ax3通过container运行clash透明网关，抛弃旁路由，单机自由上网

折腾缘由

最近新买了个mikrotik hap ax3无线路由器，问为什么买就是因为喜欢ros了。

因为想体验完全使用原生ros来上网的感觉，所以这次不想使用旁路由了，否则又要外接个小主机跑openwrt，使用上和观感上都觉得累赘。不像单独使用小主机，装虚拟机跑ros，再装个虚拟机跑openwrt作为旁路由无所谓，因为所有东西都在小主机里面。

但是因为访问外网是刚需，又习惯了使用软路由时电脑和手机只需要接入wifi，无需做任何设置的方便。所以即使在上一篇帖子**"ax3通过container安装clash与yacd网页界面"**中在ax3的container中装好了clash，通过浏览器中安装的switchyomega能访问外网了，也还是不满意，因为要时不时手动打开或关闭SwitchOmega插件，在AX3或者其他软路由的环境中才能正常访问外网。

所以就折腾了快1个星期，终于基本上解决了这个问题，网络配置上网关和dns正常配置为最常规的192.168.1.1的配置，不需要指定为clash运行的ip地址（例如本文中clash配置的ip地址为192.168.1.6），这样就可以使用原生的ros系统来正常访问国内网站，用clash访问国外网站，同时即使container中运行的clash 出了问题，也不影响正常的国内上网，只对访问外网有影响。

Rb5009配置应该也一样，现在到处都买不到价格正常的全新rb5009，前段时间有点魔怔，一直想买rb5009，然后最近这段时间折腾ax3觉得性能也还不错，能满足满速跑pt（300m下30m上）的同时外网看4k60fps的视频，cpu消耗最多偶尔到30%，还带双频wifi，虽然信号一般，但也不是不能用，呵呵，暂时不在纠结rb5009了，有货价格正常了再看看。：）

运行环境

Ros 7.8stable

Ros 的dns 配置为 192.168.1.1 223.5.5.5

Ros的dhcp server配置为网关192.168.1.1 dns配置为192.168.1.1 和 223.5.5.5

Clash安装于192.168.1.6

参考资料及操作

安装配置clash

Clash运行在192.168.1.6中，这里使用的是dreamacro大佬的clash-premium

可参考我的上一篇帖子**“ax3通过container安装clash与yacd网页界面”**，从下面的网址
https://registry.hub.docker.com/r/dreamacro/clash-premium
在container中安装好clash

2楼贴出的是能正常访问外网的clash配置文件，大家在只需要修改里面的服务器配置即可，编辑修改好config.json后，重启clas待用，执行完下面的配置后就能正常访问外网。

配置使用指定dns解析网址的gfwlist列表

https://github.com/ruijzhan/chnroute **持续更新的中国IP 地址列表和gfwlist 域名列表**

上面的帖子中参考小节

3.1 在RouterOS 中用环境变量指定无污染 DNS 服务器

的内容下载好gfwlist.rsc

Ros中创建个脚本，名字任意，例如set_dns_local
内容为
```
{
  :global dnsserver 192.168.1.6;
}
```

自行更改为你对应的clash地址，然后运行这个脚本，然后检查是否设置成功，执行
/system/script/environment/print
查看变量是否设置成功。

然后再执行/im file=gfwlist.rsc
将gfw网址列表导入ros

导入的网址在/ip dns static 中查看

这样ros在发现访问的是gfwlist中的地址后会到我们指定的运行在ip地址例如192.168.1.6中的clash去查询对应的真实ip地址，因为我们配置的clash使用的是fake-ip方式运行，返回的其实是个198.18.*.*段的地址，这样就实现了国外地址的分流。

而如果访问的是国内网站，就会通过我们配置的正常的例如223.5.5.5去查询返回正常真实的国内ip地址。

可以使用ping国外或国内网址来查看是否如上所述。

配置国内ip地址

https://www.truenasscale.com/2022/04/23/1011.html**RouterOS使用IP地址**

列表分流，分流给旁路由或者virtual**

上面的帖子中下载属于中国的ip地址cnip.rsc

下载好后执行
/imfile=cnip.rsc
将国内ip段导入ros

导入的国内ip地址在 /ip firewall address list 中可以看到。

配置路由表
/routingtable
adddisabled=no fib name=gfw_list

配置地址列表
/ipfirewall address-list
add address=198.18.0.0/16list=fake_ip
addaddress=192.168.1.155 list=dont_proxy
add address=192.168.1.6list=dont_proxy

192.168.1.6是clash的地址，所以不需要代理，需要跳过。

192.168.155是我这里用来跑pt的服务器，所以不需要代理。这里做个演示可以配置需要跳过代理的内网ip地址。

重要的是fake_ip这个地址配置，后面的mangle中需要用到，发现是目标地址是fake_ip地址段的都送到clash的192.168.1.6去代理出去

配置路由标签

/ipfirewall mangle

add action=acceptchain=prerouting src-address-list=dont_proxy
#发现是不需要代理的地址例如是clash的ip地址就通过

**add action=mark-routingchain=prerouting dst-address-list=fake_ip dst-address-type="" **
in-interface-list=LANnew-routing-mark=gfw_list passthrough=yes
#发现目标地址是fake_ip的地址，说明是需要代理的地址，标记成gfw_list路由表，准备通过下面配置的路由送到clash所在的192.168.1.6处理，达到访问外网的目的

**add action=mark-routingchain=prerouting dst-address-list=!CNIP dst-address-type=!local **
in-interface-list=LANnew-routing-mark=gfw_list passthrough=yes

#上面是发现漏网之鱼的访问，只要是访问非中国区的ip地址，都送往clash进行代理访问
#我对ros的防火墙不太熟悉，这里只是个能使用的配置，优化请有兴趣改进的大佬不吝指点。

addaction=change-mss chain=forward comment="Change MSS"new-mss=clamp-to-pmtu \
passthrough=yes protocol=tcp tcp-flags=syn

addaction=change-mss chain=output comment="Change MSS"new-mss=clamp-to-pmtu \
    passthrough=no protocol=tcp tcp-flags=syn

配置路由处理

/ip route
add check-gateway=pingdisabled=no distance=1 dst-address=198.18.0.1/16 gateway=
**   192.168.1.6 pref-src=""routing-table=gfw_list scope=30 suppress-hw-offload=no **
target-scope=10

重要，将上面mangle通过访问fake_ip段的已经标记**routing-table=gfw_list**的访问重新送往clash，clash发现目标地址是fake_ip段，在内部进行处理，使用代理服务器进行连接，达到上外网的目的。

特别注意，特别注意，特别注意，
上面这条命令中将新建的路由的distance（优先级）配置为1

需要将你原来的上外网的接口的优先级配置为2，

例如我是通过拨号上网的，则在 interface中，双击pppoe-out1，点击dial out，将里面的default route distance修改为2

使用其他连接上网的操作类似。

防火墙优化

https://www.shawnleetttt.cyou/posts/71e7c44b/ RouterOS+旁路由IP地址列表分流

参考其中的

修改 ROS 默认防火墙
打开 IP > Firewall > FilterRules
找到 **action=drop chain=forward comment="drop invalid" connection-state=invalid** 这一条,双击打开,将 General 下的 In. Interface List 改为 !LAN 防止防火墙将加密过后的流量标记为 invalid 而造成 TCP 流量握手缓慢

这条 **防止防火墙将加密过后的流量标记为 invalid 而造成 TCP 流量握手缓慢** 似乎是有用的，我最初刚刚成功的时候，能访问外网，但是打开页面非常慢，7,8秒钟才能打开外网网页，后面不知道是clash的配置做好了，还是这条配置有用，估计是clash的配置做好了，这条可能是锦上添花，后面继续测试吧。

修改 Fasttrack 相关
打开IP > Firewall > FilterRules
打开 fasttrack connection ,将 General 下的 In. Interface List 改为 PPPoE 端口名称防止 Fasttrack 与 Mangle 冲突
我这里是将ax3的fasttrack中对应的这条更改成pppoe-out1

遗留问题

Tele使用问题

因为我们这里使用了clash的fake_ip机制通过域名代理来访问外网，对tele这种直接使用ip访问外网的的app就代理不了了。

https://blog.lv5.moe/p/use-dns-to-create-split-routing-for-different-domain-or-ip-ranges

巧用 DNS 实现国内外域名 ip 分流上网中

为直接使用 IP 的 APP 设置路由 这一节给出了个解决方案

直接使用 ip 的软件没有经过 DNS 自然就无法获取到Clash 的 fake-ip，对于这种情况需要在主路由上添加静态路由将这些软件使用的 ip 的下一跳路由改为 Clash 的 fake-ip
目前我只发现 Tele 存在这种情况，需要添加的路由如下：
192.18.1.254 是 fake-ip，可以从 fake-ip-range 中随便选择一个route add -net 91.108.4.0/22 gw 192.18.1.254route add -net 91.108.8.0/22 gw 192.18.1.254route add -net 91.108.12.0/22 gw 192.18.1.254route add -net 91.108.16.0/22 gw 192.18.1.254route add -net 91.108.56.0/22 gw 192.18.1.254route add -net 149.154.160.0/20 gw 192.18.1.254

但我对ros还不太熟，不知道上面这个操作怎么完成，在mangle中使用prerouting的action配置为route来没有实现。希望有大佬能够指点下。

看网上资料说clash的tun配置中配置auto_route为true能解决这个问题，但是因为ros的container不完善还是不标准，配置这个参数后启动输出一条警告，说参数错误，估计是ros的container没有privilge特权模式造成的。

好了，做到这里，ax3已经能够单独流畅透明的访问外网了，不需要在配置一台小主机来作为旁路由啥的，当然如果有需要，也是可以装个小主机openwrt来配合ax3更好的上网的，看个人需要了。