

**温馨提示：使用文档时，打开视图中的导航窗格，可方便查看和定位目录**

## **初次登录** —— Web 登录、本地控制台、云登录等

### **登录到路由**

#### **初次启动**

系统启动后，可连接显示器和键盘，在控制台登录，更改 IP 或 Web 管理账号密码等操作。

系统启动完毕后，主板蜂鸣器会发出三声短暂的提示音：“滴—滴滴”。

LAN 口默认 IP：192.168.0.1，默认为第一个网口。

Web 管理登录地址：<http://192.168.0.1/>

Web 管理超级管理员账号及密码：admin

默认 Guest（客人）账号处于关闭状态，该账号只有查看（只读）权限，无法修改任何设置。

您可在 “系统-》登录管理-》登录账号” 中设置。

系统

常规设置

登录管理

报警 & 通知

计划任务

磁盘存储

防火墙

### 登录管理

配置Web访问、SSH登录时的信息, 包括登录密码、端口等。

Web 登录 控制台 SSH 登录 云登录 登录账号

共1条记录/1页, 每页显示 200 请输入关键字 搜索 Q 清除 x 新建账号

ID	帐号	帐号等级	备注	状态
1	demo	游客		成功

系统

常规设置

登录管理

报警 & 通知

计划任务

磁盘存储

防火墙

### 登录管理

配置Web访问、SSH登录时的信息, 包括登录密码、端口等。

Web 登录 控制台 SSH 登录 云登录 登录账号

共1条记录/1页, 每页显示 200 请输入关键字 搜索 Q 清除 x 新建账号

ID	帐号	帐号等级	备注	状态
1	demo	游客		成功

## 权限说明

- (1). 关键操作只能管理员才能执行, 比如: 修改 LAN 口设置、重启、关机、查看/导入/导出配置、恢复出厂
- (2). 自定义菜单的账号, 首页只显示有限的键信息
- (3). 游客账号不能修改任何配置

## 控制台登录

本地控制台登录是指通过物理连接的方式访问系统, 如连接键盘和显示器, 或通过 RS232 串口线连接到 CONSOLE 口或串口。

控制台登录一般用于紧急维护使用（通过 Web 无法登录到系统时），

主要执行以下操作：

修改 LAN 口 IP、Web 管理端口、Web 登录账号及密码

修改 WAN 口 IP 等信息

恢复出厂设置

默认控制台登录账号为 root，密码为 123456，无需密码即可登录

为了安全起见，建议修改默认密码，并启用“控制台登录时需要密码”

## 配置控制台登录

进入“系统” -》“登录管理” -》“本地控制台”，配置如下：

The screenshot shows the 'System' configuration page with the 'Login Management' section selected. The 'Local Console' tab is active. The settings are as follows:

Category	Setting	Value
控制台登录密码	root 帐号登录密码	为空不修改
	控制台登录时需要验证	是
串口登录	允许通过串口登录	是
	数据传输波特率	115200
其他	允许按 <b>Ctrl + Alt + Del</b> 组合键重启	否

At the bottom right, there is a blue button labeled '保存设置' (Save Settings).

按下回车键，即可登录：

```
=====
系统控制台 | 2016-02-23 16:21:01
=====

Web管理地址 http://192.168.1.254:80
初始账号/密码均为 admin, 登录后可配置所有系统参数

LAN 口状态: 192.168.1.254/255.255.255.0/00-0c-29-4c-90-81 <网线已连接>
WAN 口状态: NOT Available <网线状态未知>

1. 修改Web管理登录用户名及密码
-----
2. 修改LAN口配置及Web管理端口
-----
3. 修改WAN口配置
-----
4. 显示系统当前状态信息
-----
5. 保存配置 & 恢复出厂
-----
6. 重启或关闭系统
-----
7. 清除IP与MAC地址绑定
-----

请输入 1~7 之间的一个数字(输入q退出): _
```

## 控制台修改 LAN 口 IP

步骤：输入 2-》输入网卡位置-》输入 IP 端口信息，格式为：IP、IP:端口、IP/子网掩码、IP/子网掩码:端口

- 改 IP，输入如 192.168.1.1
- 改 IP+子网掩码，输入如 192.168.1.1/255.255.254.0 或 192.168.1.1/23
- 改 IP+Web 管理端口，输入如 192.168.1.1:81
- 改 IP+子网掩码+Web 管理端口，输入如 192.168.1.1/255.255.254.0:81 或 192.168.1.1/23:81



## 串口登录

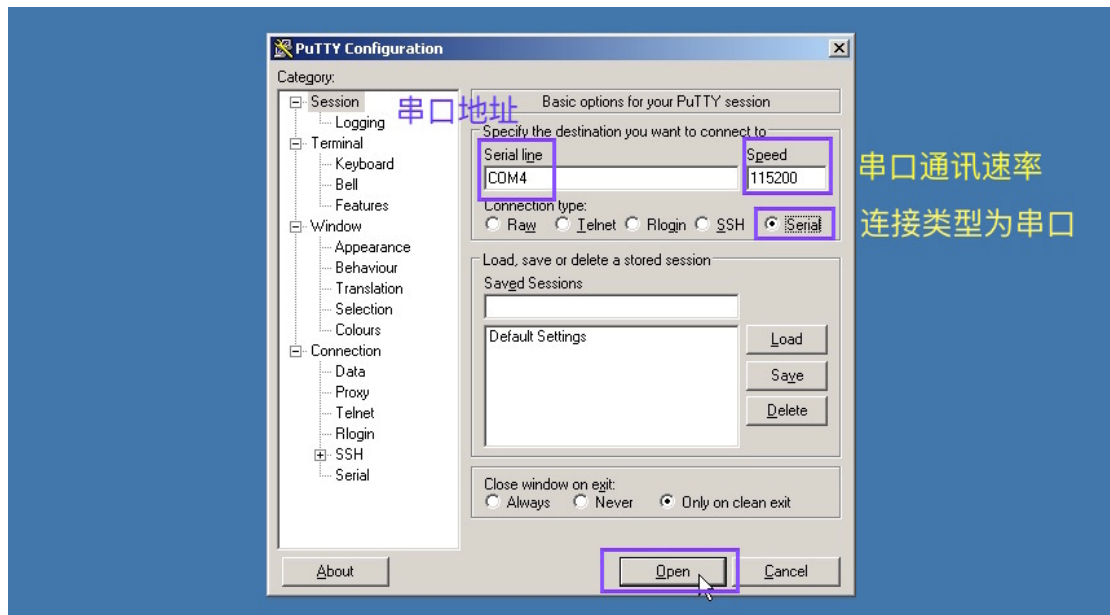
如果您的电脑上有串口, 将串口线直连到该口, 如果没有串口, 可以使用 USB 转串口的数据线

在桌面“计算机”图标上点击鼠标右键, 管理-》设备管理器-》端口, 查看所连接的 COM 口编号, 比如 COM4



打开 putty 工具，连接类型选择 Serial，Serial line 为串口编号，Speed 为数据传输波特率

下载 putty



点击“Open”按钮登录，输入密码，成功登录后如下：



## 登录问题 FAQ

---

### 1. 打开 Web 登录页时提示 “您的浏览器版本太旧...”

解决办法：升级 IE 浏览器到 IE9 或更高版本，或换用其他浏览器（Google Chrome 或 Firefox）。

## 单 WAN 上网——最简单的网络结构（外网单线接入）

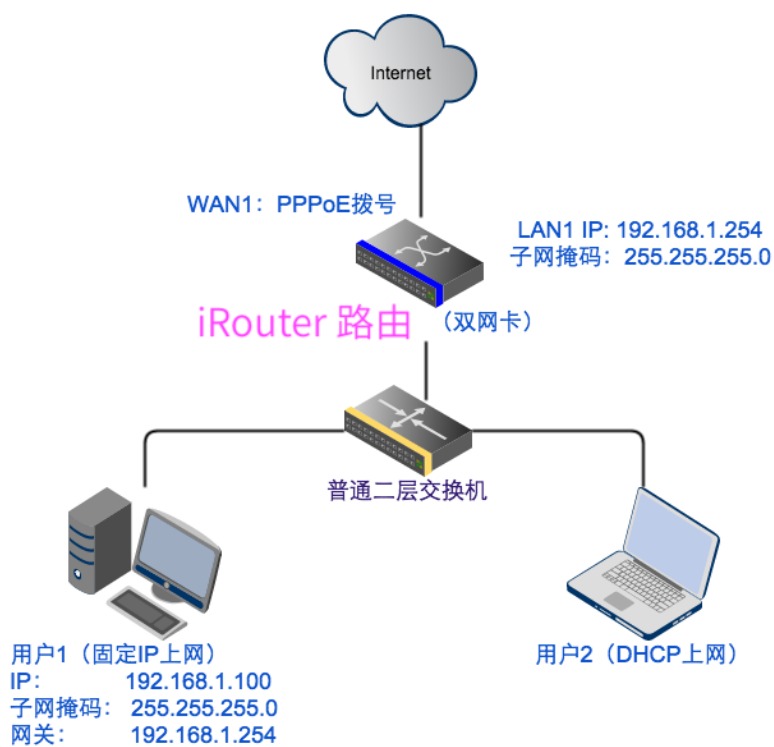
### 外网单线接入（单 WAN）部署

#### 网络拓扑

最常见的一进一出网络结构，路由上双网卡，一个网卡连接 LAN（局域网），一个网卡连接 WAN（Internet）。

网络拓扑图如下：

## 路由双网卡单WAN部署



## 绑定网卡

如果已绑定，可忽略此步骤。

进入“网络” -> “网卡绑定” -> “新增规则”，创建 wan1 接口



接口名格式: wanXX 或 lanXX (XX为数字) 选择一块空闲的网卡绑定给wan1

接口名:

接口类型:

网卡设备位置:   
 eth1 - Realtek Semiconductor RTL8111/8168/8411 PCI Express Gigabit - 空闲 | 已连接  
 lan1 - Realtek Semiconductor RTL8111/8168/8411 PCI Express Gigabit - LAN-1 | 已连接

MAC地址:

备注:

激活:

可以加个说明, 便于区分

网卡绑定

将 LAN、WAN 接口和物理网卡对应起来

接口列表 新增规则 点击接口名进入配置页

ID	接口名	类型	物理网卡 <设备名 - 型号 - MAC - 网线插入状态>	备注	状态	编辑
1	lan1	独立物理网卡	lan1 - Realtek RTL8111/8168/8411 Gigabit - b8-97-5a-6c-e2-65 - <input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input type="button" value="编辑"/>
2	wan1	独立物理网卡	wan1 - Realtek RTL8111/8168/8411 Gigabit - b8-97-5a-6c-b8-b7 - <input checked="" type="checkbox"/>	电信100M	<input checked="" type="checkbox"/>	<input type="button" value="编辑"/>

全选 / 全不选

创建成功后, 点击 wan1 进入 WAN 口配置页面

## 配置 WAN 接口

选择接入方式为 “ADSL/PPPoE 拨号”, 输入账号和密码

网络

WAN 配置 线路检测

物理接口

LAN (局域网)

VLAN (虚拟局域网)

WAN (广域网)

DNS 参数

IP-MAC 绑定

DHCP 服务

4G/5G 上网

PPTP/L2TP VPN 隧道

SSL VPN 隧道

网线已连接, 速度: 100Mb/s (工作模式: 全双工模式)

上行流量统计: 共发送 1.60 GB, 发送包 0.39G, 出错 0, 丢弃 0

下行流量统计: 共接收 2.36 GB, 接收包 0.44G, 出错 0, 丢弃 1.35M

MAC地址 00-76-ca-3a-1f-81

MAC地址克隆

Internet 接入方式 ADSL/PPPoE 拨号

分别输入PPPoE 拨号账号和密码

帐号 17364065676

密码 为空不修改 显示密码

最下方“其他参数”中，一定要勾选“此网关作为默认路由”

发送存活包间隔 默认为 20 秒

存活包检测数量 默认为 3

其他参数

此线路的网关作为默认路由

禁止NAT

启用端口隔离

系统会自动开始拨号，并实时刷新状态，如下：

<wan1> 已连接

wan1 / 17364065676 - 连接状态	
设备名:	ppw0 @ wan1
建立时间:	2020-07-11 09:03:12
已连接:	3天3小时12分8秒 <span>断开</span>
IP地址:	221.232.59.224
网关:	221.232.56.1
DNS 服务器:	202.103.24.68, 202.103.44.150
公网IP:	221.232.59.224
IP地理位置:	湖北省武汉市 电信
PPPoE 服务器 MAC 地址:	e4-72-e2-f6-86-ac

[连接日志](#) ← 若拨号不成功, 点击这里查看错误日志

## 测试 Internet 连接

进入“工具” -》系统体检, 勾选 WAN1, 诊断:

**工具**

- PING 探测
- 局域网扫描
- 实用工具
- 在线抓包
- 文件管理
- 性能测试
- 系统体检**
- S905L机顶盒定制

网络接口  wan1 <wan1/ppw0/221.232.59.224/221.232.56.1 湖北省武汉市 电信>

全选 / 全不选

系统磁盘分区文件系统  /dev/mmcbk0p1 ext4 (8GTF4R)

**诊断**

```
** 测试到达 Internet 网关 221.232.56.1 的延时
ICMP reply from 221.232.56.1: icmp_seq=0 time=1.287 ms
ICMP reply from 221.232.56.1: icmp_seq=1 time=2.874 ms
ICMP reply from 221.232.56.1: icmp_seq=2 time=1.201 ms
小计: 共发送3个包, 收到3个包, 丢包率 0.0%, 平均延时 1.787 ms
测试目标线路 wan1
本地IP: 221.232.59.224, 网关: 221.232.56.1, 最大传输单元 (MTU) : 1492
查询公网出口IP及位置信息... 公网IP 221.232.59.224 [湖北省武汉市 电信]
测试访问网站 www.baidu.com ... 访问站点成功, 耗时 359 ms, 传输数据 280.30 KB, 约 192 个包
测试访问网站 www.163.com ... 访问站点成功, 耗时 71 ms, 传输数据 482.80 KB, 约 331 个包
测试外网下载带宽 ... 获得9个下载链接
从 https://dldir1.qq.com/qqfile/QQforMac/QQ_6.6.7.dmg 下载文件 ... 51.92 MB
下载耗时 7 秒, 传输文件 51.9M, 平均速度 7.42 MB/s, 带宽大小 59.3Mbps
```

## 常见问题

## 1. 能 ping 通外网，但无法上网

如果是 PPPoE 拨号上网，可以尝试更改 PPPoE 拨号连接的 MTU（默认为 1492），改小，如 1480/1460。

# 磁盘管理 —— 存储磁盘管理

## 存储磁盘管理

系统磁盘通常只需 1-2G，如果硬盘上有空闲空间，可以用作其他应用的数据存储，比如 网站服务器、KVM 虚拟化、Docker 容器 等等。

### 普通分区操作

分为如下 3 个步骤：**创建分区-》格式化-》挂载分区到目录**

(2020/08/15 以后版本已简化为一个步骤完成)



The screenshot shows a disk management interface with a sidebar on the left containing menu items: 系统, 常规设置, 登录管理, 报警 & 通知, 计划任务, 磁盘存储 (highlighted), and 防火墙. The main area displays '本地磁盘分区' with tabs for 'RAID阵列' and '逻辑卷(LVM)'. Below this, a header for '磁盘 sda' shows its model, serial number, and capacity (53.7GB). A table lists the partitions:

分区	大小	文件系统	使用率	已用	剩余	挂载目录	动作
sda1	258MB	fat32					挂载 创建PV / 格式化 - 删除
*sda2	8332MB	ext4	1%	98.4M	7.1G	%system%	扩充系统分区

At the bottom, it indicates '未分配空间: 45.1GB' and includes a '创建新分区' button.

可以指定分区大小或使用所有空闲空间：

磁盘 sda

容量大小 53.7GB

磁盘型号 QEMU HARDDISK

序列号 NO\_SN\_FOUND

使用所有剩余空间  是 剩余 45.1GB

用作交换分区  否

[创建](#)

[关闭](#)

格式化分区（默认格式化为 ext4 文件系统）：

磁盘 sda - 型号: QEMU HARDDISK - 序列号: NO\_SN\_FOUND - 容量: 53.7GB

分区	大小	文件系统	使用率	已用	剩余	挂载目录	动作
sda1	258MB					-	创建PV / 格式化 - 删除
*sda2	8332MB	ext4	1%	98.4M	7.1G	%system%	扩充系统分区
sda3	45.1GB	ext4					先格式化，后挂载 <a href="#">挂载</a> 创建PV / 格式化 - 删除

挂载分区到指定目录，目录名可自定义：

磁盘 sda

容量大小 53.7GB

磁盘型号 QEMU HARDDISK

序列号 NO\_SN\_FOUND

挂载目录 /disk/  挂载目录名自定义，字母数字组成

启用 SSD TRIM 优化  否

[挂载](#)

挂载成功后如下：

分区	大小	文件系统	使用率	已用	剩余	挂载目录	动作
sda1	258MB					-	创建PV / 格式化 - 删除
*sda2	8332MB	ext4	1%	98.4M	7.1G	%system%	扩充系统分区
sda3	45.1GB	ext4	0%	47.9M	39.1G	/disk/data	卸载

## LVM 动态磁盘

LVM 是逻辑卷管理 (Logical Volume Manager) 的简称，它是建立在物理存储设备之上的一个抽象层，LVM 将存储虚拟化，允许你生成逻辑存储卷，与直接使用物理存储在管理上相比，提供了更好灵活性。

比起普通的硬盘分区管理方式，LVM 的优点如下：

- 将多块硬盘看作一块大硬盘。
- 使用逻辑卷 (LV)，可以创建跨越众多硬盘空间的分区。
- 可以创建小的逻辑卷 (LV)，在空间不足时再动态调整它的大小。
- 在调整逻辑卷 (LV) 大小时可以不用考虑逻辑卷在硬盘上的位置，不用停止应用或卸载文件系统。
- 可以在线对逻辑卷 (LV) 和卷组 (VG) 进行创建、删除、调整大小等操作。

如果您有多块磁盘，推荐使用 LVM 来管理磁盘。

建立 LVM 的步骤为：创建 PV（物理卷） -》创建 VG（卷组） -》创建 LV-》格式化-》挂载

## 1. 在整个磁盘或某个分区上创建 PV

磁盘 sdb - 型号: QEMU HARDDISK - 序列号: NO_SN_FOUND - 容量: 4295GB							
分区	大小	文件系统	使用率	已用	剩余	挂载目录	动作
未分配空间: 4295GB							<a href="#">创建PV</a> / <a href="#">创建新分区</a>

## 2. 在 PV 上创建 VG

本地磁盘分区    RAID阵列    逻辑卷(LVM)

当前没有活动的逻辑卷组

选择创建过PV的磁盘或分区

请选择PV    /dev/sdb -- 3.91 TiB

VG 卷组名    data

名字自定义，字母数字组成

✓ 创建/扩展VG

### 3. 在 VG 上创建 LV

逻辑卷组 vgdata <span>🔄 激活所有VG</span> <span>🚫 禁用所有VG</span> <span>🗑️ 删除卷组及所有LV</span>	
格式:	lvm2
VG 大小:	<span>3.91 TiB</span>
已分配空间:	0 PE / 0
剩余空间:	1023999 PE / 4095996MB (3.91 TiB) <span>👉 创建新的逻辑卷</span>
PE 总数/大小:	1023999 / 4.00 MiB
使用中的LV:	0
PV 总数: 1	<p>物理卷: <code>/dev/sdb</code> <span>🗑️</span></p> <p>PV 大小: <span>3.91 TiB</span></p> <p>PE 数量: 1023999 (已分配 0, 剩余 1023999)</p>
LV 总数: 0	

LV 大小可自定义，开始不用创建太大，因为后期可以动态扩充：

磁盘	<input type="text" value="逻辑卷 vgdata"/>
容量大小	<input type="text" value="3.91 TiB"/>
逻辑卷名	<input type="text" value="test"/>
分区大小	<input type="text" value="100G"/>
使用所有剩余空间	<input type="checkbox"/> 否 剩余 3.91 TiB
用作交换分区	<input type="checkbox"/> 否
	<span>👉 分区大小根据需要设置，后期可以扩充</span>
	<span>👉 创建</span>



## 4. 格式化 LV

LV 总数: 1

逻辑卷:	/dev/vgdata/test 
LV 大小:	97.66 GiB <a href="#">扩充LV</a>
状态:	正常 <空闲>
文件系统:	<input type="text" value="格式化"/>

## 5. 挂载 LV 到指定目录

磁盘	逻辑卷 /dev/vgdata/test - 容量: 97.66 GiB
容量大小	97.66 GiB
磁盘型号	LVM
序列号	IGLYx7-zHiy-QPmy-DzvN-Sk6h-BI7t-qCf6G6
挂载目录	/disk/ <input type="text" value="test"/>
启用 SSD TRIM 优化	<input type="checkbox"/> 否
<input type="button" value="挂载"/>	

最后挂载状态如下:

LV 总数: 1

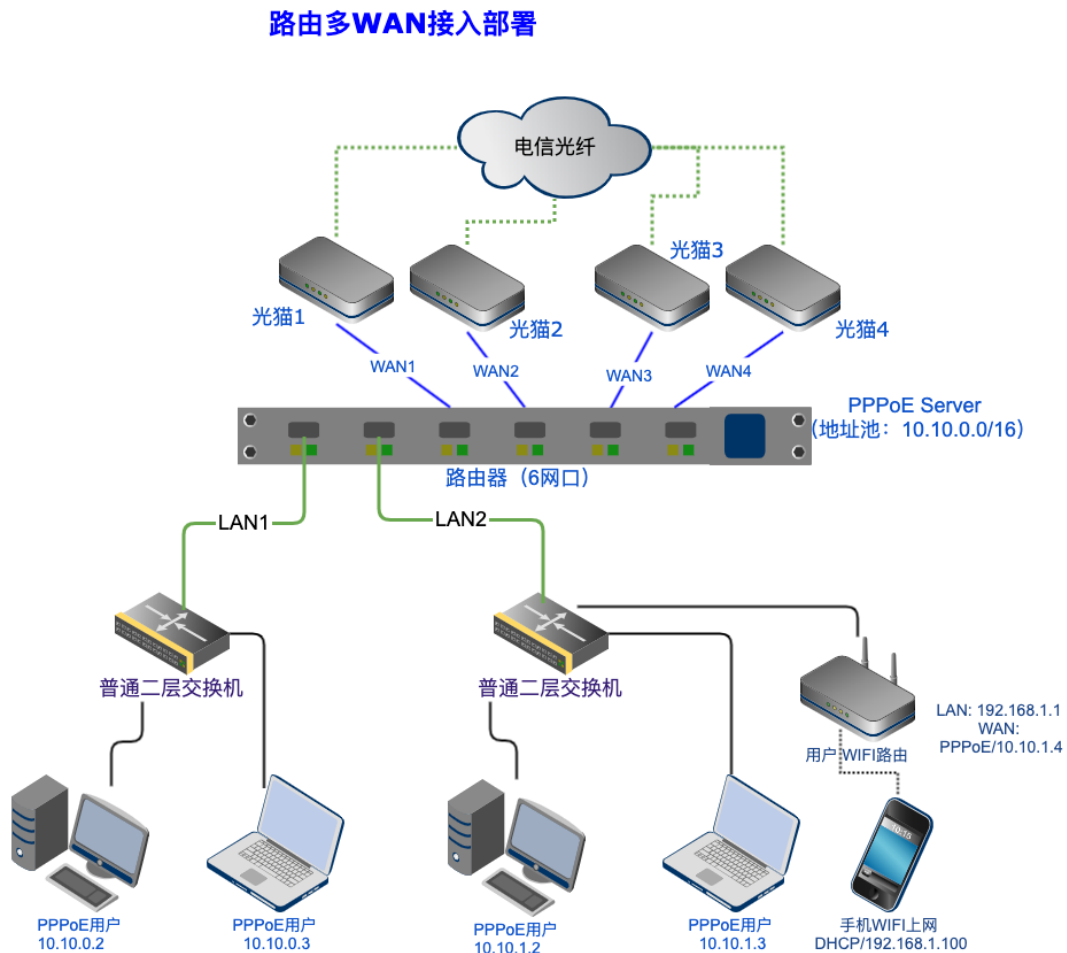
逻辑卷:	/dev/vgdata/test 
LV 大小:	97.66 GiB <a href="#">扩充LV</a>
状态:	正常 <使用中>
文件系统:	ext4
使用详情:	已用 59.6M, 剩余 91.0G
使用率:	0% <div style="width: 0%;"></div>
挂载目录:	<a href="#">/disk/test</a> <a href="#">卸载</a>

# 多 WAN 上网 —— 外网多线接入

## 外网多线接入（多 WAN）部署

路由上有多块网卡，外网多线接入，每条外线接一块网卡。

### 网络拓扑



### 绑定网卡

进入“网络” -》“网卡绑定” -》“新增规则”，创建 wan1~wan4 接口

### 物理接口

将 LAN、WAN 接口和物理网卡对应起来

ID	接口名	类型	物理网卡 <设备名 - 型号 - MAC - 网线插入状态>	备注	状态	编辑	选择
1	lan1	以太网	网卡1-1口 - lan1 - -- mt7530 switch port -- - 00-76-ca-3a-1f-80 - <input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>		<input type="checkbox"/>
2	wan1	以太网	网卡1-2口 - wan1 - -- mt7530 switch port -- - 00-76-ca-3a-1f-81 - <input checked="" type="checkbox"/>	电信光纤01	<input checked="" type="checkbox"/>		<input type="checkbox"/>
3	wan2	以太网	网卡1-3口 - wan2 - -- mt7530 switch port -- - 00-76-ca-3a-1f-82 - <input checked="" type="checkbox"/>	电信光纤02	<input checked="" type="checkbox"/>		<input type="checkbox"/>
4	wan3	以太网	网卡1-4口 - wan3 - -- mt7530 switch port -- - 00-76-ca-3a-1f-83 - <input checked="" type="checkbox"/>	电信光纤03	<input checked="" type="checkbox"/>		<input type="checkbox"/>
5	wan4	以太网	网卡1-5口 - wan4 - -- mt7530 switch port -- - 00-76-ca-3a-1f-84 - <input checked="" type="checkbox"/>	电信光纤04	<input checked="" type="checkbox"/>		<input type="checkbox"/>

新增规则 全选 / 全不选

## 配置每个 WAN

依次接入每个 WAN 口对应的外线，并配置好每个 WAN 口，然后开启线路检测（用于掉线自动切换）

网络

物理接口

LAN (局域网)

VLAN (虚拟局域网)

WAN (广域网)

DNS 参数

IP-MAC 绑定

DHCP 服务

4G/5G 上网

PPTP/L2TP VPN 隧道

SSL VPN 隧道

VTUN 隧道

请选择网卡设备: WAN-4 - wan4 - 以太网

依次配置每个WAN口

WAN 配置 线路检测

服务运行状态 运行中 <PID: 5424> 查看日志

线路 wan4

检测方法 PING + TCP/SYN (默认)

PING 目标 空表示PING网关

PING 最大延时 ms

本地运营商站点或门户网站

SYN 目标 www.baidu.com 选择

SYN 端口 80

注：光猫工作模式分为 2 种

- 桥接模式（路由器拨号）
- 路由模式（光猫拨号，路由器充当二级路由，路由器的 WAN 通过 DHCP 上网）

### 光猫为路由模式时：

一般光猫默认的 LAN 口 IP 是 192.168.1.1，路由器接光猫的 LAN 口通过 DHCP 获得 IP 上网。

如果有多个光猫，请将 WAN 口改为固定 IP 模式，并且每个 WAN 的 IP 不要重复。

同时，线路检测的 PING 目标应设为外网域名或 IP，或者使用 TCP/SYNC 探测模式，否则将无法检测到光猫外网断线。

## 配置多线负载策略

进入“路由” -> “多线负载策略”，启用多线



The screenshot shows the 'Multi-line Load Strategy' configuration page. At the top, there is a checkbox labeled '启用多线负载及策略' (Enable Multi-line Load Strategy) which is checked. Below this, there are tabs for '多线配置' (Multi-line Configuration), '线路分组' (Line Grouping), '自定义策略' (Custom Strategy), and '路由表' (Routing Table). The main content is a table with the following data:

ID	线路	连接状态 (网卡/设备名/IP)	线路类型	负载权重	禁止自动负载
1	WAN-1	wan1/ppw0/221.232.59.224 <湖北省武汉市 电信>	默认线路	1	<input type="checkbox"/>
2	WAN-2	wan2/ppw3/221.232.56.9 <湖北省武汉市青山区 /洪山区>	默认线路	1	<input type="checkbox"/>
3	WAN-3	wan3/ppw2/221.232.59.100 <湖北省武汉市 电信>	默认线路	1	<input type="checkbox"/>
4	WAN-4	wan4/ppw1/221.232.56.62 <湖北省武汉市青山区 /洪山区>	默认线路	1	<input type="checkbox"/>

负载权重根据带宽的大小，计算其比率，比如这里 wan1 和 wan2 分别是 100M 和 50M，负载权重可以分别设为 2 和 1。

如果想让某条线单独设置策略，在其后面勾选“禁止自动负载”。

## 查看线路负载状态

进入“状态” -> “接口” -> “路由表”，可以查看多线的路由信息：

**接口**

这里显示了所有的活动接口信息、接口流量和包计数、路由表条目、ARP 缓存记录。

接口状态    接口负载    连接    路由表

默认路由:

221.232.56.1	通过	wan1/ppw0 (221.232.59.224)	负载权重 25.00%	累计流量 454.79 GB / 150.34 GB
221.232.56.1	通过	wan2/ppw3 (221.232.56.9)	负载权重 25.00%	累计流量 3.66 GB / 3.82 GB
221.232.56.1	通过	wan3/ppw2 (221.232.59.100)	负载权重 25.00%	累计流量 367.33 MB / 2.67 GB
221.232.56.1	通过	wan4/ppw1 (221.232.56.62)	负载权重 25.00%	累计流量 4.57 GB / 3.67 GB

4 线路

## 自定义策略

通过自定义策略，可以设置内网指定 IP 访问外网时，走指定的线路。

举例：内网指定的 IP 访问外网 443 端口时，走 WAN1 线路

名称  自定义，可以是中文

优先级 0

协议 TCP

线路 wan1 <wan1/ppw0/221.232.59.224 湖北省武汉市电 >

源IP   
  
  
  
 内网IP

目的IP  = IP 类型 =

源端口

目的端口  访问的外网端口

# 交换机—WAN 多拨上网——外网线路接入到 VLAN

交换机

## VLAN 交换机扩展—WAN 多拨

路由上有多块网卡，外网多线接入，每个运营商的所有线路通过 VLAN 交换机与路由的一个网卡连接。

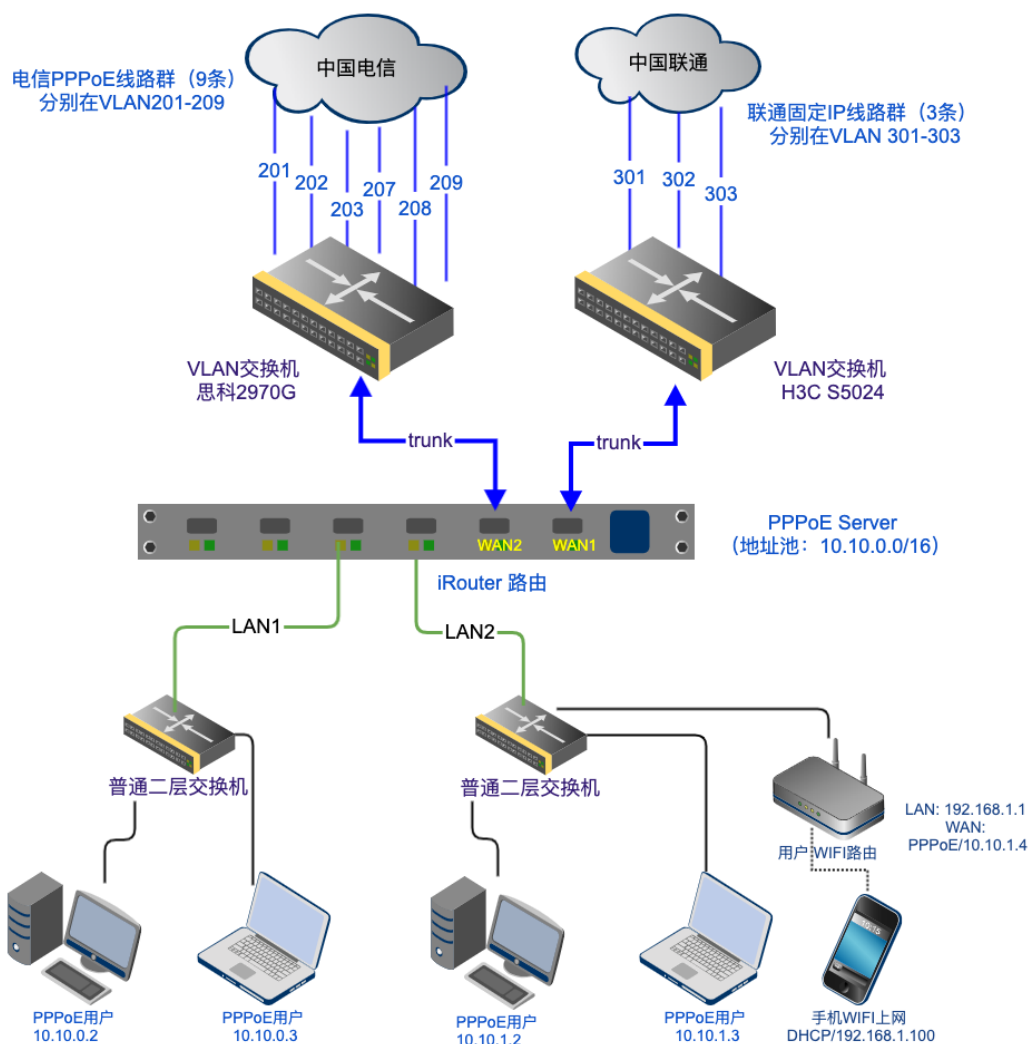
这里的 VLAN 扩展方式为：**基于端口的 VLAN**，在一个网卡上创建 VLAN 子接口，与交换机上的 VLAN 互通。

—WAN 多拨的另外一种方式，请参考：[网卡 VLAN 扩展—WAN 多拨](#)

网络拓扑

---

## 外网VLAN交换机扩展 (—WAN多拨) 部署



这里以电信、联通 2 个运营商为例，每个运营商都有多条线路，而路由上网卡数量有限，只能分 2 个网卡给 WAN 使用。

这时候，通过 VLAN 交换机来扩展 WAN 是非常好的解决方案。

## 网卡绑定及交换机配置



## 1. 绑定 wan 口

进入“网络”->“网卡绑定”->“新增规则”，创建 wan1~wan2 接口

网卡绑定				
将 LAN、WAN 接口和物理网卡对应起来				
接口列表		新增规则		
ID	接口名	类型	物理网卡 <设备名 - 型号 - 网线插入状态>	备注
1	lan1	独立物理网卡	网卡1-1口 - lan1 - Broadcom NetXtreme II BCM5709 Gigabit - 14-fe-b5-d7-54-72 - <input checked="" type="checkbox"/>	
2	lan2	独立物理网卡	网卡2-1口 - lan2 - Intel I350 Gigabit - 2c-53-4a-01-65-de - <input checked="" type="checkbox"/>	pppoe server vlan
3	lan3	独立物理网卡	网卡2-2口 - lan3 - Intel I350 Gigabit - 2c-53-4a-01-65-df - <input checked="" type="checkbox"/>	pppoe server lan
4	lan4	独立物理网卡	网卡1-4口 - lan4 - Broadcom NetXtreme II BCM5709 Gigabit - 14-fe-b5-d7-54-78 - <input checked="" type="checkbox"/>	radius
5	lan5	独立物理网卡	网卡1-2口 - lan5 - Broadcom NetXtreme II BCM5709 Gigabit - 14-fe-b5-d7-54-74 - <input checked="" type="checkbox"/>	iptv
6	wan1	独立物理网卡	网卡2-3口 - wan1 - Intel I350 Gigabit - 2c-53-4a-01-65-e0 - <input checked="" type="checkbox"/>	联通固定IP专线
7	wan2	独立物理网卡	网卡2-4口 - wan2 - Intel I350 Gigabit - 2c-53-4a-01-65-e1 - <input checked="" type="checkbox"/>	电信PPPoE线路

## 2. 配置 VLAN 交换机

实际上只用一台也是可以的，交换机上分别创建 VLAN（201-209，301-303），并将连接路由网卡的那个交换机端口设为 trunk 模式（允许和所有 VLAN 互访）

### 配置 WAN1（固定 IP/VLAN）

配置 WAN1（联通专线固定 IP），选择接入方式为“固定/静态 IP(VLAN 模式)”

WAN-1 配置    扩展配置    WAN-2

网线已连接, 速度: 1000Mb/s (工作模式: 全双工模式)

上行流量统计: 共发送 8.70 TB, 发送包 39.64G, 出错 0, 丢弃 0

下行流量统计: 共接收 54.96 TB, 接收包 54.57G, 出错 0, 丢弃 0.42M

网络接口: WAN-1 - wan1 - 独立物理网卡

MAC地址: 2c-53-4a-01-65-e0

MAC地址克隆:

Internet 接入方式: 固定/静态IP (VLAN 模式)

显示高级参数 >

保存设置

联通专线为固定IP

进入 WAN1 的“扩展配置”，点击“新增规则”，配置每个 VLAN 中的线路参数

如果实现同一个 VLAN 多账号拨号，请将 VLAN 标识设为如：

<VLAN\_ID>.<自定义字符，开头为字母>，如 4015.ctc001、

4015.ctc002。

名称: 301

MAC地址: 38-c3-9d-84-2a-60 (随机生成)

IP地址: 61.156.x.x

子网掩码: <此网段可容纳 1022 台主机> /22 = 255.255.252.0

网关: 61.156.x.x

禁止NAT: 否

检测方法: PING

PING 目标:

配置完成后如下:

WAN-1 配置 **扩展配置** WAN-2

共 3 条记录 / 1 页, 每页显示 默认 条 请输入关键字 搜索 Q 清除 x 新增规则

ID	名称	IP/掩码/网关	MAC地址	备注	状态
1	301	61.156.x.x/255.255.252.0/61.156.x.x	38-c3-9d-84-2a-60		✓
2	302	61.156.x.x/255.255.252.0/61.156.x.x	d0-2b-80-79-0f-69		✓
3	303	218.59.1.x/255.255.255.252/218.59.x.x	fc-16-de-ae-0d-11		✓

名称为VLAN号, 不能重复

## 配置 WAN2 (PPPoE/VLAN)

配置 WAN2 (电信 PPPoE 线路), 选择接入方式为 “ADSL/PPPoE 拨号(VLAN 模式)”



进入 WAN2 的“扩展配置”，点击“新增规则”，配置每个 VLAN 中的线路参数



配置完成后如下:

WAN-2 配置 **扩展配置** WAN-1

共 9 条记录 / 1 页, 每页显示 默认 条 请输入关键字  搜索 Q 清除 x 新增规则 探测 PPPoE 服务

生成批量 PPPoE 账号

VLAN 号, 不能重复

ID	名称	PPPoE账号	MAC地址	备注	状态
1	201	054600001000	f2-45-3e-8d-44-0c		✓
2	202	054600002000	f2-45-3e-8d-44-01		✓
3	203	t54600003000	f2-45-3e-8d-44-1c		✓
4	204	t54600004000	f2-45-3e-8d-44-11		✓
5	205	t54600005000	f2-45-3e-8d-44-12		✓
6	206	t54600006000	f2-45-3e-8d-44-13		✓
7	207	t54600007000	f2-45-3e-8d-44-14		✓
8	208	t54600008000	f2-45-3e-8d-44-15		✓
9	209	t54600009000	f2-45-3e-8d-44-16		✓

## 配置多线策略

进入“路由” -> “多线负载策略”，激活线路，并启用多线

具体方法请参考：[配置多线负载策略](#)

## 单网卡一 WAN 多拨上网 —— 网卡 VLAN 扩展多

### PPPoE 拨号

### 网卡 VLAN 扩展一 WAN 多拨

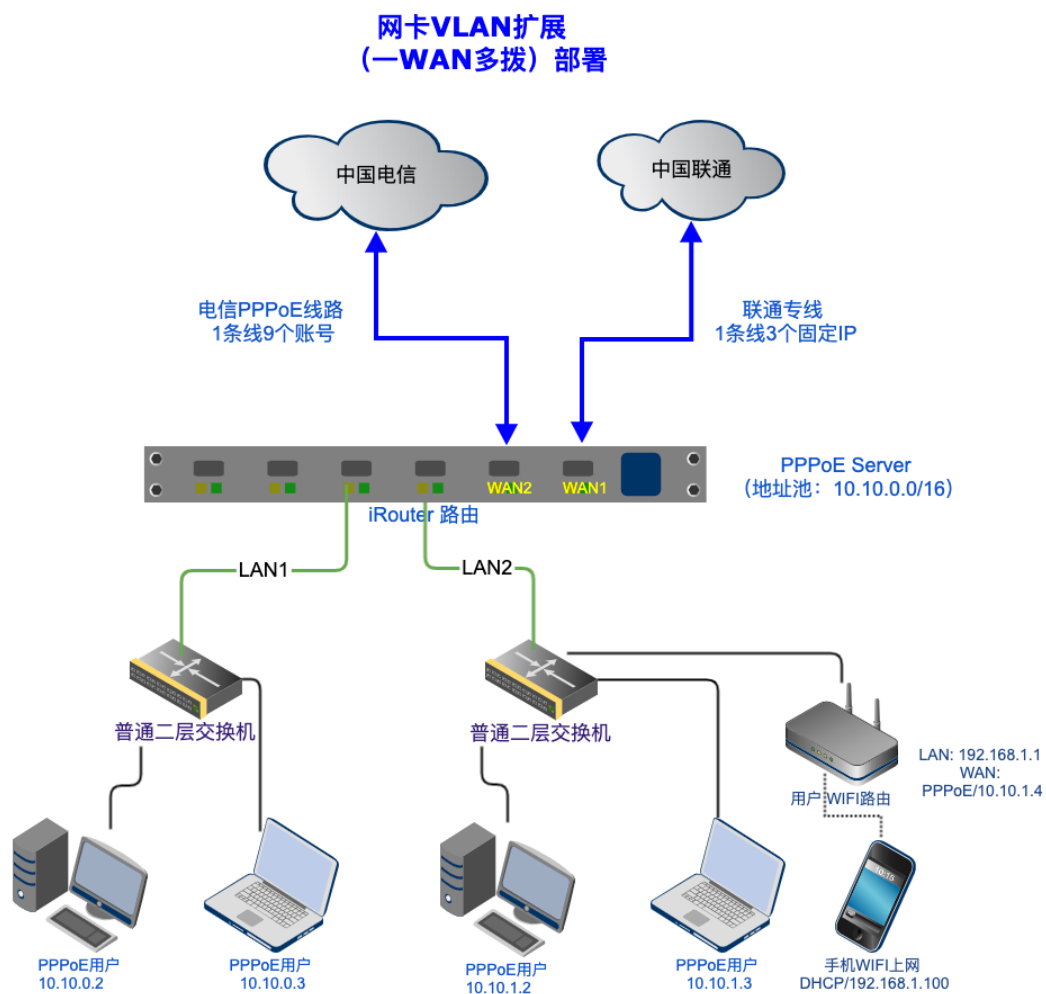
路由上有多块网卡，外网多个运营商接入，每个运营商一条物理线路进来，每条线绑定有多个 PPPoE 账号或多个固定 IP。

每个运营商的物理线路直连路由的一块物理网卡。

这里的 VLAN 扩展方式为：**基于 MAC 的 VLAN**，在一个网卡上虚拟多个 MAC 地址，来扩展网络接口。

— WAN 多拨的另外一种方式，请参考：[VLAN 交换机扩展—WAN 多拨](#)

## 网络拓扑



这里以电信 PPPoE、联通固定 IP 专线为例，电信和联通各有一条物理线路进来，分别接路由的 WAN1 和 WAN2 口。

这时候，需要通过网卡本身的 VLAN 扩展来实现多个 PPPoE 账号同时拨号，以及绑定多个固定 IP。

## 网卡绑定

进入“网络” -》“网卡绑定” -》“新增规则”，创建 wan1~wan2 接口

ID	接口名	类型	物理网卡 <设备名 - 型号 - MAC - 网线插入状态>	备注	状态
1	lan1	独立物理网卡	lan1 - Red Hat, Virtio network device - 94-f9-3d-76-22-7d - <input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>
2	wan1	独立物理网卡	wan1 - Red Hat, Virtio network device - 4a-8b-17-44-dd-e0 - <input checked="" type="checkbox"/>	联通固定IP专线	<input checked="" type="checkbox"/>
3	wan2	独立物理网卡	wan2 - Intel I350 Gigabit - 2c-53-4a-02-05-0f - <input checked="" type="checkbox"/>	电信PPPoE线路	<input checked="" type="checkbox"/>

## 配置 WAN1 (固定 IP/VLAN)

配置 WAN1 (联通专线固定 IP)，选择接入方式为“固定/静态 IP(VLAN 模式)”

WAN-1 配置    扩展配置    WAN-2

网线已连接, 速度: 未知 (工作模式: 未知)

上行流量统计: 共发送 0.00 KB, 发送包 0, 出错 0, 丢弃 0

下行流量统计: 共接收 0.00 KB, 接收包 0, 出错 0, 丢弃 0

网络接口: WAN-1 - wan1 - 独立物理网卡

MAC地址: 4a-8b-17-44-dd-e0

MAC地址克隆:

Internet 接入方式: 固定/静态IP (VLAN 模式)

显示高级参数 >

WAN1 联通固定IP专线

进入 WAN1 的“扩展配置”，点击“新增规则”，每个固定 IP 一条规则

字母和数字组成，不能为全数字

VLAN 标识: cnc101

MAC地址: e8-75-cd-04-09-86    随机生成

IP地址: 219.158. [redacted]

子网掩码: <此网段可容纳 1022 台主机> 219.158.100.1~219.158.103.254  
/22 = 255.255.252.0

网关: 219.158. [redacted]

禁止NAT: 否

检测方法: PING

PING 目标: 为空表示PING网关

注意这里的“VLAN 标识”不能为纯数字，纯数字用于有交换机扩展 VLAN 的场景。



配置完成后如下：

WAN-1 配置    扩展配置    WAN-2

共 3 条记录/ 1 页, 每页显示 默认 条    请输入关键字    搜索 Q    清除 x    新增规则

ID	名称	IP/掩码/网关	MAC地址	备注	状态	线路检测状态	编辑
1	cnc101	219.158.120.0/255.255.252.0/219.158.120.1	e8-75-cd-04-09-86		✓	正常	
2	cnc102	219.158.120.0/255.255.252.0/219.158.120.1	2e-b9-cb-a8-eb-33		✓	正常	
3	cnc103	219.158.120.0/255.255.252.0/219.158.120.1	1c-ac-2a-12-22-4e		✓	正常	

## 配置 WAN2 (PPPoE/VLAN)

配置 WAN2 (电信 PPPoE 线路) , 选择接入方式为 “ADSL/PPPoE 拨号(VLAN 模式)”

WAN-2 配置    扩展配置    WAN-1

网线已连接, 速度: 1000Mb/s (工作模式: 全双工模式)

上行流量统计: 共发送 966.55 KB, 发送包 9.23K, 出错 0, 丢弃 0

下行流量统计: 共接收 2.98 MB, 接收包 12.18K, 出错 0, 丢弃 0

网络接口: WAN-2 - wan2 - 独立物理网卡

MAC地址: 2c-53-4a-02-05-0f

MAC地址克隆:

Internet 接入方式: ADSL/PPPoE 拨号 (VLAN 模式)

显示高级参数 >

WAN2 电信PPPoE线路

进入 WAN2 的“扩展配置”，点击“新增规则”，每个 PPPoE 账号一条规则

不能为纯数字

随机生成

宽带账号及密码

VLAN 标识: ctc101

MAC地址: 3c-96-34-9c-07-1f

帐号名: a712986231

密码: .....

最大传输单元(MTU): 默认为 1492

最大接收单元(MRU): 默认为 1492

禁止NAT: 否

检测方法: PING

配置完成后如下:

WAN-2 配置 扩展配置 WAN-1

共 9 条记录 / 1 页, 每页显示 默认 条

请输入关键字 搜索 Q 清除 x 新增规则 探测PPPoE服务

生成批量PPPoE账号

名称不能为纯数字

ID	名称	PPPoE账号	MAC地址	备注	状态	线路检测状态	编辑
1	ctc101	a712986231	3c-96-34-9c-07-1f		✓	正常	编辑
2	ctc102	a712986232	3c-96-14-9c-07-2f		✓	正常	编辑
3	ctc103	a712986233	3c-96-24-9c-07-3f		✓	正常	编辑
4	ctc104	a712986234	3c-96-34-9c-07-4f		✓	正常	编辑
5	ctc105	a712986235	3c-96-14-9c-07-5f		✓	正常	编辑
6	ctc106	a712986236	3c-96-24-9c-07-6f		✓	正常	编辑
7	ctc107	a712986237	3c-96-34-9c-07-7f		✓	正常	编辑
8	ctc108	a712986238	3c-96-14-9c-07-8f		✓	正常	编辑
9	ctc109	a712986239	3c-96-24-9c-07-9f		✓	正常	编辑

查看所有拨号连接的状态：

共 9 个 PPPoE 连接 (0 连接中, 9 已连接)    停止所有拨号    启动所有拨号

<wan2.ctc101> 已连接

wan2.ctc101 / a712986231 - 连接状态

设备名:	ppw2 @ wan2.ctc101
上线时间:	2016-03-25 17:45:55
已连接:	12分28秒    断开
IP地址:	100.10.0.32
网关:	100.10.0.1
DNS 服务器:	100.10.0.1, 223.5.5.5
PPPoE 服务器 MAC 地址	02-8b-07-41-a2-f3

拨号日志    ← 如果拨不上号，这里看日志

## 配置多线策略

进入“路由” -》“多线负载策略”，激活线路，并启用多线

具体方法请参考：[配置多线负载策略](#)

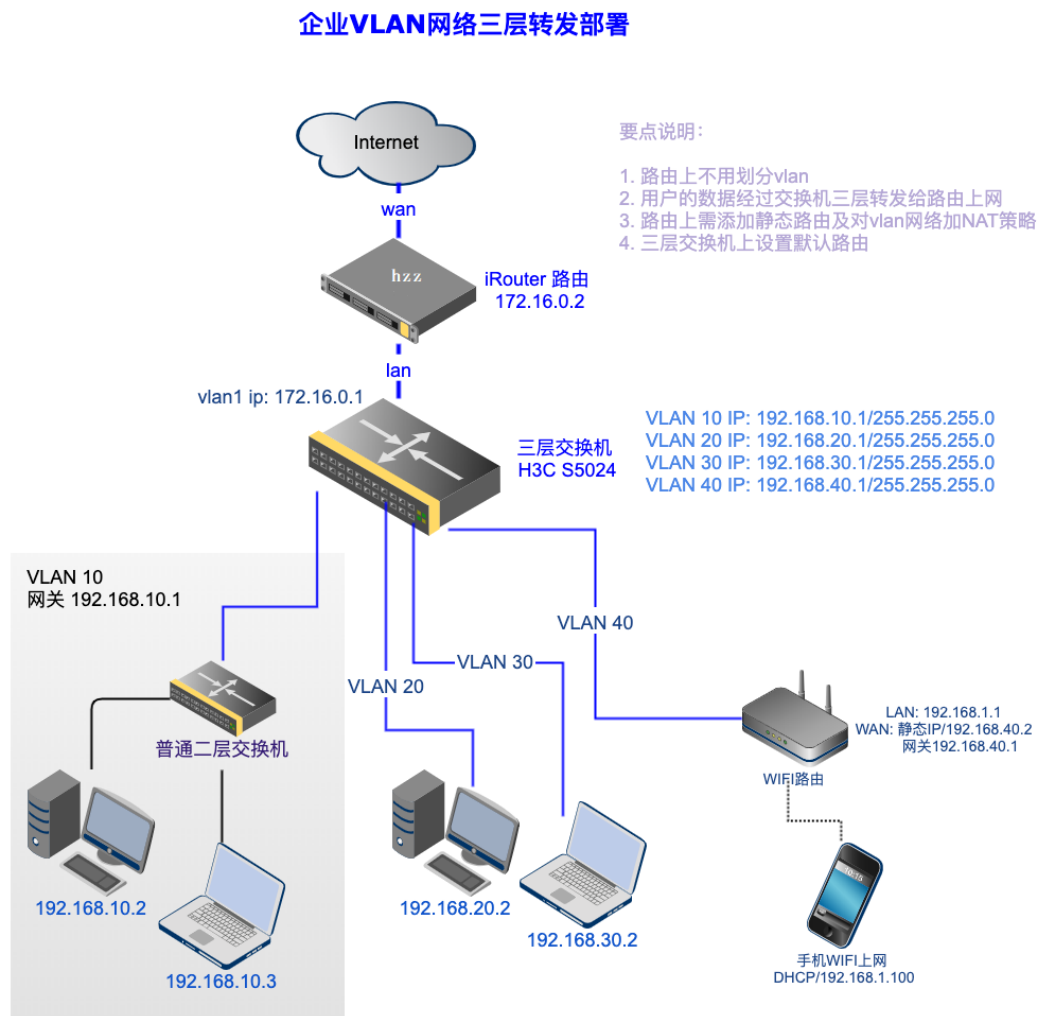
## 企业 VLAN 网络三层转发

三层交换机上划分有多个 VLAN，路由上不划分 VLAN，接交换机的普通端口（VLAN1）。

另外参考：

- [企业网络 VLAN 穿透部署](#)
- [QinQ 双层 VLAN 透传](#)

## 网络拓扑



## 路由上的配置

## 1. 对三层下的 VLAN 添加 NAT 规则

IP地址 172.16.0.2

子网掩码 <此网段可容纳 254 台主机> 192.168.1.1~192.168.1.254  
/24 = 255.255.255.0 (默认)

网关

此网关作为默认路由  否

扩展IP配置 >

隐藏高级参数 <

三层交换机VLAN网络

- 192.168.10.0 / 255.255.255.0
- 192.168.20.0 / 255.255.255.0
- 192.168.30.0 / 255.255.255.0
- 192.168.40.0 / 255.255.255.0

IP地址 192.168.10.0

子网掩码 255.255.255.0

新增 + 删除 x

三层交换机所有VLAN的网络地址加入这里

默认只有和 LAN 同网段的 IP 才能上网，加入后三层下的客户机才能正常上网。

## 2. 添加静态路由，让 VLAN 下的客户机和路由能互通

进入“路由/NAT” -》“静态路由”

启用“静态路由”，依次添加 4 条规则（每个 VLAN 一条），如下：

目标网络 192.168.10.0/24

自动探测网关  否

网关 172.16.0.1

跳数 1

线路 LAN-1 <lan1/lan1/172.16.0.2>

备注 VLAN10

激活  是

保存设置

最后的规则如下：

静态路由  开启

规则列表 [新增规则](#) [静态路由状态](#)

共 4 条记录 / 1 页, 每页显示  条

ID	目的网络	出口网关	线路	跳数	备注	状态
1	192.168.10.0/255.255.255.0	172.16.0.1	lan1	1	VLAN10	✓
2	192.168.20.0/255.255.255.0	172.16.0.1	lan1	1	VLAN20	✓
3	192.168.30.0/255.255.255.0	172.16.0.1	lan1	1	VLAN30	✓
4	192.168.40.0/255.255.255.0	172.16.0.1	lan1	1	VLAN40	✓

点击“静态路由状态”，确认静态路由正常

LAN1/lan1 (当前共有 4 条静态路由)

目的网络	网关	出口设备	跳数
192.168.10.0/24	172.16.0.1	lan1	1
192.168.20.0/24	172.16.0.1	lan1	1
192.168.30.0/24	172.16.0.1	lan1	1
192.168.40.0/24	172.16.0.1	lan1	1

注：如果 192.168.X.X 网段没有其他用途，可以只添加一条规则（目的网络 192.168.0.0/16）

## 三层交换机上的配置

这里以 H3C S5024 为例

```
vlan 10 20 30 40
## 默认 VLAN1 IP 地址
interface Vlanif1
 ip address 172.16.0.1 255.255.255.0
## VLAN10 IP 地址
interface Vlanif10
 ip address 192.168.10.1 255.255.255.0
## VLAN20 IP 地址
interface Vlanif20
 ip address 192.168.30.1 255.255.255.0
## VLAN30 IP 地址
interface Vlanif30
 ip address 192.168.30.1 255.255.255.0
## VLAN40 IP 地址
interface Vlanif40
 ip address 192.168.40.1 255.255.255.0
## 端口 1-5 在 VLAN-10 中
#-----
```

```
interface GigabitEthernet0/0/1
  port link-type access
  port default vlan 10
#
... 省略 ...
#
interface GigabitEthernet0/0/5
  port link-type access
  port default vlan 10
#-----
## 端口 6-10 在 VLAN-20 中
#-----
interface GigabitEthernet0/0/6
  port link-type access
  port default vlan 20
#
... 省略 ...
#
interface GigabitEthernet0/0/10
  port link-type access
  port default vlan 20
#-----
## 端口 11-15 在 VLAN-30 中
#-----
interface GigabitEthernet0/0/11
  port link-type access
  port default vlan 30
#
... 省略 ...
#
interface GigabitEthernet0/0/15
  port link-type access
  port default vlan 30
#-----
## 端口 16-20 在 VLAN-40 中
#-----
interface GigabitEthernet0/0/16
  port link-type access
  port default vlan 40
#
... 省略 ...
#
interface GigabitEthernet0/0/20
  port link-type access
```



```
port default vlan 40
#-----
## 其他端口在默认 VLAN1 中
#-----
#
interface GigabitEthernet0/0/21
... 省略 ...
#
interface GigabitEthernet0/0/24
#
#-----
## 交换机的默认路由 (设为路由的 LAN1 口的 IP)
ip route-static 0.0.0.0 0.0.0.0 172.16.0.2
```

注：路由接在 21~24 中的任一默认 VLAN1 端口

## 网络诊断及测试

---

### 1. 内网互通测试

使用任——台电脑 (IP 设为和路由 LAN 口相同网段 172.16.0.X)

接入三层交换机的任一默认 VLAN1 端口 (21-24 口) , 进入路由-》

“工具” -》 “PING 测试” , 依次

- PING 交换机的 VLAN1 的 IP 地址, 如不通, 检查交换机的 vlan1 接口 ip 设置
- PING 交换机的其他各个 VLAN(10~40)的 IP 地址, 如不通, 检查路由上的静态路由是否正常, 或交换机的 vlan 接口的 ip 设置

- PING 交换机下某一 VLAN 下的客户机的 IP，比如 VLAN10 下的 192.168.10.2，如果不通，检查交换机上的默认路由是否设置正确

## 2. 访问外网测试

在 VLAN 下的客户机电脑上（比如 VLAN10 中的 192.168.10.2），访问外网，如果不通，检查

- 其网关是否设为三层交换机对应 VLAN 的接口 IP（192.168.10.1）
- 路由上是否针对 VLAN 网络添加了 NAT 策略

## 三层转发方案的优缺点

---

优点：内网不同 VLAN 之间的数据直接通过交换机转发，对路由压力小。

缺点：

- 不能使用路由上的 DHCP 为 VLAN 下的客户机分配 IP
- VLAN 下的客户机无法通过 PPPoE 拨号穿透三层交换机到路由
- 路由上无法获得 VLAN 下客户机的 MAC 地址

另外参考：[企业网络 VLAN 穿透部署](#)

# 锐捷三层交换机配置

```
Ruijie>en
Ruijie#config terminal
Ruijie(config)#interface TenGigabitEthernet 0/31
Ruijie(config-if-TenGigabitEthernet 0/31)#switchport mode trunk
Ruijie(config-if-TenGigabitEthernet 0/31)#switchport trunk allowed vlan all
```

## H3C S5130 配置 WEB 登陆

### 1. 建立用户名密码

```
local-user admin class manage
password simple admin123
service-type telnet http https
authorization-attribute user-role level-15
authorization-attribute user-role network-admin
quit
```

### 2. 启用服务

```
[H3C]telnet server enable
[H3C]ip http enable
[H3C]ip https enable
```

### 3. 建立接口地址:

```
[H3C]interface Vlan-interface 1
ip address 192.168.0.237 255.255.255.0
```

### 4. 配置虚接口:

```
[H3C]line vty 0 63
authentication-mode scheme
```

```
quit  
[H3C]quit  
<H3C>save
```

这几步配置完成，就可以通过 telnet、web 方式登录了。

## 企业网络 VLAN 穿透/透传部署

三层交换机上划分有多个 VLAN（也可以使用二层 VLAN 交换机），路由上创建对应的 VLAN，路由 LAN 口接交换机的 trunk 口。

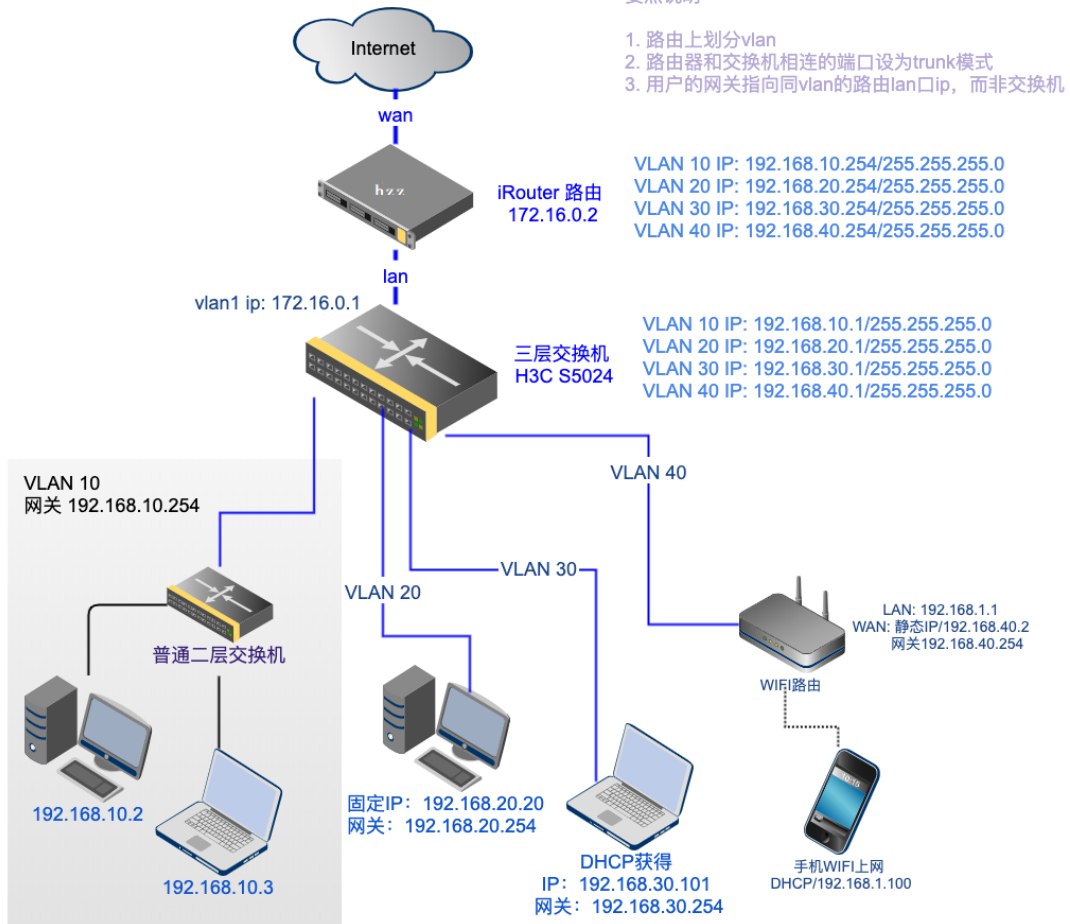
另外参考：

- [企业 VLAN 网络三层转发](#)
- [QinQ 双层 VLAN 透传](#)

## 网络拓扑

---

## 企业网络VLAN透传部署



## 路由上的配置

### 1. 在路由上创建和三层交换机对应的 VLAN

进入“网络” -> “虚拟局域网 (VLAN)” -> “新增 VLAN”

名称

线路

**VLAN ID**  **VLAN 号，和交换机上的VLAN对应**

IP地址  **路由的LAN口在这个VLAN的IP**

MAC地址  **随机生成**

子网掩码 **<此网段可容纳 254 台主机> 192.168.10.1~192.168.10.254**

备注

激活

**保存设置** **关闭**

全部添加后，然后开启“VLAN (虚拟局域网) 功能”，如下：

**VLAN (虚拟局域网)**

VLAN列表 **新增VLAN** VLAN状态

共 4 条记录 / 1 页, 每页显示  条  **搜索** **清除** **快速添加VLAN**

ID	名称	线路	VLAN	IP地址	子网掩码	备注
1	vlan10	lan1	10	192.168.10.254	255.255.255.0	
2	vlan20	lan1	20	192.168.20.254	255.255.255.0	
3	vlan30	lan1	30	192.168.30.254	255.255.255.0	
4	vlan40	lan1	40	192.168.40.254	255.255.255.0	

最后，可以点击“VLAN 状态”查看创建的VLAN的状态，确认

## VLAN 创建成功

VLAN	MAC 地址	IP 地址	子网掩码
10	ba-53-8a-79-38-20	192.168.10.254	255.255.255.0
20	ba-53-8a-79-38-20	192.168.20.254	255.255.255.0
30	ba-53-8a-79-38-30	192.168.30.254	255.255.255.0
40	ba-53-8a-79-38-40	192.168.40.254	255.255.255.0

## 2. 配置 DHCP，为每个 VLAN 分配 IP

如果 VLAN 下面的客户机是固定 IP 或 PPPoE 拨号上网，此步可忽略。

进入“网络” -》“DHCP 服务” -》“IP 地址池” -》“新建 IP 地址池”，

添加 4 条地址池规则（或点击“一键生成默认地址池”快速添加），最后的规则如下：

DHCP 服务  开启

参数设置 IP地址池 固定IP分配 当前分配信息

点击这里可以快速添加地址池

共 5 条记录 / 1 页, 每页显示 默认 条 请输入关键字 搜索 清除 新建IP地址池 一键生成默认地址池

ID	分配的IP地址段	子网掩码	网关	备注	状态	编辑	选择
1	172.16.0.100-172.16.0.200	255.255.255.0	172.16.0.2		✓		<input type="checkbox"/>
2	192.168.10.100-192.168.10.200	255.255.255.0	192.168.10.254		✓		<input type="checkbox"/>
3	192.168.20.100-192.168.20.200	255.255.255.0	192.168.20.254		✓		<input type="checkbox"/>
4	192.168.30.100-192.168.30.200	255.255.255.0	192.168.30.254		✓		<input type="checkbox"/>
5	192.168.40.100-192.168.40.200	255.255.255.0	192.168.40.254		✓		<input type="checkbox"/>

### 3. 配置 PPPoE 拨号服务，让 VLAN 下面的客户机可以通过 PPPoE 拨号上网（可选）

进入“应用” -> “PPPoE 拨号服务” -> “参数配置”，在监听网络接口中，勾选所有的 VLAN 接口，然后保存设置即可

PPPoE/BRAS 服务  开启

参数配置 上网策略 通知提醒 地址池管理 PPPoE 透传 账号管理 在线用户

PPPoE 服务实时监测

PPPoE 连接: 建立中 0, 活动 0

服务运行状态 **运行中 <PID: 3308>** 详情...

监听网络接口

- LAN-1 <lan1/lan1/172.16.0.2>
- LAN-1.10 <lan1/lan1.10/192.168.10.254>
- LAN-1.20 <lan1/lan1.20/192.168.20.254>
- LAN-1.30 <lan1/lan1.30/192.168.30.254>
- LAN-1.40 <lan1/lan1.40/192.168.40.254>

## 三层交换机上的配置

这里以 H3C S5024 为例

```
vlan 10 20 30 40
## 默认 VLAN1 IP 地址
interface Vlanif1
 ip address 172.16.0.1 255.255.255.0
## VLAN10 IP 地址
interface Vlanif10
 ip address 192.168.10.1 255.255.255.0
```



```
## VLAN20 IP 地址
interface Vlanif20
  ip address 192.168.30.1 255.255.255.0
## VLAN30 IP 地址
interface Vlanif30
  ip address 192.168.30.1 255.255.255.0
## VLAN40 IP 地址
interface Vlanif40
  ip address 192.168.40.1 255.255.255.0
## 端口 1-5 在 VLAN-10 中
#-----
interface GigabitEthernet0/0/1
  port link-type access
  port default vlan 10
#
... 省略 ...
#
interface GigabitEthernet0/0/5
  port link-type access
  port default vlan 10
#-----
## 端口 6-10 在 VLAN-20 中
#-----
interface GigabitEthernet0/0/6
  port link-type access
  port default vlan 20
#
... 省略 ...
#
interface GigabitEthernet0/0/10
  port link-type access
  port default vlan 20
#-----
## 端口 11-15 在 VLAN-30 中
#-----
interface GigabitEthernet0/0/11
  port link-type access
  port default vlan 30
#
... 省略 ...
#
interface GigabitEthernet0/0/15
  port link-type access
  port default vlan 30
```

```
#-----  
## 端口 16-20 在 VLAN-40 中  
#-----  
interface GigabitEthernet0/0/16  
  port link-type access  
  port default vlan 40  
#  
... 省略 ...  
#  
interface GigabitEthernet0/0/20  
  port link-type access  
  port default vlan 40  
#-----  
## 端口 21~23 在默认 VLAN1 中  
#-----  
#  
interface GigabitEthernet0/0/21  
... 省略 ...  
#  
interface GigabitEthernet0/0/23  
#  
## 端口 24 接路由的 LAN 口，端口模式为 trunk 口（允许所有 VLAN 访问）  
#-----  
#  
interface GigabitEthernet0/0/24  
  port link-type trunk  
  port trunk allow-pass vlan 2 to 4094  
#-----
```

## 网络诊断及测试

---

### 1. 内网互通测试

使用任一一台电脑（IP 设为和路由 LAN 口相同网段 172.16.0.X），

接入三层交换机的任一默认 VLAN1 端口（21-23 口），进入路由

Web-》“工具”-》“PING 测试”，依次

- PING 交换机的 VLAN1 的 IP 地址，如不通，检查交换机的 vlan1 接口 ip 设置
- PING 交换机的其他各个 VLAN(10~40)的 IP 地址，如不通，检查路由上 VLAN 设置由是否正确，或交换机的 vlan 接口的 ip 设置
- PING 交换机下某一 VLAN 下的客户机的 IP，比如 VLAN10 下的 192.168.10.2，如果不通，检查交换机上的 vlan 设置是否正确

## 2. 访问外网测试

在 VLAN 下的客户机电脑上（比如 VLAN10 中的 192.168.10.2），访问外网，如果不通，检查

- 数字列表项目其网关是否设为路由 LAN 口对应 VLAN 的接口 IP (192.168.10.254)

## VLAN 穿透方案的优缺点

优点：

- 路由上的 DHCP 可以为 VLAN 下的客户机分配 IP
- VLAN 下的客户机可以通过 PPPoE 拨号穿透三层交换机到路由
- 路由上可获得 VLAN 下客户机的 MAC 地址

缺点：VLAN 之间的互访需通过路由转发

另外参考：[企业 VLAN 网络三层转发](#)

## QinQ 双层 VLAN 穿透/透传

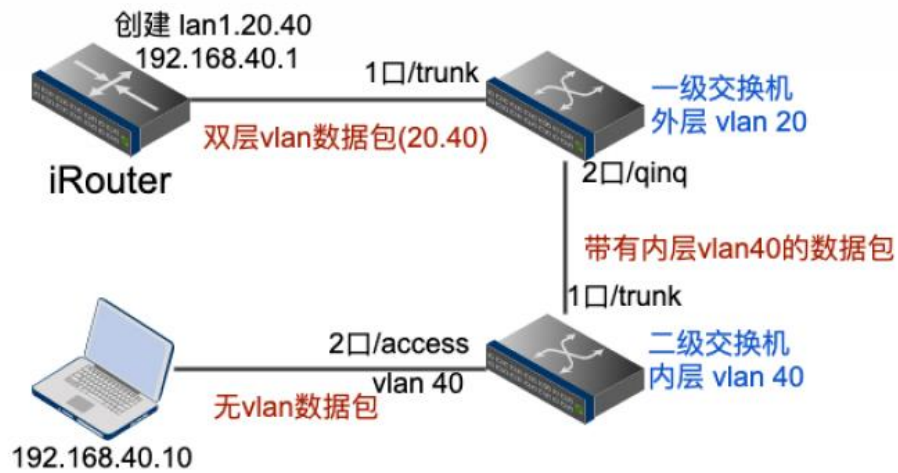
三层交换机及 OLT 支持 QinQ VLAN，路由上创建对应的 QinQ VLAN，路由 LAN 口接交换机的 trunk 口。

### 什么是 QinQ

QinQ 是指在 802.1Q VLAN 的基础上增加一层 802.1Q VLAN 标签，从而拓展 VLAN 的使用空间。在公网的传输过程中，设备只根据外层 VLAN Tag 转发报文，并根据报文的外层 VLAN Tag 进行 MAC 地址学习，而用户的私网 VLAN Tag 将被当作报文的数据部分进行传输。

### 网络拓扑

## iRouter QinQ 双层VLAN透传



## 路由上创建 QinQ VLAN

网络-》VLAN-》创建 VLAN:

QinQ VLAN ID 格式: <内层 VLAN>.<外层 VLAN>, 例如 20.40

在LAN1接口创建QinQ VLAN

名称	lan1.20.40	外层VLAN: 20 内层VLAN: 40
线路	lan1 <lan1.br/192.168.2.73>	
VLAN ID	20.40	
QinQ VLAN 外层标签类型(TPID)	802.1q (默认)	
IP地址	192.168.20.1	
MAC地址	00-68-1e-a7-c7-06	随机生成
子网掩码	<此网段可容纳 254 台主机> 192.168.20.1~192.168.20.254 /24 = 255.255.255.0(默认)	

## QinQ 报文

QinQ 报文根据外层标签的不同，分为 2 种：802.1q 和 802.1ad

802.1q: 外层标签类型和内层相同，都是 0x8100 (大多数是这  
种)：

```
▶ Frame 8: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
▼ Ethernet II, Src: 00:68:1e:a7:c7:06 (00:68:1e:a7:c7:06), Dst: 00:77:92:bf:c4:8f (00:77:92:bf:c4:8f)
  ▶ Destination: 00:77:92:bf:c4:8f (00:77:92:bf:c4:8f)
  ▶ Source: 00:68:1e:a7:c7:06 (00:68:1e:a7:c7:06) QinQ 数据包类型1
  Type: 802.1Q Virtual LAN (0x8100) 外层VLAN
▼ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 20
  000. .... = Priority: Best Effort (default) (0)
  ...0 .... = CFI: Canonical (0)
  .... 0000 0001 0100 = ID: 20
  Type: 802.1Q Virtual LAN (0x8100) 内层VLAN
▼ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 40
  000. .... = Priority: Best Effort (default) (0)
  ...0 .... = CFI: Canonical (0)
  .... 0000 0010 1000 = ID: 40
  Type: IPv4 (0x0800)
▶ Internet Protocol Version 4, Src: 192.168.20.1, Dst: 192.168.20.2
▶ Transmission Control Protocol, Src Port: 6964, Dst Port: 5201, Seq: 1, Ack: 1, Len: 0
```

802.1ad: 外层标签类型是 0x88a8

```
▶ Frame 7: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
▼ Ethernet II, Src: 00:77:92:bf:c4:8f (00:77:92:bf:c4:8f), Dst: 00:68:1e:a7:c7:06 (00:68:1e:a7:c7:06)
  ▶ Destination: 00:68:1e:a7:c7:06 (00:68:1e:a7:c7:06)
  ▶ Source: 00:77:92:bf:c4:8f (00:77:92:bf:c4:8f) QinQ 数据包类型2
  Type: 802.1ad Provider Bridge (Q-in-Q) (0x88a8) 外层VLAN
▼ IEEE 802.1ad, ID: 20
  000. .... = Priority: 0
  ...0 .... = DEI: 0
  .... 0000 0001 0100 = ID: 20
  Type: 802.1Q Virtual LAN (0x8100) 内层VLAN
▼ 802.1Q Virtual LAN, PRI: 0, CFI: 0, ID: 40
  000. .... = Priority: Best Effort (default) (0)
  ...0 .... = CFI: Canonical (0)
  .... 0000 0010 1000 = ID: 40
  Type: IPv4 (0x0800)
▶ Internet Protocol Version 4, Src: 192.168.20.2, Dst: 192.168.20.1
▶ Transmission Control Protocol, Src Port: 5201, Dst Port: 5116, Seq: 1, Ack: 41993, Len: 0
```

可根据所在网络的情况在创建 QinQ 时进行修改。

注：修改 QinQ 外层标签类型后，需要先禁用该 VLAN，然后重新启用生效。

## 三层交换机上的配置

以华为 S5700 为例：外层 vlan20，内层 vlan40

一级交换机 A 上的配置：

```
## 创建外层 VLAN
vlan batch 20
## 上联路由端口，设为 trunk，允许外层 vlan 通过
interface GigabitEthernet0/0/1
    port link-type trunk
    port trunk allow-pass vlan 20
## 下联二级交换机 B，设为 QINQ 接口（灵活 QINQ：为具有不同内层 VLAN ID 的报文添加不同的外层 VLAN Tag）
interface GigabitEthernet0/0/2
    qinq vlan-translation enable
    port hybrid untagged vlan 20          《= 发出去的包剥离外层 vlan 20（发给二级交换机）
    port vlan-stacking vlan 40 stack-vlan 20    《= 为内层 vlan40 添加外层 vlan 20（从二级交换机进来的包）
## 下联二级交换机 B，设为 QINQ 接口（基于端口的 QINQ）
interface GigabitEthernet0/0/3
    port link-type dot1q-tunnel
    port default vlan 20
#
```

这里两种 QINQ 方式都可以，二级交换机可以接 2 口或 3 口。

二级交换机 B 上的配置：

```
### 创建用户 vlan（内层 vlan）
vlan batch 40
### 上联一级交换机的口，设为 trunk，允许内层 vlan 通过
interface GigabitEthernet0/0/1
    port link-type trunk
    port trunk allow-pass vlan 40
#
### 接终端设备，access 口，用户 vlan
interface GigabitEthernet0/0/2
    port link-type access
    port default vlan 40
```

更多关于交换机的设置，请参考 [常见交换机配置](#)

## OLT 支持 QinQ

适用场景：多个小区共用一台 OLT，每个小区一个独立的外层 VLAN，内层 VLAN 相同。

网络环境：外层 vlan 为 20，内层 vlan 为 46，48，4015

网络拓扑：路由(光口) — OLT — 分光器 — 光猫

路由 LAN 口创建 QinQ VLAN 如下：

启用VLAN (虚拟局域网)

VLAN列表 | VLAN状态

共 4 条记录/1页, 每页显示 10 请输入关键字

ID	名称	线路	VLAN	IP地址 MAC地址	子网掩码	备注	状态
1	lan2.20	lan2	20	192.168.20.254	255.255.255.0		<input checked="" type="checkbox"/>
2	lan2.20.4015	lan2	20.4015	192.168.40.254	255.255.255.0		<input checked="" type="checkbox"/>
3	lan2.20.46	lan2	20.46	192.168.46.254	255.255.255.0		<input checked="" type="checkbox"/>
4	lan2.20.48	lan2	20.48	192.168.48.254	255.255.255.0		<input checked="" type="checkbox"/>

华为 MA5680T OLT 配置如下：

```
vlan 20 smart
vlan attrib 20 q-in-q
port vlan 20 0/19 1
interface gpon 0/1
  ont add 1 23 sn-auth "434D4443000EA2AF" omci ont-lineprofile-id 20 ont-srvprofile-id 20
  desc "qinq_test"
```



```

dba-profile add profile-id 10 profile-name "ftth" type4 max 1024000
ont-srvprofile gpon profile-id 20 profile-name "qinq"
  ont-port pots adaptive eth adaptive
  commit
  quit
ont-lineprofile gpon profile-id 20 profile-name "qinq"
  tr069-management ip-index 0
  tcont 1 dba-profile-id 10
  gem add 0 eth tcont 1
  gem add 1 eth tcont 1
  gem add 2 eth tcont 1
  gem mapping 0 1 vlan 4015
  gem mapping 1 1 vlan 46
  gem mapping 2 1 vlan 48
  commit
  quit
service-port 256 vlan 20 gpon 0/1/1 ont 23 gempport 0 multi-service user-vlan 4015 \
  tag-transform translate-and-add inner-vlan 4015 inbound traffic-table index 6 outbound
traffic-table index 6
service-port 254 vlan 20 gpon 0/1/1 ont 23 gempport 1 multi-service user-vlan 46 \
  tag-transform translate-and-add inner-vlan 46 inbound traffic-table index 6 outbound traffic-
table index 6
service-port 255 vlan 20 gpon 0/1/1 ont 23 gempport 2 multi-service user-vlan 48 \
  tag-transform translate-and-add inner-vlan 48 inbound traffic-table index 6 outbound traffic-
table index 6

```

## 路由 DHCP 服务设置 QinQ VLAN IP 地址池：

IP地址池
固定IP分配
当前分配信息

共 7 条记录/1页, 每页显示 200
请输入关键字
搜索
清除
新建IP地址池
一键生成默认地址池

ID	IP 地址段 接口	子网掩码	网关	备注
1	192.168.48.100-192.168.48.200 lan2.20.48	255.255.255.0	192.168.48.254	
2	192.168.46.100-192.168.46.200 lan2.20.46	255.255.255.0	192.168.46.254	
3	192.168.40.100-192.168.40.200 lan2.20.4015	255.255.255.0	192.168.40.254	

成功后，光猫会获得 IP，例如：

The screenshot shows a network management interface for TR069. A modal window displays the configuration for the WAN interface 'WAN - 1\_TR069\_R\_VID\_4015', which is currently connected. The configuration details are as follows:

WAN - 1_TR069_R_VID_4015 < 已连接 >	
连接模式:	路由
承载业务:	TR069
上线时长:	0天0小时0分24秒
MAC地址:	44:C8:74:50:EC:20
地址类型:	DHCP
IP地址/子网掩码:	192.168.40.101 / 255.255.255.0
网关:	192.168.40.254

## 独臂路由模式部署

独臂路由（又称单臂路由），用于路由器只有一块物理网卡的情况。

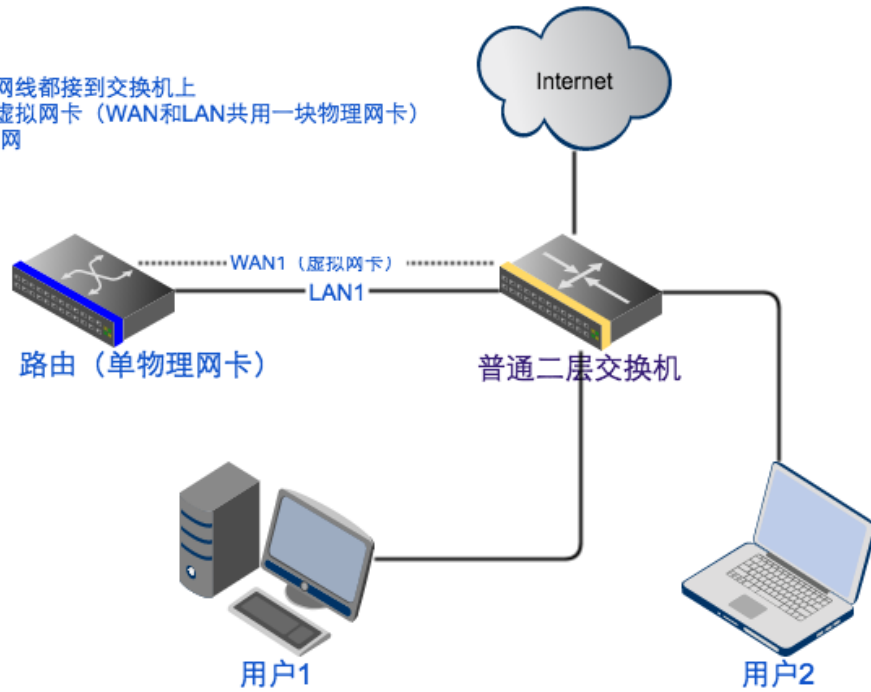
## 网络拓扑

---

## 路由单网卡部署（独臂路由）

步骤及要点：

1. 将内网和外网线都接到交换机上
2. 路由中创建虚拟网卡（WAN和LAN共用一块物理网卡）
3. 配置WAN上网



## 创建虚拟接口

进入“网络” -> “虚拟接口”，启用“虚拟接口”功能：

网络配置界面截图，显示“虚拟接口”功能已启用。

左侧菜单：网络 > 虚拟接口

右侧内容：

虚拟接口

在一个物理网卡上通过VLAN虚拟多个接口，每个接口都拥有独立的MAC地址，如同多个物理网卡

虚拟接口  已开启 ← 开启功能 & 新增规则

虚拟接口列表  ← 虚拟接口状态

共 0 条记录 / 1 页，每页显示 默认 条

ID	接口名	VLAN	MAC地址	网卡	备注
----	-----	------	-------	----	----

添加规则，在 lan1 接口上创建 wan1，VLAN 填 0（表示基于 MAC 的 VLAN），MAC 地址随机生成：

在LAN1网卡上创建虚拟网卡WAN1

接口名

VLAN

MAC地址

物理网卡

备注

激活

创建成功后，点击 wan1 进入 WAN 口配置页面

虚拟接口列表   新增规则   虚拟接口状态   [点击直接跳转到wan1的配置页](#)

共 1 条记录 / 1 页, 每页显示  条        

ID	接口名	VLAN	MAC地址	网卡	备注	状态
1	<input type="text" value="wan1"/>	0	42-98-3c-e3-50-75	lan1		✓

## 配置 WAN 口

WAN-1 配置    线路检测

当前网卡不支持网线状态探测

上行流量统计: 共发送 0.12 KB, 发送包 3, 出错 0, 丢弃 0

下行流量统计: 共接收 140.93 KB, 接收包 1.41K, 出错 0, 丢弃 0

根据网络环境选择对应的接入方式

网络接口: WAN-1 - wan1 - 虚拟接口

MAC地址: 42-98-3c-e3-50-75

MAC地址克隆:

Internet 接入方式:  固定/静态IP  
 DHCP自动获取IP  
 ADSL/PPPoE 拨号

IP地址: 192.168.1.76

子网掩码: <此网段可容纳 254 台主机> 192.168.1.1~192.168.1.254  
/24 = 255.255.255.0

扩展IP配置 >>

网关: 192.168.1.10

## 内网多 LAN 接入

多 LAN 分为以下几种情况:

- 1. 独立的多 LAN 口: 每个 LAN 口有自己的 IP, 且不同网段  
每个 LAN 口接不同的设备, 如交换机或服务器, 如果 LAN  
口下的终端是 DHCP 上网, 需要为这个 LAN 添加 IP 地址池  
(默认地址池只对 LAN1 分配)
- 2. 多 LAN 口汇聚: 多个网口汇聚成一个 LAN 口使用, 共用  
一个 IP

LAN 口网卡都接到同一个交换机上，同时交换机上也需开启端口汇聚，可实现带宽叠加和故障转移。

- 3. 多 LAN 口网桥：多个网口桥接在一起，共用一个 IP  
LAN 口网卡都在同一个网段，相当于处于一个大的交换机下。每个网口可以接不同的设备，但不能将 2 个网口接到同一个交换机上，否则会形成环路。

## 独立的多个 LAN 口

第一步：绑定多个 LAN 口到物理网卡，名字可以自定义，如 lan2,lan3 ...



网络

物理接口 独立的多LAN口

将 LAN、WAN 接口和物理网卡对应起来

ID	接口名	类型	物理网卡 <设备名 - 型号 - MAC - 网线插入状态>	备注	状态
1	lan1	网桥	网卡1-1口 - lan1 - Broadcom BCM5720 2-port Gbit - 34-64-a9-9a-8a-78 - <span style="color: red;">✖</span>		🟢
2	lan4	以太网	网卡2-2口 - lan4 - Intel 82599ES 10-Gbit SFI/SFP+ - 00-1b-21-bc-72-72 - <span style="color: red;">✖</span>	光纤跳线	🟢
3	lan5	以太网	网卡2-1口 - lan5 - Intel 82599ES 10-Gbit SFI/SFP+ - 00-1b-21-bc-72-70 - <span style="color: red;">✖</span>	万兆线缆	🟢
4	wan1	以太网	网卡1-2口 - wan1 - Broadcom BCM5720 2-port Gbit - 34-64-a9-9a-8a-79 - <span style="color: blue;">✔</span>	电信固定IP	🟢

第二步：为每个 LAN 口配置 IP

IP 不能和其他 LAN 口重复或在同一网段

物理网卡 独立的多LAN，每个LAN拥有不同网段的IP

设备名	网卡型号	MAC/IP地址	上/下行实时/累计流量
lan5 万兆线缆	Intel 82599ES 10-Gbit SFI/SFP+ <span>网卡2-1口</span>	00-1b-21-bc-72-70 <b>192.168.100.73 / 24</b>	0.00 Mbps / 0.00 Mbps 0.00 KB / 0.00 KB
lan4 光纤跳线	Intel 82599ES 10-Gbit SFI/SFP+ <span>网卡2-2口</span>	00-1b-21-bc-72-72 <b>192.168.200.73 / 24</b>	0.00 Mbps / 0.00 Mbps 0.00 KB / 0.00 KB
lan1	Broadcom BCM5720 2-port Gbit <span>网卡1-1口</span> <span>63.0°C</span>	<span>网桥1</span> lan1.br 34-64-a9-9a-8a-78 <b>192.168.2.73 / 24</b> <span>VLAN</span> <span>2</span>	0.00 Mbps / 0.00 Mbps 220.27 MB / 979.22 MB
wan1 电信固定IP	Broadcom BCM5720 2-port Gbit <span>网卡1-2口</span> <span>63.0°C</span>	34-64-a9-9a-8a-79	<span>1Gb</span>

第三步：

### 3.1 为 LAN 口设置 DHCP IP 分配地址池（可选）

网络 为每个LAN口分配不同的地址池

参数设置 IP地址池 固定IP分配 当前分配信息

共 6 条记录/1页, 每页显示 10 请输入关键字 搜索 清除 新建IP地址池 一键生成默认地址池

ID	IP 地址段	子网掩码	网关	备注	状态	编辑
1	172.73.0.100-172.73.0.200	255.255.255.0	172.73.0.1		☑	<span>编辑</span>
2	192.68.30.100-192.68.30.200	255.255.255.0	192.68.30.73		☑	<span>编辑</span>
3	192.68.40.100-192.68.40.200	255.255.255.0	192.68.40.73		☑	<span>编辑</span>
4	<b>192.168.2.100-192.168.2.200</b>	255.255.255.0	192.168.2.73		☑	<span>编辑</span>
5	192.168.100.100-192.168.100.200	255.255.255.0	192.168.100.73		☑	<span>编辑</span>
6	192.168.200.100-192.168.200.200	255.255.255.0	192.168.200.73		☑	<span>编辑</span>

### 3.2 PPPoE 服务增加监听网卡（可选）

☑ PPPoE/BRAS 服务

参数配置 上网策略 通知提醒 PPPoE 透传

PPPoE 服务实时监测

PPPoE 连接: 0 连接中, 50 已连接

服务运行状态 运行中 <PID: 6289> 更多...

监听网络接口

<input checked="" type="checkbox"/>	lan1 <lan1/192.168.10.254>
<input checked="" type="checkbox"/>	lan2 <lan2/192.168.100.254>

[编辑列表](#)

修改网卡后，需要重启 PPPoE 服务生效，重启服务时，当前已连接的用户会断线重播。

## 多 LAN 口汇聚

需要交换机支持，通常用的较多的汇聚类型是 802.3ad LACP（动态链路聚合）

在物理网卡绑定时，选择汇聚或汇聚网桥类型：

接口名

接口类型

汇聚模式

传输哈希策略

接口成员

<input checked="" type="checkbox"/>	网卡1-1口 - lan1 - Broadcom Limited BCM5716 Gbit - LAN-1   已连接
<input checked="" type="checkbox"/>	网卡1-2口 - eth1 - Broadcom Limited BCM5716 Gbit - LAN-1   已连接



汇聚成功后在首页可以看到汇聚状态：

设备名	网卡型号	MAC/IP地址	上/下行实时/累计流量	
lan1	Broadcom Limited BCM5716 Gbit 网卡1-1口	汇聚网桥1 lan1.br d4-ae-52-a6-8f-05 192.168.1.75 / 24 VLAN 1 扩展IP 4 公网IP 221.232.56.119 湖北省武汉市青山区 / 洪山区	0.10 Mbps / 0.28 Mbps 46.06 GB / 305.04 GB	汇聚 2Gb 1Gb
eth1	Broadcom Limited BCM5716 Gbit 网卡1-2口	汇聚1 lan1.bd d4-ae-52-a6-8f-06		1Gb

交换机上的设置（以 H3C S5720 为例）：

```
interface Eth-Trunk2
description Linked to DELL R710
port link-type trunk
port trunk allow-pass vlan 2 to 4094
mode lacp
interface GigabitEthernet0/0/1
eth-trunk 2
interface GigabitEthernet0/0/3
eth-trunk 2
```

## 多 LAN 口网桥

此类型用的较少，和单 LAN 网桥类似，只是绑定多个网卡。

LAN 口网桥主要用于 KVM 虚拟机的场合，虚拟机的虚拟网卡和物理网卡桥接，更多参考 [虚拟机网络类型](#)

## 汇聚网桥

多个 LAN 先汇聚，提供冗余及加倍带宽，然后基于汇聚设备创建网桥，可以和虚拟机桥接。



## 动态路由协议

### 功能介绍

动态路由协议通过路由信息的交换生成并维护转发引擎所需的路由表。

当网络拓扑结构改变时动态路由协议可以自动更新路由表，并负责决定数据传输最佳路径。

动态路由协议包括： RIP V1/V2 OSPF BGP IS-IS

### 路由 AD 管理距离值表

协议名称	距离值
外部 BGP	20
OSPF	110

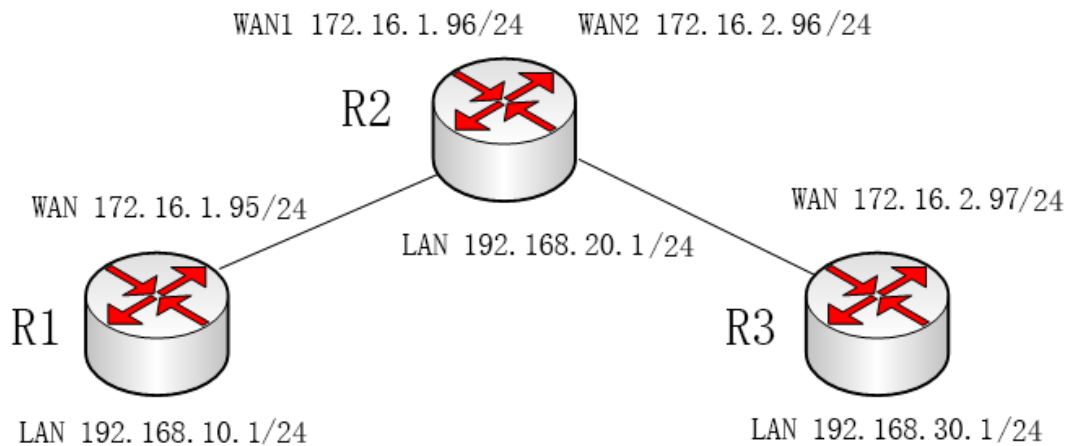
IS-IS	115
RIP	120
内部 BGP	200

距离值越小信任度越高越优先，有高优先级就仅保留一条路由表，当高优先级路由表不存在时才更新低优先级路由表

## 部署环境

进入“应用” -》“模块管理”，点击“检查更新”，安装

“drouting” 动态路由协议 模块，每个需要建立动态路由协议的路由都要安装



R1 R2 R3 是三个路由，其中 R1 和 R3 通过 R2 相连，各个之间都没有互指网关和添加对方内部路由表。 安装并配置好任意一种动态路由协议后，可以实现 R1 与 R3 之间及其 LAN 的互通

## RIP V1

1. 进入“路由” → “动态路由协议”，开启应用，勾选“RIP V1/V2 路由协议”，密码任意配置

动态路由协议	<input type="checkbox"/> 开启
参数配置	运行状态
服务运行状态	运行中 <PID: 9944>
Telnet 管理密码	admin
BGP 默认 AS ID	6500
运行的路由协议	<input checked="" type="checkbox"/> RIP V1/V2 路由协议 ( 端口2602 )

2. telnet 进入路由的 2602，做如下配置

```
Password:
ripd>
ripd> enable ← 进入特权模式
ripd#
ripd# configure terminal ← 进入全局配置模式
ripd(config)#
ripd(config)# router rip ← 进入RIP配置
ripd(config-router)#
ripd(config-router)# version 1 ← RIP版本号
ripd(config-router)# network 172.16.1.0/24
ripd(config-router)# network 192.168.10.0/24 ← 将所有接口网段加入
ripd(config-router)#
ripd(config-router)# write
Configuration saved to /etc/config/ripd.conf
```

3. 所有路由的 RIP 都配置好后，telnet 进入路由的 2601 端口，输入如下命令显示路由表

```

Password:
Router>
Router> show ip route ← 显示当前路由表
Codes: K - kernel route, C - connected, S - static, R - RIP,
       0 - OSPF, I - IS-IS, B - BGP, P - PIM, A - Babel, N - NHRP,
       > - selected route, * - FIB route

C>* 127.0.0.0/8 is directly connected, lo
C>* 172.16.1.0/24 is directly connected, wan1
R 172.16.2.0/24 [120/2] via 172.16.1.96, wan1, 00:08:43
K>* 172.16.2.0/24 via 172.16.1.96, wan1
C>* 192.168.10.0/24 is directly connected, lan1
R 192.168.20.0/24 [120/2] via 172.16.1.96, wan1, 00:08:43
K>* 192.168.20.0/24 via 172.16.1.96, wan1
R>* 192.168.30.0/24 [120/3] via 172.16.1.96, wan1, 00:00:29

```

前面带有 R 的是新建立的 RIPv1 动态路由表，可以看它到 R2 R3 所经过的接口和跳数

4. 可以用 ping 测试到其它路由内部接口的通路

## RIP V2

1. RIP V2 配置过程类似 RIP V1，telnet 进入路由的 2602，做如下配置

```

Password:
ripd>
ripd> enable
ripd#
ripd# configure terminal
ripd(config)#
ripd(config)# router rip ← 进入RIP配置
ripd(config-router)#
ripd(config-router)# version 2 ← RIP版本号
ripd(config-router)#
ripd(config-router)# network 172.16.1.0/24 将所有接口网段加入
ripd(config-router)#
ripd(config-router)# network 192.168.10.0/24
ripd(config-router)# exit
ripd(config)#
ripd(config)# interface wan1 ← 进入与其它设备通讯的接口
ripd(config-if)#
ripd(config-if)# ip rip authentication key-chain test 配置RIP通讯的验证码
ripd(config-if)#
ripd(config-if)# write
Configuration saved to /etc/config/ripd.conf
ripd(config-if)#

```

所有需要相通讯的 RIP 协议设备需要配置相同的 key 验证码

2. 所有路由的 RIP 都配置好后，telnet 进入路由的 2601 端口，输入如下命令显示路由表

```
Router> show ip route ← 显示当前路由表
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, P - PIM, A - Babel, N - NHRP,
       > - selected route, * - FIB route

C>* 127.0.0.0/8 is directly connected, lo
C>* 172.16.1.0/24 is directly connected, wan1
R>* 172.16.2.0/24 [120/2] via 172.16.1.96, wan1, 00:01:41
C>* 192.168.10.0/24 is directly connected, Vlan1
R>* 192.168.20.0/24 [120/2] via 172.16.1.96, wan1, 00:21:26
R>* 192.168.30.0/24 [120/3] via 172.16.1.96, wan1, 00:00:29
```

前面带有 R 的是新建立的 RIPv2 动态路由表

RIP V1/V2 区别:

Version 1 所有版本需用相同的子网掩码，更新路由不带有子网掩码信息;

Version 2 所有设备无需相同的子网掩码，更新路由传送子网掩码信息，并且带有接口验证功能

## OSPF

1. 进入“路由” → “动态路由协议”，开启应用，勾选“OSPF 路由协议”，密码任意配置

运行的路由协议

RIP V1/V2 路由协议 ( 端口2602 )

OSPF 路由协议 ( 端口2604 )

2. telnet 进入路由的 2604，做如下配置

```
Password:
ospfd>
ospfd> enable ← 进入特权模式
ospfd#
ospfd# configure terminal ← 进入全局模式
ospfd(config)#
ospfd(config)# router ospf ← 进入OSPF配置
ospfd(config-router)#
ospfd(config-router)# router-id 1 配置ID标识
ospfd(config-router)#
ospfd(config-router)# network 172.16.1.95/24 area 0
ospfd(config-router)#
ospfd(config-router)# network 192.168.10.1/24 area 0 将所有接口宣告
ospfd(config-router)#
ospfd(config-router)# write
Configuration saved to /etc/config/ospfd.conf
ospfd(config-router)#
```

3. 所有路由的 OSPF 都配置好后，telnet 进入路由的 2601 端口，输入如下命令显示路由表

```
Password:
Router>
Router> show ip route ← 显示当前路由表
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, P - PIM, A - Babel, N - NHRP,
       > - selected route, * - FIB route

C>* 127.0.0.0/8 is directly connected, lo
O 172.16.1.0/24 [110/10] is directly connected, wan1, 00:22:27
C>* 172.16.1.0/24 is directly connected, wan1
O>* 172.16.2.0/24 [110/20] via 172.16.1.96, wan1, 00:04:57
O 192.168.10.0/24 [110/10] is directly connected, lan1, 00:22:16
C>* 192.168.10.0/24 is directly connected, lan1
O>* 192.168.20.0/24 [110/20] via 172.16.1.96, wan1, 00:04:57
O>* 192.168.30.0/24 [110/30] via 172.16.1.96, wan1, 00:04:57
Router>
```

前面带有 O 的是新建立的 OSPF 动态路由表，可以看它到 R2 R3 所经过的接口和距离值

4. 可以用 ping 测试到其它路由内部接口的通路

## BGP

1. 进入“路由” → “动态路由协议”，开启应用，勾选“BGP 路由协议”，每个区域配置不同的 AS 自治系统号，密码任意配置

Telnet 管理密码	<input type="text" value="admin"/>
BGP 默认 AS ID	<input type="text" value="6500"/>
运行的路由协议	<input type="checkbox"/> RIP V1/V2 路由协议 ( 端口2602 )
	<input type="checkbox"/> OSPF 路由协议 ( 端口2604 )
	<input checked="" type="checkbox"/> BGP 路由协议 ( 端口2605 )

相同的 AS 自治系统号属于内部 BGP，不同 AS 自治系统号属于外部 BGP。一般 1-64511 为公有 AS，64512-65535 为私有 AS

## 2. telnet 进入路由的 2605，做如下配置

```
Password:
bgpd> enable
bgpd# configure terminal
bgpd(config)# router bgp 6500 ← 进入BGP的AS号
bgpd(config-router)# bgp router-id 192.168.30.1 ← ID一般配置内网LAN地址
bgpd(config-router)# network 172.16.2.0/24 ← 宣告BGP网段
bgpd(config-router)# redistribute connected ← 配置重建分发
bgpd(config-router)# neighbor 172.16.2.96 remote-as 5500 ← 配置邻居接口
bgpd(config-router)# write
configuration saved to /etc/config/bgpd.conf
```

router-id 不可写 0.0.0.0

## 3. 所有路由的 BGP 都配置好后，telnet 进入路由的 2601 端口，输入如下命令显示路由表



```
Router> show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, P - PIM, A - Babel, N - NHRP,
       > - selected route, * - FIB route

C>* 127.0.0.0/8 is directly connected, lo
B 172.16.1.0/24 [20/0] via 172.16.2.96, wan1, 00:32:07
K>* 172.16.1.0/24 via 172.16.2.96, wan1
C>* 172.16.2.0/24 is directly connected, wan1
B 192.168.10.0/24 [20/0] via 172.16.2.96, wan1, 00:32:07
K>* 192.168.10.0/24 via 172.16.2.96, wan1
B 192.168.20.0/24 [20/0] via 172.16.2.96, wan1, 00:32:07
K>* 192.168.20.0/24 via 172.16.2.96, wan1
C>* 192.168.30.0/24 is directly connected, lan1
Router>
```

前面带有 B 的是新建立的 BGP 动态路由表

4. 可以用 ping 测试到其它路由内部接口的通路

## IS-IS

1. 进入“路由” → “动态路由协议”，开启应用，勾选“IS-IS 路由协议”，密码任意配置

Telnet 管理密码	admin
BGP 默认 AS ID	5500
运行的路由协议	<input type="checkbox"/> RIP V1/V2 路由协议 (端口2602) <input type="checkbox"/> OSPF 路由协议 (端口2604) <input type="checkbox"/> BGP 路由协议 (端口2605) <input checked="" type="checkbox"/> IS-IS 路由协议 (端口2608)

2. telnet 进入路由的 2608，做如下配置

```

Password:
isisd> enable
Password:
isisd#
isisd# configure terminal
isisd(config)# router isis DEAD ← 进入默认ISIS进程名
isisd(config-router)#
isisd(config-router)# no net 47.0023.0000.0003.0300.0100.0102.0304.0506.00
isisd(config-router)#
isisd(config-router)# net 47.0023.0000.0003.0300.0100.0102.0304.0508.00 ← 修改默认net标识
isisd(config-router)# exit
isisd(config)#
isisd(config)# interface wan1
isisd(config-if)#
isisd(config-if)# ip router isis DEAD ← 进入各接口宣告启用ISIS进程名
isisd(config-if)# exit
isisd(config)#
isisd(config)# interface lan1 ← 进入各接口宣告启用ISIS进程名
isisd(config-if)# ip router isis DEAD
isisd(config-if)# write
Configuration saved to /etc/config/isisd.conf

```

默认的 ISIS 进程名和 net 标识在运行状态中可以查看

参数配置
运行状态

路由协议
IS-IS

当前配置

```

isis circuit-type level-1
interface lo
interface tun0
interface wan1
ip router isis DEAD
isis circuit-type level-1
interface wan2
ip router isis DEAD
isis circuit-type level-1
router isis DEAD ← IS-IS协议的默认配置
net 47.0023.0000.0003.0300.0100.0102.0304.0506.00
metric-style wide
is-type level-1
log-adjacency-changes
line vty
end

```

net 为网络实体标识，一般以 47 开头，00 结尾，每个设备的 net 标识不要相同

- 所有路由的 IS-IS 都配置好后，telnet 进入路由的 2601 端口，输入如下命令显示路由表

```
Router> show ip route
Codes: K - kernel route, C - connected, S - static, R - RIP,
       O - OSPF, I - IS-IS, B - BGP, P - PIM, A - Babel, N - NHRP,
       > - selected route, * - FIB route

C>* 127.0.0.0/8 is directly connected, lo
I>* 172.16.1.0/24 [115/20] via 172.16.2.96, wan1, 00:00:41
I 172.16.2.0/24 [115/20] via 172.16.2.96 inactive, 00:00:41
C>* 172.16.2.0/24 is directly connected, wan1
I>* 192.168.10.0/24 [115/30] via 172.16.2.96, wan1, 00:00:26
I>* 192.168.20.0/24 [115/20] via 172.16.2.96, wan1, 00:00:41
C>* 192.168.30.0/24 is directly connected, lan1
```

前面带有 I 的是新建立的 IS-IS 动态路由表

#### 4. 可以用 ping 测试到其它路由内部接口的通路

提示:

终端配置完毕后进入特权模式或全局模式可以随时输入 show running-config 查看整体配置

任何模式下输入 write 均可保存配置。

## VRRP 双机热备

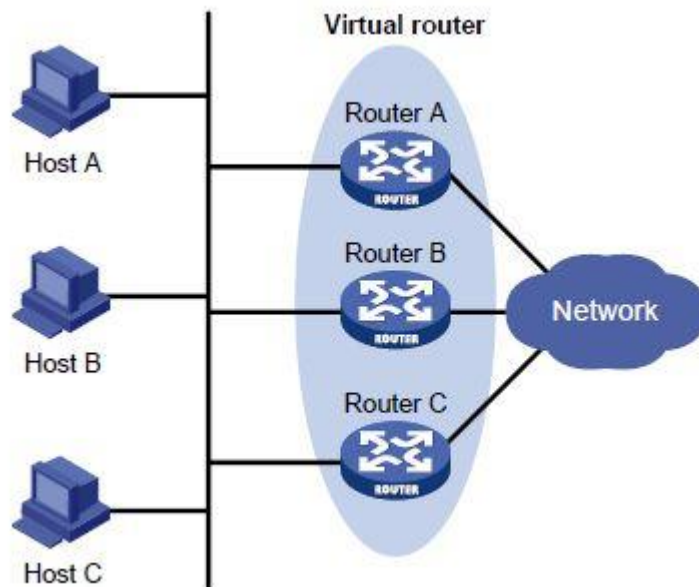
### VRRP 简介

VRRP (Virtual Router Redundancy Protocol, 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 是一种容错协议, 在提高可靠性的同时, 简化了主机的配置。

在具有多播或广播能力的局域网 (如以太网) 中, 借助 VRRP 能在某

台路由器出现故障时仍然提供高可靠的缺省链路，有效避免单一链路发生故障后网络中断的问题，而无需修改动态路由协议、路由发现协议等配置信息。



## 工作原理

---

VRRP 的工作过程如下：

(1) 路由器开启 VRRP 功能后，会根据优先级确定自己在备份组中的角色。优先级高的路由器成为 Master 路由器，优先级低的成为 Backup 路由器。Master 路由器定期发送 VRRP 通告报文，通知备份组内的其他路由器自己工作正常；Backup 路由器则启动定时器等待通告报文的到来。

(2) 当 Backup 路由器收到 VRRP 通告报文后，会将自己的优先级与通告报文中的优先级进行比较。如果大于通告报文中的优先级，则成为 Master 路由器；否则将保持 Backup 状态。

(3) 如果 Backup 路由器的定时器超时后仍未收到 Master 路由器发送来的 VRRP 通告报文，则认为 Master 路由器已经无法正常工作，此时 Backup 路由器会认为自己是 Master 路由器，并对外发送 VRRP 通告报文。备份组内的路由器根据优先级选举出 Master 路由器，承担报文的转发功能。

如果 Backup 路由器在等待了 3 个间隔时间后，依然没有收到 VRRP 通告报文，则认为自己是 Master 路由器，并对外发送 VRRP 通告报文，重新进行 Master 路由器的选举。

用户可以通过设置 VRRP 定时器来调整 Master 路由器发送 VRRP 通告报文的时间间隔，推荐使用默认间隔：1 秒。

## 安装模块

应用-》模块-》检查更新，找到 “vrrp ” 模块，点击安装。

安装成功后，访问菜单：路由-》VRRP 双机热备

## 主路由上的设置

---

✔ VRRP 双机热备

功能开关

参数配置

运行日志

服务运行状态 运行中 <PID: 18453>

默认工作模式  主节点  备份节点 一台设为主，其他设为备份

虚拟路由器的标识(VRID)  所有路由设为相同，表示在同一个VRRP组内

优先级  主路由优先级数字高于备份节点

虚拟 IP 地址  所有路由设为相同，  
这个IP是局域网用户上网的网关

虚拟IP 通告时间间隔  秒

通信密钥

监控物理接口  lan1 <lan1.br/192.168.2.73>

虚拟路由器的标识(VRID)范围：1-254

优先级范围：1-254

通信密钥可自定义：数字和字母组成，长度 6-24 字符。

## 备份路由上的设置

---

虚拟路由器的标识(VRID)、虚拟路由地址、通信密钥均设为和主路由一样，优先级设为比主路由小。

VRRP 双机热备

参数配置

运行日志

服务运行状态 运行中 <PID: 1773>

默认工作模式  主节点  备份节点

虚拟路由器的标识(VRID) 100 设为和主路由相同

优先级 50 数字比主路由小

虚拟 IP 地址 192.168.2.254 和主路由相同

虚拟IP 通告时间间隔 1 秒

通信密钥 v123456 和主路由相同

监控物理接口  lan1 <lan1.br/192.168.2.34>

## 路由切换测试

将主路由的 LAN 口网线拔掉，主路由进入故障模式，3 秒左右，备份路由将自动切换为主路由，并接管网关 IP 192.168.2.254

将主路由网线插回，主路由以备份路由角色上线，3 秒左右（VRRP 选举协商后），再次切换回主路由角色。

参数配置

运行日志

主路由VRRP切换

VRRP 运行日志:

自动刷新

```
2020-07-30 17:23:38 INSTANCE VI_1 master 初始为主路由
2020-07-30 17:23:56 INSTANCE VI_1 fault 拔掉LAN口网线后
2020-07-30 17:24:16 INSTANCE VI_1 backup 重新插上网线，以备份路由角色上线
2020-07-30 17:24:19 INSTANCE VI_1 master 重回主路由角色
```

VRRP 运行日志:

自动刷新

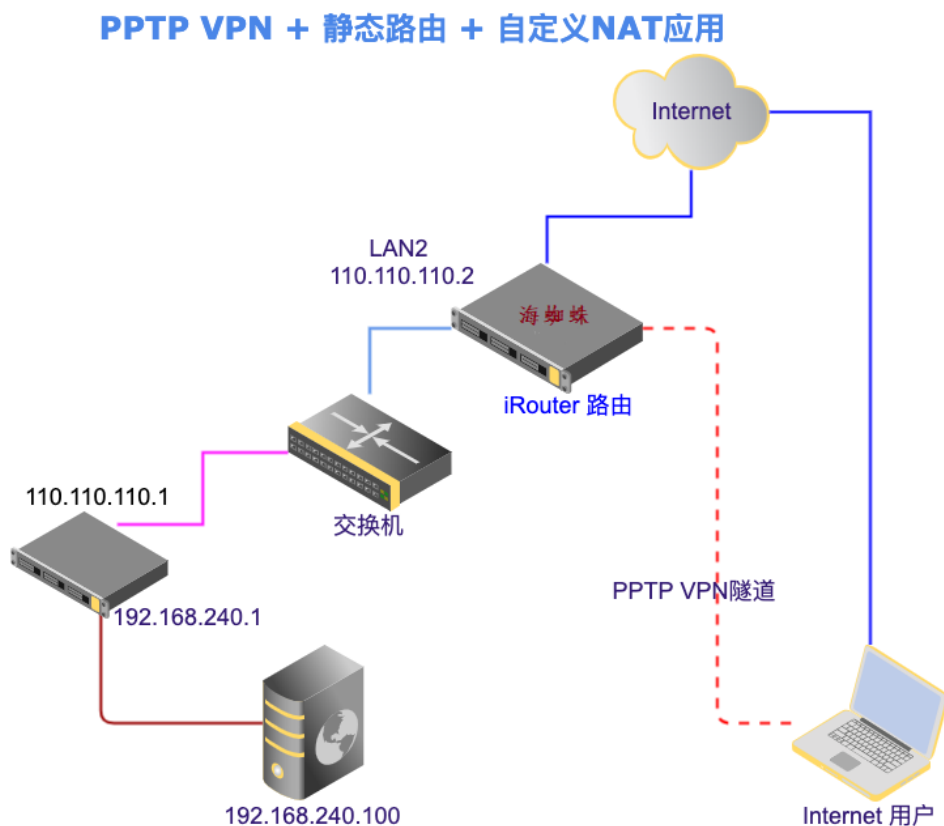
```
2020-07-30 17:23:46 INSTANCE VI_1 backup 初始为备份路由
2020-07-30 17:23:59 INSTANCE VI_1 master 检测到主路由故障, 接管主路由
2020-07-30 17:24:16 INSTANCE VI_1 backup 主路由正常回归, 退居二线成为备胎
```

## 自定义 NAT 规则

自定义源地址转换 (SNAT) 或目的地址转换规则 (DNAT)

### 场景: PPTP VPN + 静态路由访问内网指定网段

#### 网络拓扑





路由上开启 PPTP VPN 服务，LAN2 口 (IP 为 110.110.110.2) 通过静态路由可访问到局域网内另外一个网段。

路由上的设置：

静态路由规则：

启用静态路由

规则列表    静态路由状态

共1条记录/1页, 每页显示 200 请输入关键字

ID	目的网络	出口网关	线路 / 备份线路	跳数	备注	状态	编辑	选择
1	192.168.240.0/255.255.255.0	110.110.110.1	lan2	1		<input checked="" type="checkbox"/>	<input type="button" value="编辑"/>	<input type="checkbox"/>

PPTP VPN 服务端：

PPTP VPN 服务    PPTP VPN 服务配置

VPN 服务实时监测

PPTP VPN 连接: 建立中 0, 活动 0

服务运行状态 **运行中 <PID: 6684>**

分配给客户的地址池范围 178.10.10.0/24

用户认证模式 本机 RADIUS 认证

允许VPN客户访问Internet  否  是

自动设置分配给用户的DNS  是  否

VPN客户只能访问内网不能上外网

要求：客户通过 VPN 拨号后，能访问到上述网段 (192.168.240.0/24)，不能通过 VPN 访问外网。

## 自定义 NAT 规则：

新增规则如下：



源IP 178.10.10.0/24 PPTP VPN 网段

目的IP 192.168.240.0/24 要访问的目标网段

协议 TCP+UDP

目的端口 1~65535

类型  SNAT (源地址转换)  DNAT (目的地址转换)  禁止连接跟踪

动作 进行地址转换(NAT)

NAT 后的地址 110.110.110.2 伪装成LAN2口的IP去访问

添加完成后如下：

启用自定义 NAT

共1条记录/1页, 每页显示 10 请输入关键字

ID	名称 备注	优先级	源IP	目的IP 目的端口	类型	动作	状态	编辑	选择
1	pptp_lan240	1	178.10.10.0/24	192.168.240.0/24	snat	donat: 110.110.110.2	<input checked="" type="checkbox"/>	<input type="button" value="编辑"/>	<input type="checkbox"/>

PPTP VPN网段 目标网段 源地址转换 伪装成lan2口的IP

全选 / 全不选

# 交换机配置

## Console 口连接

通过 USB 转 Console 线, 或者 USB 转串口+串口 Console 线, 连接路由器的 USB 到交换机到 Console 口

2020/12/17 以后版本支持



## 华为 S5700 交换机配置

通过 Console 口连接交换机, 串口波特率 9600

### 恢复出厂设置

```
reset saved-configuration
```

输入 Y

```
reboot
```

输入 N

输入 Y

详细操作如下:

<Quidway>reset saved-configuration =》 恢复出厂设置指令

Warning: The action will delete the saved configuration in the device.

The configuration will be erased to reconfigure. Continue? [Y/N]:Y =》 输

入 Y 确认恢复

Warning: Now clearing the configuration in the device.

Oct 1 2008 00:16:06-05:13 Quidway %%01CFM/4/RST\_CFG(l)[0]:The user chose Y

when deciding whether t

o reset the saved configuration.

Info: Succeeded in clearing the configuration in the device.

<Quidway>reboot =》 重启

Info: The system is now comparing the configuration, please wait.

Warning: The configuration has been modified, and it will be saved to the next

startup saved-config

uration file . Continue? [Y/N]:N =》 输入 N 不保存配置

Info: If want to reboot with saving diagnostic information, input 'N' and then

execute 'reboot save

diagnostic-information'.

System will reboot! Continue?[Y/N]:Y =》 输入 Y 确认重启

Oct 1 2008 00:16:31-05:13 Quidway %%01CMD/4/REBOOT(l)[1]:The user chose Y  
when deciding whether to

reboot the system. (Task=co0, Ip=\*\*, User=\*\*)

Info: System is rebooting, please wait...

Oct 1 2008 00:16:32-05:13 Quidway %%01SRM/4/MSTRSCURST(l)[2]:Master SCU  
is reset.

Oct 1 2008 00:16:32-05:13 Quidway %%01SRM/4/RESETREASON(l)[3]:Board  
reset by VRP command or net ma  
nager.

System reboot at 00:16:33

BIOS loading ...

漫长的等待... 约 1 分钟...

Recover configuration...OK!                   => 恢复配置成功

Press ENTER to get started.

恢复成功后，第一次启动时会提示设置登录密码，输入 Y，然后 2 次输入新密码即可：

An initial password is required for the first login via the console.

Continue to set it? [Y/N]: Y                   =》 输入 Y 设置密码

Set a password and keep it safe. Otherwise you will not be able to login via the  
console.

Please configure the login password (8-16)   =》 2 次输入密码，8-16 个字符

Enter Password:

Confirm Password:

### 配置管理口 IP

```
<Quidway>sys
```

```
[Quidway]interface MEth 0/0/1
```

```
[Quidway-MEth0/0/1]ip address 10.11.0.57 255.255.255.0
```

```
[Quidway-MEth0/0/1]quit
```

```
[Quidway]
```

### 开启 Telnet

```
[Quidway]telnet server enable
```

Warning: Telnet is not a secure protocol, and it is recommended to use Stelnet.

创建 telnet 登录账号 admin, 密码 mq123456

```
[Quidway]aaa
```

```
[Quidway-aaa] undo local-user admin
```

```
[Quidway-aaa]local-user admin password cipher mq123456
```

<= 配置用户名、密码

```
[Quidway-aaa]local-user admin privilege level 15
```

<= 配置用户权限为 15, 最高权限

```
[Quidway-aaa]local-user admin service-type telnet
```

<= 配置用户的接入类型为 telnet

```
[Quidway-aaa]quit
```

```
[Quidway]user-interface vty 0 4
```

```
[Quidway-ui-vty0-4]authentication-mode aaa          <= 配置 VTY 用户的验证界面为 AAA
```

```
[Quidway-ui-vty0-4]protocol inbound all           <= 配置 VTY 用户界面支持的协议为所有
```

```
[Quidway-ui-vty0-4]quit
```

```
[Quidway]
```

在 AAA 视图下面给 admin 用户修改密码的时候提示错误无法修改成功； 告警信息

```
[S7706-aaa] local-user admin password cipher Huawei@123!@#
```

```
Error: The password encryption mode cannot be changed.
```

解决办法：先 undo local-user admin

### 华为交换机 Console 密码重置

- 1、通过 Console 口连接交换机，并重启交换机。
- 2、当界面出现以下打印信息时，及时按下快捷键“Ctrl+B”并输入 BootROM/BootLoad 密码，进入 BootROM/BootLoad 主菜单
- 3、密码： Admin@huawei.com A 必须大写。
- 4、选着 7 Clear password for console user （选择清除 console 用户密码模式）。
- 5、选择 1 Boot with default mode（键入 1 启动默认模式），进入后更改 Console 及 telnet 密码。

Wind River Linux 6.0.0.30 localhost console

localhost login: root (automatic login)

Jan 23 2017, 19:22:34

BootLoad version : 020a.0001

Backup U-Boot ..... done

Press Ctrl+B or Ctrl+E to enter BootLoad menu: 1

Password: <= 输入密码 Admin@huawei.com

The default password is used now. Change the password.

#### BootLoad Menu

1. Boot with default mode
2. Enter serial submenu
3. Enter startup submenu
4. Enter ethernet submenu
5. Enter filesystem submenu
6. Enter password submenu
7. Clear password for console user
8. Reboot

(Press Ctrl+E to enter diag menu)

Enter your choice(1-8): 7

Note: Clear password for console user? Yes or No(Y/N): Y

Clear password for console user successfully.

Note: Choose "1. Boot with default mode" to boot, then set a new password



### BootLoad Menu

1. Boot with default mode
2. Enter serial submenu
3. Enter startup submenu
4. Enter ethernet submenu
5. Enter filesystem submenu
6. Enter password submenu
7. Clear password for console user
8. Reboot

(Press Ctrl+E to enter diag menu)

Enter your choice(1-8): 1

Now, the current startup file is flash:/s5720ei-v200r010c00spc600.cc

## 动态域名解析 (DDNS)

支持动态域名解析提供商：

- [阿里云](#)
- [腾讯 DNSPod](#)
- [花生壳](#)
- [3322](#)
- [金万维](#)

- 其他国外 DDNS

以花生壳为例，设置如下：

需要解析的域名  动态域名

显示更多选项 >

动态域名提供商

用户名或 Key ID  账号/密码

密码或 Key Secret

线路  外网线路

备份线路

备注

激活  是

点击更新域名，查看日志：

```
2021-01-28 20:55:03 restart2013.vicp.cc A 当前记录为 61.142.176.23，新记录为 221.232.58.158
2021-01-28 20:55:03 正在更新域名 restart2013.vicp.cc ...
S: 220 oray.cn DDNS ServerX6 Ready.
C: auth router6
S: 334 3eg6nlunJ...FwLWDJm3g==
C: cmVzdGFydDIwMTMgl...oCayqwWE2i...j...y8oAxUFq
S: 250 Auth passed at level <0>
restart2013.vicp.cc
.
C: regi a restart2013.vicp.cc
S: 250 Register successfully
C: cnfm
S: 250 10706983 165051115
== 成功 221.232.58.158
```

# PPPoE 拨号服务/宽带运营

## 功能介绍

为局域网内的主机通过 PPPoE 拨号上网服务

## 快速配置

### 1. PPPoE 服务主要参数配置

The screenshot shows a configuration interface for PPPoE service. It includes the following elements:

- 服务运行状态:** A green button indicating the service is running with PID 5703, and a link for more details.
- 监听网络接口:** A list of three interfaces: lan1 (192.168.2.73), lan1.30 (192.68.30.73), and lan1.40 (192.68.40.73), each with a checked checkbox. Includes an '编辑列表' (Edit List) link and a '全选 / 全不选' (Select All / Deselect All) link.
- PPPoE 服务名字:** A text input field containing 'PPPoE\_Server'.
- 分配给客户机的地址段:** A text input field containing '10.10.0.0/22'.
- 用户认证模式:** A dropdown menu set to '本机 RADIUS 认证'.
- 自动设置分配给用户的DNS:** A radio button set to '是' (Yes).
- 操作按钮:** '保存设置' (Save Settings), '默认设置' (Default Settings), and '重启服务' (Restart Service).

分配给客户机的地址段 通常使用内网 IP 段或不常用的外网 IP 段, 第一个 IP 为 PPPoE 服务器使用。 比如 172.XX.YY.ZZ 或 10.XX.YY.ZZ 或 100.XX.YY.ZZ 或 200.XX.YY.ZZ

### 2. PPPoE 服务高级配置

会话最长在线时间(超过强制下线)  分钟

最大空闲时间(超过则主动断开连接)  秒

**额外运行参数**

账号首次拨号时自动绑定其MAC

防止同一个MAC地址多次拨入相同的账号

- 拨号账号不区分大小写
- 自动绑定客户机的 MAC 地址
- 允许 PPPoE 客户之间互访
- 使用内部限速模式(效率更高,但不支持限速白名单)
- 启用调试
- 每个MAC限制一个会话,新的会话将终止旧的会话
- 禁止自动踢下线(默认同一账号超出登录数限制,则将最早登录的用户踢下线)

其中每个 MAC 限制一个会话,不启用时,在账号登录数限制为 1 时,有些路由或者恶意攻击者会使用同一个 MAC 将一个账号同时拨入多次。

配置完成后,在“账号管理”中添加账号,拨号测试即可。

### 本地认证账号

管理 PPPoE/FTP/Samba/PPTP VPN/IPsec VPN等服务的用户账号信息

账号管理 套餐管理 导入导出

共2条记录/1页,每页显示 10 请输入关键字  搜索  帐号状态 所有

ID	用户名	姓名	- 可用功能 - 分配固定IP	使用期限 (开通 - 到期) 上线/下线时间	套餐	备注	状态	编辑	选择
1	aaa <sup>1</sup>	我就测试而已	PPPOE FTP PORTAL PPTPVPN SSLVPN IPSECVPN FILESERVER	~ 上线时间: 2020-07-22 16:09:39		这里是备注	上线	<input type="button" value="编辑"/>	<input type="checkbox"/>
2	bbb		PORTAL	~2020-06-24			<input checked="" type="checkbox"/>	<input type="button" value="编辑"/>	<input type="checkbox"/>

7天 续费 批量修改套餐 专家模式 导出 全选 / 全不选

### 3. 查看 PPPoE 客户端拨号状态

访问菜单：状态-》接口-》连接

The screenshot shows a web interface for network management. On the left is a sidebar menu with options: 状态 (Status), 总览 (Overview), 接口 (Interface), 硬件信息 (Hardware Info), 端口信息 (Port Info), 日志查看 (Log View), 统计报表 (Statistics Report), NAT会话 (NAT Session), and 实时流量 (Real-time Traffic). The main content area is titled '接口' (Interface) and has sub-tabs for '接口状态' (Interface Status), '接口负载' (Interface Load), '连接' (Connection), and '路由表' (Routing Table). The '连接' tab is active. Below the tabs, there are search and refresh controls. A table displays one record for a PPPoE client.

ID	设备名	本地IP 远程IP	流量	建立时间 已连接	类型	帐号	备注
1	ppp0	10.10.0.1 10.10.0.2	8.60 KB 16.82 KB	2020-07-22 16:09:39 0天0小时1分56秒	PPPoE 客户 « 4c-32-75-99-c5-95	aaa 我就测试而已	这里是备注

注意事项：

用户认证模式和 RADIUS 对接参数变化时，需重启 PPPoE 服务生效

## 和外部计费系统对接

### 海蜘蛛计费系统

#### 1. 计费系统上的配置

添加 NAS (路由)

文鼎网络 基本设置 用户管理 费用管理 状态报表 网络相关 运行了 23 天 3 小时 54 分钟 负载: 0.00

快速菜单 添加 NAS禁用列表 刷新列表

### 添加路由

*NAS名称:	海蜘蛛路由测试	✔ 输入正确!
*负责人:	张三	✔ 输入正确!
*电话:	911	✔ 输入正确!
备注:		💡 写备注是一个良好的习惯
*NAS类型:	Ros路由	💡 非海蜘蛛路由用户请选择其它NAS
*NAS通讯端口:	880	💡 请输入海蜘蛛路由的Web管理端口, 用于扩展功能通讯
*NAS IP类型:	动态IP	💡 如果NAS使用固定IP地址, 请选择静态IP。否则请选择动态IP
*NAS服务器标识:	hzzrouter	✔ 输入正确!
是否校验标识:	<input type="checkbox"/>	💡 如果启用, 用户将不能跨NAS认证
*NAS IP:	0.0.0.0/0	✔ 输入正确!
*共享密钥:	test123	⚠ 【所有动态NAS使用同一个密钥, 请谨慎修改】,[4-20]个字母数字

和路由上设为一致

确定 关闭

然后创建套餐，及用户账号

文鼎网络 基本设置 用户管理 费用管理 状态报表 网络相关

快速菜单 新增用户 刷新 更多操作

### 用户开户

*用户帐号:	aaa	✔ 该用户名可以注册
*密码:	.....	✔ 输入正确
*确认密码:	.....	✔ 密码一致
*所属NAS服务器:	海蜘蛛路由对接测试	✔ 谢谢配合
是否设置专拨:	<input type="checkbox"/>	💡 专用PPPOE
*计费套餐:	10M包月	✔ 谢谢配合
立即生效:	<input checked="" type="checkbox"/> 是	💡 勾选后, 自动选择生效时间为今天
检测在线状态:	<input type="checkbox"/> 是	💡 勾选后, 自动检测在线状态
*购买套餐数:	1	💡 需要购买的套餐数量
*需支付金额:	100	💡 实际需要支付的金额
自动续费:	<input checked="" type="checkbox"/> 是	💡 用户即将过期并且用户余额大于0, 系统会自动为用户续费
登录方式:	PPP	💡 可以限定用户使用web,ppp或者

打印票据 确定 关闭

## 2. 路由上的配置

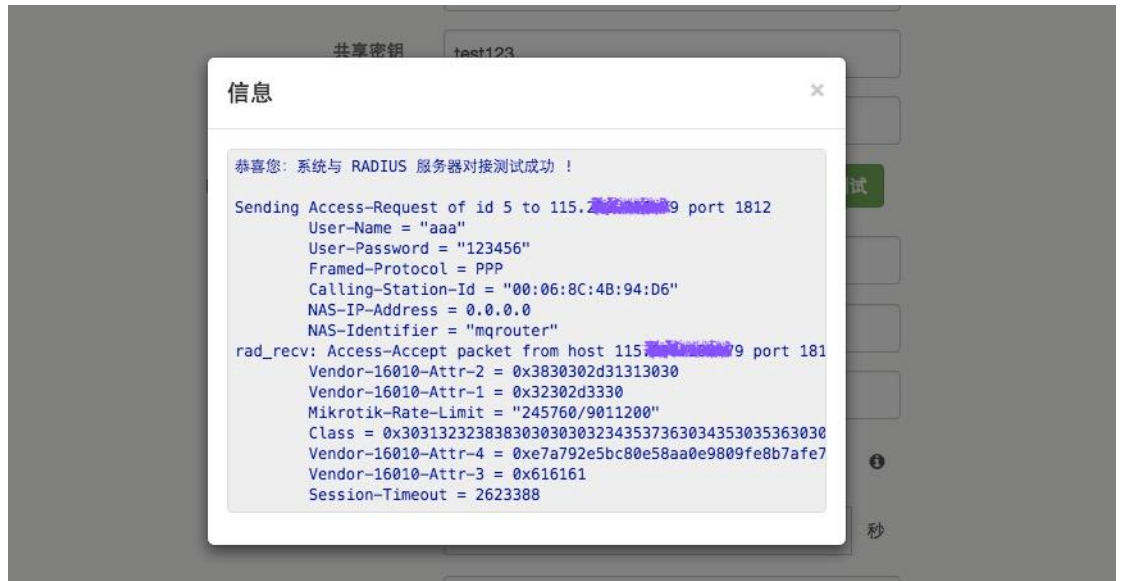
用户认证模式	外部 RADIUS 认证
RADIUS 计费服务器地址	115.2... 计费服务器IP
共享密钥	test123 和计费服务器上的一致
认证端口	1812
RADIUS 测试账号及密码	aaa 123456 对接测试
记账端口	1813
NAS 服务器标识	hzzroute 和计费服务器上的一致
NAS 服务器IP	0.0.0.0
COA 通信端口	3799 ⓘ
实时记账时间间隔	300 秒

注意事项:

- 如果计费系统在外网，路由的外网是动态 IP 或多线，通常“NAS 服务器 IP” 设为 '0.0.0.0'
- 如果计费系统在内网(如 IP 为 192.168.10.100)，NAS 服务器 IP 设为和计费系统同网段的 IP (如 192.168.10.254)

## 3. 对接测试

首先在路由上使用测试账号进行对接测试



然后在用户电脑上使用 PPPoE 拨号测试

## 蓝海卓越计费系统

1. 计费系统上的配置，进入“计费设置” - “NAS 管理”，添加 NAS 设备

IP地址：	219.139.10.10	请输入合法的IP地址
设备名称：	mqtest	请输入设备名称
厂商：	linux	请选择厂商
COA端口：	3799	* 合法的端口，1-65535
共享密钥：	natshell	请输入共享密钥
备注：	测试	

配置好区域项目和产品管理后，进入“用户管理” - “添加用户”



*选择运营商：	本地	
所属区域：	mqtest2	
用户属性：	新装	
用户帐号：	mqtest01	不允许修改账号
用户密码：	123456	配置账号密码
用户名称：	mq	
证件号码：		
手机号码：	13000002211	
固定电话：		
入户方式：	未指定	
*所属区域：	<a href="#">点击选择客户所属区域</a>	
*详细住址：	湖北 > 武汉, 光谷世贸中心	联系地址不能为空,

## 2. 路由上的设置

用户认证模式	外部 RADIUS 认证
RADIUS 计费服务器地址	125.71. [REDACTED] 蓝海计费地址
共享密钥	natshell 同计费系统
认证端口	1812
RADIUS 测试账号及密码	mqtest01 123456 <span>对接测试</span>
记账端口	1813
NAS 服务器标识	mqtest 同计费系统
NAS 服务器IP	219.139. [REDACTED]
COA 通信端口	3799
实时记账时间间隔	300 秒

### 3. 对接测试

首先在路由上使用测试账号进行对接测试

恭喜您：系统与 RADIUS 服务器对接测试成功！

```
Sending Access-Request of id 212 to 125.71. port 1812
  User-Name = "mqtest01"
  User-Password = "123456"
  Framed-Protocol = PPP
  Calling-Station-Id = "00:A9:BE:99:9D:15"
  NAS-IP-Address = 219.139.
  NAS-Identifier = "mqtest"
rad_recv: Access-Accept packet from host 125.71. port 1812, id=2
12, length=134
  Framed-Protocol = PPP
  Framed-Compression = Van-Jacobson-TCP-IP
  Vendor-12341-Attr-7 = 0x696e23313d616c6c20736861706520353132303
030202039363030302070617373
  Vendor-12341-Attr-7 = 0x6f757423323d616c6c207368617065203230393
7313532203339333231362070617373
  Acct-Interim-Interval = 300
  Framed-MTU = 1480
  Session-Timeout = 2588560
```

然后在用户电脑上使用 PPPoE 拨号测试

## 卓迈计费系统

1. 计费系统上的配置，进入“模板配置” - “NAS 管理”，添加新 NAS

**NAS修改**

NAS地址:  \* 如: niaomuniao  
 NAS地址:  \* 如: 172.16.0.1  
 设备厂商:  \* 对应路由COA通信端口  
 端口:  \* 1-9的数字, 如: 3799  
 共享密钥:  \*  
 设备标识:

然后创建套餐，进入“模板配置” - “计费模板”，添加新模板

我的主页 | NAS管理 | 计费模板

名称:  检索

说明: 是指  修改

添加  编号

30  
 29  
 31

名称:  \* 计费类型:

流量类型:  最短使用周期:  \* 年

费用:  \* 元 初装费用:  \* 元

所属地区(组):  优惠策略:

周期类型:  续费开始时间:

排序:  \*

创建用户账号，进入“用户管理” - “用户开户”

**用户资料:**

用户帐号:  \* 用户密码:  \*

真实姓名:  证件号码:

证件附件:  上传图片 查看图片

工作电话:  家庭电话:

手机号码:  电子邮件:  x

联系地址:  在线人数:

## 2. 路由上的设置

用户认证模式	外部 RADIUS 认证
<b>RADIUS 计费服务器地址</b>	192.168.10.250 <b>卓迈计费地址</b>
<b>共享密钥</b>	mqtest2017 <b>同计费系统</b>
认证端口	1812
RADIUS 测试账号及密码	test 123456 <b>对接测试</b>
记账端口	1813
<b>NAS 服务器标识</b>	mq <b>同计费系统</b>
NAS 服务器IP	192.168.10.1
<b>COA 通信端口</b>	3799
实时记账时间间隔	300 秒

## 3. 对接测试

在路由上使用测试账号进行对接测试

## 信息



恭喜您：系统与 RADIUS 服务器对接测试成功！

```
Sending Access-Request of id 247 to 192.168.10.250 port 1812
  User-Name = "qwer"
  User-Password = "123456"
  Framed-Protocol = PPP
  Calling-Station-Id = "00:3D:2F:DA:23:FB"
  NAS-IP-Address = 192.168.10.1
  NAS-Identifier = "mq"
rad_recv: Access-Accept packet from host 192.168.10.250 port 1812, id=247, length=20
```

然后在电脑上使用 PPPoE 拨号时，计费会出现在线用户

编号	帐号	拨号时间	在线时间	IP 地址	MAC地址	网关地址	
<input type="checkbox"/>	1	test12	2017-06-16 17:27:23		20.20.0.1	3c:97:0e:b5:e7:e7	192.168.10.1

## 第三方 RADIUS 计费支持

计费软件	限速	地址池	到期管理	RADIUS 强制踢下线	选择设备类型
蓝海	支持	支持	支持	支持	Mikrotik/ROS
凌风	支持	支持	支持	支持	Mikrotik/ROS
Radius Manager 3.9	支持	支持	不支持	下一版支持	Mikrotik/ROS
Radius Manager 4.X	即将支持	即将支持	即将支持	即将支持	即将支持
安腾	支持	不支持	不支持	暂不支持	Mikrotik/ROS

## RADIUS 字典

项目	Attributes 属性	取值 (实例)	说明
IP 地址	Framed-IP-Address	10.10.0.10	下发 IP 地址
计费更新	Acct-Interim-	60	计费更新时间间隔【秒】

时间	Interval		
上行限速 1	RP-Upstream-Speed-Limit	125	单位为 KB/S, 换算 上行 1Mbps
下行限速 1	RP-Downstream-Speed-Limit	1250	单位为 KB/S, 换算 下行带宽 10Mbps
限速方式 2	Mikrotik-Rate-Limit	1000k/10000k 1000000/10000000	或 上行 1000kbps/ 下行 10000kbps
到期时间	Session-Timeout	86400	86400 秒后强制踢下线, 0 或不 下发此属性表示不强制下线
PPPOE 地址	NAS-IP-Address	192.168.1.254	与 RADIUS 服务器连接的接口的 IP 地址
接口 VLAN	NAS-Port-Id	10	用户端 VLAN 标识, 用于 RADIUS 校验或绑定
踢用户下 线	COA 3799 端口	此机制遵循 RFC 3576	此机制遵循 RFC 3576

## Portal/Web 认证

### 功能介绍

提供 Portal/Web 上网认证服务, 客户上网时, 跳转到指定认证页面, 输入账号/密码后, 才能访问 Internet。

### 安装模块

应用-》模块-》检查更新, 找到 “braserver ” 模块, 点击安装。

共 1 条记录/1页, 每页显示 200 ▾ 请输入关键字

ID	名称	备注	版本 发布时间	大小 占用内存	自动更新	选择
1	brserver 	PPPoE / PPTP VPN / Portal 认证服务 <a href="#">更多...</a> 为局域网提供上网认证服务, 包括PPPoE拨号、PPTP VPN、及Portal Web认证。	1.4.6 2021-03-22 21:03:36	1.53 MB 6.84 MB	<input checked="" type="checkbox"/>	<input type="checkbox"/>

安装成功后, 访问菜单: 应用-》Portal/Web 认证

## 典型设置

根据需要, 对所有内网启用 Portal 认证, 或对指定 IP 段启用认证:

上网 Portal 认证

参数配置    本地认证模板    通知提醒

强制所有用户 Portal 认证上网  关

[上网时需要认证的IP及网段](#) 

192.168.201.0/24  
192.168.1.100-192.168.1.200  
192.168.2.0/255.255.255.0  
192.168.3.1

3 种认证模式可选, 若本地认证, 需要在应用-》本地认证账号中创建账号:





如果需要自定义认证模版，先上传模版后，再启用。

## 默认认证页面



## 在线用户

状态-》接口-》连接，可以查看已认证 Portal 用户：

The screenshot shows the '接口' (Interface) section of a network management system. The '连接' (Connections) tab is selected. A table displays active connections, with the IP address '192.168.201.81' highlighted in red. Below the table, there is a link '点击踢下线' (Click to kick offline).

ID	设备名	本地IP / 远程IP	建立时间 / 已连接	类型	Portal 认证客户	帐号
1		192.168.201.81 -	98.35 MB / 4.01 MB 2021-03-23 12:00:36 / 0天0小时0分26秒	Portal 认证客户	« 0c-d7-46-51-4f-f0	aaa 20M

## 认证日志

状态-》日志查看：

The screenshot shows the '日志查看' (Log View) section. The '日志类型' (Log Type) dropdown is set to 'PPPoE/VPN/Portal 认证'. The table below shows two log entries, with the second entry indicating a successful Portal authentication for the user 'aaa' from IP '192.168.201.81'.

ID	日期时间	内容
1	2021-03-23 12:00:36	加载限速模板: 192.168.201.81 => 20M
2	2021-03-23 12:00:36	aaa [192.168.201.81 - 0c-d7-46-51-4f-f0] Portal认证成功

## 自定义认证模版

步骤：下载模版-》修改-》压缩-》上传-》保存模版

参数配置 本地认证模板 通知提醒

当前模板文件大小: 610.35 KB

1). 下载默认模版到电脑上 2). 修改模版 3. 压缩成zip文件, 确保index.htm 文件必须在根目录下

↓ 下载默认模板 ↓ 下载当前模板

请点击 "上传" 按钮上传文件 (ZIP/TAR/TGZ格式):

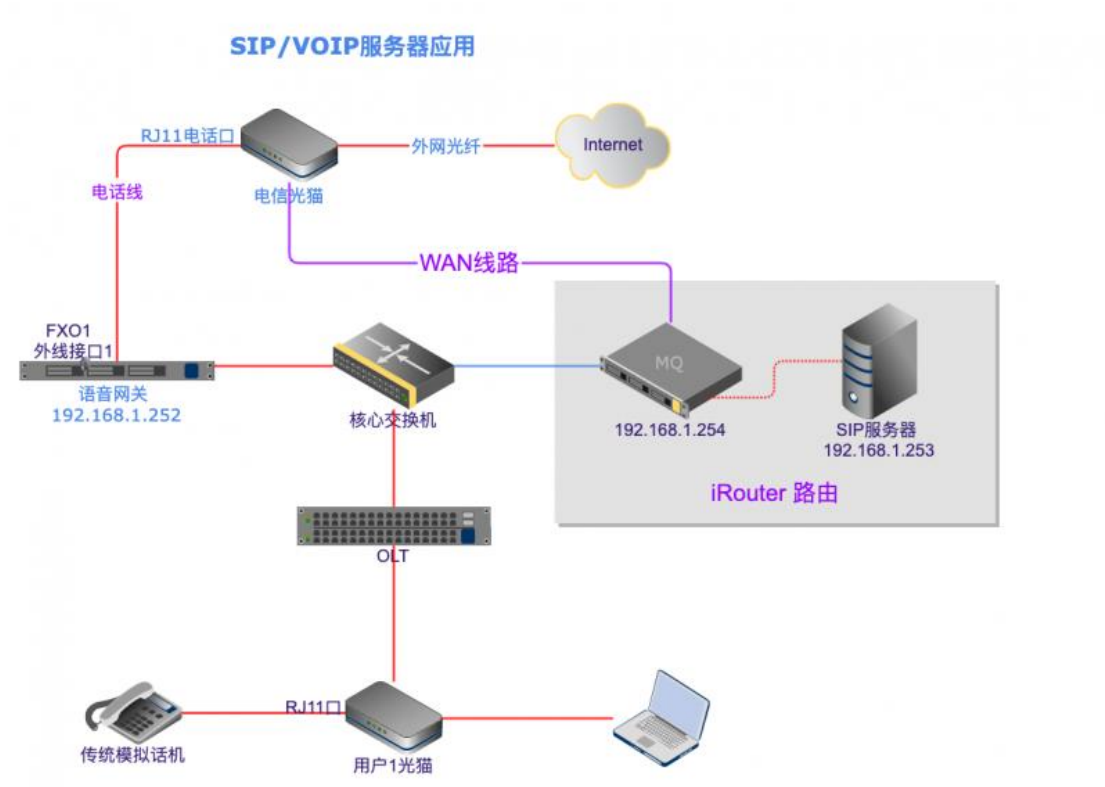
⌂ 上传模板 保存模板

4. 上传模版-》保存模版

## SIP/VOIP 服务器

提供 VOIP 网络电话服务, 配合语音网关或运营商提供的 SIP 服务器, 还可拨打外线 (市话、长途、手机等)。

## 网络拓扑



## 运行条件

此模块是一个独立的子系统，需要运行在 KVM 的虚拟机中。

## 安装模块

应用-》模块-》检查更新，找到 “sipserver ” 模块，点击安装。

	<b>SIP/VOIP 服务</b> 提供VOIP 网络电话服务，配合语音网关或运营商提供的SIP服务器，还可拨打外线。 <a href="#">更多...</a>	1.0.28 2020-10-21 16:02:03	28.95 MB 52.70 MB
---	---	-------------------------------	----------------------

## 配置 SIP 服务端

## 1. 配置并开启 KVM 功能

详情见 [【KVM 虚拟化】](#) 部分

## 2. 克隆安装 sip 虚拟机

□ SIP/VOIP 服务

参数设置

1. 第一步克隆安装SIP虚拟机

⚠ 没有发现SIP虚拟机模块，点击一键安装

服务运行状态 已停止

SIP 服务器IP地址 192.168.2.125  
需和LAN1口在同一网段

保存设置 重启SIP服务器 登录SIP Web管理

等待克隆完成：

参数设置

服务运行状态 已停止

SIP 服务器IP地址 192.168.2.125  
需和LAN1口在同一网段

保存设置 重启SIP服务器 登录SIP Web管理

```
2020-07-02 16:46:43 拉取虚拟机 sip 配置...
2020-07-02 16:46:43 写入虚拟机配置...
2020-07-02 16:46:43 下载镜像包...
2020-07-02 16:46:43 镜像包大小 297.88 MB
2020-07-02 16:46:43 开始下载...
85.09% => 253.47 MB <平均下载速度: 10.14 MB/s, 估计剩余时间: 4秒>
```

## 3. 配置 SIP 服务器 IP

SIP/VOIP 服务 **第3步：启用服务**

参数设置

服务运行状态 **已停止**

SIP 服务器IP地址 **192.168.2.125**  
需和LAN1口在同一网段

**第2步：设置SIP服务器IP**

```
2020-07-02 16:46:43  抽取虚拟机 sip 配置...
2020-07-02 16:46:43  写入虚拟机配置...
2020-07-02 16:46:43  下载镜像包...
2020-07-02 16:46:43  镜像包大小 297.88 MB
2020-07-02 16:46:43  开始下载...
2020-07-02 16:47:12  克隆成功, 请关闭窗口, 启动虚拟机。
```

## 4. 启用 SIP 服务

系统将自动启动 sip 虚拟机，大约需要 1-2 分钟启动完成。

SIP/VOIP 服务

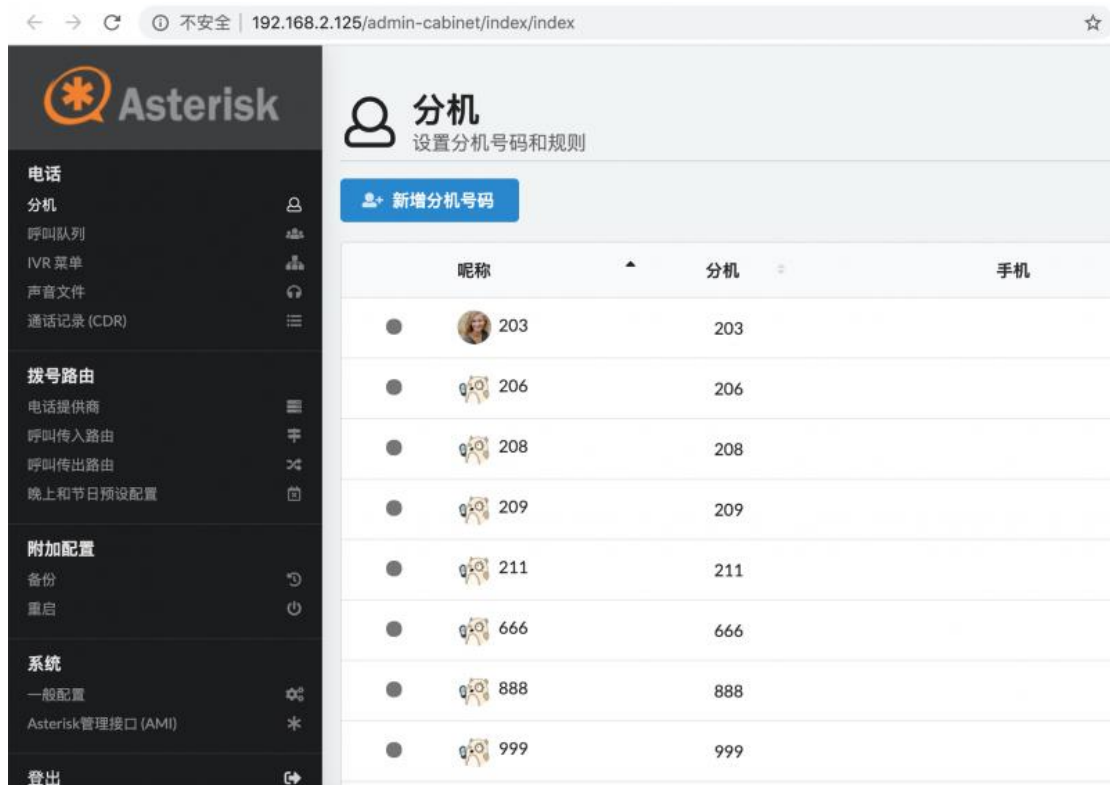
参数设置

服务运行状态 **运行中 <PID: 35923>**

SIP 服务器IP地址 **192.168.2.125**  
需和LAN1口在同一网段

```
[ 1.601710] esas2r: driver will not be loaded because no ATTO esas2r devices were found
Mounting sysdisk ...
Loading config ...
Starting PBX service ...
Boot Success
2020-07-02 16:53:16 SIP 系统启动完成
```

## 5. 一键登录 SIP 服务器的 web 管理



SIP 服务器 Web 登录账号/密码: admin/sip123456

## 新建 SIP 账号/分机

左侧菜单-》电话-》分机-》新增分机号码:



输入用户名、分机号、SIP 密码, 保存配置:

# 分机

设置分机号码和规则

状态更新

基本配置 呼叫路由配置

用户名  
101 这里是昵称，也可以是中文

分机  
101 分机号，通常为3-6位数字

手机

SIP密码  
101 密码 建立一个新密码

高级设置

+ 更改图像 删除

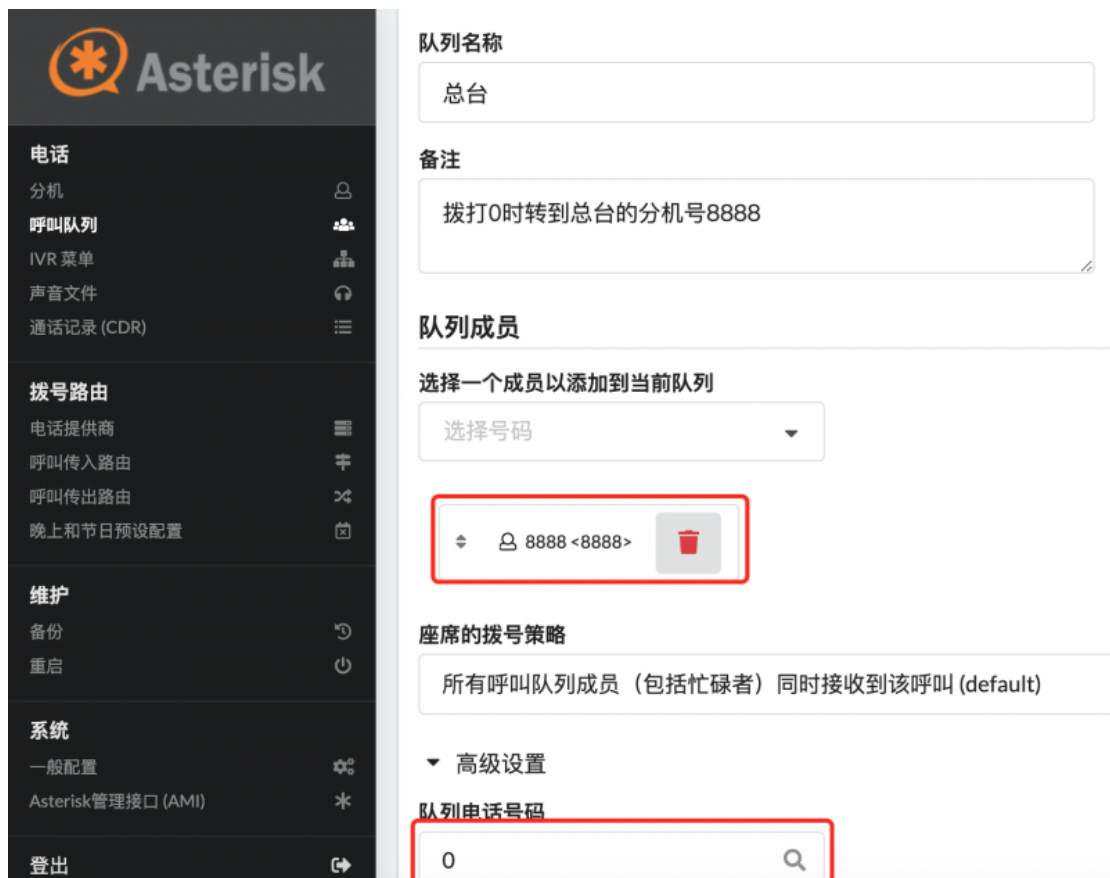
返回列表 保存配置

默认分机号码是 3 位数，如需修改（范围：3~6 位数），访问左侧菜单-》系统-》一般配置：





设置呼叫队列，拨打 0 时，转到总台分机号 8888:



## 终端 - HG510 融合终端

硬件配置：

- 光纤上行：EPON/GPON 上行、1 千兆 1 百兆 LAN 口、机顶盒一体（S905L 芯片）、1 个 RJ11 电话口、2.4G WIFI
- 网口上行：1WAN（千兆）+2LAN（百兆）、机顶盒一体（S905L 芯片）、1 个 RJ11 电话口、2.4G WIFI



电脑连接 WIFI（CMCC-free），无密码，访问 <http://192.168.1.1>

账号：CMCCAdmin， 密码：aDm8H%MdA

访问菜单：应用-》宽带电话设置：

### 1. 设置 SIP 服务器参数

智能融合网关 型号: HG510E

状态 网络 安全 应用 管理 诊断

DDNS配置 高级NAT配置 UPNP配置 宽带电话设置 IGMP/MLD设置

语音协议: Soft Switch SIP

主用SIP服务器

代理服务器地址: 192.168.2.125

代理服务器端口号: 5060

注册服务器地址: 192.168.2.125

注册服务器端口号: 5060

出局代理启用:

出局代理服务器地址: 192.168.2.125

出局代理服务器端口号: 5060

端口都是 5060

SIP服务器IP

## 2. 设置 SIP 账号/密码:

线路1 账号

启用

用户号码: 666

用户账号: 666

用户密码: ...

sip账号/分机号

sip密码

保存/应用

### 3. 查看注册状态



智能融合网关 型号: HG510E

状态 网络 安全 应用 管理 诊断 帮助

设备信息 网络侧信息 用户侧信息 **宽带语音信息** 远程管理状态

**宽带语音信息**

注册状态	Up
电话号码	666

Up 表示已注册成功

## 终端 - MSG1200-FE 企业网关

硬件配置:

- 5 百兆网口 (1WAN + 4LAN) , 1 个 RJ11 口电话, 2.4GWIFI

电脑连接 WIFI (见企业网关正面左上角, WIFI 名称如 MSG-1200—XXYYZZ) , 然后访问 <http://192.168.2.1>

账号: user, 密码: admin

将地址栏中的 URL 改为

[http://192.168.2.1/voip/SIP\\_Account1.asp](http://192.168.2.1/voip/SIP_Account1.asp)

设置如下：



## 确认注册状态

将普通话机连接设备的 PHONE 口，摘机：

- 如果听到拨号音（长嘟），表示注册成功
- 如果听到“注册失败”，表示异常，检查 SIP 参数配置是否正确，网络是否通

## 语音网关对接

目前支持的语音网关型号：上海迅时 HX4G 系列

请联系技术客服进行调试对接。

# Docker 应用 - KMS 激活服务

用途：搭建自己的 Windows/Office 激活服务器

**注：本镜像来源于网络，本方法仅供学习研究使用，请勿用于商业用途。**

## 1. 安装 KMS 容器

方法一：容器列表-》专家模式，复制粘贴以下配置：

```
[kms]

active = yes

command = /usr/bin/vlmcsd -D -e

desc = KMS

hostname = kms

image = teddysun/kms

name = kms
```

```
onboot = yes
```

```
overwrite_entrypoint = no
```

```
portmap = 1688
```

等待系统通过网络下载镜像，并创建容器，大约 20 秒左右。

方法二：点击按钮“从网络克隆”，端容器名称输入 kms，其他为空即可。



云端容器名称:

目标容器名称:

目标容器备注:

克隆到本地

```
2020-08-07 23:25:07 拉取容器 kms 配置...
2020-08-07 23:25:07 写入容器配置...
2020-08-07 23:25:07 下载镜像包...
2020-08-07 23:25:07 镜像包大小 2.63 MB
2020-08-07 23:25:07 开始下载...
2020-08-07 23:25:08 下载完成, 准备导入...
2020-08-07 23:25:08 导入镜像...
2020-08-07 23:25:09 克隆成功, 请关闭窗口, 启动容器。
```

然后启动容器即可。

[参数设置](#)[容器列表](#)[镜像管理](#)

共1条记录/1页, 每页显示 200 ▾

请输入关键字

搜索 🔍

清除 ✕

自动刷新 ↻

新建容器

&lt;1个容器运行中&gt;

ID	名称 备注	存储	网络	端口映射状态	运行状态	状态	编辑	选择
*1	kms KMS		自动分配	0.0.0.0:1688->1688/tcp	运行中 (2 小时) [停止]   [重启]	🟢	✎	<input type="checkbox"/>

## 2. Windows 激活

激活前提是 windows 是 VOL (团体批量许可证, 也叫 VL) 版本, 网上下载的基本都是 VOL 版本。

已测试可支持 Win7/Win8/Win10 系统的激活。

Windows 激活指令 (需要以管理员权限运行命令提示符)

```
## 设置 KMS 服务器地址
```

```
slmgr /skms <路由器 IP 地址或域名>
```

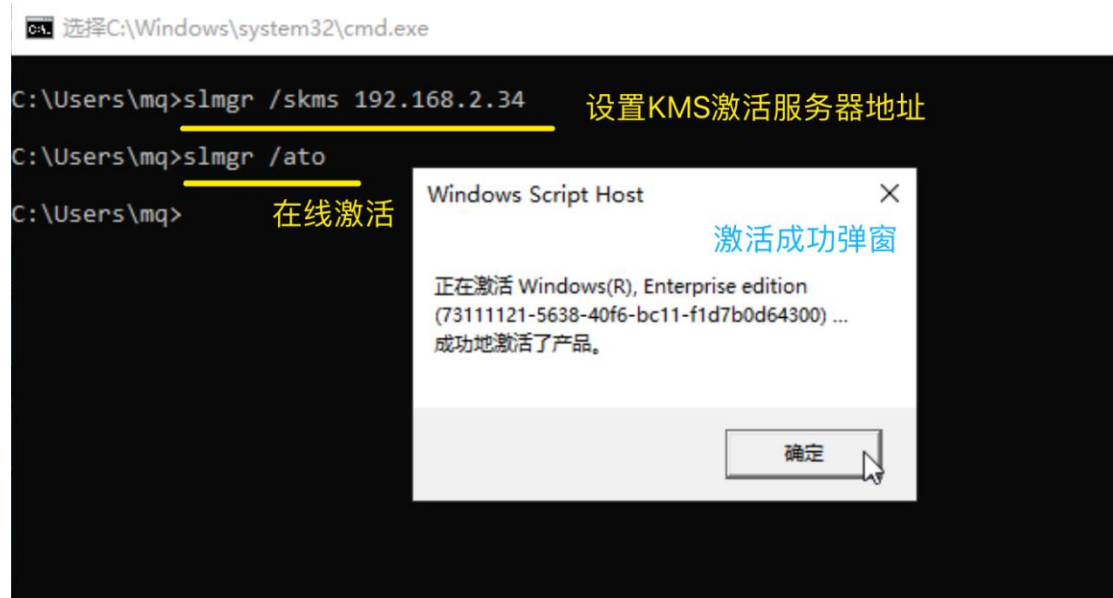
```
### 在线激活
```

```
slmgr /ato
```



### 查看激活信息

slmgr /dlv



### 3. Office 激活

首先你的 OFFICE 必须是 VOL (也叫 VL) 版本, 否则无法激活。找到你的 office 安装目录, 比如

```
## 32 位系统
```

```
C:\Program Files (x86)\Microsoft Office\Office16
```

```
## 64 位系统
```

```
C:\Program Files\Microsoft Office\Office16
```

**Office16 表示 office2016, Office15 是 2013, Office14 是 2010。**

Office 激活指令 (需要以管理员权限运行命令提示符) :

```
## 切换到 Office 目录
```

```
cd C:\Program Files\Microsoft Office\Office16
```

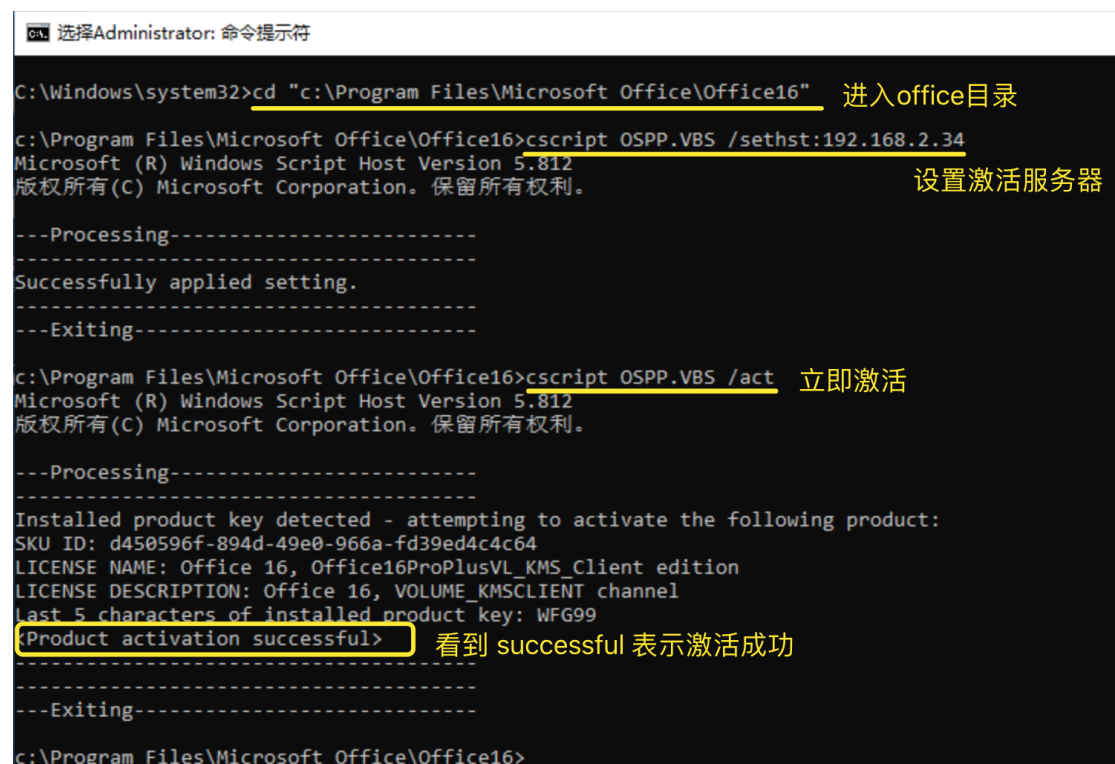
```
## 设置 KMS 激活服务器地址
```

```
cscript ospp.vbs /sethst:192.168.2.34
```

## 立即激活

```
cscript ospp.vbs /act
```

如果提示看到 successful 的字样，那么就是激活成功了，重新打开 office 即可。



```
选择Administrator: 命令提示符
C:\Windows\system32>cd "c:\Program Files\Microsoft Office\Office16" 进入office目录
c:\Program Files\Microsoft Office\Office16>cscript OSPP.VBS /sethst:192.168.2.34
Microsoft (R) Windows Script Host Version 5.812
版权所有(C) Microsoft Corporation。保留所有权利。 设置激活服务器

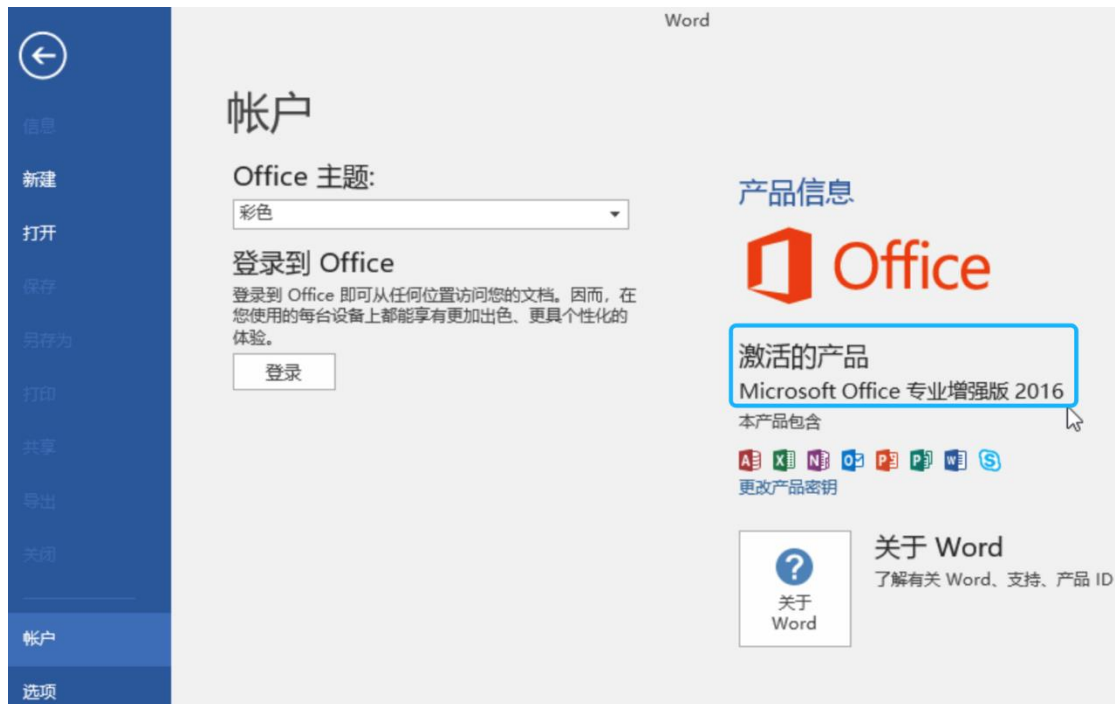
---Processing-----
Successfully applied setting.
---Exiting-----

c:\Program Files\Microsoft Office\Office16>cscript OSPP.VBS /act 立即激活
Microsoft (R) Windows Script Host Version 5.812
版权所有(C) Microsoft Corporation。保留所有权利。

---Processing-----
Installed product key detected - attempting to activate the following product:
SKU ID: d450596f-894d-49e0-966a-fd39ed4c4c64
LICENSE NAME: Office 16, Office16ProPlusVL_KMS_Client edition
LICENSE DESCRIPTION: Office 16, VOLUME_KMSCLIENT channel
last 5 characters of installed product key: WFG99
Product activation successful> 看到 successful 表示激活成功
---Exiting-----
c:\Program Files\Microsoft Office\Office16>
```

**确认已激活：**

运行 word-》打开其他文档-》账户，即可看到激活信息：



## 常见问题

1. 激活 Office 错误: “No Office KMS licenses were found on the system.”

原因: 系统里安装的 Office 版本是 Retail 版, 也就是零售版

解决办法: 卸载当前的 Office Retail 版, 重新下载安装 VOL 版

## Docker 应用 - Socks5 代理/网络加速

用途: 搭建 Socks5 代理服务器, 用于网络加速 (比如 GIT 克隆源码仓库等)。

克隆容器

点击按钮“从网络克隆”，云端容器名称输入 socks5s，其他为空即可。

云端容器名称: 克隆云端Docker镜像

socks5s

目标容器名称:

名称

目标容器备注:

备注

[克隆到本地](#)

```
2020-08-07 23:15:18 拉取容器 socks5s 配置...
2020-08-07 23:15:18 写入容器配置...
2020-08-07 23:15:18 下载镜像包...
2020-08-07 23:15:18 镜像包大小 53.58 MB
2020-08-07 23:15:18 开始下载...
2020-08-07 23:15:29 下载完成, 准备导入...
2020-08-07 23:15:31 导入镜像...
2020-08-07 23:15:35 克隆成功, 请关闭窗口, 启动容器。
```

克隆完成后，启动容器即可：

参数设置 容器列表 镜像管理

共2条记录/1页, 每页显示 200 请输入关键字 [搜索 Q](#) [清除 x](#) [禁用刷新](#) [新建容器](#) [从网络克隆](#) <2个容器运行中>

ID	名称 备注	存储	网络	端口映射状态	运行状态	状态
*1	kms KMS Server		自动分配	0.0.0.0:1688->1688/tcp	运行中 (2 小时) [停止]   [重启]	☑
2	socks5s Socks5 Proxy Server		自动分配	0.0.0.0:1080->1080/tcp	运行中 (1 秒) [停止]   [重启]	☑

Socks5 代理端口：1080。

若需要修改代理端口（如改为 10080），编辑容器，将端口映射规则改为如 10080:1080，然后点击“重建”按钮重建容器。

## 客户端配置

路由器 (Socks5 服务器) IP 为 11.22.33.44，端口为 1080

### 1. GIT 使用 Socks5 代理

```
git config --global http.proxy 'socks5://11.22.33.44:1080'
```

```
git config --global https.proxy 'socks5://11.22.33.44:1080'
```

## 2. WGET 使用 Socks5 代理

对于 Linux 系统, 可使用 tsocks 实现, Debian/Ubuntu 下可以使用如下命令安装 tsocks

```
apt-get install tsocks
```

然后修改 /etc/tsocks.conf 配置文件:

```
## 把代理服务器 IP 加到本地网络列表中, 直连访问

## 否则会出现错误提示: SOCKS server X.X.X.X is not on a local subnet!

local = 11.22.33.44/255.255.255.255

## socks5 服务器 IP

server = 11.22.33.44

## socks 代理类型, 5 表示 socks5

server_type = 5

## socks5 服务器端口

server_port = 1080
```

然后 wget 套上 tsocks 运行, 就可以访问代理了。

```
tsocks wget https://www.google.com/
```

### 用户名密码验证

默认 Socks5 代理服务是无需验证的，如果需要用户名/密码验证，编辑容器，将“启动命令”修改如下：

```
## 默认的启动命令

-e SS_USER= -e SS_PASS=

## 修改后的启动命令 (用户名 test, 密码 123456)

-e SS_USER=test -e SS_PASS=123456
```

修改完成后，点击“重建”按钮重建容器即可。

## Rsync 远程备份

Rsync 是一个远程数据同步工具，可通过网络快速同步多台主机之间的文件。

本文将介绍在 Windows 下用 DeltaCopy 工具将本地的文件同步到路由上，及将路由上的文件同步到本地电脑。

依赖条件：需要额外的存储空间，请参考 [磁盘管理](#)

---

# 服务端配置

## 1. 安装模块，开启服务

进入菜单：应用-》模块管理-》检查更新，安装 rsync 模块

完成后，进入菜单：应用 -》 Rsync 远程备份

开启服务，并设置允许访问服务的地址段：

参数设置 资源管理

服务运行状态 运行中 <PID: 28660>

监听端口 873

传输带宽限制 0 KBps

允许访问的IP或网段

192.168.0.0/24  
192.168.1.100-254  
192.168.3.123  
192.168.4.0/255.255.254.0

为空表示所有IP都可以访问 Rsync 服务

保存设置

## 2. 新增备份

在资源管理-》新增备份结点：



名称  备份模块名，英文/数字组成

授权用户名

授权访问密码

磁盘分区位置

路径  目录名，建议也用英文/数字

访问模式  只读  读写

[显示更多选项 >>](#)

Rsync 远程备份服务

参数设置 资源管理

共1条记录/1页, 每页显示 10 请输入关键字

ID	名称	磁盘分区位置	路径	授权用户名	允许访问的IP或网段	备注
1	movie	/disk/data	movie	mq	所有	

## Windows 客户端配置

下载并运行 DeltaCopy, 这里用的是在 v1.4 基础上的修改包, 支持中文文件名 (不会出现乱码) 和深路径。

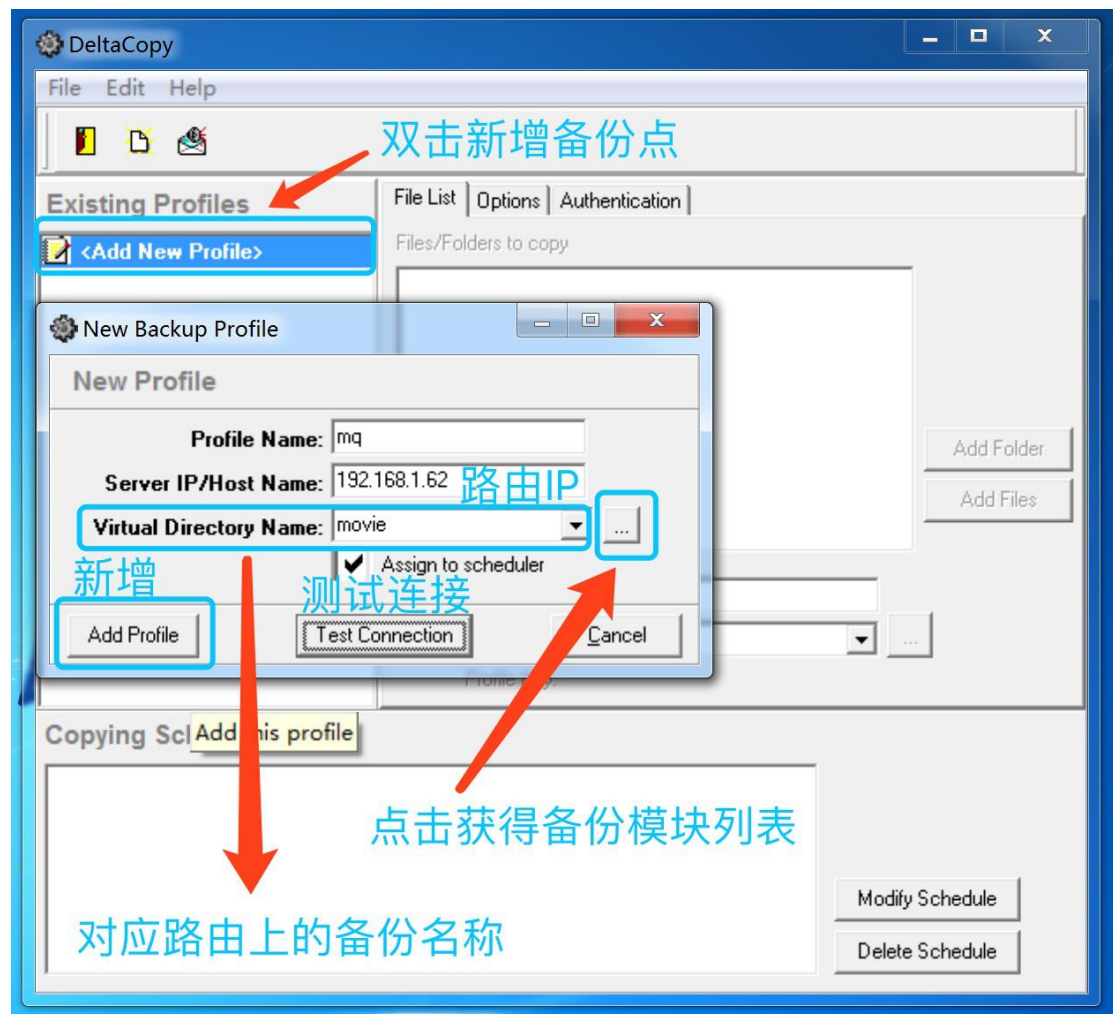
[DeltaCopyRaw.v1.4 nzt repack 20130218.rar](#)

size: 4.50MB

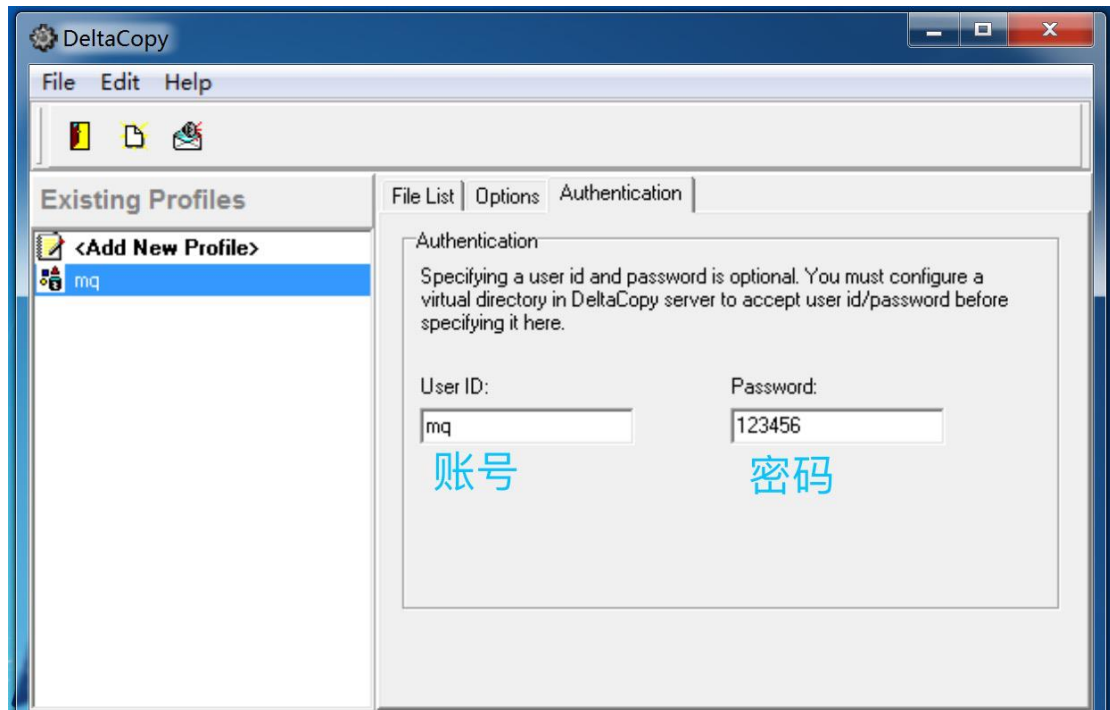
MD5: 120a368d1cc354c674b74172562340f6

DeltaCopyRaw.v1.4\_nzt\_repack\_20130218.rar

## 1. 新增 Profile:

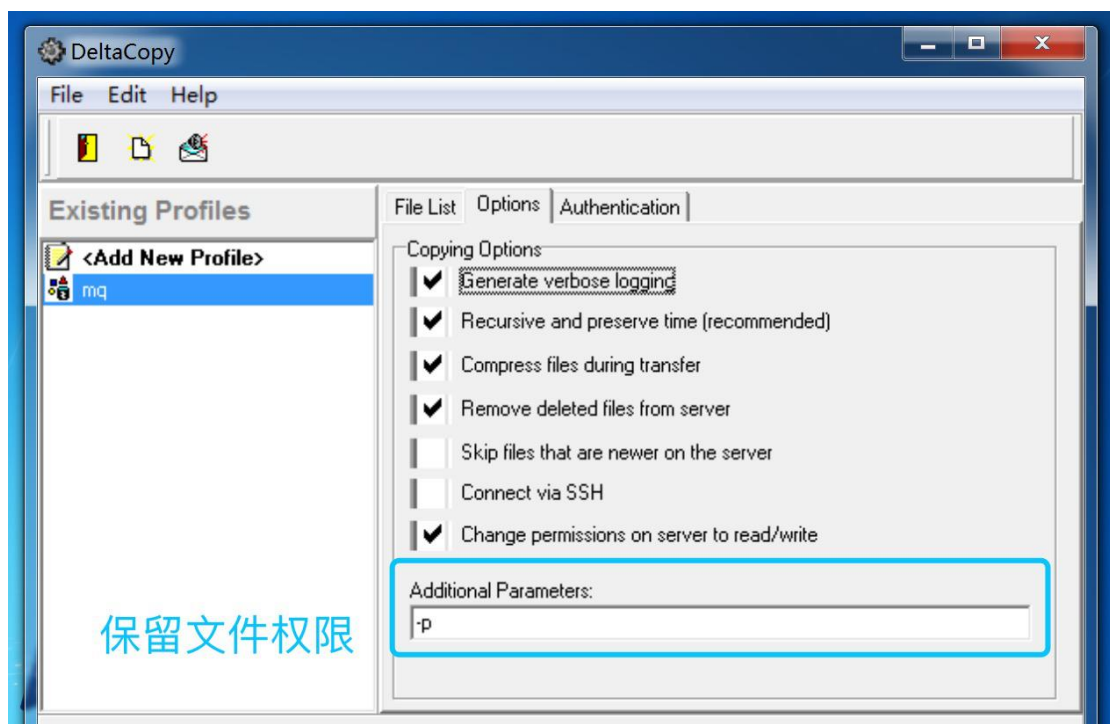


## 2. 设置账号和密码:

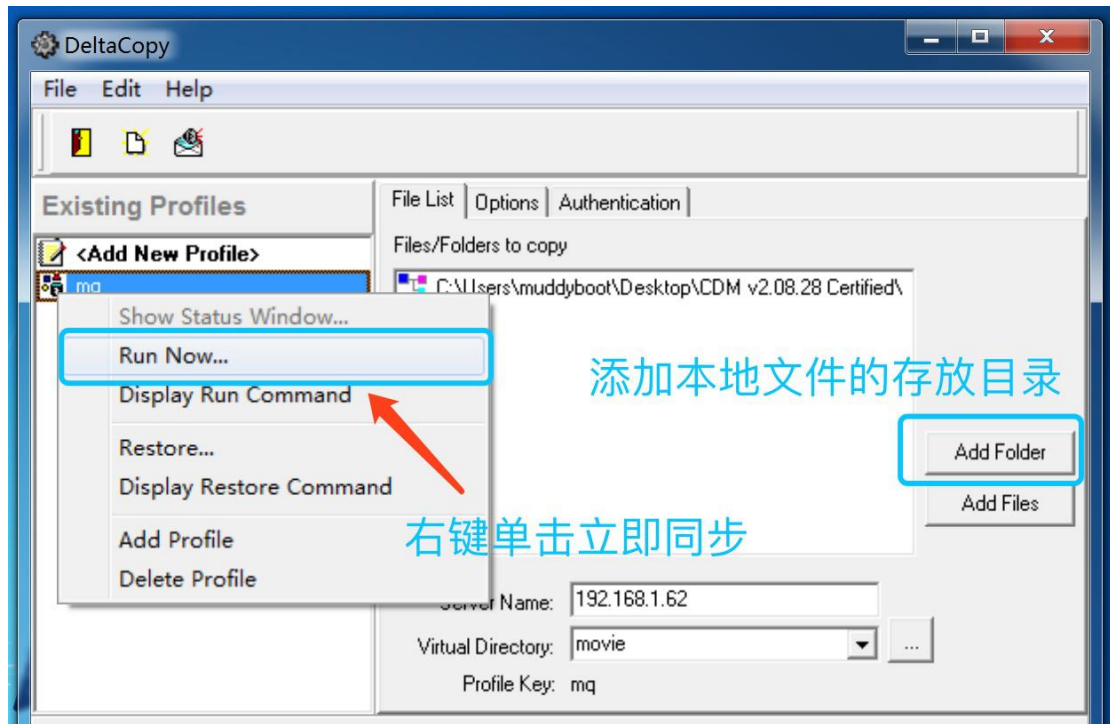


### 3. 设置同步参数:

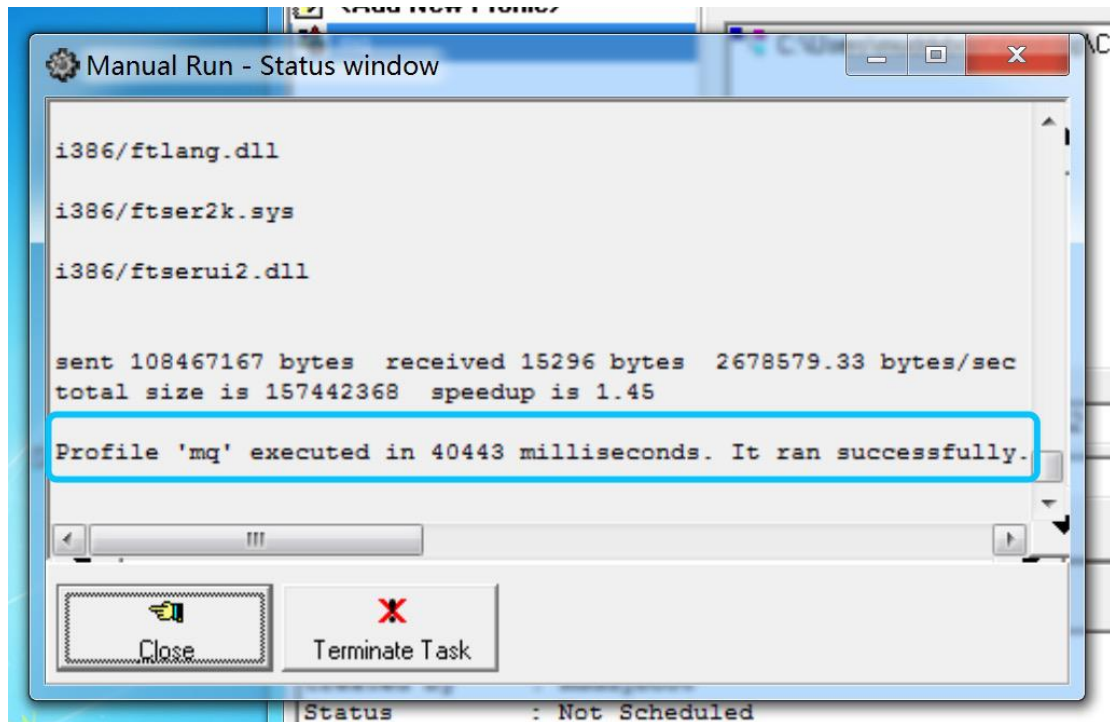
-p 表示保留文件和目录权限，这里必须加，否则同步到路由上到目录将无法访问



#### 4. 添加本地文件目录（这些文件和目录将被上传到路由上）：



#### 5. 运行同步，同步完成后如下：



最后，在路由上查看刚刚客户端上传同步的文件

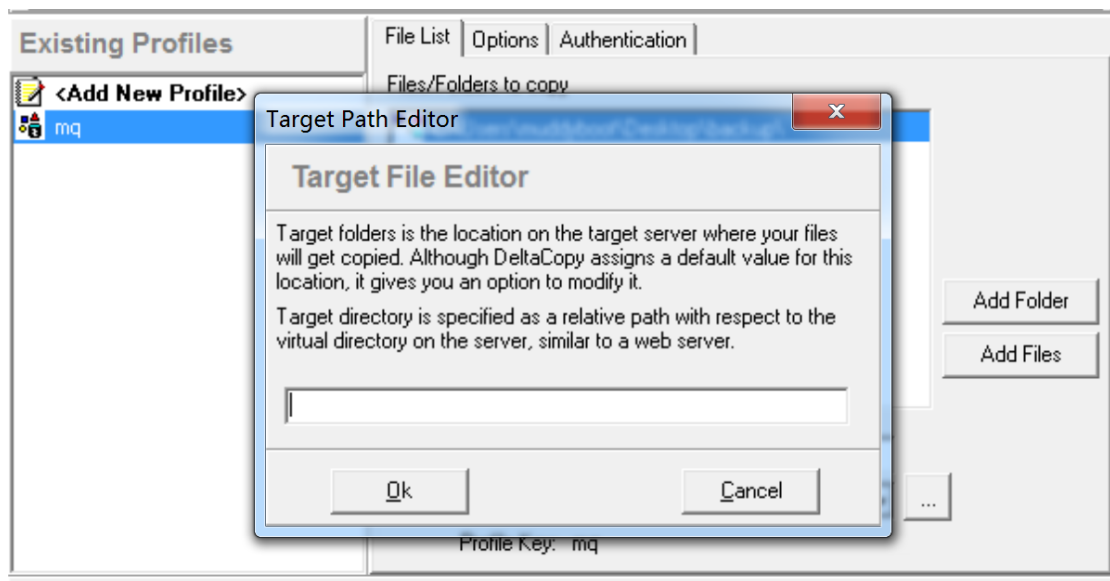
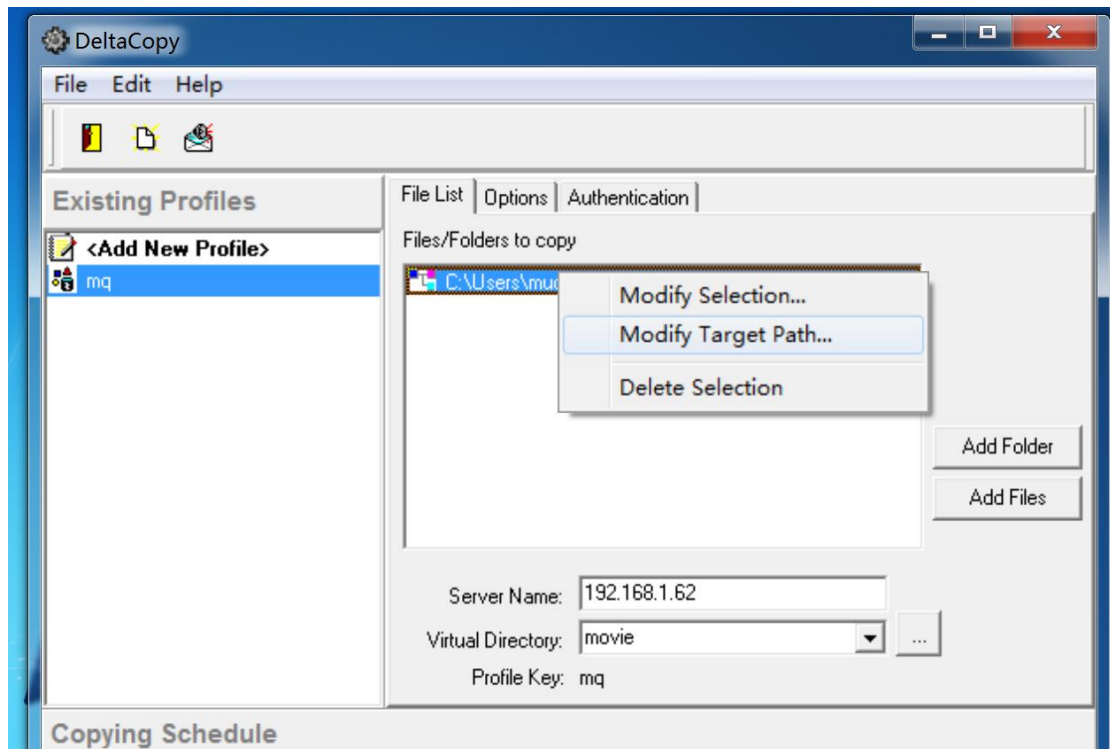
ID	名称	大小	创建时间
1	ftbusui.dll	103.35 KB	2013-01-18 15:54:10
2	ftcserco.dll	67.85 KB	2013-01-22 14:25:48
3	ftd2xx.dll	214.35 KB	2013-01-18 15:54:14
4	ftd2xx.lib	19.94 KB	2013-01-18 15:54:12
5	ftdibus.sys	61.98 KB	2013-01-22 14:25:54
6	ftlang.dll	196.85 KB	2013-01-18 15:54:06
7	ftser2k.sys	71.85 KB	2013-01-22 14:25:44
8	ftserui2.dll	52.35 KB	2013-01-22 14:25:40

## 将路由上的文件同步到本地电脑

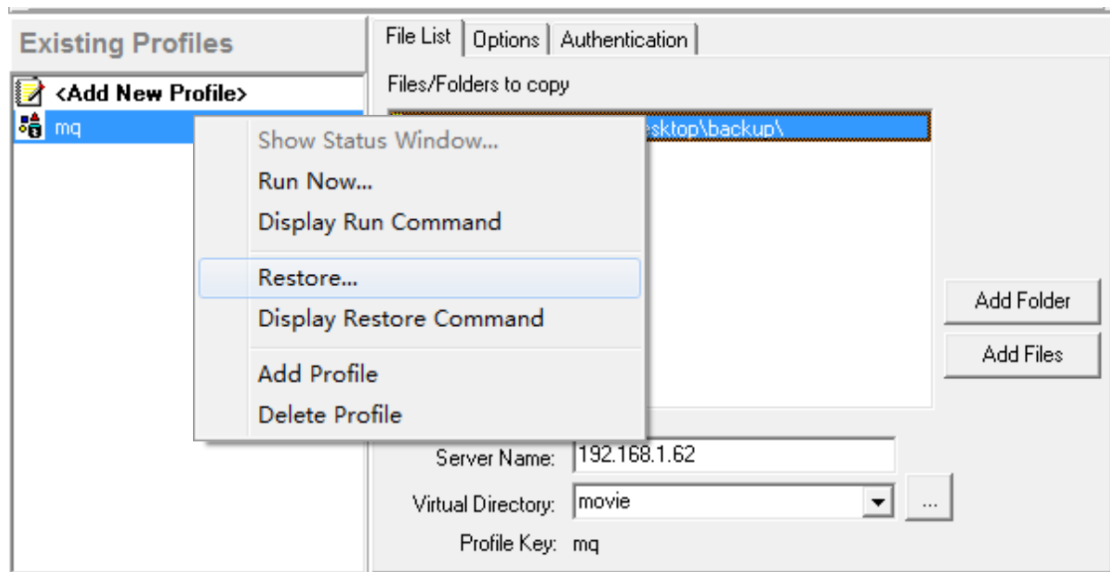
这里强烈建议将路由上的备份结点里的“访问模式”设为只读，以免误操作，导致路由上的文件被删除。

先在本地创建一个空目录，比如 backup，右键单击修改目标路径

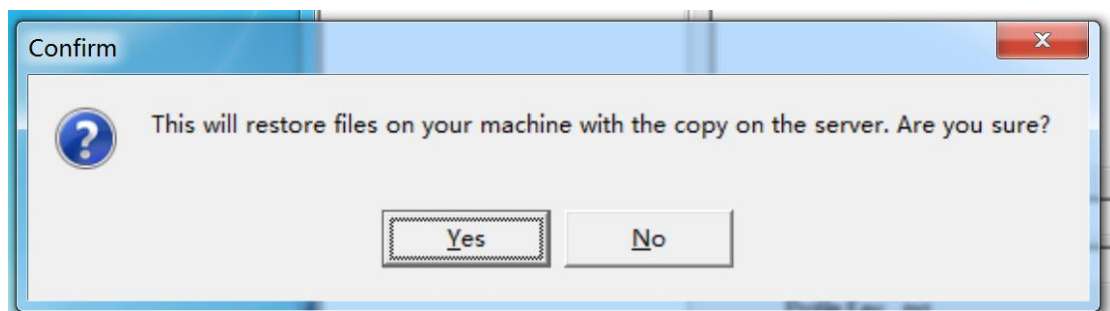
(Target Path) 为空，意为这个目录对应服务器上备份结点的根目录。



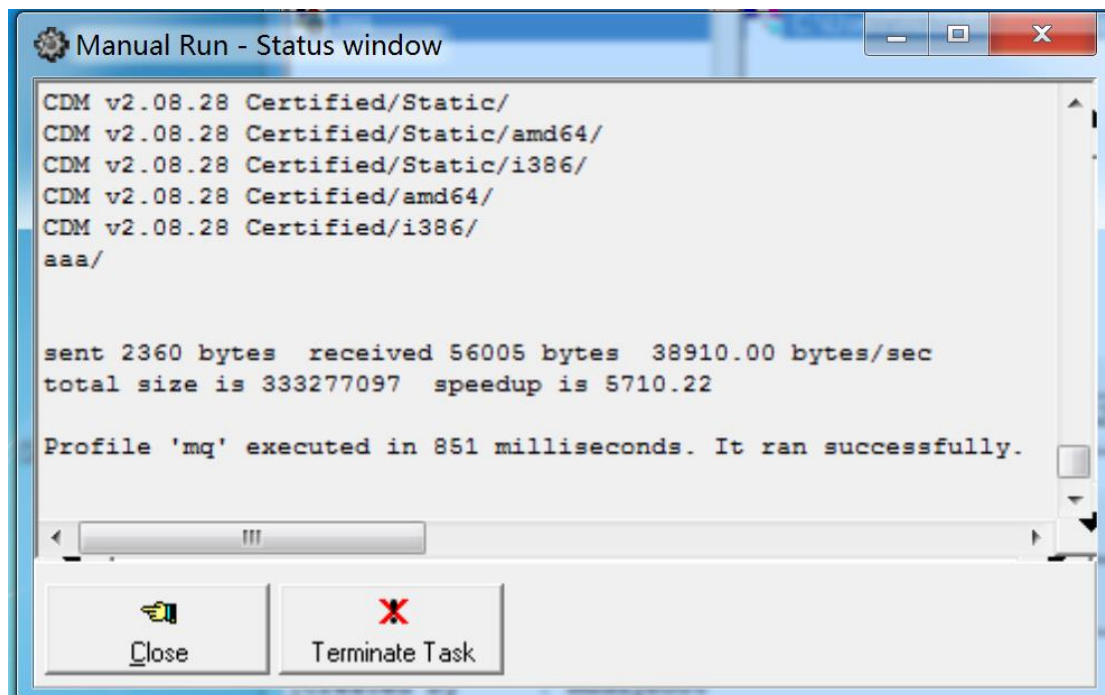
然后右键单击 Profile，点击恢复（Restore...），注意别点成了“Run Now”（将本地文件同步到路由）



弹出警告确认，点 Yes



最后文件从路由上拉取到本地，同步完成。



## 常见问题 FAQ

---

1. 本地文件名包含中文的文件或目录同步到路由上后，在路由上显示乱码

原因：官方版本的 DeltaCopy 不支持中文，请使用修改版，文中有下载链接

2. 上传到路由的文件无法显示大小，目录访问提示用户名验证

原因：客户端同步参数没有加 -p，导致同步到路由上到文件权限有问题



# 网上邻居文件共享服务

文件服务器可用于局域网文件统一存放，用于内部的文件共享和交流，并且可以通过网上邻居方便地访问。

依赖条件：需要额外的存储空间，请参考 [磁盘管理](#)

---

## 安装模块

应用-》模块-》检查更新，找到 “fileserver ” 模块，点击安装。

	网上邻居文件共享 使用SMB协议，为局域网内用户提供文件存储服务。 <a href="#">查看更多...</a>	1.3.5 2020-10-21 17:27:21	2.76 MB 14.52 MB		<input type="checkbox"/>
---	--	------------------------------	---------------------	---	--------------------------

## 服务端配置

### 1. 基本参数配置

文件存储共享服务

开启功能

参数设置
共享管理
连接信息

服务运行状态

共享根目录

网上邻居标识 (NetBIOS名字)

文件管理员帐号

运行中 <PID: 6264>
选择默认文件存储位置

本地磁盘 /dev/nvme0n1p1 -- /disk/data (共 458.3G, 剩余 397.9G) ▾

我的文件服务器

fileadmin

默认密码为123456, 点击图标可修改

可选, 通过http方式访问共享

启用 HTTP 映射

HTTP 映射端口

是

1234

显示更多选项 >

绑定网络接口  否

## 2. 添加共享

参数设置
共享管理
连接信息

共1条记录/1页, 每页显示 200 ▾

请输入关键字

搜索 🔍

清除 ✕

新增共享

ID	名称 ↕	磁盘分区位置 ↕	路径 ↕	访问权限 ↕	备注 ↕	状态 ↕	编辑	选择
1	tmp	/disk/data	tmp	<div style="display: flex; gap: 5px; font-size: small;"> <span style="border: 1px solid #00aaff; padding: 1px 5px; border-radius: 3px;">HTTP 映射</span> <span style="border: 1px solid #00aaff; padding: 1px 5px; border-radius: 3px;">可写</span> <span style="border: 1px solid #00aaff; padding: 1px 5px; border-radius: 3px;">公开</span> </div>		<input checked="" type="checkbox"/>	<input type="text"/>	<input type="checkbox"/>

专家模式

导出规则

全选 / 全不选

名称 tmp 共享名，建议用英文、数字组成

磁盘分区位置 本地磁盘 /dev/nvme0n1p1 -- /disk/data (共 458.3G, ▾)

路径 tmp 为空表示磁盘分区的根目录

共享权限设置

根据需要设置访问权限

- 游客可访问 (无需登录验证)
- 允许修改和写入
- 启用 HTTP 映射

全选 / 全不选

HTTP 映射名称 tmp

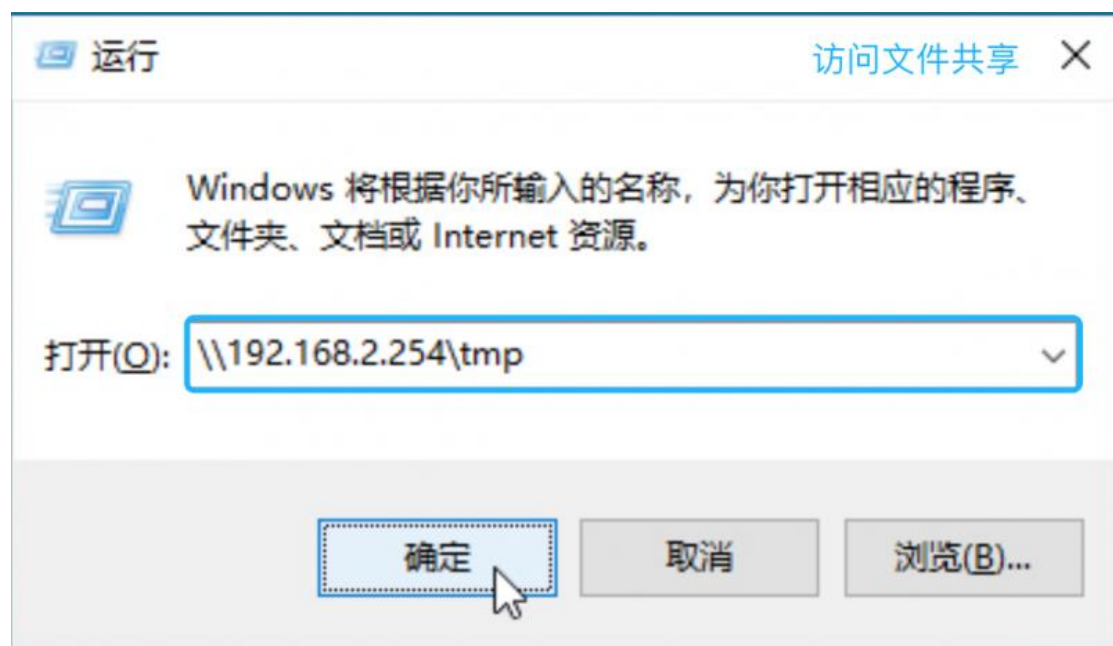
备注 启用HTTP映射后可以通过 <http://<ip>:端口/<映射名>> 访问共享

激活  是

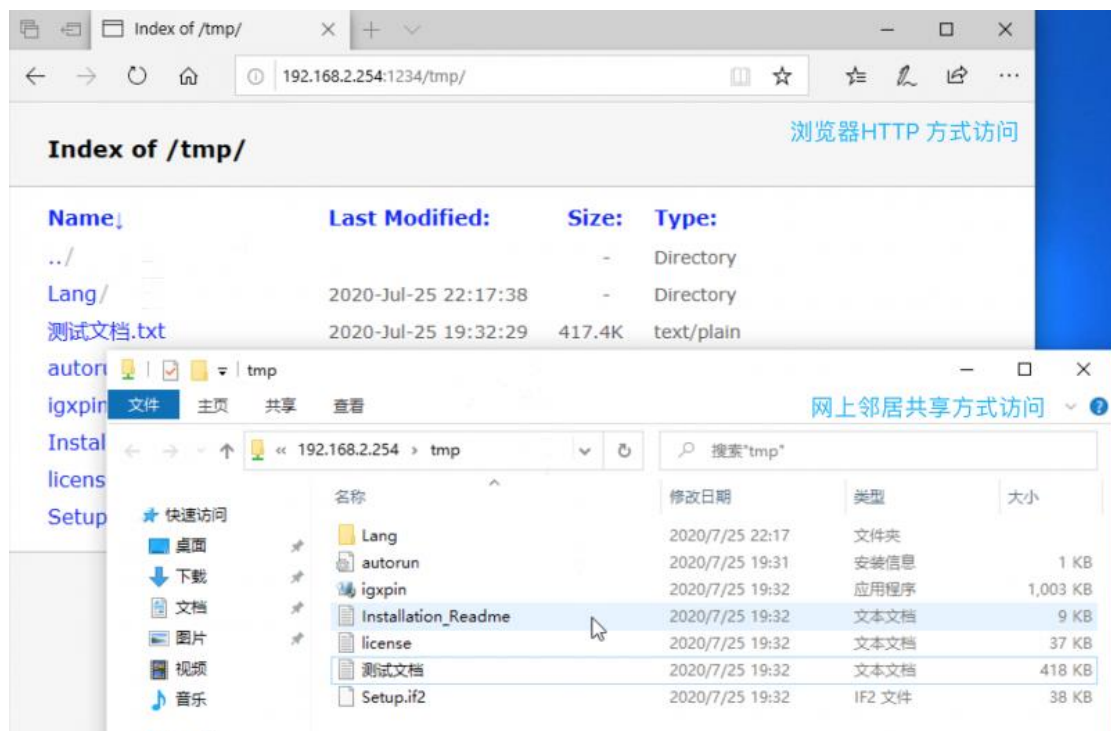
## Windows 客户端访问

开始菜单-》运行 (Win+R 快捷键)，输入如下格式地址：

\\<路由器 IP>\<共享名>



如果开启了 HTTP 映射，在上传文件后，可以通过浏览访问：



## macOS 客户端访问

访达-》前往-》连接服务器(Command+K 快捷键)，输入如下格式地址：

```
smb://<路由器 IP>/<共享名>
```



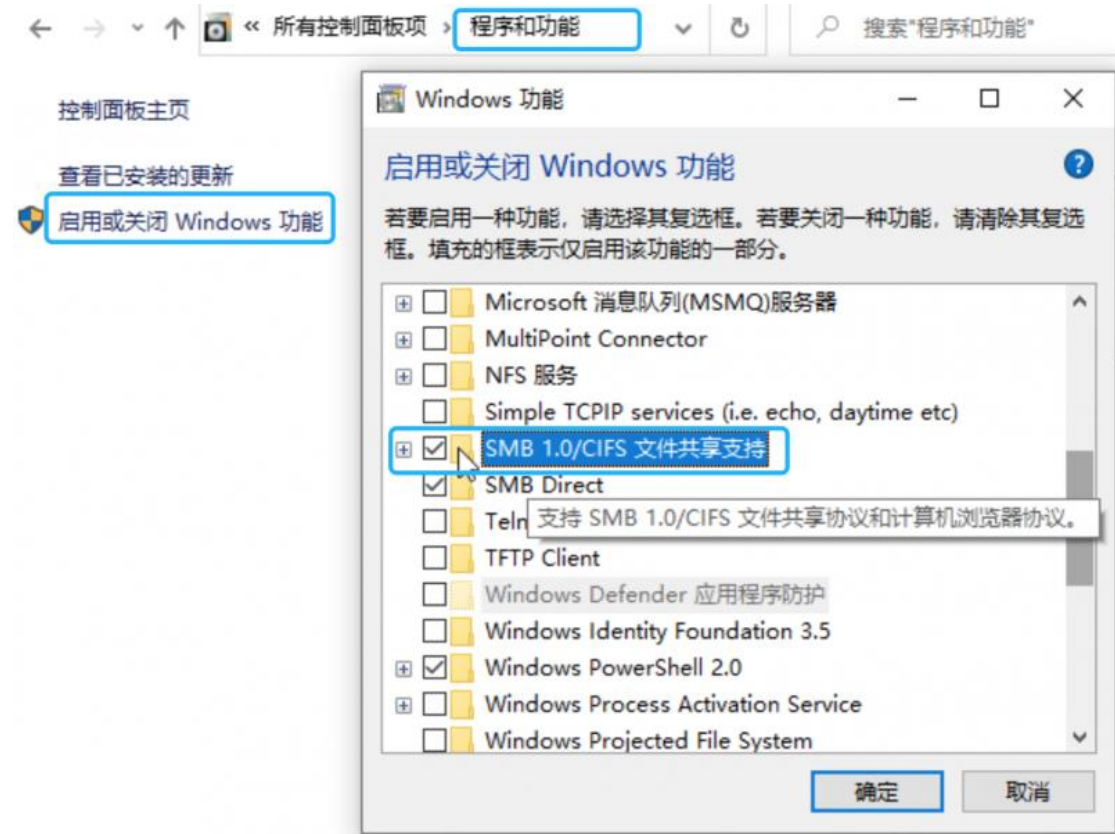
## 常见问题 FAQ

### 1. Windows 10 访问提示 “共享不安全，不能连接” 错误



#### 解决办法：

控制面板-》程序和功能-》启用和关闭 Windows 功能，勾选 “SMB 1.0/CIFS 文件共享支持”



设置完成后，需 **重启电脑** 后生效。

## NFS 网络存储服务

通过 NetHDD 将本地物理磁盘作为网络磁盘，以标准 NFS 协议对外提供存储服务（支持 NFS v3/v4 协议）。

依赖条件：需要额外的存储空间，请参考 [磁盘管理](#)

## 安装模块

应用-》模块-》检查更新，找到 “nethdd ” 模块，点击安装。

	<b>NetHDD 网络存储</b> 将本地物理磁盘作为网络磁盘，以标准NFS协议对外提供存储服务（支持NFS v3/v4协议）。 <a href="#">更多...</a>	1.1.90 2020-10-21 15:59:07	883.98 KB 3.12 MB	
---	--	-------------------------------	----------------------	---

## 服务端设置

进入 “系统” -》 “磁盘存储” ， 设置好并成功挂载磁盘。

进入 “应用” -》 “网络存储” ， 开启服务， 设置可访问服务器的 IP 或 IP 段， 如下图：



The screenshot shows the NetHDD service configuration interface. At the top, there is a toggle switch for "网络存储 (NetHDD) 服务" (Network Storage (NetHDD) Service) which is checked. A red arrow points to this switch with the text "开启功能" (Enable function). Below this, there are two tabs: "参数设置" (Parameter Settings) and "资源管理" (Resource Management). The "参数设置" tab is active. Under "服务运行状态" (Service Running Status), it shows "运行中 <PID: 6244>" (Running <PID: 6244>). Below that, under "允许访问本服务的IP或网段列表" (List of IP addresses or network segments allowed to access this service), there is a text input field containing "192.168.2.0/24". At the bottom right, there is a "保存设置" (Save Settings) button.

在资源管理标签-》新增存储节点：

允许连接的IP/地址段 \* \* 表示所有IP均可连接

权限

磁盘分区位置

目录  / 表示整个磁盘分区

备注

激活

参数设置

资源管理

共1条记录/1页, 每页显示

请输入关键字

搜索

清除

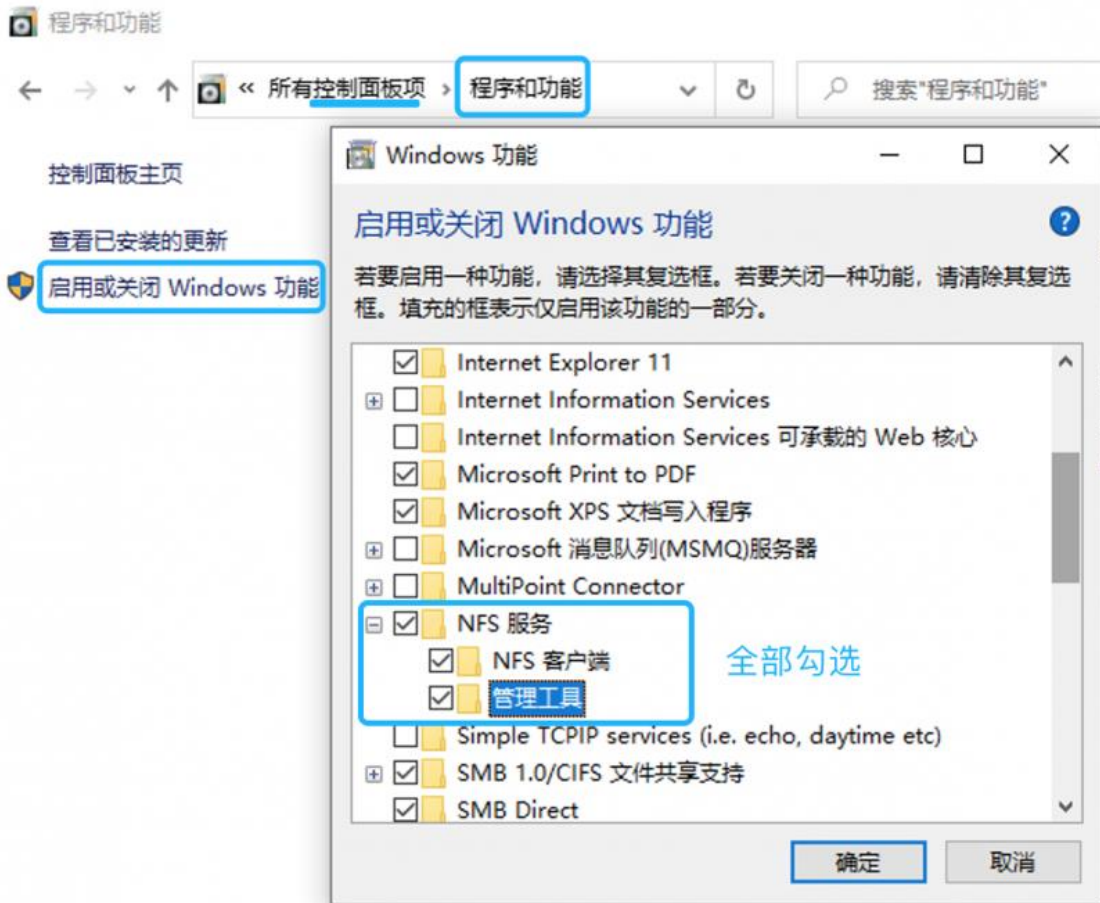
新增存储节点

ID	允许连接IP	访问路径	备注	状态	编辑	选择
1	*	/disk/data/		<input checked="" type="checkbox"/>	<input type="button" value="编辑"/>	<input type="checkbox"/>

## Windows 客户端连接

以 Windows 10 为例, 进入控制面板-》程序和功能-》打开或关闭 Windows 功能, 勾选 “NFS 服务下的所有选项”:





此外，建议启用 UTF-8 支持（避免 NFS 共享中文件目录名出现乱码）：



以上设置后需重启电脑生效。

**接下来的操作在命令提示符窗口完成。**

查看远程电脑 NFS 共享的目录:

```
showmount -e NFS 服务器 IP
```

```
showmount -e 192.168.2.254
```

挂载远程文件系统到本地盘符

```
mount \\NFS 服务器 IP\共享目录路径 本地盘符
```

```
mount \\192.168.2.254\disk\data Z:\
```

```
C:\Users\mq>mount \\192.168.2.254\disk\data Z:\ 挂载NFS磁盘到 Z: 盘
Z: is now successfully connected to \\192.168.2.254\disk\data

The command completed successfully.

C:\Users\mq>showmount -e 192.168.2.254 查看NFS服务器上的共享目录
Exports list on 192.168.2.254:
/disk/data *

C:\Users\mq>umount Z: 卸载NFS磁盘

Disconnecting Z: \\192.168.2.254\disk\data
The command completed successfully.
```

## NFS 文件读写性能测试

---

读取/下载文件测试:

已完成 94%

正在将 1 个项目从 iso 复制到 桌面

已完成 94%

速度: 106 MB/秒

名称: cn\_windows\_10\_business\_2020\_x64\_dvd\_b3e1f3a6.iso  
剩余时间: 大约 5 秒  
剩余项目: 1 (257 MB)

NFS服务器-》本地电脑

简略信息

写入/上传文件测试:

正在将 1 个项目从 桌面 复制到 upload

已完成 95%

速度: 90.6 MB/秒

名称: cn\_windows\_10\_business\_2020\_x64\_dvd\_b3e1f3a6.iso  
剩余时间: 大约 5 秒  
剩余项目: 1 (219 MB)

本地=》NFS服务器

简略信息

读取和写入速度平均值基本都在 90MB/s ~ 100MB/s。

# 路由上挂载网络磁盘

首页-》功能搜索框，输入 nas ， 点击下方菜单进入：



网络磁盘-》新的 NFS 网络磁盘：

NAS/NFS 服务器IP	192.168.201.33
远端磁盘目录	/disk/data
挂载点	nas <span>自定义，建议字母及数字组成</span>
<input type="button" value="挂载"/>	

连接成功后如下：

找到网络磁盘

网络磁盘 netdisk://192.168.201.33:/disk/data	
服务器IP:	192.168.201.33
远程存储目录:	/disk/data
连接状态:	正常 <已挂载>
连接成功时间:	2020-07-27 11:43:22 <9分54秒>
挂载状态:	<p>传输协议: NFS V3</p> <p>总空间大小: <b>458.3G</b></p> <p>已用/剩余空间: 55.0G / 380.0G</p> <p>使用率:  13%</p> <p>挂载点: /disk/nas <a href="#">卸载</a></p>

## 网络磁盘性能测试

2020-07-27 11:43:38 开始磁盘 /disk/nas 性能测试  
共8项, 每项测试时间: 30 秒, 临时文件大小: 2G

2020-07-27 11:48:54 测试完成, 总耗时 5分16秒

测试结果:

	读 (MB/s   IOPS)		写 (MB/s   IOPS)	
Seq 顺序	<b>89.3MiB/s</b>	85	<b>110MiB/s</b>	106
512K 随机	88.7MiB/s	173	110MiB/s	216
4K 随机	73.8MiB/s	18.9k	9535KiB/s	2379
4K-QD32 随机	58.7MiB/s	15.2k	9111KiB/s	2276

# 建 WWW 网站服务器 -

## PHP/MySQL/Web

提供 PHP/CGI 运行环境、MySQL 服务器、Web 服务器运行环境。

依赖条件：需要额外的存储空间，请参考 [磁盘管理](#)

---

### 安装模块

应用-》模块-》检查更新，找到 “Inmp ” 模块，点击安装。

	PHP/MySQL/Web服务套件 提供MySQL 数据库服务器、Web 服务器运行环境，支持 PHP/CGI 建站及Web应用的部署。 <a href="#">更多...</a>	1.1.98 2020-10-21 17:30:20	22.23 MB 139.88 MB	
---	---	-------------------------------	-----------------------	---

### 服务配置

应用-》MySQL/PHP/HTTP 服务：

全局设置 MySQL 配置 PHP 配置 HTTP 服务配置

数据存储位置

MySQL/HTTP 存储主目录 本地磁盘 /dev/nvme0n1p1 -- /disk/data (共 458.3G, 剩余 399.0G) ▾

启用 MySQL 数据库服务  是

网站服务器 → 启用 HTTP Web 服务  是

启用 PHP/FastCGI 支持  是

数据库及PHP/CGI支持, 根据需要开启

启用 CGI 支持  否

保存设置

配置上传密码:

全局设置 MySQL 配置 PHP 配置 HTTP 服务配置

服务运行状态 运行中 <PID: 3890>

根域名 (不含www.前缀)

HTTP Web 服务端口 8080

启用 HTTPS 支持  否

隐藏更多选项 <<

HTTP 请求最大数据大小 1~200, 默认为 20 MB

HTTP 站点根目录 默认为 /

SFTP 上传密码 www123456

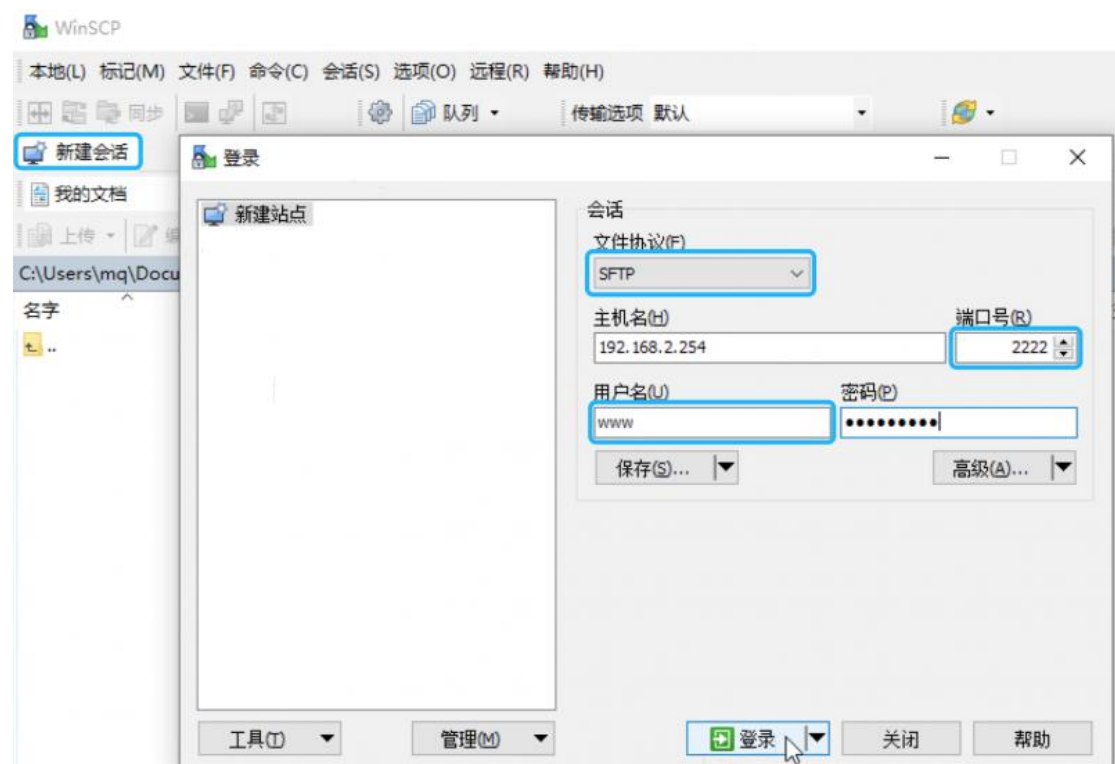
## 上传网站数据

提供 SFTP 安全方式上传, Windows 下建议使用开源客户端 [WinSCP](#)。

站点 SFTP 上传账号 www，请先在 “系统” -》“登录管理” -》SSH 登录，开启 SSH 远程登录服务。

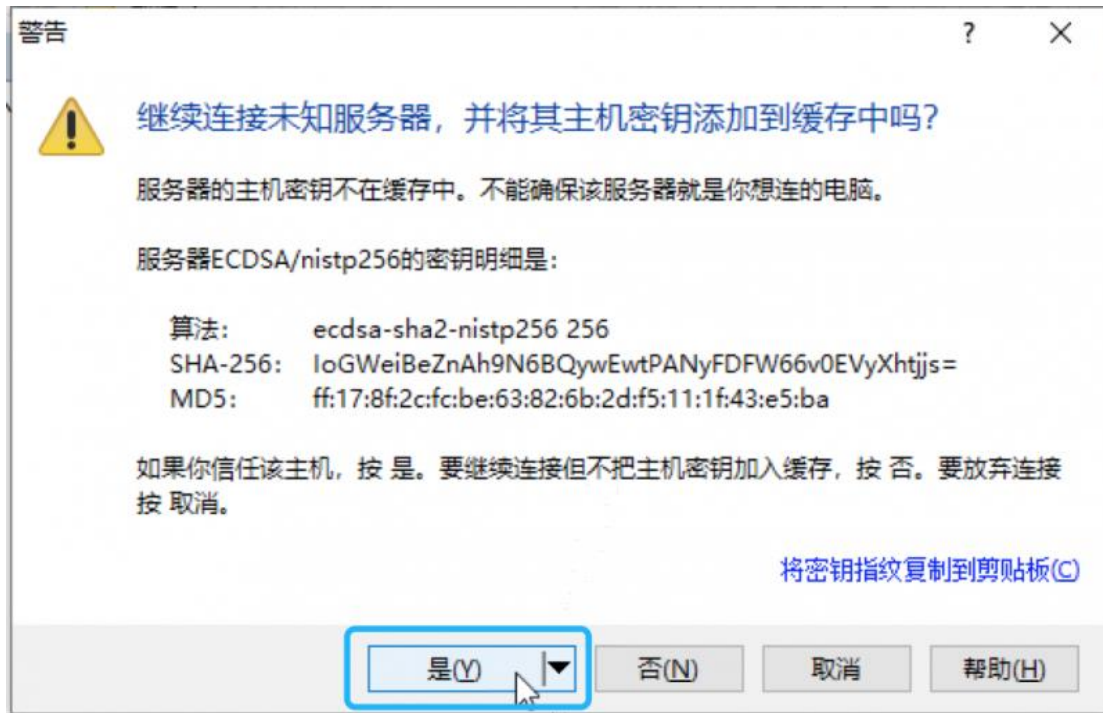
连接参数：

```
sftp://www@<服务器 IP>:2222
```

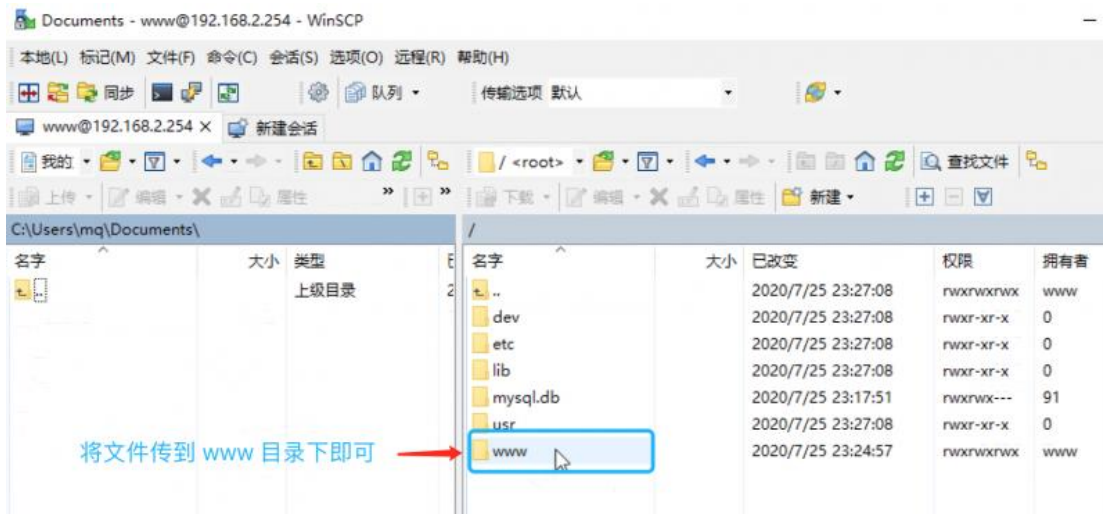


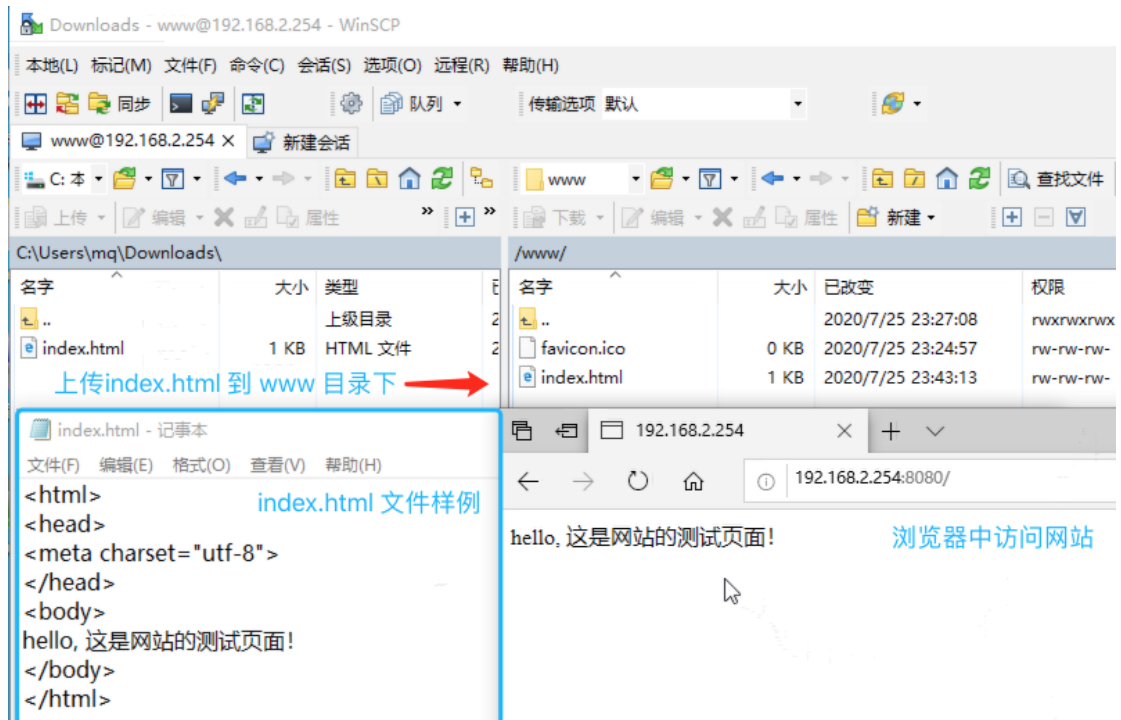
弹出存储 SSH 密钥警告，点击确认继续：





将本机文件拖到右边 www 目录下即可，www 目录为网站根目录。





index.html 文件内容样例:

```
<html>

<head>

<meta charset="utf-8">

</head>

<body>

hello, 这是网站的测试页面!

</body>

</html>
```

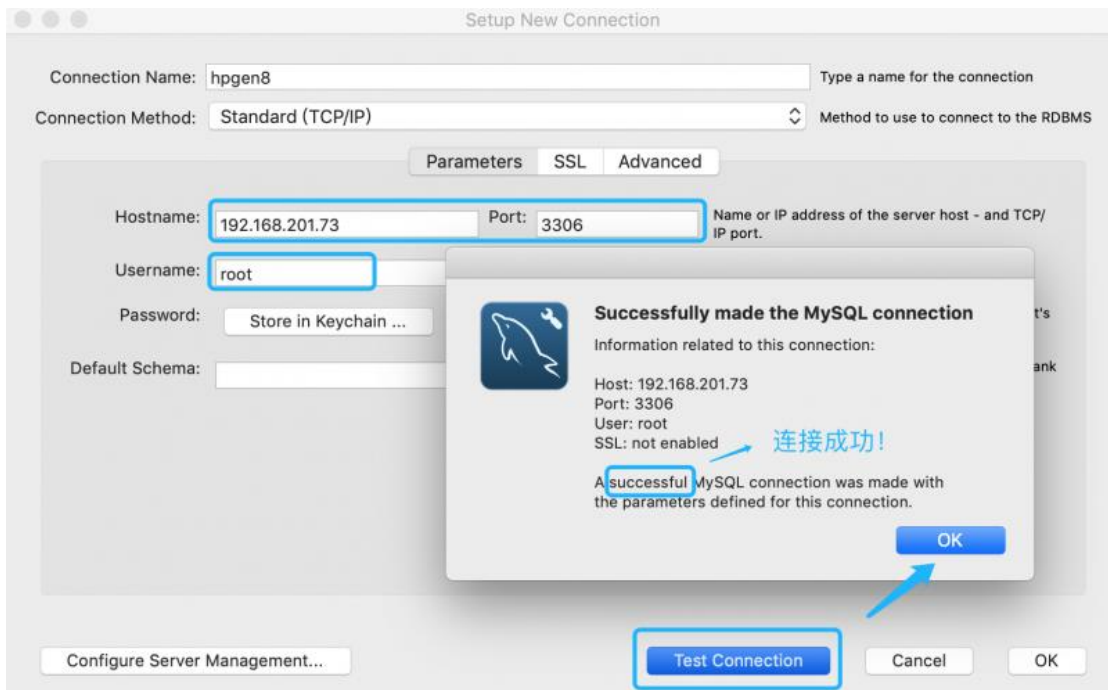
## MySQL 数据库

请使用 127.0.0.1 进行数据库连接, MySQL 初始 root 密码为 secret。

如果需要从外部连接 MySQL, 修改 MySQL 服务参数-》监听 IP 为所有网络接口:



客户端连接 (以 [MySQL Workbench](#) 为例):



# PPTPVPN 服务

PPTP VPN 服务用于远程用户通过拨号方式与服务器建立安全连接。

PPTP VPN 需要 GRE 协议支持才能正常连接, 使用 TCP/1723 端口。

最大支持 1022 个 PPTP VPN 连接。

## VPN 服务端配置

### 1. 配置服务

VPN 服务实时监测

PPTP VPN 连接: 建立中 0, 活动 2

服务运行状态 运行中 <PID: 5263> [更多...](#)

分配给客户的地址池范围

VPN地址池范围和LAN不能相同

用户认证模式

允许VPN客户访问Internet

自动设置分配给用户的DNS

[显示更多选项 >>](#)

初次配置可点击“默认设置”加载默认的参数。

### 2. 创建账号



### 3. 查看 VPN 客户端连接

ID	设备名	本地IP 远程IP	流量	建立时间 已连接	类型	帐号
1	ppp6	10.11.0.1 10.11.0.22	9.16 KB 1.43 KB	2020-07-22 14:44:44 0天0小时2分28秒	PPTP VPN 客户 « 192.168.201.73 <内部局域网>	pptp
2	ppp5	10.11.0.1 10.11.0.21	47.97 KB 92.96 KB	2020-07-22 05:03:05 0天9小时44分8秒	PPTP VPN 客户 « 116.20.38.143 <广东省佛山市 电信>	
3	ppp4	10.11.0.1 10.11.0.20	146.24 KB 146.24 KB	2020-07-21 09:05:06 1天5小时42分7秒	PPTP VPN 客户 « 171.113.241.219 <湖北省 电信>	

## Win7 客户端配置

### 1. 设置新的连接

右键点击桌面 网络，选择 属性，点击 设置新的连接或网络。

查看活动网络

[连接或断开连接](#)



访问类型: Internet  
连接: 本地连接

更改网络设置

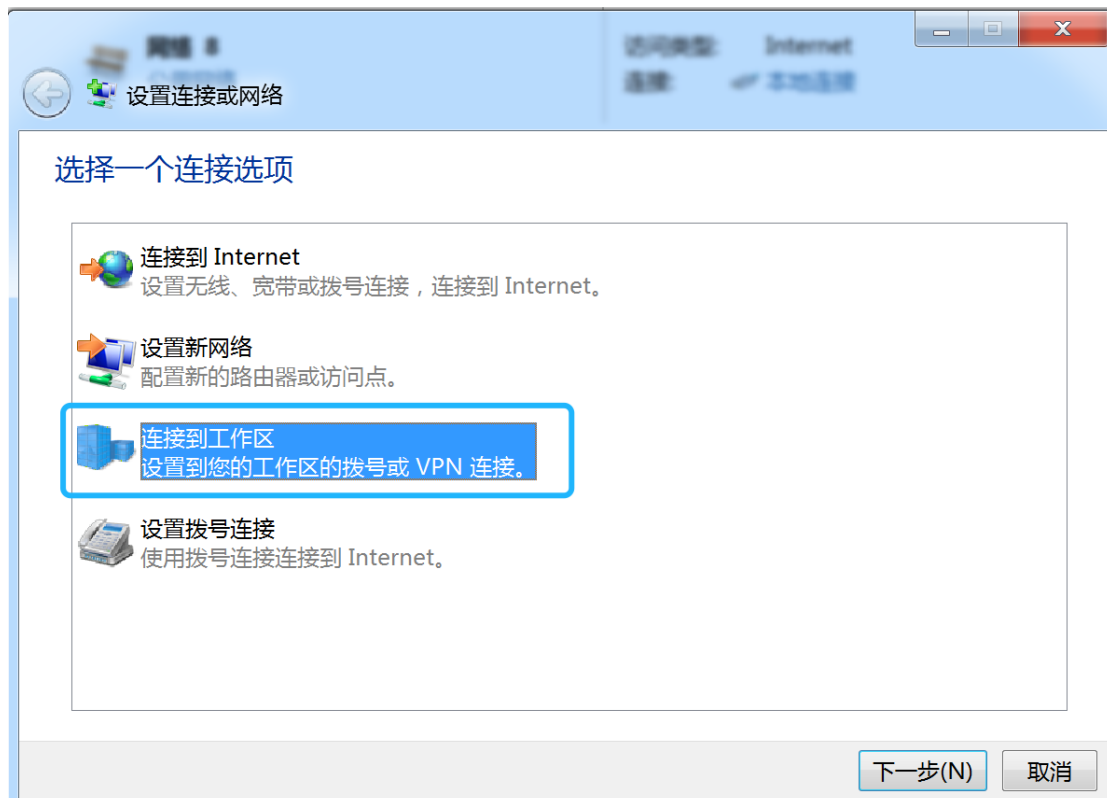
[设置新的连接或网络](#)  
设置无线、宽带、拨号、临时或 VPN 连接；或设置路由器或访问点。

[连接到网络](#)  
连接到或重新连接到无线、有线、拨号或 VPN 网络连接。

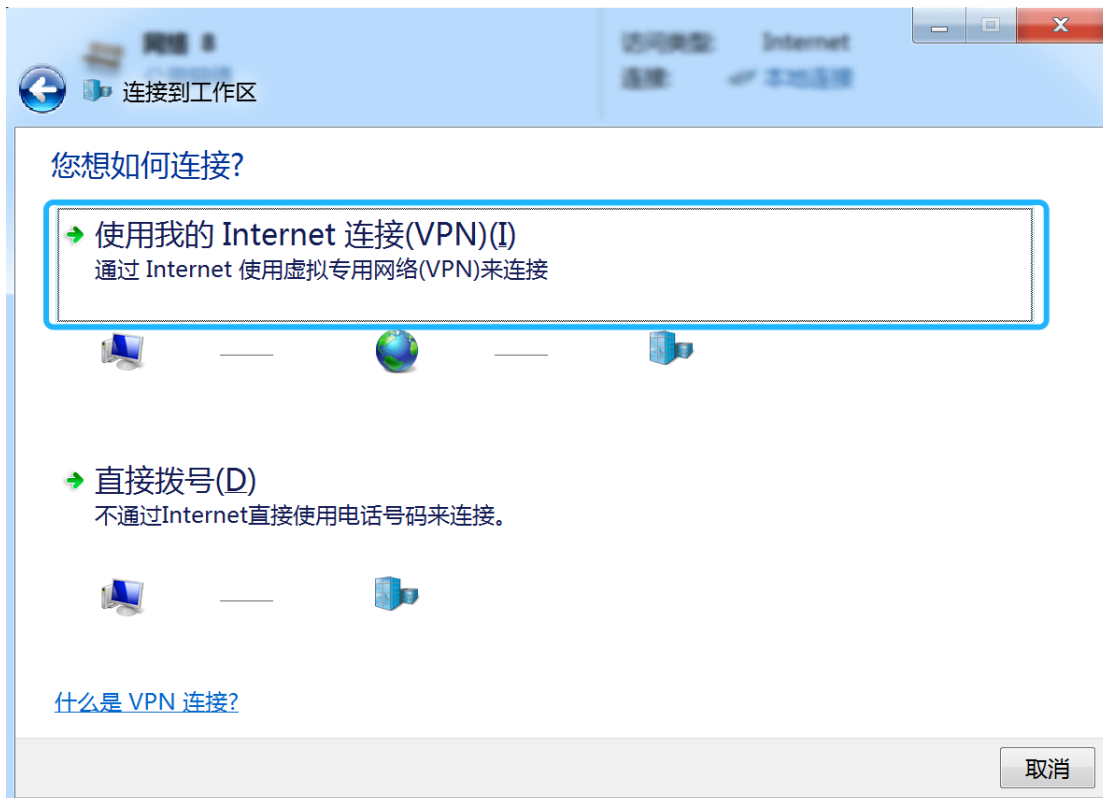
[选择家庭组和共享选项](#)  
访问位于其他网络计算机上的文件和打印机，或更改共享设置。

[疑难解答](#)  
诊断并修复网络问题，或获得故障排除信息。

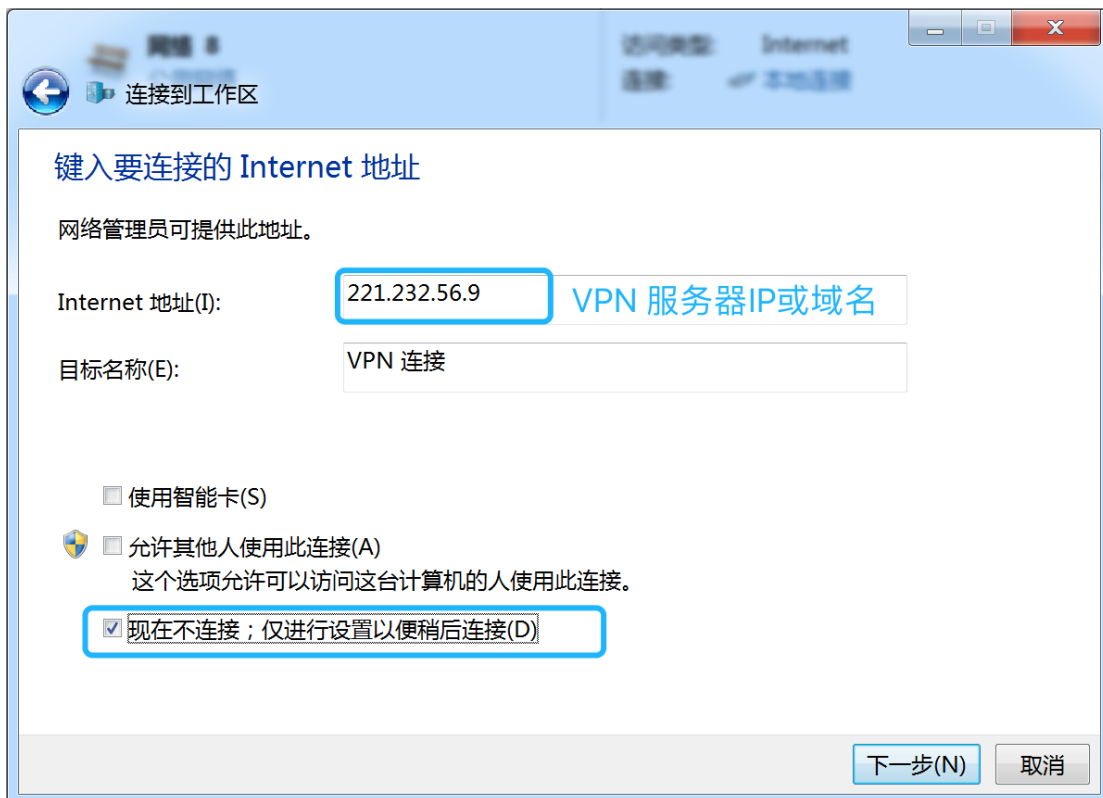
## 2. 连接到工作区



## 3. 使用 Internet 连接 VPN



#### 4. 填写 VPN 服务器 IP 或域名



## 5. 填写 VPN 账号和密码

键入您的用户名和密码

用户名(U): pptp 输入VPN账号

密码(P): pptp 输入VPN密码

显示字符(S)

记住此密码(R)

域(可选)(D):

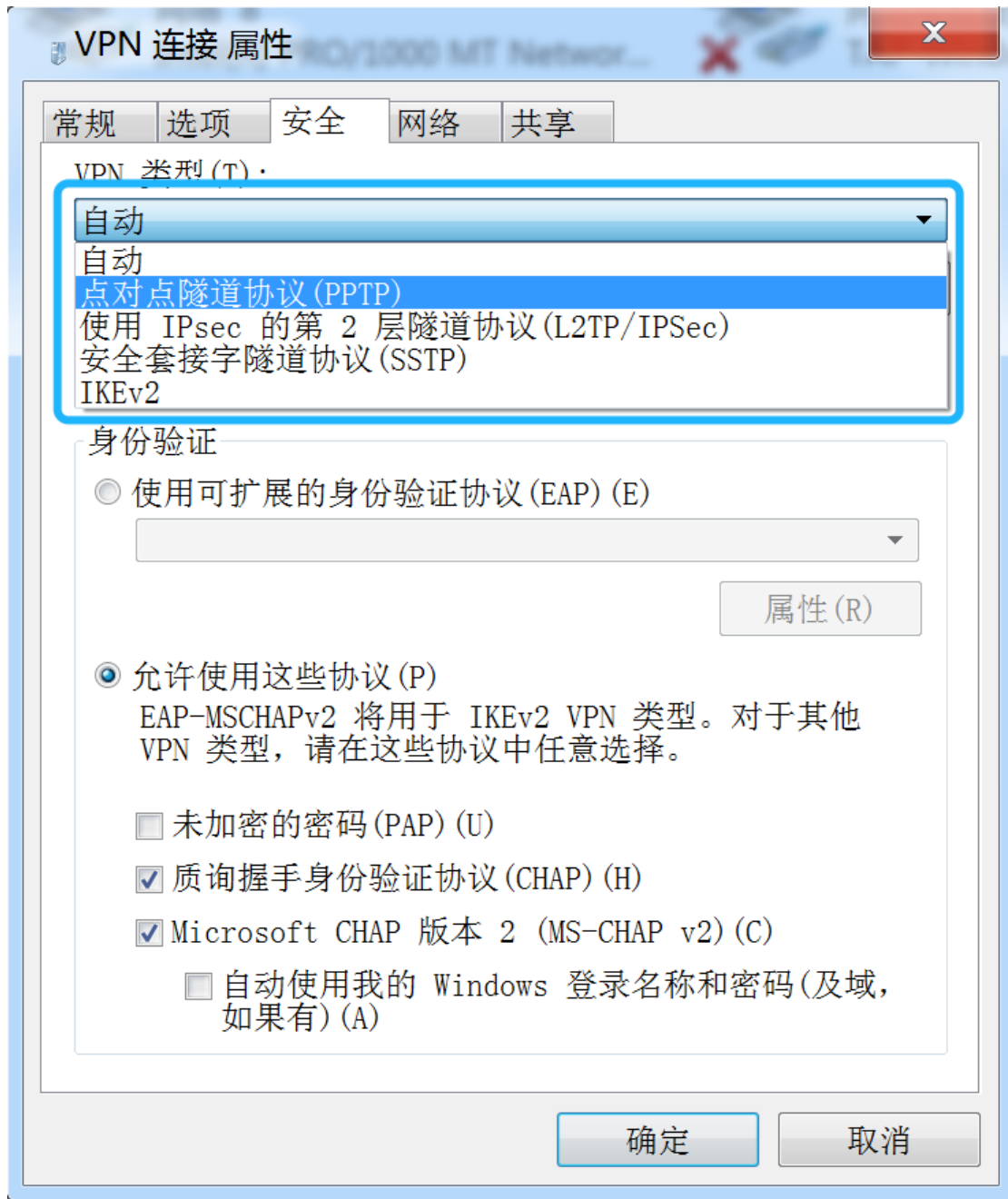
创建(C) 取消

## 6. 修改 VPN 连接属性

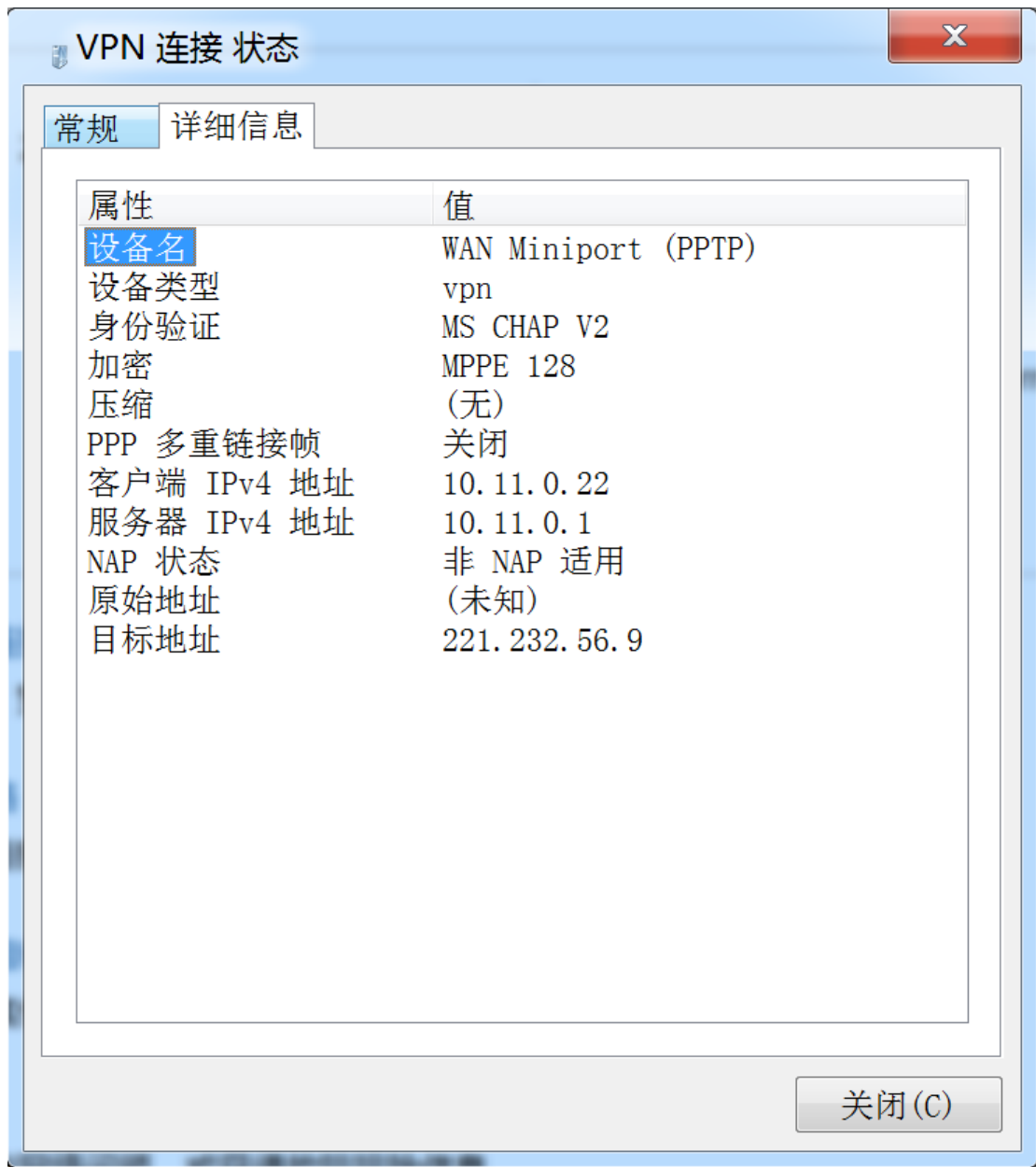




安全-》VPN 类型：选择为点对点协议（PPTP）：



点击连接，连接成功后查看状态：



## iRouter 客户端配置

### 1. 创建连接

网络-》PPTP VPN 客户端隧道-》新建连接:

名称 ptp

VPN 协议  PPTP VPN  L2TP VPN

远程服务器地址 221.232.56.9

帐号 ptp

密码 ....

更多选项-》启用 MPPE 加密:

隐藏更多选项 <

支持的身份验证协议  PAP  CHAP  MS-CHAP  MS-CHAP V2

全选 / 全不选

启用调试  否

启用 MPPE 数据加密(没有就断开)  是

## 2. 连接 VPN

共 1 个VPN连接 (0 连接中, 1 已连接)

<vpn\_pptp> 已连接

vpn\_pptp / pptp - 连接状态

设备名:	ppt0
已连接:	2020-07-22 15:21:48
已连接:	0天0小时0分40秒 <span>断开</span>
IP地址:	10.11.0.24
网关:	10.11.0.1
远程服务器地址:	221.232.56.9

[连接日志](#)

查看连接日志:

```
2020-07-22 15:21:44 Prepare to starting pptp tunnel for xstp_vpn.vpn_pptp ...
Using interface ppt0
Connect: ppt0 <--> /dev/pts/0
CHAP authentication succeeded
MPPE 128-bit stateless compression enabled
local IP address 10.11.0.24
remote IP address 10.11.0.1
```

### 3. 设置多线策略

启用多线负载及策略

多线配置 [线路分组](#) [自定义策略](#) [路由表](#)

ID	线路	连接状态 (网卡/设备名/IP)	线路类型	负载权重	禁止自动负载
1	PPTP-vpn_pptp	ppt0/10.11.0.24	默认线路	1	<input checked="" type="checkbox"/>
2	WAN-1	wan1/192.168.10.135 <湖北省 电信>	默认线路	1	<input type="checkbox"/>

在自定义策略中，设置访问 VPN 服务器背后的设备时，走 VPN 线路：

多线配置 线路分组 自定义策略 路由表

共2条记录/1页, 每页显示 10 请输入关键字 搜索 清除 新增规则

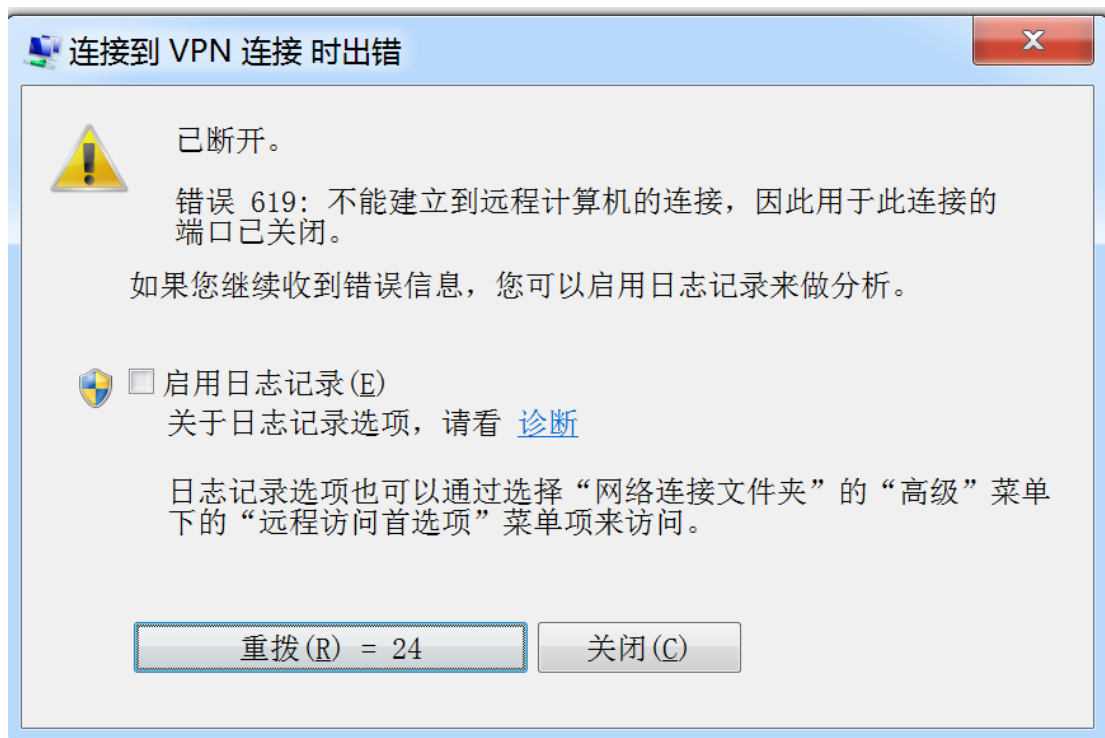
ID	优先级	名称	协议	源IP - 源端口	目的IP - 目的端口	备注	线路	状态	编辑	选择
1	0	sip	所有	:	192.168.1.30:	讯时sip	pptp.vpn_pptp	☑	✎	<input type="checkbox"/>
2	1	72服务器	所有	:	192.168.1.72:		pptp.vpn_pptp	☑	✎	<input type="checkbox"/>

专家模式 导出规则 全选 / 全不选

## 常见问题 FAQ

### 1. 错误提示 691

错误 691:不能建立到远程服务器到连接。



检查 VPN 服务器是否可访问，如果 VPN 服务器在其他地方能正常连接，则可能是客户端的网络问题，检查客户端的出口的路由器上是否开启了 GRE/PPTP VPN 穿透：

## 防火墙

防火墙用于保护内网安全, 过滤非法的数据包、抵御入侵和攻击

基本策略    攻击防御    黑白名单    ACL 规则

<input type="checkbox"/> 关闭防火墙功能（不推荐，除非作为服务器在内网使用）
<input type="checkbox"/> 关闭 NAT 功能（仅做转发，用于有上级路由做NAT的环境）
<input type="checkbox"/> 禁止外网 PING 本机(推荐选上)
<input type="checkbox"/> 完全禁止 PING 本机 (不响应所有 ICMP echo 请求, 不推荐勾选)
<input type="checkbox"/> 启用常见欺骗防护(IP/源路由/ICMP等)
<input type="checkbox"/> 修改 NAT 连接老化时间 (谨慎)
<input checked="" type="checkbox"/> 启用 NAT 穿透支持(GRE/PPTP/SIP/H323 等)

全选 / 全不选

保存设置    默认设置

## PPTP VPN 上网访问控制

需求：指定的账号 VPN 拨号后，能通过 VPN 访问 Internet，其他的账号只能访问 VPN 内网资源。

基本步骤：

1. VPN 服务参数中不勾选 “允许 VPN 客户访问 Internet” ，  
或者在 WAN 口连接中勾选 “禁止 NAT”

- 应用-》本地认证账号，创建 VPN 账号，为需要上网的 VPN 账号分配固定 IP
- 路由-》自定义 NAT 策略，设置上述固定 IP 对应的 NAT 规则

## 1. 禁止 VPN 访问 Internet

服务运行状态 运行中 <PID: 3874> [更多...](#)

[分配给客户的地址池范围](#) 193.67.67.0/24

用户认证模式 本机 RADIUS 认证 [账号管理](#)

允许VPN客户访问Internet  否

自动设置分配给用户的DNS  是

## 2. VPN 账号分配固定 IP

分配的固定 IP 必须在 VPN 地址范围内：

共54条记录/1页, 每页显示 200  [搜索](#) [清除](#) 帐号状态 所有 [新建账号](#)

ID	用户名	姓名	- 可用功能 - 分配固定IP	使用期限 (开通 - 到期) 上线/下线时间	套餐	备注	状态
1	mqtest <sup>1</sup>		<b>PPTPVPN</b> 193.67.67.100	~ 上线时间: 2020-08-27 16:24:18			上线

## 3. 自定义 NAT 规则



**源IP** 193.67.67.100  
VPN账号中分配的固定IP

**目的IP**

**协议** TCP+UDP

**目的端口** 1~65535

**类型**  
 REDIRECT (重定向)  DNAT (目的地址转换)  
 SNAT (源地址转换)  禁止连接跟踪

**动作** 进行地址转换(NAT)

**NAT 后的地址** 119.67.67.100 WAN口IP

## 4. VPN 测试

在其他路由上创建 VPN 隧道（网络-》PPTP/L2TP VPN 隧道），工具-》系统体检，选择 VPN 线路测试。

禁止访问 Internet 时：

```
** 测试到达 Internet 网关 193.67.67.1 的延时
ICMP reply from 193.67.67.1: icmp_seq=0 time=72.354 ms
ICMP reply from 193.67.67.1: icmp_seq=1 time=55.399 ms
ICMP reply from 193.67.67.1: icmp_seq=2 time=64.574 ms
小计：共发送3个包，收到3个包，丢包率 0.0%，平均延时 64.109 ms
测试目标线路 pptp.vpntest
本地IP: 193.67.67.100 网关：193.67.67.1，最大传输单元 (MTU) : 1436
查询公网出口IP及位置信息... 公网IP 193.67.67.100 [荷兰]
测试访问网站 www.baidu.com ... 失败 ERR: 500 Can't connect to www.baidu.com:80 (connect: timeout)

测试访问网站 www.163.com ... 失败 ERR: 500 Can't connect to www.163.com:80 (connect: timeout)

测试外网下载带宽 ... 失败 ERR: 500 Can't connect to mac.qq.com:443 (connect: Connection timed out)
```

允许访问 Internet 时：

```
** 测试到达 Internet 网关 193.67.67.1 的延时
ICMP reply from 193.67.67.1: icmp_seq=0 time=49.691 ms
ICMP reply from 193.67.67.1: icmp_seq=1 time=52.872 ms
ICMP reply from 193.67.67.1: icmp_seq=2 time=50.844 ms
小计: 共发送3个包, 收到3个包, 丢包率 0.0%, 平均延时 51.136 ms
测试目标线路 pptp.vpn-test
本地IP: 193.67.67.100, 网关: 193.67.67.1, 最大传输单元 (MTU) : 1436
查询公网出口IP及位置信息... 公网IP 193.67.67.100 [荷兰]
测试访问网站 www.baidu.com ... 访问站点成功, 耗时 1212 ms, 传输数据 279.20 KB, 约 199 个包
测试访问网站 www.163.com ... 访问站点成功, 耗时 614 ms, 传输数据 493.13 KB, 约 351 个包
测试外网下载带宽 ... 获得9个下载链接
从 https://dldir1.qq.com/qqfile/QQforMac/QQ_6.6.8.dmg 下载文件 ... 52.32 MB
下载耗时 20 秒, 传输文件 39.4M, 平均速度 1.97 MB/s, 带宽大小 15.8Mbps
```

## IPsec VPN

此应用用于创建虚拟专用网络(Virtual Private Network)加密通道, 用于点到网的认证连接, 支持 IPsec/L2TP 和 Cisco IPsec (IPsec/XAuth) 两种模式, 支持 Windows、iOS、macOS、Android 客户端连接。

IPsec/L2TP VPN 使用 UDP 500/4500/1701 端口。

---

## 安装模块

进入“应用” -> “模块管理”, 点击“检查更新”, 安装“ipsecvpn” 模块

## 服务端配置

进入“应用” -》 “IPsec/L2TP VPN 服务”

IPsec/L2TP VPN 服务

服务运行状态 运行中 <PID: 27223>

允许VPN客户访问Internet 是

VPN 接口本地 IP 178.20.0.1

IPsec 共享密钥 12345678

自动设置分配给用户的DNS 是

显示更多选项 >

操作成功 默认设置 重启服务

进入“应用” -》 “本地认证账号” -》，添加 IPsecVPN 账号

帐号 ipsec

密码 ipsec

可用功能  PPPoE  FTP  Portal/Web  PPTP VPN  
 SSL VPN  IPsec/L2TP VPN  Samba/File  
全选 / 全不选

姓名

显示更多选项 >

## 客户端配置

### L2TP - Windows 客户端

适用于：Windows 7/8/10

1. 右键单击系统托盘中的无线/网络图标，选择 **打开网络与共享中心**，单击 **设置新的连接或网络**。

选择 **连接到工作区**，然后单击 **下一步**，单击 **使用我的 Internet 连接 (VPN)**。

2. 在 **Internet 地址** 字段中输入路由 WAN 口或 LAN 口的 IP 地址，在 **目标名称** 字段中输入任意内容。单击 **创建**。

连接到工作区

键入要连接的 Internet 地址

网络管理员可提供此地址。 **路由WAN口或LAN口的IP地址**

Internet 地址(I): 202.103.24.68

目标名称(E): VPN 连接

**任意**

使用智能卡(S)

记住我的凭据(R)

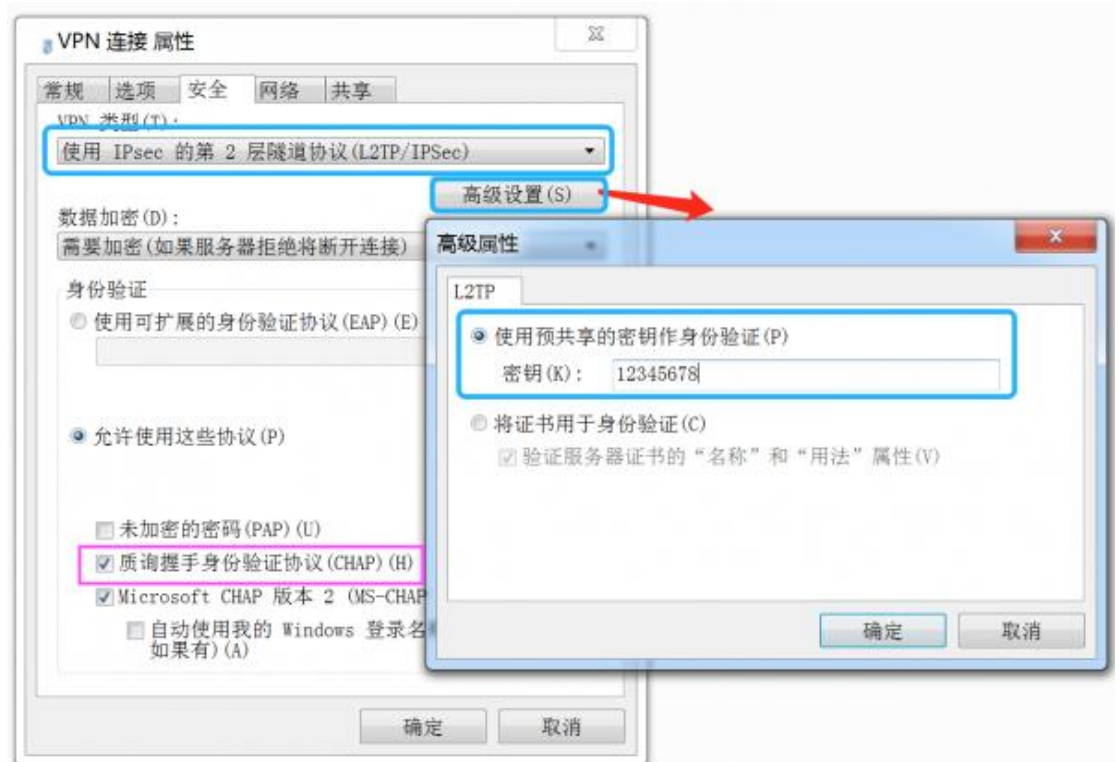
允许其他人使用此连接(A)  
这个选项允许可以访问这台计算机的人使用此连接。

创建(C) 取消

3. 修改连接属性

将 VPN 类型修改为：使用 IPsec 的第 2 层隧道协议 (L2TP/IPSec)

单击 **高级设置** 按钮，**使用预共享密钥作身份验证** 并在 **密钥** 字段中输入路由服务端配置的共享密钥。

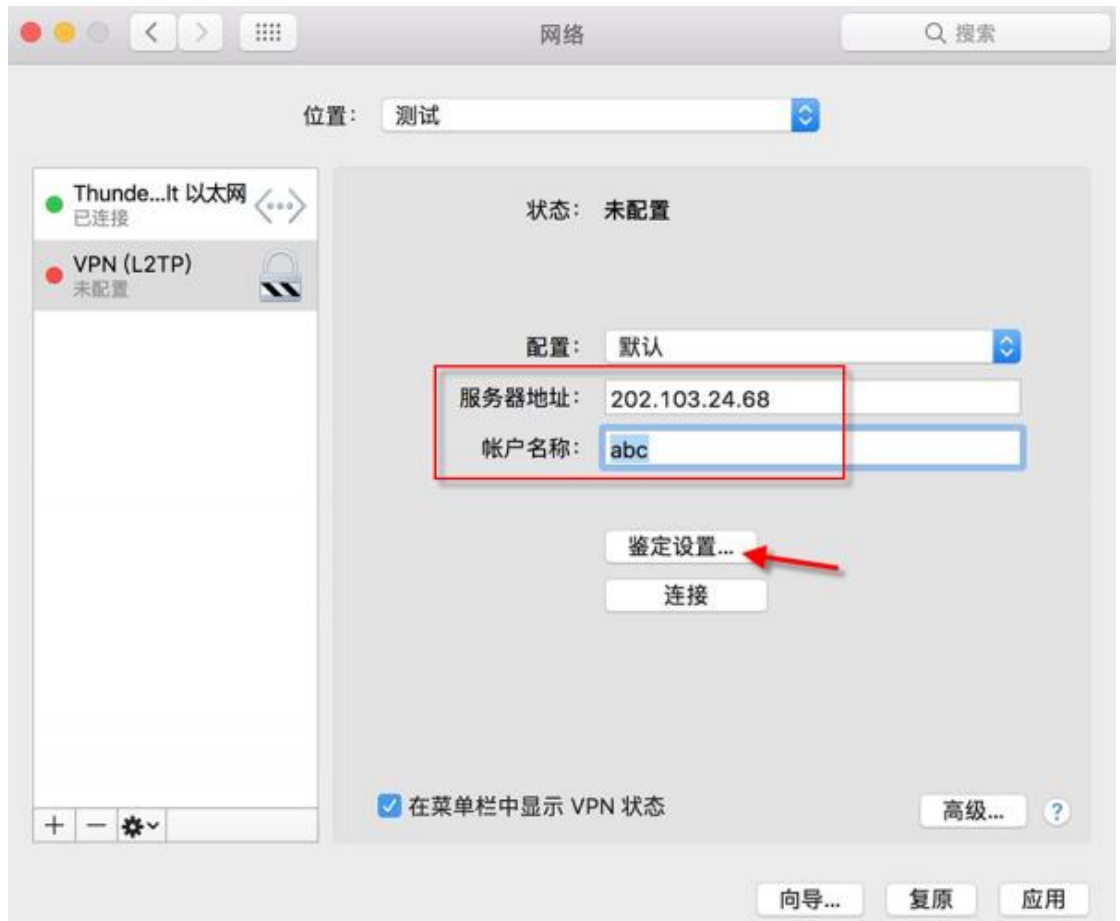


## L2TP - macOS 客户端

1. 打开系统偏好设置-》网络，在窗口左下角单击 + 按钮。
2. 从 **接口** 下拉菜单选择 **VPN**，**VPN 类型** 下拉菜单选择 **IPSec 上的 L2TP**，在 **服务名称** 字段中输入任意内容，单击**创建**。



3. 在 **服务器地址** 字段中输入路由 WAN 口或 LAN 口的 IP 地址，**帐户名称** 字段中输入路由上创建的 VPN 用户名，单击 **鉴定设置** 按钮。



4. 在 **用户鉴定** 部分，选择 **密码** 单选按钮，然后输入路由上创建的 VPN 密码；在 **机器鉴定** 部分，选择 **共享的密钥** 单选按钮，然后输入服务端的共享密钥。

用户鉴定：

密码：

RSA SecurID

证书

Kerberos

CryptoCard

机器鉴定：

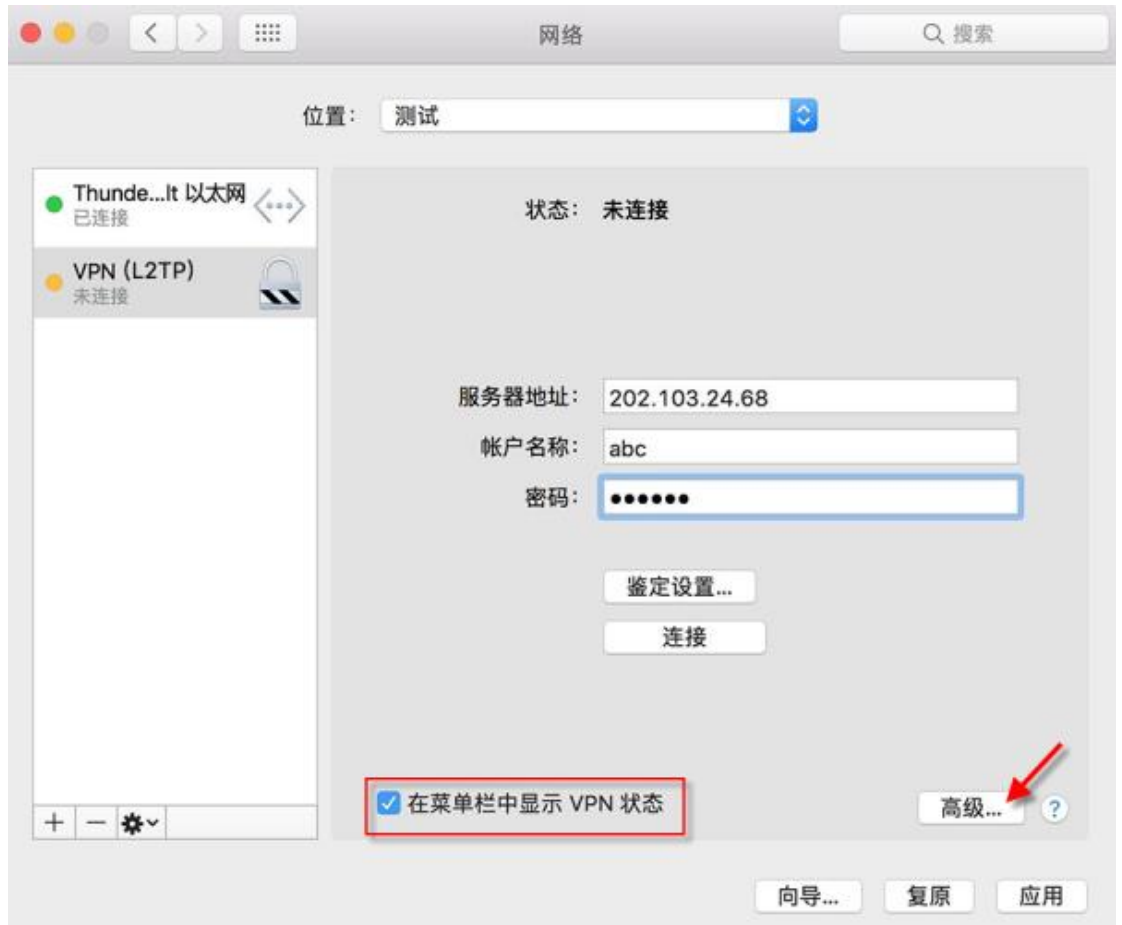
共享的密钥：

证书

群组名称：

(选填)

5. 选中 **在菜单栏中显示 VPN 状态** 复选框，单击 **高级** 按钮

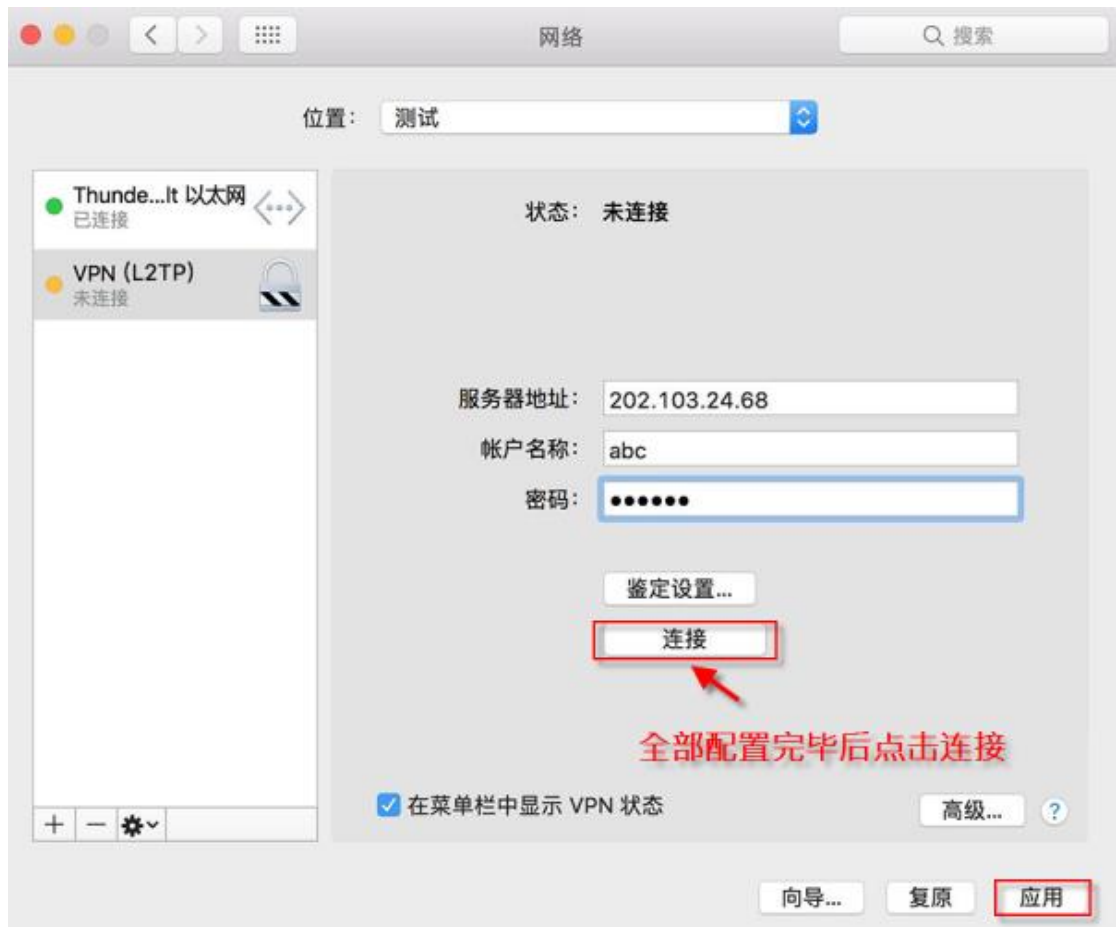


6. 在 **选项** 标签页中选中 **通过 VPN 连接发送所有通信** 复选框





7. 然后单击 **应用** 保存 VPN 连接信息，点击 **连接** 即可拨号



## L2TP - Android 客户端

1. 打开 **设置**，在 **无线和网络** 部分单击 **更多...**，在弹出的菜单中选择 **VPN**，选择 **添加 VPN 网络**



2. 在 **名称** 字段中输入任意内容，在 **类型** 下拉菜单选择 **L2TP/IPSec PSK**，在 **服务器地址** 字段中输入路由 WAN 口或 LAN 口的 IP 地址，在 **IPSec 预共享密钥** 字段中输入服务端的共享密钥，配置完后选择 **保存**。

## 编辑 VPN 网络

名称

vpn

类型

L2TP/IPSec PSK >

服务器地址

202.103.24.68

L2TP 密钥

(未使用)

IPSec 标识符


(未使用)

IPSec 预共享密钥

.....

显示高级选项

取消

保存 

3. 点击进入新建的 VPN 连接，在 **用户名** 和 **密码** 字段中输入服务端配置的账号密码，选中 **保存帐户信息** 复选框，单击 **连接**。



连接到vpn

用户名

abc

密码

.....

保存帐户信息

全部配置完后连接

取消 连接

## L2TP - iOS 客户端

1. 进入 **设置** → **通用** → **VPN** → **添加 VPN 配置**

2. 选择 **L2TP**，在 **描述** 中可输入任意内容，在 **服务器** 字段中输入路由 WAN 口或 LAN 口的 IP 地址，在 **帐户** 和 **密码** 中输入服务端配>置的账号密码，在 **密钥** 字段中输入服务端的共享密钥，启用 **发送所有流量** 选项，最后单击右上角的 **完成**。



取消 添加配置 完成

类型 L2TP >

描述 L2tp IPsec

服务器	201.103.24.68
帐户	abc

RSA SecurID

密码	●●●●●●
密钥	●●●●●●

发送所有流量

服务端配置的共享密钥

3. 全部配置好后，启用 **VPN** 连接。

## 常见问题 FAQ

### 1. Windows 错误 809

错误 809: 无法建立计算机与 VPN 服务器之间的网络连接, 因为远程服务器未响应。

原因: 默认情况下, Windows 不支持连接到 NAT 设备后面的 IPsec 服务器。

解决办法: 开始菜单-》附件-》命令提示符, 右键点击选择“使用管理员权限运行”, 输入以下命令:

Win7/8/10 使用:

```
REG ADD  
HKLM\SYSTEM\CurrentControlSet\Services\PolicyAgent /v  
AssumeUDPEncapsulationContextOnSendRule /t REG_DWORD  
/d 0x2 /f
```

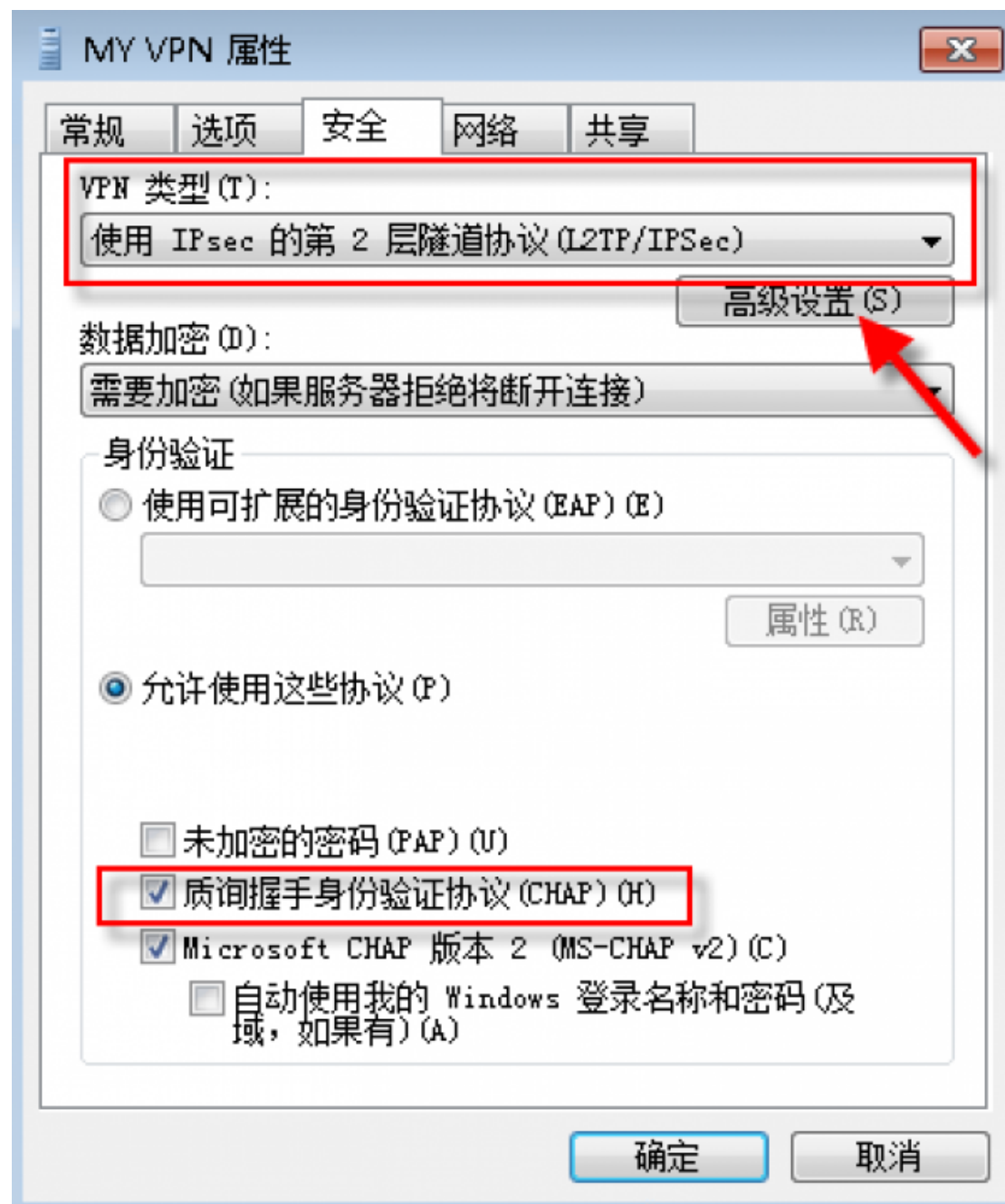
WinXP 使用:

```
REG ADD HKLM\SYSTEM\CurrentControlSet\Services\IPSec /v  
AssumeUDPEncapsulationContextOnSendRule /t REG_DWORD  
/d 0x2 /f
```

完成后须重启计算机生效。

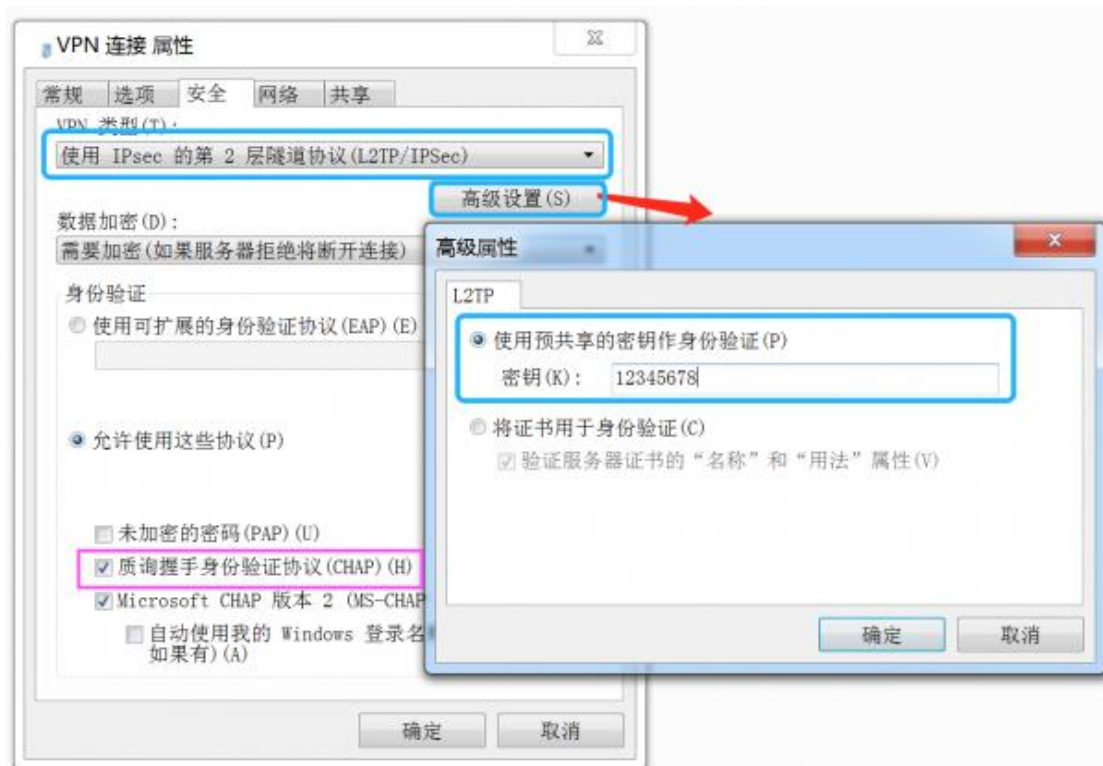
## 2. Windows 错误 628

错误 628: 在连接完成前, 连接被远程计算机终止。



确保 VPN 连接属性-》安全-》选中 “质询握手身份验证协议 (CHAP)”



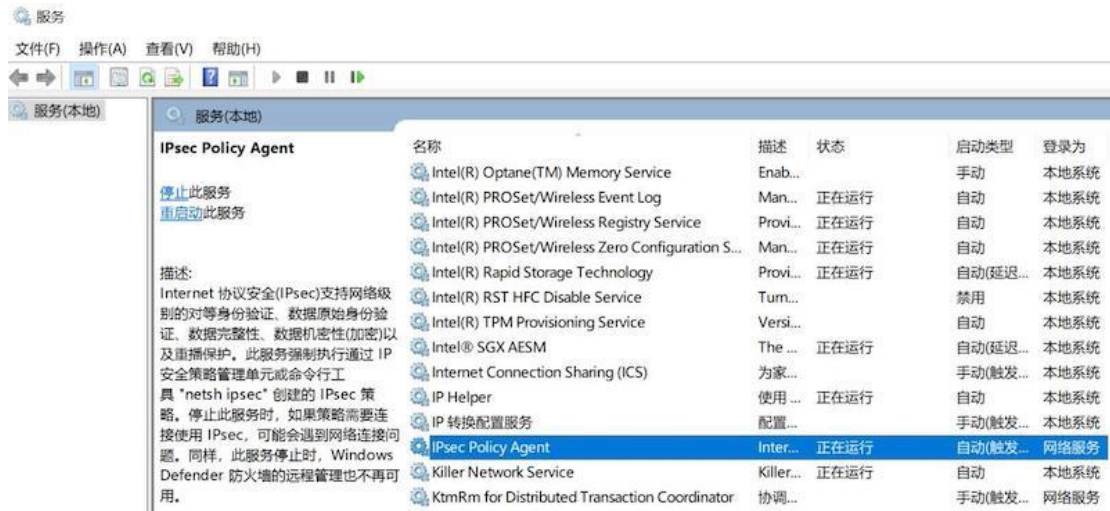


### 3. L2TP 连接尝试失败

win10 下提示错误：L2TP 连接尝试失败，因为安全层在初始化与远程计算机的协商时遇到了一个处理错误

解决步骤如下：

- a. 查看服务是否开启：windows+r 运行 输入 services.msc
- b. 查找 ipsec policy agent 启动服务



### c. 修改注册表

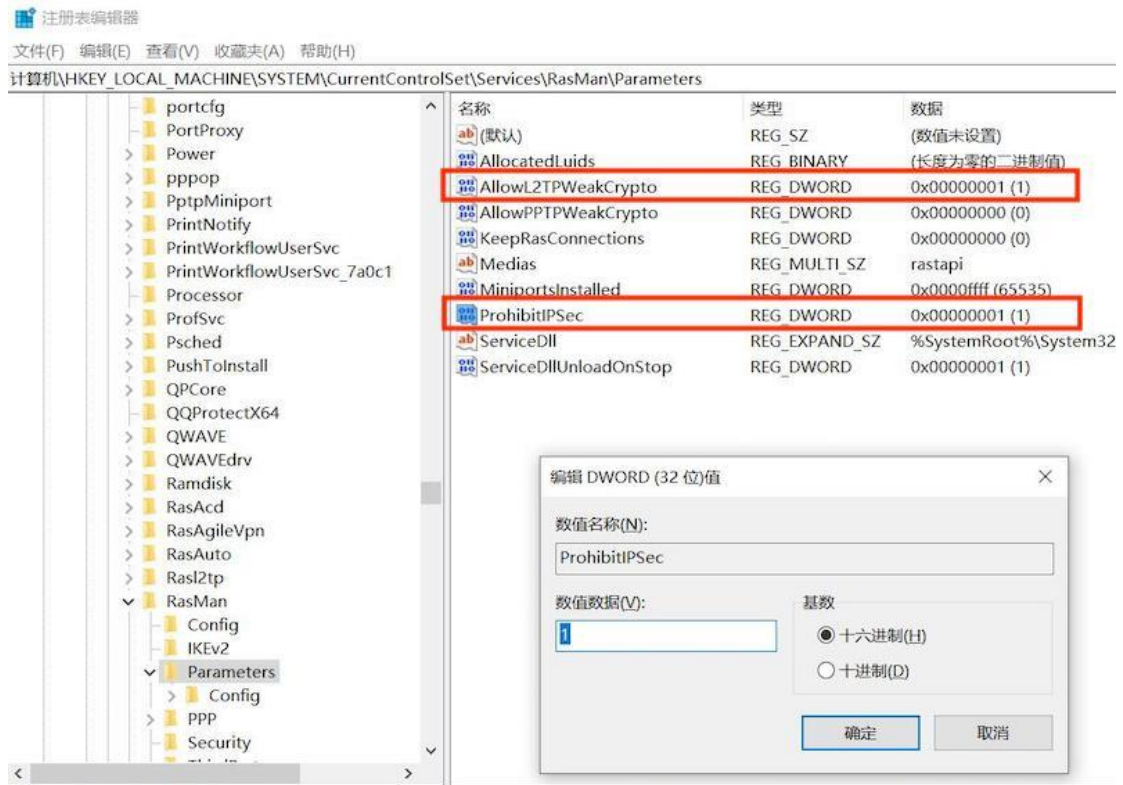
在注册表编辑器中，找到并单击以下注册表子项：

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters
```

单击 allowL2TPweakcrypthto 修改值为 1

在空白处新建，然后单击 DWORD(32) 值(D),重命名

“ProhibitIpSec” ,修改值为 1



d. 重启计算机

## SSL VPN

### 功能介绍

SSL VPN 用于创建虚拟专用网络(Virtual Private Network)加密通道。使用 SSL VPN 可以方便地在不同网络访问场所之间搭建类似于局域网的专用网络通道。

本篇主要介绍 SSL VPN 的常用操作，若需要实现局域网互联，请参考：[SD-WAN 异地局域网互联（组网）](#)

默认加密算法：AES-256-GCM

## 安装模块

进入“应用” -》“模块管理”，点击“检查更新”，安装“sslvpn” 模块

## 路由服务端设置

1. 进入“应用” -》“SSL VPN 服务”
2. 初次配置可以依次点击“默认参数”和“一键生成证书”，然后点击“保存设置”

协议类型  UDP (默认)  TCP

[VPN 服务端口](#) 1150 端口默认是1194, 建议修改为其他的

[VPN 子网地址](#) 10.10.0.0/16 网段不要和内网及PPPoE等其他的冲突就行

CA 证书状态 正常 [一键生成证书](#) [导出服务端证书](#) [生成客户端配置](#)

安全参数

- 允许VPN客户端之间互访
- 允许客户端访问本地局域网
- 允许客户端通过VPN访问Internet

全选 / 全不选

[推送路由](#) 192.168.9.0/24  
192.168.10.0/24 [清空](#)

VPN客户端连上后访问这些IP或网段将走VPN隧道

建议修改默认端口（1194），有的运营商可能对此端口有限制。

3. 进入“应用” -》“本地认证账号”，为账号开通“SSL VPN” 权限
4. 导出服务端证书，解压缩导出的文件，里面的 ca.crt 会在后面用于客户端的连接

## 路由客户端配置

1. 进入“网络” -》“SSL VPN 连接”，新建一个连接：

协议类型  UDP (默认)  TCP 和服务端一致

VPN 服务器地址

VPN 服务端口  CA 证书

CA 证书内容

将ca.crt文件用文本编辑器打开，然后复制后粘贴到这里，文件的内容应该像下面这样：

```
-----BEGIN CERTIFICATE-----  
...此处省略N行...  
-----END CERTIFICATE-----
```

帐号名  ✕

密码

2. 连接成功后，可以看到如下的信息：

共 1 个VPN连接 (0 连接中, 1 已连接)

<SSLVPN> 已连接

SSLVPN / VPN - 连接状态

设备名:	tun0
上线时间:	2017-04-20 10:00:42
已连接:	44分44秒 <span>断开</span>
IP地址:	10.10.0.6
网关:	10.10.0.5
VPN 服务器地址	[REDACTED]

拨号日志

同时, 在服务端上也可以看到客户端的连接信息:

SSL VPN 服务

参数设置 | 连接状态

共2条记录/1页, 每页显示 10 | 请输入关键字 | 搜索 | 清除 | 自动刷新 | 2020-07-22 16:28:10

ID	客户端VPN 地址 附属子网地址	用户名	远程IP / 端口	上行总流量/下行总流量	建立时间 存活时间	已连接
1	10.200.0.16	m...kup	171.113.241.219:41389 湖北省 电信	4.44 MB / 8.19 MB	2020-07-18 09:44:42 2020-07-22 16:28:01	4 天 6 小时 43 分 28 秒
2	10.200.0.14 192.168.10.0/24 192.168.10.11	n...one	171.113.241.219:41476 湖北省 电信	230.53 MB / 29.29 MB	2020-07-18 09:46:03 2020-07-22 16:27:31	4 天 6 小时 42 分 7 秒

点击IP可强制踢下线

## 隧道测试

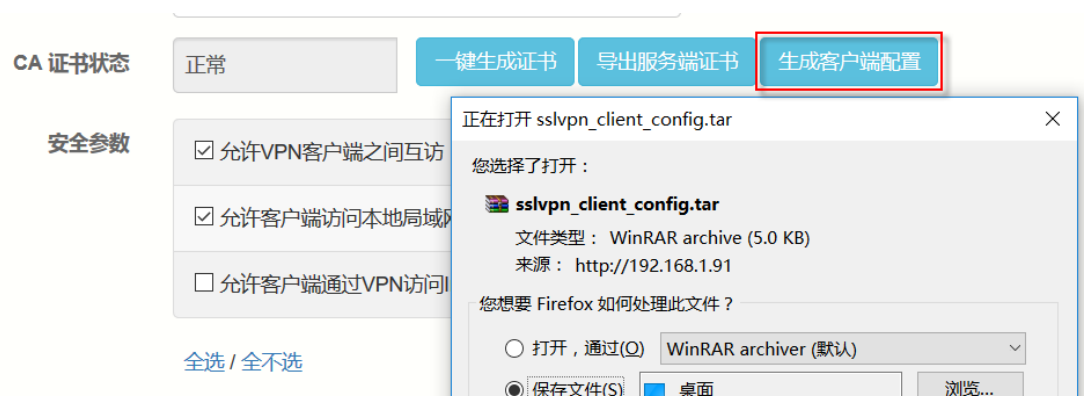
VPN 服务端的 IP 为 “VPN 子网地址” 的第一个 IP, 比如子网设为 10.10.0.0/16 时, 服务端的 VPN 设备 IP 为 10.10.0.1

1. 在客户端上用 PING 工具测试服务端 IP, 10.10.0.1
2. 在服务端上 PING 客户端连接后获得的 IP, 比如 10.10.0.6
3. 在客户端上 PING 服务端推送的内网的 IP 或网段, 比如 192.168.9.X 或 192.168.10.X

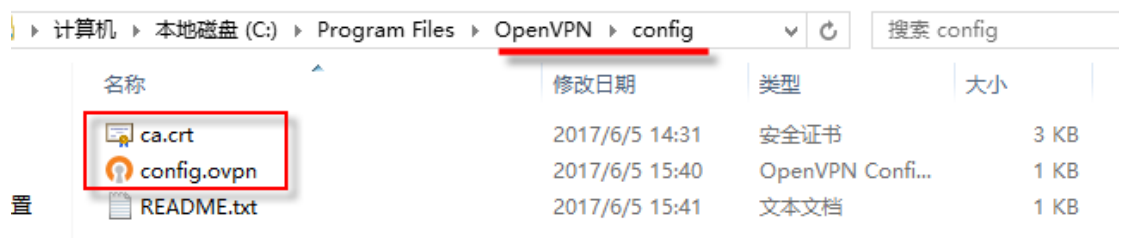
## windows 客户端配置

[官网](#) 下载对应的 openvpn

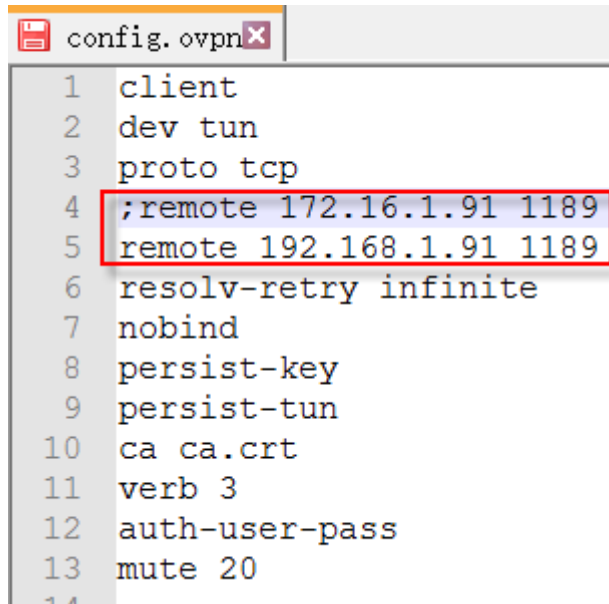
1. 安装好以后, windows 客户端先进入路由的 SSLVPN 服务, 点击“生成客户端配置”, 将弹出的 tar 文件保存到本地。



2. 进入 OPENVPN 的安装目录下的 config 目录, 将刚保存的 tar 解压缩后放入此目录

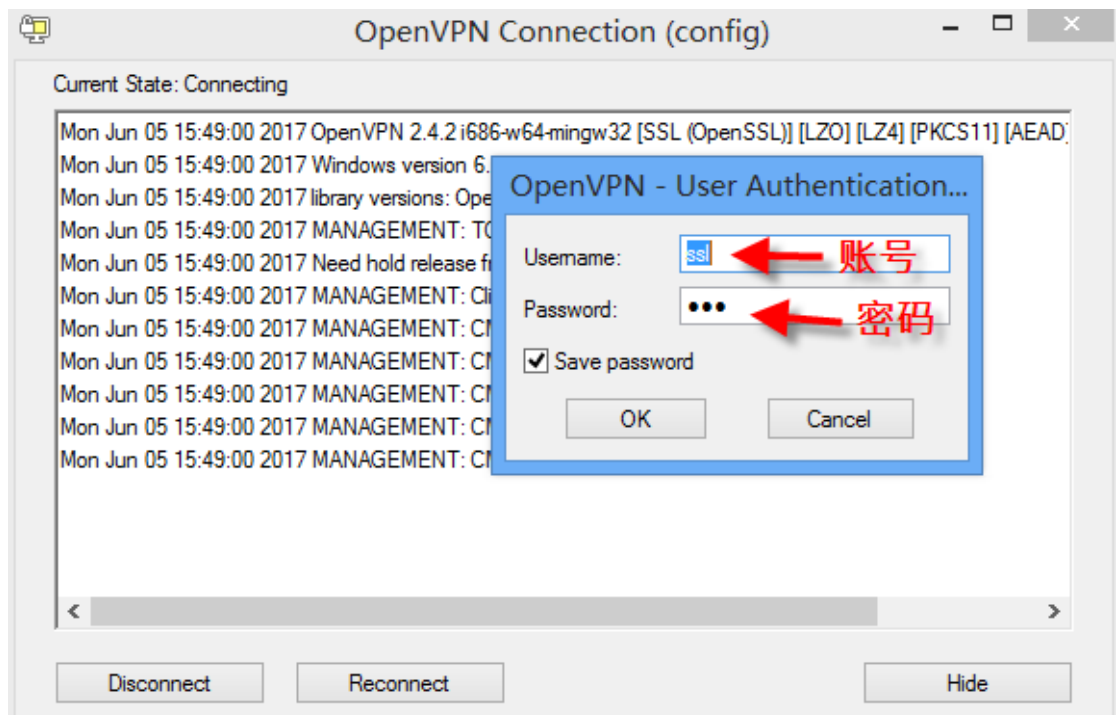


- 用文本编辑器修改 config.ovpn 文件，将要连接的 IP 前面的 “;” 去掉，不需要连接 IP 前面加上 “;”



```
1 client
2 dev tun
3 proto tcp
4 ;remote 172.16.1.91 1189
5 remote 192.168.1.91 1189
6 resolv-retry infinite
7 nobind
8 persist-key
9 persist-tun
10 ca ca.crt
11 verb 3
12 auth-user-pass
13 mute 20
14
```

- 双击运行 OPENVPN 图标，右下角会多出一个运行图标，右键点击此图标，选择 “connect” ，会弹出登录窗口





5. 输入 SSLVPN 的账号密码，点击 “OK” ，即可自动连接，成功后服务端和客户端各有对应的 IP 显示

```
Current State: Connected
Mon Jun 05 15:52:49 2017 Notified TAP-Windows driver to set a DHCP IP/netmask of 12.12.11.6/255.255.255.252 on interface (B631D4B9-2A6D-41
Mon Jun 05 15:52:49 2017 Successful ARP Flush on interface [24] (B631D4B9-2A6D-4B9D-BD77-E3368C59D666)
Mon Jun 05 15:52:50 2017 do_ifconfig, tt->did_ifconfig_ipv6_setup=0
Mon Jun 05 15:52:50 2017 MANAGEMENT: >STATE:1496649170,ASSIGN_IP,,12.12.11.6,...
Mon Jun 05 15:52:55 2017 TEST ROUTES: 2/2 succeeded len=2 ret=1 a=0 u/d=up
Mon Jun 05 15:52:55 2017 MANAGEMENT: >STATE:1496649175,ADD_ROUTES,.....
Mon Jun 05 15:52:55 2017 C:\Windows\system32\route.exe ADD 192.168.1.0 MASK 255.255.255.0 12.12.11.5
Mon Jun 05 15:52:55 2017 Route addition via service succeeded
Mon Jun 05 15:52:55 2017 C:\Windows\system32\route.exe ADD 12.12.11.0 MASK 255.255.255.0 12.12.11.5
Mon Jun 05 15:52:55 2017 Route addition via service succeeded
Mon Jun 05 15:52:55 2017 Initialization Sequence Completed
Mon Jun 05 15:52:55 2017 MANAGEMENT: >STATE:1496649175,CONNECTED,SUCCESS,12.12.11.6,192.168.1.251,1190,192.168.1.99,55320
```

ID	客户端VPN 地址	用户名	远程IP	远程端口	上行/下行流量	连接建立时间 存活时间	连接时长
1	12.12.11.6	ssl	192.168.1.99 内部局域网	55320	18.54 KB / 4.75 KB	2017-06-5 15:52:29 2017-06-5 15:52:30	1分12秒

## MacOS 客户端配置

[官网](#) 下载对应的 tunnelblick

1. 安装好以后，MacOS 客户端先进入路由的 SSLVPN 服务，点击 “生成客户端配置” ，将弹出的 tar 文件保存到本地。

**VPN 服务端口**

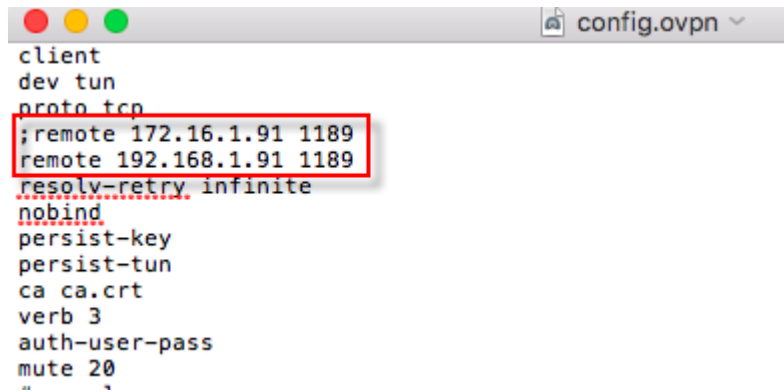
**VPN 子网地址**

**CA 证书状态** 正常 一键生成证书 导出服务端证书 生成客户端配置

**安全参数**

- 允许VPN客户端之间互访
- 允许客户端访问本地局域网
- 允许客户端通过VPN访问Internet

2. 将此 tar 解压缩，进入文件夹中，用文本编辑器修改 config.ovpn 文件，将要连接的 IP 前面的 “;” 去掉，不需要连接 IP 前面加上 “;”

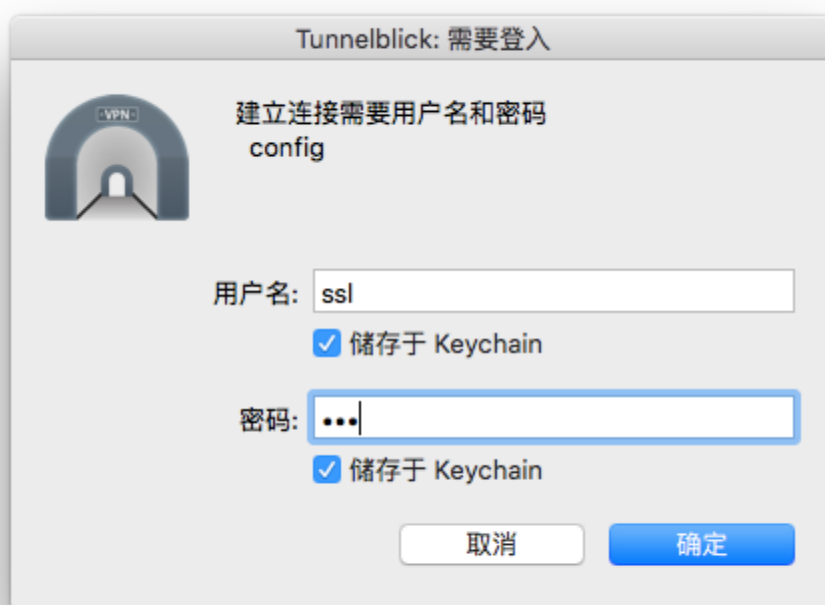


```
client
dev tun
proto tcp
;remote 172.16.1.91 1189
remote 192.168.1.91 1189
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
verb 3
auth-user-pass
mute 20
```

3. 右键点击 config.ovpn 文件并打开，打开方式选择 “Tunnelblick”，系统会自动提示配置已安装，接着点击右上角 tunnelblick 图标，选择 “连接 config”



4. 输入 SSLVPN 的用户名和密码，点击确认



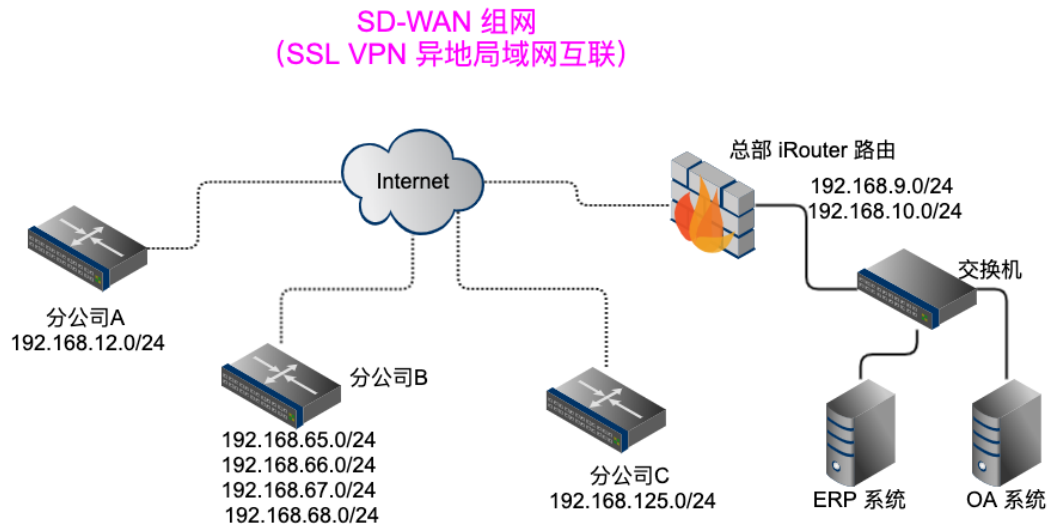
5. 拨号成功后，右上角拨号状态会显示已连接



## SD-WAN 异地局域网互联

本篇主要介绍通过 SSLVPN 实现异地局域网互联，关于 SSL VPN 的常规配置，请参考：[SSL VPN](#)

# 网络拓扑



环境要求：

总部需要有固定公网 IP 的外网线路（可以是 PPPoE 拨号接入，但 IP 必须是固定不变的）。

## 总部服务端配置

### 1. 配置 SSL VPN 服务端参数

协议  UDP (默认)  TCP

VPN 服务端口 1150

VPN 子网地址 10.100.9.0/24 自定义私网地址

CA 证书状态  查看 生成证书 导出 生成客户端配置

自动设置分配给用户的DNS  是

可选参数

- 允许VPN客户端之间互访
- 允许客户端访问本地局域网
- 允许客户端通过VPN访问Internet

全选 / 全不选 将服务端的局域网子网或IP加到这里

推送路由

- 192.168.9.254/255.255.255.0
- 192.168.10.254/255.255.255.0

清空

## 2. 添加 VPN 账号

为每一个分公司创建不同的 VPN 账号。

应用-》本地认证账号-》新建账号：

帐号

密码

可用功能  PPPoE  FTP  PPTP VPN  SSL VPN  
 IPsec/L2TP VPN  Samba/File  SIP/VOIP  
[全选 / 全不选](#)

姓名  ← 可以填写分公司名称

[显示更多选项 >](#)

开通日期  × 日历

账号到期日期  × 日历 7天 ▾

最大同时登录用户数  ← 账号不允许同时登录多次

账号属性中，需要填写分公司的局域网子网地址，且不能有重复：

[分配固定IP](#) 10.100.9.12 可选，为VPN账号分配固定IP

---

[SSL VPN客户端子网地址](#) 192.168.12.0/24 分公司的局域网地址

如果分公司有多个子网，逗号分隔填写：

[分配固定IP](#) 10.100.9.66 如有多个子网，用逗号分隔

---

[SSL VPN客户端子网地址](#) 192.168.65.0/24,192.168.66.0/24,192.168.67.0/24,192.168.68.0/24

最后所有的账号创建完毕如下：

共7条记录/1页, 每页显示 10 请输入关键字  搜索  帐号状态 所有

ID	用户名	姓名	SSL VPN 分配固定IP	使用期限 (开通 - 到期) 上线/下线时间	套餐	备注	状态	编辑	选择
1	hzj		SSLVPN 10.100.9.12 192.168.12.0/24	~ 上线时间: 2020-07-20 07:02:18		杭州...隧道	上线	<input type="button" value="编辑"/>	<input type="checkbox"/>
2	h		SSLVPN 10.100.9.66 192.168.65.0/24 192.168.66.0/24 192.168.67.0/24 192.168.68.0/24	~ 上线时间: 2020-07-21 06:04:20		杭州...隧道	上线	<input type="button" value="编辑"/>	<input type="checkbox"/>
3	j		SSLVPN 10.100.9.126 192.168.125.0/24	~ 上线时间: 2020-07-23 15:10:54		...	上线	<input type="button" value="编辑"/>	<input type="checkbox"/>
4	h		SSLVPN 10.100.9.96 192.168.95.0/24	~ 上线时间: 2020-07-20 07:01:58		...主隧道	上线	<input type="button" value="编辑"/>	<input type="checkbox"/>
5	h		SSLVPN 10.100.9.104 192.168.103.0/24	~ 上线时间: 2020-07-23 07:04:11		...隧道	上线	<input type="button" value="编辑"/>	<input type="checkbox"/>

## 分公司路由配置

网络-》SSLVPN 隧道-》新建连接:

名称: ...SSLVPN

协议:  UDP (默认)  TCP

VPN 服务器地址: ... 服务端IP或域名

VPN 服务端口: 1150 CA 证书

帐号: ...

其他参数:  禁止NAT

检测方法: PING + TCP/SYN (默认)

PING 目标: 10.100.9.1 ← 服务端VPN地址, VPN子网的第一个IP

线路检测的 PING 目标需要填写 VPN 服务端的 IP (VPN 子网的第一个 IP)

连接成功后，状态如下：

<返回> SLVPN > 已连接

SLVPN / tianyun - 连接状态

设备名:	tun0
已连接:	2020-07-12 11:14:02
已连接:	11天5小时7分34秒 <span>断开</span>
IP地址:	10.100.9.222
网关:	10.100.9.221
远程服务器地址:	10.100.9.221

[连接日志](#) / [附加路由表](#)

查看服务端推送的路由表是否正确：

```
10.100.9.0/24 via 10.100.9.221
10.100.9.221 proto kernel scope link src 10.100.9.221
10.100.9.0/24 via 10.100.9.221
10.100.9.0/16 via 10.100.9.221
10.100.9.0/16 via 10.100.9.221
10.100.9.0/16 via 10.100.9.221
10.100.9.0/16 via 10.100.9.221
10.100.9.0/16 via 10.100.9.221
10.100.9.0/24 via 10.100.9.221
192.168.9.248/29 via 10.100.9.221
192.168.10.248/29 via 10.100.9.221
192.168.12.0/24 via 10.100.9.221
192.168.17.0/24 via 10.100.9.221
192.168.65.0/24 via 10.100.9.221
192.168.66.0/24 via 10.100.9.221
192.168.67.0/24 via 10.100.9.221
192.168.68.0/24 via 10.100.9.221
192.168.95.0/24 via 10.100.9.221
192.168.103.0/24 via 10.100.9.221
192.168.125.0/24 via 10.100.9.221
```

## 查看互联状态

在总部服务端查看 VPN 客户端连接状态：



参数设置 连接状态

共7条记录/1页, 每页显示 10 请输入关键字 搜索 清除 自动刷新 2020-07-23 16:25:26

ID	客户端VPN地址 附属子网地址	用户名	远程IP / 端口	上行总流量/下行总流量	建立时间 存活时间	已连接
1	10.100.9.96 机房互通主隧道 192.168.95.0/24		183.141.100.10119 信中心网络	949.93 MB / 2.38 GB	2020-07-20 07:01:58 2020-07-20 07:01:58	3天9小时23分28秒
2	10.100.9.104 隧道 192.168.103.0/24		125.22.32:33788 市电信	157.13 MB / 542.30 MB	2020-07-23 07:01:20 2020-07-23 07:01:20	9小时24分6秒
3	10.100.9.18 隧道 192.168.17.0/24		115.182:49243 市电信	72.72 MB / 254.41 MB	2020-07-22 07:01:06 2020-07-22 07:01:06	1天9小时24分20秒
4	10.100.9.12 隧道 192.168.12.0/24		115.139:39273 市电信	1.11 GB / 85.05 MB	2020-07-20 07:02:18 2020-07-23 16:25:19	3天9小时23分8秒
5	10.100.9.222 天翼云测试隧道 172.16.253.0/24 172.16.253.240	天翼云测试	115.10:5903 浙江省 电信	2.21 GB / 2.02 GB	2020-07-20 07:02:15 2020-07-23 16:25:17	3天9小时23分11秒

## 连通性测试

测试工具：工具-》PING 测试，依次测试如下项：

- 分公司路由上 PING 总部的 VPN IP
- 分公司路由上 PING 总部局域网口 IP
- 分公司路由上 PING 总部局域网内其他设备的 IP
- 分公司路由内网电脑 PING 总部局域网内网 IP （双方局域网内 IP 互访测试）

输入IP或域名 
选择 ▾
PING
路由追踪
MTR

VPN 服务端 IP →

线路  ▾

PING 类型  ▾

[显示更多选项 >](#)



Target IP address: 10.100.9.1 [内部局域网]  
 Default routing interface: tun0 [10.100.9.222]

2020-07-23 16:37:28 Send 10 PING packets via routing policy

```

PING 10.100.9.1 (10.100.9.1): 56 data bytes
64 bytes from 10.100.9.1: seq=0 ttl=64 time=7.465 ms
64 bytes from 10.100.9.1: seq=1 ttl=64 time=7.468 ms
64 bytes from 10.100.9.1: seq=2 ttl=64 time=7.484 ms
64 bytes from 10.100.9.1: seq=3 ttl=64 time=7.542 ms
64 bytes from 10.100.9.1: seq=4 ttl=64 time=7.476 ms
64 bytes from 10.100.9.1: seq=5 ttl=64 time=7.417 ms
64 bytes from 10.100.9.1: seq=6 ttl=64 time=7.438 ms
64 bytes from 10.100.9.1: seq=7 ttl=64 time=7.438 ms
64 bytes from 10.100.9.1: seq=8 ttl=64 time=7.436 ms
64 bytes from 10.100.9.1: seq=9 ttl=64 time=7.414 ms
  
```

Target IP address:  [内部局域网]  
 Default routing interface: tun0 [10.100.9.222]

PING VPN服务端的LAN口IP

2020-07-23 16:56:58 Send 10 PING packets via routing policy

```

PING 192.168.9.254 (192.168.9.254): 56 data bytes
64 bytes from 192.168.9.254: seq=0 ttl=64 time=7.430 ms
64 bytes from 192.168.9.254: seq=1 ttl=64 time=7.470 ms
64 bytes from 192.168.9.254: seq=2 ttl=64 time=7.475 ms
64 bytes from 192.168.9.254: seq=3 ttl=64 time=7.524 ms
64 bytes from 192.168.9.254: seq=4 ttl=64 time=7.506 ms
64 bytes from 192.168.9.254: seq=5 ttl=64 time=7.487 ms
64 bytes from 192.168.9.254: seq=6 ttl=64 time=7.501 ms
64 bytes from 192.168.9.254: seq=7 ttl=64 time=7.458 ms
64 bytes from 192.168.9.254: seq=8 ttl=64 time=7.496 ms
64 bytes from 192.168.9.254: seq=9 ttl=64 time=7.479 ms
  
```

```

--- 192.168.9.254 ping statistics ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 7.430/7.482/7.524 ms
  
```

Target IP address: 192.168.9.250 [内部局域网]  
Default routing interface: tun0 [10.100.9.222]

PING VPN 服务器局域网内的IP

2020-07-23 17:02:59 Send 10 PING packets via routing policy

```
PING 192.168.9.250 (192.168.9.250): 56 data bytes
64 bytes from 192.168.9.250: seq=0 ttl=62 time=7.753 ms
64 bytes from 192.168.9.250: seq=1 ttl=62 time=7.783 ms
64 bytes from 192.168.9.250: seq=2 ttl=62 time=7.748 ms
64 bytes from 192.168.9.250: seq=3 ttl=62 time=7.706 ms
64 bytes from 192.168.9.250: seq=4 ttl=62 time=7.710 ms
64 bytes from 192.168.9.250: seq=5 ttl=62 time=7.798 ms
64 bytes from 192.168.9.250: seq=6 ttl=62 time=7.756 ms
64 bytes from 192.168.9.250: seq=7 ttl=62 time=7.721 ms
64 bytes from 192.168.9.250: seq=8 ttl=62 time=7.773 ms
64 bytes from 192.168.9.250: seq=9 ttl=62 time=7.835 ms

--- 192.168.9.250 ping statistics ---
10 packets transmitted, 10 packets received, 0% packet loss
round-trip min/avg/max = 7.706/7.758/7.835 ms
```

## 隧道带宽性能测试

### 1. 安装性能测试模块

应用-》模块-》检查更新，安装 benchmark 性能测试模块，总部和分公司路由均需安装。

### 2. IPerf 测试

总部开启 Iperf 服务端，分公司运行客户端：

工具

- PING 探测
- 局域网扫描
- 实用工具
- 在线抓包
- 文件管理
- 性能测试**
- 系统体检
- 监测助手

## 性能测试

使用一系列的测试工具对系统及硬件的性能、稳定性进行测试

总部点击这里运行服务端

**IPerf3 服务端**

端口: 默认为5201

IPerf3

分公司点击这里, 分别测试上/下行带宽

**IPerf3 客户端**

服务端地址: 10.100.9.1

IPerf3 上行 IPerf3 下行

端口: 默认为5201  UDP 模式, 发包带宽 默认为10 M

时长: 单位秒, 默认为60

### 3. 查看测试结果

默认测试时间为 1 分钟, 测试结果显示在页面下方:

下载测试:

```

2020-07-23 17:12:05 IPerf3 客户端已启动, 目标 10.100.9.1:5201/TCP, 测试时长 60 秒 【反向测试/对方发包】
2020-07-23 17:13:05 测试完成
[ 5] 36.00-37.00 sec 17.6 MBytes 148 Mbits/sec
[ 5] 37.00-38.00 sec 19.5 MBytes 163 Mbits/sec
[ 5] 38.00-39.00 sec 21.5 MBytes 180 Mbits/sec
[ 5] 39.00-40.00 sec 21.4 MBytes 179 Mbits/sec
[ 5] 40.00-41.00 sec 20.8 MBytes 175 Mbits/sec
[ 5] 41.00-42.00 sec 15.8 MBytes 133 Mbits/sec
[ 5] 42.00-43.00 sec 24.7 MBytes 208 Mbits/sec
[ 5] 43.00-44.00 sec 21.5 MBytes 180 Mbits/sec
[ 5] 44.00-45.00 sec 21.2 MBytes 178 Mbits/sec
[ 5] 45.00-46.00 sec 19.5 MBytes 164 Mbits/sec
[ 5] 46.00-47.00 sec 18.6 MBytes 156 Mbits/sec
[ 5] 47.00-48.00 sec 17.8 MBytes 150 Mbits/sec
[ 5] 48.00-49.00 sec 17.0 MBytes 142 Mbits/sec
[ 5] 49.00-50.00 sec 17.7 MBytes 148 Mbits/sec
[ 5] 50.00-51.00 sec 17.3 MBytes 145 Mbits/sec
[ 5] 51.00-52.00 sec 17.7 MBytes 148 Mbits/sec
[ 5] 52.00-53.00 sec 15.8 MBytes 133 Mbits/sec
[ 5] 53.00-54.00 sec 17.6 MBytes 148 Mbits/sec
[ 5] 54.00-55.00 sec 19.2 MBytes 161 Mbits/sec
[ 5] 55.00-56.00 sec 18.7 MBytes 157 Mbits/sec
[ 5] 56.00-57.00 sec 16.5 MBytes 139 Mbits/sec
[ 5] 57.00-58.00 sec 15.5 MBytes 130 Mbits/sec
[ 5] 58.00-59.00 sec 16.4 MBytes 138 Mbits/sec
[ 5] 59.00-60.00 sec 19.7 MBytes 165 Mbits/sec
-----
[ ID] Interval      Transfer      Bandwidth      Retr
[ 5]  0.00-60.00  sec  1.15 GBytes  165 Mbits/sec  101545
[ 5]  0.00-60.00  sec  1.15 GBytes  164 Mbits/sec

```

上传测试:

```

2020-07-23 17:17:42 IPerf3 客户端已启动, 目标 10.100.9.1:5201/TCP, 测试时长 60 秒【本地发包】
2020-07-23 17:18:42 测试完成
[ 5] 36.00-37.00 sec 21.2 MBytes 178 Mbits/sec 0 402 KBytes 上传测试
[ 5] 37.00-38.00 sec 21.2 MBytes 178 Mbits/sec 0 402 KBytes
[ 5] 38.00-39.00 sec 21.2 MBytes 178 Mbits/sec 0 405 KBytes
[ 5] 39.00-40.00 sec 21.2 MBytes 178 Mbits/sec 0 407 KBytes
[ 5] 40.00-41.00 sec 17.5 MBytes 147 Mbits/sec 0 776 KBytes
[ 5] 41.00-42.00 sec 23.8 MBytes 199 Mbits/sec 2780 402 KBytes
[ 5] 42.00-43.00 sec 21.2 MBytes 178 Mbits/sec 0 402 KBytes
[ 5] 43.00-44.00 sec 22.5 MBytes 189 Mbits/sec 0 402 KBytes
[ 5] 44.00-45.00 sec 21.2 MBytes 178 Mbits/sec 0 400 KBytes
[ 5] 45.00-46.00 sec 21.2 MBytes 178 Mbits/sec 0 400 KBytes
[ 5] 46.00-47.00 sec 21.2 MBytes 178 Mbits/sec 0 381 KBytes
[ 5] 47.00-48.00 sec 21.2 MBytes 178 Mbits/sec 0 400 KBytes
[ 5] 48.00-49.00 sec 21.2 MBytes 178 Mbits/sec 0 402 KBytes
[ 5] 49.00-50.00 sec 21.2 MBytes 178 Mbits/sec 0 402 KBytes
[ 5] 50.00-51.00 sec 18.8 MBytes 157 Mbits/sec 0 5.26 KBytes
[ 5] 51.00-52.00 sec 23.8 MBytes 199 Mbits/sec 3108 407 KBytes
[ 5] 52.00-53.00 sec 21.2 MBytes 178 Mbits/sec 0 421 KBytes
[ 5] 53.00-54.00 sec 21.2 MBytes 178 Mbits/sec 0 407 KBytes
[ 5] 54.00-55.00 sec 21.2 MBytes 178 Mbits/sec 0 405 KBytes
[ 5] 55.00-56.00 sec 21.2 MBytes 178 Mbits/sec 0 431 KBytes
[ 5] 56.00-57.00 sec 21.2 MBytes 178 Mbits/sec 0 405 KBytes
[ 5] 57.00-58.00 sec 21.2 MBytes 178 Mbits/sec 0 415 KBytes
[ 5] 58.00-59.00 sec 21.2 MBytes 178 Mbits/sec 0 429 KBytes
[ 5] 59.00-60.00 sec 21.2 MBytes 178 Mbits/sec 0 405 KBytes
-----
[ ID] Interval      Transfer      Bandwidth    Retr
[ 5]  0.00-60.00 sec 1.25 GBytes  179 Mbits/sec 15678
[ 5]  0.00-60.00 sec 1.25 GBytes  179 Mbits/sec

```

测试的时候在首页查看线路的实时流量：

线路/设备名	IP地址/子网掩码	网关	累计上传/下载	上/下行实时流量	连接状态
SSLVPN-/VPN tun0	10.100.9.222 公网IP 61.	10.100.9.221 浙江电信	6.00 GB/8.21 GB	197.41 Mbps / 3.81 Mbps	11天6小时4分35秒 » 61.1%
WAN1 wan1	172.16.0.2 / 29 公网IP 115.	172.16.0.1 浙江电信	96.92 GB/148.86 GB	206.79 Mbps / 8.84 Mbps	

## VPN 带宽实战测试 2

## VPN 服务端 50M 专线:

2020-08-19 09:34:14 Speedtest 带宽测速 VPN服务端50Mbps专线  
出口线路 wan1 => 61.100.110.110 江苏省无锡市 电信

Speedtest by Ookla

Selecting server:

- 5396: 4.61 ms; 中国 电信 JiangSu 5G - 苏州
- 30852: 42.71 ms; Duke Kunshan University - 昆山
- 24447: 9.54 ms; 中国 联通 5G - 上海
- 3633: 7.88 ms; 中国 电信 - 上海
- 7509: 9.62 ms; 中国 电信 ZheJiang Branch - 杭州
- 5317: 4.55 ms; 江苏电信5G - Nanjing
- 13704: 4.21 ms; 中国 联通 - Nanjing
- 27249: 13.91 ms; 中国 移动 jiangsu 5G - Nanjing
- 26352: 3.56 ms; 中国 电信 JiangSu 5G - Nanjing
- 34986: 157.13 ms; Jelly Digital Internet - Chula Vista, CA

Server: 中国 电信 JiangSu 5G - Nanjing (id = 26352)  
ISP: 中国 电信

Latency: 4.31 ms (0.27 ms )

Download: 47.15 Mbps (data used: 30.2 MB)

Upload: 47.35 Mbps (data used: 73.3 MB)

Packet Loss: 0.0%

Result URL: <https://www.speedtest.net/result/c/cb732d19-fb14-4a8c-8274-5ccd1c65440d>  
[查看测速详情](#)

## VPN 客户端带宽测试:

WAN口线路 <共 2 条>		SSLVPN客户端				
线路/设备名	IP地址/子网掩码	网关	累计上传/下载	上/下行实时流量	连接状态	
SSLVPN-tun0	10.10.0.110	10.10.0.109 No NAT	326.91 MB/818.43 MB	0.14 Mbps / 0.35 Mbps	32分56秒 » 61.100.110.110	

## 下行带宽测试:

2020-08-19 09:36:17 IPerf3 客户端已启动, 目标 10.10.0.1:5201/TCP, 测试时长 60 秒 【反向测试/对方发包】

2020-08-19 09:37:18 测试完成

```
[ 5] 36.00-37.00 sec 5.32 MBytes 44.6 Mbbits/sec
[ 5] 37.00-38.00 sec 5.30 MBytes 44.5 Mbbits/sec
[ 5] 38.00-39.00 sec 5.32 MBytes 44.6 Mbbits/sec
[ 5] 39.00-40.00 sec 5.28 MBytes 44.3 Mbbits/sec
[ 5] 40.00-41.00 sec 4.31 MBytes 36.2 Mbbits/sec
[ 5] 41.00-42.00 sec 5.35 MBytes 44.9 Mbbits/sec
[ 5] 42.00-43.00 sec 4.96 MBytes 41.6 Mbbits/sec
[ 5] 43.00-44.00 sec 5.08 MBytes 42.6 Mbbits/sec
```

```

[ 5] 44.00-45.00 sec 4.49 MBytes 37.7 Mb/s/sec
[ 5] 45.00-46.00 sec 5.30 MBytes 44.5 Mb/s/sec
[ 5] 46.00-47.00 sec 5.31 MBytes 44.5 Mb/s/sec
[ 5] 47.00-48.00 sec 5.29 MBytes 44.4 Mb/s/sec
[ 5] 48.00-49.00 sec 5.31 MBytes 44.6 Mb/s/sec
[ 5] 49.00-50.00 sec 5.31 MBytes 44.6 Mb/s/sec
[ 5] 50.00-51.00 sec 5.18 MBytes 43.4 Mb/s/sec
[ 5] 51.00-52.00 sec 5.31 MBytes 44.6 Mb/s/sec
[ 5] 52.00-53.00 sec 4.94 MBytes 41.5 Mb/s/sec
[ 5] 53.00-54.00 sec 5.24 MBytes 44.0 Mb/s/sec
[ 5] 54.00-55.00 sec 5.30 MBytes 44.5 Mb/s/sec
[ 5] 55.00-56.00 sec 5.30 MBytes 44.5 Mb/s/sec
[ 5] 56.00-57.00 sec 5.31 MBytes 44.5 Mb/s/sec
[ 5] 57.00-58.00 sec 5.22 MBytes 43.8 Mb/s/sec
[ 5] 58.00-59.00 sec 5.30 MBytes 44.4 Mb/s/sec
[ 5] 59.00-60.00 sec 5.30 MBytes 44.4 Mb/s/sec

```

```

-----
[ ID] Interval          Transfer      Bandwidth      Retr
[ 5]  0.00-60.00 sec    310 MBytes  43.3 Mb/s/sec    0
[ 5]  0.00-60.00 sec    309 MBytes  43.2 Mb/s/sec

```

iperf Done.

## 上行带宽测试:

2020-08-19 09:44:22 IPerf3 客户端已启动, 目标 10.10.0.1:5201/TCP, 测试时长 60 秒【本地发包】

2020-08-19 09:45:23 测试完成

```

[ 5] 36.00-37.00 sec 5.17 MBytes 43.4 Mb/s/sec 0 116 KBytes
[ 5] 37.00-38.00 sec 5.17 MBytes 43.4 Mb/s/sec 0 123 KBytes
[ 5] 38.00-39.00 sec 3.88 MBytes 32.5 Mb/s/sec 0 60.4 KBytes
[ 5] 39.00-40.00 sec 4.31 MBytes 36.1 Mb/s/sec 0 108 KBytes
[ 5] 40.00-41.00 sec 5.17 MBytes 43.4 Mb/s/sec 0 113 KBytes
[ 5] 41.00-42.00 sec 5.17 MBytes 43.4 Mb/s/sec 1 99.8 KBytes
[ 5] 42.00-43.00 sec 3.88 MBytes 32.5 Mb/s/sec 0 110 KBytes
[ 5] 43.00-44.00 sec 5.17 MBytes 43.4 Mb/s/sec 0 131 KBytes
[ 5] 44.00-45.00 sec 5.17 MBytes 43.4 Mb/s/sec 0 105 KBytes
[ 5] 45.00-46.00 sec 5.17 MBytes 43.4 Mb/s/sec 0 113 KBytes
[ 5] 46.00-47.00 sec 4.74 MBytes 39.7 Mb/s/sec 0 99.8 KBytes
[ 5] 47.00-48.00 sec 4.31 MBytes 36.1 Mb/s/sec 0 108 KBytes
[ 5] 48.00-49.00 sec 5.17 MBytes 43.4 Mb/s/sec 0 110 KBytes
[ 5] 49.00-50.00 sec 3.01 MBytes 25.3 Mb/s/sec 0 86.6 KBytes
[ 5] 50.00-51.00 sec 4.31 MBytes 36.1 Mb/s/sec 0 94.5 KBytes
[ 5] 51.00-52.00 sec 5.17 MBytes 43.4 Mb/s/sec 0 91.9 KBytes

```



```

[ 5] 52.00-53.00 sec 5.17 MBytes 43.4 Mb/s 0 81.4 KBytes
[ 5] 53.00-54.00 sec 5.17 MBytes 43.4 Mb/s 0 91.9 KBytes
[ 5] 54.00-55.00 sec 5.17 MBytes 43.4 Mb/s 0 91.9 KBytes
[ 5] 55.00-56.00 sec 3.01 MBytes 25.3 Mb/s 0 49.9 KBytes
[ 5] 56.00-57.00 sec 5.17 MBytes 43.4 Mb/s 0 113 KBytes
[ 5] 57.00-58.00 sec 5.17 MBytes 43.4 Mb/s 0 94.5 KBytes
[ 5] 58.00-59.00 sec 5.17 MBytes 43.4 Mb/s 0 91.9 KBytes
[ 5] 59.00-60.00 sec 3.01 MBytes 25.3 Mb/s 0 28.9 KBytes
-----
[ ID] Interval      Transfer    Bandwidth    Retr
[ 5]  0.00-60.00  sec  289 MBytes 40.4 Mb/s    1          sender
[ 5]  0.00-60.00  sec  288 MBytes 40.3 Mb/s    0          receiver

iperf Done.

```

## VPN 客户端访问 VPN 服务端局域网内文件共享服务器：

[网上邻居文件共享](#)

VPN服务器LAN内文件服务器

服务端地址: 192.168.200.212

浏览共享

登录账号/密码: 格式: 账号 密码, 为空表示游客身份登录

文件路径: /h/201.bak

文件测试

列出目录文件

```

2020-08-19 12:26:53  连接到 //192.168.200.212/h, 目标目录 /

获取目标文件信息 ... /201.bak
目标文件大小 335.73 MB
当前空闲内存大小 3311 MB
发现空闲磁盘 /disk/cache, 可用空间 870.02 GB
下载文件到内存
下载文件 /201.bak ... 存储位置 /tmp
Domain=[WIN-4N0064H0SVP] OS=[Windows Server 2016 Datacenter 14393] Server=[Windows_Server_2016_Datacenter_6.3]
getting file \201.bak of size 352038400 as smb.tmpfile (5.1 MBytes/s) 【平均下载速度 5.1 MBytes/s】
Current directory is \
2020-08-19 12:28:00  下载完成, 大小 335.73 MB

上传文件 /201.bak => /201.bak.1
Domain=[WIN-4N0064H0SVP] OS=[Windows Server 2016 Datacenter_14393] Server=[Windows_Server_2016_Datacenter_6.3]
putting file smb.tmpfile as \201.bak.1 (4.9 MBytes/s) 【平均上传速度 4.9 MBytes/s】
Current directory is \

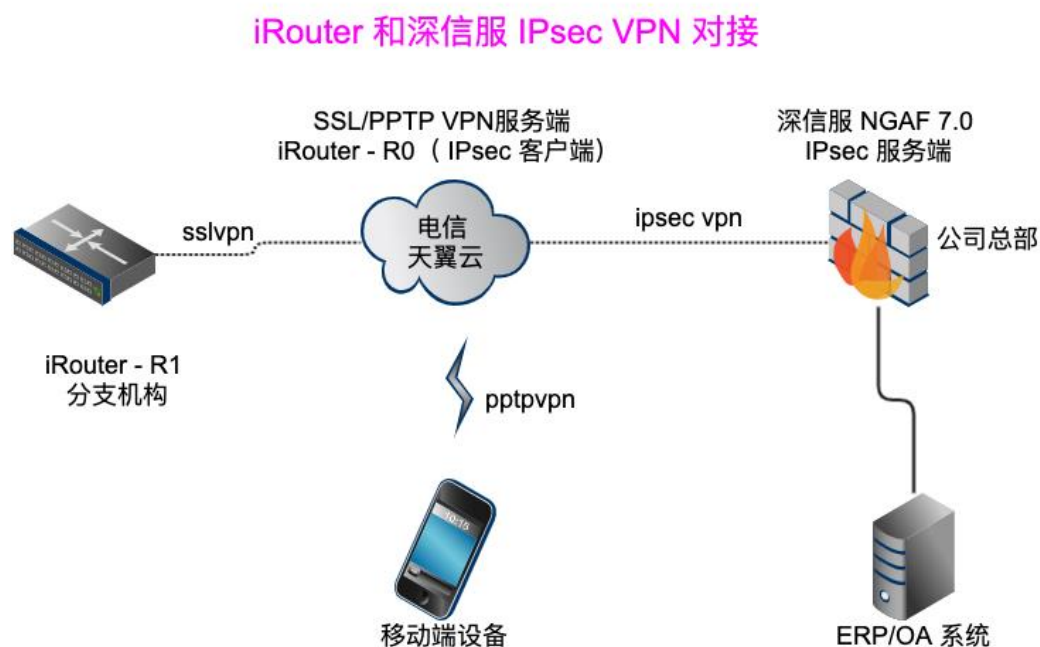
```

小结: 50Mbps 带宽, VPN 能跑到 40~44Mbps

# IPsec 隧道和深信服对接

iRouter 路由作为 IPsec 客户端，和深信服 NGAF 服务端对接。

## 网络拓扑



iRouter 路由-R0 为云端路由，部署在电信天翼云上，通过 IPsec 隧道和总部的深信服对接，同时充当 SSL VPN 和 PPTP VPN 服务端

分支机构的路由 R1 通过 SSL VPN 接入到路由 R0，中转访问总部。

移动端手机或 PAD 通过 PPTP VPN 拨号到路由 R0，中转访问总部。

## 深信服上的配置

### 1. 第一阶段：

The screenshot displays the configuration interface for the first stage of a VPN setup. The left sidebar shows the navigation menu with 'VPN' expanded and 'IPSecVPN' selected. Under 'IPSecVPN', '第三方对接' (Third-party connection) is highlighted, and '第一阶段' (First stage) is selected. The main area is titled '第一阶段' and contains several configuration fields:

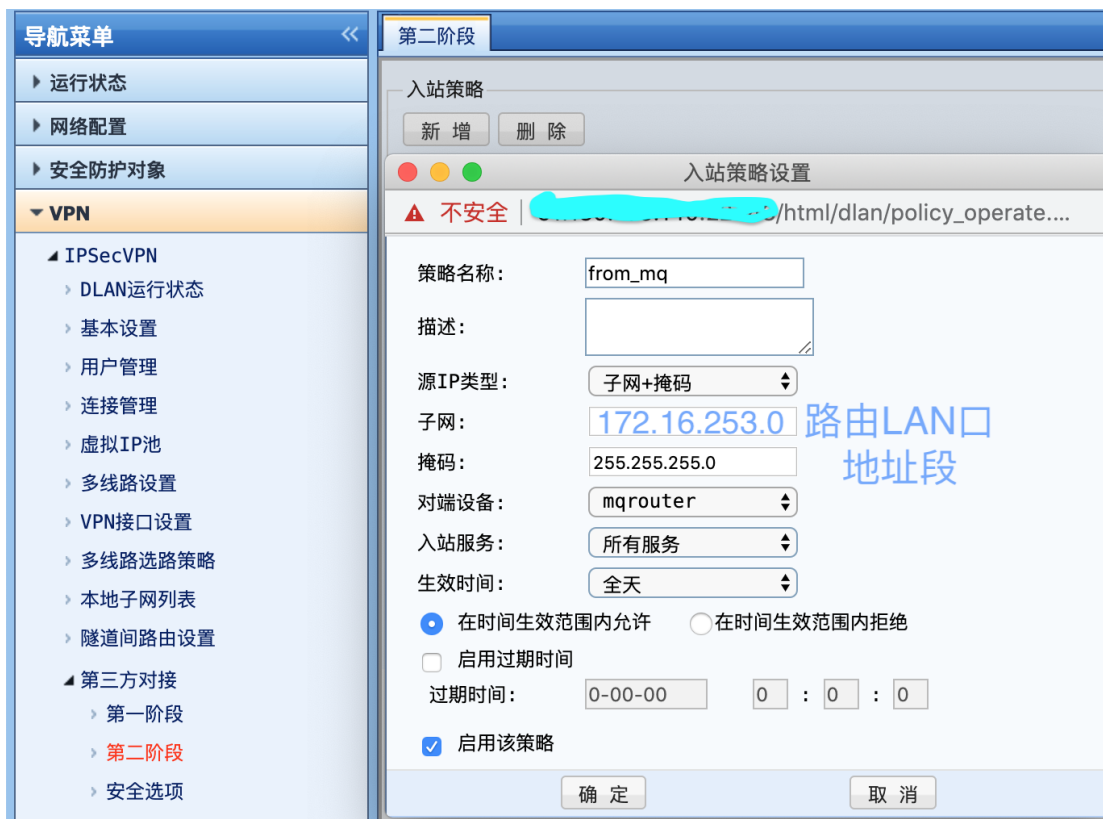
- 新增** (Add) button is highlighted with a blue box and labeled (2).
- 设备名称** (Device name): mqrouter
- 设备地址类型** (Device address type): 对端是动态IP (Peer is dynamic IP)
- 认证方式** (Authentication method): Pre-shared key (预共享密钥) and Confirm key (确认密钥) fields are present.
- 预共享密钥** (Pre-shared key) and **确认密钥** (Confirm key) fields are highlighted with blue boxes.
- 启用设备** (Enable device) checkbox is checked and highlighted with a blue box and labeled (3). A red arrow points to the **启用主动连接** (Enable active connection) checkbox.
- 高级** (Advanced) button is highlighted with a blue box and labeled (5).
- 确定** (OK) button is highlighted with a blue box and labeled (4).

On the right side, the ISAKMP configuration is shown:

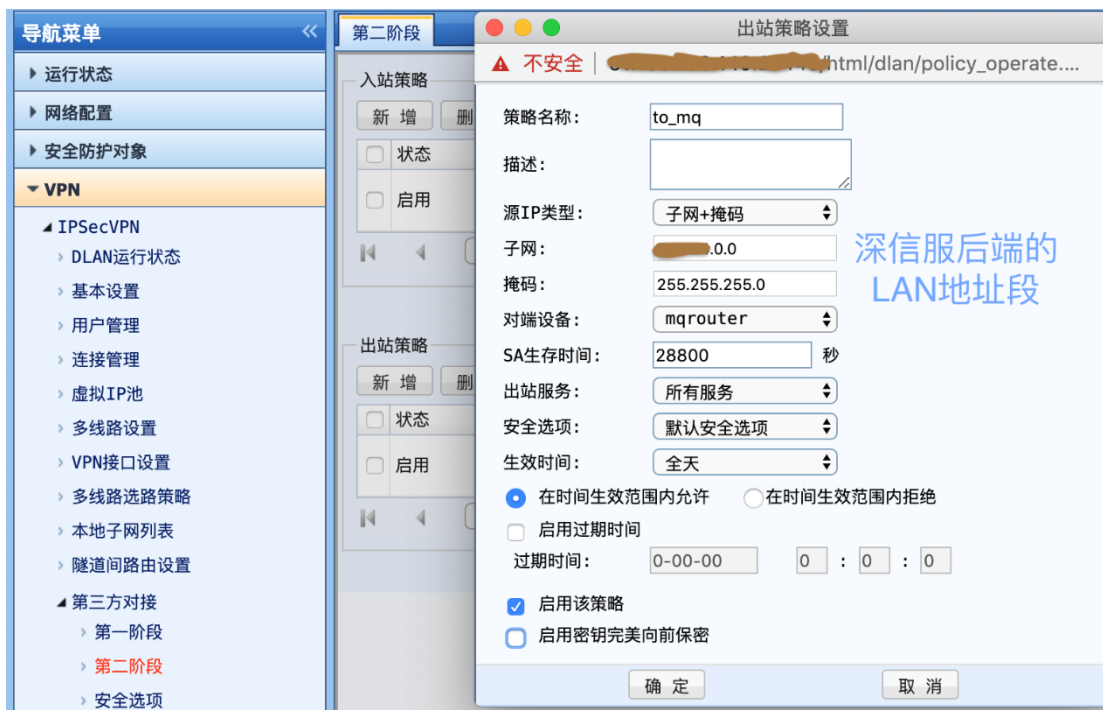
- ISAKMP存活时间** (ISAKMP lifetime): 3600 秒
- 重试次数** (Retries): 10
- 支持模式** (Supported modes): 野蛮模式 (Aggressive mode)
- D-H群** (D-H groups): MODP1024群 (2)
- 我方身份类型** (My identity type): 域名字符串 (FQDN)
- 我方身份ID** (My identity ID): sangfor
- 对端身份类型** (Peer identity type): 域名字符串 (FQDN)
- 对方身份ID** (Peer identity ID): mq
- 启用DPD** (Enable DPD) checkbox is checked.
- DPD设置** (DPD settings):
  - 检测间隔** (Detection interval): 5 秒 (5-60)
  - 超时次数** (Timeout count): 5 次 (1-6)
- ISAKMP算法列表** (ISAKMP algorithm list):
  - 认证算法** (Authentication algorithm): MD5
  - 加密算法** (Encryption algorithm): 3DES
- 确定** (OK) button is highlighted with a blue box.

### 2. 第二阶段：

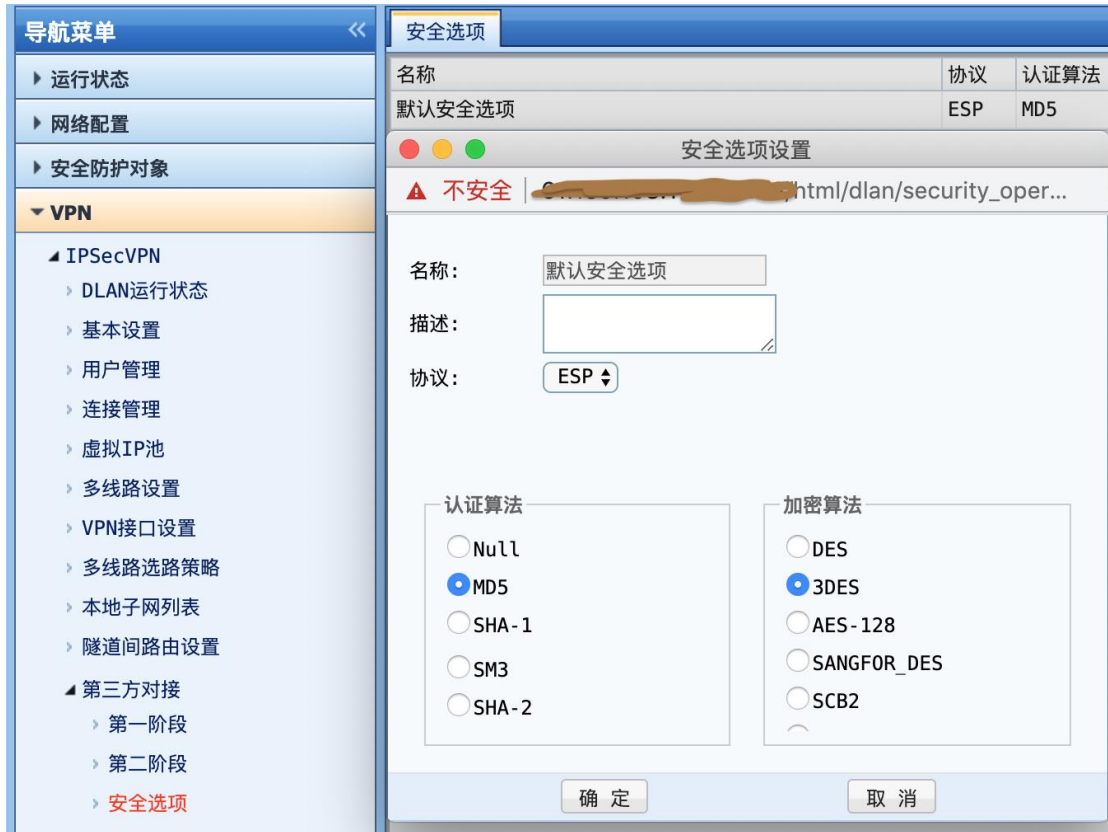
进站策略：添加对端 R0 路由的 LAN 字网地址



出站策略：添加总部 LAN 子网地址，如果有多个，可以添加多条策略



### 3.安全选项：默认即可



## 路由上的配置

进入应用-》模块-》检查更新，安装 IPsecVPN 模块。

进入网络-》IPSec 隧道，创建连接：

名称

线路 wan1 <wan1/172.16.0.2  电信> ▾

远程服务器地址  总部深信服IP或域名

本地标识 mq

对方标识 sangfor

本地LAN子网地址 172.16.253.0/24

对端LAN子网地址

IKE 协商 野蛮模式 ▾ IKEv1 ▾ MD5 ▾ 3DES ▾ MODP1024 ▾

IKE 生存时间 3600 秒

预共享密钥  和总部设为一致，字母数字组成即可

ESP 加密算法 MD5 ▾ 3DES ▾

ESP 生存时间 8 小时

存活检测IP .0.9 填写总部可以访问的设备IP，可选

备注 总部线路

激活

等待隧道建立连接：

## IPsec 隧道

创建 IPsec 隧道

共1条记录/1页, 每页显示 10 请输入关键字 搜索 Q 清除 x 新建连接 自动刷新

ID	名称 状态	远程服务器地址 远端LAN子网	本地IP 本地LAN子网	备注	激活	编辑	选择
1	<a href="#">连接详情</a>	172.16.0.0/24 172.16.0.0/16 172.16.0.0/16 172.16.0.0/16 172.16.0.0/16	wan1 172.16.253.0/24		<input checked="" type="checkbox"/>	<a href="#">编辑</a>	<input type="checkbox"/>

专家模式 导出规则 全选 / 全不选 刷新 删除

共1条记录/1页, 每页显示 10 请输入关键字 搜索 Q 清除 x 新建连接 自动刷新

ID	名称 状态	备注	激活	编辑	选择
1	<a href="#">连接详情</a>		<input checked="" type="checkbox"/>	<a href="#">编辑</a>	<input type="checkbox"/>

**IPsec 隧道详情**

本地: 172.16.0.2  
对端: 172.16.253.0/24  
连接时间: 2 minutes  
上行流量: 0.16 KB / 2 pkts  
下行流量: 0.16 KB / 2 pkts

专家模式 导出规则 全选 / 全不选 刷新 删除

连接成功后，在深信服也可以看到状态：

导航菜单 << DLAN运行状态

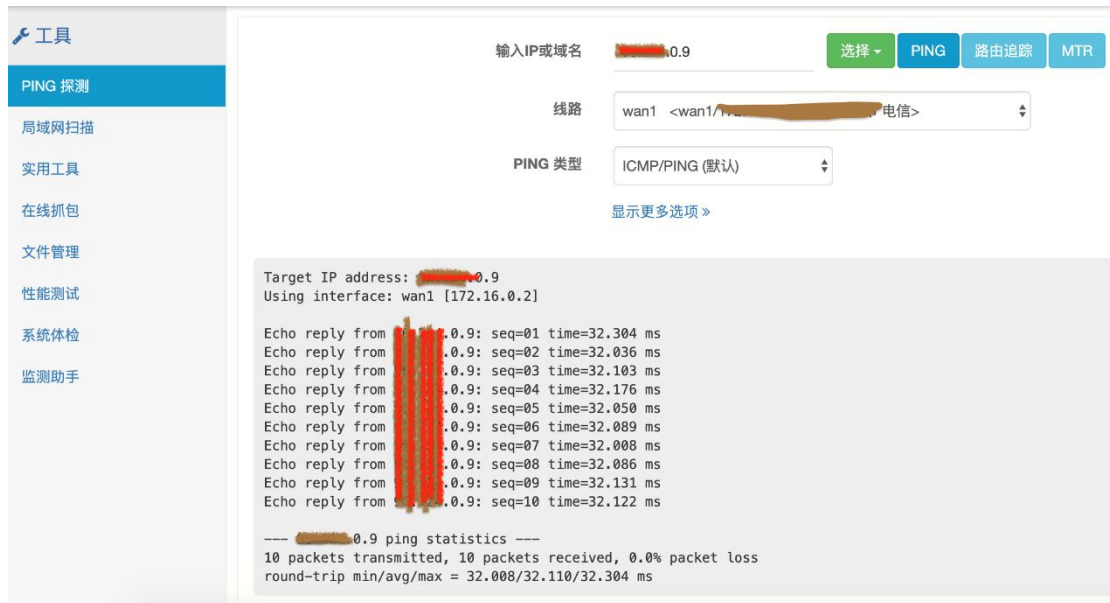
当前VPN状态: 运行中 当前连接总数: 1 第三方剩余授权: [49] 移动用户剩余授权: [0]

外网流量: 接收: 0 Byte/s 发送: 0 Byte/s  
VPN流量: 接收: 84 Byte/s 发送: 136 Byte/s

每页显示条数: 50 << >> 1/1 页 共1 条 第1页 分支NAT状态 刷新状态 显示选项 停止服务 用户模糊搜索

断开连接	连接名称	用户名	描述	类型	实时流量 (接收/发送)	Internet IP	内网IP	接入时间	传输类型
<input checked="" type="checkbox"/>	to_mq-from_mq	mqrouter	第三方设备	84/136			172.16.253.0	2020-03-22 22:17:19	IPSEC_ESP

最后在路由上使用 PING 测试工具验证下：



## 其他说明

- 1.标准 IPSEC 不允许连接的双方都是动态 IP , 只能允许其中一方为动态 IP
- 2.一方是公网部署有公网 ip, 一方是路由部署 (前方设备映射的公网 ip) , 必须要使用野蛮模式连接, 本文就是这种场景。

## VTUN 隧道

VTUN 提供点对点的隧道服务, 基于 UDP 协议, 支持 AES-128/AES-256 加密。



## 服务端配置

服务端需安装 vtun\_server 模块

进入菜单：应用-》模块-》检查更新，找到 “vtun\_server “ 模块，点击安装。

完成后，进入菜单：应用-》VTUN 服务，配置如下：

<input checked="" type="checkbox"/> VTUN 隧道服务	VTUN 服务配置
服务运行状态	运行中 <PID: 13322>
线路	wan1 <wan1/103.103.103.103 亚太地区> ▼
监听端口	10011 <a href="#">端口自定义</a>
本地IP	10.101.0.1 <a href="#">IP自定义，和LAN及VPN不重复即可</a>
<a href="#">VTUN 共享密钥</a>	test123456
加密算法	AES-128 ▼
可选参数	<input checked="" type="checkbox"/> 允许客户端通过隧道访问Internet

## 客户端配置

客户端无需安装模块，路由默认内置，进入菜单：网络-》VTUN 隧道：

隧道接口名	lamo	数字、字母组成
远程服务器地址	103.10.10.10	服务器IP
端口	10011	端口
本地IP	10.101.0.100	本地隧道IP (和服务端隧道IP同网段)
远程IP	10.101.0.1	服务端隧道IP
最大传输单元(MTU)	1300	
密码	test123456	和服务端相同
加密算法	AES-128	

连接成功后，可以看到状态：

共1条记录/1页, 每页显示 10 请输入关键字     隧道连接状态

ID	名称	远程服务器地址	端口	本地IP	远程IP	备注	状态	激活	编辑	选择
1	lamo	103.10.10.10	10011	10.101.0.100	10.101.0.1		224.34 ms	<input checked="" type="checkbox"/>	<input type="button" value="编辑"/>	<input type="checkbox"/>

## 通过隧道访问 Google

预设条件：服务端所在的当地线路，能合法地访问 Google。

### 1. 设置 DNS 重定向规则

网络-》DNS 参数-》DNS 代理/缓存，启用强制 DNS 代理：

DNS 参数

DNS 代理/缓存

DNS 过滤

服务运行状态

运行中 <PID: 11287>

启用 DNS 本地缓存及加速

开

启用强制客户端使用 DNS 代理

是

然后勾选“启用域名重定向”，添加规则如下：

```
google url=https://raw.githubusercontent.com/googlehosts/hosts/master/hosts-files/hosts
```

启用域名重定向

是

DNS 重定向

域名重定向记录

```
google
url=https://raw.githubusercontent.com/googlehosts/hosts/master/hosts-files/hosts
```

清空

注：初次配置系统会下载 google 服务器相关的 dns 解析文件，根据网络的快慢，可能需要 1-3 分钟不等。

## 2. 设置多线规则

路由-》多线负载策略：

启用多线负载及策略

多线配置

线路分组

自定义策略

路由表

VTUN隧道禁止自动负载

ID	线路	连接状态 (网卡/设备名/IP)	线路类型	负载权重	禁止自动负载
1	VTUN-1	vtun.lan /o/10.101.0.100 <亚太地区>	默认线路	1	<input checked="" type="checkbox"/>
2	WAN-1	wan1/219... <山东...市电信>	默认线路	1	<input type="checkbox"/>
3	WAN-2	wan2/ppw0/144... <山东...市电信>	默认线路	1	<input type="checkbox"/>

## 自定义策略-》新增规则:

访问google服务器走VTUN线路

名称: google

优先级: 1

协议: TCP+UDP

线路: vtun.lan /o <vtun.lan /o/10.101.0.100 亚太地区>

源IP: [ ] = IP 类型 =

目的IP: @google = IP 类型 =

@后面的名字和域名重定向对应

## 最终规则如下:

多线配置 线路分组 自定义策略 路由表

共1条记录/1页, 每页显示 10 请输入关键字 搜索 清除 新增规则

ID	优先级	名称	协议	源IP - 源端口	目的IP - 目的端口	备注	线路	状态	编辑	选择
1	1	google	所有	:	@google:		vtun.lan /o	<input checked="" type="checkbox"/>		<input type="checkbox"/>

**注：本策略只能用于访问 Google 搜索、Gmail 邮箱服务，仅供学**

**习、研究参考，请遵守计算机及互联网相关法律法规。**

## 隧道性能测试

测试环境：隧道使用 AES256 加密，服务端 400Mbps 上下对等，客户端 200Mbps 上下对等带宽。

测试工具：iRouter 自带性能测试模块之 [IPerf 网络测试](#)

2020-08-15 20:35:45 IPerf3 客户端已启动, 目标 10.253.9.1:5201/TCP, 测试时长 3600 秒 【反向测试/对方发包】

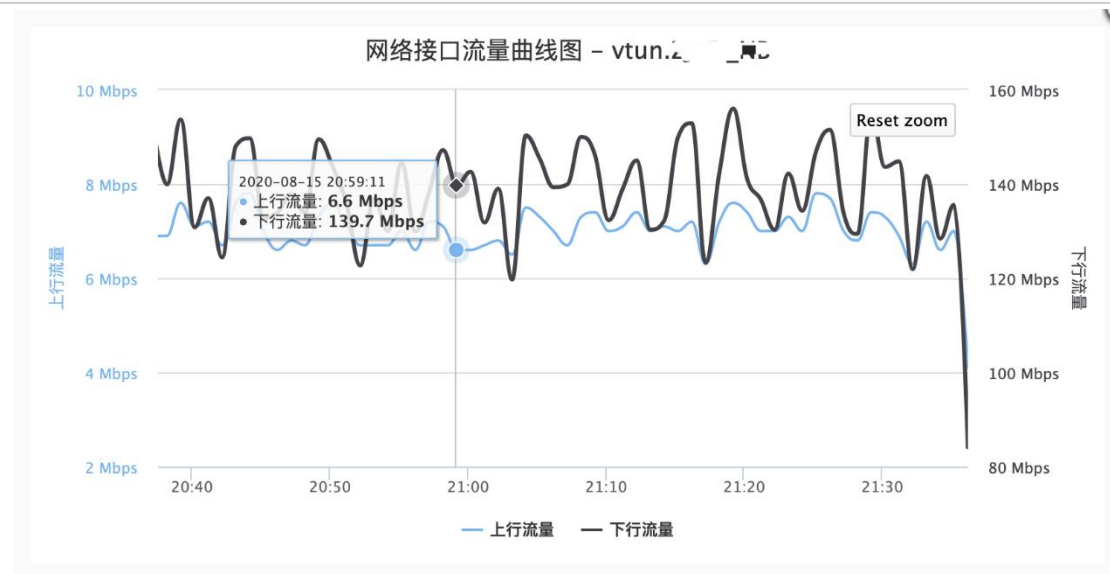
2020-08-15 21:35:46 测试完成

[ 5]	3576.00-3577.00 sec	18.4 MBytes	154 Mbbits/sec
[ 5]	3577.00-3578.00 sec	18.4 MBytes	155 Mbbits/sec
[ 5]	3578.00-3579.00 sec	18.3 MBytes	153 Mbbits/sec
[ 5]	3579.00-3580.00 sec	17.9 MBytes	150 Mbbits/sec
[ 5]	3580.00-3581.00 sec	17.0 MBytes	143 Mbbits/sec
[ 5]	3581.00-3582.00 sec	18.3 MBytes	153 Mbbits/sec
[ 5]	3582.00-3583.00 sec	14.7 MBytes	124 Mbbits/sec
[ 5]	3583.00-3584.00 sec	18.2 MBytes	153 Mbbits/sec
[ 5]	3584.00-3585.00 sec	19.0 MBytes	159 Mbbits/sec
[ 5]	3585.00-3586.00 sec	19.3 MBytes	162 Mbbits/sec
[ 5]	3586.00-3587.00 sec	19.1 MBytes	161 Mbbits/sec
[ 5]	3587.00-3588.00 sec	18.8 MBytes	158 Mbbits/sec
[ 5]	3588.00-3589.00 sec	18.8 MBytes	158 Mbbits/sec
[ 5]	3589.00-3590.00 sec	18.4 MBytes	154 Mbbits/sec
[ 5]	3590.00-3591.00 sec	14.4 MBytes	120 Mbbits/sec
[ 5]	3591.00-3592.00 sec	14.2 MBytes	119 Mbbits/sec
[ 5]	3592.00-3593.00 sec	15.4 MBytes	129 Mbbits/sec
[ 5]	3593.00-3594.00 sec	16.2 MBytes	136 Mbbits/sec
[ 5]	3594.00-3595.00 sec	16.1 MBytes	135 Mbbits/sec
[ 5]	3595.00-3596.00 sec	18.7 MBytes	157 Mbbits/sec
[ 5]	3596.00-3597.00 sec	19.9 MBytes	167 Mbbits/sec
[ 5]	3597.00-3598.00 sec	15.1 MBytes	127 Mbbits/sec
[ 5]	3598.00-3599.00 sec	18.8 MBytes	157 Mbbits/sec
[ 5]	3599.00-3600.00 sec	18.6 MBytes	156 Mbbits/sec

-----

[ ID]	Interval	Transfer	Bandwidth	Retr	
[ 5]	0.00-3600.00 sec	57.9 GBytes	138 Mbits/sec	5971940	sender
[ 5]	0.00-3600.00 sec	57.9 GBytes	138 Mbits/sec		receiver

iperf Done.



## 性能测试

### 功能介绍

使用一系列的测试工具对系统及硬件的性能、稳定性进行测试，测试对象包括：网卡、CPU、内存、磁盘及综合评分测试。

### 安装模块

进入“应用” -》“模块管理”，点击“检查更新”，安装“benchmark” 模块



基准测试工具套件  
使用一系列的测试工具对系统及硬件的性能、稳定性进行测试。  
[更多...](#)

1.1.89  
2020-10-21 17:29:17

4.77 MB  
22.32 MB

## PCIe 总线性能

PCI Express 总线性能<sup>[2][3]</sup>

PCI Express 版本	推出	Line 编码	原始传输率 <sup>[1]</sup>	带宽 (带宽) <sup>[1]</sup>				
				x1	x2	x4	x8	x16
1.0	2003	8b/10b	2.5 GT/s	250 MB/s	0.50 GB/s	1.0 GB/s	2.0 GB/s	4.0 GB/s
2.0	2007	8b/10b	5.0 GT/s	500 MB/s	1.0 GB/s	2.0 GB/s	4.0 GB/s	8.0 GB/s
3.0	2010	128b/130b	8.0 GT/s	984.6 MB/s	1.97 GB/s	3.94 GB/s	7.88 GB/s	15.8 GB/s
4.0	2017	128b/130b	16.0 GT/s	1969 MB/s	3.94 GB/s	7.88 GB/s	15.75 GB/s	31.5 GB/s
5.0 <sup>[5][6]</sup>	2019 <sup>[7][8]</sup>	NRZ 128b/130b	32.0 GT/s <sup>[11]</sup>	3938 MB/s	7.88 GB/s	15.75 GB/s	31.51 GB/s	63.0 GB/s
6.0	2021	PAM4 & FEC 128b/130b	64.0 GT/s	7877 MB/s	15.75 GB/s	31.51 GB/s	63.02 GB/s	126.03 GB/s

i. <sup>1</sup> 1.0<sup>1.1</sup> 每条通道 (lane) 是全双工通道。

ii. <sup>2</sup> 出于技术可行性，最初也考虑过25.0 GT/s

以PCIe 2.0为例，每秒5GT (Gigatransfer) 原始数据传输率，编码方式为8b/10b (每10个比特只有8个有效数据)，即有效带宽为4Gb/s = 500MByte/s。

更多信息参考: [PCI Express 规范](#)

## USB 3.0 磁盘性能测试

2020-07-25 16:36:36 开始磁盘 /disk/xxx 性能测试  
共8项，每项测试时间：30 秒，临时文件大小：2G

USB3.0 32G Sandisk U盘

2020-07-25 16:42:32 测试完成，总耗时 5分56秒

测试结果：

	读 (MB/s   IOPS)		写 (MB/s   IOPS)	
Seq 顺序	128MiB/s	123	35.5MiB/s	31
512K 随机	115MiB/s	225	19.1MiB/s	36
4K 随机	5232KiB/s	1303	892KiB/s	219
4K-QD32 随机	5271KiB/s	1316	677KiB/s	168

## NVME SSD 磁盘测试

### 磁盘I/O测试

X4 PCIE 2.0 接口 NVME SSD  
SanDisk Ultra 3D 500G

选择磁盘: 本地磁盘 /dev/nvme0n1p1 -- /disk/data (共 458.3G, 剩余 398.5G) ▾ I/O测试

2020-07-24 13:12:48 开始磁盘 /disk/data 性能测试  
共8项, 每项测试时间: 30 秒, 临时文件大小: 2G

2020-07-24 13:17:36 测试完成, 总耗时 4分48秒

测试结果:

	读 (MB/s   IOPS)	写 (MB/s   IOPS)
Seq 顺序	1720MiB/s 1715	1312MiB/s 1307
512K 随机	1553MiB/s 3101	1290MiB/s 2574
4K 随机	198MiB/s 50.9k	44.2MiB/s 11.4k
4K-QD32 随机	197MiB/s 50.4k	48.3MiB/s 12.4k

## SATA 3.0 台式机硬盘测试

### 磁盘I/O测试

希捷 ST1000NM0033-9ZM 1T SATA 硬盘读写测试

选择磁盘: 本地磁盘 /dev/sda2 -- /disk/sda (共 914.9G, 剩余 866.4G) ▾ I/O测试

2020-07-26 13:42:24 开始磁盘 /disk/sda 性能测试  
共8项, 每项测试时间: 30 秒, 临时文件大小: 2G

2020-07-26 13:47:22 测试完成, 总耗时 4分58秒

测试结果:

	读 (MB/s   IOPS)	写 (MB/s   IOPS)
Seq 顺序	175MiB/s 174	174MiB/s 174
512K 随机	61.5MiB/s 122	94.6MiB/s 188
4K 随机	697KiB/s 174	1601KiB/s 400
4K-QD32 随机	2092KiB/s 522	1426KiB/s 355

## IPerf 网络测试



[IPerf3](#) 是一个网络性能测试工具，IPerf 可以测试最大 TCP 和 UDP 带宽性能，支持 Windows/Linux/macOS/Android/iOS。

iRouter 路由同时支持客户端和服务端。

The screenshot displays the IPerf3 configuration interface, divided into two main sections: 'IPerf3 服务端' (Server) and 'IPerf3 客户端' (Client). The server section includes a port field set to '默认为5201' and a blue 'IPerf3' button. The client section includes a '服务端地址: IP地址' field, two buttons for 'IPerf3 上行' and 'IPerf3 下行', a port field set to '默认为5201', a checkbox for 'UDP 模式' (unchecked), a bandwidth field set to '默认为10 M', and a duration field set to '单位秒, 默认为60'.

IPerf 服务端运行参数:

```
iperf3 -s
```

IPerf 客户端运行参数:

```
iperf3 -c 服务端 IP -p 端口 (默认 5201, 可选) -i 1 -t 运行时长 (秒)
```

```
iperf3 -c 192.168.2.254 -i 1 -t 60
```

# KVM 虚拟化

## KVM 简介

基于内核的虚拟机 (KVM) 是一种内建于 Linux 中的开源虚拟化技术，需要 x86 架构的，支持虚拟化功能的硬件支持（比如 Intel-VT, AMD-V），是一种全虚拟化架构。

近几年，阿里云、腾讯云、华为云等国内云服务提供商迅速崛起，KVM 被这几大云服务提供商广泛采用，使得它成为云计算世界里事实上的虚拟化标准。

KVM 虚拟化可以在支持虚拟化的硬件设备上创建一个或多个虚拟机。

必备条件：

1. 需要 CPU 支持虚拟化
2. KVM 虚拟化需要存储空间，请参考 [磁盘管理](#)

---

## 支持虚拟化的 CPU

**Intel CPU:**

最低配置为 1037U, I3/I5/I7/志强系列的 CPU 都支持虚拟化, D525 不支持

详细 Intel CPU 型号列表: [支持虚拟化的 Intel 处理器](#)

如果需要将 PCI 物理设备(如网卡、显卡、声卡等) 透传给虚拟机直接使用, 还需要 CPU 和主板芯片组同时支持定向 I/O 虚拟化技术 (VT-d), 并在首页-》功能视图-》“系统” -》“启动参数” -》“内核参数” 中勾选 “启用 Intel IOMMU”

支持硬件透传(VT-d)的 Intel CPU 型号列表: [同时支持 VT-d 的 Intel 处理器](#)

## AMD CPU:

64 位的 AMD CPU 基本都支持虚拟化

## BIOS 设置

开机时按 Del 键进入 BIOS 设置-》Advanced (高级) -》CPU Configuration 或 Processor Configuration (处理器配置) :

将 Intel Virtualization Technology 设为 Enabled。

如果 CPU 支持 VT-D 特性 (用于物理设备透传, 比如透传网卡给虚拟机), 也设为 Enabled。



## 安装模块

应用-》模块-》检查更新，找到 “kvm ” 模块，点击安装。

ID	名称	备注	版本 发布时间	大小 占用内存
1	kvm	KVM 虚拟化 <a href="#">更多...</a> 成为一台虚拟化服务器，管理和运行多个虚拟机。	1.6.60 2020-10-22 10:16:28	23.60 MB 128.79 MB

## 配置虚拟网络

虚拟机网络类型：

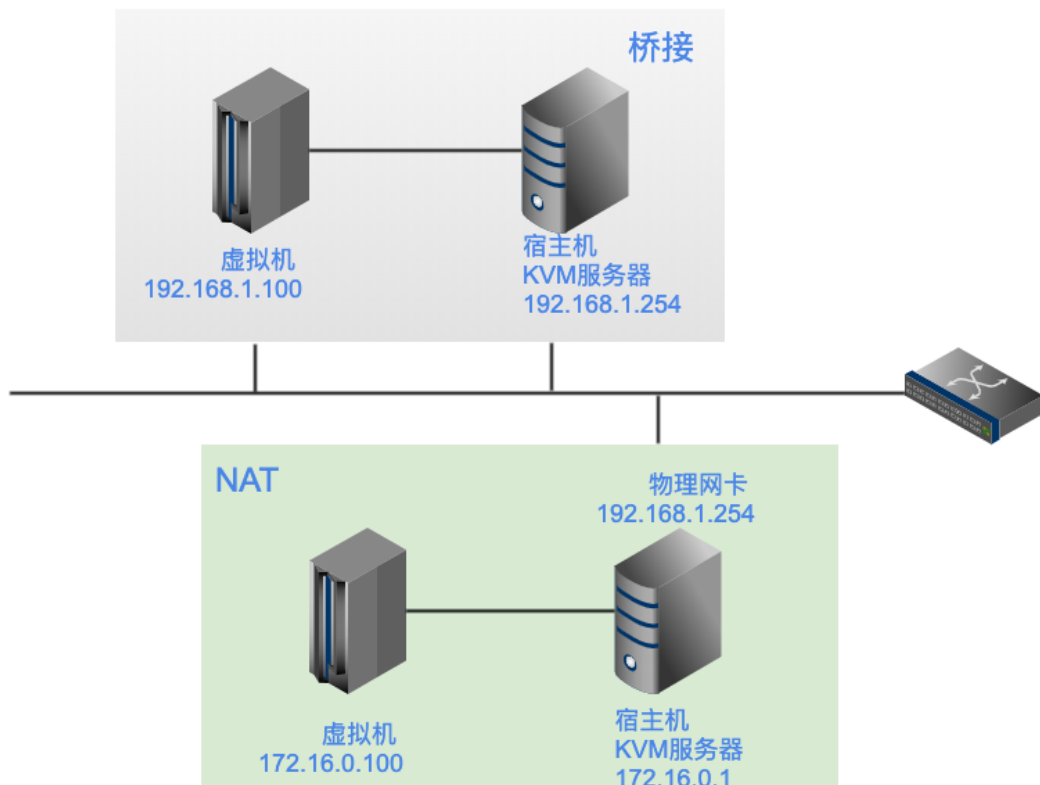
### 1. 桥接

虚拟机的网卡和系统的 LAN 口桥接，虚拟机可以和 LAN 口的设备直接互访，如同虚拟机接在 LAN 口交换机下。

## 2. NAT

创建虚拟交换机，虚拟机的网卡接在此交换机上，虚拟机对 LAN 口的设备不可见，如同虚拟机接在二级路由下。

虚拟机的网络类型（桥接、NAT）



以桥接为例：

KVM 虚拟化服务

参数设置 虚拟机 资源管理 网络 一键将LAN1口改为桥接

**⚠ 没有发现系统网桥，虚拟机将无法和LAN口主机互访，点击一键开启网桥**

共1条记录/1页, 每页显示 200

ID	虚拟交换机名	端口数量	IP地址/子网掩码	MAC地址	备注
1	k1	32	172.73.0.1/255.255.255.0	64-33-38-e0-f3-c9	

如果 KVM 服务器本身不能上网（比如无 WAN 口或 WAN 口未连接），虚拟机必须使用桥接模式（通过 LAN 口其他路由器上网），否则虚拟机也无法上网。

## 新建虚拟磁盘

资源管理-》新建磁盘：

文件名

虚拟空间  100M~8000G  
磁盘空间按实际使用来分配

[显示更多选项 >](#)

## 上传 ISO 文件

ISO 文件用于安装系统。

您还可以将 ISO 拷贝到 U 盘中，然后从 U 盘导入，参考：[U 盘导入 ISO/IMG 镜像](#)

有两种方式：

- 当文件小于 200M 时，通过浏览器上传本地文件，上传成功后，单击“继续”，
- 当文件大于 200M 时，通过远程获取文件，输入下载链接 (URL)，单击“下载”，等待下载完成。



注：通过远程获取文件时，推荐使用单文件 HTTP 服务器 [HFS](#)

## 新建虚拟机

根据虚拟机里面运行系统的不同，选择 CPU 及操作系统类型：

名称  名称可自定义，支持中文

操作系统类型

CPU数量

绑定到指定CPU运行  否

内存大小  MB (32~10071)

VNC端口  VNC 端口范围：5901~5999，不重复即可

VNC密码

磁盘

= 可用磁盘文件列表 =  
1.img  
r1.img  
sip-disk1.img  
siotest-disk1.ima

点击“生成 MAC 地址” -> “新增”，可增加网卡

网卡

为虚拟机添加网卡，可以多个

共享文件夹

启用PCI设备透传  否

启用PCI SR-IOV  否

光驱位置  选择ISO文件

单击虚拟机网卡的 MAC 地址，可更改网络连接类型：

7	vm001	<input type="text" value="vm001.img"/> <input type="text" value="MQ-iRouter_V1.2"/>	<input type="text" value="00-0d-e7-40-02-87"/> -- lan1.br 网络拓扑	已停止	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
8	win7	<input type="text" value="win7.img"/> <input type="text" value="virtio-win-0.1-"/>	<input type="text" value="ac-e5-22-91-1f-2f"/> -- lan1.br 网络拓扑	已停止	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>





注：如果虚拟机操作系统支持虚拟化网卡，请选择 VirtIO network device 网卡驱动类型，以获得最佳性能，若不支持，可用选择 Intel 或 Reltek 网卡

Windows 下使用 Virtio 网卡需要安装驱动：[VirtIO for Windows](#)

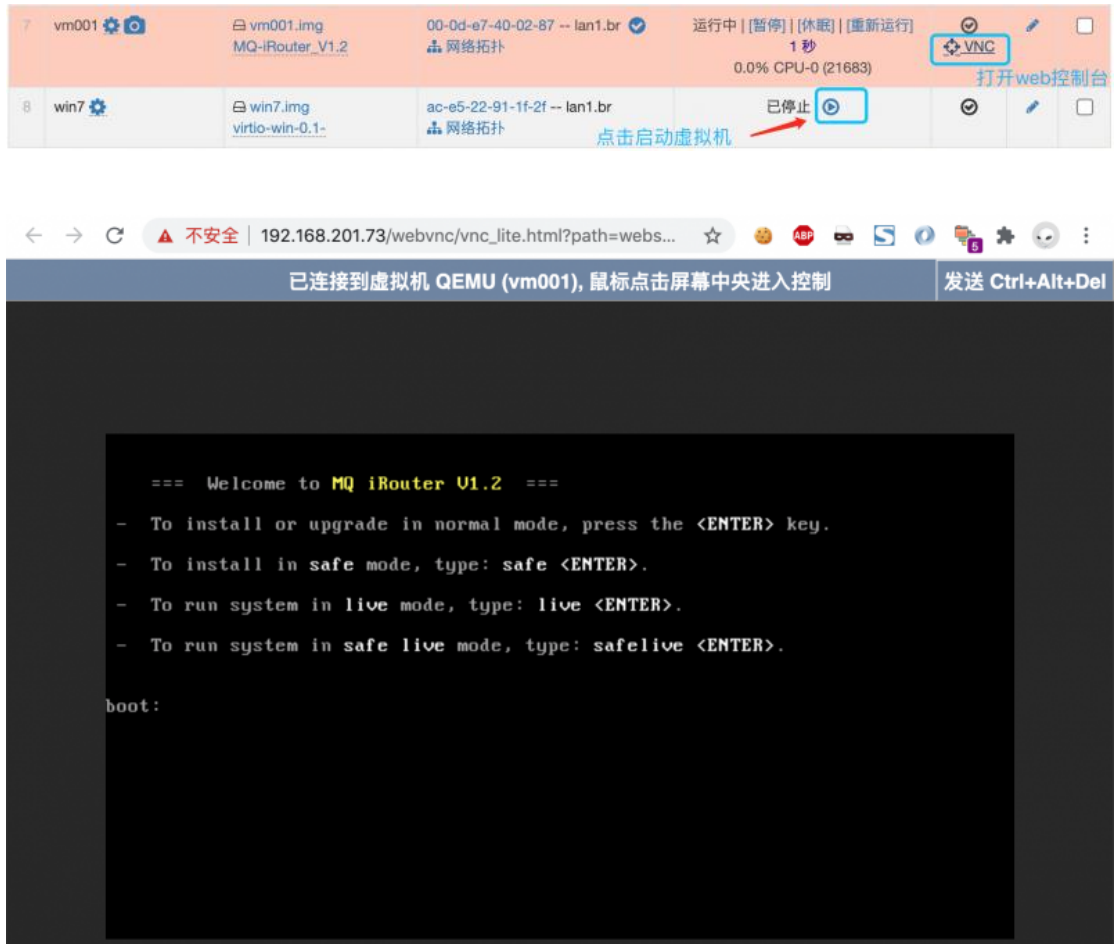
至本文更新时，当前最新版本为 virtio-win-0.1.187.iso

下载后挂载 ISO 到虚拟机光驱后安装。

## 安装系统

---

启动虚拟机，通过 VNC 在浏览器中，远程安装系统。



**注：如果浏览器中无法显示 VNC 控制台，请使用最新版本的 Chrome 浏览器访问。**

或者通过 VNC 客户端（如 [VNCViewer](#)）直连路由的 VNC 端口。

如同本地物理机器上安装系统一样，完成安装后，返回虚拟机列表界面，点击“CD-ROM”列表中的“修改”进行“卸载”ISO 文件，避免进入循环安装。



最后选择虚拟机，点击“重启”或“重新运行”。

## 常见问题 FAQ

### 1. 路由上能同时运行多少个虚拟机？

取决于硬件资源（CPU、内存），虚拟机分配的内存非预分配，而是根据虚拟机实际使用情况动态调配，所以运行的虚拟机总内存可能大于实际物理内存。

比如一台 HPGen8 的服务器，配有 10G 内存（2G+8G），运行 8 个虚拟机，实际使用内存不到 5G。

### 2. 能运行 Windows 吗？

可以，测试可以支持 32 位和 64 位的 Windows XP/Win7/Win10。

因 Windows 对图形处理要求比较高，要运行流畅，建议透传物理显卡给虚拟机使用。

### 3. VirtIO 磁盘及网卡驱动

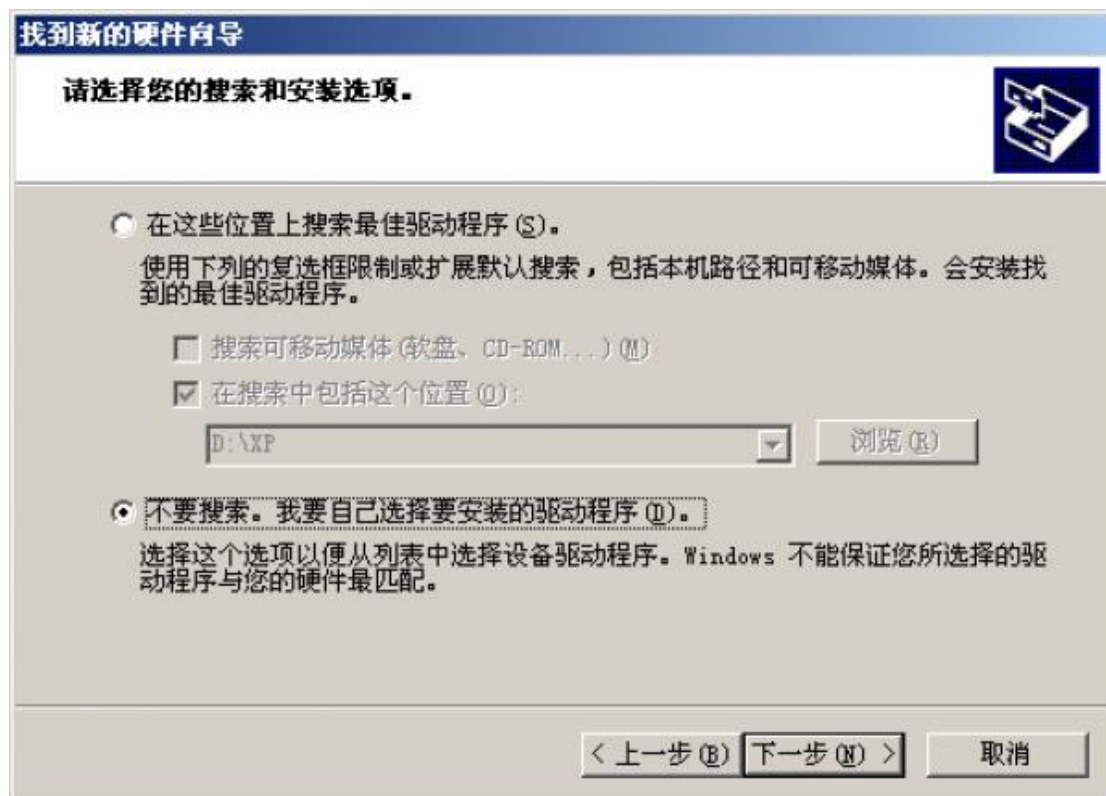
Windows 下的 VirtIO 驱动下载: [VirtIO for Windows](#)

下载 virtio-win-0.1-74.iso 以上版本即可

Windows XP 下安装 VirtIO 网卡驱动提示 “Windows 无法加载这个硬件的设备驱动程序。驱动程序可能已损坏或不见了。(代码 39)”

时,

不使用 自动 搜索安装, 而采用 手动 选择驱动路径安装:



通过 从磁盘安装(H)... 按钮, 选择驱动文件路径:



驱动路径是 D:\XP\X86，而不是 D:\WXP\X86

#### 4. 系统启动时屏幕提示 kvm: disabled by bios

原因：BIOS 中未开启虚拟化支持，参考 BIOS 中开启虚拟化支持

## Docker 容器

容器对进程进行封装隔离，属于操作系统层面的轻量级虚拟化解决方案（进程虚拟化）。

容器和虚拟机的区别：

- 容器是一个应用层抽象，用于将代码和依赖资源打包在一起。

多个容器可以在同一台机器上运行，共享操作系统内核，但各自独立。与虚拟机相比，容器占用的资源和空间较少，瞬间就能完成启动。

- 虚拟机 (VM) 是一个物理硬件层抽象，用于将一台服务器变成多台服务器。

管理程序允许多个 VM 在一台机器上运行。每个 VM 都包含一整套操作系统，因此占用大量空间。而且 VM 启动也十分缓慢。

依赖条件：需要额外的存储空间，请参考 [磁盘管理](#)

## 安装模块

应用-》模块-》检查更新，找到 “docker ” 模块，点击安装。

## 服务配置

Docker 容器服务

参数设置 容器列表 镜像管理

服务运行状态 运行中 <PID: 6527> [选择磁盘存储](#)

Docker 主目录 本地磁盘 /dev/nvme0n1p1 -- /disk/data (共 458.3G, 剩余 373.7)

后端存储驱动 overlay

默认网络本地接口 IP 172.17.0.1 [初次配置](#)

自定义网络本地接口 IP 172.18.0.1

## 创建镜像

参数设置 容器列表 镜像管理

共 8 条记录/1页, 每页显示 200 请输入关键字

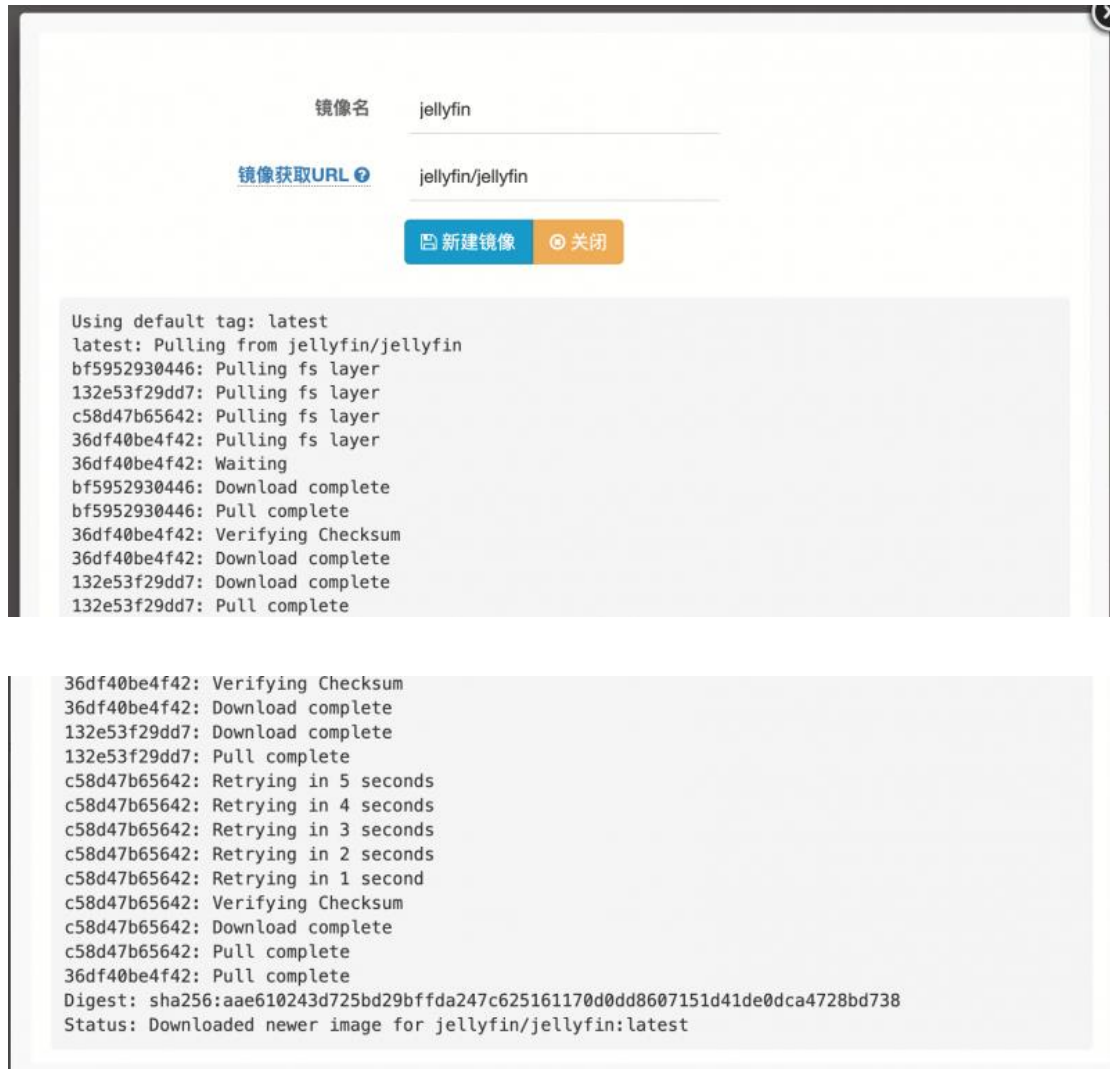
ID	镜像名 镜像ID	标记	镜像大小	创建时间	选择
1	secfa/docker-awvs 18fd39929d0d	awvs13-20200310	708MB	2020-03-10 18:04:04	<input type="checkbox"/>
2	teddysun/kms 234cd61ae414	latest	5.65MB	2020-05-29 10:56:58	<input type="checkbox"/>
3	secfa/docker-awvs 6d45cb16d459	latest	738MB	2020-06-02 17:43:47	<input type="checkbox"/>
4	jellyfin/jellyfin 360585541fa2	latest	490MB	2020-08-31 06:12:36	<input type="checkbox"/>

镜像获取 URL:

- 从 Docker 官方仓库获取: 直接输入路径, 例如  
jellyfin/jellyfin
- 从其他 Docker 仓库获取: 例如  
hub.c.163.com/library/centos

- 从自定义包获取：例如 <http://example.com/dir/myos.txz>

注：这个过程可能需要较长时间，取决于镜像大小及网络状况。



## TR069 管理 & ACS

TR069 全称是用户终端设备广域网管理协议（CPE WAN

Management Protocol），简称 CWMP，用于通过 ACS（自动配置

服务器）从网络侧对家庭网络中的网关、路由器、机顶盒等设备进行



远程集中管理，包括初始化自动配置、远程故障诊断修复和设备监控等。

ACS 也有其他的叫法：

电信将其称之为 ITMS (Integrated Terminal Management System) 终端综合管理系统。

联通、移动称之为 RMS (Remote Management Server) 远程管理服务器。

### 终端兼容性列表

- 支持三大运营商（原版、中性版固件）出品的光猫及融合网关
- 支持主流电视厂家出品的光猫及融合网关（创维）
- 支持国内主流光猫及融合网关生产厂家出品的光猫（中兴、华为、烽火、锐捷、深圳友华、瑞斯康达、上海贝尔）

我们将尽可能兼容和适配市面上主流的光猫及融合网关设备

海蜘蛛 TR069 的优势：光猫即插即用、全程远程配置下发

- 易用方便：光猫无需刷机，运营商原版光猫拿来即用

- 简单易懂：客户无需关心复杂的 TR069 参数及属性名，无需为光猫建模，亦无需了解不同运营商不同光猫的配置参数差异，复杂的底层我们已封装好，只需简单的定义配置模版
- 无缝兼容：光猫无需任何配置（路由上域名重定向自动引导到 ACS 上）
- 运维告警：光猫异常、配置变化、上下线微信通知
- 定时重启：无需担心光猫长时间运行发热大、运行变慢等问题
- 复位自动下发配置：光猫被强制复位了也无需运维干预
- OLT 联合管理：配合即插即用的傻瓜型 EPON，或华为 MA5680/5800/5683 系列 OLT+秒开 OLT 管理，OLT 管理中开启自动注册，光猫插上就能用。
- 灵活部署：可作为主路由，也可以旁路部署，支持基本 QinQ 及灵活 QinQ 网络

## ACS 功能

- 发现光猫
- 下发 LAN（含 DHCP）、WAN、WIFI（单/双频）、SIP 电话等配置，支持中文 SSID
- 配置支持实时下发和工单自动下发（实时下发需内网部署）
- 重启/恢复出厂设置
- 查看/修改超级管理员账号/密码
- 开启/关闭光猫 Telnet

- 解除光猫上网限制 & 终端数量限制(屏蔽客户机上网弹出光猫注册页面)
- 查看状态: LAN 口/WAN 连接/SIP 语音注册, WIFI 状态显示 (SSID/信道/连接终端数量)
- 显示光模块信息 (收/发光功率、电流/电压、温度等)
- 实时浏览 TR069 所有属性名、属性值 (仅支持内网部署)
- 配置模版 (LAN/WAN 桥接/WAN DHCP/WAN PPPoE/WAN 固定 IP/SIP/WIFI 2.4G/WIFI 5.8G)
- 业务模版 (包含多个配置模版)
- 工单业务 (预先根据光猫 SN/MAC/LOID 关联模版, 及设置独有参数), 设备上线自动执行
- 开启 WAN 口访问 HTTP/Telnet/SSH (华为光猫支持)
- 查看连接的 WIFI 终端信息
- 显示光猫注册时的 ONT SN
- 去掉 WIFI SSID 运营商前缀 (部分光猫支持)
- 光猫上线、下线、重启等告警微信推送通知  
(2020/11/03)
- 定时重启光猫
- 永久工单 (光猫恢复出厂设置后上线时, 自动下发配置模版)
- 针对单个光猫单独修改 WIFI SSID、频道、密码参数, 单独修改 SIP 电话参数

- 光猫光衰过大或光功率过强告警
  - 光猫分组管理 (2020/11/29)
  - 导出光猫配置文件 (2020/12/16)
  - 使用内置 SIP 服务器时, 下发 SIP 电话模版自动创建 SIP 账号
  - 自定义 TR069 参数值/指令下发 (2020/12/17)
- 

兼容指数说明 (10 为完美兼容) :

- 10: 光猫内置域名格式的 ACS 地址, 第一个 WAN 口为 TR069 连接, 能自动连到 ACS 上, 接受 ACS 的管理。  
新光猫或恢复出厂后, 无需对光猫做任何设置, 即可在路由上通过 TR069 发现它, 并对其下发配置。

注: 需提前在路由上做好 DNS 域名重定向解析 (解析 ACS 域名到 TR069 VLAN 接口的 IP 上)

- -A: 下发 LAN 时光猫会自动重启
- -B: 光猫没内置 ACS 地址, 为纯净固件, 恢复出厂后无 TR069 连接, 需手动创建或通过 OLT 下发, 其他所有功能正常
- -C: 下发 WAN 口配置后, 需重启光猫 WAN 口才能连接

- -D: 部分固件语音为 H.248 协议，需升级光猫固件才支持 SIP 电话

## 典型 & 成功案例

参考 [TR069 光猫管理案例](#)

# 海蜘蛛无线 AP

## 产品型号

请参考：请参考官网或咨询客服人员

## 部署说明

---

### 1. 路由上开启 DHCP 服务

进入网络-》DHCP 服务，启用“DHCP 服务器”

在 配置标签页“IP 地址池”-》一键生成默认地址池，或根据需要修改地址池范围

注意：请确认网内没有其他 DHCP 服务器，并且 DHCP 分配的网关是路由 LAN 口的 IP

### 2. AP 接入网络

将 AP 接入到路由 LAN 口所在到交换机下，等待大约 1 分钟左右

### 3. 开启 AP/AC 管理

进入应用-》AP 控制器/AC 管理，启用“AC”功能，即可发现上线的 AP 设备

AC 控制器管理服务

参数配置 AP 列表 配置模板 固件升级

共1条记录/1页, 每页显示 10 请输入关键字 搜索 清除 自动刷新 显示离线设备

ID	设备型号 / MAC IP 地址 / 备注 最后在线时间 运行时长	2.4G SSID 信道   加密方式	5G SSID 信道   加密方式	2.4G终端 5G终端	状态	选择
1	海蜘蛛HAP150X / 1c-88-79-5b-d4-70 192.168.2.101 修改备注 2020-07-24 09:19:29 2小时19分8秒	AP-D470 6   无	AP-D470 157   无	无 1	🟢	<input type="checkbox"/>

== 2.4 GHz 配置模板 == == 5 GHz 配置模板 == 批量下发配置 重启AP 恢复出厂 全选 / 全不选

点击IP可直达AP的web管理

## 禁用 2.4G

创建 2.4G 模版，状态设为“禁用”：

参数配置 AP 列表 配置模板 固件升级 新建2.4G模版，状态设为禁用

ID	名称	工作频段	SSID	频道	验证方式	无线密码	备注	状态	编辑	选择
1	2.4G模版【禁用】	2.4GHz	MQAP-	自动	wpa2	88888888		🚫		<input type="checkbox"/>
2	2.4G默认模版	2.4GHz	MQAP-	自动	wpa2	88888888		🟢		<input type="checkbox"/>
3	5G默认模版	5GHz	MQAP-5G-	自动	wpa2	88888888		🟢		<input type="checkbox"/>

一键生成默认模版 新增2.4G配置 新增5G配置 全选 / 全不选

然后下发配置模版即可：

ID	设备型号 / MAC IP 地址 / 备注 最后在线时间 运行时长	2.4G SSID 信道   加密方式	5G SSID 信道   加密方式	2.4G终端 5G终端	状态	选择
1	MQAP1200-DC / 1c-88-79-5b-d4-70 192.168.2.105 修改备注 2020-07-30 11:42:28 38分5秒	MQAP-D470 1	MQAP-D470-5G 36	无 2	☑	<input checked="" type="checkbox"/>

(1) 选择AP

(2) 选择模版

(3) 下发配置

2.4G模版【禁用】 (SSID: MQAP-) == 5 GHz 配置模版 == 批量下发配置 重启AP 恢复出厂 全选 / 全不选

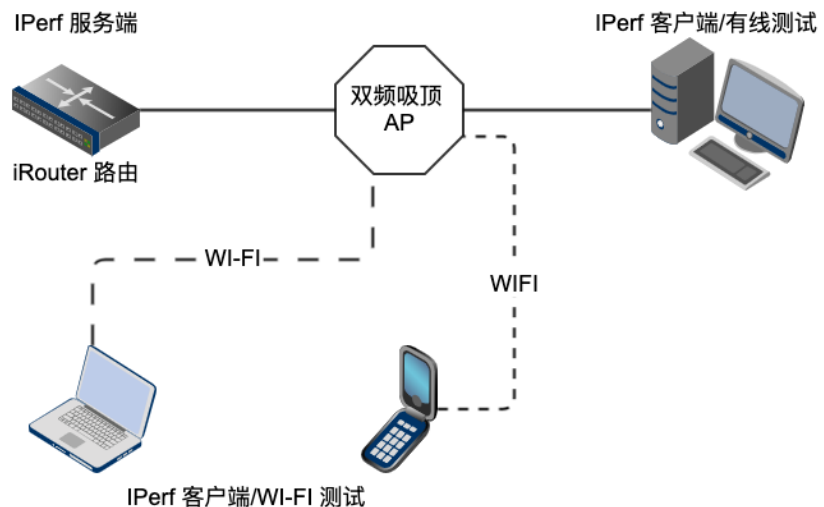
大约 1 分钟内生效：

ID	设备型号 / MAC IP 地址 / 备注 最后在线时间 运行时长	2.4G SSID 信道   加密方式	5G SSID 信道   加密方式	2.4G终端 5G终端	状态	选择
1	MQAP1200-DC / 1c-88-79-5b-d4-70 192.168.2.105 修改备注 2020-07-30 11:47:13 42分50秒		MQAP-D470-5G 36	无 2	☑	<input type="checkbox"/>

为空表示2.4G已被禁用

## 无线性能测试

### 1. 网络拓扑



## 2. 手机端 5G 无线测试

The screenshot shows the iPerf mobile application interface. At the top, the status bar displays '中国电信' (China Telecom), the time '18:25', and a battery level of '46%'. The app header includes 'Help', 'iPerf', and 'Start' buttons. The main configuration area is titled '服务端IP/端口' (Server IP/Port) and includes the following settings:

- Server address: 192.168.2.73
- Server port: 5201
- Transmit mode: Download (selected)
- Streams: 5 (selected)
- Test duration: 5 min (selected)

A red arrow points to the 'Download' button, which is labeled '下载测试' (Download Test). Below the configuration, the test results are displayed: '415 Mbits/s' with a horizontal line underneath, and 'min: 250 max: 501' below it. The text '测试5分钟' (Test 5 minutes) is also present.

下载带宽测试结果: **最低 250Mbps, 最大 501Mbps, 平均 415 Mbps**



### 上传测试

Server address

Server port

Transmit mode  Upload  Download

Streams  1  2  3  4  5

Test duration  10s  30s  5 min

# 422 Mbits/s

min: 284 max: 467

上传带宽测试结果：最低 284Mbps, 最大 467Mbps, 平均 422 Mbps

2.4G 采用相同测试方法, PC 端和手机端测试方法类似。

# 测试结果汇总

速度单位：Mbps

测试对象	上传最小带宽	上传最大带宽	上传平均值	下载最小带宽	下载最大带宽	下载平均值
手机 5G	284	467	<b>422</b>	250	501	<b>415</b>
手机 2.4G	6	40	<b>25</b>	9	34	<b>22</b>
电脑有线	728	944	<b>880</b>	672	942	<b>917</b>

以上测试结果仅供参考，不同环境（干扰、不同测试设备等）下数据可能会有偏差。

## 典型案例

某夜店，人员密集场所，17 台 AP，无缝漫游，单台 AP 可负载 80 终端。

共 17 条记录/2页, 每页显示 10 请输入关键字  搜索    显示离线设备 无线终端(2.4G/5G): 258 (11/245)

ID	设备型号 / MAC IP 地址 / 备注 最后在线时间 运行时长	2.4G SSID 信道   加密方式 2.4G终端	5G SSID 信道   加密方式 5G终端	状态	选择
1	./... / 1c-88-79-5a-e2-c3 192.168.10.10 修改备注 2020-11-03 22:33:18 17小时32分32秒		Supermuse 60 27	☑	<input type="checkbox"/>
2	./... / 1c-88-79-5a-e2-bb 192.168.10.11 修改备注 2020-11-03 22:31:37 17小时30分33秒		Supermuse 60 73	☑	<input type="checkbox"/>
3	./... / 1c-88-79-5a-e4-bb 192.168.10.13 修改备注 2020-11-03 22:32:42 17小时31分55秒		Supermuse 60 70	☑	<input type="checkbox"/>

61	D8:63:75:...	192.168.11.185	MI6-xiaomishouji	-70	165 MB / 221 MB
62	B8:C9:B5:...	192.168.10.30	OPPO-Reno3-5G	-67	26 MB / 276 MB
63	6E:3E:07:...	192.168.11.35	laodie	-67	184 MB / 245 MB
64	B2:6A:0C:...	192.168.10.132	iPhone11	-63	165 MB / 276 MB
65	24:FB:65:...	192.168.11.52	HUAWEI_P20-18...	-74	165 MB / 221 MB
66	E6:2E:2E:...	0.0.0.0	iPhone-2	-70	6 MB / 184 MB
67	7E:CA:7C:...	192.168.11.90		-72	165 MB / 276 MB
68	1A:DD:26:...	192.168.11.30	iPhone	-77	82 MB / 184 MB
69	B8:7B:C5:...	192.168.10.254	yanshaodeiPhone	-71	122 MB / 58 MB
70	5E:3F:6A:...	0.0.0.0	OnePlus7Pro	-59	248 MB / 276 MB
71	48:3F:E9:...	192.168.10.192	HUAWEI_Mate_20-...	-59	248 MB / 307 MB
72	F4:06:16:...	0.0.0.0	shirokakiiPhone	-70	138 MB / 245 MB
73	7E:FC:0D:...	0.0.0.0	iPhone	-65	184 MB / 276 MB

## VLAN 隔离部署

AP 设备在管理 VLAN(48), 连接 AP 的无线终端在业务 VLAN(201), 相互隔离。

将 AP 连接交换机到端口设为 trunk, pvid 设为 管理 vlan, 透传业务 vlan

```
interface GigabitEthernet0/0/6

description to AP

port link-type trunk

port trunk pvid vlan 48

port trunk allow-pass vlan 48 201
```

如果 AC 旁路部署，将 AC 连接交换机到端口设为 access 口，管理 vlan 中，或设为 trunk，透传管理 vlan

AC 上开启 DHCP 服务，为 AP 分配 IP。