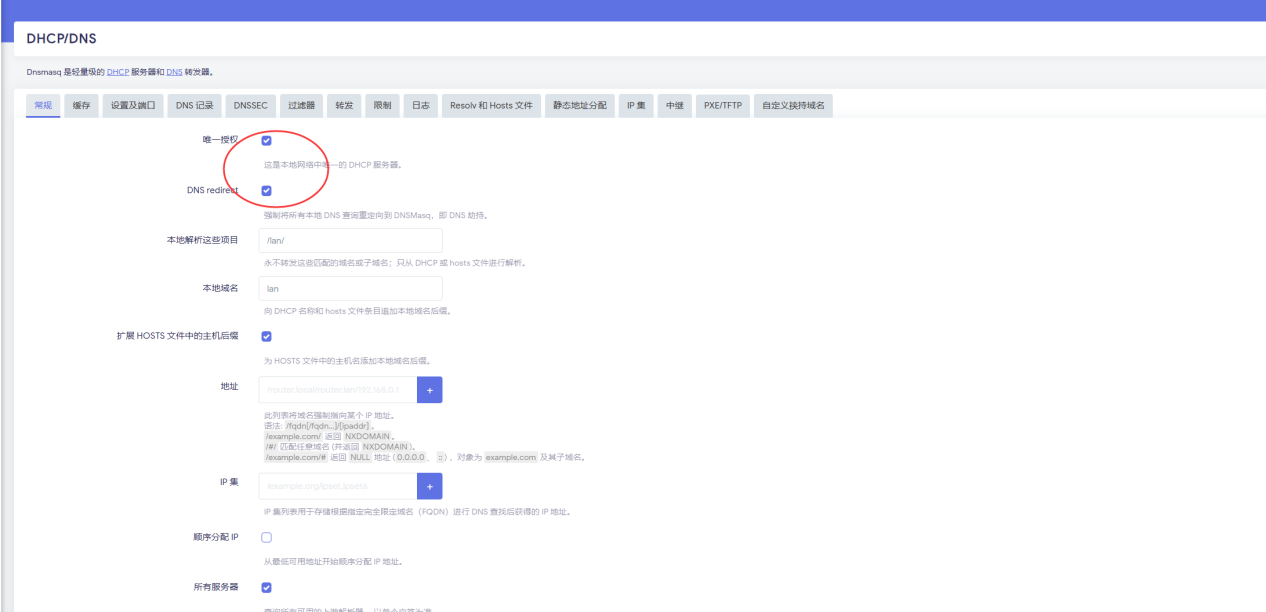
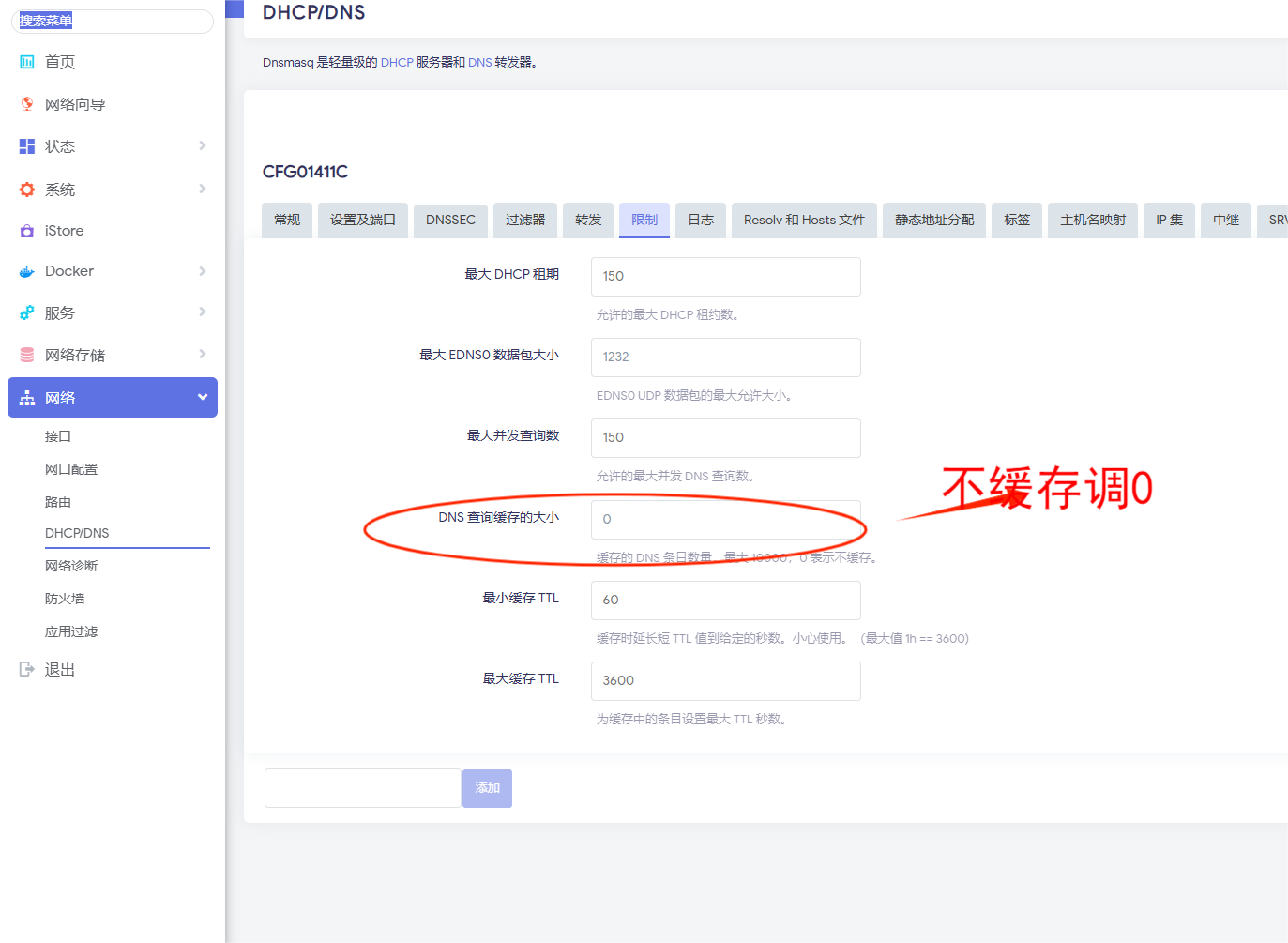
# Clash配置

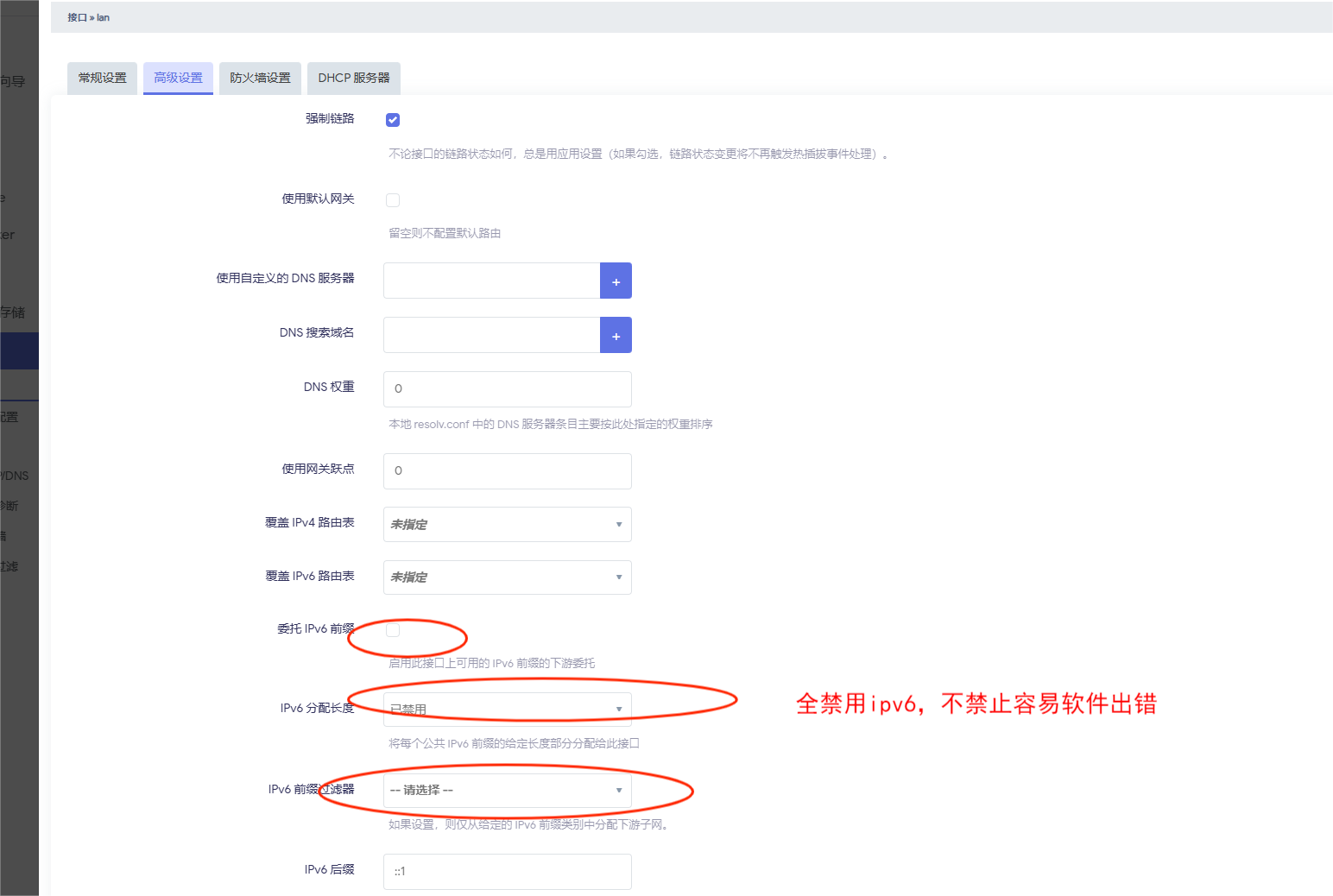
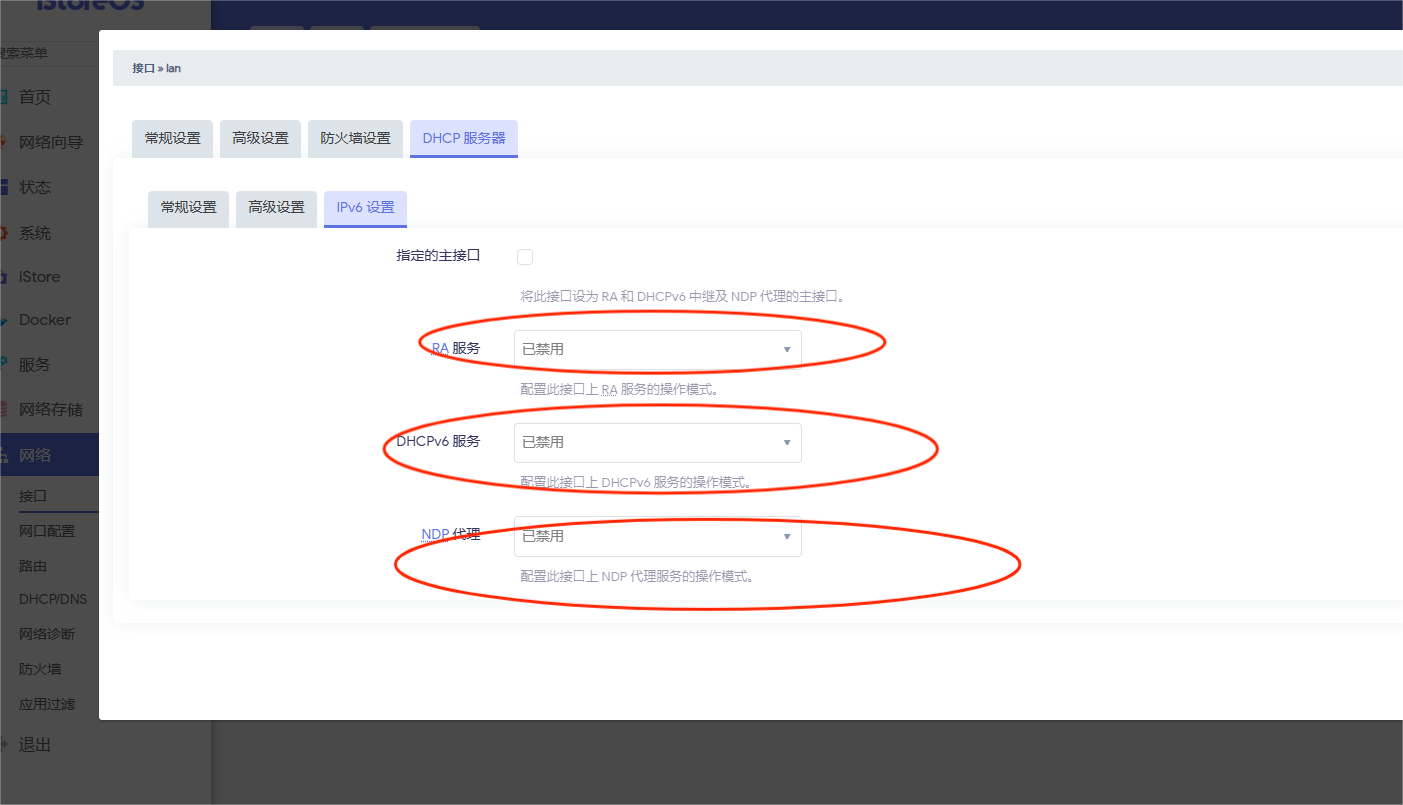
### **软路由关键设置**

### **DHCP/DNS**









### **Openclash关键设置**

****

#### 

### **Adguardhome关键设置**

#### 1、基本知识

-Clash开发者说明书地址https://github.com/vernesong/OpenClash/wiki/%E5%B8%B8%E8%A7%84%E8%AE%BE%E7%BD%AE

##### （1）模式选择建议：

首选Fake-IP（增强）模式

有稳定需求，或对NAT敏感时选择Redir-Host（兼容）模式

**Fake-IP（增强）模式**

客户端进行**通讯时会先进行DNS查询目标IP地址，拿到查询结果后再尝试进行连接**。

Fake-IP 模式在客户端发起DNS请求时会立即返回一个保留地址（198.18.0.1/16），同时向上游DNS服务器查询结果，如果判定返回结果为污染或者命中代理规则，则直接发送域名至代理服务器进行远端解析。

此时客户端立即向Fake-IP发起的请求会被快速响应，节约了一次本地向DNS服务器查询的时间。

实际效果：**客户端响应速度加快，浏览体验更加顺畅，减轻网页加载时间过长的情况。**

**Redir-Host（兼容）模式：**

客户端进行通讯时DNS由Clash先进行并发查询，等待返回结果后再尝试进行规则判定和连接。

当判定需要代理时，使用fallback组DNS的查询结果进行通讯

实际效果：客户端响应速度一般，可能出现网页加载时间过长的情况。

##### （2）DNS

NameServer 走国内DNS

FallBack 走国外DNS

Default-NameServer第一个NameServer选的加密服务器才需要添加此项dns进行解析

（3）127.0.0.1代表本地

127.0.0.1加上端口号等于。指向端口，如127.0.0.1#53