陆初

脑子不太好用的普通人。

终于稳定实现校园网免流

说起来，我好像很久没有写和计算机有关的文章了……

> *终于做到了同时上内网和外网*

前情提要

大家好久不见。

距离上一次真真正正写有用的东西已经经过了好久啊……在这期间其实发生了不少的事情，不过现在也不需要记录了。写这篇东西主要是想记录实现最终目的一个过程，仅此而已。

最终目的：在校园网覆盖范围内让外网流量通过宿舍转发，达到免流上网。

要达到这个最终目的，我需要做两个工作：

1. 让宿舍内的一台设备可以同时上内网和外网，并且可以自动判断该走哪个。
2. 让这台设备可以接收到来自校园网的流量，并且转发。（也就是作为一个正向代理服务器）

完成工作1：

有关第一个工作，其实已经在前请提要的那篇文章讲过了。采用的方法无非就是调路由表，只不过不是调整我的笔记本电脑，而是调整路由器/树莓派而已。

修改这两种功能设备的路由表的唯一区别就是：windows和linux修改路由表的语句格式不一样。其逻辑都是差不多的，网上搜一下「linux如何修改路由表」，到处都有方法，这里就不讲语句了。

整体拓扑图大概长这样（
拓扑图中的椭圆形：指不是直接有一条物理链路连接到两端，中间可能会有多条不同的链路）

以下的用词可能会引起歧义，所以在某种情况下这两个词等价，如果觉得理解困难不妨尝试代换一下。

内网：指校园网

外网：指联通宽带

实际上，上校园网和联通网用的是同一个网线口，把网线插进去后，默认会得到网络中心DHCP方式提供的ip，此时就可以通过物理链路（以太网）连接到校园网。然后再随便打开一个网页验证一下校园网账号就能通过校园网上外网了。

连接联通宽带的话，则是通过PPPoE方式，使用运营商提供的账号和密码登录，就可以通过联通宽带上网了。

所以，理论上来讲，插入网线后再通过PPPoE拨号，设备就会有两个网络接口（linux设备会显示eth0和ppp0）。

然后只要配好路由表（某个ip网段该走校园网还是外网），一条网线可以做到同时上两个网。
例如，宿舍楼的有线网关的ip是10.x.x.254，如果我要通过有线网关上内网的话，只要配置10.0.0.0/8这个网段的下一跳是10.x.x.x254就好了。

如果路由器是一个linux设备，那只需要配置好宿舍内的路由器，把转发的工作交给路由器就好。所有连接上宿舍路由器的设备都可以同时上内外网而不需要做额外的配置。根本就不需要多加一个树莓派当做转发路由器。

那么在这里为什么还要多此一举要多一个树莓派连上路由器呢【

那当然是有原因的。

宿舍采用的路由器十分垃圾……在使用PPPoE方式上网之后，路由表就会写死。

刚才那样例子，写了一个10.0.0.0/8下一跳是10.x.x.254的路由表项后，它会自己添加一个10.x.x.254走PPPoE对端（也就是图中蓝色那条线）的路由表项，也就是，必须走联通宽带。根本没办法访问内网。

所以我的路由器无法成为一个能同时上内外网的设备。

那怎么办呢，只能曲线救国了。

解决方法：

一个宿舍有四个人，每个宿舍位置都有一个网线口。

路由器通过我舍友的网线口接入联通宽带，而我的网线口则与树莓派连接，同时树莓派的WLAN连接上宿舍路由器的无线网。

然后再对树莓派的路由表进行配置。

这样，我的树莓派就达到了我对设备的要求：能同时上内外网。

其实修改完路由表之后，任务1差不多就已经完成了。

额外问题（DHCP带来的麻烦）：

配置完路由表后，我遇到了一个说大不大说小不小的问题。

由于内网地址是通过DHCP分配的，隔一段时间路由表就会因为DHCP重新分配地址而刷新一下。在我这边则体现为，增加了一条应该删除的路由表项：

```
Kernel IP routing table
Destination     Gateway         Genmask     Flags   Metric  Ref Use     Iface
0.0.0.0         10.25.25.254    0.0.0.0     UG      202     0   0       eth0
```

这样会导致路由表有相互冲突的表项：

```
Kernel IP routing table
Destination     Gateway         Genmask     Flags   Metric  Ref Use     Iface
0.0.0.0         10.25.25.254    0.0.0.0     UG      202     0   0       eth0
0.0.0.0         192.168.1.1     0.0.0.0     UG      303     0   0       wlan0
```

（192.168.1.1是路由器的地址）

这时候树莓派就不知道要选哪个路由项转发IP包了。

在我这里的情况为，选择走校园网。

就算删掉了这一项，每隔几分钟还是十几分钟DHCP还是会把它加回来，体现到具体情况就是每隔一段时间就会断网，然后我要手动删掉那一项才能恢复正常。

这可太麻烦了【。

就算写了一个脚本，那也还是要每隔几分钟就运行一下这个脚本。

就算设置了自动每隔一段时间运行，那在运行的时候也会突然断一下网，造成的影响还是有的。

在查了google啊百度啊必应啊看了各种抄来抄去和被抄的CSDN博客后，得知可以修改Metric这个值。

Metric值越高，优先级越低。现在回过头来看上图，会发现走校园网的Metric比较低，所以会走校园网。

那么就简单了。我只要把走校园网那一项的Metric删掉，然后把走联通网那一项的Metric改到0，就算刷新了也还是会走联通网吧?

结。果。

DHCP牛逼啊！不仅会修改自己的Metric还会修改其他的表项的Metric！！！

Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 10.25.25.254 0.0.0.0 UG 202 0 0 eth0
0.0.0.0 192.168.1.1 0.0.0.0 UG 303 0 0 wlan0

我手动设置的0会变成303。

妈个鸡哦。

然后我一气之下加了好多条一样的路由，Metric分别是1,2,3。

Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface

0.0.0.0 192.168.1.1 0.0.0.0 UG 1 0 0 wlan0

0.0.0.0 192.168.1.1 0.0.0.0 UG 2 0 0 wlan0

0.0.0.0 192.168.1.1 0.0.0.0 UG 3 0 0 wlan0

0.0.0.0 10.25.25.254 0.0.0.0 UG 202 0 0 eth0

0.0.0.0 192.168.1.1 0.0.0.0 UG 303 0 0 wlan0

最后会变成这样。

结果还真的歪打正着，多条路由的话就不会被修改了，所以也不会断网了。

可喜可贺。

到这里，任务1就真的完美结束了。

完成工作2：

完成工作1之后，工作2就变得很简单了。

打通了路由表后，树莓派拥有校园网的一个内网ip，处于校园网内的设备都可以连接到树莓派。

树莓派只需要提供一种代理服务就好。

我采用了两种方式。

1.SHADOWSOCKS

大名鼎鼎的ss，不用多说。

不知道为什么我的树莓派没有办法运行libev版……反正也不是为了科学上网，旧一点也没关系，所以采用版本老旧的python版。

按照教程安装完，写好json配置文件，再开启服务就好。

网上到处都有教程啦，这个就不用多说了。搜「shadowsocks 配置 服务端」一大堆。

想要无线流量上网的话，只要装好ss客户端再，填好配置，再连接就好。

缺点：无法真正全局。

根据客户端的不同，不一定能做到全局流量都跑ss，某些客户端就算开了全局模式，有些流量还是不能走ss……（例如 iOS 的 shadowbroken 就没有办法让啤梨啤梨的视频走代理）

就算配合proxifier一起使用，还是会有走不了的ss流量（没错说的就是那堆混蛋的win10 metro应用，包括edge）。

2.VPN（PPTP）

这个也是大名鼎鼎了，甚至已经成为【哔——】上网的代名词。

VPN全称 virtual private network ，本质上是提供一个能够加密内容的隧道，把所有的流量定向转发到VPN服务器，由服务器代理所有的上网。

用这种方式，可以确保所有的流量都走到我的树莓派上。

（说来好笑，VPN在【哔——】上网中的缺点在我这里反而变成了优点）

有几种协议可以实现VPN。PPTP，L2TP，openVPN都是可以采用的协议。

pptp在树莓派上比较好部署，所以我选择了pptp。

（顺便说一下，pptp已经被证明不够安全了，ios和mac os的系统原生VPN客户端好像也已经不支持pptp了。由于我只是想完成一个路由转发的功能，而且流量是在校园网内走的，所以对安全没有多大的要求，就采用了pptp，有安全要求的就不要选pptp了吧。）

https://blog.csdn.net/dongdong9223/article/details/80790203

↑ 我所参考的文章，按照这个一步一步走就差不多了。

比较重要的步骤就两个，

> *修改 /etc/sysctl.conf：*

> *把 net.ipv4.ip_forward=1 的注释去掉。*
>
> *第二个就是配置防火墙（iptables）：*
>
> *iptables -t nat -A POSTROUTING -s 192.168.2.0/16 -o eth0 -j MASQUERADE*
>
> *//是ifconfig得到的IP*
>
> *iptables-save > /etc/iptables.pptp*
>
> *// 保存防火墙状态*

在我这边的话，配置防火墙的部分不同。

我的树莓派有两个网络接口，eth0是校园网，wlan0是联通网，所以需要两个端口都参与转发。

// 我给vpn客户端保留的ip段为192.168.2.0/24

iptables -t nat -A POSTROUTING -s 192.168.2.0/24 -o eth0 -j MASQUERADE

iptables -t nat -A POSTROUTING -s 192.168.2.0/24 -o wlan0 -j MASQUERADE

按照上面那个博客的流程走完之后，我的手机就可以通过VPN上网了！

耶！！！大功告成！

……在我用电脑连之前，是这么想的。

今天下午上实验课的时候我用电脑连了一下VPN，虽然成功连上了。但是居然……上不了网？？？？

浏览器显示的是「找不到www.baidu.com对应的ip」。

噢，那就是DNS出问题了嘛。我没有配置dns，行，那就配置dns呗。

打开 /etc/ppp/pptpd-options ，在 ms-dns 字段填写 dns 服务器的地址，保存。

好，这下应该行了吧。

结果……

还是不行。

这次更狠，直接显示「无法连接到服务器」。也就是说我根本连不上网。

这……？咋回事？

这时候，就该解决问题了。

DEBUG阶段：

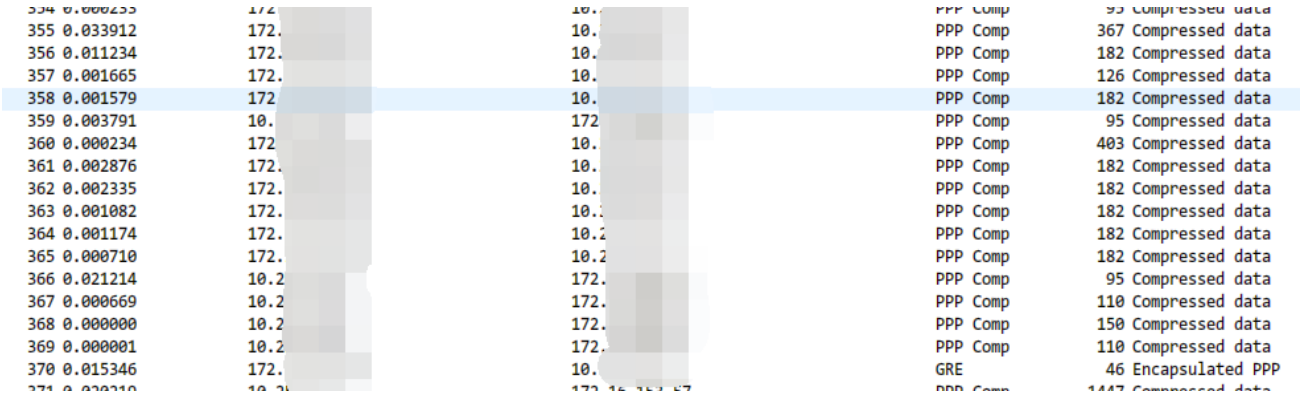
现在可以确认的事实有：

1. 我的电脑已经连上了树莓派的VPN服务器
2. 我的电脑没有办法通过浏览器访问网络
3. 我的手机可以连上树莓派的VPN服务器并且正常上网

根据事实1，可以确定从我的电脑到树莓派这段路是绝对没有问题的。

也就是说，是树莓派访问外网，或者是树莓派到我的电脑，这两条路的某个地方出了问题。

遇到网络问题肯定要先抓包了，那么，wireshark启动！



结果是抓到一堆PPP包

这就神奇了，按照抓包结果来看，我的电脑和树莓派之间是正常通信的，没有任何一方有收不到包或者发不出包的问题。

那么问题就应该不是出现树莓派到我的电脑这条路径上。

在我完全没有头绪的时候，我随便点开搜藏夹的网站，然后发现，必应，和某些内网站点，居然能打开！

这就说明网络本身应该是通的，只是因为什么策略问题包被过滤了或者丢弃了。

然后我就开始以「pptpd linux 无法打开网页」之类的关键词去搜索，结果搜到了这么一句话：

> *如果VPN服务器是用来代理上网的，仅有上面的配置会出现访问网站缓慢的情况，需要手动修改一下转发包的mss*

https://www.nigesb.com/setup-your-own-vpn-with-pptp.html

虽然我的情况是根本上不了网而不是缓慢就是了。

然后我再以「pptp mss」为关键词搜索，找到了这篇关键的文章：

http://www.361way.com/pptp-mtu-mss/5173.html

里面有这么一段话：

> *这里假设连接vpn 进行上面的一台主机为A主机，提供VPN服务的主机为B主机。能过 tcpdump抓包会发现会有unreachable -need to frag (mtu 1396)这样的提示。主机B返回了一个ICMP不可达的差错报文。其含义是VPN主机收到了一个需要分片才能通过的数据包，而这个数据包在其IP头部又设置了不能分片（DF）的标志。所以该数据包不能通过VPN主机。*

卧——槽——

吓得我赶紧远程树莓派用tcpdump抓了包试试看，结果发现还真的是这么一回事！

那么事情就好办了，原因就是mtu在搞鬼。

在网上找了很多修改的语句在我这都不适用……不知道为什么。

最后用了这一句：

iptables -I FORWARD -p tcp –syn -i ppp+ -j TCPMSS –set-mss 1356

连上VPN，打开网页！

好了！总算能打开了！大功告成！

估计接下来很长一段时间都会用这个方式来进行免流了。

（顺便吐槽一点，不知道为什么我用的两台手机都不能一直开着VPN。只要开了VPN，某些时候它在后台就会给我关掉。每隔一段时间就要手动打开，啊靠，真的累）

作者： 陆初

脑子不太好用的普通人。 顺带一提性格也有点古怪。 在老妈子和厌世肥宅中来回切换。

查看陆初的所有文章

陆初 / 2019-05-22 / 网络 /

《终于稳定实现校园网免流》有4个想法

Vivid

2019-05-27 18:15

大佬都喜欢写这么硬核的文章的吗…

🙃🙃🙃

是说我什么时候才能写出这么长篇幅的文章啊

每次都是等到要写什么的时候就不知到该写什么

陆初

2019-05-31 15:09

其实这个并不硬核啦，只是简单的配置而已，业内黑话比较多，没学过的人看不懂很正常的【
其实我也不想写这么长的，可是流程就是有那么长我也没办法orz

Vivid

2019-06-03 16:14

免流是免流量吗？是说大佬学校的校园网是按流量计费的？感觉有点坑……

还是我理解错了吗……

我这里是按月租固定计费的，网络感觉还行吧，就是联机打游戏很难受。

明明是国内的服务器，但是不用加速器就是不让你连得上。

🙁

陆初

2019-06-08 10:54

正是如此哦，校园网是按流量计费的。现在大概是一天2g吧。