

单网口OpenWrt旁路由OpenClash redir-host完整配置文档（含自检清单）

文档说明

适用场景：单网口OpenWrt软路由作为旁路由，搭配OpenClash redir-host模式，实现**按需代理**。仅手动修改网关的设备走代理，全屋其余设备、群晖NAS、qBittorrent均直连主路由，不受软路由干扰。

设备环境：

- 主路由：192.168.1.1（全屋默认网关）
- 软路由：单网口OpenWrt、fw4(nftables)防火墙、OpenClash核心
- 业务设备：群晖NAS + Docker qBittorrent

核心目标：彻底关闭全局ARP劫持，解决全网卡顿；采用redir-host精准分流，兼顾代理需求与内网稳定性，BT下载流量纯净直连。

一、整体网络拓扑

主路由(192.168.1.1) ↔ 交换机 ↔ 软路由（单网口旁路由）、群晖NAS、手机、电脑等局域网终端

- 普通设备/群晖：网关=主路由，流量直连上网，不经过软路由
- 需要代理设备：网关改为软路由IP，流量由OpenClash接管代理

二、软路由基础前置配置

2.1 关闭软路由DHCP服务

软路由仅做旁路由，禁止分配IP，避免局域网IP冲突、网关错乱。

操作路径：LuCI → 网络 → DHCP/DNS → 停用DHCP服务器 → 保存应用

2.2 关闭系统自带DNS劫持

清理OpenWrt原生DNS转发规则，避免与OpenClash DNS劫持冲突，防止解析异常、DNS泄漏。

2.3 彻底关闭ARP劫持（解决全网卡顿核心方案）

故障根源：OpenClash ARP劫持会全局劫持内网所有去往主路由的流量，单网口软路由性能薄弱，满载后直接导致全网延迟高、网速卡顿。本场景按需代理，完全不需要ARP劫持。

1. 查看ARP劫持状态（SSH执行）

代码块

```
1  # 查看ARP劫持进程
2  ps | grep arpspoof
3
4  # 查看ARP相关防火墙规则
5  iptables -L | grep -i arp
```

判定：有arpspoof进程输出，代表ARP劫持正在生效。

2. 临时关闭ARP劫持（立即生效，重启内核复原）

代码块

```
1  killall arpspoof 2>/dev/null
```

3. 永久关闭（必做）

OpenClash网页 → 设置 → 取消勾选【ARP劫持/局域网ARP欺骗】→ 保存配置 → 停止并重启OpenClash内核。

4. 客户端清理ARP缓存（macOS）

代码块

```
1  sudo arp -d 192.168.1.1
```

校验：执行arp -a，192.168.1.1对应的MAC为**主路由原生MAC**，非软路由MAC即为正常。

三、OpenClash redir-host模式核心配置（fw4/nftables）

3.1 模式原理

redir-host基于nftables实现TCP/UDP精准劫持，**仅对网关指向软路由的设备生效**，不影响全屋其他设备；自带DNS劫持、QUIC拦截，杜绝DNS泄漏、协议绕过代理问题。

3.2 网页关键参数配置

- 运行模式：redir-host
- 监听网卡：选择软路由唯一LAN网卡
- ARP劫持：完全关闭

- DNS设置：开启OpenClash内置DNS劫持，关闭上游UDP DNS，防泄漏
- QUIC拦截：开启，拒绝境外UDP443流量，防止绕过代理

3.3 内核运行状态校验

代码块

```
1 ps | grep clash
```

正常输出：存在clash主进程、openclash_watchdog看门狗守护进程，代表内核正常运行。

3.4 nftables规则校验（fw4环境专用）

OpenWrt 22.03+默认fw4防火墙，无传统iptables CLASH链，需用nft命令查看规则。

代码块

```
1 nft list ruleset | grep -i clash
```

正常规则特征：

1. DNS劫持规则：th dport 53 redirect to :53（接管全网DNS解析）
2. 流量转发规则：ip protocol tcp/udp jump openclash（TCP/UDP流量送入内核处理）
3. QUIC拦截规则：udp dport 443 reject（拦截境外QUIC绕过代理）

备注：chain openclash 空链为fw4环境正常现象，转发逻辑由Clash内核内部处理，非故障。

四、群晖NAS qBittorrent专项配置

核心需求：BT下载Peer流量纯净直连、不走代理；Tracker节点按需走代理，保证下载连通性。

- 群晖系统网关：固定192.168.1.1（不修改软路由网关，完全避开代理劫持）
- qBittorrent设置：仅开启Tracker代理，Peer连接关闭代理
- 校验方式：查看QB日志，确认Peer流量直连、Tracker按需走代理

五、常见故障排查方案

- **开启OpenClash全网卡顿：**ARP劫持未彻底关闭，重新关闭ARP欺骗、清理客户端ARP缓存、重启内核
- **内核运行但无代理效果：**检查监听网卡是否选错，重新保存配置并重启内核注入nft规则
- **存在DNS泄漏：**开启OpenClash DNS劫持，禁用上游UDP DNS，全覆盖53端口解析
- **单网口性能占用高：**更换轻量内核、精简规则集，避免超大规则库导致CPU满载

快速自检核对清单（修改配置后必检）

◆ 一、ARP劫持核心检查（杜绝全网卡顿）

- [] SSH执行 `ps | grep arpspoof`，无任何arpspoof进程
- [] 终端`arp -a`查询，192.168.1.1 MAC为原生主路由MAC，无篡改
- [] OpenClash网页ARP劫持功能已关闭，保存并重启内核

◆ 二、OpenClash内核与规则检查

- [] `ps | grep clash` 正常存在主进程+看门狗进程
- [] nft规则包含：DNS劫持、TCP/UDP转发、QUIC拦截规则
- [] 运行模式为redir-host，监听网卡绑定本机单LAN口

◆ 三、设备分流业务测试

设备A：网关192.168.1.1（全屋普通设备、群晖NAS）

- [] ifconfig.me 显示家庭宽带公网IP，非代理IP
- [] dnsleaktest 检测无境外DNS泄漏

设备B：网关为软路由IP（代理设备）

- [] 国内站点直连宽带IP，境外规则站点正常走代理
- [] DNS由OpenClash接管，无解析泄漏
- [] `ping 223.5.5.5` 延迟稳定、无丢包、全网无卡顿

◆ 四、qBittorrent专项自检

- [] 群晖网关保持主路由192.168.1.1
- [] QB仅Tracker走代理，Peer下载流量纯直连
- [] 日志无异常代理劫持、无下载断连问题

（注：部分内容由豆包工作 AI 生成）