网络拓扑结构如下图所示



下面说搭建的过程

需要说明的是，这个网络拓扑是在vmware中搭建的。

一 准备工作

1 下载openwrt的镜像，openwrt是一个虚拟化的路由器。

2 下载开源的防火墙ipfire

3 配置三个虚拟网桥vmnet2-vmnet4

4 准备至少2台虚拟机

二 安装openwrt路由器

1 下载openwrt的img或者vmdk文件

如果找不到vmdk文件，那么使用starwindconverter工具转换成vmdk即可。

下载链接：<http://cy.198443.com/starwindconverter.zip>

2 使用现成的虚拟机安装openwrt

假设VMware中已经装好了一个不用的linux虚拟机，那么直接进入该虚拟机的文件夹中，将该虚拟机的vmdk虚拟磁盘文件替换成我们转换好的openwrt的磁盘文件

图形用户界面, 表格

描述已自动生成

直接替换就完事了。

接着在VMware中设置该虚拟机

图形用户界面, 文本, 应用程序

描述已自动生成

把方框里的路径替换成openwrt的vmdk文件路径即可；

3 启动虚拟机完成openwrt的安装。

三 安装ipfire

1 下载ipfire的ISO文件

这个直接官网下载即可。

<https://ftp.yz.yamagata-u.ac.jp/pub/network/security/ipfire/releases/ipfire-2.x/2.25-core157/ipfire-2.25.x86_64-full-core157.iso>

2 安装

在VMware新建虚拟机，系统选择linux较高版本即可，然后点击下一步正常安装。需要注意的是路由器和防火墙的cpu、内存不需要很高，防火墙的硬盘大小设置为8G即可。

图片包含 日程表

描述已自动生成

3 启动

启动部分在后面讲。

四 配置各个机器的网卡信息

在上面的路由器和防火墙安装完成之后，默认安装完成了2台linux和windows虚拟机。

网桥对应ip段如下：

vmnet2 192.168.6.0/24

vmnet3 192.168.5.0/24

vmnet4 192.168.7.0/24

1 路由器网卡信息

图形用户界面, 应用程序

描述已自动生成

需要注意的是，网卡的名称一般都是eth0-eth\*，编号的顺序是与网络适配器的顺序一致，只不过从0开始编号而已。

2 ipfire防火墙网卡信息



3 pc终端网卡信息

内网终端：

图形用户界面, 应用程序

描述已自动生成

外网终端：

图形用户界面

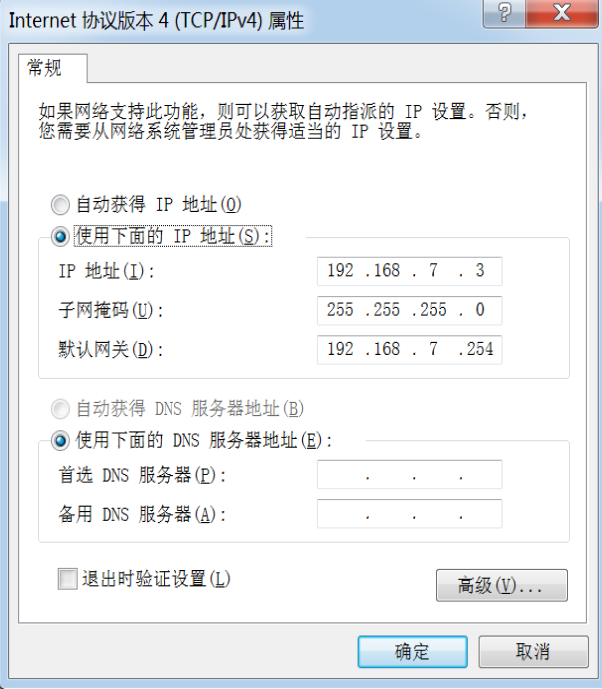
描述已自动生成

--------------------------------------------------------------------------

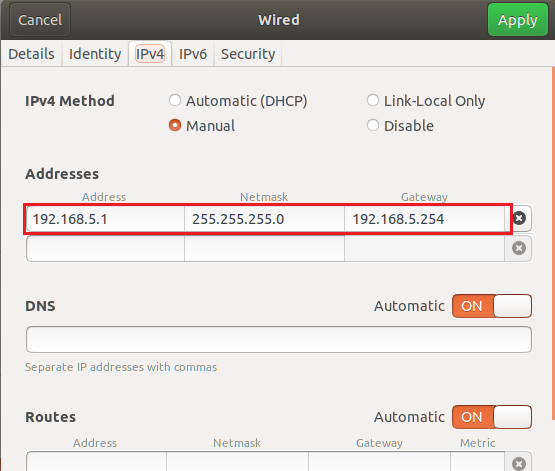
把各个机器的网卡配好以后，就需要到每台机器上配置ip、网关、子网掩码，到路由器防火墙上修改配置。

pc的网络配置很简单，不写在笔记里了。

外网pc



内网pc



--------------------------------------------------------------------------

五 路由器配置

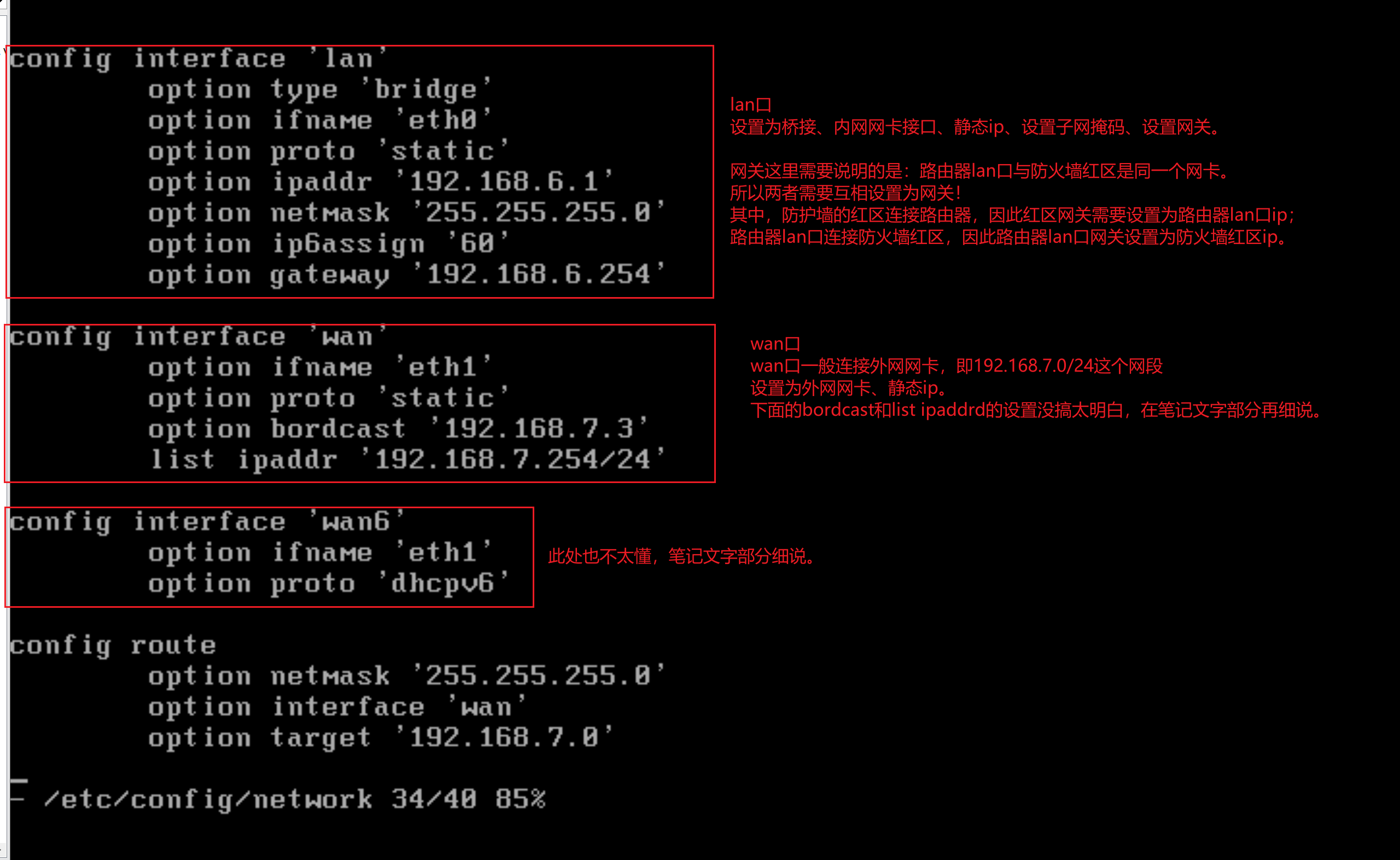
1 开机进入路由器命令行界面

openwrt是基于linux内核开发的，所以命令与linux一致

a 修改网络配置

配置信息说明在截图中有写

vim /etc/config/network



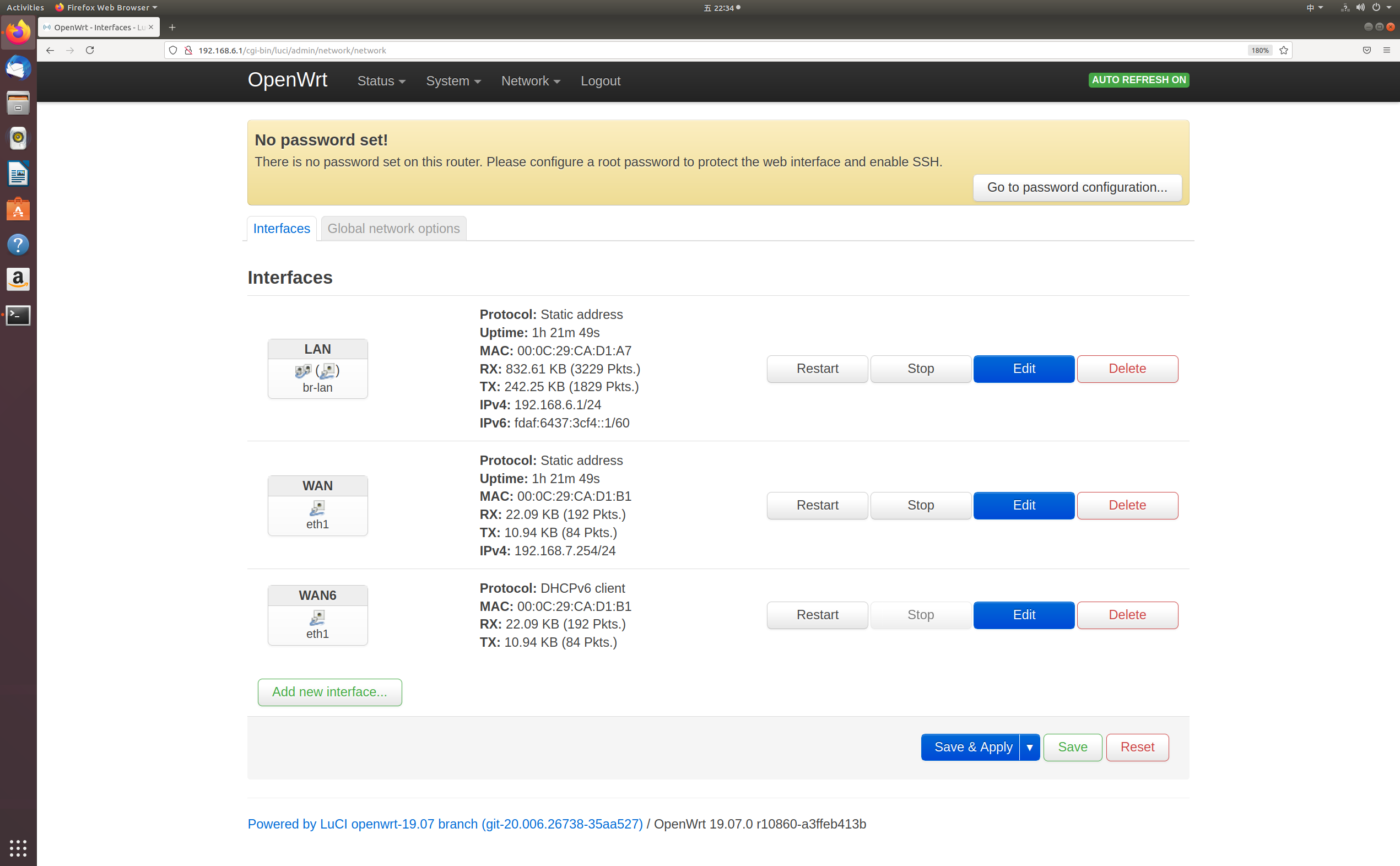
b web管理界面配置静态路由

这一步需要在内网pc可以ping通路由器lan口ip之后进行。

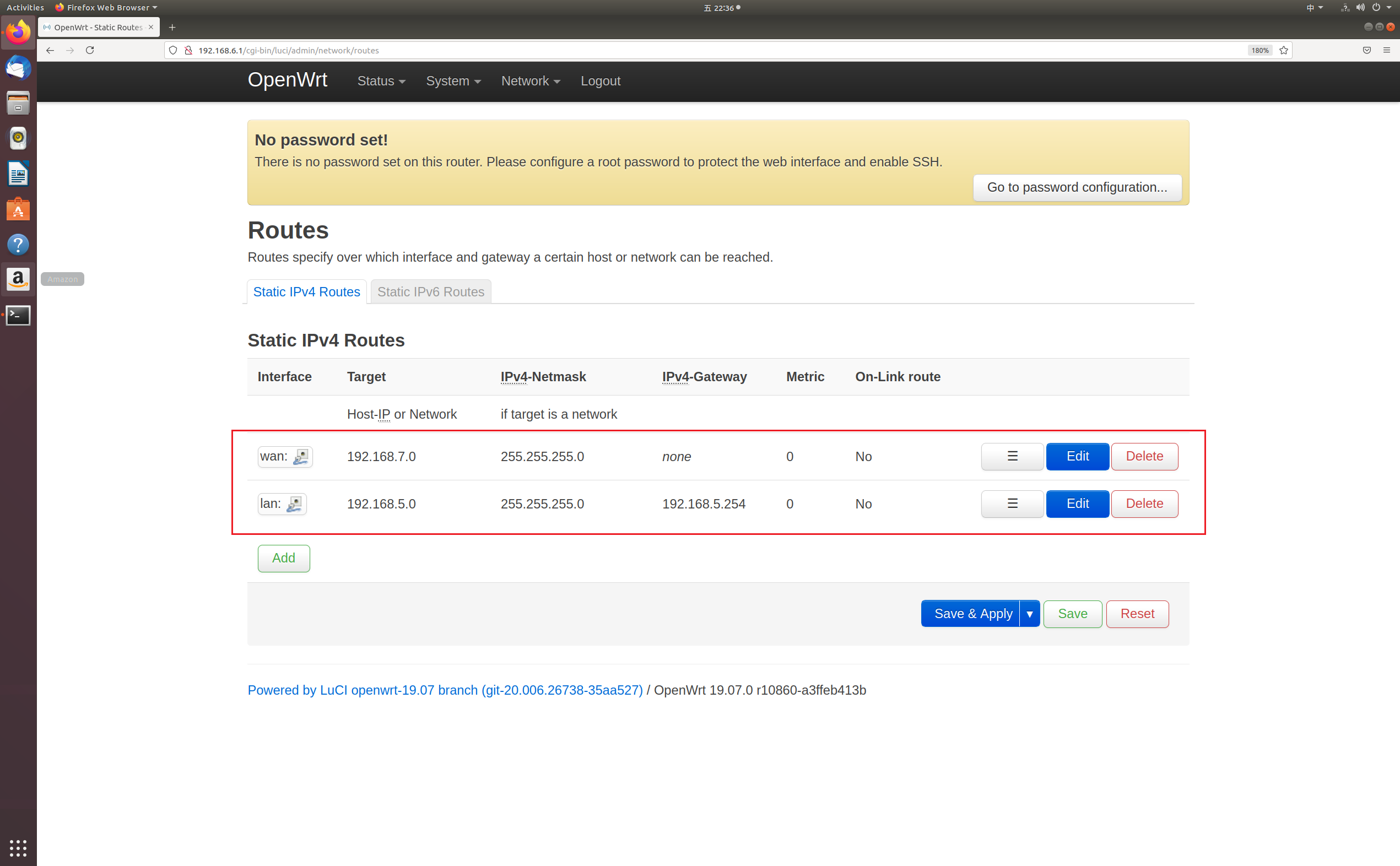
访问ip

192.168.6.1

密码默认为空，点击登录即可进入管理界面



进入静态路由设置界面



静态路由设置说明：

为什么要设置静态路由？

因为路由表中没有任何信息，需要我们自己去给它添加静态路由告诉它该去找哪个网关。

设置思路：

内网pc需要访问外网pc，需要从wan口的出去找外网pc，因此网口选择wan口，目的ip选择外网pc所在网段，由于外网pc的网关就是路由器，所以不需要填写网关。

外网pc访问内网pc，需要从lan口的出去找内网pc，因此网口选择lan口，目的ip选择内网pc所在网段，网关填写内网pc的网关。

六 防火墙配置

1 启动ipfire虚拟机

经过设置语言、时区、账号密码等信息之后，开始网络相关的配置

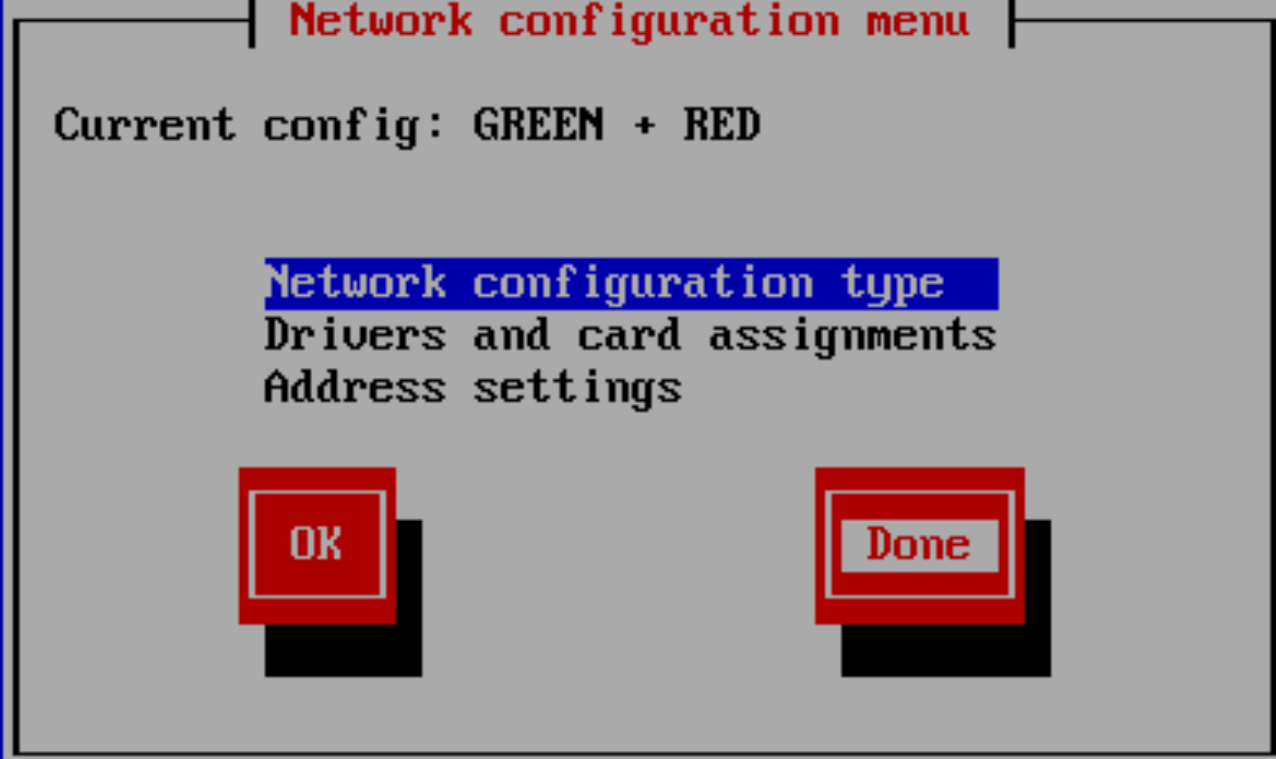
2 network配置

选择network

图形用户界面

描述已自动生成

选择网络配置类型，即防火墙分区选择，选择红+绿即可



文本

描述已自动生成

接着选择第二项配置网卡信息，绑定网卡mac

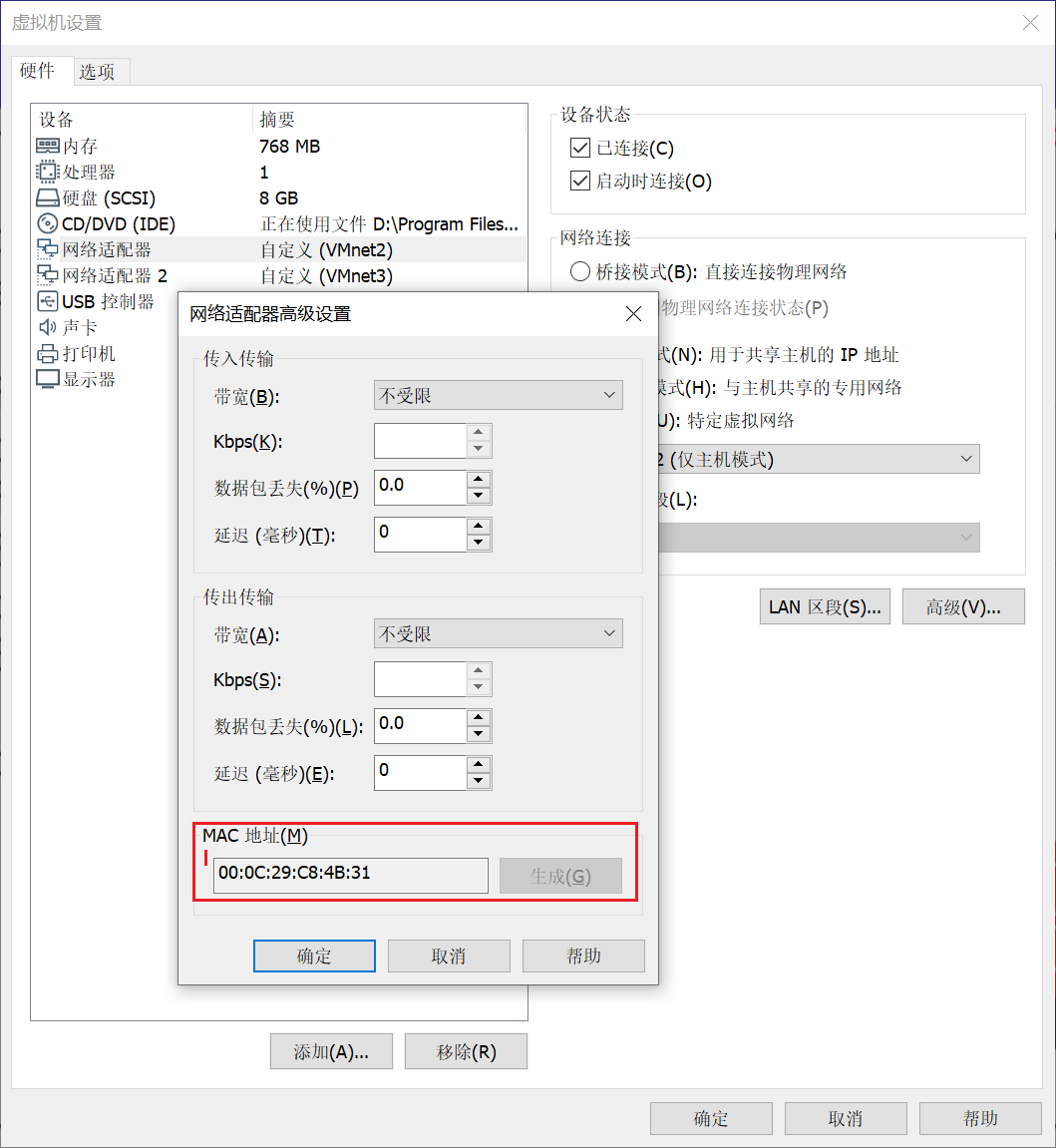
图片包含 图示

描述已自动生成

图形用户界面, 文本

描述已自动生成

网卡mac不要选错了，mac地址在虚拟机设置中的网络适配器-高级中查看



接着选择地址设置，地址设置分为红绿区两个部分

首先是绿区的配置

图片包含 文本

描述已自动生成

绿区不需要配置网关

下面是红区的配置，需要设置静态ip和网关，网关设置为相邻路由器的lan口ip即可。

图形用户界面, 文本

描述已自动生成

防火墙在虚拟机中的配置完成

3 防火墙规则配置

a 在内网pc浏览器中访问绿区ip

图形用户界面

低可信度描述已自动生成

b 配置规则

总体规则如下：

图表, 条形图

描述已自动生成

具体配置如下：

图形用户界面

描述已自动生成

图形用户界面

低可信度描述已自动生成

其他的选项和更多的规则配置后面再摸索，现在的规则相当于所有流量都是可以通过的。

七 效果展示

文本

描述已自动生成文本

描述已自动生成