。

步骤 **4** 设定以下参数：

▪ **MAC** 地址 — 输入要过滤的 MAC 地址。

▪ 起止时间 — 输入 MAC 地址过滤规则生效的起始和终止时间。

▪ 星期 — 勾选每星期中 MAC 地址过滤规则生效的日期。

步骤 **5** 单击 “ 确定 ”。返回到 “MAC 地址过滤 ” 页面。

防 ARP 攻击

“ 防 ARP 攻击 ” 页面可启用或禁用常见的 ARP 攻击防护功能以及设置 IP/MAC 地址绑定规则。

设置 ARP 攻击防护功能的步骤：

步骤 1 选择 “ 安全配置 ” > “ 防 **ARP** 攻击 ”。打开 “ 防 ARP 攻击 ” 页面。

步骤 2 设定以下参数：

- 防 **ARP** 攻击 — 选择启用或禁用防 ARP 攻击功能。
- 启用自动学习 — 启用或禁用自动学习功能。若启动自动学习机制，系统会根据使用者的上网形态来判定该 IP/MAC 是否为合法的 IP/MAC。若判定为合法的 IP/MAC ，则系统会进行自动绑定 IP/MAC 的动作。
- **ARP Flooding** 阈值 — 输入 ARP Flooding 攻击的阈值。该数值决定每一秒系统接受 ARP 包的数目。当值设得越大，代表系统该秒内可允许收到的 ARP 包越多。若要防止系统被 ARP Flooding 攻击而瘫痪，这个值必须设为较小的值。
- **ARP** 广播间隔 — 输入 ARP 广播的间隔时间。为了要让所有网络使用者可以得到正确的系统 IP/MAC 值，系统会定期发出信息更新网络使用者系统的 IP/MAC，这个数值代表的是系统发信息的间隔时间，单位是秒。 “0” 代表系统关闭该功能。

步骤 3 单击 “ 确定 ”。

步骤 4 在 “**IP & MAC** 地址绑定规则 ” 区域，单击 “ 添加 ” 可手动添加 IP/MAC 地址绑定规则。

步骤 5 设定以下参数：

- **IP** 地址 — 输入 IP 地址。
- **MAC** 地址 — 输入与该 IP 地址进行绑定的 MAC 地址。

步骤 6 单击 “ 确定 ”，保存您的配置信息并返回到 “ 防 ARP 攻击 ” 页面。

ALG

“ALG” 页面可设置路由器的应用层网关 （Application Level Gateway， ALG）功能。

设置 ALG 功能的步骤：

步骤 1 选择 “ 安全配置 ”>“**ALG**” 菜单。打开 “ALG” 页面。

步骤 2 启用或禁用相应协议类型的 ALG 支持。路由器提供 GRE、 SIP、 H.323、 IPSEC、 L2TP、 RTSP 和 IPsec NAT-T 等应用协议的 ALG 支持。

步骤 3 单击 “ 确定 ” 。

9

系统管理

本章介绍如何设置路由器的各项系统管理功能。您可以备份系统配置，恢复设备出厂设置，升级固件版本，执行系统诊断操作，设置系统时间，管理远程访问方法以及设置系统日志等。

本章包括以下内容：

- 设备重启
- 密码复杂度设置
- 用户管理
- 恢复系统配置
- 配置维护
- 软件升级
- 故障诊断工具
- 系统时间设置
- **TR-069** 配置
- **SNMP** 配置
- 远程管理
- 系统日志管理

设备重启

用户可以通过以下两种方式重启路由器：

- 使用回形针或笔尖长按路由器后面板的重置按钮 （**RESET**）至少 1 秒钟但不超过 5 秒钟，路由器将自动重启。
- 通过基于 web 的设备管理器重启路由器。

通过基于 web 的设备管理器重启路由器的步骤：

步骤 1 选择 “ 系统管理 ”>“ 设备重启 ” 菜单。打开 “ 设备重启 ” 页面。

步骤 2 单击 “ 重启 ”。

步骤 3 重启设备将会使当前网络断开几秒钟，确认请单击 “**OK**”。

密码复杂度设置

“ 密码复杂度 ” 页面可修改系统的密码复杂度设置。系统默认的最低密码复杂度要求包括：

- 新密码不能与用户名相同
- 新密码不能与当前密码相同
- 密码长度至少为 8 个字符
- 密码必须包含至少 3 种字符类型 （字符类型包括大写字母、小写字母、数字和特殊字符）

设置密码复杂度的步骤：

步骤 1 选择 “ 系统管理 ” >“ 密码复杂度 ” 菜单。打开 “ 密码复杂度 ” 页面。

步骤 2 设定以下参数：

- 密码复杂度配置 — 启用或禁用密码复杂度配置。
- 最小密码长度 — 输入允许的最短密码长度。默认为 8 个字符长度。
- 最小字符类型数 — 输入密码至少应包含几种字符类型。可用的字符类型包括大写字母、小写字母、数字和特殊字符。默认至少包含 3 种字符类型。
- 新密码不能与当前密码相同 — 启用此选项，新密码不能与现在的密码相同。
- 密码老化 — 启用此选项，密码过期后用户必须重新设置密码。
- 密码老化时间 — 输入密码有效期的最大时间。默认为 180 天。

步骤 3 单击 “ 确定 ”。

用户管理

“用户管理”页面可查看用户信息，修改用户密码，以及添加或删除普通用户。

查看用户信息

选择“系统管理”>“用户管理”菜单。打开“用户管理”页面。

在“用户列表”栏，显示所有用户（包括默认的系统管理员账号和访客账号以及由管理员自定义的普通用户）的基本信息，其中“访问等级”表示用户的访问权限。

路由器支持普通用户和系统管理员 2 个访问等级。系统管理员拥有完全设置系统参数和添加普通用户的权限，而普通用户只能查看基本的系统信息和修改其默认的密码。普通用户不能添加新用户或设置其它系统参数。

路由器默认提供 1 个系统管理员账号（cisco）和 1 个访客账号（guest）。默认的系统管理员账号和访客账号的名称不能修改，但可以修改其密码。系统管理员账号的默认密码为 cisco，访客账号的默认密码为 guest。为防止未经授权的访问，建议您首次登录之后立即修改系统管理员账号的密码。

添加新用户

如需添加新用户，您必须以系统管理员账号登录。路由器最多支持 5 个用户，包括系统默认的管理员账号和普通账号在内。

添加新用户的步骤：

步骤 1 选择“系统管理”>“用户管理”菜单。打开“用户管理”页面。

步骤 2 在“添加本地用户”栏设定以下参数：

- 用户名 — 输入用户名称。
- 密码 — 输入用户密码。如果您启用了密码复杂度设置，新密码应满足密码复杂度的要求。默认情况下，密码应包含至少三种字符类型（字符类型包括大小写字母、数字和特殊字符）且密码长度不少于 8 个字符。
- 确认密码 — 再次输入新设的密码。

步骤 3 单击“添加”。

修改用户密码

为防止未经授权的访问，建议您首次登录之后立即修改默认的管理员密码。您也可以修改普通用户的密码。

修改用户密码的步骤：

步骤 1 选择“系统管理”>“用户管理”菜单。打开“用户管理”页面。

步骤 2 在“用户列表”栏，勾选要修改密码的用户。

步骤 3 单击“修改密码”，设定以下参数：

- 当前密码 — 输入用户当前使用的密码。
- 新密码 — 输入一个新密码。如果您启用了密码复杂度设置，新密码应满足密码复杂度的要求。默认情况下，密码应包含至少三种字符类型（字符类型包括大小写字母、数字和特殊字符）且密码长度不少于 8 个字符。
- 确认密码 — 再次输入新设的密码。

步骤 4 单击“确定”。

删除用户

以管理员账号登录，可从本地数据库删除管理员自定义的普通用户。系统默认的管理员账号和访客账号无法删除。

删除普通用户的步骤：

步骤 1 选择“系统管理”>“用户管理”菜单。打开“用户管理”页面。

步骤 2 在“用户列表”栏内，勾选要删除的普通用户。

步骤 3 单击“删除”。

步骤 4 单击“OK”，成功删除用户。

恢复系统配置

路由器支持 2 种恢复出厂配置方式：

- 使用回形针或笔尖长按路由器后面板的重置按钮 （**RESET**）超过 5 秒。路由器将自动重启并恢复到出厂设置。您之前所做的任何配置信息都将丢失。
- 通过基于 web 的设备管理器恢复出厂配置。

注 意 在恢复出厂设置过程中，请不要断开设备电源，拔出连接的以太网电缆，或以其它任何方式打断或干扰恢复出厂设置过程。恢复出厂设置需要一些时间。当路由器电源指示灯长亮时，说明路由器已重启完毕并恢复到出厂设置。

通过基于 web 的设备管理器恢复路由器的出厂设置的步骤：

步骤 **1** 选择 “ 系统管理 ” > “ 恢复出厂配置 ” 菜单。打开 “ 恢复出厂配置 ” 页面。

步骤 **2** 单击 “ 恢复出厂配置 ”。

步骤 **3** 单击 “**OK**”。

此操作将会恢复路由器的出厂配置。您之前所作的配置信息将被清除。恢复出厂设置后，路由器将自动重启。

配置维护

“ 配置维护 ” 页面可备份当前的系统配置，从保存的配置文件中恢复系统配置，或者向上级管理平台上传系统配置文件。

维护系统配置的步骤：

步骤 **1** 选择 “ 系统管理 ” > “ 配置维护 ” 菜单。打开 “ 配置维护 ” 页面。

步骤 **2** 如需将当前系统配置导出为一个配置文件作为备份，单击 “ 导出配置文件 ”。选择配置文件的保存路径，然后单击 “ 保存 ”。

步骤 **3** 您也可以导入一个配置文件，将当前的系统配置恢复到该配置文件所保存的配置信息。单击 “ 浏览 ”，选择一个配置文件然后单击 “ 导入 ”。路由器将会自动重启，并恢复到配置文件中所保存的配置信息。

步骤 4 路由器支持向上级管理平台上传系统配置文件。单击“上传配置文件”，路由器将会向上级管理平台发送上传系统配置文件的请求。管理平台收到该请求之后将自动获取路由器当前的系统配置文件。

注 此功能只支持上传系统配置文件到 TR-069 服务器。在上传系统配置文件之前，请先设置 TR-069 服务器的相关参数。详细信息请参考“**TR-069 配置**”一节的说明。

软件升级

“软件升级”页面可查看系统当前使用的固件版本和作为备份的固件版本，从指定的网站上下载最新的固件版本，以及升级系统固件版本。

注 意 在固件升级过程中，请不要断开设备电源，拔出连接的以太网电缆，或以其它任何方式打断或干扰固件升级过程。否则将造成固件升级失败，并无法正常启动设备。固件升级过程可能需要几分钟的时间。

升级系统的固件版本的步骤：

步骤 1 选择“系统管理”>“软件升级”菜单。打开“软件升级”页面。

此页面显示以下字段：

- 设备型号 — 显示设备型号。
- **PID VID—** 显示产品型号与版本号。
- 当前固件版本 — 显示系统当前使用的固件版本（主用固件版本）。
- 备份固件版本 — 显示系统的备份固件版本。

步骤 2 在“下载最新固件”栏，单击“下载”可从指定的网站上下载最新版本的固件。此功能要求路由器当前接入到互联网。

步骤 3 在“请选择升级的固件文件”栏，单击“浏览”，选择已下载的固件文件。

步骤 4 单击“升级”，开始升级系统固件版本。

当您升级系统固件时，新的固件版本将替换系统默认的备份固件版本并自动重启。固件升级成功后，新的固件版本将作为主用固件版本为系统所使用，而之前使用的主用固件版本此时将成为备份固件版本。

故障诊断工具

“ 故障诊断 ” 模块提供多个系统诊断工具，帮助您解决网络问题。

Ping

使用 Ping 工具可测试路由器与网络上其它设备的连通性。在测试设备与互联网的连通性时，您需要 ping 一个完整有效的域名地址或 IP 地址，例如 www.cisco.com。

步骤 1 选择 “ 系统管理 ” > “ 故障诊断工具 ”>“**Ping**” 菜单。打开 “Ping” 页面。

步骤 2 输入目的 IP 地址或者主机名称，单击 “ 开始 ”。

在 “ 概要信息 ” 栏可查看诊断结果。

Traceroute

使用 Traceroute 工具能够显示从路由器到目标 IP 地址之间的所有路由信息。

步骤 1 选择 “ 系统管理 ” > “ 故障诊断工具 ”>“**Traceroute**” 菜单。打开 “Traceroute” 页面。

步骤 2 输入路由追踪的目的 IP 地址或者主机名称。

步骤 3 单击 “ 开始 ” 开始追踪路由路经。单击 “ 停止 ” 停止路由追踪。

在 “ 结果 ” 栏可查看路由追踪的结果。

HTTP Get

使用 HTTP Get 工具可获取指定站点的相关信息。

步骤 1 选择 “ 系统管理 ” > “ 故障诊断工具 ”>“**HTTP Get**” 菜单。打开 “HTTP Get” 页面。

步骤 2 输入目的 URL 地址。

步骤 3 单击 “ 开始 ”。

在 “ 概要信息 ” 栏可查看获取的站点信息。

DNS Query

使用 DNS Query 工具可查询 Internet 上终端 （如 Web 服务器、 FTP 服务器或者邮件服务器）的 IP 地址。

步骤 1 选择 “ 系统管理 ” > “ 故障诊断工具 ” > “**DNS Query**” 菜单。打开 “DNS Query” 页面。

步骤 2 输入需要查询 DNS 的域名。

步骤 3 单击 “ 开始 ”，开始查询 DNS。

在 “ 概要信息 ” 栏可查看 DNS 查询的结果。

系统时间设置

“ 时间配置 ” 页面可设置系统时间和日期等信息。配置完成之后， 系统可从指定的 NTP 服务器自动取得时间信息或者使用您手动设置的时间信息。

设置系统时间的步骤：

步骤 1 选择 “ 系统管理 ” > “ 时间配置 ” 菜单。打开 “ 时间配置 ” 页面。

“ 当前系统时间 ” 栏显示系统当前的日期和时间信息。

步骤 2 如需手动设置系统的时间和日期，选择 “ 手动设置 ” 并分别在 “ 日期 ” 和 “ 时间 ” 栏设定对应的值。

步骤 3 如需自动设置系统的时间和日期，选择 “ 自动同步 ” 并设定以下参数：

- **NTP** 服务器 **1**— 输入主用 NTP 服务器的 IP 地址或域名。
- **NTP** 服务器 **2**— 输入备用 NTP 服务器的 IP 地址或域名。

路由器将与指定的 NTP 服务器进行时间同步，并更新系统的时间和日期设置。

步骤 **4** 单击 “ 确定 ”。

TR-069 配置

TR-069 全称为 CPE 广域网管理协议，它提供了对下一代网络中家庭网络设备进行管理配置的通用框架和协议，用于从网络侧对家庭网络中的网关、路由器、机顶盒等设备进行远程集中管理。

“TR-069 配置 ” 页面可启用或禁用 TR-069 服务器功能，并设置 TR-069 服务器的相关参数。

设置 TR-069 服务器的步骤：

步骤 **1** 选择 “ 系统管理 ” > “**TR-069** 配置 ” 菜单。打开 “TR-069 配置 ” 页面。

步骤 **2** 在 **“TR-069** 配置 **”** 栏，启用或禁用 TR-069 服务器功能。

步骤 **3** 如您启用 TR-069 服务器，在 “**ACS**” 栏设置 ACS 远程管理服务器的相关信息：

- **URL**— 输入 ACS 远程管理服务器的 URL。
- 用户名 — 输入登录 ACS 远程管理服务器的用户名。
- 密码 — 输入登录 ACS 远程管理服务器的密码。

步骤 **4** 在 “**CPE**” 栏，设置 TR-069 远程管理 CPE 端的信息：

- 用户名 — 输入远程管理服务器的用户名，向 CPE 做出连接要求。
- 密码 — 输入远程管理服务器的密码，向 CPE 做出连接要求。
- 发送 **Inform** 报文 — （可选）启用或禁用发送 Inform 报文功能。
- 发送周期 — 如启用发送 Inform 报文功能，输入发送报文的周期。默认为 43200 秒。
- 请求连接端口 — 输入 TR-069 请求连接端口的端口号。
- 请求下载 — （可选）选择下载请求的类型并单击 “ 发送 ” 发送相应的请求。

- 固件文件 — 向 TR-069 远程服务器发起下载系统固件文件的请求。
- Vendor 配置 — 向 TR-069 远程服务器发起下载配置文件的请求。

- 请求上传 — （可选）选择请求上传类型并单击 “ 发送 ” 发送相应的请求。
  - 配置文件 — 向 TR-069 远程服务器发起上传系统当前配置文件的请求。
  - Vendor 配置 — 向 TR-069 远程服务器发起上传出厂默认配置文件的请求。
- 配置文件格式 — （可选）选择从 TR-069 远程服务器下载的配置文件的格式。
  - 未压缩 — 配置文件格式为未压缩的文件格式。
  - 压缩 — 配置文件格式为压缩文件格式。
- 请求变更账号 — 单击 “ 发送 ”，向 TR-069 远程服务器发起变更管理密码请求。

步骤 **5** 单击 “ 确定 ”。

SNMP 配置

SNMP 是一种流行的网络监控和管理协议。它使网络管理员能够对路由器的状态进行监控，并在路由器发生任何重大事件时收到通知。

设置 SNMP 服务的步骤：

步骤 **1** 选择 “ 系统管理 ” > “**SNMP**” 菜单。打开 “SNMP” 页面。

步骤 **2** 在 **“SNMP”** 栏，选择启用或禁用 SNMP 远程管理功能。

步骤 **3** 如启用 SNMP 功能，设定以下参数：

- **SNMP** 版本 —（可选）选择 SNMP v1 & v2 或 SNMPv3。如果不需要 SNMP v3 的增强能力或者您的管理软件不支持 SNMP v3，请选择 SNMP v1&v2 ；反之则选择 SNMP v3。
- 联系信息 — 设定路由器的联系人信息。
- 系统名称 — 输入路由器的系统名称。
- 设备位置 — 输入路由器的位置信息。
- 安全用户名 — （仅对于 SNMPv3）输入创建访问和管理 SNMP MIB 对象的管理员账户。

- 认证密码 — （仅对于 SNMPv3）输入管理员账号的认证密码。
- 认证方式 — （可选）选择 HMAC-MD5 或 HMAC-SHA 作为认证方式。
- 加密密码 —（仅对于 SNMPv3）输入管理员管理通信时进行数据加密的专用密码。
- 加密方式 — （可选）选择 None （不加密）或 CBC-DES 加密。
- **SNMP** 只读口令 — 输入 SNMP 只读口令，缺省为 public。
- **SNMP** 读写口令 — 输入 SNMP 读写口令，缺省为 private。
- **Trap** 口令 — 输入 SNMP 只读口令，缺省为 public。
- **SNMP** 信任主机 — 输入 SNMP 信任主机 IP 地址。
- **Trap** 接收主机 — 输入 Trap 接收主机 IP 地址。

步骤 **4** 单击 “ 确定 ”。

远程管理

用户可通过 HTTP、 HTTPS 或 SSH 协议从本地或远程主机安全地访问路由器。

远程访问协议和端口配置

“ 远程访问协议和端口 ” 页面可设置远程访问路由器的协议类型和相应的端口号。

设置远程访问协议和端口的步骤：

步骤 **1** 选择 “ 系统管理 ” > “ 远程管理 ” > “ 远程访问协议和端口 ” 菜单。打开 “ 远程访问协议和端口 ” 页面。

步骤 **2** 设定以下参数：

- **HTTP** 服务 — 启用或禁用 HTTP 远程访问功能。
- 端口号 — 设置 HTTP 远程访问的端口号。缺省为 80。
- **HTTPS** 服务 — 启用或禁用 HTTPS 远程访问功能。
- 端口号 — 设置 HTTPS 远程访问的端口号。缺省为 443。

步骤 3 单击 “ 确定 ”。

远程访问信任主机设置

“ 远程信任主机 ” 页面可设定允许远程访问路由器的主机。只有受信任的主机才能从 WAN 侧访问指定的服务。

设置远程访问信任主机的步骤：

步骤 1 选择 “ 系统管理 ” > “ 远程管理 ” > “ 远程信任主机 ” 菜单。打开 “ 远程信任主机 ” 页面。

步骤 2 选择 “ 任意 **IP** 地址 ”，允许任意一台主机远程访问路由器。

步骤 3 选择 “ 特定 **IP** 地址 ”，允许特定的主机远程访问路由器。输入远程访问信任主机的 IP 地址，然后单击 “ 确定 ”。

SSH 远程访问设置

SSH 协议允许网络设备之间建议一条安全的远程访问连接。 “SSH” 页面可启用路由器的 SSH 远程访问功能并设置相关参数，使得远程用户通过 SSH 协议远程访问路由器，进行系统故障诊断。

设置 SSH 远程访问的步骤：

步骤 1 选择 “ 系统管理 ” > “ 远程管理 ” > “**SSH**” 菜单。打开 “SSH” 页面。

步骤 2 在 “ 启用 **SSH**” 栏，选择启用或禁用路由器的 SSH 远程访问功能。

步骤 3 如启用 SSH 远程访问功能，设定以下参数：

- 端口号 — 输入远程 SSH 客户端连接到路由器的端口号。
- 远程支持密码 — 输入 SSH 客户端远程访问路由器的密码。通常，此密码由系统管理员通过特定的 SSH 密码生成工具手动生成，有效期为 1 个小时。当密码过期后，系统管理员需重新生成一个密码并在此页面重新设置。
- 显示密钥 — 勾选以明文形式显示远程支持密码。

步骤 4 单击 “ 确定 ”。

步骤 5 单击 “ 收集设备状态信息 ”，开始自动收集路由器的配置信息和其他重要的路由信息。路由器的配置信息和相关路由信息将被压缩成一个 zip 文件包，单击此按钮可将此 zip 文件包保存到本地，以便进行系统故障诊断。

系统日志管理

路由器可记录系统事件和防火墙安全事件，以便跟踪潜在的安全隐患。用户可以选择将日志信息保存在本地、 USB 存储设备或远程日志服务器。此外，用户还可以选择将严重级别较高的系统日志通过邮件定期发送给指定的管理人员。

设置系统日志基本参数

“ 日志设置 ” 页面可设置系统日志的基本参数，包括本地日志缓存大小、保存到 USB 存储设备的日志文件名称和文件大小、远程系统日志服务器和日志邮件通知等。

设置系统日志基本参数的步骤：

步骤 1 选择 “ 系统管理 ”>“ 系统日志 ”>“ 日志设置 ” 菜单。打开 “ 日志设置 ” 页面。

步骤 2 如需将系统日志保存到本地缓存，在 “ 日志缓存大小 ” 栏输入本地日志的缓存大小。

步骤 3 如需将系统日志保存到 USB 存储设备上，在 “**USB**” 栏设定以下参数：

- 日志文件名 — 输入保存到 USB 存储设备上的日志文件名称。
- 日志文件大小 — 输入保存到 USB 存储设备上的日志文件的大小。

注 此功能要求用户首先将 USB 存储设备插入到路由器后面板 USB 接口。如未插入或未检测到 USB 存储设备，此处将显示一条告警信息 “USB 设备未插入或未检测到 ”。

步骤 4 如需将系统日志保存到指定的远程系统日志服务器，在 “**Syslog** 服务器 ” 栏设定以下参数：

- **IP** 地址 — 输入远程系统日志服务器的 IP 地址。
- 端口号 — 输入远程系统日志服务器的端口号。

步骤 5 如需将系统日志通过邮件定期发送到指定的邮件接收人，在 “ 电子邮件通知 ” 栏设定以下参数：

- 寄件人 — 输入发送日志邮件的邮箱地址。

- 收件人 — 输入接收日志邮件的邮箱地址。
- **SMTP** 服务器 — 输入 SMTP 服务器的 IP 地址。
- **SMTP** 端口号 — 输入 SMTP 服务器的端口号。
- 邮件主题 — 输入日志邮件的标题。
- 日志数量 — 输入通过邮件一次可发送的日志消息数量。
- 发送邮件间隔 — 输入发送日志邮件通知的时间间隔。
- 用户名 — 输入访问 SMTP 服务器的用户名。
- 密码 — 输入访问 SMTP 服务器的密码。

步骤 **6** 单击 “ 确定 ”。

设置日志类型

“ 日志模块 ” 页面可启用或禁用系统日志功能，选择要记录日志的事件类型、事件严重级别和存储方式。

设置日志类型的步骤：

步骤 **1** 选择 “ 系统管理 ”>“ 系统日志 ”>“ 日志模块 ”。打开 “ 日志模块 ” 页面。

步骤 **2** 在 “ 日志服务状态 ” 栏，选择启用或禁用系统日志功能。

步骤 **3** 如启用系统日志功能，勾选需要记录日志的事件类型。路由器支持记录与 Kernel 和 System 操作相关的事件。

步骤 **4** 在 “ 严重级别 ” 下拉框内，选择要记录日志的事件严重级别。下面按照从高到低的顺序列出了事件的严重级别：

- **Emergency** （紧急，严重级别最高） — 系统无法使用。
- **Alert** （警报） — 需要立即执行操作。
- **Critical** （严重） — 系统处于高危状态。
- **Error** （错误） — 系统出错。
- **Warning** （警告） — 系统发出警告。
- **Notice** （通知） — 系统功能正常工作，但发出了系统通知。
- **Information** （信息） — 设备信息。

- **Debug**（调试，严重级别最高） — 调试信息。

选择记录日志的事件严重级别后，此级别以上的所有事件都会自动存储在日志中，而此级别以下的事件则不会存储在日志中。例如，如果您选择了 “Warning”，则会将严重级别为警告及更高级别 （即严重级别为紧急、警报、严重、错误和警告）的所有事件存储在日志中，而严重级别低于警告 （即严重级别为通知、报告和调试）的事件则不会保存。

步骤 **5** 设定不同类型的系统日志的存储位置，其中：

- 本地 — 勾选此选项，系统日志保存到本地缓存。
- **USB**— 勾选此选项，系统日志保存到插入到路由器 USB 接口的 USB 存储设备。此功能要求用户首先将 USB 存储设备插入到路由器后面板的 USB 接口，并在 “ 日志设置 ” 页面的 “USB” 栏定义好相关参数。
- 电子邮件通知 — 勾选此选项，系统日志通过邮件定期发送给指定的邮件接收者。此功能要求用户首先在 “ 日志设置 ” 页面的 “ 电子邮件通知 ” 栏定义好相关参数。
- **Syslog** 服务器 — 勾选此选项，系统日志保存到指定的远程日志服务器。此功能要求用户首先在 “ 日志设置 ” 页面的 “Syslog 服务器 ” 栏定义好相关参数。

步骤 **6** 单击 “ 确定 ”。

查看系统日志

“ 查看日志 ” 页面可查看所有系统日志的详细信息，或根据特定的条件筛选要查看的系统日志。

查看系统日志的步骤：

步骤 **1** 选择 “ 系统管理 ”>“ 系统日志 ”>“ 查看日志 ”。打开 “ 查看日志 ” 页面。

步骤 **2** 如需筛选要查看的系统日志，设定以下参数：

- 服务类型 — 从下拉框中选择要查看的事件类型。
- 按关键字过滤 — 输入要筛选的系统日志的关键字。比如，您可以输入 VPN 查看所有与 VPN 有关的日志信息 。路由器仅支持用户筛选与 WAN、 VPN、Firewall 和 TR-069 事件相关的日志信息。

步骤 **3** 单击 “ 过滤器 ”，所有符合过滤条件的系统日志将显示在本页面。

步骤 **4** 单击 “ 下载所有日志 ”，下载本地保存的所有系统日志到指定的路径。

步骤 5 单击 “ 清除日志 ”，清除本地保存的所有系统日志。

设置防火墙日志

“ 防火墙日志 ” 页面可启用或禁用防火墙日志功能，以及设置需要记入日志的防火墙事件的严重级别和类型。

设置防火墙日志功能的步骤：

步骤 1 选择 “ 系统管理 ”>“ 系统日志 ”>“ 防火墙日志 ”。打开 “ 防火墙日志 ” 页面。

步骤 2 在 “ 防火墙日志 ” 栏，选择启用或禁用防火墙日志功能。

步骤 3 如启用防火墙日志功能，设定以下参数：

- 严重级别 — 选择需要记录日志的防火墙事件的严重级别。
- 日志类别 — 勾选要记录日志的防火墙事件的类型（如 SPI 和 DoS 攻击），然后输入每条日志信息可包含多少条相应类型的事件数量。

步骤 4 单击 “ 确定 ”。

A

快速索引

思科为您提供了丰富完整的文档资料，帮助您和您的客户获取关于思科无线 VPN 路由器的完整信息。

资源	地址
产品主页	www.cisco.com/go/cn/cvr328w
客户支持中心	www.cisco.com/web/CN/smallbusiness
产品渠道合作伙伴中心	www.cisco.com/web/CN/partners/smb_kr/index.html
软件下载	www.cisco.com/web/CN/solutions/industry/segment_sol/small/index.html#small_down
开放源许可通知	www.cisco.com/web/CN/solutions/industry/segment_sol/small/products/routers/cvr328w.html#~Resources
产品兼容性和安全信息	www.cisco.com/web/CN/solutions/industry/segment_sol/small/products/routers/cvr328w.html#~Resources
产品保修条款	www.cisco.com/web/CN/solutions/industry/segment_sol/small/index.html#~service
产品服务热线	8008888168（固定电话） 4006282616（移动电话）