

隧道接口协议

本页面描述了可用的所有可用的隧道协议 `/etc/config/network` 及其选项。在页面末尾提供了一些示例配置。

请注意，对于大多数协议，安装`opkg`包是协议支持所必需的。

协议“pptp”（点到点隧道协议）

⚠️ 该软件包 `pptp` 必须安装到使用PPTP。您需要有另一部分来配置“父”设备，您可能需要在防火墙的“wan”区域中添加“`<vpn>`”（`<vpn>`是本节的“逻辑接口名称”）。

名称	类型	需要	默认	描述
<code>server</code>	IP地址	是	（没有）	远程PPTP服务器
<code>username</code>	串	没有（？）	（没有）	PAP / CHAP身份验证的用户名
<code>password</code>	串	没有（？）	（没有）	PAP / CHAP身份验证密码
<code>buffering</code>	布尔	没有	1	启用缓冲和重新排序数据包， 0 禁用它（<code>-nobuffer</code>） pptp缓冲选项在r32482中删除
<code>keepalive</code>	整数	没有	?	尝试重新连接的次数
<code>defaultroute</code>	布尔	没有	1	是否通过隧道创建默认路由
<code>peerdns</code>	布尔	没有	1	使用PPTP提供的DNS (Domain Name System)服务器
<code>delegate</code>	布尔	没有	?	使用内置的IPv6管理
<code>iface</code>	串	没有（？）	<code>pptp- <vpn></code>	物理接口名称 默认为 <code>pptp-<vpn></code> 无论你使用什么

协议“aiccu”（自动IPv6连接客户端实用程序）

⚠️ **aiccu** 必须安装该软件包以使用此协议。该实用程序不是以无头模式运行。如果您有其他选择，请不要使用它。只有**AYIYA**隧道类型已经过测试。对于静态或心跳隧道，可以使用本机**6in4**隧道，也可以使用**he.net**隧道代理。

⚠️ 该协议仅适用于障碍断路器和较新版本。

名称	类型	需要	默认	描述
username	串	是	(没有)	服务器用户名
password	串	是	(没有)	服务器密码
protocol	串	没有	(没有)	隧道建立协议使用 (tic, tsp, l2tp)
server	串	没有	tic.sixxs.net	隧道设置服务器使用
ip6addr	IPv6地址 (CIDR)	没有	(没有)	本地IPv6地址委托给隧道端点 (不需要)
ntpsynctimeout	整数	没有	90	等待几秒钟的NTP同步 (可从aiccu 20070115开始使用 (https://github.com/openwrt/packages/pull/57))
tunnelid	整数	没有	(没有)	TIC服务器隧道ID
ip6prefix	IPv6前缀	没有	(没有)	下行接口的路由IPv6前缀
defaultroute	布尔	没有	1	是否通过隧道创建IPv6默认路由
sourcerouting	布尔	没有	1	是否仅从委派的前缀路由数据包
tunnelid	整数	没有	(没有)	TIC服务器隧道ID
requiretls	布尔	没有	0	要求TLS连接到TIC服务器
nat	布尔	没有	1	通知用户检测到NAT类型的网络
heartbeat	布尔	没有	1	做心跳
verbose	布尔	没有	0	详细记录到系统日志

注意：此协议类型不需要 `ifname` 在接口部分中设置选项。接口名称是从节名称派生的，例如 `config interface sixbone` 会导致一个名为的接口 `aiccu-sixbone`。

协议“中继”（Relayd Pseudo Bridge）

🚨 relayd 必须安装该软件包以使用此协议。

名称	类型	需要	默认	描述
network	逻辑接口名称列表	是	（没有）	指定中继流量之间的网络
gateway	IPv4地址	没有	（网络默认）	覆盖DHCP响应中发送给客户端的网关地址
expiry	整数	没有	30	主机到期超时（以秒为单位）
retry	整数	没有	5	主机被认为死机之前的ARP重试次数
table	整数	没有	16800	自动添加路由的表ID
forward_bcast	布尔	没有	1	启用转播广播流量，0 禁用它
forward_dhcp	布尔	没有	1	启用DHCP请求和响应的转发，0 将其禁用

GRE协议的常用选项

🚨 gre 必须安装该软件包以使用GRE。此外，您需要 kmod-gre 和/或 kmod-gre6 。

在障碍断路器中引入了GRE支持。定义了四个协议（“gre”，“gretap”，grev6“和”grev6tap“），将生成名为”

协议	GRE型	接口名称
GRE	IPv4 GRE	gre4- <逻辑接口名称>
gretap	GRE-TAP IPv4	gre4t- <逻辑接口名称>
grev6	GRE IPv6	gre6- <逻辑接口名称>
grev6tap	GRE-TAP IPv6	gre6t- <逻辑接口名称>

所有四个协议都接受以下常见选项：

名称	类型	需要	默认	描述
mtu	整数	没有	1280	MTU
ttl	整数	没	64	封装包的TTL

		有		
tunlink	逻辑接口名称	没有	(没有)	将隧道绑定到此接口 (dev “ip tunnel”选项)
zone	区域名称	没有	“WAN”	要添加接口的防火墙区域
tos	串	没有	(没有)	服务类型 (IPv4), 流量类 (IPv6): “继承” (外部头继承内部头部的值) 或十六进制值 (仅限于混沌Calmer和更高版本)
ikey	整数	没有	0	输入数据包的密钥
okey	整数	没有	0	输出数据包的密钥
icsum	布尔	没有	假	需要输入校验和
ocsum	布尔	没有	假	计算出去的校验和
iseqno	布尔	没有	假	需要传入数据包序列化
oseqno	布尔	没有	假	执行传出数据包序列化

协议“gre” (通过IPv4的GRE隧道)

除了以上所有常见选项之外, 还支持以下选项:

名称	类型	需要	默认	描述
ipaddr	IPv4地址	没有	WAN IP	本地端点
peeraddr	IPv4地址	是	(没有)	远程端点
df	布尔	没有	真正	在封装数据包时设置“不分片”标志

协议“gretap” (IPv4以太网GRE隧道)

除了以上所有常见选项之外, 还支持以下选项:

名称	类型	需要	默认	描述
ipaddr	IPv4地址	没有	WAN IP	本地端点
peeraddr	IPv4地址	是	(没有)	远程端点
df	布尔	没有	真正	在封装数据包时设置“不分片”标志
network	逻辑接口名称	没有	(没有)	将添加隧道的逻辑网络 (桥接)

协议“greov6”（GRE隧道通过IPv6）

除了以上所有常见选项之外，还支持以下选项：

名称	类型	需要	默认	描述
ip6addr	IPv6地址	没有	WAN IP	本地端点
peer6addr	IPv6地址	是	（没有）	远程端点
weakif	逻辑接口名称	没有	lan	如果ip6addr参数为空并且没有WAN IP可用，则从中选择本地端点的逻辑网络

协议“greov6tap”（IPv6以太网GRE隧道）

除了以上所有常见选项之外，还支持以下选项：

名称	类型	需要	默认	描述
ip6addr	IPv6地址	没有	WAN IP	本地端点
peer6addr	IPv6地址	是	（没有）	远程端点
weakif	逻辑接口名称	没有	lan	如果ip6addr为空并且没有WAN IP可用，则从中选择本地端点的逻辑网络
network	逻辑接口名称	没有	（没有）	将添加隧道的逻辑网络（桥接）

协议“vti”（IPv4上的VTI隧道）

VTI隧道是具有fwmark集的IPsec策略。流量被重定向到匹配的VTI接口。

名称	类型	需要	默认	描述
ipaddr	IPv4地址	没有	WAN IP	本地端点
peeraddr	IPv4地址	是	（没有）	远程端点
mtu	整数	没有	1280	MTU
tunlink	逻辑接口名称	没有	（没有）	将隧道绑定到此接口（ dev “ip tunnel”选项）
zone	区域名称	没有	“WAN”	要添加接口的防火墙区域

ikey	整数	没有	0	输入数据包的key / fwmark
okey	整数	没有	0	输出数据包的key / fwmark

协议“vtiv6”（IPv6上的VTI隧道）

除了以上所有常见选项之外，还支持以下选项：

名称	类型	需要	默认	描述
ip6addr	IPv6地址	没有	WAN IP	本地端点
peer6addr	IPv6地址	是	（没有）	远程端点
mtu	整数	没有	1280	MTU
tunlink	逻辑接口名称	没有	（没有）	将隧道绑定到此接口（ dev “ip tunnel”选项）
zone	区域名称	没有	“WAN”	要添加接口的防火墙区域
ikey	整数	没有	0	输入数据包的key / fwmark
okey	整数	没有	0	输出数据包的key / fwmark

协议“wireguard”（Wireguard VPN）

⚠️ 该软件包 `wireguard-tools` 和 `kmod-wireguard` 必须安装使用 `wireguard`。

每个线保护接口分为两部分：

- 配置相对于接口本身（私钥，MTU，UDP端口绑定等）
- 配置相对于每个对等体（公钥，IP地址等）

接口配置（使用 `proto wireguard`）：

名称	类型	需要	默认	描述
private_key	串	是	（没有）	Wireguard私钥，生成与 <code>wg genkey</code>
listen_port	INT	没有	<i>wireguard</i> 专用	用于传出和传入数据包的UDP端口
mtu	整数	没有	<i>wireguard</i> 专用	接口MTU
preshared_key	串	没有	（没有）	可选的共享秘密，为后量子电阻提供了一个额外的对称密钥加密层

网络接口的名称将是配置部分的名称。

对等配置，对于每个对等体：

	类	需		

名称	型	要	默认	描述
public_key	串	是	(没有)	对等体的公钥
allowed_ips	前缀列表	是	(没有)	该对等体在隧道内允许使用的IP地址和前缀，也用于Wireguard的内部路由表。适用于IPv4和IPv6
route_allowed_ips	布尔	没有	假	为该对等体自动创建每个允许的IP的路由
endpoint_host	串	没有	(没有)	对等体的IP地址或主机名。如果未指定，Wireguard将等待来自对等体的连接
endpoint_port	INT	没有	51820	对端的UDP端口
persistent_keepalive	INT	没有	0	Keepalive消息之间的秒数，0表示禁用

对等体节的名称必须是 wireguard_xx 其中 xx 是wireguard接口部分的名称。

例子

以下是特殊的非标准接口配置的几个例子。

列出由路由器上的软件创建的界面，如vpn


例如，vpn接口通常是“tun0”。要在uci配置文件中列出（因此在luci中）：

```
配置界面'tun0'
  选项ifname'tun0'
  选项proto'none'
```

静态IPv6-in-IPv4隧道

以下示例说明 /etc/config/network 了Hurricane Electric (he.net) 经纪人的文件中的静态隧道配置。Option ipaddr 指定本地IPv4地址，peeraddr 是代理IPv4地址和 ip6addr 通过隧道路由的本地IPv6地址。

```
config'interface''henet'
  选项'proto''6in4'
  选项'ipaddr''178.24.115.19'
  选项'peeraddr''216.66.80.30'
  选项'ip6addr''2001:0DB8:1f0a:1359::2/64'
```

 您还应该将路由IPv6网络中的地址添加到“lan”界面。

❗ 要将IPv6防火墙规则应用于隧道接口，请将其添加到“wan”区域中 `/etc/config/firewall`：

```
配置'区域'  
  选项'name''wan'  
  选项'network''wan henet' #重要  
  选项'input''REJECT'  
  选项'forward''REJECT'  
  选项'输出''ACCEPT'  
  选项'masq''1'
```

❗ 如果您为隧道接口定义一个新的专用区域，请确保设置 `option contrack 1` 为强制启用连接跟踪，否则单向转发规则将无法正常工作。

❗ 如果要在其间路由IPv6流量，请勿忘记在 LAN (Local Area Network) 和隧道之间设置转发规则。
(Local Area Network)

设置在一对一NAT之后

如果你的公网IP (<http://checkip.dyndns.org/>)，例如 178.24.115.19，不匹配，您的ISP可能使用您的WAN接口的IP地址一到一个NAT (<http://shorewall.net/NAT.htm#One-to-one>)（又名全锥形NAT (http://en.wikipedia.org/wiki/Network_address_translation#Methods_of_Port_translation)），你将无法建立静态的IPv6-IN- IPv4隧道。您可以通过以下命令获取WAN接口的IP地址：

```
。 /lib/functions/network.sh; network_get_ipaddr ip wan; echo $ ip
```

如果是这种情况，您应该将WAN IP地址填写为 `ipaddr` 选项，而不是在隧道创建期间可能提供给飓风电机 (<http://he.net/>)的实际公用IP。¹⁾ 或者您可以完全省略可选 `ipaddr` 选项，并自动使用当前的WAN IPv4地址IP。

如果您的WAN IP是动态的（即通过DHCP获取）或者您不确定，那将是首选解决方案。

`/etc/config/network` 输入 示例：

```
config'interface''henet'  
  选项'proto''6in4'  
  选项'peeraddr''216.66.80.30'  
  选项'ip6addr''2001: 0DB8: 1f0a: 1359 :: 2/64'
```

动态IPv6-in-IPv4隧道（仅限HE.net）

下面的示例说明了启用IP更新的Hurricane Electric（he.net）代理的动态隧道配置。自动确定本地IPv4地址，并提供`tunnelid`，用户名和密码进行IP更新。

```
config'interface''henet'  
  选项'proto''6in4'  
  选项'peeraddr''216.66.80.30'  
  选项'ip6addr''2001: 0DB8: 1f0a: 1359 :: 2/64'  
  选项'tunnelid''12345'  
  选项'username''myusername'  
  选项'密码''098f6bcd4621d373cade4e832627b4f6'
```

❗ 您还应该将路由IPv6网络中的地址添加到“lan”界面。

❗ 要将IPv6防火墙规则应用于隧道接口，请将其添加到“wan”防火墙区域，具体请参见上面的示例。

❗ 上面输入的密码应该是用于登录tunnelbroker.net的密码的md5sum。

L2TPv3桥接到LAN的伪线

此示例建立一个伪线隧道，并将其桥接到LAN (Local Area Network)端口。现有的lan接口使用协议l2tp而不是static。

```
config interface lan
    选项 proto l2tp
    选项 type bridge
    选项 ifname eth0
    选项 ipaddr 192.168.1.1
    选项 netmask 255.255.255.0
    选项 localaddr 178.24.154.19
    选项 peeraddr 89.44.33.61
    选项 encap udp
    选项 sport 4000
    选项 dport 5410
```

LAN和无线站之间的中继

该示例 relayd 在无线客户端网络和LAN (Local Area Network)之间建立伪桥接器，使其与Broadcom桥接客户端模式类似。

无线配置（摘录）：

```
配置wifi-iface
    选项 device radio0
    选项 mode sta
    选项 ssid 一些无线网络
    选项 加密 psk2
    选项 key 12345678
    选项 网络 wwan
```

网络配置（摘录）：

❗ 请注意，LAN (Local Area Network)子网必须与无线网络DHCP所使用的不同。

```
config interface lan
    选项 ifname eth0.1
    选项 proto static
    选项 ipaddr 192.168.1.1
    选项 netmask 255.255.255.0

config interface wwan
    选项 proto dhcp

config interface stabridge
    选项 proto relay
    选项 网络 lan wwan
```

与真正的桥接相反，以这种方式转发的流量受到防火墙规则的影响，因此无线客户端网络和lan网络应该被同一个LAN (Local Area Network)防火墙区域覆盖，转发策略设置 `accept` 为允许两个接口之间的流量流动：

```
配置'区域'  
  选项'name''lan'  
  选项'network''lan wwan' # 重要  
  选项'input''ACCEPT'  
  选项'forward''ACCEPT' # 重要  
  选项'输出''ACCEPT'
```

GRE隧道的静态寻址

创建一个静态地址为10.42.0.253/30的GRE隧道，将其添加到现有的防火墙区域 `tunnels`：

```
配置界面mytunnel  
  选项代码gre  
  选项区域隧道  
  选项peeraddr 198.51.100.42  
  
配置界面mytunnel_addr  
  选项原型静态  
  选项ifname @mytunnel  
  选项ipaddr 10.42.0.253  
  选项网络掩码255.255.255.252  
  # 修复IPv6组播（内核中长期存在的错误）。  
  # 有用的，如果你运行Babel或OSPFv3。  
  选项ip6addr'fe80 :: 42/64'
```


WireGuard隧道静态寻址

创建一个名为 `foo` 连接到一个对等体（`vpn.example.com`上的VPN服务器）的WireGuard隧道接口，并允许另一个对等体（例如道路战士）连接。对等体配置通过一个或多个 `wireguard_<ifname>` 部分进行管理。

```
配置界面'foo'  
  option proto'wireguard'  
  选项private_key'qLvQnx5CpXPDo6oplzdIvXLNqkbgpXip3Yv4ouHWZ0Q ='  
  列表地址'fd00: 13: 37: ffff :: 1/64'  
  
config wireguard_foo  
  选项public_key'9mD + mTiOp7SGIkB4t3ZfWAcfp5iA / WwQRdVypKKwrjY ='  
  选项route_allowed_ips'1'  
  list allowed_ips'fd00: 13: 37 :: / 64'  
  option endpoint_host'vpn.example.com'  
  选项persistent_keepalive'25'  
  
config wireguard_foo  
  选项public_key'4mLeSytW6 / y4UcOT6rNorw1Ae9nXSxhXUjxsdzMWkUA ='  
  选项preshared_key'M1IbkkDVwXsQbFbURiMXiVe / iUCjC5TKHcmemVs + oLQ ='  
  list allowed_ips'fd00: 13: 37: ffff :: 2'
```

1)

在创建Hurricane Electric隧道时，您应该始终使用您的公共IP，因此不要因为您在一对一NAT之后而改变它。

 最后修改：2017/05/10 07:41 由danrl

除非另有说明，本维基的内容将根据以下许可证获得许可：CC Attribution-Share Alike 4.0 International
(<http://creativecommons.org/licenses/by-sa/4.0/>)

▣