

open VPN 使用方法

最近有很多用户因为 open VPN 的操作步骤问题导致 VPN 无法正常拨号访问内网。

下面详细介绍一下 open VPN 的操作步骤

第一步：添加账号

首先在服务认证计费--认证账号管理--账号管理中添加账号。

认证计费 > 认证账号管理 > 账号管理

账号:	123	*
密码:	***	*
认证类型:	不限	
套餐类型:	自定义	*
上行速率:	0	KB/s *
下行速率:	0	KB/s *
开始时间:	2021-08-20 11:23:05	*
到期时间:	选择日期	
收款金额:		
共享数:	1	*
绑定VLAN:	0	*
<small>默认值为0, 仅支持PPPoE, 支持QinQ, 如: 2008.100</small>		
<input checked="" type="checkbox"/> 自动绑定VLAN		
绑定网卡:	任意	
<small>仅支持PPPoE</small>		
绑定MAC:	手动	
MAC地址:		
<small>添加MAC, 每行输入一个MAC</small>		
固定IP:	10.7.7.100	

账号和密码：根据自己需求设置。

认证类型：可以选择不限或者 OpenVPN。

套餐类型：选择自定义。

固定 IP：填写 open VPN 网段地址，open VPN 默认网段为 10.7.7.0/24，填写网段中任意一个地址即可，此处固定 IP 以 10.7.7.100 为例讲解。

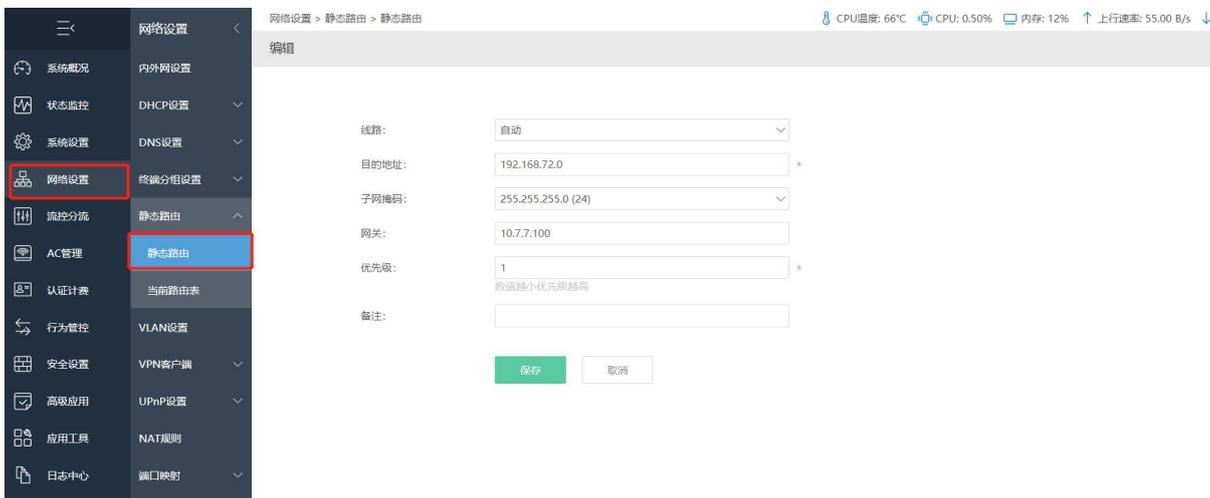
其他设置可以默认不用去更改，需要设置可参考账号管理帮助文件。

设置完成点击保存。

第二步：设置静态路由

服务端静态路由设置：

在网络设置--静态路由中添加静态路由



目的地址/子网掩码：填写客户端内网网段及掩码。

网关：填写在账号管理中设置的固定 IP。

客户端静态路由设置：



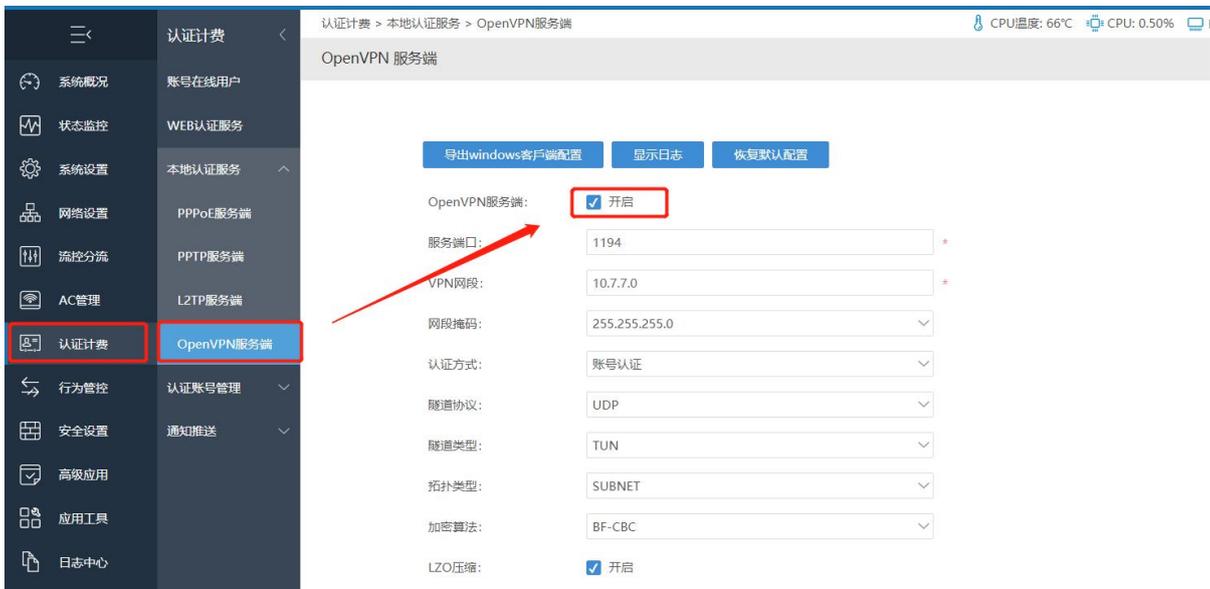
目的地址/子网掩码：填写服务端内网网段及掩码

网关：填写 VPN 网段网关地址：10.7.7.1

第三步：配置 VPN 服务端及客户端

服务端配置：

在认证计费--本地认证服务--OpenVPN 服务端功能内开启 OpenVPN，认证方式选择账号认证。



推送路由：填写服务端内网网段及子网掩码

推送路由：

IP	子网掩码	操作
192.168.67.0	255.255.255.0(24)	编辑 删除
10.7.0.0	255.255.0.0(16)	编辑 删除

客户端配置：

在网络设置--VPN 客户端--添加 OpenVPN



拨号名称：根据自己需求设置

服务器 IP/域名：填写服务端 IP 地址或域名

服务器端口：默认端口 1194，客户端端口要和服务端设置相同

认证方式：选择账号认证

用户名/密码：填写在服务端账号管理中设置的用户名密码

隧道协议、隧道类型、加密算法、LZO 压缩、MTU 这几个参数要与服务端选择一致。

网络设置 > VPN客户端 > OpenVPN

CA证书:	<pre>gyOrnmmwBzStqr195r ChEh+1eCVym+ZLWueBSQD8752RxU83MW8s9HblBY Bui4a0Q45kSoFI7UIf+KiEBT Cezw3lh111h8RtuMFLjUzI9tPCqIqOiLhwfmV0mY84S OSIQRQanZhYPAaLjSPr4 gmFwkrWSrZ1ZRI6Mk2JKsnc+a7+o -----END CERTIFICATE-----</pre>
客户端证书:	<input type="text"/>
客户端私钥:	<input type="text"/>
附加配置:	<p>例如:</p> <pre>tcp-queue-limit 32 mtu-disc no</pre>
服务器路由推送:	<input checked="" type="checkbox"/> 开启
添加路由:	<p>格式: 192.168.1.0/24</p> <input type="text"/>
定时重拨:	<input type="checkbox"/> 开启

CA 证书: 两端都是爱快路由情况下，直接将服务端的 CA 证书复制到客户端即可。

客户端证书/私钥: 爱快服务端不校验客户端证书及私钥，所以客户端证书/私钥可不填写。如服务端不是爱快设备，客户端证书/私钥由服务端提供。

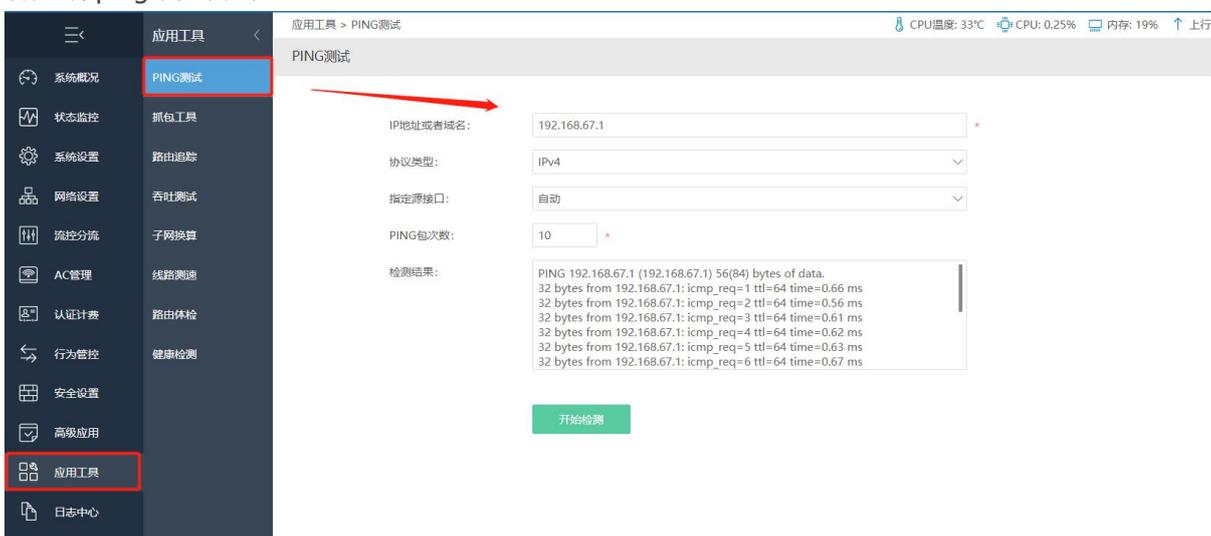
设置完成点击保存。

刷新页面显示获取到本地 IP 代表拨号成功。

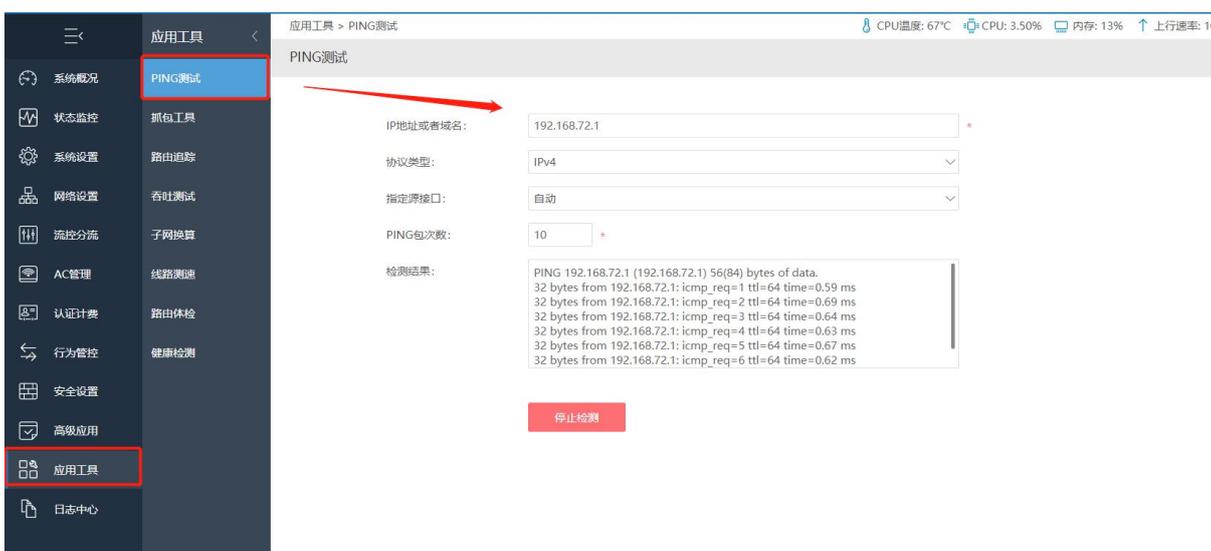


最后在测试 VPN 服务端和客户端内网是否能互访, 在服务端和客户端分别使用应用工具--ping 测试, ping 对端网关能 ping 通代表 VPN 内网搭建成功。

客户端 ping 测试结果:



服务端 ping 测试结果:



双机热备

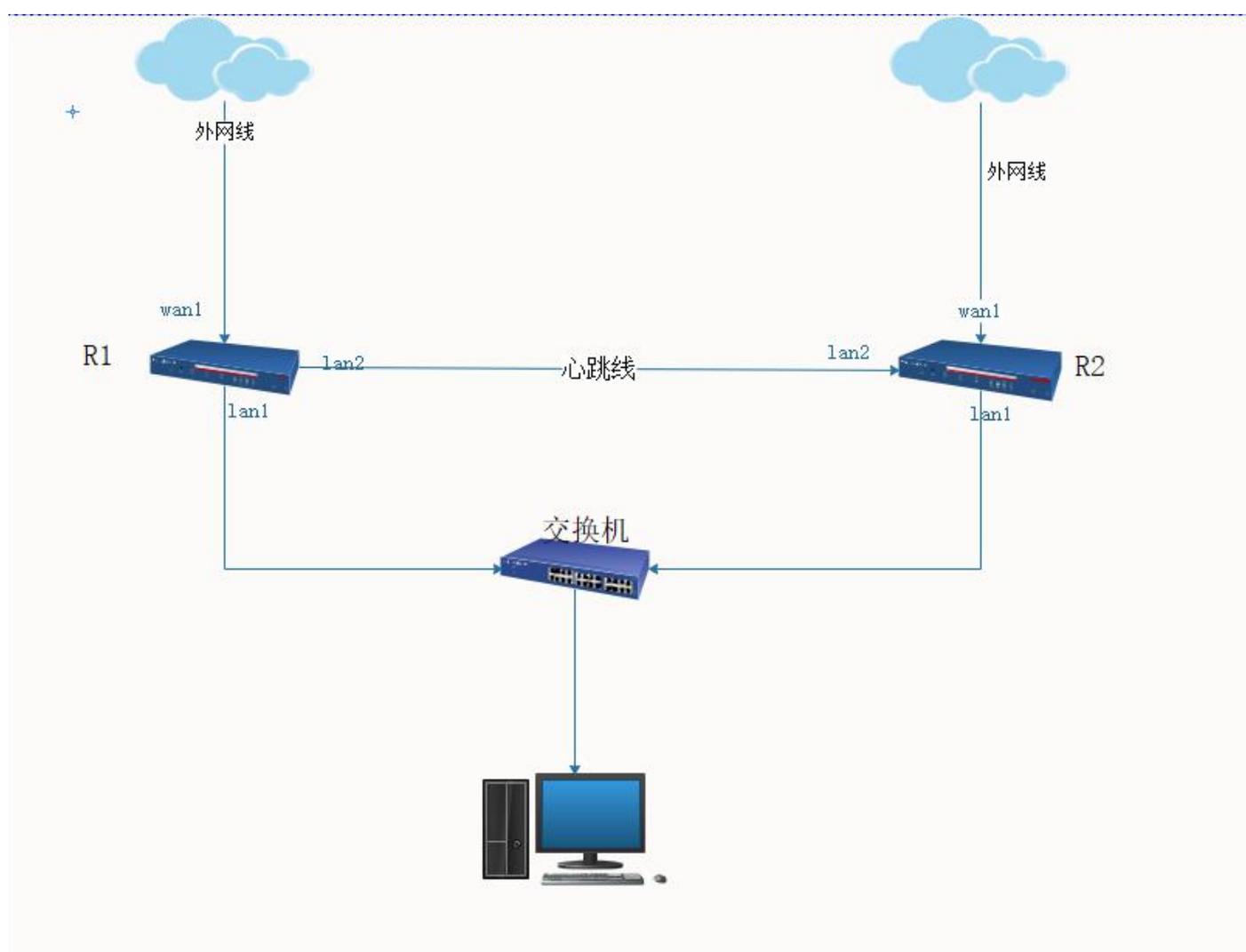
一、名词解释

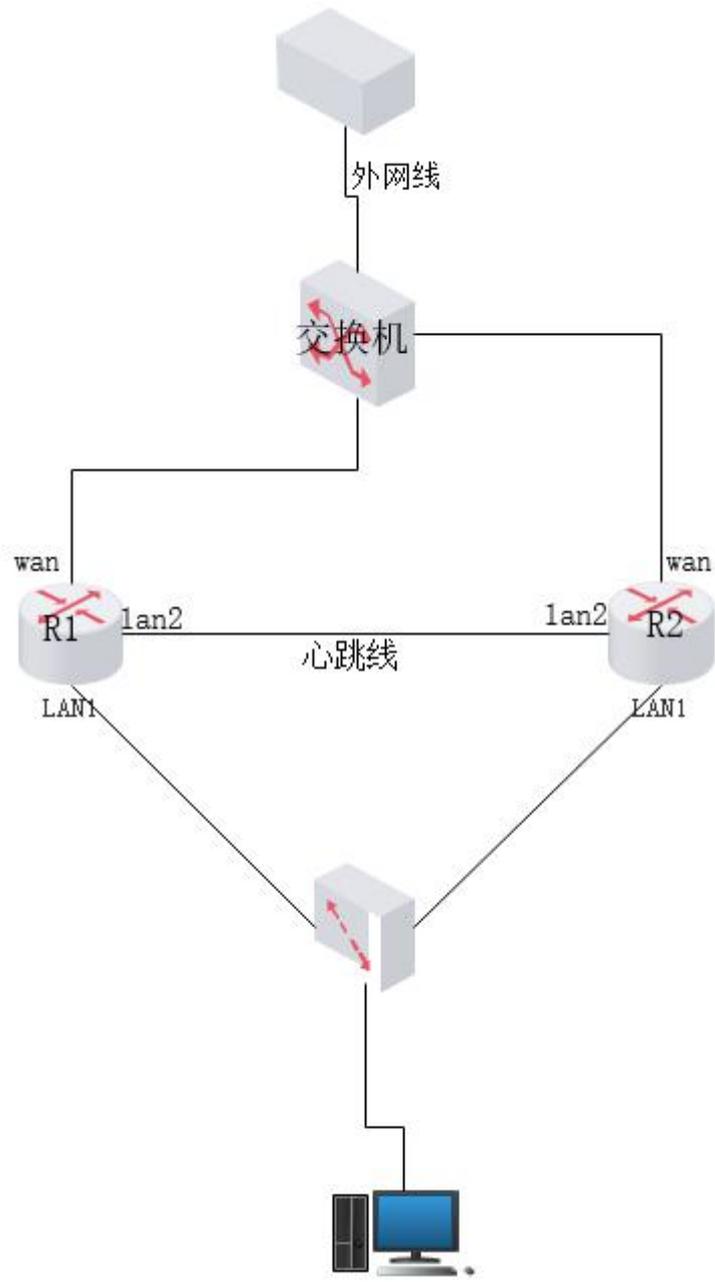
在无需网络管理员或者网络运维人员的情况下，当其中一台网关宕机时，另一台网关能在短时间内主动承担起宕机网关的所有业务，从而实现网关冗余的一种功能

二、拓扑架构

双机热备目前支持多线使用与单线使用

(1)、多线环境双机热备架构图

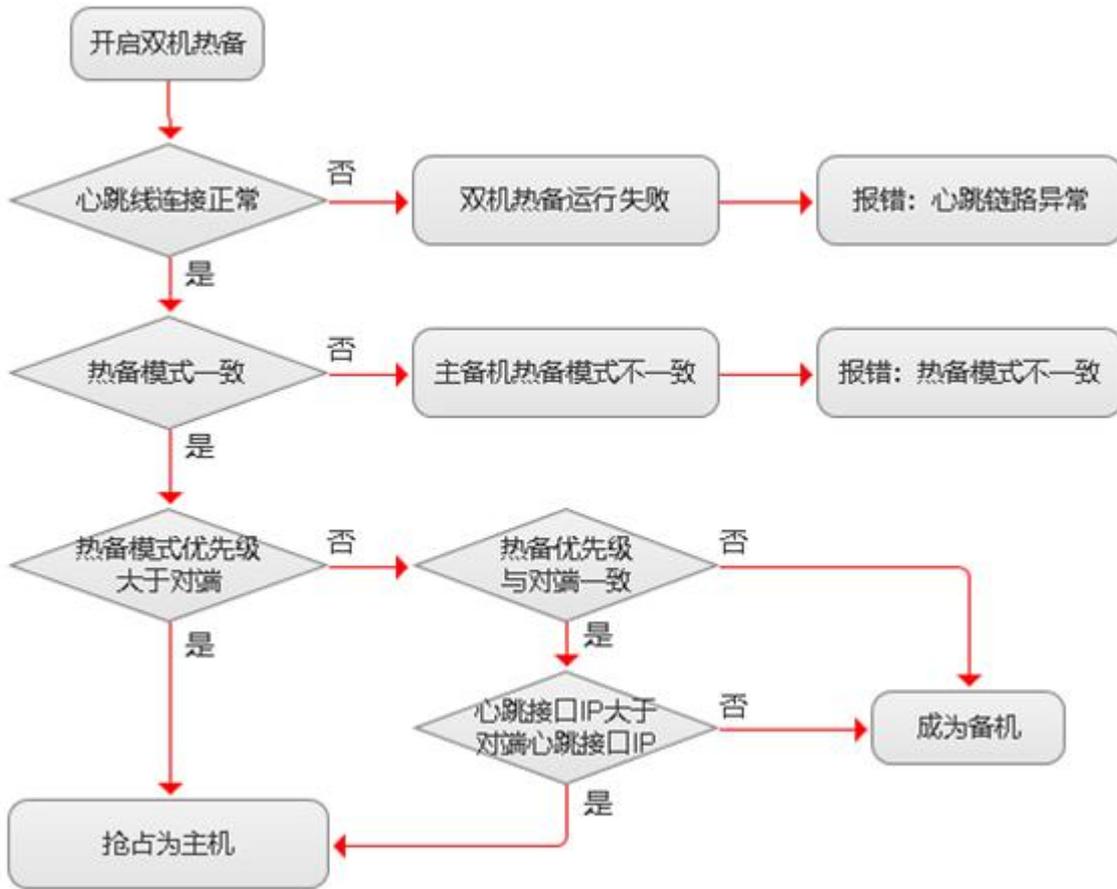




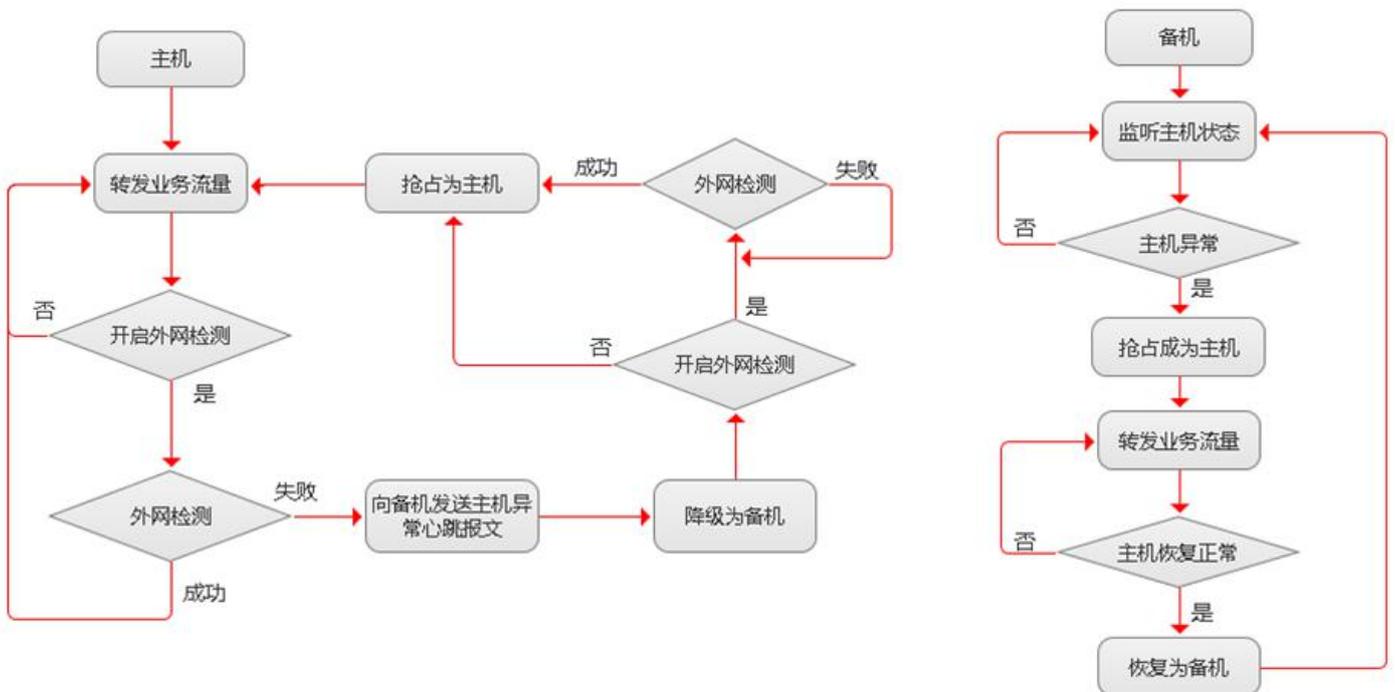
(2)、单线环境网络拓扑

三、功能流程（功能流程建立在物理链路无任何问题的基础上）

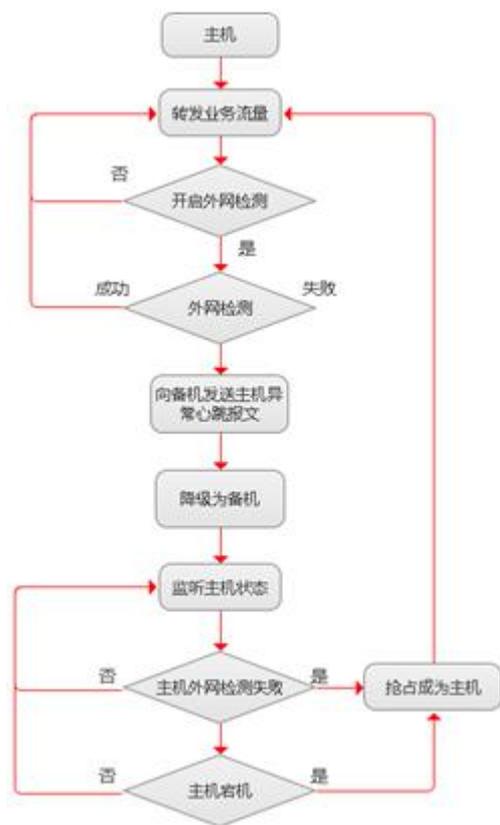
1、双机热备初次建立流程



2、主备模式运行流程



3、单线热备功能流程



四、参数说明

1、双机热备主页

双机热备

已开启双机热备

热备设置 手工回步

心跳链路状态

设备名称	心跳接口	心跳IP	运行状态
iKuai15.1(本端)	lan3	172.16.20.254	心跳连接正常
iKuai(对端)	lan2	172.16.20.1	

主备机状态

设备名称	热备模式	状态
iKuai15.1(本端)	主备模式	主机
iKuai(对端)	主备模式	备机

数据链路

传输链路	设备名称	虚拟网关
传输链路1	iKuai15.1(本端)	192.168.15.99/24
	iKuai(对端)	192.168.15.99/24

(1)、心跳链路状态

【设备名称】：双机热备中本端路由名称和对端路由名称

【心跳接口】：热备路由建立心跳连接所使用的接口

【心跳 IP】：热备路由建立心跳连接的接口 IP 地址，如果心跳链路异常则本端心跳 IP 和对端心跳 IP 均显示为 “-- --”

【运行状态】：双机热备的心跳链路是否建立成功（心跳链路正常/心跳链路异常）

（2）、主备机状态

【设备名称】：双机热备中本端路由名称和对端路由名称

【热备模式】：双机热备的工作模式，主备机的热备模式需保持一致，如果主备机热备模式不一致，报错：热备模式配置不一致

【状态】：路由器在双机热备中的身份，一般情况下建议用户配置主路由器为高优先级，备路由器为低优先级，如果两端配置的优先级相同，则比较两端路由器的心跳链路的接口 IP，心跳接口 IP 大则竞争为主路由器，心跳接口 IP 小则为备路由器

（3）、数据链路状态

【传输链路】：传输链路的编号，和配置统一

【设备名称】：双机热备中本端路由名称和对端路由名称

【虚拟网关】：主备路由器两端的传输链路，正常情况下同一条传输链路主备机的虚拟网关需保持一致，如果不一致会报错

2、热备设置页面

系统设置 <

基础设置

双机热备

爱快云绑定

登录管理 >

升级备份 >

硬件信息

重启关机

系统设置 > 双机热备

基础设置

双机热备模式: 主备模式 负载模式

优先级: 主机 备机 (两端优先级不能保持一致)

单线热备: 开启

外网检测: 开启

Ping: *

检测周期: s *

检测端口:

心跳线设置

心跳线接口: ▼

对端IP地址: * (两端IP地址需保证同一网段)

传输链路设置

添加传输链路: 添加

接口名	虚拟网关	操作
lan1	188.188.188.1/24	编辑 删除

注: 虚拟网关子网掩码长度为1-29位
虚拟网关格式: 192.168.1.254/24

保存
取消

【双机热备模式】：分为主备模式和负载模式

主备模式：主机一直处于工作状态，备机运行但不工作，主机出现断电、宕机、外网检测失败自动切换到备机

负载模式：主机和备机同时运行工作，下面设备上网随机出口，当一端出现断电、宕机、外网检测失败自动切换

【优先级】：分为主机和备机模式，上网优先从主机转发，主机出现故障自动切换到备机

【外网检测】：检测本端路由是否可以通外网，建议开启

【ping】：填写 IP 或者域名格式

【检测周期】：外网检测的周期

【检测端口】：检测指定外网线路无法访问外网时，切换到备机上网。

【心跳线接口】：设置用于主备机的相互通信的接口

【对端 IP 地址】：对端 lan 口 IP 地址，两端的地址必须为同一网段但不能相同

【传输链路】：内网业务冗余备份的路由接口，冗余备份时设置的虚拟网关需一致

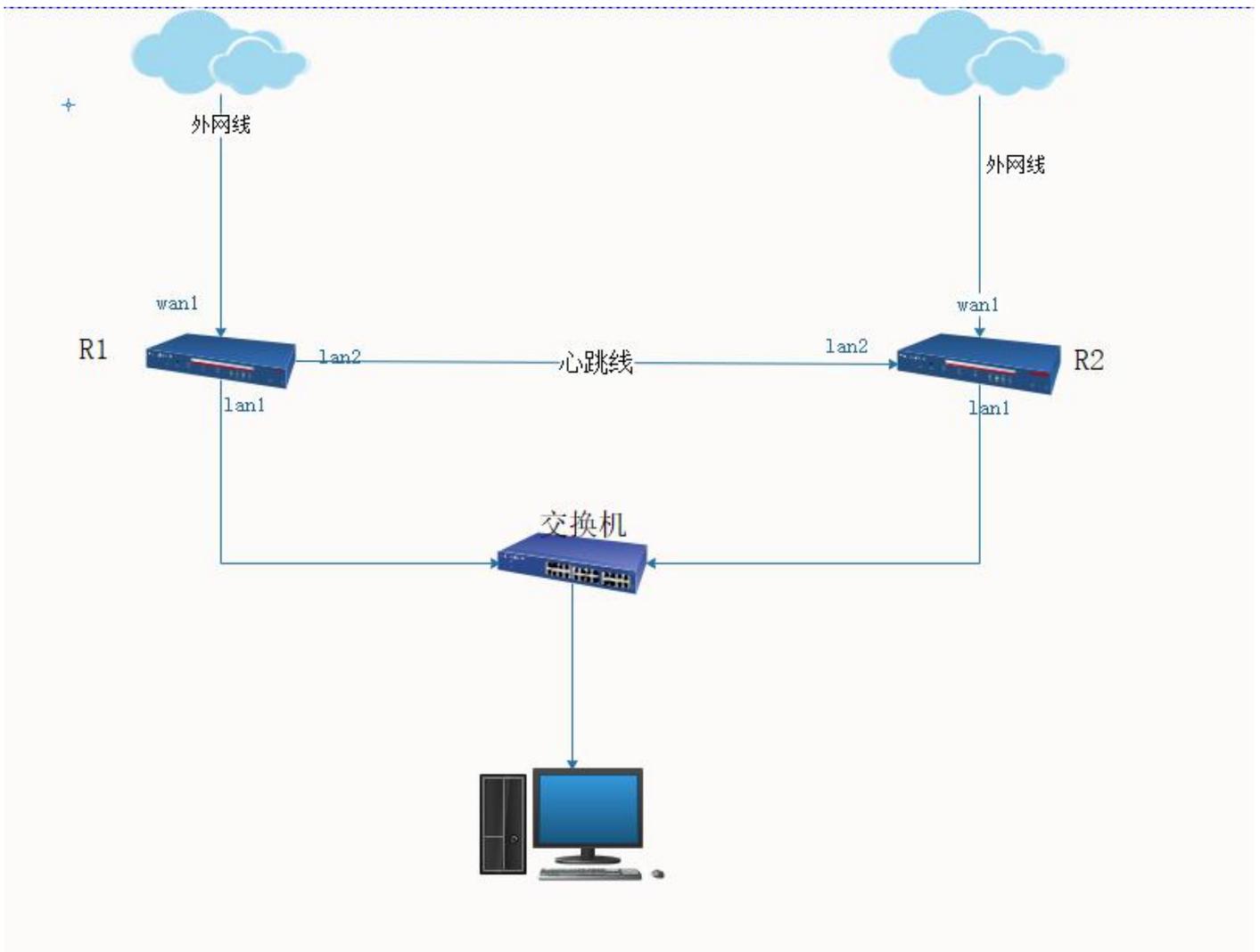
【虚拟网关】：虚拟网关两端需填写一致，可填写和 lan 口同网段未使用的地址。

注意：

- ①、当勾选外网检测后，如果不勾选任何端口，则当主机所有接口外网均无法访问时切换为备机，原备机启动切换成主机
- ②、当勾选外网检测后，如果勾选任何端口，则当主机勾选的任意外网接口外网无法访问时切换为备机，原备机启动切换成主机
- ③、当不勾选勾选外网检测后，仅当主机宕机时切换为备机，原备机启动切换成主机

五、配置举例

1、多线环境配置案例：



A 端路由 : lan1 虚拟网关:188.188.188.1 lan2:10.10.10.2

B 端路由 : lan1 虚拟网关:188.188.188.1 lan2:10.10.10.1

A 和 B 通过 lan2 作为心跳线

A 端配置 :

系统设置 > 双机热备 CPU: 0.00%

系统设置

基础设置

双机热备

磁盘管理

应用绑定

爱快云绑定

高级设置

登录管理

升级备份

硬件信息

重启关机

网络设置

流控分流

AC管理

认证计费

行为管控

安全设置

高级应用

应用工具

日志中心

基础设置

双机热备模式: 主备模式 负载均衡

优先级: 主机 备机 (两端优先级不能保持一致)

外网检测: 开启

Ping: *

检测周期: s *

检测端口:

心跳线设置

心跳线接口:

对端IP地址: * (两端IP地址需保证同一网段)

传输链路设置

添加传输链路: 添加

接口名	虚拟网关	操作
lan1	188.188.188.1/24	编辑 删除

注: 虚拟网关子网掩码长度为1~29位
虚拟网关格式: 192.168.1.254/24

B端配置：

基础设置

双机热备

爱快云绑定

登录管理

升级备份

硬件信息

重启关机

网络设置

流控分流

AC管理

认证计费

行为管控

安全设置

应用工具

日志中心

基础设置

双机热备模式: 主备模式 负载均衡

优先级: 主机 备机 (两端优先级不能保持一致)

外网检测: 开启

Ping: *

检测周期: s *

心跳线设置

心跳线接口:

对端IP地址: * (两端IP地址需保证同一网段)

传输链路设置

添加传输链路: 添加

接口名	虚拟网关	操作
lan1	188.188.188.1/24	编辑 删除

注: 虚拟网关子网掩码长度为1~29位
虚拟网关格式: 192.168.1.254/24

保存
取消

注意事项：

两端的数据链路虚拟网关必须一致

视频教程：

<http://ikurl.cn:555/externalLinksController/chain/%E5%8F%8C%E6%9C%BA%E7%83%AD%E5%A4%87.mp4?ckey=XNbOJd9MewiUiLw3fBl1Ma3za0YmA9jHvlQsn35ikjTmFEpFePiuJmGjThclRC9G>

六、注意事项

- 1、 两台路由器的固件版本需一致才能建立起心跳线连接
- 2、 两台路由器需配置相同双机热备模式才能建立起心跳线连接
- 3、 双机热备开启后，备机的 DHCP 功能失效
- 4、 建立起双机热备的两台路由器的之间同一传输链路虚拟网网关必须一致
- 5、 双机热备的外网链路检测的检测周期可输入范围：1~30 s，检测外网断开后，切换的时间是自己所设置时间的 3 倍，总共检测 3 次才会切换
- 6、 同一路由器的每个接口无法同时应用在心跳链路和传输链路中（且双机热备不能使用扩展 IP 作为心跳 IP）
- 7、 同一路由器的每个接口无在传输链路中应用两次
- 8、 双机热备下行传输链路需通过二层设备互联，即路由器 A LAN1 和路由器 B LAN1 在同一网段，且为二层直连互通
- 9、 目前仅支持通过备机的心跳 IP 和 WAN 口 IP 访问备机 WEB 界面
- 10、 双机热备主机宕机出现故障时，6 s 后才会切换到备机上。
- 11、 双机热备虚拟网关的条数不能超过 32 条，超出会导致双机热备不能正常使用。
- 12、 企业版路由双机热备只能和企业版对接，免费版本双机热备只能和免费版本对接。

七、常见问题

1、内网 pppoe VPN web 认证情况下如何切换

答：

web 认证：两边同步 WEB 认证配置情况下，主备机同步在线用户列表，当主备切换时，终端可正常上网，无需再次认证

若两 边不同的 WEB 认证配置，即认证方式不同，只要在主机认证过，主备切换后，在线终端会同步，终端无需认证仍能上网

PPPOE: PPPOE 服务端同步后，主机宕机后，内网终端 PPPOE 被断开，重拨到原备机（现主机），当原主机恢复后，内网终端 PPPOE 连接再被断开，内网终端重拨到原主机

VPN: 内网终端拨远程 VPN，当主机宕机后，内网终端 VPN 目前不会被断开，需手工断开重新拨号；当主机恢复后，内网终端 VPN 目前不会被断开，需手工断开重新拨号

2、双机热备的手工同步能将备机的配置同步给主机吗？

答：

不可以，双机热备的手工同步需要同时满足如下条件：

- ①、主备机心跳连接正常
- ②、主备机的热备模式一致
- ③、同步方向：主机→备机

3、AP 的识别（lan 虚拟网关不同网段 DHCP 配置虚拟网关网段是否可以识别）

lan 网段必须与物理接口在同一网段，否则 DHCP 显示失效；虚拟网关与 lan 可以不在同一网段，虚拟网关不影响 AP 识别，AP 接在哪个 lan 下，就由哪个 lan 来分配 ip

4、双机热备的负载模式支持 PPPOE 服务端功能热备吗？

答：

不支持，PPPOE 服务端功能仅支持主备模式的热备

5、双机热备的主备机的 DHCP 地址池如何设定（地址池范围为虚拟网关网段还是物理接口网段）？

答：

当虚拟网关和物理地址不一致时，DHCP 地址池范围需和物理接口配置一致

6、双机热备的主备机 PPTP 的服务端配置一致，主备模式和负载模式分别如何工作？

答：

当 PPTP 服务端账号共享数大于 1 时，无论是主备模式还是负载模式，主备机都能拨号成功，各自生效