

新版路由配置说明书

目 录

1.进入路由器配置.....	2
2.上网配置说明	3
2.1 3G 拨号方式上网设置	3
2.2 有线上网方式配置	4
2.3 WIFI 客户端上网	5
2.4 路由器上网状态	6
3.VPN 配置说明	7
3.1 PPTP 服务端配置说明	7
3.2 PPTP 客户端配置说明	8
3.3 L2TP 服务端配置说明	9
3.4 L2TP 客户端配置说明	10
3.5 IPsec 服务端配置说明	12
3.6 IPsec 客户端配置说明	14
4.NAT 端口转发	15
4.1 NAT/端口转发配置说明	15
4.2 端口范围转发说明	15
4.3 DMZ 使用说明	16
5. 串口应用配置说明	16
5.1 串口 DTU 功能	17
5.2 纯 TCP/纯 UDP 应用	18
5.3 TCP 服务器说明	19
6. 动态域名解析（DDNS）使用说明	19
6.1 3322 动态域名配置说明	20
6.2 花生壳动态域名配置说明	20
6.3 88ip 动态域名配置说明	21
7. 双链路版本使用说明	22
7.1 WIFI 为主 3G 备份配置说明	22
7.2 带宽叠加（负载均衡）配置	24

声明：

本文档为测试指导性文档，对于配置部分均为参考性配置，具体配置请按照实际条件进行配置。有不了解的参数请参照光盘中的产品说明书。

本文档通用型功能针对 F3X34/F3X24/F3X25/F3B3X 系列有效，特殊功能仅对具体型号具备的功能有效。

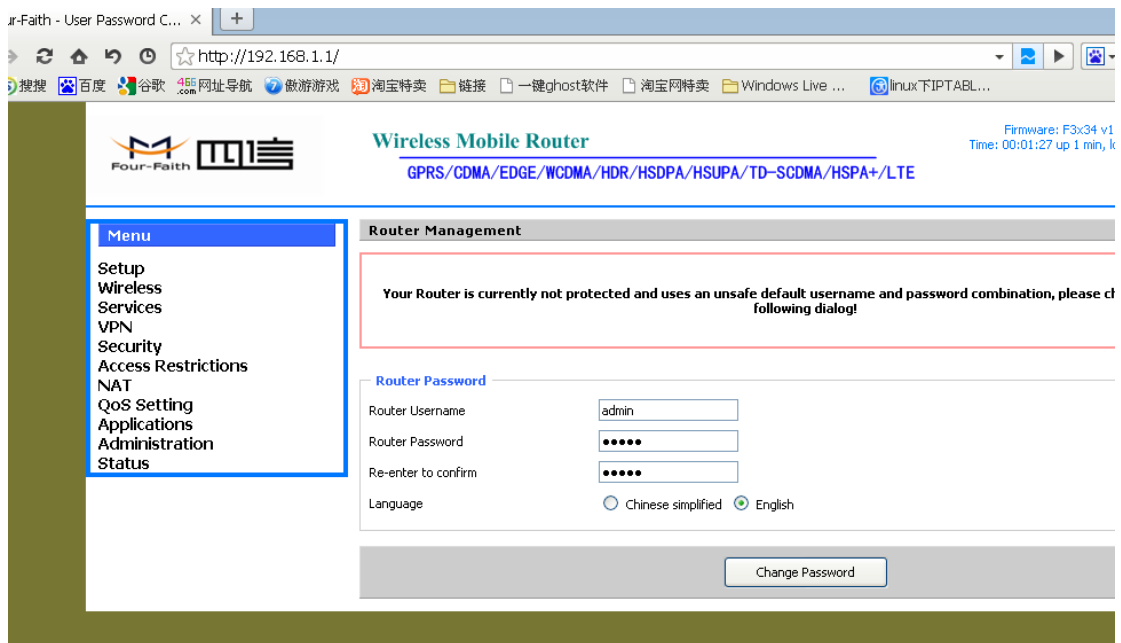
四信技术部 刘斌

1.进入路由器配置

四信路由器上电后，电脑用网线跟路由器 LAN 口连接，然后在浏览器输入网关地址即可进入路由器 WEB 配置页面。F3X34 默认为 192.168.1.1，F3X24 默认为 192.168.1.2。或者 PC 网络设置为自动获取方式，然后查看 PC 获得的 IP 和网关。如下所示：



首次进入 WEB 配置页面会有如下所示的语言选择和帐号密码设置，设置完登录 WEB 页面的帐号密码及配置页面显示的语言后，点击下面按钮，即可保存生效并进入配置页面。



2.上网配置说明

2.1 3G 拨号方式上网设置

3G 拨号上网时，正常情况下插入对应的运营商 SIM 卡后路由器即会自动拨号上网。这种情况下设置主要为路由器 WAN 口的拨号基本设置。进入配置页面后，“设置”----“基本设置”中的“WAN 口连接类型”选择为 3G/UMTS/4G/LTE。

The screenshot shows the 'WAN设置' (WAN Settings) page. Under 'WAN连接类型' (WAN Connection Type), the '连接类型' (Connection Type) dropdown menu is open, displaying options: 3G/UMTS/4G/LTE, 已禁用 (Disabled), 静态IP (Static IP), 自动配置 - DHCP (Automatic Configuration - DHCP), PPPoE, PPTP, L2TP, and 3G/UMTS/4G/LTE (highlighted). Other fields like '用户名' (Username), '密码' (Password), and '呼叫中心号码' (Service Number) are visible but not filled.

选择上网方式为 3G 后，下面的用户名、密码和呼叫中心号码为各个运营商网络下的设置。以电信的 3G 为例，设置如下：

This screenshot shows the same 'WAN设置' page with the '连接类型' (Connection Type) set to '3G/UMTS/4G/LTE'. A pink box highlights the configuration fields for Telia 3G: '用户名' (Username) is 'card', '密码' (Password) is masked with dots, and '呼叫中心号码' (Service Number) is '#777 (CDMA/EVDO)'. There are also checkboxes for '显示密码' (Show Password) next to the password and PIN fields.

各运营商拨号参数如下：

运营商	类别	编码	APN	用户名与密码	呼叫中心号码
移动/联通	2G	GSM	cmnet	无	无
移动/联通	2.5G	GPRS	uninet	无	*99***1#
电信	2.5G	CDMA	无	card, card	#777
移动	2.75G	EDGE	cmnet	无	*99****1#
联通	3G	WCDMA/HSDPA/HSUPA	3gnet	无	*99#
移动	3G	TD-SCDMA/HSDPA/HSUPA	cmnet	无	*98*1#
电信	3G	CDMA2000 1xEVDO	无	card, card	#777

在线保持

在线保持是 3G 拨号上网方式下的一个功能设定，为了避免路由器无通信数据发生时被运营商踢下线，我们通过在线保持的设定来维持路由器 3G 链路一直在线。此功能默认为开启，如下：

在线保持方式	Route
在线保持检测时间间隔	60 秒
在线保持检测主服务器IP	8 . 8 . 8 . 8
在线保持检测副服务器IP	166 . 111 . 8 . 238

在线保持方式：可选择 route、ping、ppp 三种方式或者关闭。

以 ping 方式为例，设置好在线保持检测时间间隔和检测服务器 IP 之后，每隔设定的检测时间，路由器就会向检测服务器 IPping 四个包，以有无得到服务器 IP 对 ping 包的回应来判断路由器是否在线。

2.2 有线上网方式配置

路由器有线上网方式即通过 WAN 口有线上网，单口路由无此功能。有线上网方式分固定 IP（固定宽带）和 PPPoE/ADSL 拨号两种。

固定 IP 方式

当有线上网为固定宽带时，路由器“基本设置”中“WAN 口连接类型”为“静态 IP”，然后在下方填入宽带的 IP 等配置，示例如下：

菜单 设置 - 基本设置 - 动态DNS (DDNS) - MAC地址克隆 - 高级路由 - VLANs - 网络 无线 服务 VPN 安全 访问限制 NAT QoS设置 应用 管理 状态	WAN设置 WAN连接类型 连接类型: 静态IP WAN IP地址: 10 . 63 . 114 . 40 子网掩码: 255 . 255 . 255 . 255 网关: 10 . 63 . 114 . 10 静态DNS 1: 218 . 85 . 152 . 99 静态DNS 2: 218 . 85 . 157 . 99 静态DNS 3: 0 . 0 . 0 . 0 STP: ☐ 启用 ☒ 禁用 可选设置 路由器名称: Four-Faith
--	--

PPPoE/ADSL 拨号

当有线上网方式为 PPPoE/ADSL 拨号时，路由器“基本设置”中“WAN 口连接类型”为“PPPoE”，然后在下方填入 PPPoE 账户信息，示例如下：

2.3 WIFI 客户端上网

路由器作为 WIFI 客户端上网时，WAN 口通过 WIFI 接入 AP 的方式上网。设置如下：

配置路由器 WIFI 参数，首先要配置好 AP 路由器，然后依照 AP 路由器来配置作为客户端的 WIFI 配置。进入配置页面，“无线”----“基本设置”，即可配置 WIFI 的各项参数。

“无线模式”，配置为“客户端”方式。其余配置均与 AP 路由器的配置一致。示例如下：

如果 AP 路由器有配置加密，则进入“无线安全”配置项配置，配置与 AP 路由器的安全配置一致。假如 AP 路由器安全模式采用 WPA2P，TKIP 加密，密码为 12345678，则客户端路由器配置示例如下：



WIFI 客户端模式下无线参数配置完后,再依据 AP 路由器来配置 WAN 口的设置,如果 AP 路由器有启用 DHCP 服务器功能,则 WAN 口设置可以为“自动配置-DHCP”方式或者“静态 IP”方式。如果 AP 路由器没有启用 DHCP 服务器,则 WAN 口设置为“静态 IP”方式。

2.4 路由器上网状态

路由器上网方式配置好以后,可以在状态页面中看到路由器 WAN 口的网络状态。“状态”----“WAN”即可看到。以 3G 拨号上网方式为例,其 WAN 口状态如下:



可以看到 3G 登录状态、信号强度、网络类型、连接时间、3G 拨号获取的 IP 地址等等。

通过状态可以看到路由器工作的各项信息。

3.VPN 配置说明

3.1 PPTP 服务端配置说明

进入路由页面打开 vpn 选项：启用 PPTP 服务器功能。

The screenshot shows the 'PPTP服务器' (PPTP Server) configuration page. The left sidebar contains a menu with options like '设置', '无线', '服务', 'VPN', '安全', '访问限制', 'NAT', 'QoS设置', '管理', and '状态'. The main content area is titled 'PPTP服务器' and includes the following fields and annotations:

- PPTP服务器**: Radio buttons for '启用' (Enabled) and '禁用' (Disabled). A red arrow points to '启用' with the annotation '启用pptp服务器'.
- 广播支持**: Radio buttons for '启用' (Enabled) and '禁用' (Disabled).
- 强制MPPE加密**: Radio buttons for '启用' (Enabled) and '禁用' (Disabled).
- DNS1**: Text input field.
- DNS2**: Text input field.
- WINS1**: Text input field.
- WINS2**: Text input field.
- 服务器IP**: Text input field containing '200.200.200.1'. A red arrow points to it with the annotation '指定一个服务器隧道IP'.
- 客户端IP**: Text input field containing '200.200.200.2-100'. A red arrow points to it with the annotation '指定一组客户端隧道IP'.
- 本地用户管理(CHAP Secrets)**: Text area containing 'test * test *'. A red arrow points to it with the annotation '添加客户端登陆用户名，用户名和密码之间用*号隔开，添加多个用户名时，每个用户名为一行'.

Below the configuration fields is a section titled 'PPTP客户端' (PPTP Client).

服务器隧道 IP 不能和客户端隧道 IP 相冲突，最好给服务端指定一个独立的 IP

填写客户端 IP 时可以将客户端 ip 的范围填写进去 L 例如 200.200.200.2--100

填写本地用户管理时用户名和密码之间用*号隔开，用户名和*及密码之间要用空格，填写多个用户名时，每个用户名为一行。

服务端建起来之后，客户端连接上 VPN 通道后会在状态下的 LAN 口界面下显示 PPTP 客户端连接的信息，如下所示。

- 状态
- 路由器
- WAN
- LAN
- 无线
- 带宽
- 系统信息

活动的客户端

主机名	IP地址	MAC地址	连接数	比例 [4096]
*	192.168.100.55	04:7D:7B:31:22:34	249	6%

动态主机配置协议

DHCP 状态	
DHCP 服务器	已启用
DHCP 守护进程	DNSMasq
起始IP地址	192.168.100.100
结束IP地址	192.168.100.149
客户端租约时间	1440 分钟

DHCP 客户端

主机名	IP地址	MAC地址	客户端租约时间
- 无 -			

PPTP 客户端

接口	用户名	Local IP	Remote IP
ppp1	test	200.200.200.2	120.42.46.98

3.2 PPTP 客户端配置说明

进入路由配置界面，开启 PPTP 客户端。

- PPTP
- L2TP
- OPENVPN
- IPSEC
- 安全
- 访问限制
- NAT
- QoS设置
- 管理
- 状态

PPTP客户端

PPTP客户端选项 ☒ 启用 ☐ 禁用

服务器IP或DNS名称 ← 填写服务器端公网IP或域名

远程子网 ← 填写服务器端子网IP

远程子网掩码 ← 填写服务器端子网的子网掩码

MPPE加密

MTU (预设: 1450)

MRU (预设: 1450)

NAT ☒ 启用 ☐ 禁用

启用手动设置隧道IP ☐ 启用 ☒ 禁用

用户名 ← 填写服务器端设置的用户名和密码

密码 ☐ 显示密码

服务器 IP 或域名要填写服务器端公网的 IP 或绑定在路由上的域名。

远程子网 IP 和子网掩码填写服务器端子网的 IP 和子网掩码。

填入在服务器端设置的用户名和密码。

客户端建起来之后，服务端连接上 VPN 通道后会在状态下的 LAN 口界面下显示 PPTP 服务端连接的信息

The screenshot shows the router's configuration page with a sidebar menu on the left containing: 菜单, 状态, 路由, WAN, LAN, 无线, 带宽, and 系统信息. The main content area is titled '本地DNS' with the value '0.0.0.0'. Below this is the '活动的客户端' (Active Clients) section, which contains a table with columns: 主机名, IP地址, MAC地址, 连接数, and 比例 [4096]. The table has one entry with IP 192.168.2.100 and MAC 44:37:E6:4E:99:87. Below the table is the '动态主机配置协议' (Dynamic Host Configuration Protocol) section. It includes a 'DHCP 状态' (DHCP Status) section where 'DHCP 服务器' is '已启用' (Enabled), 'DHCP 守护进程' is 'uDHCPd', '起始IP地址' is '192.168.2.100', '结束IP地址' is '192.168.2.149', and '客户端租约时间' is '1440 分钟'. Below this is the 'DHCP 客户端' (DHCP Clients) section with a table showing one client with IP 192.168.2.100 and MAC 44:37:E6:4E:99:87. At the bottom is the 'PPTP 服务器' (PPTP Server) section with a table showing one server with Local IP 200.200.200.2 and Remote IP 200.200.200.1. A '自动刷新[开启]' (Auto Refresh [On]) button is at the bottom right.

3.3 L2TP 服务端配置说明

进入路由配置界面，开启 L2TP 服务端。

The screenshot shows the 'L2TP 服务器' (L2TP Server) configuration page. The sidebar menu on the left includes: 菜单, 设置, 无线, 服务, VPN, PPTP, L2TP, OPENVPN, IPSEC, 安全, 访问限制, NAT, QoS设置, 管理, and 状态. The main content area is titled 'L2TP 服务器'. It includes a 'L2TP 服务器选项' (L2TP Server Options) section with 'L2TP 服务器选项' set to '启用' (Enabled) and '强制IPSEC加密' (Force IPSEC Encryption) set to '禁用' (Disabled). Below this is the '服务器IP' (Server IP) field set to '200.200.200.1' and the '客户端IP' (Client IP) field set to '200.200.200.2-10'. The '本地用户管理(CHAP Secrets)' (Local User Management (CHAP Secrets)) field is set to 'test * test *'. Below this is the 'L2TP 客户端' (L2TP Client) section with 'L2TP 客户端选项' (L2TP Client Options) set to '禁用' (Disabled). Red arrows point from the sidebar menu to the configuration fields: '启用L2TP服务器' points to the 'L2TP 服务器选项' section, '设定一个服务端隧道IP' points to the '服务器IP' field, '设定一组客户端隧道IP' points to the '客户端IP' field, and '添加客户端连接用户及密码，切记用户名和密码及*号之间用一个空格，建立多用户时在下一行建立' points to the '本地用户管理(CHAP Secrets)' field. At the bottom are buttons for '保存设置' (Save Settings), '应用' (Apply), and '取消' (Cancel).

服务器隧道 IP 不能和客户端隧道 IP 相冲突，最好给服务端指定一个独立的 IP。

填写客户端 IP 时可以将客户端 ip 的范围填写进去 L 例如：

200.200.200.2--100。

填写本地用户管理时用户名和密码之间用*号隔开，用户名和*及密码之间要用空格，填写多个用户名时，每个用户名为一行。

服务端建起来之后，客户端连接上 VPN 通道后会在状态下的 LAN 口界面下显示 L2TP 客户端连接的信息。如下所示。

状态

路由器

WAN

LAN

无线

带宽

系统信息

活动的客户端

主机名	IP地址	MAC地址	连接数	比例 [4096]
*	192.168.100.55	04:7D:7B:31:22:34	54	1%

动态主机配置协议

DHCP 状态

DHCP 服务器	已启用
DHCP 守护进程	DNSMasq
起始IP地址	192.168.100.100
结束IP地址	192.168.100.149
客户端租约时间	1440 分钟

DHCP 客户端

主机名	IP地址	MAC地址	客户端租约时间	删除
- 无 -				

L2TP 客户端

接口	用户名	Local IP	Remote IP	删除
ppp1	test	200.200.200.2	120.42.46.98	

3.4 L2TP 客户端配置说明

进入路由配置界面，开启 L2TP 客户端。

设置

无线

服务

VPN

安全

访问限制

NAT

QoS设置

管理

状态

L2TP服务器

L2TP服务器选项

☐ 启用 ☒ 禁用

L2TP客户端

L2TP客户端

L2TP客户端选项

☒ 启用 ☐ 禁用

用户名

test

填入在服务器端设置的用户名和密码

密码

•••••

☐ 显示密码

L2TP服务器

140.243.56.244

远程子网

192.168.100.0

远程子网掩码

255.255.255.0

MPPE加密

MTU

1450

(预设: 1450)

MRU

1450

(预设: 1450)

NAT

☒ 启用 ☐ 禁用

启用手动设置隧道IP

☐ 启用 ☒ 禁用

允许CHAP认证协议

☒ 是 ☐ 否

拒绝PAP认证协议

☒ 是 ☐ 否

允许认证协议

☒ 是 ☐ 否

保存设置

应用

取消

服务器 IP 或域名要填写服务器端公网的 IP 或绑定在路由上的域名。
远程子网 IP 和子网掩码填写服务器端子网的 IP 和子网掩码。
填入在服务器端设置的用户名和密码。

客户端建起来之后,服务端连接上 VPN 通道后会在状态下的 LAN 口界面下显示 L2TP 客户端连接的信息。如下所示。

状态

- 路由置
- WAN
- LAN
- 无线
- 带宽
- 系统信息

活动的客户端

主机名	IP地址	MAC地址	连接数	比例 [4096]
"	192.168.2.100	44:37:E6:4E:99:87	56	1%

动态主机配置协议

DHCP 状态

DHCP 服务器: 已启用

DHCP 守护进程: uDHCPd

起始IP地址: 192.168.2.100

结束IP地址: 192.168.2.149

客户端租约时间: 1440 分钟

DHCP 客户端

主机名	IP地址	MAC地址	过期	删除
20110810-1802	192.168.2.100	44:37:E6:4E:99:87	23:40:01	

L2TP 服务器

接口	Local IP	Remote IP	删除
ppp0	200.200.200.2	200.200.200.1	

3.5 IPsec 服务端配置说明

进入 IPSCE 配置界面，点击添加一个 IPsec 服务端。

菜单

- 设置
- 无线
- 服务
- VPN
 - PPTP
 - L2TP
 - OPENVPN
 - IPSEC
- 安全
- 访问限制
- NAT
- QoS设置
- 管理
- 状态

Wireless Mobile Router

GPRS/CDMA/EDGE/WCDMA/HSDF

全局设置

全局设置

连接状态及操作

连接状态及操作

名称	类型	通用名称
添加		

点击添加

添加一个 IPsec 服务端

The screenshot displays the VPN configuration interface with several sections:

- 连接配置 (Connection Configuration):** Includes fields for Name (FOUR), Local WAN Interface (ppp0), Local Subnet (192.168.2.0/24), Local Host ID, Remote Host Address, Remote Subnet (192.168.1.0/24), and Remote Host ID. Red arrows point to the Local Subnet and Remote Subnet fields with the note "填写本地子网IP后面加/24" (Add /24 after the local subnet IP).
- 检测 (Detection):** Includes checkboxes for DPD Detection (checked), Connection Detection (checked), and fields for Time Interval (60s) and Timeout (60s). A red arrow points to the Remote Subnet field with the note "填写对端子网IP后面加/24" (Add /24 after the remote subnet IP).
- 高级配置 (Advanced Configuration):** Includes checkboxes for Advanced Configuration (checked), IKE Encryption (3DES), IKE Integrity (MD5), IKE DH Group (MODP-1024), IKE Lifetime (1h), ESP Encryption (3DES), and ESP Integrity (MD5). A red oval highlights this section with the note "启用高级配置，IKE\ESP加密要和客户端一致" (Enable advanced configuration, IKE\ESP encryption must be consistent with the client).
- 认证 (Authentication):** Includes a checkbox for Pre-shared Key (checked) and a field for the key (123456). A red oval highlights this field with the note "添加一个共享密钥" (Add a shared key).

本地子网填写本地的网关 IP 加后缀/24 (/24就是子网掩码前24位为1, 即11111111.11111111.11111111.00000000, 表明子网掩码是255.255.255.0), 远程子网填写对端网关 IP 加后缀/24(注: 本地和对端的网段不能一样)。启用高级配置, IKE/ESP 加密信息的填写要和客户端一致。添加一个共享密钥。

在状态下看到 ESTABLISHED 就表示 IPsec 隧道已经连接。

服务 VPN - PPTP - L2TP - OPENVPN - IPSEC 安全 访问限制 NAT QoS设置 管理 状态	连接状态及操作				
	连接状态及操作				
	名称	类型	通用名称	状态	操作
	FOUR	隧道-server	192.168.2.0/24--[ppp0] server--[192.168.1.0/24]	ESTABLISHED	     

3.6 IPsec 客户端配置说明

进入 IPSCE 配置界面，点击添加一个 IPsec 客户端



添加一个 IPsec 客户端，参照服务端配置来进行客户端参数的配置。本地子网填写本地的网关 IP 加后缀/24，远程子网填写对端网关 IP 加后缀/24(注：本地和对端的网段不能一样)。启用高级配置，IKE/ESP 加密信息的填写要和服务端一致。共享密钥要和服务端的一样致。



在状态下看到 ESTABLISHED 就表示 IPsec 隧道已经连接。



4.NAT 端口转发

4.1 NAT/端口转发配置说明

当需要为路由器的用户应用或者服务分配端口转发时，可以在路由器的 NAT 功能中进行相应的配置。路由器配置页面中，进入“NAT”----“端口转发”。

应用程序：分配端口转发的应用程序名，可由用户自定义设置。

协议：配置转发的端口允许的协议，可选择 TCP/UDP，或者 both。

允许的源 IP 范围：允许外部访问此端口的 IP 的范围，无此项限制的话不填。

来源端口：配置端口转发的应用或者服务所使用的外部端口号。

IP 地址：用户访问的服务器内网 IP 地址，即端口转发对应服务器的内网 IP。

目的端口：配置端口转发的应用或者服务所使用的内部端口号。

配置完后勾选“启用”使配置端口转发规则生效。

示例：路由器下应用服务器内网 IP 为 192.168.1.100，内部所用端口为 6000，应用名“service”，转发协议为 TCP，外部来源端口配置为 8000，源 IP 无限制，则配置示例如下：



4.2 端口范围转发说明

假如一个应用程序或者服务需要对应 2000 个端口转发，那该怎么配置呢？

难道像上面端口转发那样一个个去配置吗？当然不是，我们可以采用“端口范围转发”功能，一次直接配置 2000 个端口转发给应用程序或者服务。

比如：要给应用程序分配 6000-8000 之间所有的 2001 个端口转发，转发协议为 TCP，内部服务器 IP 为 192.168.1.100，则配置如下：



配置完后，6000-8000 之间的 2001 个端口转发就全部映射给服务器 192.168.1.100，在端口范围转发时，转发的源端口与目的端口一致，均为开始到结束的端口号。

注意：端口范围转发不要启用过多端口，控制在 3000 个范围内，否则容易造成 CPU 超负荷运行。

4.3 DMZ 使用说明

DMZ 功能用于允许路由器下的一个用户直接暴露于 INTERNET，开启 DMZ 后，路由器将向开启 DMZ 的主机开放所有端口，使计算机暴露于外网。

示例：例如给 PC 192.168.1.100 开启 DMZ，则路由器所有端口均对此 PC 有效，到任意端口的数据均将被转发到此 IP。



5. 串口应用配置说明

四信路由器串口（路由器上标注 Console 口）除了可以输出路由器日志外，还可以通过串口线接工控设备，当作 DTU 来使用，或者作为串口服务器。

5.1 串口 DTU 功能

四信路由器可以开启串口 DTU 功能，将路由器下面的串口设备的数据发送到中心服务器，配置页面下点击“应用”----“串口应用”，选择启用“串口应用”即可看到串口应用的各项功能。

串口 DTU 功能主要在“协议类型”下选择相应的协议。选择“TCP (DTU)” / “UDP (DTU)” / “TCST” 三种类型的协议时，串口通信均为四信 DTU 协议通信，服务器将会收到注册包和心跳包（具体参考四信 DTU 数据格式说明）。

菜单

- 设置
- 无线
- 服务
- VPN
- 安全
- 访问限制
- NAT
- QoS设置
- 应用
 - 串口应用
- 管理
- 状态

串口应用

串口应用 ☒ 启用 ☐ 禁用

波特率 115200

数据位 8

停止位 1

校验 无

流控 无

协议类型 TCP(DTU)

服务端地址 120.20.20.20

服务端端口 5000

设备号码 13912345678

设备ID 12345678

心跳间隔 60

保存设置 应用 取消 重启路由器

串口通信参数设置，与下位机设备串口设置一致

数据传输协议类型

通信参数设置

DTU参数设置

DTU 功能协议类型说明：

TCP (DTU)：即 DTU 功能下数据走 TCP 协议通信，服务端软件端口需为 TCP 协议。

UDP (DTU)：即 DTU 功能下数据走 UDP 协议通信，服务端软件端口需为 UDP 协议。

TCST：自定义注册包和心跳包模式，在此模式下，DTU 通信的注册包和心跳包可由用户自定义，通信协议为 TCP 协议。

通信参数设置：

在 DTU 功能下，需要配置服务器的 IP 地址和应用程序监听端口，配置好这两项参数后，路由器的 DTU 服务将会向配置的 IP 和端口下的应用程序发起 TCP/UDP 连接，连接成功后即可互相通信。

DTU 参数设置：

设备号码：设备所用的 11 位 SIM 卡号码，可自由配置，方便后期管理和维护。

设备 ID：DTU 的 8 位 ID 号码，相当于 DTU 的“身份证”，服务端通过 ID 号来识别不同的 DTU，多个 DTU 连接同一个服务端时，每个的 ID 要不一致。

心跳间隔：此项设置为了避免 DTU 与服务器的连接因长时间无数据通信而被运营商断开，设置此时间间隔后，在无数据通信时，每隔此时间 DTU 将会向服务器发一个心跳包。配置时间间隔建议 31-60 秒。

DTU 功能使用示例：

例如：路由器开启 DTU 功能，采用 TCP 通信协议，服务端软件采用四信服务器中心模拟软件 VBdemo，服务器 PC 公网 IP 为 27.154.58.226，映射的端口为 5001，则配置如下：

菜单

设置

无线

服务

VPN

安全

访问限制

NAT

QoS设置

应用

管理

状态

串口应用

串口应用

串口应用

启用

禁用

波特率

115200

数据位

8

停止位

1

检验

无

流控

无

协议类型

TCP(DTU)

服务端地址

27.154.58.226

服务端端口

5001

设备号码

12345678901

设备ID

12345678

心跳间隔

60

配置完并应用后，在服务端的软件上即可看到 DTU 建立连接，服务端软件可看到设备的 ID 号、SIM 卡号码和路由器的 IP。

VB_Demo2.4

文件(F) 远程控制模式说明 帮助(H)

服务器配置

远程配置

自动回应

监听端口

5001

列表刷新时间

120

工作模式

小数据包

显示方式

Default

发送数据

发送文件

设备ID

用户ID

登录时间

用户电话号码

动态IP

12345678

2013-2-1 9:23:22

12345678901

10.50.50.5

服务器日志

接收数据

发送数据

配置日志

查看日志

删除日志

清除

2013-2-1 9:23:19VB_Demo_Server(小数据包)启动成功!端口号为:5001
若要进入远程修改模式，请在DTU登录后立即选择设备ID并选择“远程控制模式”！

5.2 纯 TCP/纯 UDP 应用

类似于 DTU 功能协议传输，纯 TCP/纯 UDP 下的传输只是无 DTU 协议下的注册包、心跳包等区别，在这两种协议下，串口应用将向服务器发起纯 TCP/纯 UDP 连接，服务端软件采用标准 TCP /UDP 协议即可。

示例如下：

5.3 TCP 服务器说明

TCP 服务器协议下，串口应用功能将作为一个 server 端，当路由器收到 TCP 客户端发过来的数据后，将会把收到的数据通过串口输出。

示例：例如本机服务器端口为 5001，则客户端发送至本机 5001 端口的 TCP 数据将全部从串口输出。

6.动态域名解析（DDNS）使用说明

路由器 3G 拨号上网或者 ADSL 拨号上网时，获得的 IP 一般不是固定的，而是动态变化的。当路由器下有某种应用的服务器或者端口，外部的用户需要访问此路由下的服务或者端口时，会面临 IP 变化无法访问的情况。

这种情况通过动态域名解析可以很好的解决，即通过 DDNS 将变化的 IP 绑定到一个固定的域名上，一旦 IP 变化，域名服务器会进行更新，将 IP 实时绑定到域名上。

四信路由器具有动态域名解析功能，不需要在 PC 上运行动态域名服务客户端，路由器内部即可绑定域名并实时跟服务器进行更新。

6.1 3322 动态域名配置说明

使用 3322 域名解析时，首先在 www.3322.net 上注册 3322 公云帐号，注册成功后每个帐号将可获得免费的 3322 动态域名一个（或者申请付费域名）。以免费 3322 动态域名为例，假如注册的 3322 域名为 macy.f3322.org，记住注册的用户名、帐号和此域名。

路由器配置页面进入 DDNS 配置页面，点击“设置”----“动态 DNS (DDNS)”即进入。

菜单

- 设置
 - 基本设置
 - 动态DNS (DDNS)
 - MAC地址克隆
 - 高级路由
 - VLANs
 - 网络
- 无线服务
- VPN
- 安全
- 访问限制
- NAT
- QoS设置
- 应用管理
- 状态

动态域名系统(DDNS)

DDNS

DDNS 服务: 3322.org (3322域名选择此项)

用户名: macy005 (3322注册的账户用户名与密码)

密码: ***** (显示密码)

主机名: macy.f3322.org (注册账户对应的动态域名)

类型: 动态

适配符: ☐

不使用外部IP检测: ☒ 是 ☐ 否

选项

强制更新间隔: 10 (默认: 10 天, 范围: 1 - 60)

DDNS 状态

DDNS 功能已禁用

保存设置 应用 取消 自动刷新[开/关]

配置完点击“应用”后，路由器会向 3322 的域名服务器发起请求，在下方会看到动态域名的更新状态。

选项

强制更新间隔: 10 (默认: 10 天, 范围: 1 - 60)

DDNS 状态

Sat Jan 1 00:03:51 2000: INADYN: Started 'INADYN Advanced version 1.96-ADV' - dynamic DNS updater.

Sat Jan 1 00:03:51 2000: I:INADYN: IP address for alias 'macy.f3322.org' needs update to '106.122.171.168'

Sat Jan 1 00:03:51 2000: I:INADYN: Alias 'macy.f3322.org' to IP '106.122.171.168' updated successfully.

显示更新成功

6.2 花生壳动态域名配置说明

使用花生壳动态域名解析时，首先在花生壳官网 www.oray.com 注册一个账户，记住注册的用户名和密码以及分配的免费域名，在路由器下 DDNS 功能进行配置，配置示例如下。

动态域名系统(DDNS)

DDNS

DDNS 服务

自定义

DYNDNS 服务器

ddns.oray.com

用户名

macy005

密码

.....

☐ 显示密码

主机名

macy.vicp.cc

域名

URL

/ph/update?hostname=

DDNS 附加选项

不使用外部IP检测

☐ 是 ☒ 否

WAN选用静态IP的话,“否”是更新外网IP,“是”是更新内网IP

选项

强制更新间隔

10

(默认: 10 天, 范围: 1 - 60)

DDNS 状态

Sat Jan 1 00:03:32 2000: INADYN: Started 'INADYN Advanced version 1.96-ADV' - dynamic DNS updater.
Sat Jan 1 00:03:33 2000: I:INADYN: IP address for alias 'macy.vicp.cc' needs update to '27.149.53.241'
Sat Jan 1 00:03:34 2000: I:INADYN: Alias 'macy.vicp.cc' to IP '27.149.53.241' updated successfully.
显示更新成功

DDNS 自定义下的 URL 地址为 DNS 服务器更新的 URL 地址。

6.3 88ip 动态域名配置说明

使用 88ip 动态域名解析时, 首先在 88ip 官网 www.oray.com 注册一个账户, 记住注册的用户名和密码以及分配的免费域名, 在路由器下 DDNS 功能进行配置, 配置如下。

Wireless Mobile Router

GPRS/CDMA/EDGE/WCDMA/HDR/HSDPA/HSUPA/TD-SCDMA/HSPA+/LTE

时间: 00:06:30 up 6 min
WAN IP: 27.149.115.224

动态域名系统(DDNS)

DDNS

DDNS 服务

DYNDNS 服务器

用户名

密码

主机名

URL

DDNS 附加选项

不使用外部IP检测

自定义

link.dipserver.com

fourfaith72

fourfaith72.88ip.cn

/elink/elink.dll/

☒ 是 ☐ 否

帮助

DDNS 服务

DDNS 允许的网络。这并更新您的 DynDNS.org ZoneEdit.com 册以得到此

强制更新间隔

在方框中输入间隔(天)。自动执行。率的限制以

选项

强制更新间隔

10

(默认: 10 天, 范围: 1 - 60)

DDNS 状态

Sat Jan 1 00:06:07 2000: INADYN: Started 'INADYN Advanced version 1.96-ADV' - dynamic DNS updater.

Sat Jan 1 00:06:07 2000: I:INADYN: IP address for alias 'macy.88ip.cn' needs update to '27.149.115.224'

Sat Jan 1 00:06:07 2000: I:INADYN: Alias 'macy.88ip.cn' to IP '27.149.115.224' updated successfully.

7.双链路版本使用说明

以下使用项限于双链路的版本。

7.1 WIFI 为主 3G 备份配置说明

此功能实现主链路为 WIFI 客户端上网方式，备份链路为 3G 上网方式，当 WIFI 断开时，会切换到 3G 上网方式，同时路由器会检测主链路的网络情况，当发现主链路网络恢复后，路由器又切换到 WIFI 上网方式。

以备份 3G 链路为移动网络为例，WAN 口设置如下：

The screenshot displays the WAN configuration page of a router. On the left is a navigation menu with options like '菜单', '设置', '基本设置', '动态DNS (DDNS)', 'MAC地址克隆', '高级路由', 'VLANs', '网络', '无线', '服务', '安全', '访问限制', 'NAT', 'QoS设置', '应用', '管理', and '状态'. The main area is titled 'WAN设置' and contains two main sections: '双链路配置选项' and '主链路WAN连接类型'. The '双链路配置选项' section has two checkboxes: '启用双链路备份功能' and '双链路同时在线', both of which are checked and have a '负载均衡' button next to them. The '主链路WAN连接类型' section shows '连接类型' set to '自动配置 - DHCP', '在线保持方式' set to 'Ping', and '在线保持检测时间间隔' set to '60秒'. Below this, there are fields for '在线保持检测主服务器IP' and '在线保持检测副服务器IP', both set to '8.8.8.8'. The 'STP' section has '启用' and '禁用' radio buttons, with '禁用' selected. The '备份链路WAN连接类型' section shows '连接类型' set to '3G Link 2', and fields for '用户名', '密码', '呼叫中心号码', 'APN', and 'PIN'. The '在线保持方式' is set to 'Ping', and '在线保持检测时间间隔' is set to '60秒'. The '在线保持检测主服务器IP' and '在线保持检测副服务器IP' are both set to '166.111.8.238'. The '是否启用手动设置WAN IP' section has '启用' and '禁用' radio buttons, with '禁用' selected. The '是否启用拨号失败重启机制' section has '启用' and '禁用' radio buttons, with '启用' selected. On the right side, there are sections for '域名:', '起始IP地址:', '最大DHCP用户数:', and '时间设置:'. A note on the right says '此两项均开启, 勿点击“负载均衡”项'. Another note says '1.如果 WIFI AP 点未开启 DHCP 服务器, 则“连接类型”选择静态 IP' and '2.在线保持方式选择为 ping'. A note at the bottom right says '(默认: 10 分钟)'.

注意事项:

1.主、备链路都通过在线保持方式来判断本链路是否在线, 比如示例中的配置为 ping 方式, 检测时间间隔 60 秒, 则每隔 60 秒路由器就会向检测服务器 IP 发出 4 个 ping 包, 以是否得到回应作为判断链路是否在线的依据。

2.在线保持检测时间间隔可依据实际需要来设置, 由于路由器是按这个时间间隔来检测链路是否在线的, 所以当链路断开后, 这个时间设置决定了切换到另一链路的需要时间间隔。

3.主、备链路在线保持检测的服务器 IP 不要设置为同一 IP, 同一链路下的检测主服务器 IP 和副服务器 IP 可以一样。

4.ping 或 route 方式下路由器是依靠检测服务器 IP 的回应来判断设备是否在线的, 所以在线保持 ping 方式下检测服务器 IP 必须设置为有效的全球 IP, 不然会导致路由器误判掉线。

在此提供几个有效的全球 IP:

8.8.8.8

202.108.22.5

220.181.6.19

218.30.13.36

WAN 口设置完成后，只需要再设置 WIFI 客户端配置即可。示例如下：

菜单

设置
无线

- 基本设置
- 无线安全
- MAC过滤
- 高级设置
- WDS

服务
安全
访问限制
NAT
QoS设置
应用
管理
状态

无线物理接口 wlan0 [2.4 GHz]

无线网络 ☒ 启用 ☐ 禁用

物理接口 ra0 - SSID [Four-Faith] HWAddr [00:0C:43:AF:3B:65]

无线模式 客户端

无线网络模式 混合

无线网络名 (SSID) AP

频道宽度 20 MHz

无线SSID广播 ☒ 启用 ☐ 禁用

网络配置 ☐ 未桥接 ☒ 已桥接

保存设置 应用 取消

无线模式设置为客户端，此时无线将作为客户端去连接 AP 路由器上网，因此 SSID 与 AP 路由器的 SSID 一致。

如果 AP 路由器带有加密，还需要在“无线安全”配置项中配置密钥等，与 AP 路由器一致即可，示例如下：

菜单

设置
无线

- 基本设置
- 无线安全
- MAC过滤
- 高级设置
- WDS

服务
安全
访问限制
NAT
QoS设置
应用
管理
状态

Wireless Mobile Router

时间: 09:14:3

GPRS/CDMA/EDGE/WCDMA/HDR/HSDPA/HSUPA/TD-SCDMA/HSPA+/LTE

无线安全 wlan0

物理接口 ra0 SSID [Four-Faith] HWAddr [00:0C:43:AF:3B:65]

安全模式 WPA2 Personal

WPA算法 TKIP

WPA共享密钥 APAPAPAPAP ☒ 显示密码

保存设置 应用

7.2 带宽叠加（负载均衡）配置

主要用于网络带宽的叠加。

假设主、备链路的带宽分别为 Akbps 与 Bkbps。

当禁用该均衡的时候，不符合分流列表的数据流，将只会使用主链路的出口访问互联网，只有在主链路掉线了，才会使用备份链路。

当启用均衡的时候，不符合分流列表的数据流，将同时使用主备两个出口。如果比例为 A:B（推荐比例），则总带宽为 (A+B) kbps。如果为 A:0，则数据将只使用主链路，总带宽仍为 Akbp，如果为 0: B，则数据将只使用备份了链路，总带宽为 Bkbps。

配置示例如下：

NAT

QoS设置

- 基本
- 分类
- 负载分配

应用管理状态

负载均衡

负载均衡

☒ 启用 ☐ 禁用

相对 1 : WAN1 : WAN2权重比例 1 :

保存设置
应用
取消

则主备链路将各走一半的数据流。

注意事项：在填写比例的时候，二者需要为互质整数，且双方的值越小越好。假设主链路为 390kbp, 备份链路为 130kbp, 则推荐比例为 3:1, 而非 390:130 或者 39: 13 等其他。如果主备链路分别为：400kbp 与 130kbps，二者最佳比例为 40: 13，为达到最佳效果，最好进一步约分，得到一个粗略的比例 3.07: 1，最后四舍五入为 3: 1。