InHand IR900 系列工业级路由器

用户手册

北京映翰通网络技术股份有限公司

http://www.inhand.com.cn

资料版本：V2.9---20170104

Copyright © 2012-2017 北京映翰通网络技术股份有限公司及其许可者版权所有，保留一切权利。未经本公司书面许可，任何单位和个人不得擅自摘抄、复制本书内容的部分或全部，并不得以任何形式传播。



、Inhand、INHAND、映翰通均为北京映翰通网络技术股份有限公司的商标。对于本手册中出现的其它公司的商标、产品标识及商品名称，由各自权利人拥有。

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

前言

欢迎使用 InHand IR900 系列工业级路由器产品。<< InHand IR900 系列工业级路由器用户手册>>将详细的指导您如何配置路由器。

读者对象

本手册主要适用于如下工程人员：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和网络管理人员

本手册约定

1 图形界面格式约定

格 式	意 义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
“”	带双引号“”表示窗口名、菜单名，如：弹出“新建用户”窗口。
>>	多级菜单用“>>”隔开。如“文件>>新建>>文件夹”多级菜单表示“文件”菜单下的“新建”子菜单下的“文件夹”菜单项。

2 各类标志

本手册采用醒目标志表示在操作过程中应该特别注意的地方，这些标志的意义如下：



注意

提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。



说明

对操作内容的描述进行必要的补充和说明。

技术支持联络信息

北京映翰通网络技术股份有限公司（总部）

地址：北京市朝阳区望京科技园启明国际大厦 11 层西侧

电话：（8610）6439 1099　　传真：（8610）8417 0089

网址：www.inhand.com.cn

上海办事处

电话： 021-5480 8501

地址：上海市普陀区顺义路18号1103室

广州办事处

电话：020-8562 9571

地址：广州市天河区棠东东路5号远洋新三板创意园B-130单元

成都办事处

电话：028-8679 8244

地址：四川省成都市高新区府城大道西段399号，天府新谷6栋13层06~08室

武汉办事处

电话：027-87163566

地址：湖北省武汉市洪山区珞瑜东路2号巴黎豪庭11栋2001室

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：niexy@inhand.com.cn

感谢您的反馈，让我们做得更好！

目录

一、设备简介.....7
1.1 概述.....7
1.2 包装清单.....8
1.3 面板介绍.....9
1.4 状态指示灯说明.....10
二、设备安装.....12
2.1 导轨式安装与拆卸.....12
2.1.1 导轨式安装.....12
2.1.2 导轨式拆卸.....13
2.2 壁挂式安装与拆卸.....14
2.2.1 壁挂式安装.....14
2.2.2 壁挂式拆卸.....14
2.3 SIM 卡和天线的安装.....15
2.4 电源和保护地接地的安装.....16
2.5 端子连接（仅用于带有工业接口的设备）.....17
2.6 访问设备.....18
三、基本配置.....19
3.1 管理.....19
3.1.1 系统.....19
3.1.2 系统时间.....19
3.1.3 管理访问.....20
3.1.4 AAA.....21
3.1.5 配置管理.....24
3.1.6 设备远程监控平台.....25
3.1.7 GPS 定位信息.....26
3.1.8 SNMP.....28
3.1.9 Python.....31
3.1.10 告警.....31
3.1.11 系统日志.....32
3.1.12 时间表管理.....33
3.1.13 系统升级.....33
3.1.14 重启系统.....33
3.2 二层交换.....34
3.3 网络.....35
3.3.1 以太网接口.....35
3.3.2 VLAN 接口.....36
3.3.3 拨号接口.....37
3.3.4 ADSL 拨号（PPPoE）.....41
3.3.5 WLAN 接口.....41
3.3.6 环回接口.....45
3.3.7 DHCP 服务.....45
3.3.8 DNS 服务.....47
3.3.9 动态域名.....48

3.3.10 短信服务.....49
3.4 链路备份.....51
3.4.1 SLA.....51
3.4.2 Track 模块.....52
3.4.3 VRRP.....53
3.4.4 接口备份.....54
3.5 路由.....55
3.5.1 静态路由.....55
3.5.2 动态路由.....55
3.5.3 组播路由.....62
3.6 防火墙.....64
3.6.1 访问控制（ACL）.....64
3.6.2 网络地址转换（NAT）.....65
3.6.3 MAC-IP 绑定.....66
3.7 QoS.....67
3.8 VPN.....69
3.8.1 IPSec.....69
3.8.2 GRE.....75
3.8.3 L2TP.....77
3.8.4 OPENVPN.....79
3.8.5 证书管理.....81
3.9 工业接口.....84
3.9.1 DTU.....84
3.9.1.1 串口设置.....84
3.9.1.2 DTU1.....85
3.9.2 IO 接口.....86
3.9.3 Modbus.....87
3.10 工具.....88
3.10.1 PING 探测.....88
3.10.2 路由探测.....88
3.10.3 网络抓包.....88
3.10.4 网速测试.....89
3.11 安装向导.....90
3.11.1 新建 LAN.....90
3.11.2 新建 WAN.....90
3.11.3 新建拨号.....91
3.11.4 新建 IPSec 隧道.....91
3.11.5 新建端口映射.....92
四、典型应用配置.....93
4.1 DDNS 应用举例.....93
4.2 网管平台应用举例.....95
4.3 恢复出厂设置.....96
4.3.1 网页方式.....96
4.3.2 硬件方式.....96

4.4 导入/导出配置 97
4.5 日志与诊断记录 98
4.6 上网方式 99
4.6.1 拨号上网 99
4.6.2 有线上网 99
4.7 新建 LAN 102
4.8 VRRP 典型配置举例 103
4.9 接口备份应用举例 106
4.10 静态路由应用举例 110
4.11 动态路由应用举例 112
4.12 组播路由应用举例 115
4.13 访问控制应用举例 117
4.14 网络地址转换应用举例 119
4.15 QoS 应用举例 120
4.16 DTU 应用举例 121
4.17 一对一 IPSec VPN 配置举例 124
4.18 DMVPN 组网配置举例 127
4.19 OPENVPN 应用举例 132
附录 命令行指令说明 134

正文

一、设备简介

1.1 概述

IR900 系列路由器是映翰通公司面向工业领域推出的新一代 4G 无线 VPN 路由器。

该设备凭借 4G 无线网络和多种宽带服务，提供随处可得的不间断的互联网接入，以其全面的安全性和无线服务等特性，实现多达万级的设备联网，为真正意义上的设备信息化提供数据的高速通路。IR900 路由器具有快速部署和易于管理的优点，先进的软件功能与全工业化的硬件设计平台，使企业能够在最小的投资范围内快速建设规模化的工业设备网络，提供包括数据，语音和视频在内的多业务服务。

IR900 系列路由器包含 IR9x2、IR9x5、IR9x8 三个系列，最多集成了 8 个智能端口，支持 LAN/WAN 协议，这不仅让客户有更多广域网端口接入的选择，更省去了额外的交换设备采购成本。

随着工业的发展，更多业务通过无线网络流向总部数据中心集中，将 IR900 路由器作为工业现场接入设备，可以通过远端工业现场与总部数据中心的 VPN 网关建立加密性能很高的虚拟隧道，节省昂贵的专线租用投入，数据经 IR900 安全隧道传送，可以充分保证业务信息安全、高速、可靠传输，组网示意图如图 1-1 所示。

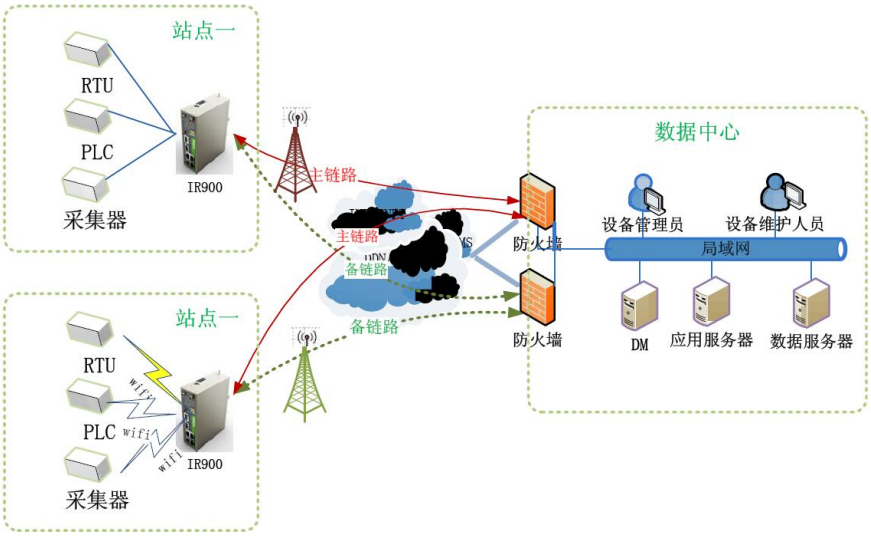


图 1-1

1.2 包装清单

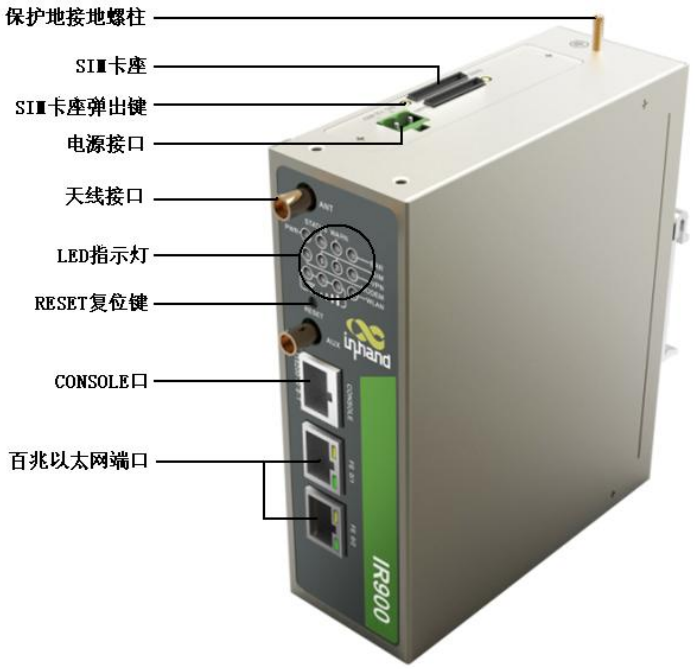
标准配件

配件	数量	描述
IR900	1 台	IR900 系列工业级 4G 路由器
产品资料	1 套	光盘和纸质快速安装手册
导轨安装配件	1 个	固定路由器
电源端子	1 个	2 针绿色电源端子
网线	1 根	1.5m 网线
天线	1 根	3G/4G 天线
产品保修卡	1 张	保修期为 1 年
合格证	1 张	IR900 系列工业级 4G 路由器合格证

可选配件

配件	数量	描述
AC 电源线	1 根	中标 AC 线
电源适配器	1 个	12VDC 电源适配器
天线	1 根	wifi 天线
串口线	1 根	思科线序串口线

1.3 面板介绍



注意

IR900 系列产品有多种面板外观，但是安装方法都是一样的，具体面板情况请以实物为准。

1.4 状态指示灯说明

运行状态指示灯说明：

POWER 电源指示灯 （红色）	STATUS 状态指示灯 （绿色）	WARN 警报指示灯 （黄色）	ERROR 错误指示灯 （红色）	说明
亮	亮	亮	灭	开机状态
亮	闪	亮	灭	开机成功
亮	闪	闪	灭	正在拨号
亮	闪	灭	灭	拨号成功
亮	闪	亮	闪	复位成功



两个 SIM 卡指示灯，在“开机状态”和“开机成功”时都是 SIM 卡 1 指示灯亮，后面情况是使用的 SIM 卡对应指示灯亮，图是以使用 SIM 卡 1 为例说明的。

信号状态指示灯及说明：

信号状态绿色指示灯 1	信号状态绿色指示灯 2	信号状态绿色指示灯 3	说明
灭	灭	灭	未检测到信号
亮	灭	灭	信号状况 1-9asu（说明信号状况有问题，请检查天线是否安装完好，SIM 卡是否正确识别，以及该地区信号状况是否良好）
亮	亮	灭	信号状况 10-19asu（说明信号状态基本正常，设备可以正常使用）
亮	亮	亮	信号状况 20-31asu（说明信号状态良好）

以太网口状态指示灯及说明

指示灯	说明
绿灯长亮	该网口为 100M，处于正常状态
绿灯长灭	该网口为 10M 或没有连接
黄灯闪烁	有数据传输
黄灯长亮	无数据传输

MODEM 指示灯及说明

MODEM 绿色指示灯	说明
亮	已经拨上号
闪	没有拨上号

WLAN 指示灯及说明

WLAN 绿色指示灯	说明
亮	WLAN 功能开启
灭	WLAN 功能关闭

二、设备安装

安装注意事项：

- 电源要求：24VDC(12～48VDC) ，请注意电源电压等级；额定电流是 0.15～0.6A。
- 环境要求：工作温度-25℃～70℃，存储温度-40℃～85℃，相对湿度 5％～95%（无凝露）。设备表面可能高温，安装时需要考虑周边环境，应安装在受限制的区域。
- 避免阳光直射，远离发热源或有强烈电磁干扰区域。
- 路由器产品需安装在工业导轨上。
- 检查是否有安装所需的电缆和接头。

2.1 导轨式安装与拆卸

2.1.1 导轨式安装

具体步骤如下：

第一步：选定设备的安装位置，确保有足够的空间。

第二步：将 DIN 卡轨座的上部卡在 DIN 轨上，在设备的下端向上稍微用力按箭头 2 所示转动设备，即可将 DIN 卡轨座卡在 DIN 轨上，确认设备可靠地安装到 DIN 轨上如图 2-1-1 中右图所示。

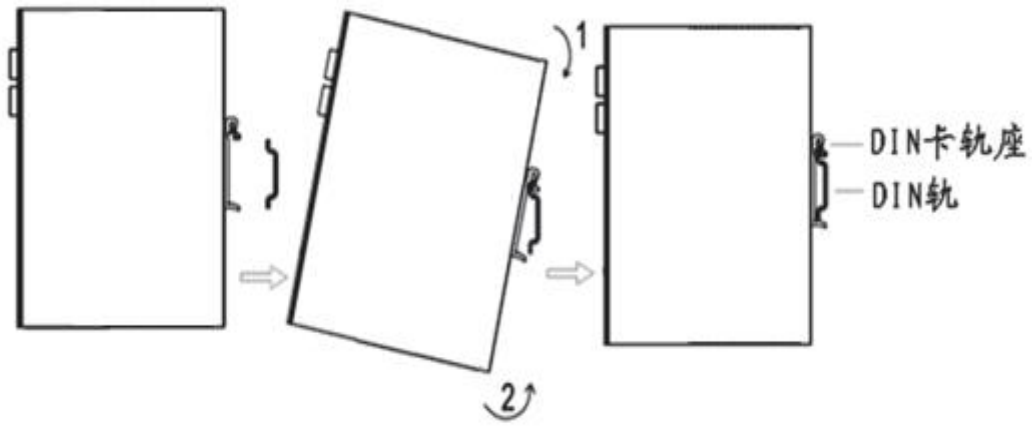


图 2-1-1

2.1.2 导轨式拆卸

具体步骤如下：

第一步：如图 2-1-2 箭头 1 所示，向下压设备使设备下端有空隙脱离 DIN 轨。

第二步：将设备按箭头 2 的方向转动，并同时向外移动设备的下端，待下端脱离 DIN 轨后向上抬设备，即可从 DIN 轨上取下设备。

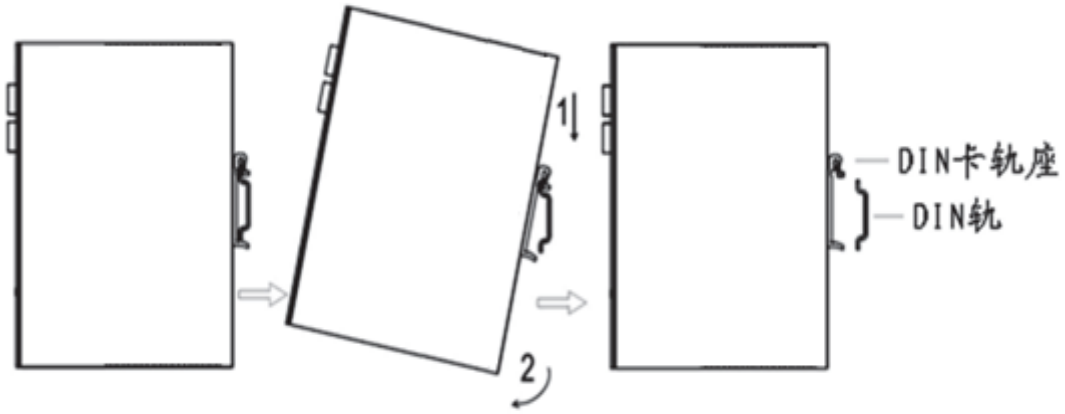


图 2-1-2

2.2 壁挂式安装与拆卸

2.2.1 壁挂式安装

具体步骤如下：

第一步：选定设备的安装位置，确保有足够的空间。

第二步：用螺丝刀把壁挂安装板安装在设备的后面，如图 2-2-1 所示。

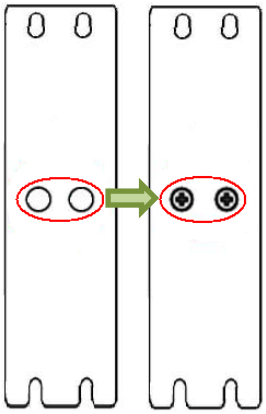


图 2-2-1

第三步：取出螺钉（与壁挂安装板配套包装），用螺丝刀将螺钉固定在安装位置上，然后下拉设备使设备处于稳定状态，如图 2-2-2 所示。



图 2-2-2

2.2.2 壁挂式拆卸

具体步骤如下：

用手扶住设备，另一只手卸掉设备上端起固定作用的螺钉，即可把设备从安装位置拆掉。

2.3 SIM 卡和天线的安装

IR900 支持双卡，按住 SIM 卡座弹出键会弹出对应卡座，装入 SIM 卡即可。

用手轻轻转动金属 SMA-J 接口可活动部分到不能转动（此时看不到天线连接线外螺纹）即可，不要握住黑色胶套用力拧天线。



说明

- IR900支持双天线，分别是ANT天线和AUX天线。其中ANT天线是收发数据的天线，AUX天线只能增强天线信号强度，不能进行数据的收发，因此不能单独使用。
- 一般情况下只使用ANT天线即可，当信号不好需要增强信号时才在使用ANT天线的同时使用AUX天线。

2.4 电源和保护地接地的安装

电源安装具体步骤如下：

第一步：将端子从路由器上取下，将端子上的锁紧螺钉旋松；

第二步：将电源线缆插入端子后将螺钉锁紧。

保护地接地具体步骤如下：

第一步：将接地螺帽拧下来；

第二步：将机柜地线的接地环套进接地螺柱上，将接地螺帽拧紧。



注意

为提高路由器的整机抗干扰能力，路由器在使用时必须接地，根据使用环境将地线接到路由器接地螺柱上。

2.5 端子连接（仅用于带有工业接口的设备）

串口和 IO 接口接入方式为端子接入，在使用前需要将对应的线接到端子上。

设备串口提供 RS232/RS485 两种接口模式。IO 接口输入端：IN 表示数字量输入端；COM 表示接地端。IO 接口输出端：RELAY 表示继电器输出端。

安装时将端子从设备上取下，将端子上的锁紧螺钉旋松，将对应线缆插入端子后将螺钉锁紧。各个线排序如图 2-5-1 所示。

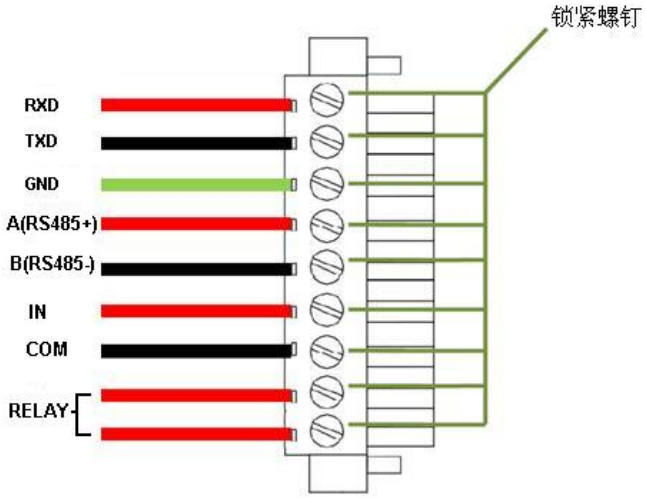


图 2-5-1

2.6 访问设备

首先要修改管理 PC 的 IP 地址使其和设备属于同一网段，可以设置管理 PC 自动获取 IP 或者设置静态 IP。设置好管理 PC 的 IP 地址并确保 WEB 没有设置代理服务器后即可通过 Web 页面登录设备

一、自动获取 IP 地址（推荐使用）

请将管理 PC 设置成“自动获得 IP 地址”和“自动获得 DNS 服务器地址”（计算机系统的缺省配置），由设备自动为管理 PC 分配 IP 地址。

二、设置静态 IP 地址

请将管理 PC 的 IP 地址（例如设置为：192.168.2.2）与设备的 FE 口 IP 地址设置在同一网段内（设备 FE 口初始 IP 地址为：192.168.2.1，子网掩码均为 255.255.255.0）。

三、取消代理服务器

如果当前管理 PC 使用代理服务器访问因特网，则必须取消代理服务。在浏览器窗口中，选择“工具>>Internet 选项”， 选择“连接”页签，单击<局域网设置>按钮，进入“局域网（LAN）设置”窗口界面。请确认未选中“为 LAN 使用代理服务器”选项；若已选中，请取消并单击<确定>。

四、登录/退出 Web 设置页面

运行 Web 浏览器，在地址栏中输入“http://192.168.2.1”，“用户名/密码”默认为：adm/123456。单击 Web 界面右上角的“退出”，确认后即可退出 Web 设置页面。


说明

- 同一时间，路由器最多允许四个用户通过Web 设置页面进行管理。当对路由器进行多用户管理时，建议不要同时对其进行配置操作，否则可能会导致数据配置不一致。
- 为了安全起见，建议您首次登录后修改缺省的登录密码，并保管好密码信息。

三、基本配置

3.1 管理

管理包含了系统、系统时间、管理访问、AAA、配置管理、SNMP、Python、告警、系统日志、时间表管理、系统升级、重启系统、网管平台和 GPS 定位信息共 14 个功能模块。

3.1.1 系统

在这里，可以查看系统状态和网络状态（包含设备固件版本、MAC 地址、路由器时间和设备启动时间等），设置路由器 WEB 配置界面的语言；自定义路由器主机名称。在网络状态部分点击 Cellular1、Fastethernet 0/1、Fastethernet 0/2、VLAN1 或 bridge 1 后的“设置”可直接进入其配置页面。

3.1.2 系统时间

为了保证本设备与其它设备协调工作，用户需要将系统时间配置准确。在这里，可以手动设置路由器和相连主机时间同步，可以手动设置系统时间为 2000 年以后的任意期望值、可以设置任意时区。还可以使用 SNTP、NTP，其目的是对网络内所有具有时钟的设备进行时钟同步，使网络内所有设备的时钟保持一致，从而使设备能够提供基于统一时间的多种应用。

表 3-1-1 SNTP 客户端参数说明

参数名称	说明	缺省值
启用	开启/关闭 SNTP 客户端	关闭
更新时间间隔	设备开启后按照设定的时间间隔去同步时间。如设置 60 秒。即设备每隔 60 秒钟去同步一次时间。	3600
源接口	指设备发出 SNTP 报文的接口。	无
源地址	指设备发出 SNTP 报文携带的源地址。	无
SNTP 服务器列表		
服务器地址	SNTP 服务器地址（域名/IP），最多可填写 10 个服务器	无
端口	SNTP 服务器的 SNTP 服务端口	123

注意

- 设置 SNTP 服务器之前，应该先确保 SNTP 服务器可达。尤其当 SNTP 服务器的地址为域名时，应该确保已配置正确的 DNS 服务器。
- 源地址和源接口只能配置一个，不能同时配置。
- 当设置多个 SNTP 服务器时，系统将轮询所有 SNTP 服务器，直到找到可用的。
- 当配置源接口为 cellular 接口时。拨号不成功情况下不会启动 SNTP 服务。

表 3-1-2 NTP 服务器参数说明

参数名称	说明	缺省值
启用	开启/关闭 NTP 服务器	关闭
NTP 服务器层级	NTP 采用分层同步方式，一般第 n+1 级与第 n 级时钟源进行同步。NTP 最多支持 16 层同步，即 0－15 层。多于 16 层将无法同步。	5
源接口	指设备发出 NTP 报文的接口。	无
源地址	指设备发出 SNTP 报文携带的源地址。	无
NTP 服务器列表		
服务器地址	NTP 服务器地址（域名/IP），最多可填写 10 个服务器	无
主 NTP 服务器	当设置多个 NTP 服务器，当勾选主 NTP 服务器时，表示我们的设备主要以该 NTP 服务器进行时间同步。	空

3.1.3 管理访问

管理访问提供创建用户、修改用户信息、删除用户和管理服务的功能。

用户分为超级用户和普通用户。

- 超级用户：由系统自动创建且只有一个，用户名为 adm，具有对路由器的所有访问权限。
- 普通用户：由超级用户创建，可以查看路由器的配置，但不能修改路由器的配置。

说明

对于超级用户（adm），不能修改其用户名，也不能删除它。但可以修改超级用户的密码。

用户权限分三个级别：

- 用户权限 1-11：只能查看参数，不能配置参数；
- 用户权限 12-14：可以配置 LAN IP、虚拟 IP 映射、系统日志、证书申请、访问控制、静态路由、系统升级和工具-ping 探测，其他显示为灰色可以查看但

不得修改配置；

- 用户权限 15：可以查看并配置所有参数。

管理服务包含 HTTP、HTTPS、TELNET 和 SSH 四种形式。

- **HTTP**：点选启用后，用户就可以通过 HTTP 协议登录设备，利用 Web 功能访问并控制设备。
- **HTTPS**：HTTPS（超文本传输协议的安全版本）是支持 SSL 协议的 HTTP 协议。
- **TELNET**：点选启用后，用户就可以通过网络提供远程登录。以服务器/客户端（Server/Client)模式工作,Telnet 客户端向 Telnet 服务器发起请求,Telnet 服务器提供 Telnet 服务。设备支持 Telnet 客户端和 Telnet 服务器功能。
- **SSH**：通过支持 RSA 认证或用加密算法 DES、3DES、AES128 对用户名密码以及传输数据进行加密的措施，实现在不安全网络上提供安全的远程登录。IR900 只支持 SSH 服务器功能，可以接收多个 SSH 客户端的连接。
- **其它参数**：设置 Web 登录超时时间，缺省值：300 秒。

表 3-1-3 管理服务参数说明

参数名称	说明	缺省值
HTTP	超文本传输协议，信息是明文传输。端口是 80。	启用
HTTPS	具有安全性的 ssl 加密传输协议。端口是 443。	关闭
TELNET	Internet 远程登陆服务的标准协议和主要方式。端口是 23。	启用
SSH	SSH 为建立在应用层基础上的安全协议。SSH 是专为远程登录会话和其他网络服务提供安全性的协议. 超时时间：SSH 会话超时时间，当 SSH 客户端在此时间内无操作，SSH 服务器将断开此连接。缺省值是 120s 密码模式：设置公钥加密方式（目前只支持 RSA）。密钥长度：设置密钥长度，可以为 512 或 1024。缺省值是 1024。	关闭



目前HTTPS支持TLS1.0、TLS1.1、TLS1.2。

3.1.4 AAA

AAA 访问控制是用来控制允许何种人访问服务器，以及一旦他们能够访问该服务器，允许他们使用何种服务的方法。是使用相同方式配置三种独立的安全功能的一种结构。它提供了完成下列服务的模块化方法：

- 认证：验证用户是否可以获得网络访问权。
- 授权：授权用户可以使用哪些服务。
- 计费：记录用户使用网络资源的情况。

1）Radius

RADIUS 协议采用了客户机/服务器（C/S）工作模式。网络接入服务器（Network Access Server，NAS）是 RADIUS 的客户端，它负责将用户的验证信息传递给指定的 RADIUS 服务器，然后处理返回的响应。RADIUS 服务器负责接收用户的连接请求，并验证用户身份，然后返回所有必须要配置的信息给客户端用户。服务器和客户端之间传输的所有数据通过使用共享密钥来验证，客户端和 RADIUS 服务器之间的用户密码经过加密发送，提供了密码使用的安全性。RADIUS 服务使用的是 UDP 协议，常应用在既要求较高安全性、又允许远程用户访问的各种网络环境中。

表 3-1-4 Radius 参数说明

参数名称	说明	缺省值
RADIUS 服务器	Radius 服务器的地址（域名/IP），最多支持 10 条	空
端口	Radius 服务器的服务端口号	1812
认证密钥	与 Radius 服务器建立连接时候需要验证的认证密钥。只有认证密钥一致才能与 Radius 服务器建立连接。	空
源接口	bridge 1、celluar 1、fastethernet 0/1	空

2）Tacacs+

Tacacs+（Terminal Access Controller Access Control System，终端访问控制器控制系统协议）是在 Tacacs 协议的基础上进行了功能增强的安全协议。该协议与 RADIUS 协议的功能类似，采用客户端/服务器模式实现 NAS 与 TACACS+服务器之间的通信。TACACS +持独立的认证（Authentication）、授权（Authorization）和计费（Accounting）功能。TACACS+应用传输控制协议（TCP）

以 Telnet 用户认证过程为例，基本消息交互流程如下：

(1) Telnet 用户请求登录设备。

(2) TACACS+客户端收到请求之后，向 TACACS+服务器发送认证开始报文。

(3) TACACS+服务器发送认证回应报文，请求用户名。

(4) TACACS+客户端收到回应报文后，向用户询问用户名。

(5) 用户输入用户名。

(6) TACACS+客户端收到用户名后，向 TACACS+服务器发送认证持续报文，其中包括了用户名。

(7) TACACS+服务器发送认证回应报文，请求登录密码。

(8) TACACS+客户端收到回应报文，向用户询问登录密码。

(9) 用户输入密码。

(10) TACACS+客户端收到登录密码后，向 TACACS+服务器发送认证持续报文，其中包括了登录密码。

(11) TACACS+服务器发送认证回应报文，指示用户通过认证。

(12) TACACS+客户端向 TACACS+服务器发送授权请求报文。

(13) TACACS+服务器发送授权回应报文，指示用户通过授权。

(14) TACACS+客户端收到授权回应成功报文，向用户输出设备的配置界面。

(15) TACACS+客户端向 TACACS+服务器发送计费开始报文。

(16) TACACS+服务器发送计费回应报文，指示计费开始报文已经收到。

(17) 用户请求断开连接。

(18) TACACS+客户端向 TACACS+服务器发送计费结束报文。

(19) TACACS+服务器发送计费结束报文，指示计费结束报文已经收到。

表 3-1-5 Tacacs+ 参数说明

参数名称	说明	缺省值
Tacacs+ 服务器	Tacacs+服务器的地址（域名/IP），最多支持 10 条	空
端口	Tacacs+服务器的服务端口号	49
认证密钥	与 Tacacs+服务器建立连接时候需要验证的认证密钥。只有认证密钥一致才能与 Radius 服务器建立连接	空

3）LDAP

LDAP 是轻量目录访问协议，英文全称是 Lightweight Directory Access Protocol，一般都简称为 LDAP。它是基于 X.500 标准的，但是简单多了并且可以根据需要定制。与 X.500 不同，LDAP 支持 TCP/IP。简要地说，LDAP 提供了访问、认证和授权的集中管理。他是很容易自定义的，并且能够实现用户和用户组管理集中化 、信息存储集中化 、设置安全和访问控制 、安全委托读取和修改权等。

表 3-1-6 LDAP 参数说明

参数名称	说明	缺省值
名称	用户自定义服务器列表名称	无
LDAP 服务器	服务器地址（域名/IP），最多支持 10 条	无
端口	与服务器端口保持一致	无
基准 DN	LDAP 目录树的最顶部	无
用户名	访问服务器的用户名	无
密码	访问服务器的密码	无
安全	加密方式共 3 种选择：None、SSL 和 StartTLS	None
验证对端	点选开启	未选

4）AAA 认证

支持以下认证方式：

- 不认证(none)：对用户非常信任，不对其进行合法检查，一般情况下不采用此方式。
- 本地认证(local)：将用户信息配置在网络接入服务器上。本地认证的优点是速度快，可以为运营降低成本，缺点是存储信息量受设备硬件条件限制。
- 远端认证：将用户信息配置在认证服务器上。支持通过 Radius 协议、Tacacs+协议和 LDAP 进行远端认证。

支持以下授权方式：

- 不授权(none)：不对用户进行授权处理。
- 本地授权(local)：根据网络接入服务器为本地用户账号配置的相关属性进行授权。
- Tacacs+授权：由 Tacacs+服务器对用户进行授权。
- Radius 认证成功后授权：认证和授权绑定在一起，不能单独使用 Radius 进行授权。
- LDAP 授权



注意

认证1和授权1要设置一致；认证2和授权2要设置一致；认证3和授权3要设置一致。



说明

当同时配置了radius,tacacs+和local时。优先级顺序遵循：1>2>3。

3.1.5 配置管理

这里可以把配置参数备份;可以导入想要的参数配置备份;可以使路由器恢复出厂设置。

表 3-1-7 配置管理参数说明

参数名称	说明	缺省值
浏览	从主机选择将要导入到路由器的配置文件	无
导入	将配置文件导入到路由器 startup-config 中,重启后会加载导入的配置。	无
备份 running-config	备份 running-config 到主机，running-config 为设备当前正在运行的配置。	无
备份 startup-config	备份 startup-config 到主机，startup-config 为设备开机启动时候的配置。	无
自动保存修改后的配置	决定是否在每次修改配置后，自动将配置保存到 startup-config	开启
加密明文密码	启用后设备在 WEB 上配置的所有带密码的参数都会以加密的方式显示。提高密码安全性。	未勾选
恢复出厂配置	将设备恢复到出厂配置，设备所有的配置被恢复到默认参数。恢复出厂后重新启动设备才生效。	无

注意

应该确保导入的配置的合法性与有序性。当导入配置时，系统会过滤格式不合法的命令，然后将正确的配置存储为startup-config，在系统重启后顺序执行这些配置。如果导入的配置内容不是按照有效的顺序排列，将导致系统不能进入期望的状态。

说明

为了不影响当前系统运行，当执行导入配置和恢复出厂配置后，需要重启路由器新的配置才能生效。

3.1.6 设备远程监控平台

设备远程监控平台是通过一个软件平台管理设备。启用设备远程监控平台后，进行相关设置，设备现场信息将定时上报给用户，使得用户可远程监管设备的工作情况。启用云网管平台后，可以通过软件平台对设备进行管理操作，使网络高效正常运行。比如，查询设备运行状态、升级设备软件、重启设备、对设备下发配置参数等等，还可以通过网管平台给设备发送控制或查询短信。

表 3-1-8 设备远程监控平台参数说明

参数名称	说明	缺省值
启用设备远程监控平台	点选启用设备远程监控平台	禁用
服务器地址	设备所在云平台服务器地址	空
注册账户	输入已注册账户名称	空
现场名称	设备所在云平台服务器现场名称	空
定位源	选择设备定位接口，可选择 GPS 或 Cellular	GPS
现场信息上报间隔	用户自定义现场信息上报时间间隔，合法值：1-65535	3600 秒
LBS 信息上报间隔	用户自定义 LBS 信息上报时间间隔，合法值：1-65535	600 秒
通道信息上报间隔	用户自定义通道信息上报时间间隔，合法值：1-65535	120 秒
设备接入点地址	用户输入设备接入点地址	空
设备接入点端口	用户定义接入点端口	0

表 3-1-9 网管平台（Device Management）参数说明

参数名称	说明	缺省值
开启 ovdp 功能	点选开启 ovdp 功能	禁用
模式	短信+IP	短信+IP
供应商	选择供应商名称	默认值
设备 ID	设备 ID 不可更改	每台设备唯一
服务器	设置网管平台 IP 地址	c.inhand.com.cn
端口	设置网管平台端口号	2003
登录重试次数	设置重试次数	3
心跳间隔时间	设置心跳间隔	120 秒
串口类型	使用 DT 时控制的串口类型，RS232/RS485	RS232
协议	连接平台使用的协议，TCP/UDP	UDP

3.1.7 GPS 定位信息

在这里可以开启或关闭 GPS 功能，配置 GPS IP 转发和 GPS 串口转发，其中 GPS IP 转发有两种类型：客户端和服务器端。

表 3-1-10 GPS-IP 转发参数说明

参数名称	说明	缺省值
GPS IP 转发-客户端		
协议	两种协议可选：TCP 协议和 UDP 协议	TCP 协议
连接类型	两种类型可选：长连接和短连接。 和服务器端保持一致	长连接
心跳间隔	当 TCP 连接建立成功后，设备发送心跳的时间间隔	100 秒
心跳重试次数	心跳超时后，继续发送心跳的次数，当达到设置的次数心跳还是超时，设备断开 TCP 连接	10
最小重连间隔	设备建立 TCP 连接时，开始使用的连接时间间隔，每 30 秒递增直到最大重连间隔	15 秒
最大重连间隔	设备建立 TCP 连接时最大重连间隔时间	180 秒
源接口	设备连接服务器时，使用源接口的地址作为源地址去建立 TCP 连接	空
上报信息间隔	设备上报 GPS 信息的时间间隔	30 秒
包含 RMC	发送 GPS 数据的 PMC 数据	启用
包含 GSA	发送 GPS 数据的 GSA 数据	启用
包含 GGA	发送 GPS 数据的 GGA 数据	启用
包含 GSV	发送 GPS 数据的 GSV 数据	启用
消息前缀	设备发送 GPS 消息时用户自定义的报文头内容	空
消息后缀	设备发送 GPS 消息时用户自定义的报文结尾内容	空
GPS IP 转发-客户端-目的 IP 地址		
服务器地址	GPS 数据上报的服务器地址	空
服务器端口	上报服务器的端口号	空
GPS IP 转发-服务器端		
连接类型	两种类型可选：长连接和短连接。 和客户端保持一致	长连接
心跳间隔	当 TCP 连接建立成功后，设备发送心跳的时间间隔。	60 秒
心跳重试次数	心跳超时后，继续发送心跳的次数，当达到设置的次数心跳还是超时，设备断开 TCP 连接。	5
本地端口号	设备当 TCP SERVER 时定义的服务端口号	10001
上报信息间隔	用户自定义设置上报信息间隔时间	30 秒
包含 RMC	发送 GPS 数据的 PMC 数据	启用
包含 GSA	发送 GPS 数据的 GSA 数据	启用
包含 GGA	发送 GPS 数据的 GGA 数据	启用
包含 GSV	发送 GPS 数据的 GSV 数据	启用
消息前缀	设备发送 GPS 消息时用户自定义的报文头内容	空
消息后缀	设备发送 GPS 消息时用户自定义的报文结尾内容	空

表 3-1-11 GPS 串口转发参数说明

参数名称	说明	缺省值
串口类型	和对端保持一致(RS232/RS485)	RS232
波特率	和对端保持一致	9600
数据位	和对端保持一致	8 bits
校验位	和对端保持一致	无校验
停止位	和对端保持一致	1 bits
软件流控	点选启用	禁用
包含 RMC	发送 GPS 数据的 PMC 数据	启用
包含 GSA	发送 GPS 数据的 GSA 数据	启用
包含 GGA	发送 GPS 数据的 GGA 数据	启用
包含 GSV	发送 GPS 数据的 GSV 数据	启用

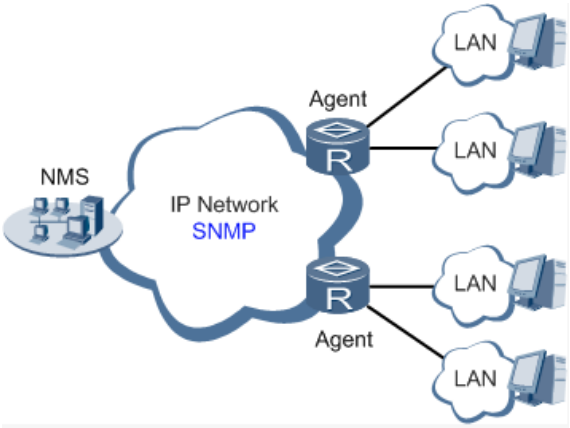
注意

GPS 串口转发和 DTU 功能不能同时使用，开启 GPS 串口转发时必须关闭 DTU 功能。

3.1.8 SNMP

管理员要对整个网络的设备进行配置和管理，这些设备分布较为分散，管理员到现场进行设备配置是不现实的。并且如果这些网络设备来自不同的厂商，而每个厂商都提供一套独立的管理接口（比如使用不同的命令行），将使得批量配置网络设备的工作量巨大。因此，在这种情况下，如果采用传统的人工方式，将会带来成本高、效率低的弊端，此时网络管理员可以利用 SNMP 远程管理和配置其下属设备，并对这些设备进行实时监控。

网管通过 SNMP 协议管理设备示意图如下图所示：



要在组网中配置 SNMP 协议，需要在管理端配置 SNMP 管理程序 NMS，同时在被管理设备端配置 SNMP 代理程序 Agent。

通过 SNMP 协议：

- 网络管理系统 NMS 可以通过 Agent 在任何时候及时地获得设备的状态信息，并实现远端控制被管理设备。
- Agent 可以及时地向 NMS 报告设备的当前状态信息，在设备发生问题时，可以立即通知 NMS。

目前设备的SNMP Agent支持SNMPv1、SNMPv2c 和SNMPv3版本。SNMPv1和SNMPv2c采用团体名认证；SNMPv3采用用户名和密码认证加密方式。

表 3-1-12 SNMPv1 和 SNMPv2c 参数说明

参数名称	说明	缺省值
启用 SNMP 功能	启用/关闭 SNMP 功能	关闭
监听地址	选择待监听网络地址，可选择：any、127.0.0.1、192.168.2.1、192.168.1.1 以及拨号所获取到的 IP 地址	any
SNMP 版本	选择管理路由器的 SNMP 版本，支持 SNMP v1/v2c/v3 V1 适用于小型网络，组网简单，对网络安全性要求不高或者网络环境本身比较安全，且比较稳定的网络，比如校园网，小型企业网。 V2C 适用于大中型网络，对网络安全性要求不高或者网络环境本身比较安全（比如 VPN 网络），但业务比较繁忙，有可能发生流量拥塞的网络。 V3 适用于各种规模的网络，尤其是对网络的安全性要求较高，确保合法的管理员才能对网络设备进行管理的网络。比如网管和被管理设备间的通信数据需要在公网上进行传输。	v2c
联系信息	填写联系信息	Beijing_Inhand_Networks_Technology_Co.,Ltd.
位置信息	填写位置地址	Beijing_China
团体名管理		
团体名	用户自定义团体名 SNMPv1、SNMPv2c 的读/写团体访问名，是网管（NMS）对设备（Agent）进行读写访问时所使用的口令，此参数需与网管配置相同。	public 和 private
访问权限	访问权限包含网管只读的 MIB 节点和网管可读写的 MIB 节点。	Read-Only(只读)
MIB 视图	选择限定网管监控和管理的 MIB 节点，目前为默认视图一种状态。	defaultView

表 3-1-13 SNMPv3 参数说明

参数名称	说明	缺省值
用户组管理		
组名	用户自定义用户组组名，长度：1-32 个字符	无
安全级别	选择该组的安全级别，分为无鉴别/无加密、鉴别/无加密、鉴别/加密共 3 种	无鉴别/无加密
只读视图	选择 SNMP 的只读视图。目前只支持 defaultView	defaultView
读写视图	选择 SNMP 的读写视图。目前只支持 defaultView	defaultView
通知视图	选择 SNMP 的通知视图。目前只支持 defaultView	defaultView
用户管理		
用户名	用户自定义用户名，长度：1-32 个字符	无
组名	选择该用户加入的用户组，首先要在用户组管理表格中定义过，才可再次选择相应的用户组。	无
认证模式	选择认证模式。提供 MD5、SHA 和无鉴别三种认证模式，选择”无鉴别”不启用认证	无鉴别
认证密码	只有认证模式不为”无鉴别”时，认证密码才可以输入。长度：8-32 个字符	无
加密模式	选择加密模式，加密分为：无加密、AES、DES 三种模式。	无加密
加密密码	只有加密模式不为”无加密”时，加密模式密码才可输入。长度：8-32 个字符	无

SNMP Trap(SNMP 陷阱)：某种入口，到达该入口会使 SNMP 被管设备主动通知 SNMP 管理器，而不是等待 SNMP 管理器的再次轮询。在网管系统中，被管理设备中的代理可以在任何时候向网络管理工作站报告错误情况。代理并不需要等到管理工作站为获得这些错误情况而轮询他的时候才会报告。这些错误情况就是众所周知的 SNMP 自陷（trap）。

表 3-1-14 SnmpTrap 配置参数说明

参数名称	说明	缺省值
目的地址(IP)	填写管理站(NMS)的 IP 地址	无
安全名	版本 v1 或 v2c 时填写相应的团体名，版本为 v3 时填写相应的用户名。长度：1-32 个字符	无
UDP 端口号	填写 UDP 端口号，可以使用默认的端口号范围：1-65535	162

SNMP Mibs（SNMP 管理信息库）：Snmp Mibs 是 SNMP 协议软件中主要的一个模块。IETF 规定的管理信息库 MIB（其中定义了可访问的网络设备及其属性，由对象识别符唯一指定）。MIB 是一个属性结构，SNMP 协议消息通过遍历 SNMP MIB 树形目录中的节点来访问网络中的设备。SnmpMibs 为用户提供了获取 Mibs 文件的接口，通过“download”按钮用户可下载自己所需要的 mib 文件。

3.1.9 Python

Python 是一种面向对象的解释型计算机程序设计语言。Python 具有丰富和强大的库，能够把用其他语言制作的各种模块很轻松地链接在一起。用户使用 Python 快速生成程序的原型（可以是程序的最终界面），然后对其中有特别要求的部分，用更合适的语言改写，而后可以封装为 Python 可以调用的扩展类库。

Python 功能模块，用户可以查看相关运行状态（扩展存储卡、AppManager 运行状态、调试服务器运行状态、程序存储空间使用率、数据日志存储空间使用率、外部存储空间使用率以及 App 名称、App 版本和 App 命令），用户可以定义、更改 AppManager 配置以及导入 Python App 包。

表 3-1-15　APPManager 配置参数说明

参数名称	说明	缺省值
使能 Python AppManager	点选启用 Python AppManager	禁用
使能调试服务器	点选启用调试服务器	禁用
使能扩展存储	点选启用扩展存储	禁用
App 管理		
ID	填写 App 编号，最多可设置 10 个 App，合法值：1-10	1
App 命令	用户自定义 App 命令	空
日志文件大小（MB）	用户自定义日志文件大小，合法值：1-70	1

表 3-1-16 Python App 参数说明

参数名称	说明	缺省值
导入 App 包	用户点击“浏览”按钮，选取将要上传的 App 包 点击“上传”按钮，导入 App 包	未选择
导入 App 配置文件名	App 名称默认 python，不可更改 点击“浏览”按钮，选取将要上传的 App 配置文件 点击“上传”按钮，导入 App 配置文件	未选择

3.1.10 告警

告警功能提供给用户一种即时获知路由器异常的方式，使得用户能尽早的发现并解决这些异常。当异常产生时路由器将发出告警，用户可以选择系统定义的多种异常并选择合适的通告方式来获知这些异常。所有告警都将被记录在告警日志中，供用户在需要时排查问题。

告警按照类型分为：系统告警和端口告警。

- 系统告警：因系统或环境出现某种异常而发出的告警，分为热启动、冷启动、

内存不足。

- 端口告警：因网络接口出现异常而发出的告警，分为 LINK-UP、LINK-DOWN。

告警状态分为：

- 存在（Raise）：表示告警发生还没有被确认
- 确认（Confirm）：表示发生的告警用户暂时不能解决
- 全部（All）：表示发生的全部告警

告警等级可分为：

- EMERG：设备发生了某种严重的错误可能导致系统重启
- CRIT：设备发生了某种不可恢复的错误
- WARN：设备发生了某种影响系统功能的错误
- NOTICE：设备发生了某种影响系统性能的错误
- INFO：设备发生了某种正常的事件

通过告警配置对话框您可以进行以下操作：

- 通过“告警状态”界面，可以查看上电以来系统产生的所有告警。
- 通过“告警输入”界面，可以自定义关心的告警类型。
- 通过“告警输出”界面，设置 Email 告警通告方式，日志记录是默认输出方式。配置此项功能，当有告警产生时，系统会自动以邮件的形式把告警内容从发送告警邮件的邮箱地址发送到目的邮箱地址。一般用户不配置此项功能
- 通过“告警映射”界面，可以灵活的将关心的告警类型映射到一种或多种告警通告方式上。告警映射有两种映射方式：CLI（console 口）和 Email。若要启用 Email 映射则要在告警输出部分启用并配置好邮箱地址。

3.1.11 系统日志

系统日志包含了网络和设备的大量信息，包括运行状态、配置变化等。通过“系统日志设置”界面，可以设置远程日志服务器，路由器将会把所有的系统日志上传到远程日志服务器，这需要主机上的远程日志软件（如:Kiwi Syslog Daemon）的配合。



注意

系统诊断记录文件为加密文件，需要使用我司的解密工具解密后才能查看。下载系统诊断记录时会把路由器的配置信息也下载下来。系统日志最大存储512K.

3.1.12 时间表管理

启用此功能，用户可以自定义设备重启时间。

当前设备定时任务仅支持设备定时重启功能（reboot），且只能设置间隔天数为每天（everyday）不可更改。系统缺省时间为 0 时 0 分.用户可以自定义重启时间。最多定义 10 条。如设置时间表为 reboot，everyday，12 时 0 分后。设备每天 12 时会自动重启设备。



注意

配置时间表管理时必须确保路由器时间和当前时间一致。可以通过WEB上点击时间同步或者开启NTP来确保路由器时间和当前时间一致。

3.1.13 系统升级

升级过程共分为两个阶段，第一阶段将升级文件写入备份固件区，即系统升级一节所描述的过程；第二阶段将备份固件区中的文件拷贝到主固件区。在软件升级的过程中，请不要在 Web 上进行任何操作，否则可能会导致软件升级中断。

使用带 WIFI 功能的设备，还需升级接口板固件。点击页面“接口板固件升级”，在弹出的对话框中选择与固件版本匹配的接口板固件版本，升级即可。升级过程与上述固件版本升级过程相同。

3.1.14 重启系统

设备重启前请保存配置，可以在 WEB 上执行重启。或通过命令行执行 reboot 命令来执行重启。

3.2 二层交换

二层交换是指设备具有二层交换机的属性。可以设置设备端口的状态、端口镜像、和广播风暴控制等功能。

端口镜像功能是将一个或多个源端口的数据流量转发到某一个指定端口来实现对网络的监听，指定端口称之为“镜像端口”或“目的端口”，在网络出故障的时候，可以快速地进行故障定位。

广播风暴控制是允许端口对网路上出现的广播风暴进行过滤。当端口收到的广播帧累计达到预定的门限值时，端口将自动丢弃收到的广播帧。从而避免广播风暴的出现。

表 3-2-1 端口基本参数说明

参数名称	说明	缺省值
端口	设备支持 4 个端口操作：FE1/1、FE1/2、FE1/3、FE1/4，用户可根据自己的需要，对相应的端口进行配置	
管理状态	设置端口的工作模式，分为：up、shutdown，用户可根据自己的需要，打开或关闭相应端口	up
端口速率	设置端口速率，可选择 auto、100Mbps、10Mbps	auto
端口模式	设置端口模式，可选择 auto、full、half	auto

表 3-2-2 端口镜像参数说明

参数名称	说明	缺省值
启用 monitor	点选启用端口镜像功能	禁用
目的端口	监听数据的端口。	none
源端口参数		
镜像方向	设置镜像方向，可选择：none、ingress、egress、both ingress:只对从该端口进入的流量进行镜像 egress:只对从该端口发出的双向流量进行镜像 both:支持对该端口收到和发出的双向流量进行镜像	none



只有IR915的FE1/1--FE1/4端口支持二层VLAN功能。

3.3 网络

网络总共包含了以太网接口、VLAN 接口、拨号接口、ADSL 拨号（PPPoE）、WLAN 接口、环回接口、DHCP 服务、DNS 服务、动态域名、短信服务共 10 个功能模块。

3.3.1 以太网接口

以太网接口支持三种连接模式：

- 自动模式：即配置接口作为 DHCP 客户端，使用 DHCP 方式获取 IP 地址。
- 手动模式：即手动为接口配置 IP 地址和子网掩码。
- PPPoE：即配置接口作为 PPPoE 客户端。

以太网接口此处配置的连接模式是手动模式，即手动为接口配置 IP 地址和子网掩码。通过状态页面，用户可直观浏览到以太网口（Fastethernet 0/1）的基本信息：连接类型、IP 地址、子网掩码、网关、DNS、MTU、状态、连接时间、剩余时间、说明。以及桥接口（Bridge 1）基本信息：IP 地址、子网掩码、网关、DNS、MTU、状态、连接时间、剩余时间。

表 3-3-1 以太网接口参数说明

参数名称	说明	缺省值
主 IP	用户可以根据需要配置或更改主 IP 地址	192.168.1.1
子网掩码	用户配置的以太网接口的子网掩码	255.255.255.0
MTU	最大传输单元，以字节为单位	1500
端口速率/端口模式	五种选择：自动协商、100M 全双工、100M 半双工、10M 全双工和 10M 半双工	自动协商
二层状态联动	勾选：端口没物理连接状态为 Down，有物理连接时为 UP 不勾选：端口有无物理连接时都显示 UP。	不勾选
说明	以太网接口的描述信息，标识作用	无
多 IP 支持	除主 IP 以外用户还可以配从 IP 地址，最多可以配置 10 个。	无

表 3-3-2 桥接口参数说明

参数名称	说明	缺省值
网桥号	网桥号只能配为 1	1
主地址-IP 地址	用户自定义配置或更改主 IP 地址	192.168.2.1
主地址-子网掩码	用户自定义配置或更改主地址子网掩码	255.255.255.0
从地址-IP 地址	除主 IP 以外用户还可以配从 IP 地址，最多可以配置 10 个	无
从地址-子网掩码	除主 IP 以外用户还可以配从地址子网掩码	无
网桥成员	加入到网桥的接口，包括 F0/1、F0/2、VLAN1 和 dot11radio 1	VLAN1 、dot11radio 1

注意

只有 IR912 和 IR915-W-XX 设备能配置桥接口，IR915 不带 wifi 设备不能配置桥接口。

3.3.2 VLAN 接口

虚拟局域网（VLAN）是一组逻辑上的设备和用户，这些设备和用户并不受物理位置的限制，可以根据功能、部门及应用等因素将它们组织起来，相互之间的通信就好像它们在同一个网段中一样，VLAN 工作在 OSI 参考模型的第 2 层和第 3 层，一个 VLAN 就是一个广播域，VLAN 之间的通信是通过第 3 层的路由器来完成的。

目前设备 VLAN 端口支持 Access 和 Trunk 两种链路类型。Access 类型的端口只能属于 1 个 VLAN，一般用于连接计算机的端口；Trunk 类型的端口可以允许多个 VLAN 通过，可以接收和发送多个 VLAN 报文，可以用于交换机之间的连接，也可以用于连接用户的计算机。用户可通过 VLAN 聚集页面根据需要选择链路类型。

本证 VLAN 是分配给 802.1Q 中继端口，802.1Q 中继端口支持来自多个 VLAN 的流量（有标记流量），也支持 VLAN 以外的流量（无标记流量）。802.1Q 中继端口会将无标记流量发送到本证 VLAN。如果交换机端口设置了本证 VLAN，则连接到该端口的计算机将产生无标记流量。用户可通过 VLAN 聚集页面根据需要自定义本证 VLAN 标号，合法值：1-4000。

表 3-3-3 VLAN 配置参数说明

参数名称	说明	缺省值
VLAN 号	即 VLAN ID，用户自定义（ID 1-4000）	空
VLAN 虚接口		
主地址-IP 地址	用户自定义配置或更改主 IP 地址	无
主地址-子网掩码	用户自定义配置或更改主地址子网掩码	无
从地址-IP 地址	除主 IP 以外用户还可以配从 IP 地址，最多可以配置 10 个	无
从地址-子网掩码	除主 IP 以外用户还可以配从地址子网掩码	无
VLAN 成员端口		
VLAN 成员端口	可选择 FE1/1、FE1/2、FE1/3、FE1/4 若在 VLAN 聚集中设置某个端口为 Access 模式，则该端口只允许属于唯一 VLAN ID 若在 VLAN 聚集中设置某个端口为 Trunk 模式，则该端口允许属于多个 VLAN ID	无

3.3.3 拨号接口

IR900 设备装入 SIM 卡，通过拨号接口拨号实现路由器的无线网络连接功能。IR900 支持拨号 SIM 卡备份功能，当主 SIM 卡出现故障或余额不足等导致网络连接断开时，可以快速的切换到备份 SIM 卡，由备份 SIM 卡来承担网络连接任务，从而提高了网络连接的可靠性。

用户可通过状态页面查看当前设备所使用模块（Modem）状态：

- 当前 SIM 卡（IR900 设备支持双卡，此项显示正在使用的为 SIM1 还是 SIM2）
- IMEI 号码（国际移动设备身份码，国际移动装备辨识码，它与每台移动设备一一对应， 该码是全世界唯一的）
- IMSI 号码（国际移动用户识别码，是区别移动用户的标志，存储在 SIM 卡中，可用于 区别移动用户的有效信息）
- ICCID 号码（集成电路卡识别码即 SIM 卡卡号）
- 电话号码（当前使用 SIM 卡电话号码）
- 信号级别（dBm 表示功率绝对值的值，这个值越大，标识信号越好；asu 代表移动设备将它的位置传递给附近的信号塔速率，以一种更加线性的方式来表示。asu 的正常范畴为 1-30，asu 信号值越大，信号强度越好。dBm=-113+2*asu。当 asu 的值为 1-10 时设备信号灯 1 亮；11-20 时设备信号灯 1,2 亮；21-30 时设备信号灯 1,2,3 全亮）
- 注册状态（当前模块的状态，如：注册网络成功、正在注册到网络）
- 运营商（显示运营商名称，如：中国移动-China Mobile、中国联通-China Unicom）
- 网络类型（显示当前设备拨号上网的网络类型，如：4G（LTE）、2G（EDGE）等）
- 位置区码（为了确定移动台的位置，每个公用陆地移动网络的覆盖区都被划分成许多位置区，位置区码则用于标识不同的位置区）
- 用户可通过状态页面查看当前设备网络连接状态：
  - 状态：显示当前是否在线，如：已连接、未连接
  - IP 地址：设备拨号成功所获取到的 IP 地址
  - 子网掩码：设备拨号成功所获取到的子网掩码
  - 网关：设备通过拨号成功所获取到的网关
  - DNS：设备通过拨号成功所获取到的网关

- MTU：最大传输单元，系统默认值 1500
- 连接时间：显示设备拨号成功到下一次重启所用时间

拨号接口支持三种连接方式：永远在线、按需拨号和手工拨号。

表 3-3-4 拨号接口参数说明

参数名称	说明	缺省值
拨号参数集	拨号策略选择，对应于拨号参数集配置索引项	~~1~~auto
启用漫游	勾选启用漫游功能，在漫游状态下可以正常拨号上网，当取消漫游选项，漫游的 SIM 卡不能拨号上网 使用本地卡时，勾选漫游和取消漫游功能都不影响 SIM 卡拨号上网	启用
PIN Code	PIN 码即 SIM 卡的个人识别密码。 如果启用 PIN 码，当不设置 PIN 码或设置错误的 PIN 码，设备拨号失败；设置正常的 PIN 码，设备可以正常拨号上网。	无
网络选择方式	五种选择：自动、2G、 3G、 4G 和 3G2G 用户根据所使用设备及 SIM 卡适用的情况，可选择特定的网络方式，或使用自动方式，设备可自行注册到适用当前网络状况的网络方式。	自动
静态 IP	拨号时是否使用静态 IP，可以手动指定 IP 地址。设备每次拨号都获得配置的静态 IP	关闭
连接方式	可选择永远在线、按需拨号、手工拨号 **永远在线**：永远在线是系统默认拨号方式，正常状态下设备一直在线只有拨号口没有任何流量时会 30 分钟掉线重新拨号 **按需拨号**：根据设备型号不同，按需拨号又分为：允许数据激活、短信激活两种拨号方式。 ● 数据激活：默认设备为不在线状态，当有去往公网数据时，自动拨号成功 ● 短信激活：通过发送短信指令，控制设备连接网络、断开网络连接、重启设备、查询设备信息（IP 地址、是否在线等） 注：短信指令相关操作详见，“网络”>>“短信服务”参数说明 **手工拨号**：用户通过 WEB 页面“网络”>>“拨号接口”状态页面的网络连接	永远在线
重拨间隔	设备每次掉线重新拨号等待的时间	10 秒
ICMP 探测服务器	要探测的远端 IP 地址或域名（同时启用两个 ICMP 探测服务器，建议同时输入 IP 地址或同时输入域名） 设备支持两个 ICMP 探测服务器：主服务器和备份服务器。当配置两个服务器后，首先检测第一个服务器，只有当第一个服务器达到最大重试次数后，系统才会检测第二个服务器。当两个服务器都检测失败的情况下，设备会重新拨号并进行下一轮 ICMP 探测	无

ICMP 探测间隔时间	设备发送 ICMP 探测报文的时间间隔	30 秒
ICMP 探测超时时间	在设置的 ICMP 探测超时时间内，没有收到 ICMP 响应包认为本次 ICMP 探测超时	5 秒
ICMP 探测最大重试次数	设置 ICMP 探测失败时的最大重试次数(达到最大次数后会重新拨号)	5
ICMP 严格探测	当设备的拨号接口有数据流量时。设备不发送 ICMP 探测。当拨号接口没有数据流量时候才会发送 ICMP 探测,可以达到节省流量目的	关闭
显示高级选项	点选启用高级选项配置	禁用
点选启用高级选项（以下各项均为启用高级选项后的相关参数）		
初始化命令	可以配置一些 AT 指令查询模块状态	空
信号查询间隔时间	用户设置信号查询间隔时间，0 表示禁用 设置信号查询间隔时间，保存配置。设备拨号成功后，将以设置的查询间隔时间定时查询信号状态。如设置查询间隔时间为 60s。设备拨号成后，拔下设备天线，等到 60s 后设备信号应该降低，在 60s 内设备信号不发生变化	120 秒
拨号超时时间	用户设置拨号超时时间。在设定的超时时间内，设备未成功拨号，认为拨号超时，设备重新检测模块并重新拨号	120 秒
MTU	设置最大传输单元，以字节为单位 如果 MTU 配置过小而报文尺寸较大，可能会造成分片过多，报文被 QoS 队列丢弃。如果 MTU 值配置过大，会造成报文的传输速度较慢，甚至会造成报文丢失	1500
启用双 SIM 卡	默认情况下，设备使用单卡模式，且使用 SIM1 卡	禁用
启用调试模式	点选启用调试模式，系统日志将打印更为详细的信息	禁用
双 SIM 卡		
选择主卡	IR900 设备支持双 SIM 卡，用户可选择指定卡为主卡（此功能适用于双 SIM 卡插入的情况），当主卡出现故障或因余额不足使网络断开连接时，备卡才承担网络连接任务。 可选择：SIM1、SIM2、随机、顺序 ● SIM1：即设定 SIM1 卡为主卡 ● SIM2：即设定 SIM2 卡为主卡 ● 随机：系统随机选择任一 SIM 卡为主卡 ● 顺序：即第一次拨号 SIM1 卡为主卡，再次拨号 SIM2 卡为主卡，再一次拨号 SIM1 卡为主卡.....	SIM1
最大拨号次数	当 SIM1 在设置的最大拨号次数内一直没拨号成功,设备将切换到 SIM2 拨号	5
最小连接时间	当设备拨号连接成功时间小于设置的最小连接时间时，设备的拨号次数会累计。当大于设置的最小连接时。设备的拨号次数将清零。0 是禁用次功能	0 秒
信号阈值	当前承担网络连接任务的 SIM 卡信号阈值。设备当前真实信号小于设置的信号阀值时，设备将按照信号探测间隔检测信号，当达到信号检测重试次数后，设备重新拨号，备卡承担网络连接任务	禁用

信号探测间隔	用户设置信号探测间隔。（当主卡信号阈值为：0-0 即禁用时，此配置项不可用） 设备拨号成功后，当真实信号小于设置的信号阀值时，会按照设置好的间隔时间，定时查询网络信号	0：禁用
信号探测重试次数	用户设置信号探测重试次数。（当主卡信号阈值为：0-0 即禁用时，此配置项不可用） 当信号探测达到最大重试次数时，信号值仍然不在信号阈值范围内，设备重新拨号，此时备卡承担网络连接任务	
备卡超时时间	当前使用的为被卡，被卡拨号成功后，当达到设定的被卡超时时间后，设备会切换到主卡拨号	0 秒
拨号参数集		
索引	对拨号参数集进行编号，此编号应用于上述对 SIM 卡进行制定拨号参数集的选择依据。	1
网络类型	用户选择设备所使用的移动网络类型，可选择： GSM、CDMA	GSM
APN(CDMA2000 系列不设置此项)	APN（Access Point Name）用来标识 WCDMA/LTE 网络的业务种类，WCDMA/LTE 系统根据用户连接 WCDMA/LTE 网络的 APN 提供相应的服务。	3gnet
拨号号码	拨号使用的拨号串。拨号串由运营商提供，请向运营商获取。 当 3G/LTE 数据卡支持 WCDMA 或 LTE 标准时，缺省拨号串为 *99***1# 。 当 3G 数据卡支持 CDMA2000 标准时，缺省拨号串为#777。	*99***1#
认证方式	用户可选择：自动、PAP、CHAP、MS-CHAP、MS-CHAPv2 PAP:密码认证协议，通过两次握手提供一种简单明文认证方式 CHAP:挑战握手认证协议，通过三次握手确认摘要信息从而进行安全认证 MS-CHAP:微软公司的 CHAP 标准 MS-CHAPv2:MS-CHAP 升级版本，它要求双向验证。	自动
用户名	指定接入外部 PDN 网络用户的用户名。由运营商提供。	gprs
密码	指定接入外部 PDN 网络用户的密码。由运营商提供。	gprs

注意

- IR900 设备当重复拨号 30 次没有拨号成功，设备会自动重启。当没有插入 SIM 卡或一直未注册网路，设备检测 120 次模块后设备自动重启
- IR900 能根据 SIM 卡自动识别 APN，一般不需要配置任何参数就能拨号成功（专网除外）

3.3.4 ADSL 拨号（PPPoE）

当设备作为 PPPoE 客户端时，PPPoE 会话可以配置在物理以太网接口接口上，当设备通过 ADSL 接口连入 Internet 的时候，需要在虚拟以太网接口配置 PPPoE 会话；当设备通过以太网接口连接 ADSL Modem 再连入 Internet 的时候，需要在以太网接口配置 PPPoE 会话。

表 3-3-5 拨号池参数说明

参数名称	说明	缺省值
池标识	用户自定义，范围 1-10	1
接口	PPPOE 会话配置的接口，可选 Fastethernet0/1、Fastethernet0/2、bridge 1、vlan1 等	Fastethernet0/1
PPPoE 列表		
标识	用户自定义，范围 1-10	1
池标识	和拨号池的池标识一致	无
认证方式	三种可选：Auto、PAP 和 CHAP Auto:PPP 建立时自动与对端协商认证方式 PAP:口令以明文方式在链路上发送，完成 PPP 链路建立后，被验证方会不停地在链路上反复发送用户名和口令，直到身份验证过程结束，所以安全性不高 CHAP:验证协议为三次握手验证协议。它只在网络上传输用户名，而并不传输用户密码，因此安全性比 PAP 认证高	Auto
用户名	PPPoE 拨号使用的用户名	无
密码	PPPoE 拨号使用的用户名。	无
本地 IP 地址	指定分配给以 PPPOE 接口的 IP 地址。本地地址不能与设备上其他接口或网络内其他设备的 IP 地址冲突。	无
远端 IP 地址	PPPOE 对端设备 IP 地址。对端地址必须与接口的 IP 地址在同一网段	无
心跳时间间隔	PPPOE 建立连接后发送心跳报文时间间隔	120
心跳重试次数	当心跳超时后，重新发送心跳报文并进行计数，当达到最大重试次数，设备重新建立连接	3
调试	点选启用调试选项，系统日志将会输出详细信息	禁用

3.3.5 WLAN 接口

WLAN 即无线局域网络。它是相对于有线网络而言的一种全新的网络组建方式。具有灵活性和移动性。在有线网络中，网络设备的安放位置受网络位置的限制，而无线局域网在无线信号覆盖区域内的任何一个位置都可以接入网络。无线局域网另一个最大的优点在于其移动性，连接到无线局域网的用户可以移动且能同时与网络保持连接。它们被广泛应用，从家

庭到企业再到 Internet 接入热点。IR900 设备为用户提供的 WLAN 接口有接入点、客户端、AP-Client 三种类型。

表 3-3-6 WLAN 参数说明

参数名称	说明	缺省值
接入点		
启用	启用或禁用 WLAN 服务。启用 WLAN 服务后，可以配置无线网络的基本参数和安全认证选项，使得无线接入的用户可以实现接入 Internet。	禁用
接口类型	选择 WLAN 工作模式，可选择接入点、客户端、AP-Client	接入点
SSID 广播	开启 SSID 广播后无线客户端能扫描到此 SSID.禁用是隐藏 SSID,SSID 隐藏后，设备发送的信标帧里面不包含 SSID 信息，接入客户端必须在无线客户端上手动配置该 SSID 标识才能接入设备	启用
AP 客户端隔离	开启 AP 客户端隔离功能后，AP 下接入的所有用户之间的二层报文相互不能进行转发，提高了用户通信安全性，	禁用
射频类型	六种类型可选：802.11g/n、802.11g、802.11n、802.11b、802.11b/g 、802.11b/g/n 802.11b:工作在 2.4G 频段，最高速率 11Mbps 802.11g:工作在 2.4G 频段，最高速率 54Mbps 802.11n:工作在 2.4G 频段，也可以工作在 5G 频段，理论最高速率 300Mbps	802.11g/n
信道	信道是以无线信号作为传输媒体的数据信号传送通道，共有 13 个信道，每个信道的载波频率不同： 信道 1，中心频率 2.412GHz；信道 2，中心频率 2.417GHz 信道 3，中心频率 2.422GHz；信道 4，中心频率 2.427GHz 信道 5，中心频率 2.432GHz；信道 6，中心频率 2.437GHz 信道 7，中心频率 2.442GHz；信道 8，中心频率 2.447GHz 信道 9，中心频率 2.452GHz；信道 10，中心频率 2.457GHz 信道 11，中心频率 2.462GHz；信道 12，中心频率 2.467GHz 信道 13，中心频率 2.472GHz	11
SSID	SSID：服务集标识。SSID 技术可以将一个无线局域网分为几个需要不同身份验证的子网络，每一个子网络都要独立的身份认证，只有通过身份认证的用户才可以进入相应的子网络，防止未被授权的用户进入网络。	InRouter900
认证方式	六种认证方式可选：开放式、共享式、WPA-PSK、WPA、WPA2-PSK、WPA2、WPASK/WPA2SK WPA 加密方式目前有四种认证方式：WPA、WPA-PSK、WPA2、WPA2-PSK ● WEP（有线等效密钥）：对在两台设备间无线传输的数据进行加密的方式，用以防止非法用户窃听或侵入无线网络 ● WPA：用来代替 WEP。WPA 增强了生成加密密钥的算法，	开放式

	WPA 中还增加了防止数据中途被篡改的功能和认证功能 ● WPA-PSK（预共享密钥 Wi-Fi 保护访问）：适用于个人或普通家庭网络，使用预先共享密钥，密钥设置的密码越长，安全性越高，使用 TKIP 加密方式 ● WPA2（WPA 第二版）：WPA2 是 WPA 的增强型版本，与 WPA 相比，WPA2 新增了支持 AES 的加密方式 ● WPA2-PSK：与 WPA-PSK 相似，适用于个人或普通家庭网络，使用预先共享密钥，支持 TKIP 和 AES 两种加密方式	
加密方式	根据不同认证方式，加密方式不同 开放式：支持 NONE、WEP40、WEP104 加密方式 共享式：支持 NONE、WEP40、WEP104 加密方式 WPA、WPA-PSK、WPA2、WPA2-PSK、WPASK/WPA2SK：支持 AES、TKIP 加密方式 注：当使用 WPA、WPA2 认证方式时需填写 RADIUS 服务器地址、以及 RADIUS 服务器端口，缺省值为 1812，同时还应选择源接口	NONE
无线频宽	指定该 AP 射频对应的信道带宽，可选择 20MHz、40MHz	20MHz
最大客户端数	设置设备支持的最大客户端数目（最多 128 个）	空
客户端		
接口类型	选择客户端模式	
SSID	填写要连接的 SSID 名称	空
认证方式	和要连接的 SSID 的认证方式保持一致	开放式
加密方式	和要连接的 SSID 的加密方式保持一致	NONE
接入点-客户端		
接口类型	选择接入点-客户端模式	
SSID 广播	开启后，用户可通过 SSID 名称搜索到无线网络。	启用
AP 客户端隔离	开启 AP 客户端隔离功能后，AP 下接入的所有用户之间的二层报文相互不能进行转发，提高了用户通信安全性，	禁用
射频类型	选择射频类型	802.11g/n
信道	选择信道（此信道应与接入点信道保持一致）	11
SSID	用户设置设备作为接入点的 SSID	InRouter900
认证方式	可选择：开放式、共享式、WPA-PSK、WPA、WPA2-PSK、WPA2、WPAPSK/WPA2PSK	开放式
加密方式	根据不同认证方式，加密方式不同 开放式：支持 NONE、WEP40、WEP104 加密方式 共享式：支持 NONE、WEP40、WEP104 加密方式 WPA、WPA-PSK、WPA2、WPA2-PSK、WPASK/WPA2SK：支持 AES、TKIP 加密方式	NONE
无线频宽	指定该 AP 射频对应的信道带宽，可选择 20MHz、40MHz	20MHz
最大客户端数	设置设备支持的最大客户端数目（最多 128 个）	空
客户端 SSID	输入设备作为客户端所要连接的接入点 SSID	空

认证方式	可选择：开放式、共享式、WPA-PSK、WPA2-PSK、	开放式
加密方式	此处加密方式应与所要连接的接入点的加密方式方式保持一致、支持网络密钥的加密方式所使用的密钥也应与所要连接的接入点的所设置的密钥保持一致 开放式：支持 NONE、WEP40、WEP104 加密方式 共享式：支持 NONE、WEP40、WEP104 加密方式 WPA-PSK、WPA2-PSK：支持 AES、TKIP 加密方式	NONE

表 3-3-7 IP 设置参数说明

参数名称	说明	缺省值
WLAN 接口---接入点		
IP 设置	不可配置	192.168.2.1
子网掩码	不可配置	255.255.255.0
WLAN 接口---客户端		
主 IP	用户自主设置 IP 地址，客户端的 IP 地址一定要和接入点网段保持一致	空
子网掩码	用户自主设置子网掩码，客户端的子网掩码一定要和接入点网段保持一致	空
WLAN 接口---接入点-客户端		
主 IP	不可配置	192.168.2.1
子网掩码	不可配置	255.255.255.1
dot11radio2 主 IP	用户自主设置 dot11radio2 的 IP 地址，客户端的 IP 地址一定要和接入点网段保持一致	空
dot11radio2 子网掩码	用户自主设置 dot11radio2 的子网掩码，客户端的子网掩码一定要和接入点网段保持一致	空
dot11radio2 多 IP 支持从 IP	用户自主设置 dot11radio2 的从 IP 地址，dot11radio2 的从 IP 地址一定要和接入点网段保持一致（最多可设置 10 个）	空
dot11radio2 多 IP 支持子网掩码	用户自主设置 dot11radio2 的子网掩码，dot11radio2 的子网掩码一定要和接入点网段保持一致（最多可设置 10 个）	空

在 WLAN 接口类型处选择客户端时，SSID 扫描功能才开启。在“SSID 扫描”界面，可以浏览到所有可用的 SSID 名称，以及该 SSID 所使用的信道、BSSID、安全（加密方式）、信号（以百分比显示信号的强弱）、模式（射频段）并可以显示设备作为客户端的连接状态。

注意

- 接入点为 AP-Client 时，信道必须与需要连接的 AP 信道保持一致才能建立连接。
- 设备配置为客户端时，一般需要在安装向导-新建 WAN 界面配置 dot11radio1 为 WAN 口，才能实现客户端下端设备与 AP 通讯。

3.3.6 环回接口

回环接口（loopback 接口），环回接口是路由器上的一个逻辑、虚拟接口。路由器默认没有环回接口。可以根据需要创建任何数目的环回接口。这些接口在路由器上与物理接口一样对待：可以给它们分配寻址信息，包括它们在路由器选择更新中的网络号，甚至在它们上可以终止 IP 连接。创建并配置好环回接口之后，它的地址是能被 ping 或 telnet 的，这就可以用来测试网络的连通性。

表 3-3-8 环回接口参数说明

参数名称	说明	缺省值
IP 地址	用户不可更改	127.0.0.1
子网掩码	用户不可更改	255.0.0.0
多 IP 支持	除上边 IP 以外用户还可以配其他 IP 地址	无



注意

环回接口由于独占一个IP地址，子网掩码一般建议设为255.255.255.255，以节省资源。

3.3.7 DHCP 服务

DHCP 采用客户端/服务器通信模式，由客户端向服务器提出配置申请，服务器返回为客户端分配的 IP 地址等相应的配置信息，以实现 IP 地址等信息的动态配置。

- 设备作为 DHCP 服务器的职责是当工作站登录进来时分配 IP 地址，并且确保分配给每个工作站的 IP 地址不同，DHCP 服务器极大地简化了以前需要用手工来完成的一些网络管理任务。
- 设备作为 DHCP 客户端，登录到 DHCP 服务器后接收 DHCP 服务器分配的 IP 地址，所以设备的以太网接口需要配置为自动方式。

表 3-3-9 DHCP 服务器参数说明

接口	参数说明	缺省值
fastethernet	点选启用	启用
	起始地址：设置地址池中分配给客户端设备的起始 IP 地址	192.168.1.2
	结束地址：设置地址池种分配给客户端设备的结束 IP 地址	192.168.1.100
	有效期：设置分配 IP 的地址的有效期，过期 DHCP 服务器将回收分配给客户端的 IP 地址并重新分配 IP 地址，不能为空	1440 分钟
bridge 1	点选启用	启用
	起始地址：设置地址池中分配给客户端设备的起始 IP 地址	192.168.2.2
	结束地址：设置地址池中分配给客户端设备的结束 IP 地址	192.168.2.100
	有效期：设置分配 IP 的地址的有效期，过期 DHCP 服务器将回收分配给客户端的 IP 地址并重新分配 IP 地址，不能为空	1440 分钟
参数名称	**说明**	**缺省值**
域名解析服务器	点击“编辑”可设置首选域名服务器和备选域名服务器	无
Windows 名称服务器（WINS）	Windows 服务器对应的地址	空
静态 IP 设置		
MAC 地址	设置一个静态指定 DHCP 的 MAC 地址（不能与其他 MAC 相同，防止冲突）	0000.0000.0000
IP 地址	设置一个静态指定的 IP 地址（必须在起始 IP 地址和结束 IP 地址范围内）	无

注意

- IR900 所有以太网口默认都开启了 DHCP 服务器功能，建议用户首先选用自动获取 IP 的方式。

一般情况 DHCP 数据包是无法穿越路由器进行传输的，就是不可能由 DHCP 服务器提供 DHCP 服务给远离两个以上路由器上连接的设备。通过 DHCP 转发可以实现让 DHCP 请求和应答数据包穿越多台路由器（宽带路由器）的功能。

表 3-3-10 DHCP 转发参数说明

参数名称	说明	缺省值
启用	开启/关闭	关闭
DHCP 服务器	设置 DHCP 服务器，最多可以配置 4 个	无
源地址	与 DHCP 服务器相连的接口地址	无

表 3-3-11 DHCP 客户端

参数名称	说明	缺省值
bridge1	开启/关闭	关闭
Dot11radio 1 Dot11radio 2	WLAN 配置为客户端或 AP-Client 才有能配置此端口）	开启
Fastethernet 0/1	开启/关闭	关闭

3.3.8 DNS 服务

域名系统（DNS，Domain Name System）是一种用于 TCP/IP 应用程序的分布式数据库，提供域名与 IP 地址之间的转换。通过域名系统，用户进行某些应用时，可以直接使用便于记忆的、有意义的域名，而由网络中的 DNS 服务器将域名解析为正确的 IP 地址。

设备支持通过配置域名服务实现如下两个功能：

- 域名服务器：设备通过 DNS 服务器进行动态域名解析。
- DNS 转发：设备作为 DNS 代理，在 DNS 客户端和 DNS 服务器之间转发 DNS 请求和应答报文，代替 DNS 客户端进行域名解析。

手动设置域名服务器，如果为空就使用拨号获得的 DNS。一般在 WAN 口使用静态 IP 的时候才需要设置此项。

表 3-3-12 域名服务器参数说明

参数名称	说明	缺省值
首选域名服务器	设备首先使用的 DNS 服务器	无
备选域名服务器	当首选 DNS 不能解析时，才会使用备选域名去解析	无

DNS 转发默认为开启状态。如果路由器开启了 DHCP 服务，那么就需要开启此服务，否则关闭此服务。您可以设置指定[域名 <=> IP 地址]对，将 IP 地址和域名相对应后，通过访问域名就可以访问对应的 IP。

表 3-3-13 DNS 转发参数说明

参数名称	说明	缺省值
启用 DNS 转发服务器	开启/关闭	启用
主机	设置指定 IP 地址<=>域名的域名名称	无
IP 地址 1	设置指定 IP 地址<=>域名的 IP 地址 1	无
IP 地址 2	设置指定 IP 地址<=>域名的 IP 地址 2	无



注意

开启 DHCP 功能后，会默认开启 DNS 转发功能并且不能关闭；要把 DNS 转发关闭就先要把 DHCP 服务器关闭了。

3.3.9 动态域名

DDNS 动态域名服务是将用户的动态 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传递把该主机的动态 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。也就是说 DDNS 捕获用户每次变化的 IP 地址，然后将其与域名相对应，这样其他上网用户就可以通过域名来进行交流。而最终客户所要记忆的全部，就是记住动态域名商给予的域名即可，而不用去管他们是如何实现的。

DDNS 采用客户端/服务器模式：DDNS 客户端：需要动态更新域名和 IP 地址对应关系的设备。Internet 用户通常通过域名访问提供应用层服务的服务器，如 HTTP、FTP 服务器。为了保证 IP 地址变化时，仍然可以通过域名访问这些服务器，当服务器的 IP 地址发生变化时，它们将作为 DDNS 客户端，向 DDNS 服务器发送更新域名和 IP 地址对应关系的 DDNS 更新请求。

DDNS 服务器：负责通知 DNS 服务器动态更新域名和 IP 之间的对应关系。接收到 DDNS 客户端的更新请求后，DDNS 服务器通知 DNS 服务器重新建立域名和服务器之间的对应关系，从而保证即使 DDNS 客户端的 IP 地址改变，Internet 用户仍然可以通过同样的域名访问 DDNS 客户端。

DDNS 功能是作为 DDNS 的客户端工具，需要与 DDNS 服务器协同工作。在使用该功能之前，需要先到对应网站如（www.3322.org）去申请注册一个域名。

IR900 的 DDNS 服务类型包括：DynAccess、QDNS(3322)-Dynamic、QDNS(3322)-Static、DynDNS-Dynamic、DynDNS-Static、NoIP、Custom。

表 3-3-14 动态域名参数说明

参数名称	说明	缺省值
方法名称	用户自定义方法名称，不能为空	无
服务类型	选择提供动态域名的服务商	无
Url	用户设置域名 URL 格式，如花生壳域名 URL 格式：http://username:password@ddns.oray.com/ph/update?&hostname=domain/	空
用户名	申请注册动态域名的用户名	无
密码	申请注册动态域名的密码	无
主机名称	申请注册动态域名的主机名称	无
更新间隔（分钟）	设备向 DDNS 服务器更新域名的间隔	60 分钟
指定接口的更新方法		
接口	用户选择指定接口，可选择：bridage1、cellular 1、fastethernet 0/1	cellular 1
方法	用户选择更新方法，与上述设置的方法名称一致	空

注意

- 一般使用 DDNS 服务时，应确保设备拨号获取的地址为公网地址。
- 服务类型选择“定制”时才能使用 URL 格式。

3.3.10 短信服务

配置短信功能，能够实现短信控制设备重启、设备连接网络、设备断开网络连接。手机号码配置为允许动作后点击<应用并保存>，就可以通过该手机号发送“reboot”指令重启设备，或者发送“cellular 1 ppp up/down”指令使设备重新拨号或断开。最多可配置 10 条短信访问控制用户。

表 3-3-15 短信服务参数说明

参数名称	说明	缺省值
启用	开启/关闭	关闭
模式	TEXT 和 PDU TEXT:是纯文本方式，可使用不同的字符集，从技术上说也可以用于发送中文短消息，但国内基本上不支持，主要用于欧美地区 PDU:可以时而用任何字符集，PDU 串表面上是一串 ASCII 码。	TEXT
查询间隔	当开启短信服务时设备按照设置的时间间隔去读取 SIM 卡短信，0 表示禁用	120

短信访问控制		
ID	用户自定义 ID	1
动作	允许和拒绝 允许：设备响应被允许手机号码发送的指令，执行相关指令 拒绝：设备不响应被拒绝手机号码发送的指令，不执行相关指令	允许
手机号码	短信访问控制的手机号码	无
DI 通知短信	点选启用 DI 通知短信 使能 DI 短信通知后，IO 接口状态发生变化时会给该号码发送短信通知	禁用



注意

IR900 设备短信功能不支持中文，只支持英文和数字。

3.4 链路备份

为了保持网络的稳定性，在设备组成的网络环境中，通常都使用一些备份连接，以提高网络的健壮性、稳定性，这里的备份连接也称为备份链路或者冗余链路。

3.4.1 SLA

InHand SLA 基本原理：1.对象跟踪：对指定对象的可达性进行跟踪。2.SLA probe：对象跟踪功能可使用 InHand SLA 向对象发出不同类型的探测。3.使用路由映射表的基于策略的路由：将跟踪结果与路由进程关联起来。4.使用静态路由和跟踪选项。

SLA 配置步骤

第一步：定义一个或多个 SLA 操作（探测）。

第二步：定义一个或多个跟踪(Track)对象，以跟踪 SLA 操作的状态 。

第三步：定义与跟踪对象相关联的措施。

表 3-4-1 SLA 参数说明

参数名称	说明	缺省值
标识	SLA 的索引或 ID，用户自定义也可自动生成 最多可添加 10 条 SLA	1
类型	探测的类型，默认为 icmp-echo，用户不可更改 Icmp-echo 数据包来探测主机地址是否存活，通过简单发送一个 ICMP-ECHO（Type8）数据包到目标主机，如果 ICMP-ECHO-Reply（ICMPtype0）数据包接收到，说明主机是存活状态	icmp-echo
目的地址	被探测的 IP 地址	无
数据大小	用户自定义数据大小，合法值：0-1000	56
探测间隔	用户自定义探测间隔，合法值：1-608400（秒） 设备按照设置的探测间隔定时发送 ICMP 探测	30
超时（毫秒）	用户自定义，合法值：1-300000（毫秒） 设备发送 ICMP 探测后在配置的超时时间内没有收到返回包认为探测失败，进行下一次探测。	5000
次数	用户自定义，即探测失败多少次为链路故障，合法值：1-1000（次） 当达到配置的探测次数后，认为 SLA 探测失败，这时 SLA 状态为 DOWN 状态。	5
生命周期	默认为 forever（即配置后永远生效），用户不可更改	forever

3.4.2 Track 模块

Track 的用途是实现联动功能。联动功能由应用模块、Track 模块和监测模块三部分组成。

联动功能是指通过建立联动项，实现不同模块之间的联动，即由检测模块通过 Track 模块触发应用模块执行某种操作。检测模块负责对链路状态、网络性能等进行探测，并通过 Track 模块将探测结果通知给应用模块。应用模块感知到网络状态的变化后，及时进行相应的处理，从而避免通信中断或服务质量的降低。

Track 模块位于应用模块和监测模块之间，主要功能是屏蔽不同监测模块的差异，为应用模块提供统一的接口。

Track 模块与监测模块联动：

用户通过配置，建立 Track 模块和监测模块之间的联动关系。监测模块负责对接口状态、链路状态等进行探测，并将探测结果通知给 Track 模块，以便及时改变 Track 项的状态：

- 如果探测成功，则对应 Track 项的状态为 Positive
- 如果探测失败，则对应 Track 项的状态为 Negative

Track 模块与应用模块联动：

用户通过配置，建立 Track 模块和应用模块之间的联动关系。Track 项的状态发生变化后，Track 模块将通知应用模块进行相应的处理。目前，可以与 Track 模块实现联动功能的应用模块包括： VRRP、静态路由、策略路由、接口备份。

在某些情况下，Track 项状态发生变化后，如果立即通知应用模块，则可能会由于路由无法及时恢复等原因，导致通信中断，所以用户可以在配置 Track 项状态发生变化时，延迟一定的时间通知应用模块。

表 3-4-2 Track 模块参数说明

参数名称	说明	缺省值
标识	Track 的索引或 ID，用户自定义也可自动生成，最多可创建 10 条	1
类型	用户可选择：sla 或 interface	sla
SLA 标识	定义过的 SLA 的索引或 ID 类型选择为 interface 时，此项不可用	1
接口	用户可选择的接口有：bridge 1、cellular 1、fastethernet 0/1 类型选择为 sla 时，此项不可用	cellular 1
异常状态延时	当接口或 sla 状态为 DOWN 时，需要多久 track 才显示异常。 0 表示立即显示，单位：秒	0
正常状态延时	当故障恢复时，可根据设置的时间(0 代表立即切换)，延迟切换，而不是立即切换	0

3.4.3 VRRP

VRRP（虚拟路由冗余协议）缺省路由为用户的配置操作提供了方便，但是对缺省网关设备提出了很高的稳定性要求。通常，同一网段内的所有主机都设置一条相同的、以网关为下一跳的缺省路由。当网关发生故障时，本网段内所有以网关为缺省路由的主机将无法与外部网络通信。

增加出口网关是提高系统可靠性的常见方法，此时如何在多个出口之间进行选路就成为需要解决的问题。VRRP 虚拟路由器冗余协议将可以承担网关功能的一组路由器加入到备份组中，形成一台虚拟路由器，由 VRRP 的选举机制决定哪台路由器承担转发任务，局域网内的主机只需将虚拟路由器配置为缺省网关。

VRRP 将局域网内的一组路由器划分在一起，由多个路由器组成，功能上相当于一台虚拟路由器。根据不同网段的 VLAN 接口 IP，可以虚拟成多个虚拟路由器。每个虚拟路由器都有一个 ID 号，最多可以虚拟 255 个。

VRRP 具有以下特点：

- 虚拟路由器具有 IP 地址，称虚拟 IP 地址。局域网内的主机仅需要知道这个虚拟路由器的 IP 地址，并将其设置为缺省路由的下一跳地址。
- 网络内的主机通过这个虚拟路由器与外部网络进行通信。
- 组内路由器根据优先级，选举出一个路由器，承担网关功能。其他路由器作为 Backup 路由器，当网关路由器发生故障时，取代网关路由器继续履行网关职责，从而保证网络内的主机不间断地与外部网络进行通信。

VRRP 的监视接口功能更好地扩充了备份功能：不仅能在某路由器的接口出现故障时提供备份功能，还能在路由器的其它接口（如连接上行链路的接口）不可用时提供备份功能。

当连接上行链路的接口处于 Down 或 Removed 状态时，路由器主动降低自己的优先级，使得备份组内其它路由器的优先级高于这个路由器，以便优先级最高的路由器成为网关，承担转发任务。

表 3-4-3 VRRP 参数说明

参数名称	说明	缺省值
启用	启用/关闭	启用
虚拟路由器 ID	用户自定义虚拟路由器 ID，合法值：1-255	无
接口	设置虚拟路由器的接口，用户可选择：bridge 1、fastethernet 0/1	无
虚拟 IP 地址	设置虚拟路由器 IP 地址	无
优先级	VRRP 优先级的取值范围为 0 到 255（数值越大表明优先级越高），优先级越高，则越有可能成为网关路由器	100
通告间隔	虚拟 IP 组内路由器之间的心跳报文发送时间间隔	1
抢占模式	抢占模式下，路由器一旦发现自己的优先级比当前的网关路由器的优先级高，就会对外发送 VRRP 通告报文。导致重新选举网关路由器，并最终取代原有的网关路由器。相应地，原来的网关路由器将会变成 Backup 路由器	启用
Track 标识	跟踪探测，定义过的 Track 的索引或 ID	无

3.4.4 接口备份

接口备份是指同一台设备的指定接口之间形成主-备份关系，当某个接口出现故障或带宽不足而导致业务传输无法正常进行时，可以将流量快速的切换到备份接口，由备份接口来承担业务传输或分担网络流量，从而提高了数据设备通信的可靠性。

当主接口链路状态由 up 转为 down 后，系统不立即切换到备份接口链路而是等待一个预先设置好的延时。若超过延时后主接口状态仍为 down，系统才切换到备份接口链路。若在延时时间段中，主接口状态恢复正常则不进行切换。

当主接口链路状态由 down 转为 up 后，系统不立即切换回主接口而是等待一个预先设置好的延时。若超过延时后主接口状态仍为 up，系统才切换回主接口。若在延时时间段中，主接口状态再次转为 down 则不进行切换。接口备份时，主接口和备份接口不能同时存在。

表 3-4-4 接口备份参数说明

参数名称	说明	缺省值
主接口	正在使用的接口，用户可选择：bridge1、cellular1、fastethernet0/1	cellular 1
备份接口	等待切换的接口，用户可选择：bridge1、cellular1、fastethernet0/1	cellular 1
启动延时	设置等待多长时间启动跟踪探测策略生效，合法值：0-300	60
Up 延时	当主接口由探测失败转换为探测成功时，可根据设置的时间(0 代表立即切换)，延迟切换，而不是立即切换，合法值：0-180	0
Down 延时	当主接口由探测成功转换为探测失败时，可根据设置的时间(0 代表立即切换)，延迟切换，而不是立即切换，合法值：0-180	0
Track 标识	跟踪探测，定义过的 Track 的索引或 ID。注：接口备份和 track 意识使用的时候，如探测地址不通后，主接口并不 down。	无

3.5 路由

路由是指分组从源到目的地时，决定端到端路径的网络范围的进程。路由工作爱 OSI 参考模型第三层的数据包转发设备。路预期通过转发数据包来实现网络互连。路由器根据收到数据包中的网络层地址以及路由器内部维护的路由表决定输出端口以及下一跳地址，重写链路层数据包头实现转发数据包。路由器通过动态维护路由表来反映当前的网络拓扑，并通过网络上其他路由器交换链路信息来维护路由表。

路由包含静态路由、动态路由、组播路由共 3 模块。

3.5.1 静态路由

静态路由需要手工设置，设置后，去往指定目的地的报文将按照您指定的路径进行转发。用户一般不需要设置此项。

表 3-5-1 静态路由参数说明

参数名称	说明	缺省值
目的网络	输入需要到达的目的 IP 地址	0.0.0.0
子网掩码	输入需要到达的目的地址的子网掩码	0.0.0.0
接口	数据到达目的网络使用的接口，用户可选择：cellular 1、bridge 1、fastethernet 0/1	cellular 1
网关	输入数据在到达目的地址前，需要经过的下一个路由器 IP 地址	无
距离	即优先权，数值越小优先级越高	255
Track 标识	Track 的索引或 ID	无

3.5.2 动态路由

用于自治系统（AS）内部的网关协议有开放式最短路径优先（OSPF）协议和寻路信息协议（RIP）。

1） RIP

RIP 主要用于规模较小的网络中。RIP 使用跳数来衡量到达目的地址的距离，称为度量值。路由器到与它直接相连网络的跳数为 0，通过一个路由器可达的网络的跳数为 1，其余依此类推。为限制收敛时间，RIP 规定度量值取 0～15 之间的整数，大于或等于 16 的跳数被定义为无穷大，即目的网络或主机不可达。为提高性能，防止产生路由环路，RIP 支持水平分割功能。RIP 还可引入其它路由协议所得到的路由。

在 RFC1058 中规定，RIP 受三个定时器的控制，分别是：Period update 定时器、Timeout 定时器和 Garbage-Collection 定时器。

每个运行 RIP 的路由器管理一个路由数据库，该路由数据库包含了到所有可达目的地的路由项，这些路由项包含下列信息：

- 目的地址：主机或网络的 IP 地址。
- 下一跳地址：为到达目的地，需要经过的本路由器相邻路由器的接口 IP 地址。
- 出接口：本路由器转发报文的出接口。
- 度量值：本路由器到达目的地的开销。
- 路由时间：从路由项最后一次被更新到现在所经过的时间，路由项每次被更新时，路由时间重置为 0。

RIP 有两个不同的版本，RIPv1 和 RIPv2 其主要区别如下：

- RIPv1 有类路由协议，RIPv2 无类路由协议
- RIPv1 不支持 VLSM，RIPv2 支持 VLSM
- RIPv1 没有认证功能，RIPv2 支持认证，并且有明文和 MD5 两种认证
- RIPv1 没有手工汇总的功能，RIPv2 可以在关闭自动汇总的前提下，进行手工汇总
- RIPv1 使用广播更新，RIPv2 通过组播进行更新
- RIPv1 对路由没有标记的功能，RIPv2 可以对路由打标机（tag），标记用于过滤和做策略
- RIPv1 发送的 updata 最多可以携带 25 条路由条目，RIPv2 在有认证的情况下最多只能携带 24 条路由
- RIPv1 发送的 updata 包里没有 next-hop 属性，RIPv2 有 next-hop 属性，可以用于路由更新的重定
- RIPv1 定时更新，每隔 30 秒更新一次，RIPv2 采用了触发更新机制来急速路由计算

表 3-5-2 RIP 参数说明

参数名称	说明	缺省值
启用	启用/关闭	关闭
更新定时器	定义了发送路由更新的时间间隔，合法值：5-2147483647，单位：秒	30 秒
超时定时器	定义路由老化时间。如在老化时间内没有收到关于某条路由的更新报文，则该条路由在路由表中的度量值将会被设置为 16。 合法值：5-2147483647，单位：秒	180 秒

清除定时器	定义一条路由从度量值变为 16 开始，直到它从路由表里被删除所经过的时间。在 Garbage-Collect 时间内，RIP 以 16 作为度量值向外发送这条路由的更新，如 Garbage-Collect 超时，该路由仍没有得到更新，则该路由将从路由表中被彻底删除 合法值：5-2147483647	120 秒
版本	RIP 的版本号，用户可选择：默认、v1、v2	~~V2~~ 默认
网络	网络号即网段中的第一个 IP 地址和子网掩码	无
高级选项		
缺省信息发布	启用后将发布缺省信息	关闭
缺省度量	本路由器到达目的地的缺省开销 合法值：1-16，16 表示不可达	1
重定向直连路由	点选启用	关闭
重定向路由度量	启用重定向直连路由后，此项用于设置重定向直连路由的路由度量 合法值：0-16	空
重定向静态路由	点选启用	关闭
重定向路由度量	启用重定向静态路由后，此项用于设置重定向静态路由的路由度量 合法值：0-16	空
重定向动态路由	点选启用	关闭
重定向路由度量	启用重定向动态路由后，此项用于设置重定向动态路由的路由度量 合法值：0-16	空
距离/度量管理		
距离	设置学习到的某条 RIP 路由的管理距离	120
IP 地址	需要设置的 RIP 路由的 IP 地址	空
子网掩码	需要设置的 RIP 路由的子网掩码	空
访问列表名	设置某条路由引用的访问策率	空
重定向路由度量	更改接口收到或发出路由的度量值	空
出/入过滤策略	用户可选择：in/out In:进入路由器的时候访问列表配置生效 Out:出路由器器的时候访问列表配置生效	空
接口	用户可选择：bridge 1、cellular 1、fastethernet 0/1	空
访问列表名	用户配置的路由策率的访问列表名称	空
路由过滤策略		
策略类型	用户可选择：access-list、prefix-list	access-list
策略名	用户配置的前缀列表名	空
出/入过滤策略	用户可选择：in、out	in
接口	用户可选择：bridge 1、cellular1、fastethernet 0/1	空
过滤发送：只允许默认路由接口	点选启用	禁用

被动接口		
被动接口	用户可选择：bridge 1、cellular1、fastethernet 0/1	空
接口		
接口	用户可选择：bridge 1、cellular1、fastethernet 0/1	空
RIP 发送版本	用户可选择：默认、v1、v2	默认
RIP 接收版本	用户可选择：默认、v1、v2	默认
水平分割/毒性翻转	用户可选择：split-horizon、disabled	空
认证方式	用户可选择：text、md5	空
密钥	RIPV2 报文交互时候使用的验证密钥	空
邻居		
IP 地址	手动配置的 RIP 邻居地址	空
网络		
IP 地址	RIP 需要发布出去接口的 IP 地址	空
子网掩码	RIP 需要发布出去接口的子网掩码	空

2） OSPF

OSPF 开放最短路径优先协议是 IETF 组织开发的一个基于链路状态的内部网关协议。

路由器 ID 号

一台路由器如果要运行 OSPF 协议，必须存在 Router ID。Router ID 可以手工配置，如果没有配置 Router ID，系统会从接口的 IP 地址中自动选择一个作为 Router ID。

其选择顺序如下：

- 如果配置了 Loopback 接口地址，则选择最后配置的 Loopback 接口的 IP 地址作为 Router ID；
- 如果没有配置 LoopBack 接口地址，则选其他接口中 IP 地址最大的为 Router ID

OSPF 的协议报文有五种报文类型：

- HELLO 报文
- DD 报文（数据库描述报文）
- LSR 报文（链路状态请求报文）
- LSU 报文（链路状态更新报文）
- LSAck 报文（链路状态确认报文）

邻居和邻接

OSPF 路由器启动后，便会通过 OSPF 接口向外发送 Hello 报文。收到 Hello 报文的 OSPF 路由器会检查报文中所定义的参数，如果双方一致就会形成邻居关系。形成邻居关系的双方不一定都能形成邻接关系，这要根据网络类型而定。只有当双方成功交换 DD 报文，交换

LSA 并达到 LSDB 的同步之后，才形成真正意义上的邻接关系。LSA 是对路由器周围网络拓扑结构的描述， LSDB 则是对整个网络的拓扑结构的描述。

表 3-5-3 OSPF 参数说明

参数名称	说明	缺省值
启用	启用/关闭	关闭
Router ID	始发该 LSA 的路由器的 ID	无
高级选项		
ABR 类型	用户可选择：cisco、ibm、standard、shortcut	cisco
RFC1583 兼容性	启用/关闭	关闭
OSPF 可选 LSA	启用/关闭 LSA:链路状态广播，是链接状态协议使用的一个分组，它包括有关邻居和本通道成本的信息。LSA 被路由器接受用于维护它们的路由选择表。	关闭
SPF 延时时间	设置 OSPF SPF 计算的延时时间 合法值：0-600000，单位：毫秒	200
SPF 初始化时间	设置 OSPF SPF 的初始化时间 合法值：0-600000，单位：毫秒	1000
SPF 最大时间	设置 OSPF SPF 的最大时间 合法值：0-600000，单位：毫秒	10000
参考带宽	合法值：1-4294967，单位：兆比特	100
接口		
接口名称	需要配置 OSPF 参数的接口，用户可选择：bridge 1、cellular1、fastethernet 0/1	无
网络	选择 OSPF 网络类型，用户可选择：Broadcast、NBMA、Point-to-Multipoint、Point-to-Point	Broadcast
Hello 定时器	发送 Hello 报文的时间间隔。如果相邻两台路由器的 Hello 间隔时间不同，则不能建立邻居关系 合法值：1-65535	10
Dead 定时器	失效时间。如果在此时间内未收到邻居发来的 Hello 报文，则认为邻居失效。如果相邻两台路由器的失效时间不同，则不能建立邻居关系 合法值：1-65535	40
重传 LSA 延迟定时器	路由器向它的邻居通告一条 LSA 后，需要对方进行确认。若在重传间隔时间内没有收到对方的确认报文，就会向邻居重传这条 LSA 合法值：3-65535	5
传送 LSA 延迟定时器	OSPF 报文在链路上传送时也需要花费时间，所以 LSA 的老化时间（age）在传送之前要增加一定的延迟时间，在低速链路上需要对该项配置进行重点考虑 合法值：1-65535	1
接口高级选项		
接口名称	用户可选择：bridge 1、cellular1、fastethernet 0/1	空

被动接口	开启被动接口后，接口只接收不发送 ospf 报文	关闭
接口开销值	设置接口运行 OSPF 时的开销值。缺省情况下，OSPF 会依据接口的带宽自动计算开销值。	10
协议优先级	配置路由器接口的 OSPF 优先级	10
认证方式	设置 OSPF 区域所使用的认证模式。 如果选择 Simple 认证模式，则还需要配置简单认证密码以及对该密码再进行一次确认。 如果选择 MD5 认证模式，则还需要配置 MD5 键值和密码以及对该密码再进行一次确认。	空
密钥 ID	只选项 MD5 生效，范围 1-255	空
密钥	Ospf 报文交换时的验证密钥	空
网络		
IP 地址	本地网络的 IP 地址	无
子网掩码	本地网络 IP 地址的子网掩码	无
域 ID	始发 LSA 的路由器所在的区域 ID	无
域		
域 ID	设置 OSPF 区域的 ID 号	空
域	设置 OSPF 区域为 Stub 或 NSSA 区域。 骨干区域（区域 ID 为 0.0.0.0）不能被设置为 Stub 或 NSSA 区域。	空
禁止路由汇总	路由汇总是把一组路由汇聚为一个单个的路由广播。路由汇聚的最终结果和最明显的好处是缩小网络上的路由表的尺寸。	关闭
认证方式	用户可选择：simple password、md5	空
域高级选项-域地址汇总		
域 ID	接口运行 OSPF 时所属的区域的 ID 号	空
IP 地址	设置接口所在网段 IP 地址。	空
子网掩码	设置接口所在网段子网掩码	空
禁止域间路由信息	禁止 ospf 域内路由信息在不同域之间路由	禁止
接口开销值	合法值：0-16777215	空
域高级选项-域过滤策略		
域 ID	选择过滤策略应用的 ospf 域号	0
路由过滤策略	用户可选择：import、export、filter-in、filter-out	空
访问列表名	根据配置的访问列表名来控制域的路由过滤。只有在配置的访问列表里的路由才生效。	空
域高级选项-域间虚链路		
域 ID	设置 OSPF 区域的 ID 号	空
ABR 地址	ABR：连接多个区域的路由器是 ABR，配置 ABR 与此域连接的接口地址	空
认证方式	用户可选择：simple password、md5	空
密钥 ID	只选项 MD5 生效，范围 1-255	空
密钥	Ospf 报文交换时的验证密钥	空

Hello 定时器	设置接口发送 Hello 报文的时间间隔。合法值:1-65535	10
Dead 定时器	发送 hello 报文的超时时间，合法值:1-65535	40
重传 LSA 延迟定时器	当 LSA 传输失败后重新发送 SLA 的时间。合法值:1-65535	5
传送 LSA 延迟定时器	SLA 发送时的延时时间，合法值:1-65535	1
路由重定向		
路由重定向类型	用户可选择：connected、static、rip	connected
指定重定向路由度量	设备发送重定向路由时指定的度量值	空
外部路由的类型	设置引入的外部路由的路由类型。其中， l Type1 外部路由表示此类路由的可信度较高，OSPF 协议认为计算出的外部路由的开销与自治系统内部的路由开销是相当的，并且和 OSPF 自身路由的开销具有可比性。即 Type1 外部路由的开销=本路由器到相应的 ASBR 的开销+ASBR 到该路由目的地址的开销。 l Type2 外部路由表示此类路由的可信度较低，OSPF 协议认为从 ASBR 到自治系统之外的开销远远大于在自治系统之内到达 ASBR 的开销。所以，OSPF 计算路由开销时只考虑 ASBR 到自治系统之外的开销，即 Type2 外部路由的开销=ASBR 到该路由目的地址的开销。	无
路由映射	目前为不可用状态	空
重定向高级选项		
总是重定向默认路由	设备启动后发送重定向默认路由	关闭
默认路由重定向度量值	发送重定向默认路由的度量值	空
默认路由重定向度量类型	用户可选择：1、2	空
指定缺省度量	路由重发布时候的默认度量	0
重定向高级选项--管理距离		
域类型	用户可选择：inter-area、external	Inter-area
距离	设置域学习的的 ospf 路由距离	空

3）路由策略

表 3-5-4 路由策略参数说明

参数名称	说明	缺省值
访问控制列表		
访问列表名	用户自定义	无
行动	可选 permit 和 deny	permit
任意地址	点选后即任意地址，不需要再配 IP 地址和子网掩码	禁用

IP 地址	用户自定义	无
子网掩码	用户自定义	无
前缀列表		
前缀列表名	用户自定义	无
序号	一个前缀列表名可以配置多个规则，一个规则对应一个序号	无
行动	可选 permit 和 deny	permit
任意地址	点选后即任意地址，不需要再配 IP 地址、子网掩码、大于前缀长度、小于前缀长度	禁用
IP 地址	用户自定义	无
子网掩码	用户自定义	无
大于前缀长度	填写子网掩码的网络标示位长度，限制 IP 段的最小 IP 地址 合法值：0-32	无
小于前缀长度	填写子网掩码的网络标示位长度，限制 IP 段的最大 IP 地址 合法值：0-32	无

3.5.3 组播路由

组播路由建立了一个从数据源端到多个接收端的无环数据传输路径，即构建组播分发树。组播路由协议用于建立和维护组播路由，并正确、高效地转发组播数据包。

基本设置主要是定义配置组播路由的数据源端。

表 3-5-5 基本设置参数说明

参数名称	说明	缺省值
启用	启用/关闭	关闭
源网络	源网络的 IP 地址	无
子网掩码	源网络的子网掩码	255.255.255.0
接口	源网络的接口 用户可选择：bridge 1、cellular1、fastethernet 0/1	Bridge 1

IGMP 是因特网协议家族中的一个组播协议，用于 IP 主机向任一个直接相邻的路由器报告他们的组成员情况。它规定了处于不同网段的主机如何进行多播通信，其前提条件是路由器本身要支持多播。它用来在 Ip 主机和与其直接相邻的组播路由器之间建立、维护组播组成员关系。IGMP 定义了一个网段内主机与组播路由器之间如何维护组成员信息。

在组播通信模型中，发送者不关注接收者的位置信息，只要将数据发送到约定的目的地址，而接收者的信息由网络设备去收集和维护。IGMP 就是这样一个在接收者网段使用的主机对路由器的信令机制。IGMP 通知路由器有关组成员的信息，路由器使用 IGMP 来获知与路由器相连的子网上是否存在组播组的成员。

组播路由协议作用：

- 发现上游接口，离源最近的接口。因为组播路由协议只关心到源的最短路径。
- 通过（S，G）对来决定真正的下游接口，当所有的路由器都知道了他们的上下游接口，那么一颗多播树就已经建立完成。根是源主机直连的路由器，而树枝是通过 IGMP 发现有组员的子网直连的路由器。
- 管理多播树。单播路由只需要知道下一跳的地址，就可以进行报文的转发。而组播，是把从一个由源产生的报文发送给一组。

表 3-5-6 IGMP 参数说明

参数名称	说明	缺省值
上联接口		
上连接口	连接上一级网络设备的接口 用户可选择：bridge 1、cellular1、fastethernet 0/1	bridge 1
下连接口列表		
下连接口	连接下终端设备的接口 用户可选择：bridge 1、cellular1、fastethernet 0/1	bridge 1
上连接口	连接上一级网络设备的接口 用户可选择：bridge 1、cellular1、fastethernet 0/1	bridge 1

3.6 防火墙

路由器的防火墙功能实现了根据报文的内容特征(比如:协议类型、源/目的 IP 地址等),来对入站方向(从因特网发向局域网的方向)和出站方向(从局域网发向因特网的方向)的数据流执行相应的控制,保证了路由器和局域网内主机的安全运行。

3.6.1 访问控制(ACL)

ACL 即访问控制列表,通过配置一系列匹配规则,对指定数据流(如限定的源 IP 地址、账号等)执行允许或禁止通过,达到对网络接口数据的过滤。当路由器的端口接收到报文后,即根据当前端口上应用的 ACL 规则对报文的字段进行分析,在识别出特定的报文之后,根据预先设定的策略允许或禁止相应的数据包通过。

ACL 通过一系列的匹配条件对数据包进行分类,这些条件可以是数据包的源 MAC 地址、目的 MAC 地址、源 IP 地址、目的 IP 地址、端口号等。

由 ACL 定义的数据包匹配规则,也可以被其它需要对流量进行区分的功能引用。

表 3-6-1 访问控制参数说明

参数名称	说明	缺省值
默认处理策略	可选择放行、阻止	放行
访问控制列表		
ID	输入 ACL 规则编号,范围 1-199	无
动作	选择允许或拒绝报文通过	允许
协议	访问控制协议	ip
源 IP 地址	输入 ACL 规则匹配报文的源地址,(不配置表示 any,代表所有网络)	无
源地址反掩码	输入 ACL 规则匹配报文的源地址反掩码	无
源端口	只有协议类型选择为 TCP 或 UDP 时,才可以指定源端口号。any 表示 TCP/UDP 报文的任何源端口都匹配。	~~any~~
目的 IP 地址	输入 ACL 规则匹配报文的目的地址,(不配置表示 any,代表所有网络)	无
目的地址反掩码	输入 ACL 规则匹配报文的源地址反掩码	无
目的端口	只有协议类型选择为 TCP 或 UDP 时,才可以指定目的端口号。any 表示 TCP/UDP 报文的任何目的端口都匹配	any
已建立的连接	表示控制已建立 TCP 连接的报文,未建立连接的 TCP 报文不控制	禁用
记录日志	点选启用,启用后系统会记录关于访问控制方面的日志	禁用
片段	控制数据包从接口发送出去时被分片的报文	
说明	便于记录访问控制各项参数意义	无

网络接口列表		
接口名称	用户可选择：bridge 1、cellular1、fastethernet 0/1	bridge 1
规则	选择入站、出站和管理规则，可选择：none、100	none

3.6.2 网络地址转换（NAT）

NAT 可以实现局域网内的多台主机通过 1 个或多个公网 IP 地址接入因特网，即用少量的公网 IP 地址代表较多的私网 IP 地址，节省公网的 IP 地址。

表 3-6-2 网络地址转换（NAT）参数说明

参数名称	说明	缺省值
动作	**SNAT**：源地址转换：是将 IP 数据包的源地址转换成另外一个地址。一般用于从路由器内部发往外部的数据 **DNAT**：目的地址转换：是将 IP 数据包的目的地址转换成另外一个地址。一般用于从路由器外部发往内部的数据 **1:1NAT**：1 对 1 转换 IP 地址。	SNAT
源网络	Inside：内部地址 Outside：外部地址	Inside
转换类型	选择网络地址转换的转换类型 用户可选择：IP to IP IP to INTERFACE IP PORT to IP PORT ACL to INTERFACE ACL to IP	IP toIP
匹配 访问控制列表	当数据转换时根据配置的 ACL 来转换地址	ACL:100
转换成的地址	用户可选择：cellular 1、bridge 1、fastethernet 0/1	cellular 1
描述信息	对一条 NAT 的作用的描述	空
内部网络接口		
ID	配置的 ID 标识	1 和 2
接口	定义的内部网络接口	ID1 对应：fastethernet 0/1 ID2 对应：bridge 1
外部网络接口		
ID	配置的 ID 标识	1
接口	定义的外部网络接口	cellular 1

注意

网络地址转换规则是将 ACL 应用于地址池，只有匹配该 ACL 的地址才进行转换。

说明

私网 IP 地址是指内部网络或主机的 IP 地址，公网 IP 地址是指在因特网上全球唯一的 IP 地址。RFC 1918 为私网预留出了三个 IP 地址块，如下：

A 类：10.0.0.0～10.255.255.255

B 类：172.16.0.0～172.31.255.255

C 类：192.168.0.0～192.168.255.255

上述三个范围内的地址不会在因特网上被分配，因此可以不必向运营商或注册中心申请而在公司或企业内部自由使用。

3.6.3 MAC-IP 绑定

MAC-IP 绑定，又叫做 ARP 绑定。ARP 绑定后，只有 MAC 地址和 ip 地址都与之前设置的参数相同时才可以正常联网。MAC-IP 绑定主要用于防范局域网内的 ARP 攻击，也可以防止用户随意接入设备，提高网络安全。

当防火墙基本设置中的默认处理策略设为禁止时，只有 MAC-IP 规定的主机才能访问外网。

表 3-6-3 MAC-IP 绑定参数说明

参数名称	说明	缺省值
MAC 地址	设置绑定的 MAC 地址	00:00:00:00:00:00
IP 地址	设置绑定的 IP 地址	空
说明	便于记录每条 MAC-IP 地址绑定规则的意义	空

注意

只有防火墙的默认处理策略设为阻止时，设置的 MAC-IP 功能才能生效。

3.7 QoS

QoS 可以对网络流量进行调控，避免并管理网络拥塞，减少报文丢包率。某些应用在给用户带来方便的同时，也占用了大量的网络带宽。为了保证局域网内所有用户都能正常使用网络资源，可以通过 IP 流量限制功能对局域网内指定主机的流量进行限制。

QoS 支持为用户提供专用带宽，为不同业务提供不同的服务质量等，完善了网络的服务能力。用户可以根据业务需要保证不同业务的不同需求，如保证时间敏感业务的低时延、多媒体业务的带宽保证等。

QoS 可以保证高优先级数据帧的接收，并加速高优先级数据帧的发送，确保关键业务不会受到网络拥塞的影响。IR900 支持 4 个服务级别，可以根据数据帧的接收端口、Tag 优先级及 IP 优先级决定其服务级别。

表 3-7-1 流量控制参数说明

参数名称	说明	缺省值
类		
名称	用户自定义流量控制类名称	无
任意报文	点选启用，启用后对任意报文都进行流量控制	禁用
源地址	流量控制的源地址对（空代表 any）	无
目的地址	流量控制的目的地址对（空代表 any）	无
协议	点选协议类型，用户可选择：icmp、igmp、tcp、udp、gre、esp、ah、ospf、vrrp、l2tp	无
策略		
名称	用户自定义新建流策略的名称。	无
类	选择需要应用的类名称	无
保证带宽 Kbps	对每条流量保留的最小带宽，当发生拥塞时候，每条流保留的最小带宽。合法值：1-100000	无
最大带宽 Kbps	每条流量的最大能保证的带宽，当发生阻塞时，实际数据不能超过设置的最大带宽。合法值：1-100000	无
本地优先级	指定匹配报文优先级的级别，包括：用户可选择：highest、high、Medium、low、lowest	无
应用 Qos		
接口	指定策略应用的接口，用户可选择：cellular 1、bridge 1、fastethernet 0/1	无
最大输入带宽 Kbps	用户自定义，但要大于输入策略的最大带宽 合法值：1-100000	无
最大输出带宽 Kbps	用户自定义，但要大于输出策略的最大带宽 合法值：1-100000	无
输入策略	表示将策略应用到接口的入方向。	无
输出策略	表示将策略应用到接口的出方向	无



注意

- 目前 IR900 配置的 QOS 策率只有对输出起作用。
- 只有当实际流量大于配置的最大输出带宽时，QOS 策率才启作用。

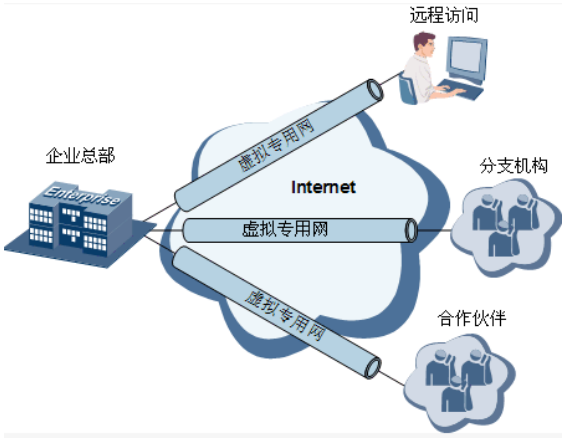
3.8 VPN

VPN 是指依靠 Internet 服务提供商 ISP 和网络服务提供商 NSP 在公共网络中建立的虚拟私人专用通信网络。“虚拟”主要指这种网络是一种逻辑上的网络。

VPN 具有以下两个基本特征：

- 专用（Private）： VPN 资源不被网络中非该 VPN 的用户所使用；且 VPN 能够提供足够的安全保证，确保 VPN 内部信息不受外部侵扰。
- 虚拟（Virtual）：VPN 用户内部的通信是通过公共网络进行的，而这个公共网络同时也可以被其他非 VPN 用户使用，VPN 用户获得的只是一个逻辑意义上的专网。这个公共网络称为 VPN 骨干网（VPN Backbone）。

通过 VPN 将远程用户、公司分支机构、合作伙伴同公司总部网络建立可信的安全连接，实现数据的安全传输，如下图所示：



VPN 的基本原理

VPN 的基本原理是利用隧道技术，把 VPN 报文封装在隧道中，利用 VPN 骨干网建立专用数据传输通道，实现报文的透明传输。

隧道技术使用一种协议封装另外一种协议报文，而封装协议本身也可以被其他封装协议所封装或承载。对用户来说，隧道是其公共电话交换网 PSTN/综合业务数字网 ISDN 链路的逻辑延伸，在使用上与实际物理链路相同。

常用的隧道协议有 L2TP、PPTP、GRE、IPSec、MPLS 等。

3.8.1 IPSec

在 Internet 的传输中，绝大部分数据的内容都是明文传输的，存在很多潜在的危险，比

如：密码、银行帐户的信息被窃取、篡改，用户的身份被冒充，遭受网络恶意攻击等。网络中部署 IPSec 后，可对传输的数据进行保护处理，降低信息泄漏的风险。

IPSec 是 IETF 制定的一组开放的网络安全协议，在 IP 层通过数据来源认证、数据加密、数据完整性和抗重放功能来保证通信双方 Internet 上传输数据的安全性。减少泄漏和被窃听的风险，保证数据的完整性和机密性，保障了用户业务传输的安全。

IPSec 包括认证头协议 AH、封装安全载荷协议 ESP、因特网密钥交换协议 IKE，用于保护主机与主机之间、主机与网关之间、网关与网关之间的一个或多个数据流。其中，AH 和 ESP 这两个安全协议用于提供安全服务，IKE 协议用于密钥交换。

IPSec 通过在 IPSec 对等体间建立双向安全联盟，形成一个安全互通的 IPSec 隧道，来实现 Internet 上数据的安全传输。

表 3-8-1 IPSec 配置参数说明

参数名称	说明	缺省值
IKEv1 策略		
标识	用户自定义 IKEv1 策略标识	空
加密算法	用户可选择：3DES、DES、AES128、AES192、AES256 3DES: 使用三个 64bit 的 DES 密钥对明文进行加密 DES：使用 64bit 的密钥对一个 64bit 的明文块进行加密 AES: 使用 128bit、192bit 或 256bit 密钥长度的 AES 算法对明文进行加密	AES128
哈希算法	用户可选择：MD5、SHA1、SHA2-256、SHA2-384、SHA2-512 MD5：通过输入任意长度消息，产生128bit 的消息摘要。 SHA1：输入长度小于 bit 消息，产生 160bit 消息摘要。 SHA2-256：输出 256bit SHA2-384：输出 384bit SHA2-512：输出 512bit 相比：md5 计算速度快，SHA1 安全强度更高	SHA1
Diffie-Hellman 密钥交换	Diffie-Hellman 算法是一种公开密钥算法。通信双方在不传送密钥的情况下通过交换一些数据，计算出共享的密钥。加密的前提是交换加密数据的双方必须要有共享的密钥。IKE 的精髓在于它永远不在不安全的网络上直接传送密钥，而是通过一系列数据的交换，最终计算出双方共享的密钥。即使第三者（如黑客）截获了双方用于计算密钥的所有交换数据，也不足以计算出真正的密钥	Group2
生命周期	设置 IKE SA 的存活时间，在设置的存活时间超时前会提前协商另一个 SA 来替换旧的 SA。	86400
IKEv2 策略		
标识	用户自定义 IKEv2 策略标识	空
加密算法	用户可选择：3DES、DES、AES128、AES192、AES256 3DES: 使用三个 64bit 的 DES 密钥对明文进行加密	AES128

	DES：使用 64bit 的密钥对一个 64bit 的明文块进行加密 AES: 使用 128bit、192bit 或 256bit 密钥长度的 AES 算法对明文进行加密	
integrity	用户可选择：MD5、SHA1、SHA2-256、SHA2-384、SHA2-512 MD5：通过输入任意长度消息，产生128bit 的消息摘要。 SHA1：输入长度小于 bit 消息，产生 160bit 的消息摘要。 SHA2-256：输出 256bit SHA2-384：输出 384bit SHA2-512：输出 512bit	SHA1
Diffie-Hellman 密钥交换	Diffie-Hellman 算法是一种公开密钥算法。通信双方在不传送密钥的情况下通过交换一些数据，计算出共享的密钥。加密的前提是交换加密数据的双方必须要有共享的密钥。IKE 的精髓在于它永远不在不安全的网络上直接传送密钥，而是通过一系列数据的交换，最终计算出双方共享的密钥。即使第三者（如黑客）截获了双方用于计算密钥的所有交换数据，也不足以计算出真正的密钥	Group2
生命周期	设置 IKE SA 的存活时间，在设置的存活时间超时前会提前协商另一个 SA 来替换旧的 SA。	86400
IPSec 策略		
名称	设置 IPSec 策略的名称。 配置 IPSec 策略成功后，该参数不可修改。	空
封装	IPSec 协议中的 AH 协议定义了认证的应用方法，提供数据源认证和完整性保证；ESP 协 议定义了加密和可选认证的应用方法，提供数据可靠性保证 AH 认证头协议：提供数据源认证、数据完整性校验和报文防重放功能。发送端对 IP 头的不变部分和 IP 净荷进行离散运算，生成一个摘要字段。接收端根据接收的 IP 报文，对报文重新计算摘要字段，通过摘要字段的比较，判别报文在网络传输期间是否被篡改 ESP：ESP 封装安全载荷协议：除提供 AH 认证头协议的所有功能之外，还可对 IP 报文净荷进行加密。ESP 协议允许对 IP 报文净荷进行加密和认证、只加密或者只认证，ESP 没有对 IP 头的内容进行保护	ESP
认证方式	多种可选,用户可选择：MD5、SHA1、SHA2-256、SHA2-384、SHA2-512 MD5：通过输入任意长度消息，产生128bit 的消息摘要。 SHA1：输入长度小于 bit 消息，产生 160bit 的消息摘要。 SHA2-256：输出 256bit SHA2-384：输出 384bit SHA2-512：输出512bit	SHA1
IPsec 模式	IPSec 协议的封装模式 隧道模式：在原始 IP 报文头外封装一个 IPSec 报文头（AH 或 ESP），然后在最外层封装新的 IP 报文头，原 IP 报文被当作有效载荷的一部分受到 IPSec 的保护。隧道模式一般用在两个安全网关之间。在一个安全网关被加密的报文，只有到达另一个安全网关才能够被解密	隧道模式

	传输模式：传输模式：在 IP 报文头和上层协议报文头之间插入一个 IPSec 报文头（AH 或 ESP）。在这种模式下，原 IP 报文头不变，只是 IP 协议字段被改为 AH 或 ESP，并重新计算 IP 报文头校验和。传输模式适用于两台主机，或者是一台主机和一个安全网关之间的通讯	
IPSec 隧道配置-基本参数		
对端地址	设置对端 IKE 对等体的 IP 地址或域名（当 IR900 为 server 时配置为 0.0.0.0）	
接口名称	设置应用 IPSec 策略的接口，用户可选择 bridge 1、cellular1、fastethernet 0/1	Cellular 1
IKE 版本	设置 IKE 协议使用的版本号，支持 IKEv1 和 IKEv2。	IKEv1
IKEv1 策略	在 IKEv1 策略列表里定义过的策略标识	
IKEv2 策略	在 IKEv2 策略列表里定义过的策略标识	
IPsec 策略	在 IPsec 策略列表里定义过的策略标识	
协商模式	设置 IKEv1 的协商模式： 主模式：主模式将密钥交换信息与身份认证信息相分离。这种分离保护了身份信息，从而提供了更高的安全性。 野蛮模式：野蛮模式缺少身份认证，但可以满足某些特定的网络环境需求。如果无法预先知道发起者的地址、或者发起者的地址总在变化，而双方都希望采用预共享密钥认证方法来创建 IKE SA，就可以用野蛮模式。	主模式
认证方式	两种认证方式可选：共享密钥和数字证书 共享密钥：用户输入共享密钥 数字证书：用户需在证书管理页面导入相应的有效证书	共享密钥
共享密钥	IKE 使用预共享密钥的认证方法时，在 IKE 协商的两端，即本端设备和对端设备需要配置相同的认证字。	空
本地子网地址	IPESC 定义的感兴趣流中的源网络	空
对端子网地址	IPESC 定义的感兴趣流中的目的网络	空
IPSec 隧道配置-IKE 高级选项（第 1 阶段）		
本地标识	设置 IKE 协商中本端设备的身份类型： IP 地址：使用接口的 IP 地址作为本端的身份，和对端进行 IKE 协商，交互身份信息。 FQDN：使用字符串作为本端身份 User FQDN：使用全域名形式作为本端身份	IP 地址
对端标识	设置 IKE 协商中对端设备的身份类型： IP 地址：填写对端建立 IPsec 接口的地址 FQDN：设置 IKE 协商中对端设备身份使用的名称，需要和对端设备上设置的保持一致 User FQDN：与对端配置的全域名一致	IP 地址
IKE 连接检测（DPD）	设置是否启用对等体存活检测 DPD 功能。 DPD 是指 IKE 对等体间通过 DPD 消息检测对方的存活。	禁用

	DPD 超时时间：当接收端触发 DPD 查询，主动向对端发送请求报文进行检测，超过超时时间仍没有收到对端的 DPD 回应报文时，将删除此 IPsec SA。合法值：10-3600 单位：秒	0，建议参数 60
	DPD 重试间隔：用于 IPSec 邻居状态的检测时间间隔。 启动 DPD 功能后，当接收端在触发 DPD 的时间间隔内收不到对端的 IPSec 加密报文时，能够触发 DPD 查询，主动向对端发送请求报文，对 IKE 对等体是否存在进行检测 合法值：10-3600，单位：秒	0，建议参数 180
XAUTH	XAUTH 用户名，XAUTH 密码	空
IPSec 隧道配置-IPSec 高级选项（第 2 阶段）		
完美前向加密（PFS）	PFS 是一种安全特性，指一个密钥被破解，并不影响其他密钥的安全性，因为这些密钥间没有派生关系。IPSec 第二阶段的密钥是从第一阶段的密钥导出的，当第一阶段 IKE 密钥被窃取后，攻击者将可能收集到足够的信息来导出第二阶段 IPSec SA 的密钥，PFS 通过执行一次额外的 DH 交换，保证第二阶段密钥的安全。	禁用
IPsec SA 生命周期	设置 IPSec SA 的生存周期。IPSec 协商建立 SA 时，采用本端设置的生存周期和对端的生存周期中较小的一个。	3600 秒
IPsec SA 空闲超时时间	当 IPsec 建立成功后在配置的空闲时间内没有数据传输，则 IPSec SA 就会失效。IPSec SA 快要失效前，IPSec 协商建立新的 SA，这样在旧的 SA 失效前新的 SA 就已经准备好。	0 秒
IPSec 隧道配置-Tunnel 高级选项		
隧道启动方式	设置 IPsec 启用方式 自动连接：应用 IPSec 策略后，自动完成 IKE 的协商建立 IPSec 隧道。常用于客户端模式 仅响应连接：只会被动接收 Ipsec 请求，不会主动发起连接。常用于 server 模式 按需连接： 接口有 IPsec 定义的报文通过时，才完成 IKE 的协商，建立 IPSec 隧道。	自动连接
本地/远端发送证书规则	用户可选择：请求时发送证书、总是发送证书、不发送证书 使用证书建立 Ipsec 时，两端都必须知道对端的证书，并验证成功才能成功建立连接。 本地的证书一般都有保存，但对端的证书可能保存，可能没有保存(常见情况)；一般情况下，在 IPSEC 建立连接时，两端都会发送“请求证书”请求，当 ipsec 服务收到该请求后就会发送自己的证书到对端。 **总是发送证书**：有些 ipsec 服务不会发送“请求证书”请求，但是它的本地又没有保存对端的证书，那么对端就必须要配置成“总是发送证书”才能建立 Ipsec。 **请求时发送证书**：只有当对端发送请求时，才发送本地证书。 **不发送证书**：不管对端是否发送请求，本地都将把自己的证书发送到对端。	总是发送证书
ICMP 探测	探测服务器 / IPsec 探测的对端主机地址	空
	探测本地地址 / IPsec 保护流量的源地址	空

	探测间隔时间	设备发送 ICMP 探测报文的时间间隔	60 秒
	探测超时时间	在设置的 ICMP 探测超时时间内，没有收到 ICMP 响应包认为本次 ICMP 探测超时	5 秒
	探测最大重试次数	设置 ICMP 探测失败时的最大重试次数（达到最大次数后会重重新启动 IPsec 服务）	10 秒

表 3-8-2 IPSec 扩展参数说明

参数名称	说明	缺省值
基本参数		
名称	设置 IPsec Profile 的名称。	无
IKE 版本	设置 IKE 协议使用的版本号，支持 IKEv1 和 IKEv2。	IKEv1
IKEv1 策略	在 IKEv1 策略列表里定义过的策略标识	空
IKEv2 策略	在 IKEv2 策略列表里定义过的策略标识	
IPsec 策略	在 IPsec 策略列表里定义过的策略标识	空
协商模式	设置 IKEv1 的协商模式： 主模式：主模式将密钥交换信息与身份认证信息相分离。这种分离保护了身份信息，从而提供了更高的安全性 野蛮模式：野蛮模式缺少身份认证，但可以满足某些特定的网络环境需求。如果无法预先知道发起者的地址、或者发起者的地址总在变化，而双方都希望采用预共享密钥认证方法来创建 IKE SA，就可以用野蛮模式	
认证方式	两种认证方式可选：共享密钥和数字证书	共享密钥
IKE 高级选项（第 1 阶段）		
本地标识	和所选本地标识类型对应的本地标识，用户可选择：IP 地址、FQDN、User FQDN	空 IP 地址
对端标识	和所选对端标识类型对应的对端标识 用户可选择：IP 地址、FQDN、User FQDN	空 IP 地址
IKE 连接检测（DPD）	**DPD 超时时间**：当接收端触发 DPD 查询，主动向对端发送请求报文进行检测，超过超时时间仍没有收到对端的 IPSec 加密报文时，将删除此 ISAKMP Profile。 合法值：10-3600，单位：秒	0
	DPD 重试间隔：用于 IPSec 邻居状态的检测时间间隔。 启动 DPD 功能后，当接收端在触发 DPD 的时间间隔内收不到对端的 IPSec 加密报文时，能够触发 DPD 查询，主动向对端发送请求报文，对 IKE 对等体是否存在进行检测。 合法值：10-3600，单位：秒	0
IPSec 高级选项（第 2 阶段）		
完美前向加密（PFS）	PFS 是一种安全特性，指一个密钥被破解，并不影响其他密钥的安全性，因为这些密钥间没有派生关系。IPSec 第二阶段的密钥是从第一阶段的密钥导出的，当第一阶段 IKE 密钥被窃取后，攻	禁用

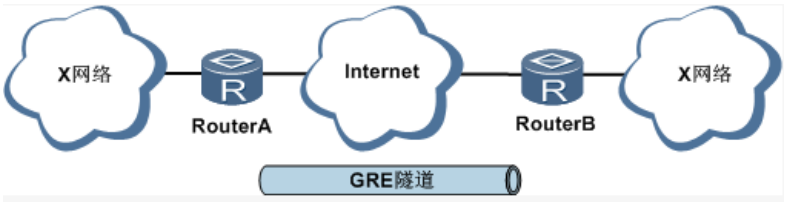
	击者将可能收集到足够的信息来导出第二阶段 IPSec SA 的密钥，PFS 通过执行一次额外的 DH 交换，保证第二阶段密钥的安全。	
IPsec SA 生命周期	设置 IPSec SA 的生存周期。IPSec 协商建立 SA 时，采用本端设置的生存周期和对端的生存周期中较小的一个。	3600



- 加密算法的安全性由高到低依次是：AES、3DES、DES，安全性高的加密算法实现机制复杂，但运算速度慢。对于普通的安全要求，DES 算法就可以满足需要。
- 当IR900作为IPsec server时，对端地址请配置成0.0.0.0，一般用于一端公网地址，一端拨号上网地址不固定场景
- IPsec扩展一般和GRE结合使用，用于组建DMVP或GRE OVER IPsec网络

3.8.2 GRE

通用路由封装（GRE）定义了在任意一种网络层协议上封装任意一个其它网络层协议的协议。GRE 可以作为 VPN 的三层隧道协议，为 VPN 数据提供透明传输通道。简单来说，GRE 是一种隧道技术，提供了一条通路使封装的数据报文能够在这个通路上传输，在隧道的两端分别对数据报进行封装及解封装。GRE 隧道应用组网如下图所示：



随着 IPv4 网络的广泛应用，为了使某些网络层协议的报文能够在 IPv4 网络中传输，可以将这些报文通过 GRE 技术进行封装，解决异种网络的传输问题。

采用 GRE 隧道传输主要用在以下几种情况：

- GRE 隧道可以像真实的网络接口那样传递多播数据包，而单独使用 IPSec，则无法对多播传输进行加密。
- 采用的某种协议无法进行路由。
- 需要用一个 IP 地址不同的网络将另外两个类似的网络连接起来。

GRE 应用举例：与 IPSec 结合，保护组播数据

GRE 可以封装组播数据并在 GRE 隧道中传输，而 IPSec 目前只能对单播数据进行加密保护。对于组播数据需要在 IPSec 隧道中传输的情况，可以先建立 GRE 隧道，对组播数据进行

GRE 封装，再对封装后的报文进行 IPSec 加密，从而实现组播数据在 IPSec 隧道中的加密传输。如下图所示：

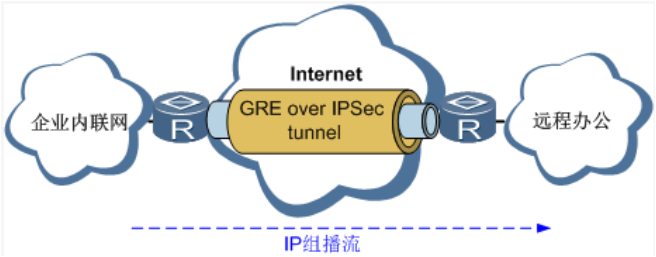


表 3-8-3 GRE 关键参数说明

参数名称	说明		缺省值
启用	启用或禁用 GRE 功能		禁用
接口标识	设置 GRE 隧道名称，范围 1-100		无
网络类型	选择 GRE 网络类型，用户可选择：点对点、子网		点对点
本地虚拟 IP	设置本地虚拟 IP 地址		无
对端虚拟 IP	设置对端虚拟 IP 地址，若为子网类型，此项为本地子网掩码		无
源地址类型	选择源地址类型，并设置对应类型的 IP 地址或接口名称		IP
本地接口名称	配置 GRE 隧道的源接口		
本地 IP 地址	配置 GRE 隧道的源地址		无
对端地址	配置 GRE 隧道的目的地址		无
密钥	设置隧道的认证密钥，两端配置需一致		无
MTU	设置 GRE 隧道的最大传输单元，以字节为单位		无
启用 NHRP	下一跳解析协议，用于连接到非广播多路访问（NBMA）式子网络的源站（主机或路由器）决定到达目标站间的“ NBMA 下一跳 ”的互联网络层地址和 NBMA 子网地址。		启用 禁用
	NHS 地址	对端 NHS 服务器地址	空
	认证密钥	NHRP 的认证密钥	空
	维持时间	合法值：1-65535	空
	禁止 NHRP Purge 消息	启用/禁止	禁止
IPsec Profile	禁用，与 IPsec 扩展结合使用		禁用
说明	GRE 隧道的描述信息		无



说明

- NHRP只用于DMVP网络，一般GRE不需要开启NHRP
- GRE一般用于两端地址都是固定公网情况。

3.8.3 L2TP

二层隧道协议 L2TP 是虚拟私有拨号网 VPDN 隧道协议的一种，扩展了点到点协议 PPP 的应用，是远程拨号用户接入企业总部网络的一种重要 VPN 技术。

L2TP 通过拨号网络（PSTN/ISDN），基于 PPP 的协商，建立企业分支用户到企业总部的隧道，使远程用户可以接入企业总部。PPPoE 技术更是扩展了 L2TP 的应用范围，通过以太网络连接 Internet，建立远程移动办公人员到企业总部的 L2TP 隧道。

L2TP 二层隧道协议。L2TP 是将来自用户网络的私有数据从二层 PPP 头部开始进行封装，数据没有加密机制，可通过 IPSec 保证数据安全。

- 主要用途：企业驻外机构和出差人员可从远程经由公共网络，通过虚拟隧道实现和企业总部之间的网络连接。

L2TP 典型组网图如下所示：

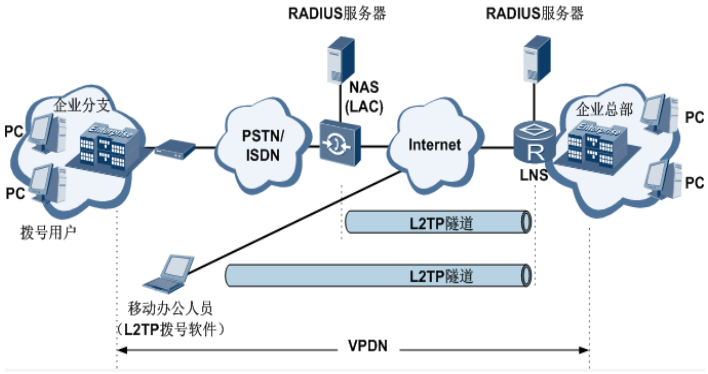


表 3-8-4 L2TP 客户端参数说明

参数名称	说明	缺省值
L2TP Class		
名称	用户自定义 L2TP Class 名称	无
认证	点选启用，启用后网络连接时需要认证对端	禁用
主机名	网络连接本端的主机名，可以不配	无
隧道认证密钥	当认证点选启用后必须配置隧道认证密钥，否则不需要配置	无
Pseudowire Class		
名称	用户自定义 Pseudowire Class 名称	无
L2TP Class	上边定义过的 L2TP Class 名称	无
源接口	选择源接口名称，用户可选择：bridge 1、cellular 1、fastethernet 0/1	~~cellular 1~~ 无
数据封装协议	用户可选择：L2TPV2、L2TPV3	L2TPV2
隧道管理协议	用户可选择：L2TPV2、L2TPV3、NONE	L2TPV2

L2TP 隧道		
启用	开启或禁用 L2TP 隧道	启用
标识	L2TP 虚拟接口标识号	1
L2TP 服务器	设置 L2TP 服务器的 IP 地址或域名	无
Pseudowire Class	上边定义过的 Pseudowire Class 名称	无
认证方式	选择认证方式，用户可选择：Auto、PAP、CHAP	Auto
用户名	对端服务器设定的合法的用户名	无
密码	对端服务器设定的合法的密码	无
本地 IP 地址	设置 L2TP 虚拟接口地址的 IP 地址，也可不配让对端服务器自动分配	无
远端 IP 地址	服务器端 L2TP 地址池的网关，也可不配	无
L2TPv3 隧道		
启用	开启或禁用 L2TPV3 隧道	启用
标识	L2TPV3 虚拟接口标识号	1
远端地址	设置 L2TPV3 服务器的 IP 地址或域名	空
Pseudowire Class	上边定义过的 Pseudowire Class 名称	空
封装协议	用户可选择：IP、UDP	IP
源端口	当使用 UDP 协议建立 L2TP 时使用的源端口	空
目的端口	当使用 UDP 协议建立 L2TP 时的目的端口	空
Xconnect 接口	用户可选择：fastethernet，L2TPV3 桥接端口	空
L2TPv3 会话		
本地隧道会话 ID	静态配置 L2TPV3 时指定的本地隧道 ID，范围 1-65535	空
远端隧道会话 ID	静态配置 L2TPV3 时指定的远端隧道 ID，范围 1-65535	空
本地隧道 ID	上面配置的 L2TPv3 隧道标识	空
本地会话 IP 地址	静态配置 L2TPV3 虚接口的地址	空

表 3-8-5 L2TP 服务器参数说明

参数名称	说明	缺省值
启用	开启或禁用 L2TP 服务器	禁用
账号	L2TP 服务器的接入账号	空
密码	L2TP 服务器的接入密码	空
认证类型	用户可选择：Auto、PAP、CHAP	Auto
本地 IP 地址	L2TP 服务器接口的虚拟地址	空
客户端起始 IP 地址	L2TP 服务器地址池的起始地址	空
客户端结束 IP 地址	L2TP 服务器地址池的结束地址	空
连接检测时间间隔	L2TP 建立成功后，发送连接检测报文的时间间隔合法值：0-32767，单位：秒	60 秒
连接检测最大失败次数	L2TP 连接检测失败后，当达到最大失败次数后，L2TP 重新建立连接。合法值：0-100	5
启用 MPPE	微软点对点加密术，规定了如何在数据链路层通信机密性保护的机制。它通过对 PPP 链接中 PPP 分组的加密以及 PPP 封装处理，实现数据链路层的机密性保护	禁用

启用隧道认证	隧道认证密钥	L2TP 建立时需要验证的隧道密钥，两端必须一致	空
	服务器端名称	建立 L2TP 时服务器的名称	空
	客户端名称	指定接入的 L2TP 客户端名称	空
专家选项（建议不填）	调试 L2TP 时用的参数		空

3.8.4 OPENVPN

允许参与建立 VPN 的单点使用预设的私钥，第三方证书，或者用户名/密码来进行身份验证。它大量使用了 OpenSSL 加密库，以及 SSLv3/TLSv1 协议。

在 OpenVpn 中，如果用户访问一个远程的虚拟地址（属于虚拟网卡配用的地址系列，区别于真实地址），则操作系统会通过路由机制将数据包（TUN 模式）或数据帧（TAP 模式）发送到虚拟网卡上，服务程序接收该数据并进行相应的处理后，通过 SOCKET 从外网上发送出去，远程服务程序通过 SOCKET 从外网上接收数据，并进行相应的处理后，发送给虚拟网卡，则应用软件可以接收到，完成了一个单向传输的过程，反之亦然。

表 3-8-6 OpenVPN 客户端参数说明

参数名称	说明	缺省值
启用	开启或禁用 OpenVPN 客户端	启用
ID	设置隧道 ID	无
OpenVPN 服务器	设置 OpenVPN 服务器的 IP 地址或域名	空
端口号	建立 OpenVPN 时	1194
协议类型	用户可选择 udp、tcp	udp
认证类型	选择认证类并配置相应认证类型的参数 用户可选择：无 用户名/密码 预共享密钥 数字证书 数字证书/用户名/密码 数字证书/TLS 认证 数字证书/TLS 认证/用户名/密码	~~用户名/密码~~ 无
隧道描述	用户自定义隧道描述内容	无
高级选项		
源接口	建立 OpenVPN 时使用的接口，用户可选择：bridge 1、cellular 1、fastethernet 0/1	无
接口类型	选择该接口发出去的数据形式。 Tun:大多时候被用于基于 IP 协议的通讯。 Tap:允许完整的以太网帧通过 Openvpn 隧道,提供非 ip 协议的支持	tun

网络类型	选择网络类型，用户可选择：net30、p2p、subnet net30:从 pool 中选择 4 个掩码为 30 的 ip，将中间两个 ip 中的大者作为 client 的虚拟网卡 ip；将小者作为 client 的对端 ip p2p:从 pool 中选择一个 ip 作为 client 的虚拟网卡 ip,将自己的实际虚拟网卡 ip 作为 client 的对端 ip Subnet:从 pool 中选择一个 ip 作为 client 的虚拟网卡 ip,将自己的子网掩码作为 client 的子网掩码 一般作为 openvpn 客户端时不需要配置由服务器端推送地址	net30
加密算法	OpenVPN 传输数据时使用的加密协议，必须与服务器保持一致	Default
HMAC	OpenVPN 传输数据时采用的校验方式，校验不通过数据传输失败。必须与服务器一致。	sha1
LZO 压缩	OpenVPN 数据传输时采用的压缩形式	关闭
重定向网关	使 Client 的默认网关指向 OpenVPN，让 Client 的所有流量都通过 OpenVPN 接口转发	关闭
Remote Float	允许远端改变它的 IP 地址/端口.	关闭
连接检测时间间隔	OpenVPN 建立成功后，发送连接检测报文的时间间隔合法值：10-1800，单位：秒	60 秒
连接检测超时时间	OpenVPN 连接检测失败后，当达到最大失败次数后，L2TP 重新建立连接。 合法值：60-3600	300 秒
MTU	OpenVPN 接口的最大传输单元，单位：字节	1500
调试日志	点选启用	禁用
专家配置	配置 OpenVPN 扩展参数	无
导入配置	选择需要导入的 OpenVPN 配置文件	空

表 3-8-7 OpenVPN 服务器参数说明

参数名称	说明	缺省值
启用	开启或禁用 OpenVPN 服务器	启用
配置方法	用户可选择：手动配置、导入配置文件	无
手动配置参数说明		
认证类型	用户可选择：无 用户名/密码 预共享密钥 数字证书 数字证书/用户名/密码 数字证书/TLS 认证 数字证书/TLS 认证/用户名/密码	无
本地 IP 地址	OpenVPN 服务器接口的虚拟 IP 地址	空
远端 IP 地址	Openvpn 客户端的虚拟 IP 地址	255.255.255.0
隧道描述	OpenVPN 隧道的描述信息	空
显示高级选项	点选启用	启用

源接口	建立 OpenVPN 时使用的接口，用户可选择：bridge 1、cellular 1、fastethernet 0/1	无
接口类型	选择该接口发出去的数据形式。 Tun:大多时候被用于基于 IP 协议的通讯。 Tap:允许完整的以太网帧通过 Openvpn 隧道,提供非 ip 协议的支持	tun
网络类型	选择网络类型，用户可选择：net30、p2p、subnet	net30
协议类型	和服务器通讯时的协议，和客户端保持一致	udp
端口号	OpenVPN 服务使用的端口号	1194
客户端互联模式	开启后允许接入的客户端互相访问，	禁用
加密算法	OpenVPN 传输数据时使用的加密协议，必须与服务器保持一致	Default
HMAC	OpenVPN 传输数据时采用的校验方式，校验不通过数据传输失败。必须与服务器一致。	sha1
LZO 压缩	OpenVPN 数据传输时采用的压缩形式。与客户端保持一致	关闭
连接检测时间间隔	OpenVPN 建立成功后，发送连接检测报文的时间间隔合法值：10-1800，单位：秒	60 秒
连接检测超时时间	OpenVPN 连接检测失败后，当达到最大失败次数后，L2TP 重新建立连接。合法值：60-3600	300 秒
MTU	OpenVPN 接口的最大传输单元，单位：字节	1500
调试日志	点选启用	禁用
专家配置	配置 OpenVPN 扩展参数	空
用户名/密码	使用用户密码认证方式时服务器配置的用户/密码	空
本地子网	OpenVPN 服务器到客户端的路由，一般填写客户端实际通讯的子网	空
客户端子网	OpenVPN 服务器推送到客户端的静态路由。	空
客户端 ID	标识客户端的属性 ID，一般为客户端证书名或用户名	空



说明

导入配置可以直接导入对端服务器生成的配置文件，导入以后将不用再手动配置 OPENVPN 客户端参数。

3.8.5 证书管理

Scep（Simple Certificate Enrollment Protocol）简单证书注册协议，是 cisco 和 Verisign 一起制定的设备证书管理的通信协议。它利用现有的 PKCS#7 和 PKCS#10 协议技术结合，享有广泛的支持客户端和 CA 的实现。

该协议现在支持以下操作：

1、 CA 证书的下载（-- getca）；

2、 证书的注册(-- enroll)；

3、 证书的查询(-- getcert)；

4、 证书吊销列表的查询(-- getcrl)

表 3-8-8 证书管理关键参数说明

参数名称	说明	缺省值
启用简单证书申请协议	开启或禁用证书申请协议	禁用
启用简单证书申请协议		
强制重新申请	强制重新申请为不检测当前证书状态，每次重新启动证书申请服务。	禁用
请求状态	当前设备申请证书的状态，分为 initialize Enrolling、Re-Enrolling、Complete 四种状态	
证书保护密钥	申请证书时候设置的证书保护密钥，起到数字证书加密作用，当导入和导出证书时配置的保护密钥和证书申请时的密钥一致才能使用	空
证书保护密钥确认	对证书保护密钥校验	空
限定 CA	设置设备信任的 CA 标识符在申请证书时，是通过一个可信实体认证机构，来完成实体证书的注册颁发，因此必须指定一个信任的 CA 标识符，将设备与该 CA 进行绑定，该设备证书的申请、获取、废除及查询均通过该 CA 执行	禁用
服务器 URL	证书服务器的 URL 地址，证书申请前必须指定注册服务器的 URL，随后实体可通过 SCEP 向该服务器提出证书申请 比如：http://100.17.145.158:8080/certsrv/mscep/mscep.dll。	空
证书名	指定要申请的证书的名称，即：证书通用名	空
FQDN	设置证书的 FQDN（Fully Qualified Domain Name，合格域名）FQDN 是实体在网络中的唯一标识，由一个主机名和域名组成，可被解析为 IP 地址。例如，www 是一个主机名，whatever.com 是一个域名，则 www.whatever.com 就是一个 FQDN	空
单位名 1	配置证书所属的单位名称 1	空
单位名 2	配置证书所属的单位名称 2	空
域名	配置证书的合格域名	空
序列号	配置申请证书的序列号	空
认证密码	设置证书申请时的挑战密码，挑战码是指撤销证书时使用的密码（可选）	空
认证密码确认	对认证密码校验，与上面配置一样。	空

主机地址	设置证书使用的 IP 地址	空
RSA 密钥长度	合法值：128-2048，单位：位	1023 位
查询时间间隔	设备向证书服务器查询当前证书状态的时间间隔，合法值：30-3600，单位：秒	60 秒
查询超时时间	设置设备查询证书状态的最大时间，当达到超时时间后，认为本次证书申请失败。合法值：30-86400，单位：秒	3600 秒
证书吊销	启用或禁用证书吊销 CA 可通过称为证书吊销的过程来缩短证书寿命。CA 发布一个证书吊销列表 (CRL)，列出被认为不能再使用的证书的序列号。CRL 指定的寿命通常比证书指定的寿命短得多。CA 也可以在 CRL 中加入证书被吊销的理由。它还可以加入被认为这种状态改变所适用的起始日期。	禁用
证书吊销参数		
CRL URL	CRL：证书吊销列表，设置 CRL 发布点的 URL	空
OCSP URL	在线证书状态协议（OCSP）可以测定所需要检验证书的（撤消）状态。 配置 OCSP 服务器的 URL，一般与证书服务器的 URL 一致	空
导入公钥证书	手动上传本地公钥到设备	空
导入私钥证书	手动上传本地私钥到设备	空
导入 CA 证书	手动上传本地 CA 证书到设备	空
导入证书回收列表	手动上传本地 CRL 到设备	空
导入 PKS12 证书	手动上传本地 PKS12 格式证书到设备	空

表 3-8-9 ROOT CA 参数说明

参数名称	说明	缺省值
导入根 CA 证书	手动上传本地根 CA 证书到设备	未选择



说明

使用证书时，确保路由器时间和实际时间同步。

3.9 工业接口

路由器可以通过工业接口与带有工业接口的终端设备相连，把带有工业接口的终端的数据通过路由器无线上传到上层设备，实现终端设备与上层设备的无线通信。

路由器工业接口有串口和 IO 接口。串口有 RS232 和 RS485 两种接口模式；IO 接口有数字量输入和继电器输出两种接口。

RS232 采用全双工通信，仅需几条信号线就可以实现，一条发送线、一条接收线及一条地线。RS232 一般用于 20m 以内的通信。

RS485 采用半双工通信，能远距离传输串行通信数据。由于工业现场的环境较为恶劣，为保证工业现场较长传输距离的情况下数据的正确性，一般工业现场设备采用 RS485 进行通讯。RS485 可以用于几十米到上千米的通信。

IO 接口的数字量输入可以把电信号转换成二进制控制信号的数字量，数字量就是逻辑变量或者开关变量：只有 0 和 1 两个状态。低电压对应“0”；高电压对应“1”

IO 接口的继电器输出相当于一个“自动开关”，可以在电路中起到自动调节、安全保护、转换电路等作用。

3.9.1 DTU

3.9.1.1 串口设置

根据与路由器相连的终端设备的串口参数设置路由器串口的参数，实现路由器与终端设备的正常通信。

表 3-9-1 串口设置参数说明

参数名称	说明	缺省值
串口类型	串口 1 类型为 RS232，串口 2 类型为 RS485，不可以更改	RS232/RS485
波特率	这是一个衡量符号传输速率的参数。它表示每秒钟传送的符号的个数。	9600
数据位	设置通信中实际数据位的参数	8 bits
校验位	在串口通信中的检错方式，一般是奇偶校验或无	无校验
停止位	用于表示单个包的最后一位。典型的值为 1，1.5 和 2 位。	1 bits
软件流控	串口通讯的流控提供了由于某种原因不能进行通讯时阻塞通讯的一种机制。流控可以使数据接收设备在不能接收数据时通知数据发送设备，使其停止发送。	关闭
串口描述	用户自定义	无

注意

- 路由器的串口参数与相连的终端设备的串口参数必须设置一致。
- DTU功能和GPS IP转发不能同时开启。

3.9.1.2 DTU1

表 3-9-2 DTU 1 参数说明

参数名称	说明	缺省值
启用	点选启用	关闭
DTU 协议	用户可选择：透明传输、TCP 服务器、RFC2217 模式、IEC101 转 104、Modbus 网桥、DC 协议。 透明传输和 TCP 服务器：若选用透明传输则设备作客户端，若选用 TCP 服务器则设备作服务器端 RFC2217 模式：选用此模式后不用再设置串口配置 IEC101 转 104：适用于电力行业，功能和 TCP 相似	透明传输
协议	两种可选：TCP 协议和 UDP 协议	TCP 协议
连接类型	两种可选：长连接和短连接 长连接：TCP 客户端和 TCP 服务器建立连接后，一直保持 TCP 连接。 短连接：TCP 客户端和 TCP 服务器建立连接后，当空闲时间内没有数据传输，自动断开与服务器 TCP 连接	长连接
心跳间隔	TCP 客户端和 TCP 服务器建立连接后，定期发送 TCP 心跳报文的时间间隔，合法值：1-3600，单位：秒	60
心跳重试次数	当 TCP 心跳超时后，设备重新发送 TCP 心跳，达到设置的心跳重试次数后，重新建立 TCP 连接。 合法值：1-100	5
串口缓存帧个数	当串口收发数据时设置的串口缓存大小，默认 4K	4
串口分帧长度	当串口发送数据时，设置的一帧数据的大小。当达到后开始发送。合法值：1-1024，单位：字节	1024
串口分帧间隔	当串口发送数据时候，当发送间隔大于设置的分帧间隔后合，设备会自动分帧发送，合法值：10-65535，单位：毫秒	100
最小重连间隔	用户自定义最小重连间隔时间。设备启动连接时如果没连接成功会按照此最小重连间隔时间重连。直到最大连接时间达到用户自定义的最大重连间隔。 合法值：15-60，单位：秒	15
最大重连间隔	用户自定义最大重连间隔时间。设备启动连接且连接时间达到最大重连间隔时间后，每隔此间隔时间（即用户自定义的最大重连间隔时间）连接一次。 合法值：60-3600，单位：秒	180

多中心策略	用户可选择：并发、轮询 **并发：** 同时去连接目的 IP 地址列表中的中心 **轮询：** 先连接列表前边的中心，若连接上就不再连接后边的；若没有连接上则按照自前往后的顺序去连接，直到连接上一个中心为止	并发
源接口	有四种选择。一般用户不用选择 用户可选择：IP、bridge 1 、cellular 1、fastethernet 0/1	IP
本地 IP 地址	源接口选择 IP 时对应的设备接口 IP 地址。一般用户不用配置，可为空	无
DTU 标识	用户自定义，成功连接服务器后自动向服务器发送的 DTU 标示。也可以不配置，保持空状态。	无
调试日志	点选开启	关闭
开启 ReportID	点选启用	禁用
心跳间隔时间	启用 ReportID 才需设置此项 合法值：1-65535，单位：秒	0
心跳包内容	启用 ReportID 才需设置此项	空
目的 IP 地址		
服务器地址	用户自定义设备要连接的服务器 IP 地址	无
服务器端口	用户自定义设备要连接的服务器端口	无

说明

- 目的IP地址最多可以设置10个。
- DTU 2的配置方法和DTU 1的配置方法完全一样。

3.9.2 IO 接口

继电器输出默认状态是闭合，可以通过手动控制使其断开或闭合，或者手动设置断开时间参数，达到设置参数后自动转为闭合。

表 3-9-3 IO 接口状态参数说明

参数名称	说明	缺省值
数字量输入		
数字量输入 1	10V 以下电压对应“低（0）”； 10V 及以上电压对应“高（1）”	低（0）
继电器输出		
继电器输出 1	默认状态是闭合。可以通过手动控制改变其状态，若不通过动作部分手动改变其状态，设备则会一直保持闭合状态	闭合
动作	断开：点击后继电器处于断开状态 闭合：点击后继电器处于闭合状态 断开->闭合：用户自定义断开时间参数，达到设置参数后自动转为闭合	断开时长：1000 毫秒

输入高动作	当数字量输入为高时，会触发 IPsec 或 OpenVpn 启用和禁用动作	空
输入低动作	当数字量输入为低时，会触发 IPsec 或 OpenVpn 启用和禁用动作	空
输出闭合的事件	当 IPsec 或 OpenVpn 连接或断开时，可以控制继电器闭合	空
输出断开的事件	当 IPsec 或 OpenVpn 连接或断开时，可以控制继电器断开	空

3.9.3 Modbus

Modbus 网络是一个工业通信系统，由带智能终端的可编程序控制器和计算机通过公用线路或局部专用线路连接而成。Modbus 协议是应用于电子控制器上的一种通用语言。通过此协议，控制器之间、控制器经由网络（例如以太网）和其它设备之间可以通信。它已经成为一种通用工业标准。有了它，不同厂商生产的控制设备可以连成工业网络，进行集中监控。

在 Modbus 系统中有 2 中传输模式即 ASCII 和 RTU（远程终端设备）可选择。在每个 Modbus 系统中只能使用一种模式，不允许两种模式混用。

表 3-9-4 Modbus Tcp 参数说明

参数名称	说明	缺省值
启用	点选启用	禁用
端口	用户自定义端口号	502

3.10 工具

3.10.1 PING 探测

提供从路由器 Ping 外网的功能。

表 3-10-1 PING 探测参数说明

参数名称	说明	缺省值
主机	需要 Ping 探测的目的主机地址	192.168.2.1
次数	设置 Ping 探测的次数	4 次
包大小	设置 Ping 探测包的大小	32 字节
专家选项	可使用 Ping 的高级参数	无

3.10.2 路由探测

用于检测网络的路由故障。

表 3-10-2 路由探测参数说明

参数名称	说明	缺省值
主机	需要探测的目的主机地址	192.168.2.1
最大跳数	设置路由探测的最大跳数	20
超时时间	设置路由探测的超时时间	3 秒
协议	可选择 ICMP/UDP	UDP
专家选项	可使用路由探测的高级参数	无

3.10.3 网络抓包

表 3-10-3 网络抓包参数说明

参数名称	说明	缺省值
接口	用户可选择：any、bridge 1、cellular 1、fastethernet0/1	any
抓包个数	指定抓包个数，当达到设置的个数停止抓包	10
专家选项	可选的抓包配置参数。可以根据设定的参数抓取包内容	无



说明

IR900抓包使用是tcpdump功能，专家选项设置时请参考tcpdump参数设置

3.10.4 网速测试

用于检测网速，通过上传和下载文件来测试网速。

表 3-10-4 网速测试参数说明

参数名称	说明	缺省值
浏览	选择要上传测试的文件	空
上传	用于测试路由器各接口上传速率	无
下载	用于测试路由器各接口上传速率	无

3.11 安装向导

简化的常规配置，在这里可以对路由器进行快速、简单、基础的配置，在这里不能显示配置结果，但配置完成后可以在前边对应的具体配置里查看到配置结果。

3.11.1 新建 LAN

表 3-11-1 新建 LAN 参数说明

参数名称	说明	缺省值
禁用桥接口	点选启用	禁用
接口	选择新建 LAN 接口，用户可选择：bridge1 、fastethernet0/1	bridge 1
主 IP	用户可以根据需要配置或更改主 IP 地址	无
子网掩码	用户可以根据需要配子网掩码（可自动生成）	255.255.255.0
DHCP 服务	启用/禁用	启用
起始地址	设置动态分配的起始 IP 地址	无
结束地址	设置动态分配的结束 IP 地址	无
有效期	设置动态分配的 IP 的有效期 合法值：30-10080，单位：分钟	1440

3.11.2 新建 WAN

表 3-11-2 新建 WAN 参数说明

参数名称	说明	缺省值
接口	选择新建 WAN 接口，用户可选择：bridge1 、fastethernet0/1	fastethernet 0/1
类型	WAN 接口 IP 地址的配置类型，用户可选择：静态 IP、动态地址(DHCP)、ADSL 拨号（PPPoE）	静态 IP
主 IP	用户可以根据需要配置或更改主 IP 地址	无
子网掩码	用户可以根据需要配子网掩码（可自动生成）	255.255.255.0
网关	设置网关 IP 地址	无
首选域名服务器	设置域名服务器地址	空
网络地址转换	点选启用，启用后可以把私网 IP 地址转换成公网 IP 地址	启用

3.11.3 新建拨号

表 3-11-3 新建拨号参数说明

参数名称	说明	缺省值
拨号参数	用户可选择：自动、定制	自动
定制参数说明		
APN	选择新建 WAN 接口	3gnet
拨号号码	移动运营商提供相关拨号参数（请根据当地运营商选择）	*99***1#
用户名	移动运营商提供相关拨号参数（请根据当地运营商选择）	gprs
密码	移动运营商提供相关拨号参数（请根据当地运营商选择）	●●●●
网络地址转换	点选启用，启用后可以把私网 IP 地址转换成公网 IP 地址	启用

3.11.4 新建 IPSec 隧道

表 3-11-4 新建 IPSec 隧道参数说明

参数名称	说明	缺省值
基本参数		
隧道序号	为建立的隧道确定一个序号	1
接口名称	选择接口名称 用户可选择：cellular 1 、bridge1、fastethernet 0/1	cellular 1
对端地址	设置 VPN 对端的 IP	无
协商模式	可选主模式，野蛮模式。 一般选择主模式	主模式
本地子网地址	设置 IPSec 本地保护子网	无
本地子网掩码	设置 IPSec 本地保护子网掩码	255.255.255.0
对端子网地址	设置 IPSec 对端保护子网	无
对端子网掩码	设置 IPSec 对端保护子网掩码	255.255.255.0
第一阶段参数		
IKE 策略	可选择 3DES-MD5-DH1 或 3DES-MD5-DH2 等	~~3DES-MD5-DH2~~ 3DES-MD5-DH1
IKE 生命周期	设置 IKE 的生命周期	86400 秒
本地标识类型	可选择 FQDN，USER FQDN，IP 地址	IP 地址
本地标识	仅限于 FQDN 和 USER FQDN。 根据选择的标识类型填入相应标识（USER FQDN 应为标准邮箱格式）	无
对端标识类型	可以选择 FQDN，USER FQDN，IP 地址	IP 地址
对端标识	仅限于 FQDN 和 USER FQDN。根据选择的标识类型填入相应标识（USER FQDN 应为标准邮箱格式）	无
认证方式	可以选择共享密钥和数字证书	共享密钥
密钥	认证方式选择为共享密钥时显示此项。 设置 IPSec VPN 协商密钥	无

第二阶段参数		
IPSec 策略	可选择 3DES-MD5-96 或 3DES –SHA1-96 等	3DES-MD5-96
IPSec 生命周期	设置 IPSec 生命周期	3600 秒



必须为每个隧道连接创建入站和出站规则。如果仅为单向连接创建筛选器，则不会应用规则。

3.11.5 新建端口映射

表 3-11-5 新建端口映射参数说明

参数名称	说明	缺省值
协议	协议可选 TCP 或 UDP	TCP
外部接口	用户根据需要选择连接外网的接口，用户可选择：cellular 1 、bridge1、fastethernet 0/1、vlan 1	bridge1
服务端口	TCP 或 UDP 数据通讯端口	无
内部地址	映射对象的设备地址	无
内部端口	映射对象的 TCP 或 UDP 端口	无
描述信息	用户自定义	无

四、典型应用配置

4.1 DDNS 应用举例

应用举例：一台 IR900，使用拨号方式获得公网 IP 地址，设置 DDNS 将用户的动态 IP 地址映射到一个固定的域名解析服务上。

路由器配置步骤如下：

第一步：配置设备的动态域名参数。如果使用定制的域名参数，配置如图 4-1-1 所示；如果使用普通的域名参数，配置如图 4-1-2 所示。

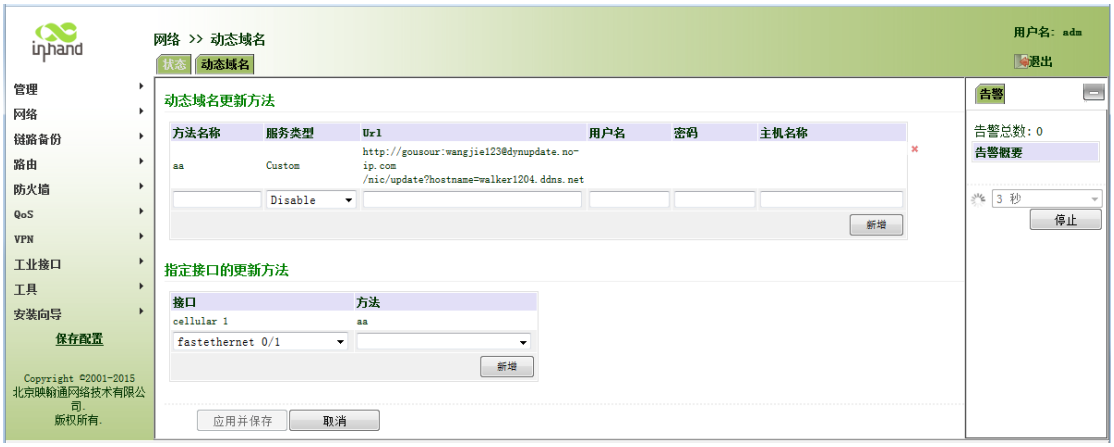


图 4-1-1

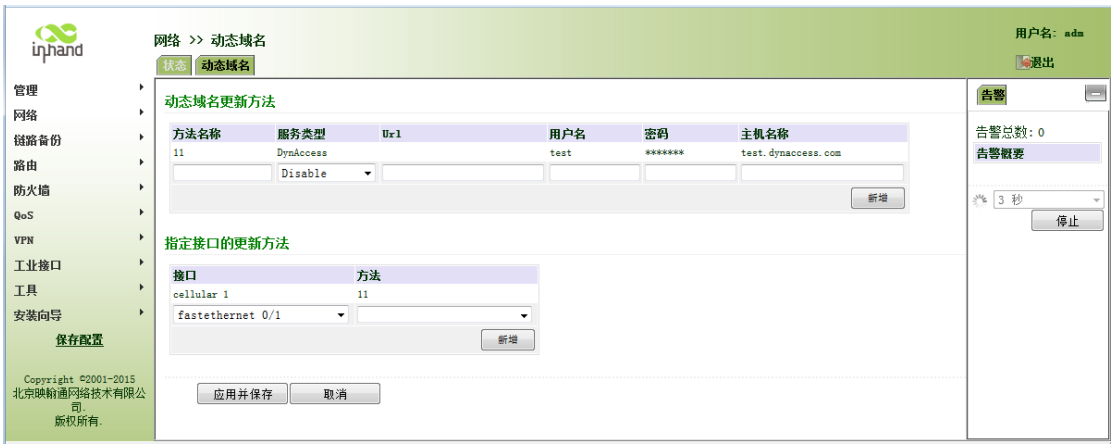


图 4-1-2

第二步：配置好动态域名保存应用以后等待几分钟，然后 ping 该域名确认动态域名配置成功，如图图 4-1-3 所示。


命令提示符
正在 Ping walker1204.ddns.net [211.136.69.179] 具有 32 字节的数据:
来自 211.136.69.179 的回复: 字节=32 时间<1ms TTL=64
来自 211.136.69.179 的回复: 字节=32 时间<1ms TTL=64
来自 211.136.69.179 的回复: 字节=32 时间<1ms TTL=64
来自 211.136.69.179 的回复: 字节=32 时间<1ms TTL=64
211.136.69.179 的 Ping 统计信息:
数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
最短 = 0ms, 最长 = 0ms, 平均 = 0ms

图 4-1-3

4.2 网管平台应用举例

应用举例：添加设备到网管平台

路由器配置步骤如下：

第一步：配置网管平台参数，其中服务器：c2.inhandnetworks.com，端口：20003，如图 4-2-1 所示。



图 4-2-1

第二步：登录网管平台（http://c2.inhandnetworks.com），添加该设备即可。

4.3 恢复出厂设置

4.3.1 网页方式

登陆 WEB 页面，单击导航树中的“管理>>配置管理”菜单，进入“配置管理”。单击<恢复出厂设置>按钮，确定恢复出厂后，重启系统，恢复出厂成功。

4.3.2 硬件方式

采用硬件方式恢复出厂设置步骤：

第一步：在设备面板上找到 RESET 复位键；

第二步：设备加电后 10 秒内长按 RESET 键不松开；

第三步：当 ERR 灯变红后，松开 RESET 键；

第四步：当 ERR 灯熄灭后，再重新按住 RESET 键 1 秒后松开：

第五步：当看到 ERR 灯闪烁三下后熄灭，表明恢复出厂设置成功

4.4 导入/导出配置

登陆 WEB 页面，单击导航树中的“管理>>配置管理”菜单，进入“配置管理”界面。

- 单击<浏览>选择配置文件，然后单击<导入>按钮。导入配置文件后，重启系统即可生效。
- 单击<备份 running-config >，导出目前正在应用的配置参数文件，保存。 导出的文件为.cnf 格式，默认文件名为 running-config.cnf。
- 单击<备份 startup-config >，导出设备开启时的配置参数文件，保存。 导出的文件为.cnf 格式，默认文件名为 startup-config.cnf。

4.5 日志与诊断记录

登陆 WEB 页面，单击导航树中的“管理>>系统日志”菜单，进入“系统日志”界面。单击对应按钮即可完成日志与诊断记录的下载。

4.6 上网方式

4.6.1 拨号上网

单击导航树中的“网络>>拨号接口”菜单，进入“拨号接口”界面。如果使用移动卡，默认参数即可；如果使用联通卡需要修改“拨号参数集”里的参数。图 4-6-1 分别举例了移动和联通对应的“拨号参数集”里的参数配置情况。

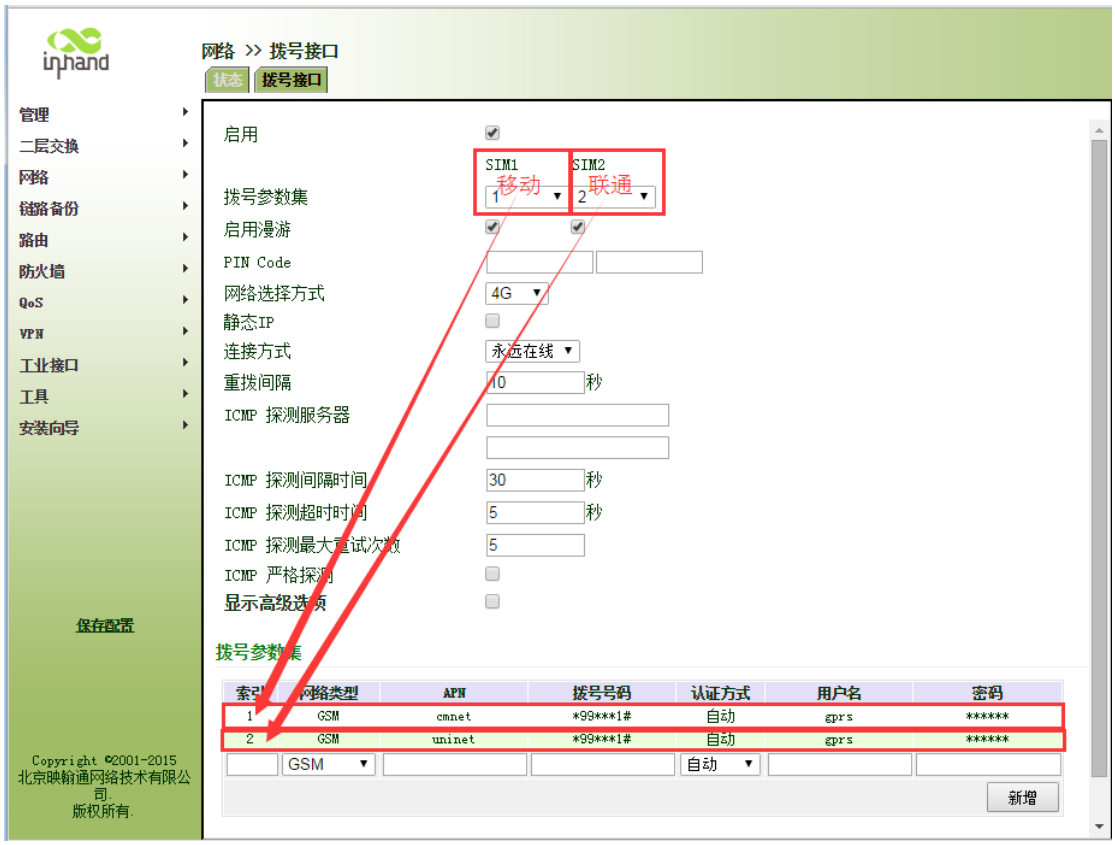


图 4-6-1

4.6.2 有线上网

第一步：禁用拨号接口。单击导航树中“网络>>拨号接口”菜单，如图图 4-6-2 所示。



图 4-6-2

第二步：新建 WAN，其中新建 WAN 类型有三种。单击导航树中“安装向导>>新建 WAN”菜单，图 4-6-3、图 4-6-4 和图 4-6-5 分别是静态 IP 类型、ADSL 拨号（PPPoE）类型和 DHCP 类型举例。



图 4-6-3


安装向导 >> 新建WAN
新建WAN
用户名:
adm
退出
管理
二层交换
网络
链路备份
路由
防火墙
QoS
VPN
工业接口
工具
安装向导
保存配置
Copyright ©2001-2015
北京映翰通网络技术有限公司.
版权所有.
接口
fastethernet 0/1
类型
ADSL拨号(PPPoE)
用户名
adm
密码
网络地址转换(NAT)
应用并保存
取消

图 4-6-4


安装向导 >> 新建WAN
新建WAN
用户名:
adm
退出
管理
二层交换
网络
链路备份
路由
防火墙
QoS
VPN
工业接口
工具
安装向导
保存配置
Copyright ©2001-2015
北京映翰通网络技术有限公司.
版权所有.
接口
fastethernet 0/1
类型
动态地址(DHCP)
网络地址转换(NAT)
应用并保存
取消

图 4-6-5

4.7 新建 LAN

单击导航树中“安装向导>>新建 LAN”菜单，如图 4-7-1 所示。



图 4-7-1

4.8 VRRP 典型配置举例

1. 组网需求

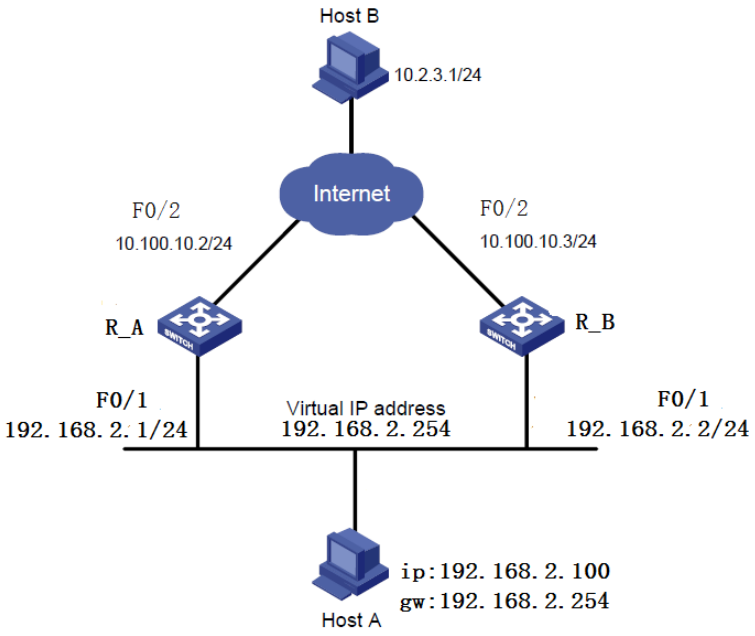
主机A把路由器A和路由器B组成的VRRP备份组作为自己的缺省网关，访问Internet 上的主机B。

VRRP 备份组构成：

- 备份组号为 1
- 备份组虚拟路由器的 IP 地址为192.168.2.254/24
- 交换机 A 做Master
- 交换机 B 做备份交换机，允许抢占

路由器	与 hostA 相连以太网接口	与 hostA 相连接口 IP 地址	优先级	工作模式
R_A	F0/1	192.168.2.1	110	抢占
R_B	F0/1	192.168.2.2	100	抢占

2. 组网图



3. 配置步骤

(1) 配置路由器A

第一步：配置F0/1

单击导航树中的“链路备份>>VRRP”进入“VRRP”界面，配置 VRRP，如图 4-8-1 所示。



图4-8-1

单击导航树中的“链路备份>>VRRP”进入“VRRP 状态”界面，查看 VRRP 状态，如图 4-8-2 所示。



图4-8-2

第二步：配置F0/2

单击导航树中的“网络>>以太网接口”进入“以太网口 0/2”界面，配置以太网口 0/2，如图 4-8-3 所示。

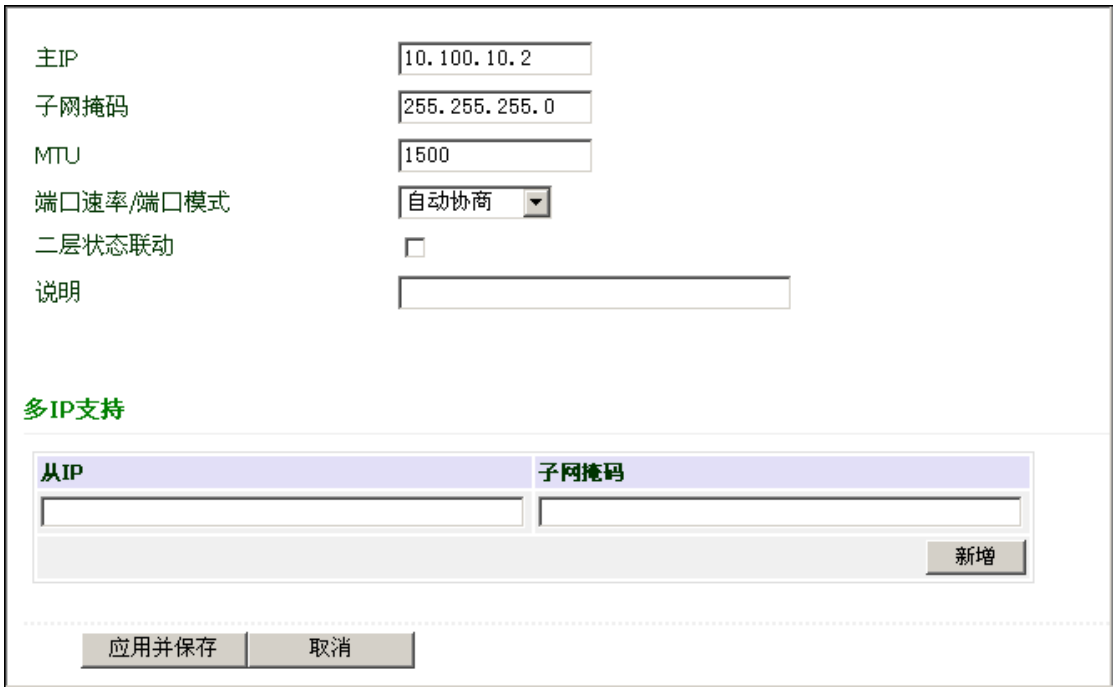


图4-8-3

(2) 配置路由器B：

第一步：配置F0/1

单击导航树中的“链路备份>>VRRP”进入“VRRP”界面，配置 VRRP，如图 4-8-4 所示。



图4-8-4

单击导航树中的“链路备份>>VRRP”进入“VRRP 状态”界面，查看 VRRP 状态，如图 4-8-5 所示。



图4-8-5

第二步：配置F0/2

单击导航树中的“网络>>以太网接口”进入“以太网口 0/2”界面，配置以太网口 0/2，如图 4-8-6 所示。



图4-8-6

主机 A 缺省网关设为 192.168.2.254。正常情况下，路由器 A 行使网关的职能，当路由器 A 关机或出现故障，路由器 B 将接替行使网关的职能。设置抢占方式的目的是当路由器 A 恢复工作后，能够继续成为 Master 行使网关的职能。

4.9 接口备份应用举例

应用举例：一台路由器 IR900，PC 连接 IR900 的 fastethernet 0/2 口，IR900 的 fastethernet 0/1 口连接有线网上网，拓扑图如下所示。配置路由器创建接口备份，使其在有线网故障时通过拨号上网。



路由器配置步骤如下：

第一步：打开“安装向导>>新建 WAN”，配置有线上网参数，如图 4-9-1 所示。



图 4-9-1

第二步：打开“网络>>DNS 服务”的“域名服务器”，配置对应参数，如图图 4-9-2 所示。配置完成后检查确认 PC 能正常上网。



图 4-9-2

第三步：打开“链路备份>>SLA”，配置对应参数，其中 IP 地址应设置为公网或专网内可 ICMP 探测的主机地址，例如 203.86.63.233 是 PC 所属的企业网关地址，如图 4-9-3 所示。



图 4-9-3

第四步：打开“链路备份>>Track 模块”，配置对应参数，如图 4-9-4 所示。



图 4-9-4

第五步：打开“链路备份>>接口备份”，配置对应参数，如图 4-9-5 所示。

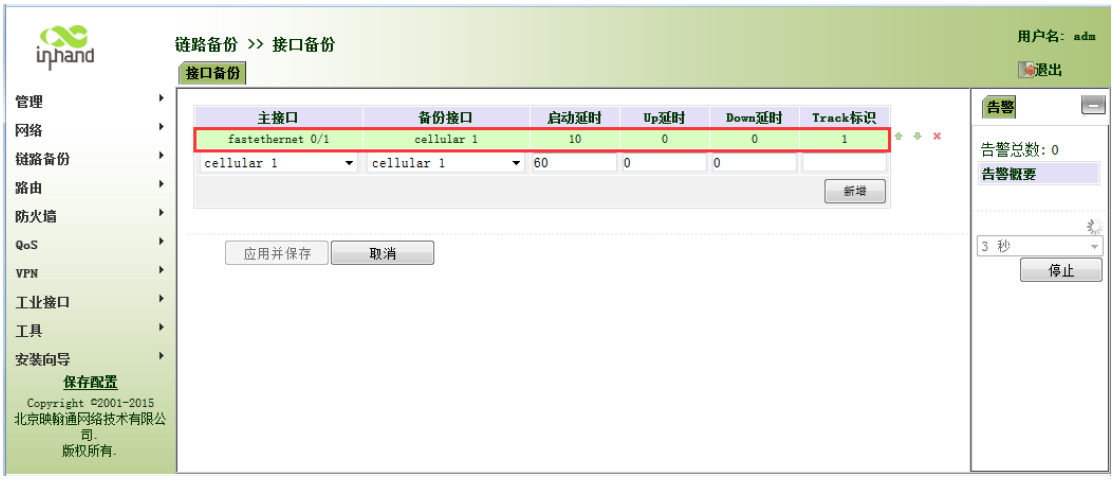


图 4-9-5

第六步：打开“路由>>静态路由”，配置对应参数新增 3 条路由，其中 10.5.3.234 是 PC 所属的局域网网关，如图 4-9-6 所示。其中距离参数表示优先权，数值越小越优先。

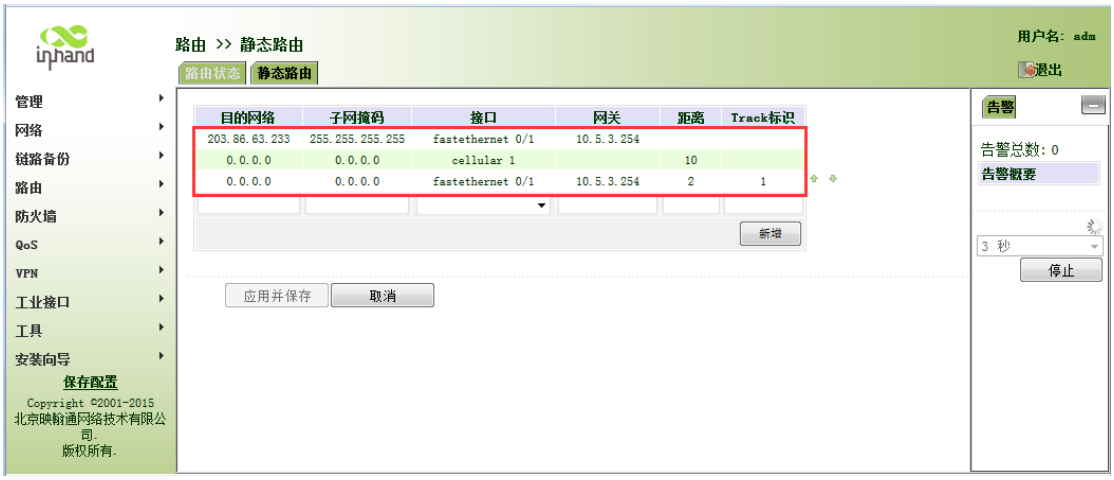
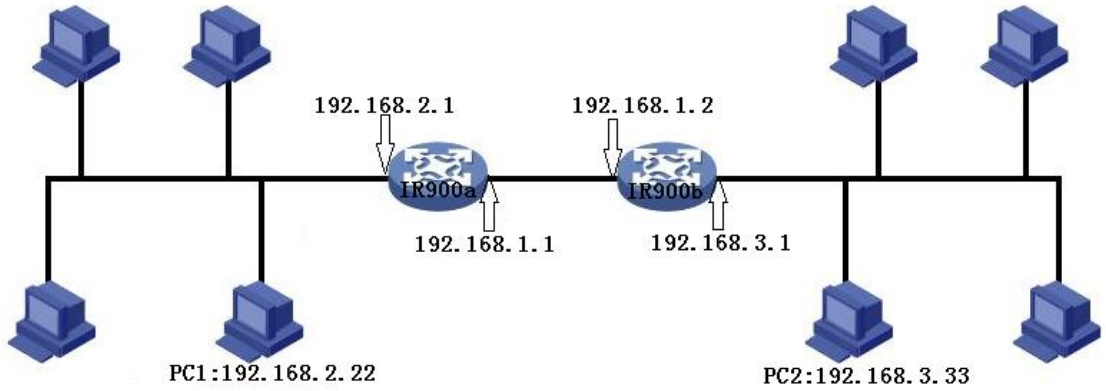


图 4-9-6

第七步：拔掉网线制造有线上网故障，稍后路由器便会通过 cellular 口拨号上网；当把网线重新连好，稍后又会使用有线上网。

4.10 静态路由应用举例

应用举例：给两个局域网之间建立静态路由，使其可以相互通信，拓扑图如下图所示。



路由器配置步骤如下：

第一步：配置 IR900a，参数配置如图 4-10-1 所示。



图 4-10-1

第二步：配置 IR900b，参数配置，如图 4-10-2 所示。

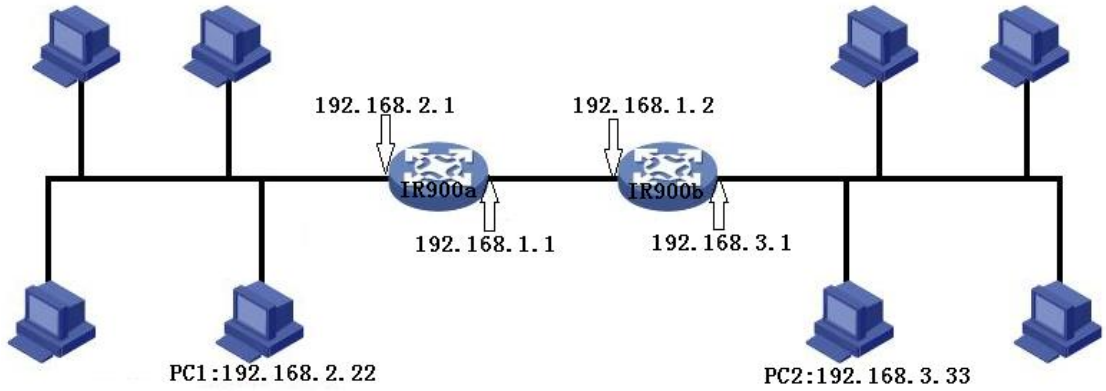


图 4-10-2

第三步：PC1 和 PC2 可以相互通信，静态路由添加成功。

4.11 动态路由应用举例

应用举例：给两个局域网之间建立动态路由，使其可以相互通信，拓扑图如下图所示。



一）RIP

路由器配置步骤如下：

第一步：配置 IR900a，参数配置如图 4-11-1 所示。



图 4-11-1

第二步：配置 IR900b，参数配置，如图 4-11-2 所示。



图 4-11-2

第三步：PC1 和 PC2 可以相互通信，动态路由添加成功。

二）OSPF

路由器配置步骤如下：

第一步：配置 IR900a，参数配置如图 4-11-3 所示。

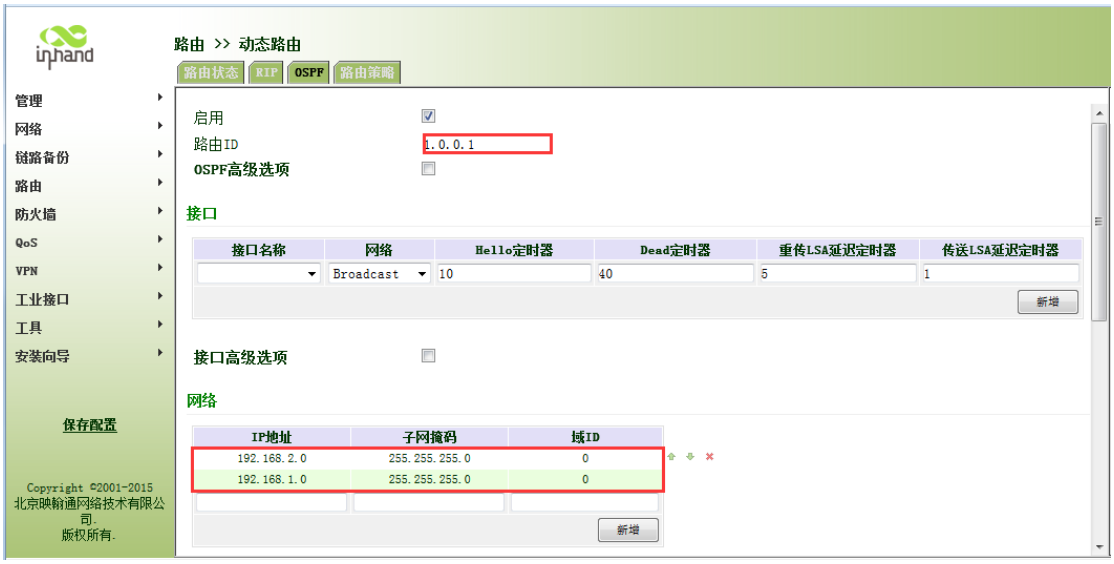


图 4-11-3

第二步：配置 IR900b，参数配置，如图 4-11-4 所示。

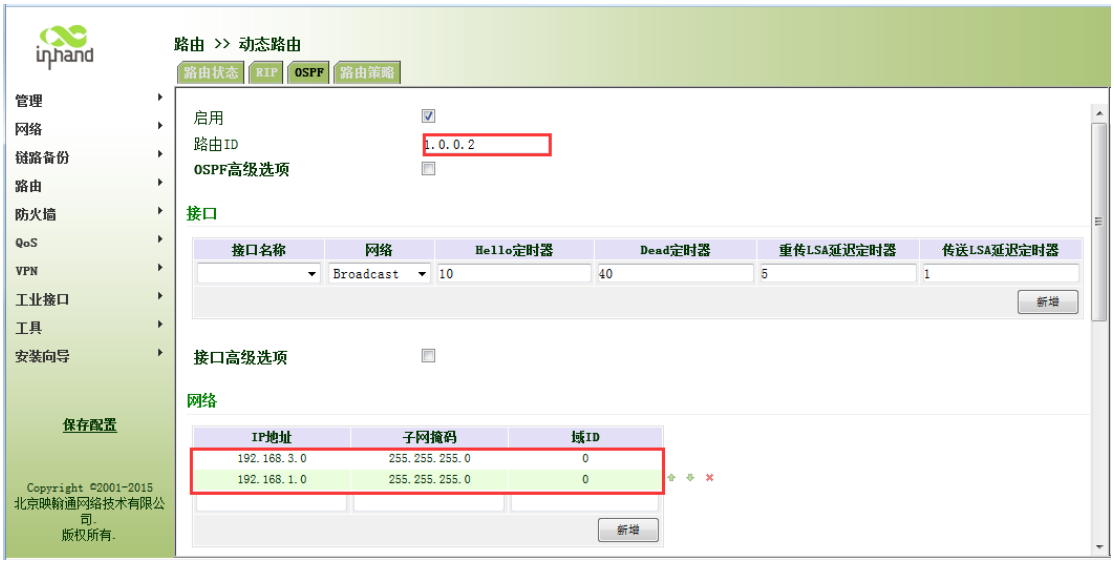
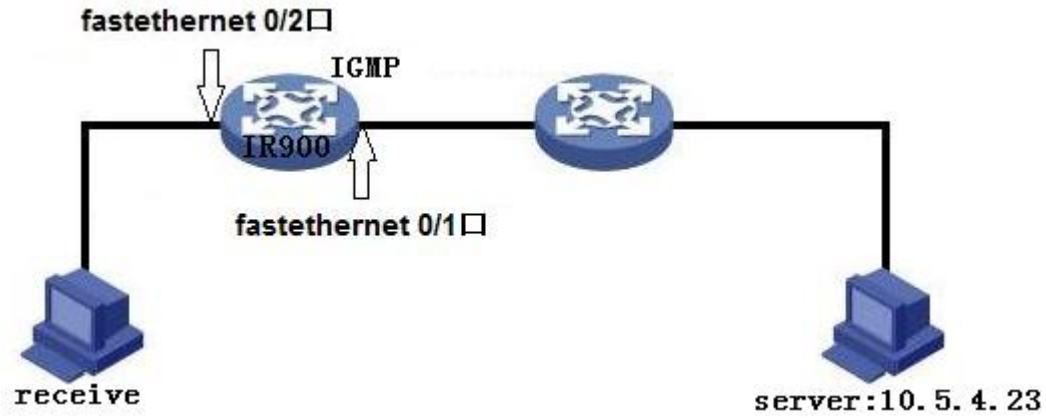


图 4-11-4

第三步：PC1 和 PC2 可以相互通信，动态路由添加成功。

4.12 组播路由应用举例

应用举例：设置路由器使其能接收来自某网络的组播数据，其拓扑图如下图所示。



路由器配置步骤如下：

第一步：启用组播路由并配置组播路由参数，如图 4-12-1 所示。



图 4-12-1

第二步：配置 IGMP 参数，如图 4-12-2 所示。


路由 >> 组播路由
用户名:
adm
退出
基本设置
IGMP
管理
网络
链路备份
路由
防火墙
QoS
VPN
工业接口
工具
安装向导
保存配置
Copyright ©2001-2015
北京映翰通网络技术有限公司.
版权所有.
上联接口
上联接口
fastethernet 0/1
下联接口列表
下联接口
上联接口
fastethernet 0/2
fastethernet 0/1
cellular 1
fastethernet 0/1
新增
应用并保存
取消
告警
告警总数: 0
告警概要
3 秒
停止

图 4-12-2

4.13 访问控制应用举例

应用举例：一台路由器 IR900，其中 FE 0/1 口连接内网，内网网段为 192.168.1.2/254；FE 0/2 口连接内网，内网网段 192.168.2.2/254。配置路由器使其 FE 0/2 口连接内网不能访问 Internet 网，而 FE 0/1 口连接内网可以正常访问 Internet 网。

路由器配置步骤如下：

第一步：打开“访问控制（ACL）”，单击<新增>添加访问控制列表，配置参数如图 4-13-1 所示。



图 4-13-1

第二步：参数配置完成后单击<应用并保存>，即可在界面中看到刚刚新建的访问控制列表 ID 为“101”的相关信息，如图 4-13-2 所示。



图 4-13-2

第三步：在“网络接口列表”里“接口名称”选择“cellular1”，“出站规则”选择“101”，单击<新增>并保存即可，如图 4-13-3 所示。



图 4-13-3

4.14 网络地址转换应用举例

应用举例：一台路由器 IR900，通过拨号上网，其中 FE 0/2 口连接一个服务器，该服务器 IP 地址为 192.168.2.23。配置路由器使其公网可以访问该服务器。

（端口映射方式）路由器配置如图 4-14-1 所示：



图 4-14-1

（DMZ 方式）路由器配置如图 4-14-2 所示：



图 4-14-2

4.15 QoS 应用举例

应用举例：设置路由器，将本地优先级分配给不同的下载通道。

路由器配置步骤如下：

第一步：添加“类”来描述下载流量，例如指定的本地主机的 IP 地址作为目的地。

第二步：添加“策略”，为每个“类”分配保证带宽和本地优先级。

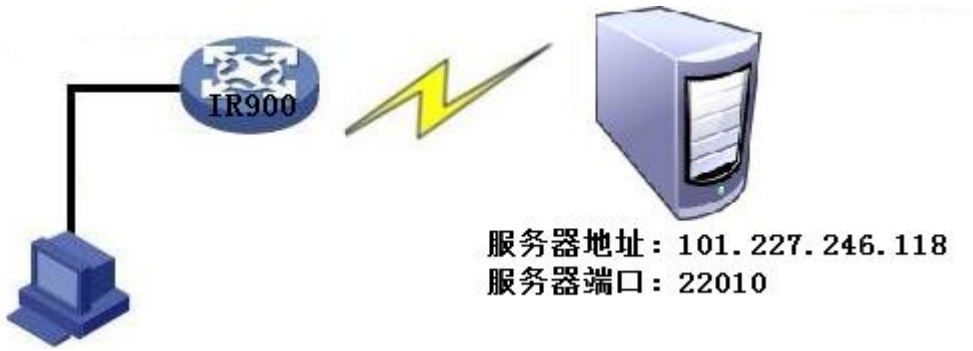
第三步：选择应用策略的出口接口，并给接口分配一个出口最大带宽。如图 4-15-1 所示。



图 4-15-1

4.16 DTU 应用举例

应用举例：一台 IR900，设置 DTU 功能，使其可以和服务器相互通信，其拓扑图如下所示。



路由器配置步骤如下：

第一步：配置 DTU 串口参数。串口参数要和对端设备串口参数保持一致，如图 4-16-1 所示。



图 4-16-1

第二步：配置 DTU 功能参数，如图 4-16-2 所示。



图 4-16-2

第三步：创建并启用服务器，IR900 通过 DTU 功能连接服务器，连接成功后 IR900 会自动向服务器发送 DTU 标示（DTU 标示参数为空则不发送），如图 4-16-3 所示。

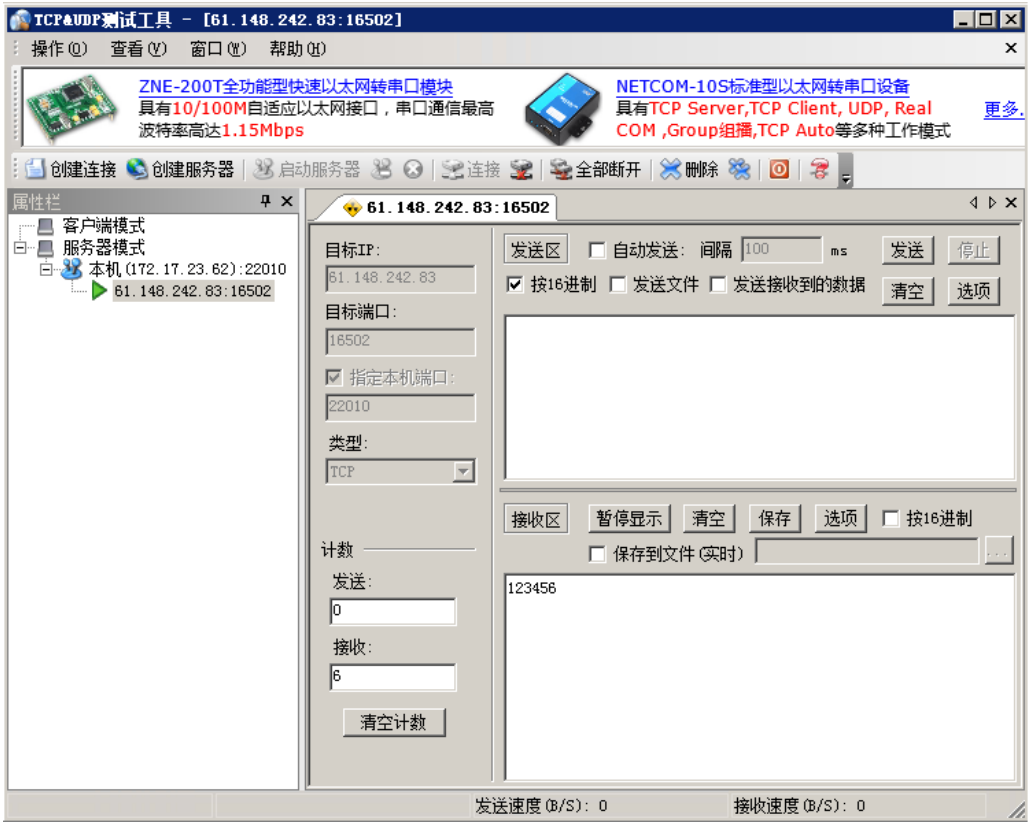


图 4-16-3

第四步：连接 IR900 的 PC 通过 DTU 功能和服务器可以相互发送数据，如图 4-16-4 和图 4-16-5 所示。



图 4-16-4

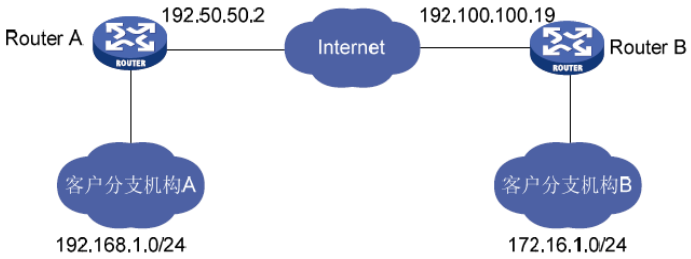


图 4-16-5

4.17 一对一 IPSec VPN 配置举例

在 Router A 和 Router B 之间建立一个安全隧道，对客户分支机构 A 所在的子网（192.168.1.0/24）与客户分支机构 B 所在的子网（172.16.1.0/24）之间的数据流进行安全保护。安全协议采用 ESP 协议，加密算法采用 3DES，认证算法采用 SHA。

组网示意图如下所示：



组网设置步骤：

（1）设置 Router A

第一步：单击导航树中的“VPN>>IPSec”进入“IPSec 配置”界面，配置参数，如图 4-17-1 所示。

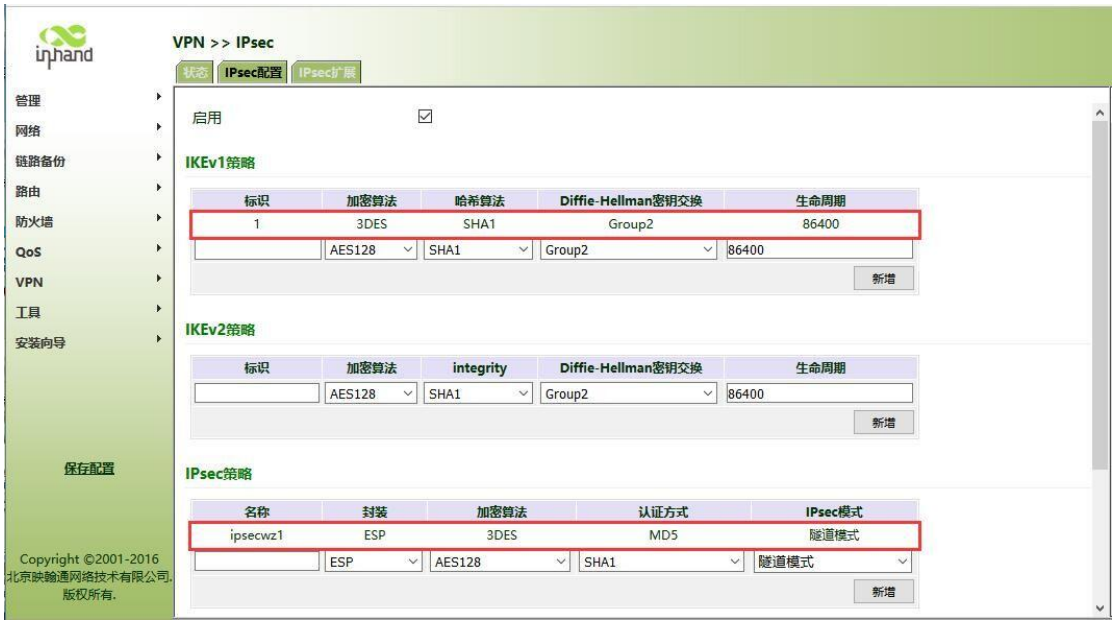


图 4-17-1

第二步：单击导航树中的“VPN>>IPSec”进入“IPSec 配置”界面，单击“IPSec 隧道配置”处的<新增>，在新打开的界面配置参数，如图 4-17-2 所示。



图 4-17-2

注意

本地标识和对端标识地址一般不用填写。

建立ipsec VPN时，IPSec Profile不用配置，只有DMVPN时才用到IPSec Profile。

（2）设置 Router B

第一步：单击导航树中的“VPN>>IPSec”进入“IPSec 配置”界面，配置参数，如图 4-17-3 所示。

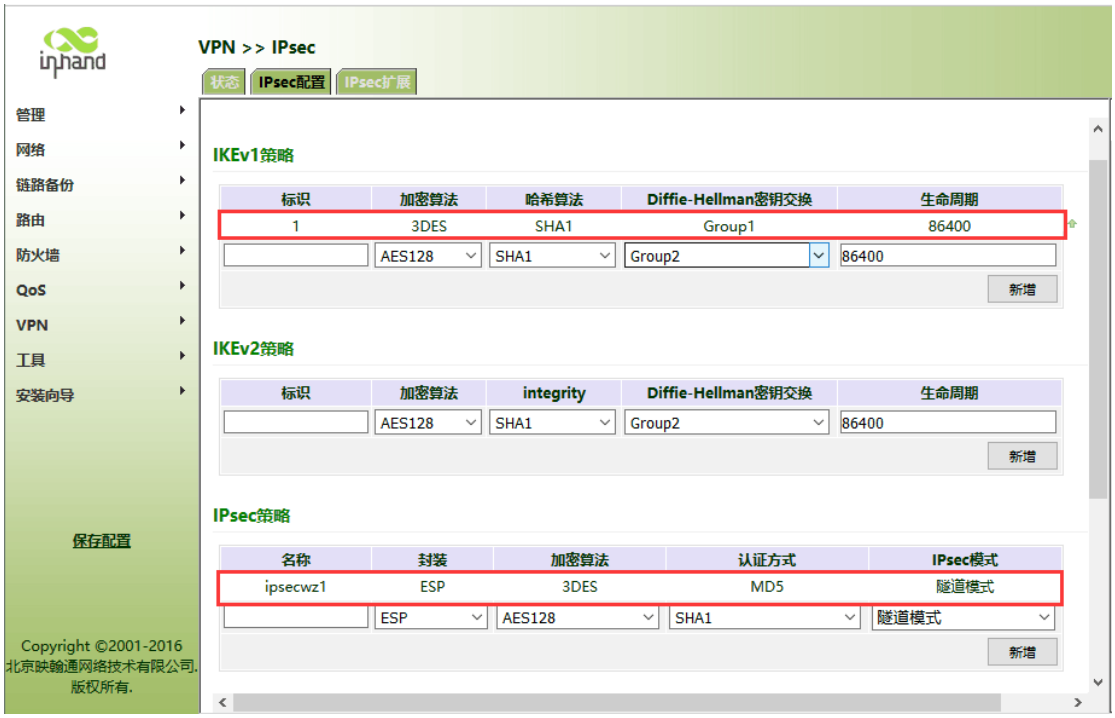


图 4-17-3

第二步：单击导航树中的“VPN>>IPSec”进入“IPSec 配置”界面，单击“IPSec 隧道配置”处的<新增>，在新打开的界面配置参数，如图 4-17-4 所示。



图 4-17-4

（3）查看 VPN 状态

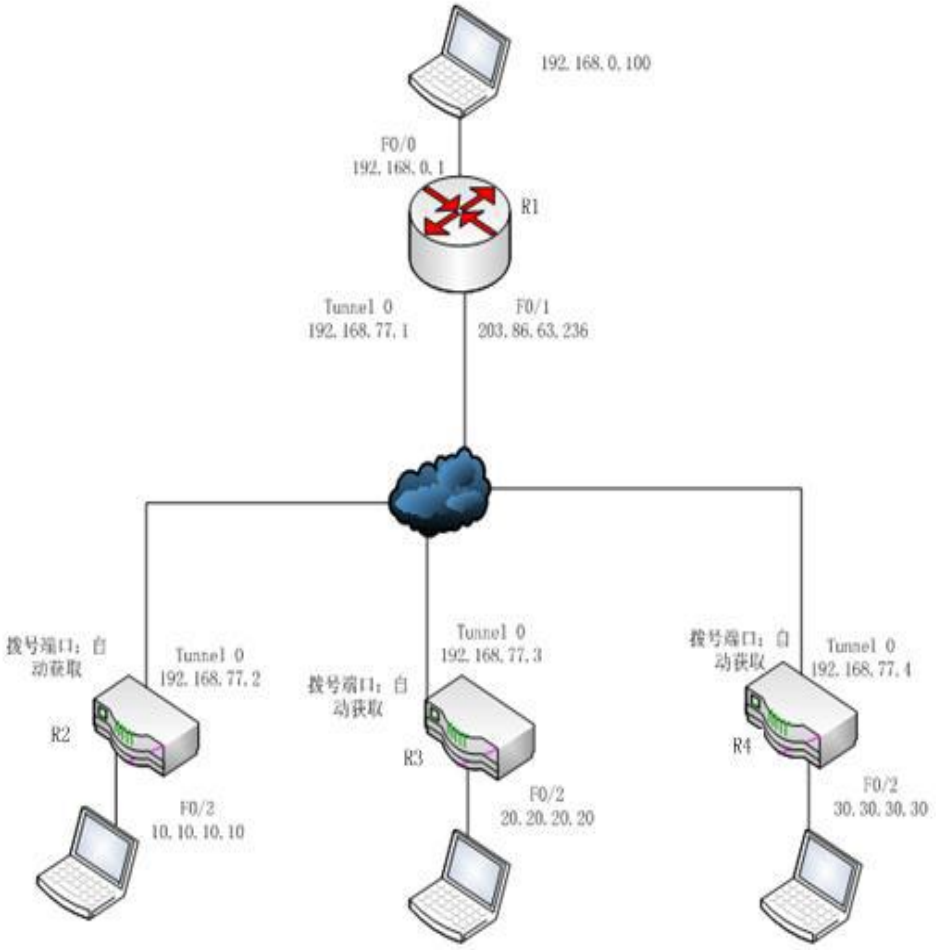
单击导航树中的“VPN>>IPSec”进入“IPSec 状态”界面，查看参数，如图 4-17-5 所示。



图 4-17-5

4.18 DMVPN 组网配置举例

网络拓扑



组网环境：

- R1:拥有固定公网IP地址（即HUB）
- R2/R3/R4:拨号上网,动态获得公网IP地址（即SPOKE ）
- 需求:R2/R3/R4与HUB建立DMVPN ， 使得各个内网均能互访.
- 涉及知识点:GRE tunel / NHRP / 动态路由协议的配置 / IPSec VPN 。

组网设置：

（1）R2/R3/R4的配置

第一步：配置IPSec

单击导航树中的“VPN>>IPSec”进入“IPSec 配置”界面，配置参数，如图 4-18-1 所示。

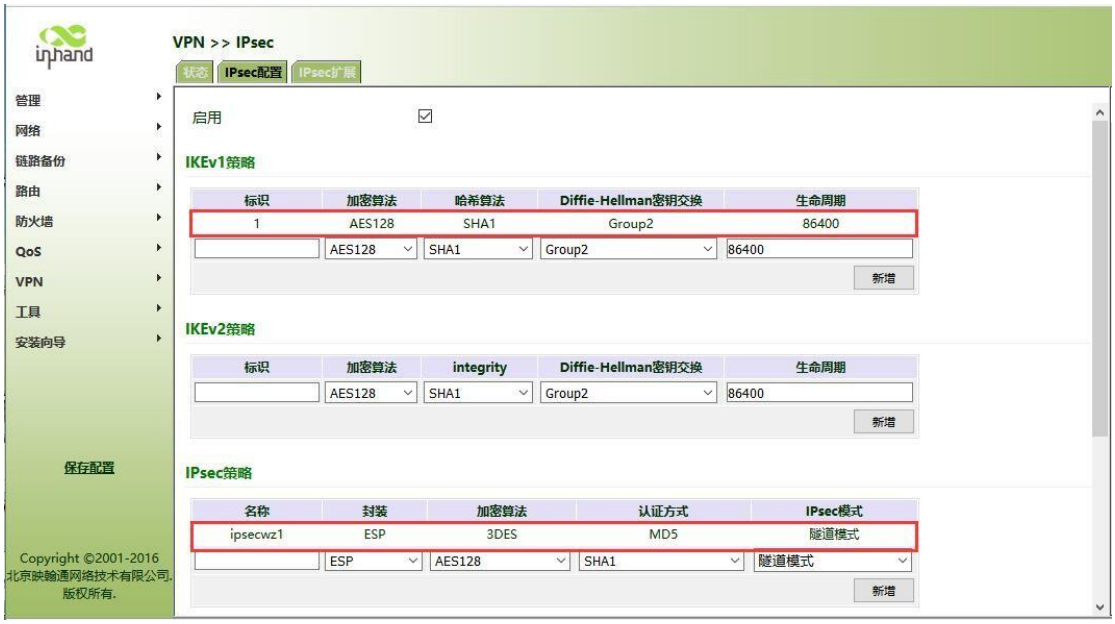


图 4-18-1

单击导航树中的“VPN>>IPSec”进入“IPSec 扩展”界面，配置参数，如图 4-18-2 所示。



图 4-18-2

第二步：配置GRE

单击导航树中的“VPN>>GRE”菜单，进入“GRE”界面，点击<新增>进入GRE配置界面，配置参数，如图4-18-3所示。



图4-18-3

第三步：配置动态路由RIP

单击导航树中的“路由>>动态路由”菜单，进入“RIP”界面，配置参数，如图4-18-4所示。



图4-18-4

第四步：查看IPSec状态

单击导航树中的“VPN>>IPSec”菜单，进入“IPSec状态”界面，查看状态，如图4-18-5

所示。



图4-18-5

（2）HUB的配置（采用命令配置方式）

第一步：配置 IPSec VPN

#ipsec config

crypto ipsec-daemon stop

crypto ikev1 policy 1

encryption 3des

hash sha1

group 2

lifetime 86400

crypto ikev1 keyring test_keyring

pre-shared-key address 0.0.0.0 0.0.0.0 key 1234567890

crypto ikev1 profile test

authentication pre-share

identity local address

match identity remote address

keyring test_keyring

policy 1

dpd 180 60

crypto ipsec transform-set ipsecwz1 esp-3des esp-md5-hmac

mode tunnel

crypto ipsec profile test

set ikev1-profile test

set transform-set ipsecwz1

set security-association lifetime seconds 3600

18:34:23 Router#第二步：配置 GRE 和 NHRP

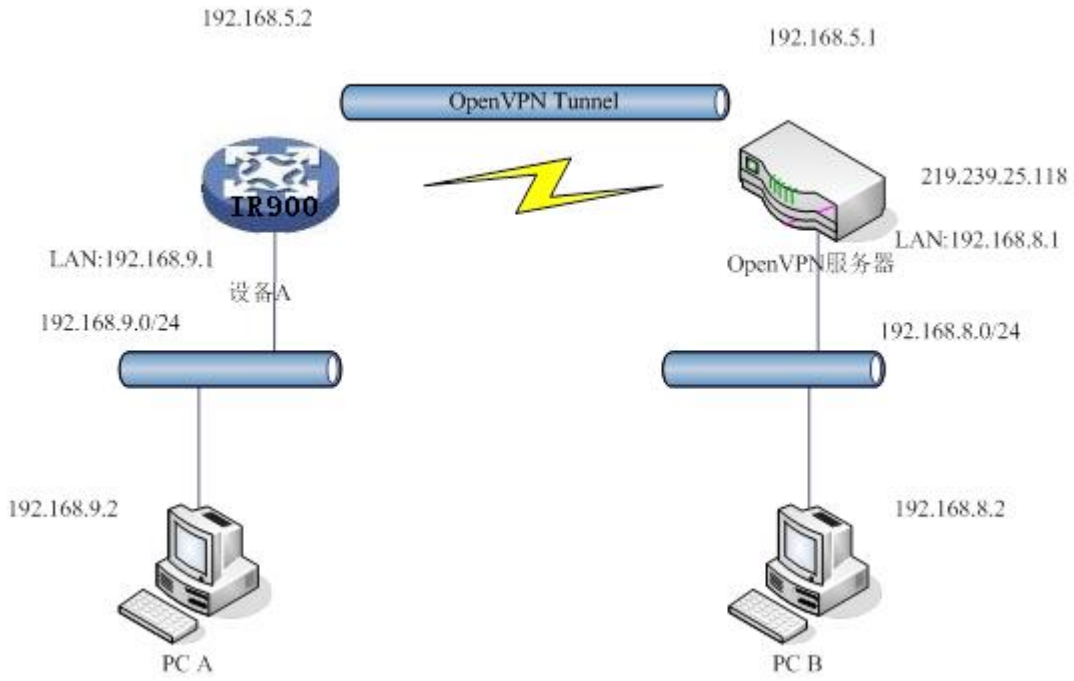
```
interface Tunnel1
 ip address 192.168.77.1 255.255.255.0
ip mtu 1436
 ip nhrp map multicast dynamic
 ip nhrp network-id 10
 ip nhrp holdtime 180
 no ip split-horizon
 tunnel source FastEthernet0/1
 tunnel mode gre multipoint
 tunnel key 123456
 tunnel protection ipsec profile abc
```

第三步：动态路由协议的配置

```
HUB(config)#router rip
HUB(config-router)#network 192.168.0.1 255.255.255.0
HUB(config-router)#network 192.168.77.1255.255.255.0
```

4.19 OPENVPN 应用举例

应用举例：OpenVPN 是基于 TCP/UDP 的 VPN，可以应用于任何端口。其举例拓扑图如下图所示。



图中，设备 A 与 OpenVPN 服务器建立一条 OpenVPN 隧道。隧道两端的虚拟 IP 分别为 192.168.5.2 和 192.168.5.1。

a. 如果设备 A 设置其 OpenVPN 为路由模式，此时去往 192.168.8.0/24 子网的将路由到 OpenVPN 隧道，到达 OpenVPN 服务器。相应地，OpenVPN 服务器也要增加一条静态路由，使得去往 192.168.9.0/24 的包路由到 OpenVPN 隧道。这样，PC A 和 PC B 通过 OpenVPN 隧道连通了，并可以双向访问。

b. 如果设备 A 设置其 OpenVPN 为 NAT 模式，OpenVPN 服务器并不需要增加关于 192.168.9.0/24 静态路由。此时 PC A 可以访问 PC B，但 PC B 不能直接访问到 PC A。适用于主动上传的情况。

路由器配置步骤如下：

第一步：配置设备的 OpenVPN 相关参数，如图 4-19-1 所示。



图 4-19-1

第二步：隧道建立成功后，对应不同认证类型需要不同证书配置。认证类型和证书对应情况如下：

None ------ 不需要证书

Pre-shared Key ----- 不需要证书

User/Password ----- 只需要 CA 证书，如：ca.crt

X.509 Cert(multi-client), X.509 Cert ----- 需要 CA 证书，设备公钥证书，设备私钥证书。如：ca.crt, my.crt, my.key

注意

1. CA 和公钥证书的后缀为.crt；私钥证书的后缀为.key。
2. 使用证书功能时，设备的时间必须是准确的。

第三步：配置好路由器以后，配置 OpenVPN 服务器。增加一条到达 192.168.2.0/24 的静态路由，route add -net 192.168.2.0 netmask 255.255.255.0 dev tun0 (假设 OpenVPN server 的网络接口为 tun0)

附录　命令行指令说明

1 帮助命令

在控制台输入 help 或 ？可获取命令帮助，在输入命令的过程中可随时输入 ？获取当前命令或命令参数的帮助，在命令或命令参数唯一时还能自动补全命令或参数。

1.1 help

【命令】help [<cmd>]

【功能】获取命令的帮助。

【视图】所有视图

【参数】<cmd>　命令名

【举例】

- ✧ 输入：　help

  获得当前所有可用命令的列表。

- ✧ 输入：　help show

  显示 show 命令的所有参数及其使用说明。

2 视图切换命令

2.1 enable

【命令】enable [15 [<*password*>]]

【功能】切换到特权用户级别。

【视图】普通用户视图

【参数】15　　用户权限级别，目前只支持权限级别15（超级用户）

<*password*>　　特权级别对应的密码，如果不输入则会给出输入密码的提示

【举例】在普通用户视图下输入：　enable adm

切换到超级用户，密码为123456。

2.2 disable

【命令】disable

【功能】退出特权用户级别。

【视图】超级用户视图，配置视图

【参数】无。

【举例】在超级用户视图下输入：　disable

返回普通用户视图。

2.3 end 和 ！

【命令】end 或 ！

【功能】退出当前视图，返回前一视图。

【视图】配置视图

【参数】无

【举例】在配置视图下输入： end

返回到超级用户视图。

2.4 exit

【命令】exit

【功能】退出当前视图，返回前一视图（如果当前为普通用户视图则退出控制台）。

【视图】所有视图

【参数】无

【举例】

- ✧ 在配置视图下输入： exit

  返回到超级用户视图。
- ✧ 在普通用户视图下输入： exit

  退出控制台。

3 查看系统状态命令

3.1 show version

【命令】show version

【功能】显示路由器的型号、软件版本等信息

【视图】所有视图

【参数】无

【举例】输入： show version

显示如下信息：

型号	：显示设备当前出厂型号
序列号	：显示设备当前出厂序列号
说明	: www.inhand.com.cn
当前版本	：显示设备当前版本

当前 Bootloader 版本　：显示设备当前版本

3.2 show system

【命令】show system

【功能】显示路由器系统信息

【视图】所有视图

【参数】无

【举例】输入：　show system

显示如下信息：

例如：00:00:38 up 0 min, load average: 0.00, 0.00, 0.00

3.3 show clock

【命令】show clock

【功能】显示路由器的系统时间

【视图】所有视图

【参数】无

【举例】输入：　show clock

显示如下信息：

例如 Sat Jan　1 00:01:28 UTC 2000

3.4 show modem

【命令】show modem

【功能】显示路由器的MODEM状态

【视图】所有视图

【参数】无

【举例】输入：　show modem

显示如下信息：

Modem 类型

状态

厂商

产品名称

信号级别

注册状态

IMSI 号码

网络类型

3.5 show log

【命令】show log [lines <n>]

【功能】显示路由器的系统日志，默认显示最新的100条日志。

【视图】所有视图

【参数】lines <*n*> 限制显示的日志条数，其中 n 为正整数时显示最新的n 条日志，为负整数时显示最早的 n 条日志，为0表示输出所有日志。

【举例】输入： show log

显示最新的100条日志记录。

3.6 show users

【命令】show users

【功能】显示路由器的用户列表。

【视图】所有视图

【参数】无

【举例】输入： show users

显示系统用户列表如下：

User:

---

* adm

其中带 * 号的用户为超级用户。

3.7 show startup-config

【命令】show startup-config

【功能】显示路由器的启动配置。

【视图】超级用户视图、配置视图

【参数】无

【举例】输入： show startup-config

显示系统的启动配置。

3.8 show running-config

【命令】show running-config

【功能】显示路由器的运行配置。

【视图】超级用户视图、配置视图

【参数】无

【举例】输入： show running-config

显示系统的运行配置。

4 查看网络状态命令

4.1 show interface

【命令】show interface

【功能】显示路由器的接口状态信息。

【视图】所有视图

【参数】无

【举例】输入： show interface

显示所有接口的状态。

4.2 show route

【命令】Show ip route

【功能】显示路由器的路由表。

【视图】所有视图

【参数】无

【举例】输入：Show ip route

显示系统的路由表。

4.3 show arp

【命令】show arp

【功能】显示路由器的ARP表。

【视图】所有视图

【参数】无

【举例】输入： show arp

显示系统的 ARP 表。

5 网络测试命令

路由器提供了 ping、telnet 和 traceroute 等网络测试工具用于网络测试。

5.1 ping

【命令】ping <*hostname*> [count <*n*>] [size <*n*>] [source <*ip*>]

【功能】对指定的主机执行ICMP探测。

【视图】所有视图

【参数】<*hostname*>　要探测的主机地址或域名

count <*n*>　探测的次数

size <*n*>　探测数据包的大小（字节）

source <*ip*>　指定探测时所使用的IP地址

【举例】输入：　ping www.g.cn

执行对 www.g.cn 的探测并显示探测结果。

5.2 telnet

【命令】telnet <*hostname*> [<*port*>] [source <*ip*>]

【功能】telnet登录到指定的主机。

【视图】所有视图

【参数】<*hostname*>　要telnet登录的主机地址或域名

<*port*>　telnet的端口

source <*ip*>　指定telnet登录时所使用的IP地址

【举例】输入：　telnet 192.168.2.2

telnet 登录到 192.168.2.2。

5.3 traceroute

【命令】traceroute <*hostname*> [maxhops <*n*>] [timeout <*n*>]

【功能】对指定的主机执行路由探测。

【视图】所有视图

【参数】<*hostname*>　要探测的主机地址或域名

maxhops <*n*>　探测的最大路由跳数

timeout <*n*>　每一跳探测的超时时间（秒）

【举例】输入：　traceroute www.g.cn

执行对 www.g.cn 的路由探测并显示探测结果。

6 配置命令

在超级用户视图下，路由器可用 configure 命令切换到配置视图对路由器进行管理。一

些设置命令同时支持 no 和 default 两种变形，其中 no 表示取消某项参数的设置，default 表示恢复某项参数为默认配置。

6.1 configure

【命令】configure terminal

【功能】切换到配置视图，从终端输入配置。

【视图】超级用户视图

【参数】无

【举例】在超级用户视图下输入： configure terminal

切换到配置视图。

6.2 hostname

【命令】hostname [<*hostname*>]

default hostname

【功能】显示或设置路由器的主机名。

【视图】配置视图

【参数】<*hostname*> 新的主机名

【举例】

- ✧ 在配置视图下输入： hostname
  显示路由器的主机名。
- ✧ 在配置视图下输入： hostname MyRouter
  设置路由器的主机名为 MyRouter。
- ✧ 在配置视图下输入： default hostname
  恢复路由器的主机名为出厂设置。

6.3 clock timezone

【命令】clock timezone <*timezone*> <*n*>

default clock timezone

【功能】设置路由器的时区信息。

【视图】配置视图

【参数】<*timezone*> 时区名称，3个大写英文字母

<*n*> 时区偏差值，-12~+12

【举例】

- ✧ 在配置视图下输入： clock timezone CST -8

设置路由器的时区为东八区，时区名为CST（中国标准时间）。

✧ 在配置视图下输入： default clock timezone

恢复路由器的时区为出厂设置。

6.4 clock set

【命令】clock set <*YEAR/MONTH/DAY*> [<*HH:MM:SS*>]

【功能】设置路由器的日期和时间。

【视图】配置视图

【参数】<*YEAR/MONTH/DAY* > 日期，格式为：年-月-日

<*HH:MM:SS* > 时间，格式为：小时-分钟-秒

【举例】在配置视图下输入： clock set 2009-10-5 10:01:02

设置路由器的时间为2009年10月5日上午10点01分02秒。

6.5 ntp server

【命令】ntp server <*hostname*>

no ntp server

default ntp server

【功能】设置网络时间服务器的客户端。

【视图】配置视图

【参数】<*hostname* > 时间服务器的主机地址或域名

【举例】在配置视图下输入： sntp-client server pool.ntp.org

设置网络时间服务器地址为pool.ntp.org。

7 系统管理命令

7.1 reboot

【命令】reboot

【功能】重启系统。

【视图】超级用户视图，配置视图

【参数】无

【举例】在超级用户视图下输入： reboot

系统重新启动。

7.2 enable password

【命令】enable password [<*password*>]

【功能】更改超级用户的密码。

【视图】配置视图

【参数】<*password*> 新的超级用户密码

【举例】在配置视图下输入： enable password

按照提示输入密码。

7.3 username

【命令】username <*name*> [password [<*password*>]]

no username <*name*>

default username

【功能】设置用户名、密码。

【视图】配置视图

【参数】无

【举例】

- ✧ 在配置视图下输入： username abc password 123
  增加一个普通用户，用户名为abc，密码为123。
- ✧ 在配置视图下输入： no username abc
  删除用户名为abc的普通用户。
- ✧ 在配置视图下输入： default username
  删除所有普通用户。