

4G 无线路由器用户手册



# 4G 无线路由器 用户手册

阳光凯讯（北京）科技有限公司

本产品用户手册内容若有变动，恕不另行通知。

Ut Eros Erat , Rutrum Ut Vulputate In , Varius Vitaenibh.Donec Eutincidunt  
Libero.Donec Purus Nisi,Porttitor Dapibus Congue Id,Rutrum Vitae Metus. Ut  
Eros Erat , Rutrum Ut Vulputate In , Varius Vitaenibh.Donec Eutincidunt  
Libero.Donec Purus Nisi,Porttitor Dapibus Congue Id,Rutrum Vitae Metus

# 4G 无线路由器用户手册

## 目录

1	产品概述.....	1
2	产品外观.....	2
3	安装及功能模块配置指导.....	3
3.1	安装调试设备.....	3
3.2	登录到配置界面.....	3
3.3	接口配置.....	5
3.4	网络应用.....	12
3.5	WIFI 配置.....	20
3.6	VPN 配置.....	22
3.7	路由配置.....	27
3.8	远程设备配置.....	30
3.9	系统配置.....	31

## 1 产品概述



4G 无线路由器是一种物联网无线通信路由器，利用运营商提供的 3G/4G 网络为用户提供上网功能。

该产品采用高性能的工业级 32 位通信处理器和工业级无线模块，以嵌入式实时操作系统为软件支撑平台，同时提供 RS232, 以太网接口, WIFI 接口，该产品已广泛应用于物联网产业中，如智能交通、金融、移动 POS 终端、供应链自动化、工业自动化、智能建筑、消防、公共安全、环境保护、气象、数字化医疗、遥感勘测、军事、空间探索、农业、林业、水务、煤矿、石化等领域。

### 工业级应用设计

- ~ 采用高性能工业级无线模块
- ~ 采用高性能工业级 32 位通信处理器
- ~ 采用金属外壳，特别适合于工控现场的应用
- ~ 宽电源输入（直流电 12V/2.0A）
- ~ 设备尺寸：192mm×36mm×122mm

### 稳定可靠

- ~ 硬软双看门狗设计，保证系统稳定
- ~ 采用完备的防掉线机制，保证数据终端永远在线
- ~ SIM/UIM 卡接口内置 15KV ESD 保护
- ~ 电源接口内置反相保护和过压保护

### 功能强大

- ~ 支持 VPN（PPTP，L2TP，IPSEC）
- ~ 支持 APN/VPDN
- ~ 支持中国移动、中国联通、中国电信三大运营商的 3G/4G 网络
- ~ 支持 DHCP，防火墙，NAT，DMZ，端口映射等功能
- ~ 支持 Telnet、TFTP、FTP、HTTP 等完善的网络协议
- ~ 支持 Web 图形界面，命令行，TR069 等管理方式

## 2 产品外观



图 2-1 产品外观

4G 无线路由器的侧面视图、正面视图及背面视图如上图所示。

其中，接口说明如下：

- ANT:外置天线连接接口；
- LAN:网线接口；
- WAN:网线接口；
- CONSOLE:使用串口线进行管理的接口；
- RESET:重启按钮（按住 5~8 秒后放开，设备会恢复出厂设置）；
- DC12V:连接 12V 电源。

### 3 安装及功能模块配置指导

#### 3.1 安装调试设备

在安装 4G 无线路由器之前，应先对比设备配置清单是否齐全，然后再连接设备进行 IP 配置。

连接方法：首先使用网线连接 PC 机的网口及路由器的 LAN 口，然后在 PC 机侧进行 IP 地址设置。

设置指定 IP 地址：设置 PC 的 IP 地址为指定 IP，例如 192.168.1.9，子网掩码设为：255.255.255.0，默认网关设为：192.168.1.1。DNS 设为当地可用的 DNS 服务器。

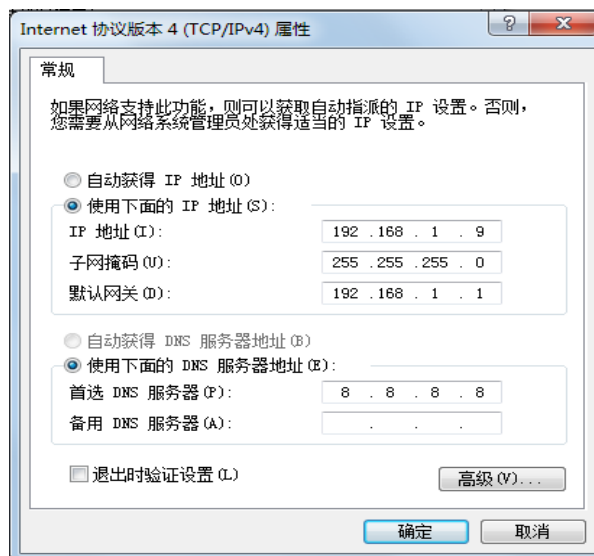


图 3-2 IP 地址设置

## 4G 无线路由器用户手册

### 3.2 登录到配置界面

4G 无线路由器支持 Web 页面配置，可通过登录浏览器进行配置，

举例说明：

打开 IE 浏览器，输入路由器出厂默认的 IP 地址（192.168.1.1）将会出现登陆页面，路由器出厂默认的用户名和密码均为“admin”。



图 3-3 登录界面

#### 3.2.1 设备概览

设备概览页面显示了设备的基本信息：3G 或 4G 无线上网卡、网络接口、VPN 的状态和流量统计等信息。

# 4G 无线路由器用户手册

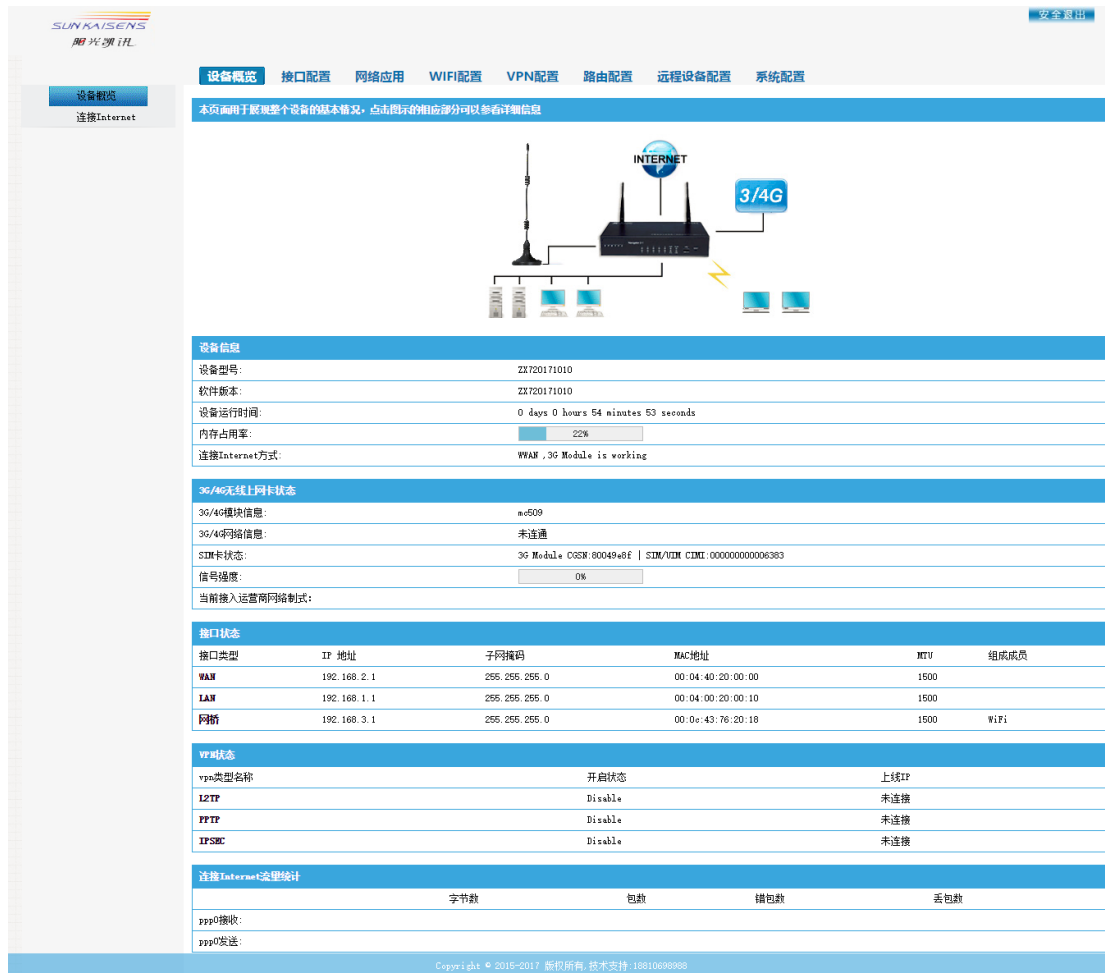


图 3-4 设备概览

## 3.2.2 连接 Internet

用于配置设备接入 Internet 上网的方式，目前支持 WWAN（3G/4G）接入、WAN 接入、WWAN（3G/4G）优先接入 WAN 备份和 WAN 优先接入 WWAN（3G/4G）备份的四种接法。

**WWAN（3G/4G）接入：**当选用此接入方式时，需要插入 WWAN 上网卡通过 3G 或 4G 模块来连接 Internet。

**WAN 接入：**当选用此接入方式时，需要插入网线指通过 WAN 口，手动

## 4G 无线路由器用户手册

配置 WAN 口 IP 或配置 PPPOE 上网账号来连接 Internet。

**WWAN (3G/4G) 优先接入 WAN 备份：**当选用此接入方式时，需要插入 WWAN 上网卡与网线，以 WWAN 上网卡为主，网线为次，当主连接 WAN 接入失效时，切换到次连接 WWAN (3G/4G) 接入；

**WAN 优先接入 WWAN (3G/4G) 备份：**当选用此接入方式时，需要插入 WWAN 上网卡与网线，

以网线为主，WWAN 上网卡为次，当主连接 WWAN (3G/4G) 接入失效时，切换到次连接 WAN 接入；

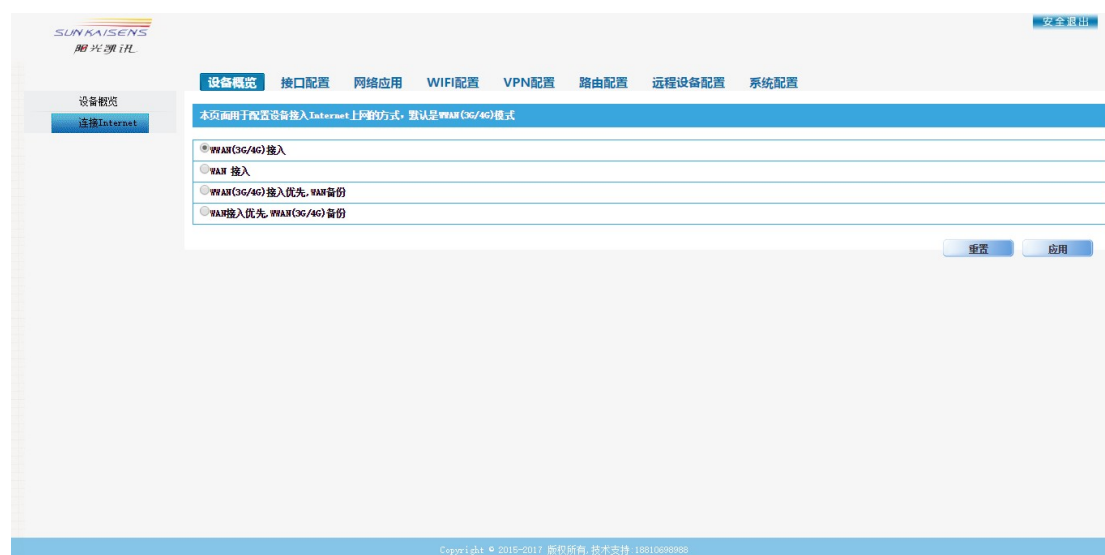


图 3-5 连接 Internet

### 3.3 接口配置

接口配置主要对于移动网络、WAN 口、LAN 口、WIFI 口以及网桥进行相



# 4G 无线路由器用户手册

应参数的配置。只有相应的接口配置正确才能保证路由器能够连接到 Internet 上。

## 3.3.1 移动网络

移动网络配置包括 3G/4G 配置，针对不同的运营商、SIM 卡类型，必须正确填写，否则无法连上运营商网络，具体页面如下图。



图 3-6 移动网络设置

参照配置项右侧的说明进行对应项的配置。其中，

### 1) APN：运营商的接入点名称

公网 APN 如下表所示，专网 APN 需联系运营商获取。

表 3-1 各运营商 APN 对应表

MCC	MNC	运营商	公网 APN
460	00	中国移动	CMNET/CMWAP
460	02	中国移动	CMNET/CMWAP
460	07	中国移动	CMNET/CMWAP
460	01	中国联通	3GNET/UNINET/

## 4G 无线路由器用户手册

			UNIWAP
460	03	中国电信	CTNET/CTLTE/CTWAP
460	11	中国电信	CTNET/CTLTE/CTWAP

### 2) 呼叫中心号码

呼叫中心号码与 APN 的对应关系如下表所示：

表 3-2 呼叫中心号码与 APN 的对应关系表

运营商 (ISP)	APN	呼叫中心号码	用户名	密码
中国联通 WCDMA	3GNET T	*99#	free	free
中国移动 TD-SCDMA	CMNET T	*98*1#	free	free
中国电信 EVDO,CDMA2000	CTLTE	#777	card	card

### 3) 网络检测

如果开启检测，必须正确填写检测目标 IP 地址,专网客户一般填写对应的数据中心服务器 IP,公网的话一般填百度等可靠服务器的 IP. 原理就是保证路由器连上网后和对端保持心跳。

### 3.3.2 WAN 配置

WAN 口连接类型共有三种：配置静态 IP，PPPoE，DHCP。

#### 1) 配置静态 IP

WAN 接口配置静态 IP 界面见下图。

# 4G 无线路由器用户手册



图 3-7 WAN 接口配置 (静态 IP)

其中：

**IP 地址**：需要自己手动配置，本例为 192.168.2.1，可以是其它 IP 地址但不能与其他口的 IP 地址冲突。

**首选 DNS 服务器**：由网络运营商提供的 DNS 服务器，例如：全国的 DNS 服务器为 114.114.114.114。

**备选 DNS 服务器**：由网络运营商提供的备选 DNS 服务器，例如：全国的备选 DNS 服务器 114.114.115.115。

**开启 NAT**：只有路由器是通过 3G/4G 模块 (WWAN) 接入外网时，此时开启 NAT 后外网与 WAN 侧 (内网) 网络设备才能互相访问。不开启只能访问内部网络。如下图所示：

## 4G 无线路由器用户手册

**网桥**：加入网桥后 WAN 口的 IP 地址将失去，此时它共享网桥的 IP 地址，

(在同一子网下，网桥的 IP 地址可查看设备概览->接口状态->网桥一栏)

### 2) PPPoE 方式

采用 **PPPoE** 方式上网，需要填写上网账号和上网密码，是否加入网桥的

选项选择“NO”，设置完成后，点击应用即可。



图 3-8 WAN 接口配置 (PPPoE)

### 3) DHCP 方式

采用 **DHCP** 方式上网，自动配置接口信息，是否加入网桥的选项选择

“NO”，设置完成后，点击应用即可。

## 4G 无线路由器用户手册

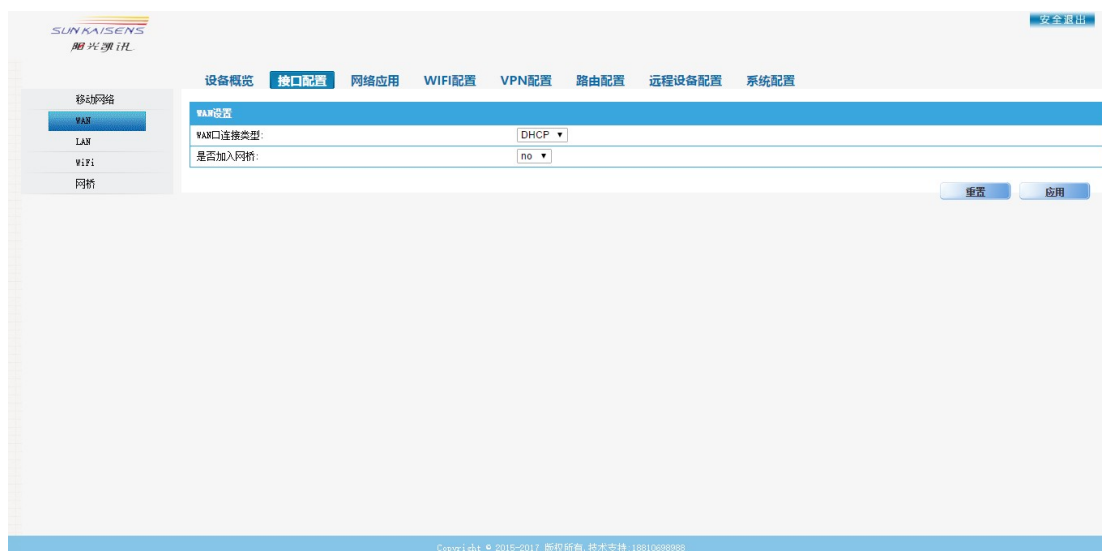


图 3-9 WAN 接口配置 (DHCP)

### 3.3.3 LAN 配置

LAN 配置页面如下图所示。



图 3-10 LAN 接口配置

其中：

**开启 NAT**：只有当 3G/4G 模块或 WAN 口以 PPPOE 方式接入外部网络时，LAN 口的 NAT 开启后外部网络与 LAN 侧的网络设备才能互相访问。不开启只

## 4G 无线路由器用户手册

能访问内部网络。

是否加入网桥：YES 或 NO，具体实际情形配置可看网桥配置一栏。

### 3.3.4 WIFI 配置

WIFI 接口配置页面如下图所示。

WiFi设置	
是否加入网桥:	yes ▼
IP地址:	<input type="text"/>
子网掩码:	<input type="text"/>
MTU:	<input type="text"/>
nat:	yes ▼

图 3-11 WIFI 接口配置

其中：

是否加入网桥：YES 或 NO，具体实际配置可看网桥配置一栏,选 YES 后，则不需要配置内网 IP 地址，内网掩码，WIFI MTU。

内网 IP 地址，子网掩码，WIFI MTU：上面 WIFI 是否加入网桥选 NO 后可以设置。

开启 **NAT**：如下图，只有当 3G/4G 模块或 WAN 口以 PPPOE 方式接入外

## 4G 无线路由器用户手册

部网络时，WIFI 口的 NAT 开启后，外部网络与 WIFI 下网络设备才能互相访问。

不开启只能访问内部网络。

下图为 WIFI 环境配置拓扑图：

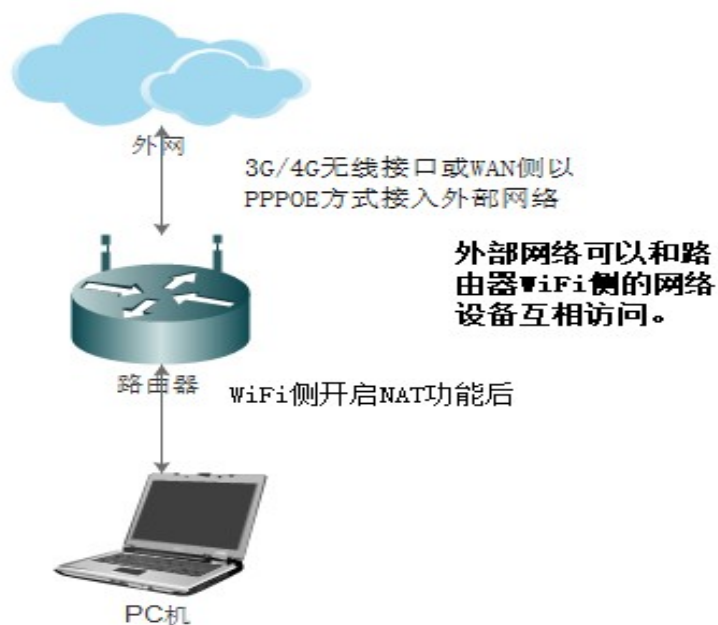


图 3-12 拓扑图

### 3.3.5 网桥配置

网桥工作在数据链路层，对加入网桥的接口，根据 MAC 地址来转发帧，

可以看作一个二层的交换机,扩展局域网最常见的方法就是使用网桥。

## 4G 无线路由器用户手册

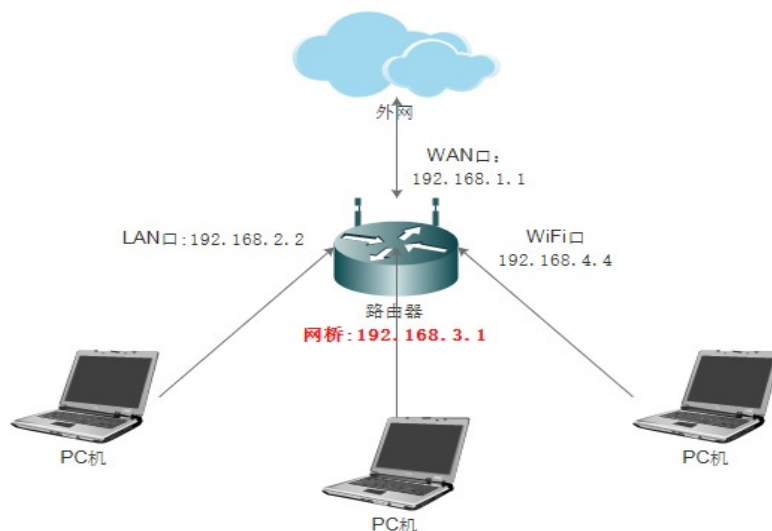


图 3-13 环境拓扑图

如图 3-13 所示的网络环境中，3 台 PC 机通过同一台路由器连接至外网，路由器的 LAN 口和 WIFI 加入网桥的前后对比见下图。加入网桥后，LAN 口和 WIFI 的 IP 地址消失，此时为一个二层口使用。

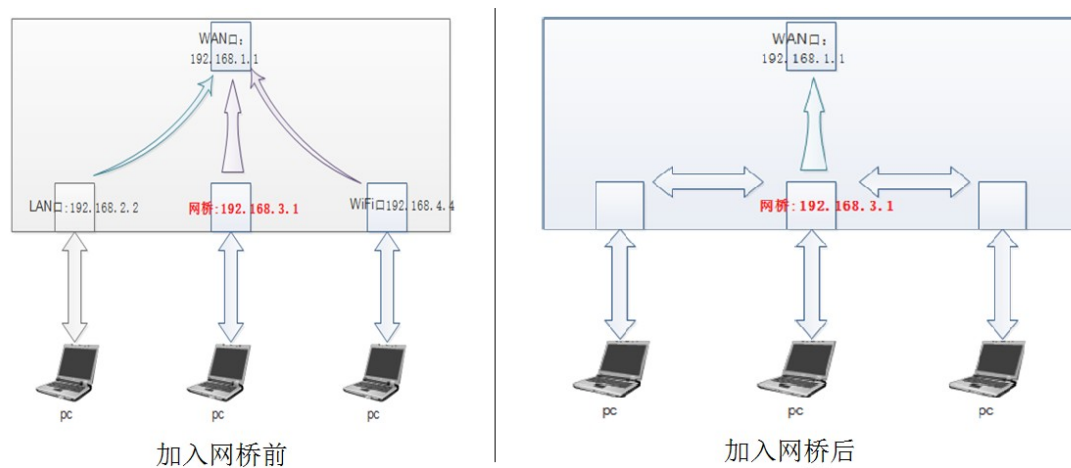


图 3-14 是否加入网桥对比图

局域网接口不足，无法接入新的主机时，可将此局域网的接口及其他的三层接口加入网桥，扩展局域网以满足新的用户接入。



# 4G 无线路由器用户手册

网桥配置页面如下图所示。



图 3-14 网桥配置

其中：

**IP 地址**：为网桥的 IP 地址，需要手动配置，可以是其它 192.168.X.X 子网下的地址，但不能与其他口的 IP 地址冲突。

**开启 NAT**：只有当 3G/4G 模块或 WAN 口以 PPPOE 方式接入外部网络时，开启 NAT 后网桥下的网络设备才能与外部网络互相访问。不开启只能访问内部网络。

## 3.4 网络应用

网络应用部分主要针对一些常用的网络功能的配置，包括 VRRP、透明代理、链路备份、端口映射、远程服务、DHCP、防火墙、动态域名、DMZ、端

## 4G 无线路由器用户手册

口限速等功能的配置。

### 3.4.1 VRRP

VRRP 是一种容错协议，通过把几台路由设备联合组成一台虚拟的路由设备，并采用一定的机制，保证当主机的下一跳设备出现故障时，可以及时将业务切换到其它设备，从而保持通讯的连续性和可靠性。

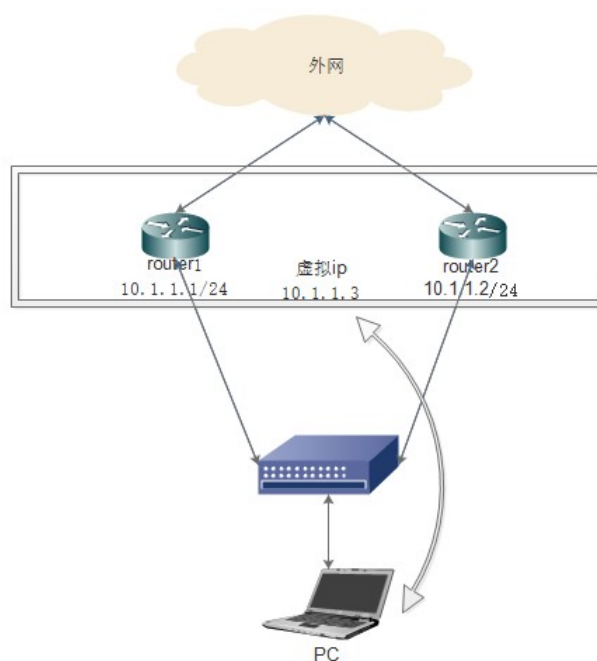


图 3-15 VRRP 环境拓扑图

在上图所示网络环境中，当 PC 机访问外部网络时，默认网关是 Route1。

当 Route1 发生故障时，PC 机无法访问外部网络。对 Route1 和 Route2 设置 VRRP 后，当 Route1 发生故障时，Route2 可代替 Route1 成为 PC 机访问网络的默认网关，从而实现内部网络与外部网络不间断通信。

VRRP 配置界面如下图所示。



图 3-16 VRRP 配置

图片说明如下：

**开启**：选择“YES”启用 VRRP 协议。

**网络接口**：选择 LAN 口。

**开启虚拟 MAC 绑定**：选择“NO”。

**虚拟 IP**：即 Route1 和 Route2 所组成虚拟路由组的虚拟 IP，可以是 Route1 或 Route2 的接口地址，本例中为 10.1.1.3。

**优先级**：在 VRRP 路由器组中，按优先级选举主控路由器，VRRP 协议中优先级范围是 0-255，255 优先级最高，优先级最高的为虚拟路由组的主控路由，其他为备份路由。

**虚拟 ID**：为 Route1 和 Route2 组成虚拟路由组的标识，范围为 1-255。

## 4G 无线路由器用户手册

**启用认证：**选择“YES”后需要验证，填写认证类型和认证密钥。

**认证类型：**可选择“Pass”和“None”，同一虚拟 VRRP 路由组中的认证类型要相同（此例中 route1 和 route2 要相同）。

**认证密钥：**由用户自己设置，同一虚拟 VRRP 路由组的认证密钥要相同。

### 3.4.2 透明代理

路由器支持透明代理功能。需要配置路由器，指定路由器上行接口和下行接口，上行接口连接外部网络，下行接口连接用户终端。路由器上行接口根据不同的接入方式获得其 IP 地址，用户终端的 IP 地址需要配置和路由器上行接口相同的 IP 地址。路由器作为透明代理，用户终端完全不感知路由器的存在，自由地访问网络。路由器透明代理功能，使路由器完全透明的存在于用户终端和网络之间，为用户终端提供多种接入方式，而不会引入额外的网络节点，也不需要用户终端的程序或配置针对不同的接入方式进行任何修改。示例拓扑如图所示。

## 4G 无线路由器用户手册

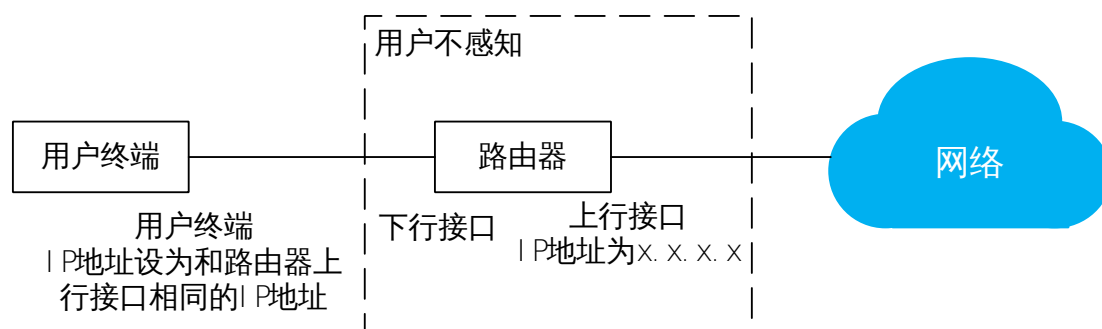


图 3-17 透明代理使用拓扑

透明代理的配置项页面如下图所示。

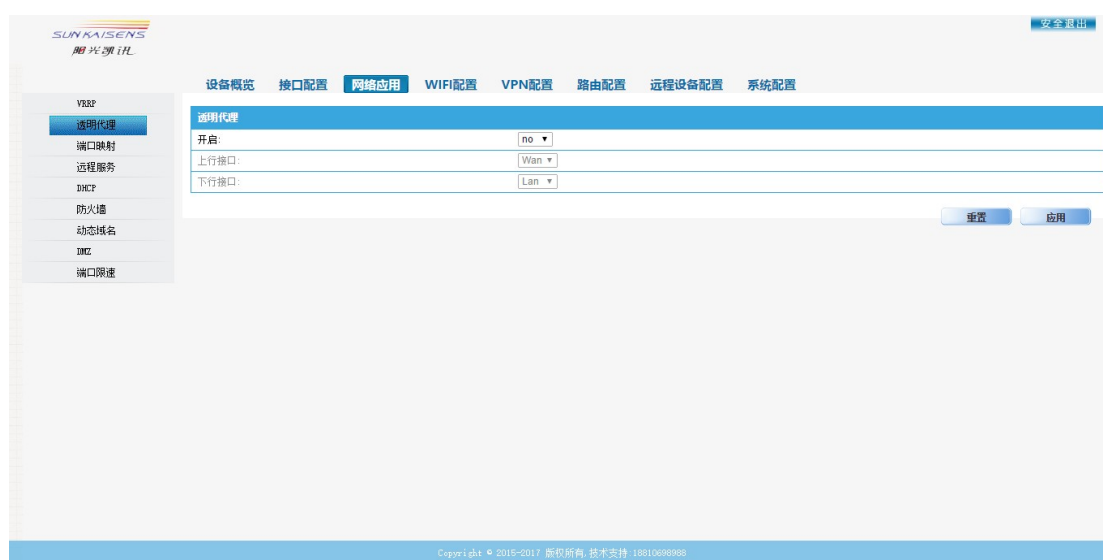


图 3-17 透明代理配置

### 3.4.3 端口映射

端口映射是 NAT 的一种，就是将外网 IP 地址的某个端口映射到内网的一台主机，以提供相应的服务。当用户访问该 IP 的这个端口时，服务器自动将请求映射到对应局域网内部的机器上。端口映射有动态和静态之分。本配置是静态的。

本产品的端口映射是关联到具体协议层次，也就是说并不是将内网 IP 端口

## 4G 无线路由器用户手册

号和外网 IP 端口号进行映射，而是将内网 IP 和端口映射到外网端口号以及外网接口，同时关注了协议类型。

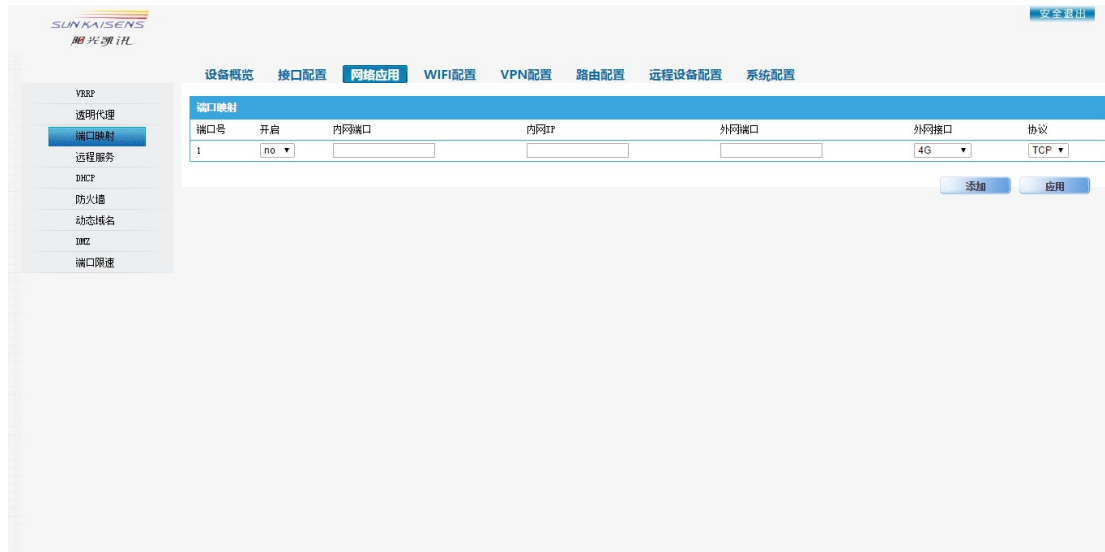


图 3-18 端口映射配置

上图示例中是将外网接口传输的 TCP 端口号 1 映射到内网 IP 地址 192.168.1.55 的 1 端口上。（前面选项中设置 NAT 地址转换不能再次添加，有冲突）

### 3.4.4 远程服务

远程服务配置主要包括对 Telnet 服务、HTTP 服务、日志服务以及 NTP 服务的使能配置。

默认 Telnet 和 HTTP 都是启动状态，不启动 Telnet 将无法远程登录到设备，不启动 HTTP，设备将无法通过 Web 进行管理。

# 4G 无线路由器用户手册



图 3-20 远程服务配置

网络日志开启可以能够搜集到 log 信息到日志服务器上，便于用户对于感兴趣的 log 信息进行搜集进行数据分析。

设备支持网络时钟同步机 NTP 的 client，因此可以配置 NTP 使能并将相应的 NTP Server 添加进入，例如：s1b.time.edu.cn（清华大学），NTP.sjtu.edu.cn(上海交通大学网络中心 NTP 服务器地址)。

### 3.4.5 DHCP 配置

支持 DHCP Server 功能。通过该功能可以对内部网络接口下的网络设备动态分配 IP 地址，可以配置 DHCP 的起始终止 IP、掩码、租约已经 DNS 等等。

## 4G 无线路由器用户手册

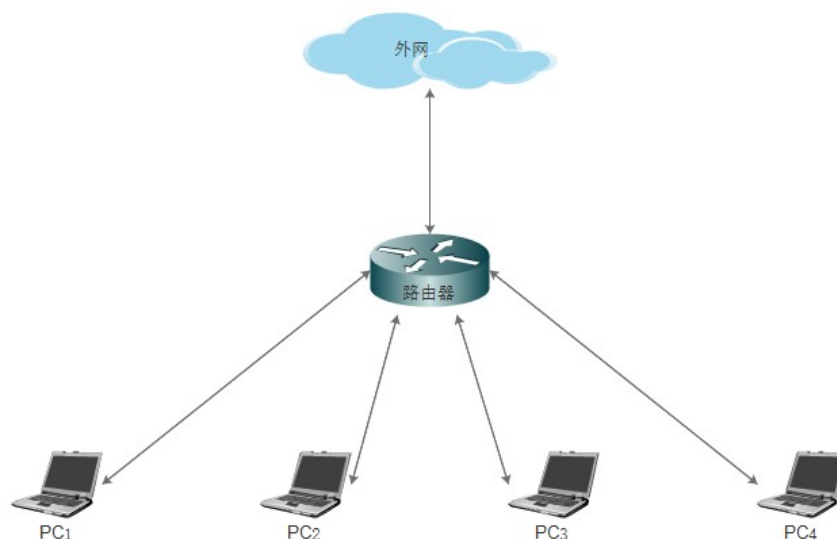


图 3-11 (DHCP 环境拓扑图)

在上图中 4 个 PC 机连接在 Router1 的内网 LAN 口下，如果手动配置 IP 地址比较麻烦，这时可采用路由器 DHCP Server 为连接路由器的 PC 机自动分配 IP 地址。

下面为 DHCP 的各个配置项。

网络接口：PC 主机连接在哪个口下，此例中 LAN 口，则选 LAN 口。

DHCP 的网络地址：DHCP 服务器的地址，本例中 192.168.1.1。

(注意：DHCP 网络地址应该和 LAN 口的 IP 地址处于同一子网)

DHCP 页面配置如下：





图 3-22 DHCP 配置

- DHCP 的子网掩码：根据具体 IP 地址的网络标识号设置。
- DHCP 的起始 IP 地址—终止 IP 地址：为连接 LAN 口下的 PC 机可分配的地址池。
- DHCP 地址租期：30 分钟，可手动更改为其它。
- DHCP DNS 模式：设置为 static（则后面的 DHCP 主 DNS、辅 DNS 需用户手动配置），设置为 dynamic，则由路由器自动配置。
- DHCP 主 DNS、辅 DNS：网络运营商提供的 DNS 服务器，也可以使用全国通用的 DNS 服务器，地址是 114.114.114.114 和 114.114.115.115
- DHCP 绑定 MAC 地址：选 NO 则后绑定 MAC 地址和绑定 MAC 地址两项不用设置，YES 的话可以为特定的主机 MAC 地址分配所指定的 IP

## 4G 无线路由器用户手册

地址，当得知 PC1 的 MAC 地址为 78:a3:51:2c:e5:0b 时，可以手动绑定所指定的 IP 地址。

### 3.4.6 防火墙配置

防火墙规则的配置，主要包含对协议，源 IP，源 MAC，目的 IP，源端口，目的端口的进行过滤相应的数据包，并做出对应的动作（如接受，拒绝，丢弃）。



图 3-23 防火墙配置

- 规则：YES 则配置的这条防火墙命令使之生效，NO 则不能。
- 链：INPUT（流进路由器的数据包），OUTPUT（流出路由器的数据包），FORWARD（本地路由器生成的包）。
- 协议：数据包的报文采用的协议，有 TCP、UDP、ICMP、ALL 等选项。

## 4G 无线路由器用户手册

- 策略：REJECT（拒绝接受报文），DROP（丢弃报文），ACCEPT（接受报文）。

### 3.4.7 DDNS 配置

DDNS（Dynamic Domain Name Server）是动态域名服务的缩写。

DDNS 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。

动态域名服务的对象是指 IP 是动态的，是变动的。普通的 DNS 都是基于静态 IP 的，有可能是一对多或多对多，IP 都是固定的一个或多个。但 DDNS 的 IP 是变动的、随机的。随着市场需求的变化，DDNS 需求功能也越来越多，越来越要求方便。

- 开启：选 YES 后启用
- 动态域名：例如：qdns
- 动态域名服务器：例如：[www.3322.org](http://www.3322.org)

## 4G 无线路由器用户手册

- 主机域名：申请到的主机域名，例如：domain.3322.org

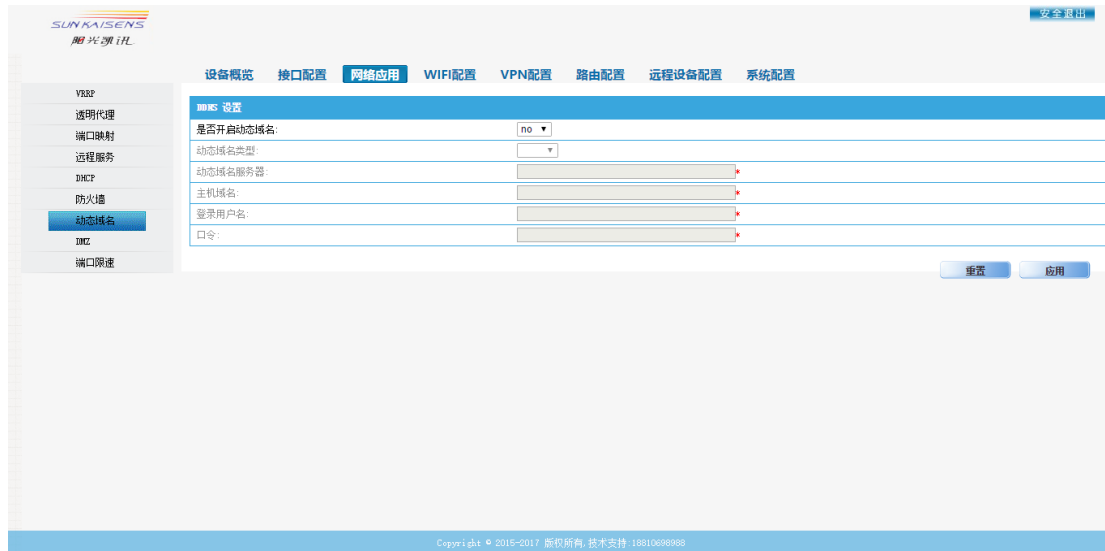


图 3-24 动态域名配置

### 3.4.8 DMZ 配置

DMZ(DemilitarizedZone)即俗称的非军事区，非军事区与军事区和信任区相对应,作用是把 Web, E-mail, 等允许外部访问的服务器单独接在该区端口，使整个需要保护的内部网络接在信任区端口后，不允许任何访问，实现内外网分离，达到用户需求。DMZ 可以理解为一个不同于外网或内网的特殊网络区域，DMZ 内通常放置一些不含机密信息的公用服务器，比如 Web、Mail、FTP 等。这样来自外网的访问者可以访问 DMZ 中的服务，但不可能接触到存放在内网中的公司机密或私人信息等，即使 DMZ 中服务器受到破坏，也不会对内网中的机密信息造成影响。

# 4G 无线路由器用户手册

DMZIP:此 IP 为内网 IP。



图 3-25 DMZ 配置

## 3.4.9 端口限速

主要是对 LAN 的 4 个端口和 WAN 口的传输速率进行限速的设置。



图 3-26 端口限速配置

## 3.5 WIFI 配置

无线路由器产品支持 WIFI 功能，对于 WIFI 的基本参数以及安全相关信息

## 4G 无线路由器用户手册

都可以配置。

### 3.5.1 基本配置

针对 WIFI 的模式、信道、SSID 等等的配置。



图 3-27 WIFI 基本配置

**SSID 号:** 为无线网络(WIFI)的名称

**开启 SSID 广播:** 设置公开无线网络名称

**开启 AP 隔离:** 开启 AP 隔离后，每一个联网的 IP 会自动划分为一个独立的 VLAN，保证用户的信息安全

### 3.5.2 安全设置

设备支持无线网络进行加密功能，支持 10 种加密方式<sup>1</sup>，以保证用户信息安全。不同的加密方式有不同的验证方法，可以根据环境来选择，一般选择应

<sup>1</sup> Disable、OPENWEP、SHAREDWEP、WEPAUTO、WPA、WPA-PSK、WPA2、WPA2-PSK、WPAPSKWPA2PSK、WPA1WPA2。

## 4G 无线路由器用户手册

用最广泛的 WPA2PSK 加密方式。



图 3-28 WPA2PSK 加密配置方式

访问策略动作有三种选择：

- wireless disable：禁止他人使用此网络（可以看到、连接到，但无法使用）
- wireless allow：允许他人连接网络并使用
- wireless reject：拒绝他人连接网络

### 3.6 VPN 配置

本设备支持 VPN 功能，共支持 L2TP、IPSEC 以及 PPTP 三种 VPN 类型。

VPN 属于远程访问技术，其主要的功能就是利用公用网络架设专用网络。

在公用网络上建立专用网络，进行加密通讯。在企业网络中有广泛应用。VPN

## 4G 无线路由器用户手册

网关通过对数据包的加密和数据包目标地址的转换实现远程访问。

### 3.6.1 L2TP

L2TP<sup>2</sup>是 VPDN<sup>3</sup>隧道协议的一种。

VPDN 是指利用公共网络（如 ISDN 或 PSTN）的拨号功能接入公共网络，实现虚拟专用网，从而为企业、小型 ISP、移动办公人员等提供接入服务。即，VPDN 为远端用户与私有企业网之间提供了一种经济而有效的点到点连接方式。

VPDN 采用专用的网络通信协议，在公共网络上为企业建立安全的虚拟专网。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，而公共网络上其它用户则无法穿过虚拟隧道访问企业网内部的资源。

**VPDN 有以下两种实现方式：**

#### (1) 接入服务器发起 VPDN 连接

如下图所示，远程系统的拨号用户通过 PPPoE/ISDN 拨入 LAC，由 LAC 端（指 NAS）发起 L2TP 隧道连接。由 LAC 通过 Internet 向 LNS 发起建立隧道连接请求。将客户的 PPP 连接直接连到企业的 VPDN 网关上，从而与

<sup>2</sup> Layer 2 Tunneling Protocol，二层隧道协议

<sup>3</sup> Virtual Private Dial-up Network，虚拟私有拨号网



## 4G 无线路由器用户手册

VPDN 网关建立隧道。



图 3-19 服务器发起 VPDN 连接拓扑

### (2) 用户发起 VPDN 连接

如下图所示，直接由 LAC 客户（指本地支持 L2TP 协议的用户）发起 L2TP 隧道连接。LAC 客户获得 Internet 访问权限后，可直接向 LNS 发起隧道连接请求，无需经过一个单独的 LAC 设备建立隧道。LAC 客户的私网地址由 LNS 分配。

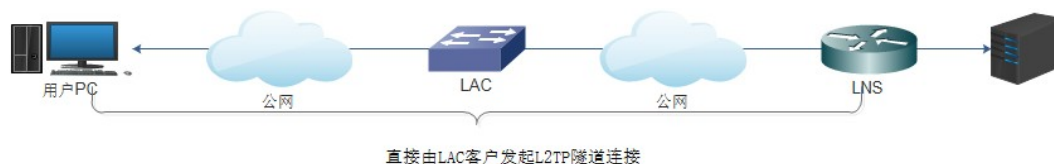


图 3-30 用户发起 VPDN 连接拓扑

下图为配置页面。



图 3-31 L2TP 配置

## 3.6.2 IPSEC

随着物联网设备不断融入人们的日常生活，物联网设备与互联网的连接就成为不可缺少的条件。那么物联网设备接入互联网时，又如何确保网络通讯的安全呢？而早已演进成熟的 IPsec 就成为物联网设备确保网络通讯安全的选择。

IPsec 协议，不是一个单独的协议，而是一系列为 IP 网络提供完整安全性的协议和服务的集合。

IPsec 协议是一个工作在 IP 网络层的协议，作为一个隧道协议实现了 VPN 通信第三层隧道协议，可以在 IP 层上创建一个安全的隧道，使两个异地的私有网络连接起来，或者使公网上的计算机可以访问远程的企业私有网络。

IPsec VPN 场景应用：（如下图所示）

1) Site-to-Site（站点到站点或者网关到网关）：

## 4G 无线路由器用户手册

如 3 个机构分布在互联网的 3 个不同的地方，各使用一个网关相互建立 VPN 隧道，企业内网（若干 PC）之间的数据通过这些网关建立的 IPsec 隧道实现安全互联。

### 2) End-to-End（端到端或 PC 到 PC）：

两个 PC 之间的通信由两个 PC 之间的 IPsec 会话保护，而不是网关。

### 3) End-to-Site（端到站点或者 PC 到网关）：

两个 PC 之间的通信由网关和异地 PC 之间的 IPsec 进行保护。

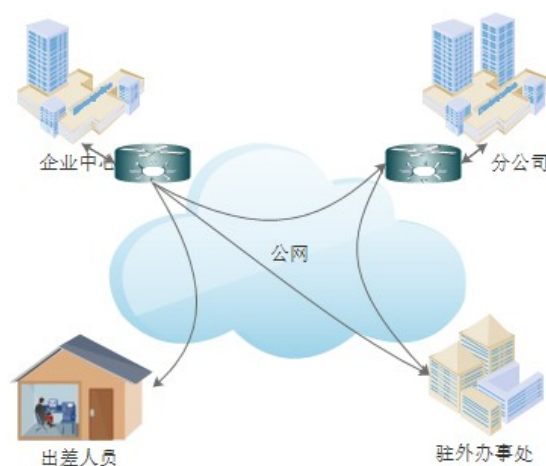


图 3-32 IPsec 应用环境拓扑

- IPsec 在企业中心与分支机构之间提供安全的隧道服务；
- 出差职员也可以通过 PC 直接发起的 IPsec 隧道介入公司总部网关；
- 连接线表示安全的 IPsec 隧道，虽在公网上传输，但都得到加密和认证保护；

# 4G 无线路由器用户手册

下图为配置页面：



图 3-33 IPsec 配置

模式选择：

主模式被设计成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；交换的身份信息受已生成的 Diffie-Hellman 共享密钥的保护。

但这增加了 3 条消息的开销。

野蛮模式则允许同时传送与 SA、密钥交换和认证相关的载荷。将这些载荷组合到一条消息中减少了消息的往返次数，但是就无法提供身份保护了。

## 3.6.3 数字证书

设备支持上传数字证书用于认证服务

数字证书又称为数字标识，是标志网络用户身份信息的一系列数据。它提供了一种在互联网上身份验证的方式，是用来标志和证明网络通信双方身份的数字信息文件。通俗地讲，数字证书就是个人或单位在互联网的身份证。

数字证书是由作为第三方的法定数字认证中心（CA）中心签发，以数字证书为核心的加密技术可以对网络上传输的信息进行加密和解密、数字签名和签名验证，确保网上传递信息的机密性、完整性，以及交易实体身份的真实性，签名信息的不可否认性，从而保障网络应用的安全性。

下图为配置页面：



图 3-34 数字证书配置

## 4G 无线路由器用户手册

### 3.6.4 PPTP

PPTP<sup>4</sup>即点对点隧道协议，是一种二层的 VPN 技术。一般用于用户终端需直接拨入 VPN 访问内网，且无需对数据使用 IPSEC 加密的场景。

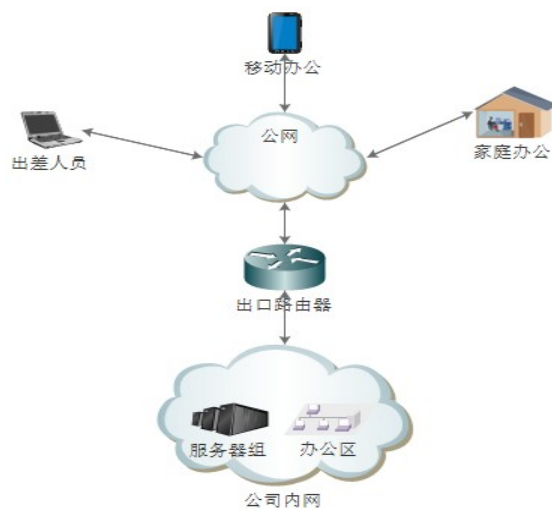


图 3-35 PPTP 环境拓扑

PPTP 主要应用在分公司或者企业的移动办公人员，需要通过公网访问企业内部的资源要连接服务器时，通过建立 PPTP 隧道，可以通过 PPTP VPN 拨入企业内网，访问企业内部资源。让用户跟服务器看起来像处于同个局域网内，实现安全通信。

下图为配置页面：

<sup>4</sup> Point to Point Tunneling Protocol



图 3-36 PPTP 配置

## 3.7 路由配置

在因特网中进行路由选择和报文转发要使用路由器，路由器根据所收到的报文的地址选择一条合适的路径（通过某一网络），并将报文传送到下一个路由器。路径中最后的路由器负责将报文送交目的主机。

### 3.7.1 路由表

每台路由器中都保存着一张本地管理路由表，同时各个路由协议也维护着自己的一张路由表。对于一个路由表，首先我们要有需要到达的目的地址网段、网关、子网掩码、出接口、

对于上表中的 br0 是网桥接口，eth2.2 对应着 WAN 口，eth2.1 对应着 LAN 口。标志常用的有 U 和 G，U 代表当前路由可用，G 代表路由需要转发可

## 4G 无线路由器用户手册

达。跳数是动态路由转达需要经过的路由器个数。



图 3-37 添加静态路由环境拓扑

以上图为例添加 PC 到服务器的静态路由：

R1 : 添加目的 IP 为 192.168.5.0 网段的，通过 eth0/1 (192.168.2.50) 发出。

R2 : 添加目的 IP 为 192.168.1.0 网段的，通过 eth0/0 (192.168.4.50) 发出。

### 3.7.2 添加路由

由用户或网络管理员手工配置的路由信息称为静态路由。

静态路由一般适用于比较简单的网络环境，能够清楚地了解网络的拓扑结构，便于设置路由信息。对于如下图所示组网，添加静态路由：

1、对于 Host A 需要配置网关为 192.168.4.3，Host B 默认网关为 192.168.2.11

2、对于 Ra 需要添加静态路由如下：



# 4G 无线路由器用户手册



图 3-38 添加静态路由配置

完成后查看路由表，如下：



图 3-39 查看路由表

这样路由器的静态路由就设置完成了。

### 3.7.3 动态路由

动态路由是指路由器能够自动地建立自己的路由表，并且能够根据实际情况的变化适时地进行调整。

## 4G 无线路由器用户手册

动态路由是默认时关闭的，需要时要手动开启，这里我们可以使用的动态路由为 RIP，时我们还可以设置动态路由的管理密码，防止别人未经许可进行设置。

RIP 是一种基于距离矢量（Distance-Vector，D-V）算法的协议，它通过 UDP 报文进行路由信息的交换。主要用于规模较小的网络中，比如结构较简单的地区性网络。

组网如下所示：

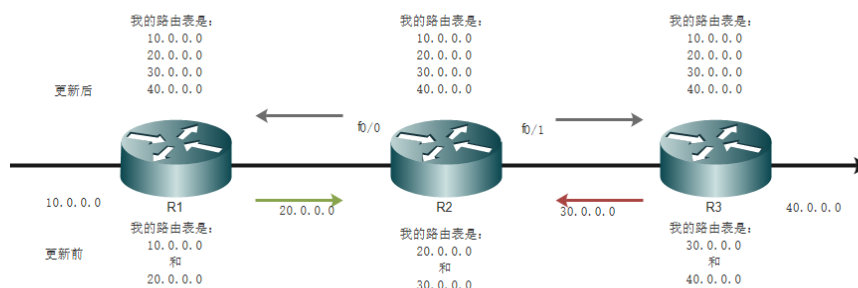


图 3-40 动态路由 RIP 交互过程

它的原理就是向相邻的路由器发送报文，更新自己的路由表。

我们需要设置的是，配置 WAN 口和 LAN 口的 IP 地址，开启动态路由如下：

## 4G 无线路由器用户手册

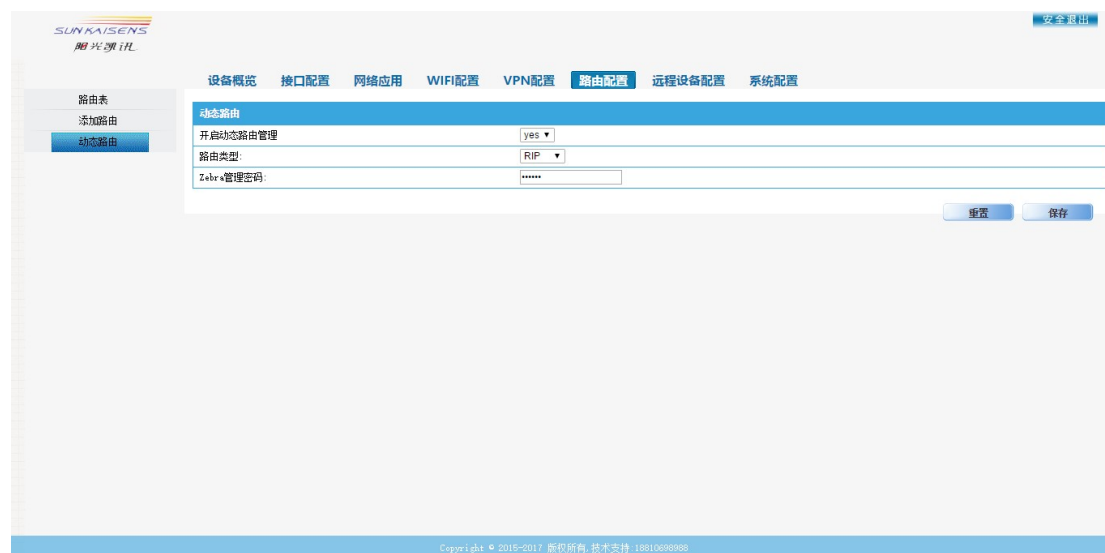


图 3-41 DHCP 配置

配置完成后，我们同样可以查看路由表进行检查。

## 3.8 远程设备配置

### 3.8.1 TR-069

TR-069，即 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、路由器等设备进行远程集中管理。

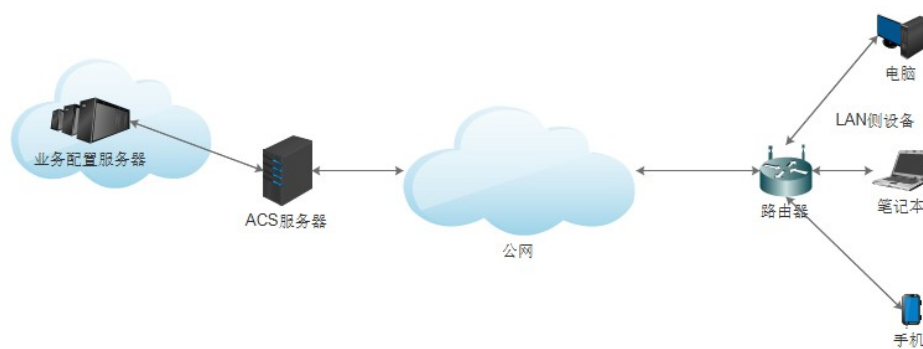


图 3-42 TR-069 环境拓扑

对于网络设备的维护传统的做法是运营商的维护人员上门进行安装或调试

## 4G 无线路由器用户手册

设备，通过 LAN 侧管理接口做一些设备配置或故障诊断的工作。但是，这种一对一的人工服务方式显然运行效率不高而且需要花费大量的人力。

而有了 ACS 服务器后，ACS 为自动配置服务器，负责对终端设备 CPE 进行管理。我们则可以通过对 ACS 服务器的修改达到控制管理用户的设备。URL，用户名/密码由服务运营商提供。



图 3-43TR-069 配置

## 3.9 系统配置

系统配置除了对于路由器基本参数配置外还提供了像软件升级、重启路由器、恢复出厂以及导入导出配置，查看系统日志等相应的动作。

### 3.9.1 系统基本配置

配置路由器的管理员账号密码以及路由器名称,开启或关闭 WatchDog 功

## 4G 无线路由器用户手册

能。

WatchDog 功能主要是针对环境恶劣，设备异常出现的假死现象，开启后设备能自动检测到并能及时通过重启修复。



图 3-44 系统基本配置

### 3.9.2 恢复出厂配置

进入恢复出厂页面，点击恢复出厂，则系统恢复到默认配置，所有的配置全部清空（要做好备份）。

# 4G 无线路由器用户手册

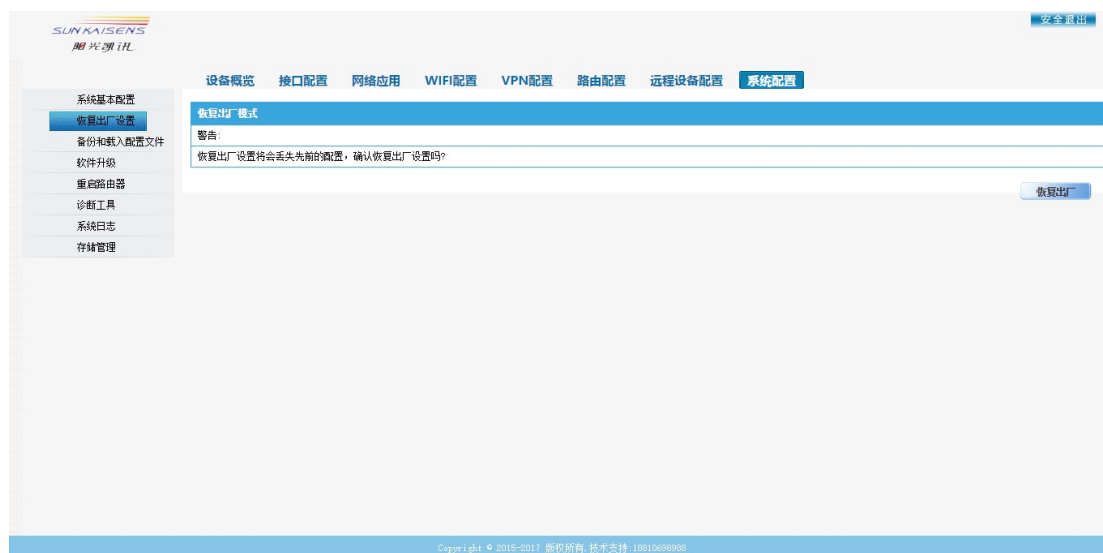


图 3-45 恢复出厂设置

## 3.9.3 备份和载入配置文件

可以将当前配置以 txt 文本文件形式保存到本地，同时也可以上传配置文件到设备中。



图 3-46 备份和载入配置文件

设置步骤：

**备份：**点击下载配置文件，选择保存路径（保存时需要更改为.txt 文件），

## 4G 无线路由器用户手册

如下图所示：

**恢复：** 点击浏览按钮，选择需要上传的配置文件，点击上传文件。

### 3.9.4 软件升级

提供软件在线升级功能，点击浏览按钮，选择需要上传的升级软件包。

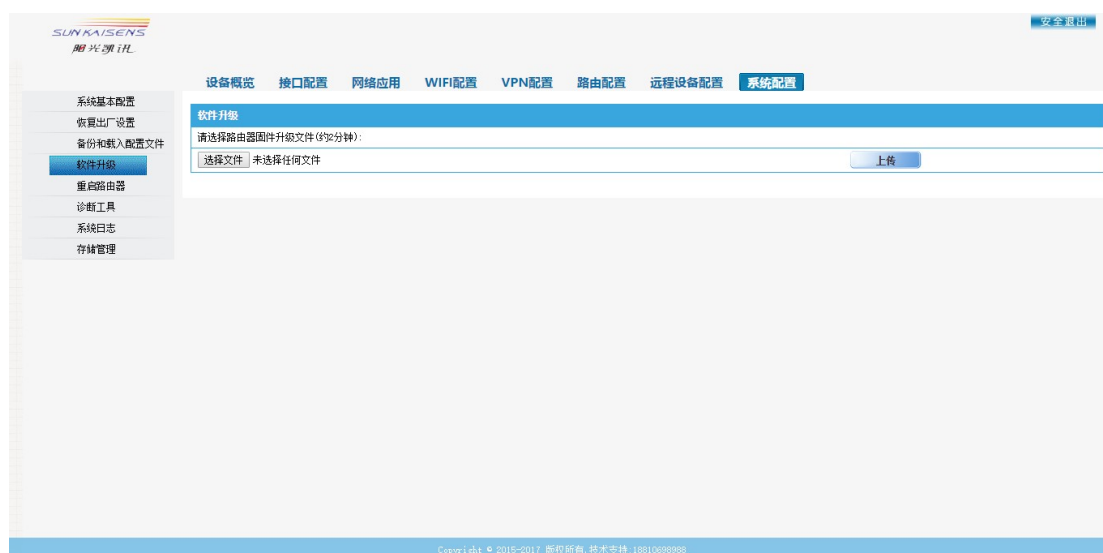


图 3-47 软件升级

### 3.9.5 重启路由器

对路由器进行重启,另外可以设置路由器自动重启功能，（重启后会恢复到保存前的配置）

## 4G 无线路由器用户手册



图 3-48 重启路由器

点击重新启动路由器，界面会显示“设备开始重启”提示信息

### 3.9.6 诊断工具

通过 ping 包进行测试网络连通性以及时延。如图：



图 3-20 诊断工具

### 3.9.7 系统日志

可以进行日志信息查询，并且可以下载到本地查看。



# 4G 无线路由器用户手册

The screenshot shows the '系统日志' (System Log) page of a 4G wireless router. The page has a sidebar on the left with navigation options: 系统基本配置, 恢复出厂设置, 备份和载入配置文件, 软件升级, 重启路由器, 诊断工具, 系统日志 (selected), and 存储管理. The main content area is titled '日志管理' and contains a '系统日志' section with a '下载' button. Below this, a log of system events is displayed, showing timestamps and messages related to AT commands and network connections for two different phone numbers (1462 and 1478). The log entries include information about carrier status, connection attempts, and successful connections.

```
t[1462]: M
Jan 1 08:04:50 (none) local2.info chat[1462]: NO CARRIER
Jan 1 08:04:50 (none) local2.info chat[1462]: -- failed
Jan 1 08:04:50 (none) local2.info chat[1462]: Failed (NO CARRIER)
Jan 1 08:04:50 (none) daemon.err pppd[916]: Connect script failed
Jan 1 08:05:22 (none) local2.info chat[1465]: abort on (NO CARRIER)
Jan 1 08:05:22 (none) local2.info chat[1465]: abort on (NO DIALTONE)
Jan 1 08:05:22 (none) local2.info chat[1465]: abort on (ERROR)
Jan 1 08:05:22 (none) local2.info chat[1465]: abort on (NO ANSWER)
Jan 1 08:05:22 (none) local2.info chat[1465]: abort on (BUSY)
Jan 1 08:05:22 (none) local2.info chat[1465]: abort on (Username/Password Incorrect)
Jan 1 08:05:22 (none) local2.info chat[1465]: send (atM)
Jan 1 08:05:22 (none) local2.info chat[1465]: expect (OK)
Jan 1 08:05:22 (none) local2.info chat[1465]: M
Jan 1 08:05:22 (none) local2.info chat[1465]: OK
Jan 1 08:05:22 (none) local2.info chat[1465]: -- got it
Jan 1 08:05:22 (none) local2.info chat[1465]: send (ATD#777M)
Jan 1 08:05:22 (none) local2.info chat[1465]: expect (CONNECT)
Jan 1 08:05:22 (none) local2.info chat[1465]: M
Jan 1 08:05:22 (none) local2.info chat[1465]: M
Jan 1 08:05:22 (none) local2.info chat[1465]: MODE: 0'M'M
Jan 1 08:05:22 (none) local2.info chat[1465]: M'M
Jan 1 08:05:22 (none) local2.info chat[1465]: 'RSSILVL:0'M'M
Jan 1 08:05:22 (none) local2.info chat[1465]: M'M
Jan 1 08:05:22 (none) local2.info chat[1465]: 'RSSILVL:0'M'M
Jan 1 08:05:22 (none) local2.info chat[1465]: M'M
Jan 1 08:05:22 (none) local2.info chat[1465]: 'CRSSI: 99'M'M
Jan 1 08:05:22 (none) local2.info chat[1465]: M'M
Jan 1 08:05:22 (none) local2.info chat[1465]: 'HRRSSI: 99'M
Jan 1 08:05:27 (none) local2.info chat[1465]: M
Jan 1 08:05:27 (none) local2.info chat[1465]: NO CARRIER
Jan 1 08:05:27 (none) local2.info chat[1465]: -- failed
Jan 1 08:05:27 (none) local2.info chat[1465]: Failed (NO CARRIER)
Jan 1 08:05:27 (none) daemon.err pppd[916]: Connect script failed
Jan 1 08:05:59 (none) local2.info chat[1478]: abort on (NO CARRIER)
Jan 1 08:05:59 (none) local2.info chat[1478]: abort on (NO DIALTONE)
Jan 1 08:05:59 (none) local2.info chat[1478]: abort on (ERROR)
Jan 1 08:05:59 (none) local2.info chat[1478]: abort on (NO ANSWER)
Jan 1 08:05:59 (none) local2.info chat[1478]: abort on (BUSY)
Jan 1 08:05:59 (none) local2.info chat[1478]: abort on (Username/Password Incorrect)
Jan 1 08:05:59 (none) local2.info chat[1478]: send (atM)
Jan 1 08:05:59 (none) local2.info chat[1478]: expect (OK)
Jan 1 08:05:59 (none) local2.info chat[1478]: M
Jan 1 08:05:59 (none) local2.info chat[1478]: OK
Jan 1 08:05:59 (none) local2.info chat[1478]: -- got it
Jan 1 08:05:59 (none) local2.info chat[1478]: send (ATD#777M)
Jan 1 08:05:59 (none) local2.info chat[1478]: expect (CONNECT)
Jan 1 08:05:59 (none) local2.info chat[1478]: M
Jan 1 08:05:59 (none) local2.info chat[1478]: M
Jan 1 08:05:59 (none) local2.info chat[1478]: MODE: 0'M'M
Jan 1 08:05:59 (none) local2.info chat[1478]: M'M
Jan 1 08:05:59 (none) local2.info chat[1478]: 'RSSILVL:0'M'M
Jan 1 08:05:59 (none) local2.info chat[1478]: M'M
Jan 1 08:05:59 (none) local2.info chat[1478]: 'RSSILVL:0'M'M
Jan 1 08:05:59 (none) local2.info chat[1478]: M'M
Jan 1 08:05:59 (none) local2.info chat[1478]: 'CRSSI: 99'M'M
Jan 1 08:05:59 (none) local2.info chat[1478]: M'M
Jan 1 08:05:59 (none) local2.info chat[1478]: 'HRRSSI: 99'M
Jan 1 08:06:04 (none) local2.info chat[1478]: M
Jan 1 08:06:04 (none) local2.info chat[1478]: NO CARRIER
Jan 1 08:06:04 (none) local2.info chat[1478]: -- failed
Jan 1 08:06:04 (none) local2.info chat[1478]: Failed (NO CARRIER)
Jan 1 08:06:04 (none) daemon.err pppd[916]: Connect script failed
Jan 1 08:06:05 (none) daemon.info pppd[916]: Exit.
Jan 1 08:21:53 (none) user.info syslog: Send at command no reply! (GetType:2, at_command:AT+CSQ'M)
Jan 1 08:51:16 (none) user.info syslog: Send at command no reply! (GetType:2, at_command:AT+CSQ'M)
Jan 1 09:19:58 (none) user.info syslog: Send at command no reply! (GetType:2, at_command:AT+CSQ'M)
```

图 3-50 系统日志