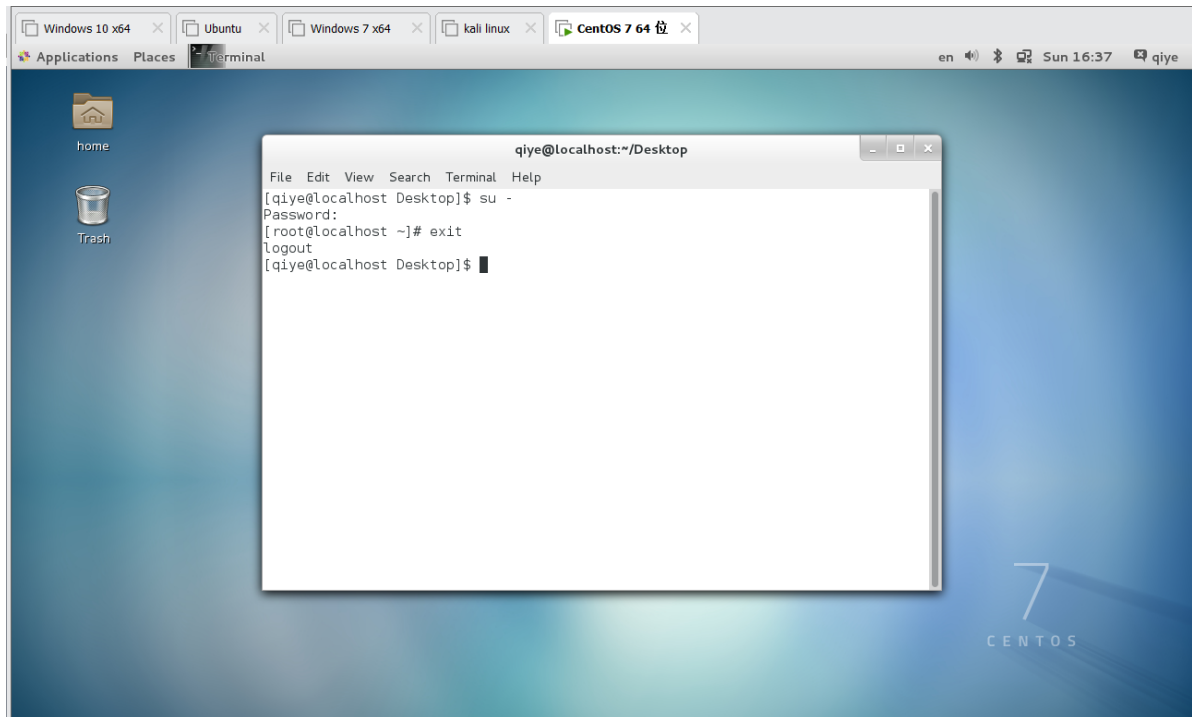


实训

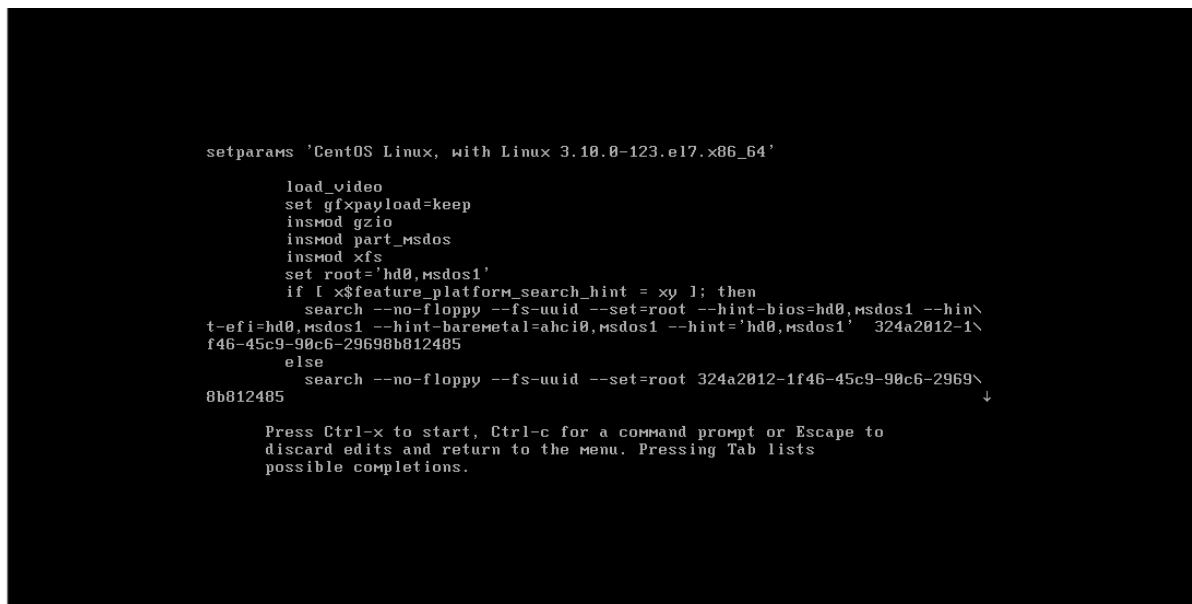
GRUB2的使用

1.忘记root密码怎么办？

首先，我们先把root密码忘了，然后重启（reboot）



在GRUB2启动屏显时，按下e键进入编辑模式



然后我们定位到linux16开头的行，按下end键直接来这段命令的末尾，并增加 rd.break，ctrl+x一下

```

[ 2.303607] sd 0:0:0:0: [sda] Assuming drive cache: write through
[ 2.306453] sd 0:0:0:0: [sda] Assuming drive cache: write through
[ 2.309916] sd 0:0:0:0: [sda] Assuming drive cache: write through

Generating "/run/initramfs/rdsosreport.txt"

Entering emergency mode. Exit the shell to continue.
Type "journalctl" to view system logs.
You might want to save "/run/initramfs/rdsosreport.txt" to a USB stick or /boot
after mounting them and attach it to a bug report.

switch_root:/# _

```

进入emergency mode界面

我有个信息收集的习惯，先fuzz一下

命令如下：

```

whoami
ls
mount

```

可以发现的是，当前是无用户情况的系统调试界面,而且xfs是只读

```

switch_root:/# whoami
sh: whoami: command not found
switch_root:/# ls
bin dev dracut-state.sh etc init lib lib64 proc root run/sbin shutdown sys sysroot tmp usr var
switch_root:/# mount
rootfs on / type rootfs (rw)
proc on /proc type proc (rw,nosuid,nodev,noexec,relatime)
sysfs on /sys type sysfs (rw,nosuid,nodev,noexec,relatime)
devtmpfs on /dev type devtmpfs (rw,nosuid,size=493268K,nr_inodes=123317,mode=755)
securityfs on /sys/kernel/security type securityfs (rw,nosuid,nodev,noexec,relatime)
tmpfs on /dev/shm type tmpfs (rw,nosuid,nodev)
devpts on /dev/pts type devpts (rw,nosuid,noexec,relatime,gid=5,mode=620,ptmxmode=000)
tmpfs on /run type tmpfs (rw,nosuid,nodev,mode=755)
tmpfs on /sys/fs/cgroup type tmpfs (rw,nosuid,nodev,noexec,mode=755)
cgroup on /sys/fs/cgroup/systemd type cgroup (rw,nosuid,nodev,noexec,relatime,xattr,release_agent=/usr/lib/systemd/systemd-cgroups-agent,name=systemd)
pstore on /sys/fs/pstore type pstore (rw,nosuid,nodev,noexec,relatime)
cgroup on /sys/fs/cgroup/cpuset type cgroup (rw,nosuid,nodev,noexec,relatime,cpuset)
cgroup on /sys/fs/cgroup/cpu,cpuacct type cgroup (rw,nosuid,nodev,noexec,relatime,cpuacct,cpu)
cgroup on /sys/fs/cgroup/memory type cgroup (rw,nosuid,nodev,noexec,relatime,memory)
cgroup on /sys/fs/cgroup/devices type cgroup (rw,nosuid,nodev,noexec,relatime,devices)
cgroup on /sys/fs/cgroup/freezer type cgroup (rw,nosuid,nodev,noexec,relatime,freezer)
cgroup on /sys/fs/cgroup/net_cls type cgroup (rw,nosuid,nodev,noexec,relatime,net_cls)
cgroup on /sys/fs/cgroup/blkio type cgroup (rw,nosuid,nodev,noexec,relatime,blkio)
cgroup on /sys/fs/cgroup/perf_event type cgroup (rw,nosuid,nodev,noexec,relatime,perf_event)
cgroup on /sys/fs/cgroup/hugetlb type cgroup (rw,nosuid,nodev,noexec,relatime,hugetlb)
configfs on /sys/kernel/config type configfs (rw,relatime)
/dev/sda3 on /sysroot type xfs (ro,relatime,attr2,inode64,noquota)
switch_root:/#

```

那就以读写的方式挂载给我改下密码：

```

mount -o remount,rw /sysroot      #以读写方式重新挂载系统分区至/sysroot
chroot /sysroot                  #改变根目录至/sysroot

```

```

/abc/suad on /sysroot type xfs (ro,relatime,attr2,noexec,no
switch_root:/# pwd
/
switch_root:/# id
sh: id: command not found
switch_root:/# id root
sh: id: command not found
switch_root:/#
switch_root:/#
switch_root:/#
switch_root:/#
switch_root:/#
switch_root:/#
switch_root:/# mount -o remount,rw /sysroot
switch_root:/# chroot /sysroot
sh-4.2# whoami
root
sh-4.2#

```

可以发现，我们通过改变根目录方式来使用root用户，那么改变密码也成为可能
本菜鸡只会两种改变密码的命令：

```

echo 123 | passwd --stdin root          //本次实训所用
passwd root

```

```

switch_root:/# id
sh: id: command not found
switch_root:/# id root
sh: id: command not found
switch_root:/#
switch_root:/#
switch_root:/#
switch_root:/#
switch_root:/#
switch_root:/#
switch_root:/# mount -o remount,rw /sysroot
switch_root:/# chroot /sysroot
sh-4.2# whoami
root
sh-4.2# echo 123 | passwd --stdin root
Changing password for user root.
passwd: all authentication tokens updated successfully.
sh-4.2#

```

SELinux 它是一个安全增强系统, 其内部有许多安全策略
针对一些操作, 如果你做了这些操作, 没有得到策略的放行, 它会给你禁止掉
比如你使用单用修改root密码是不被策略放行的
怎么让 SELinux 策略放行呢?

- ☒ "touch /.autorelabel" 创建这样一个文件其实就是在告诉SELinux放行这个策略, 就是通知一下
- ☐ 直接关闭掉 SELinux

参考: <https://blog.csdn.net/songhaixing2/article/details/109780512>

由于使用了SELinux, 必须运行:

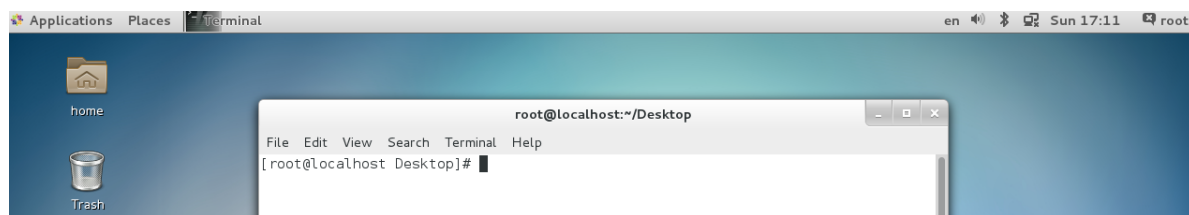
```
touch /.autorelabel
```

否则系统无法正常使用

```
Changing password for user root.  
passwd: all authentication tokens updated successfully.  
sh-4.2# touch /.autorelabel  
sh-4.2# exit  
exit  
switch_root:/# reboot
```

退出当前用户，重启system

登录root，密码123（原密码为：qiye）



可以发现成功登录root，ya☆da☆ze！

2.加把安全锁

用安全角度来看，能够使用GRUB2直接修改root密码，无疑是一种提权方法，是一种安全漏洞这就相当于，只要别人知道你家地址，便能直接进你家，所以就常识而言，为了安全，加把锁很重要

使用grub2-mkpasswd-pbkdf2 命令生成加密口令

这里密码为：qiye

```
[root@localhost Desktop]# grub-mkpasswd-pbkdf2  
bash: grub-mkpasswd-pbkdf2: command not found...  
[root@localhost Desktop]# grub2-mkpasswd-pbkdf2  
Enter password:  
Reenter password:  
PBKDF2 hash of your password is grub.pbkdf2.sha512.10000.3D4FFC21A4D44D1B2431F43  
2DB4CF66DA084DDD74B993391FC9A180E80C721EFBD08DFA053F523B9327BD681FCC93234E340BEE  
4AFDBFD22FE11C015C1A529E0.43D70C0A2973F87652326D5F39C9783383A7EA09C06E2776B8CC4C  
51BAAF5466244C3172C84C893343925695B97C622137CFAAF309CF6281AA275BEB03717738  
[root@localhost Desktop]#
```

既然是通过grub2修改的密码，那就修改他的配置文件/boot/grub2/grub.cfg

为了方便操作，新开一个终端窗口：

```
vim /boot/grub2/grub.cfg
```

可以看到，配置文件已经注释出界面顺序（太贴心了，嚶嚶嚶），我们把锁加到### BEGIN /etc/grub.d/10_linux ###下面，menuentry那一行的上面：

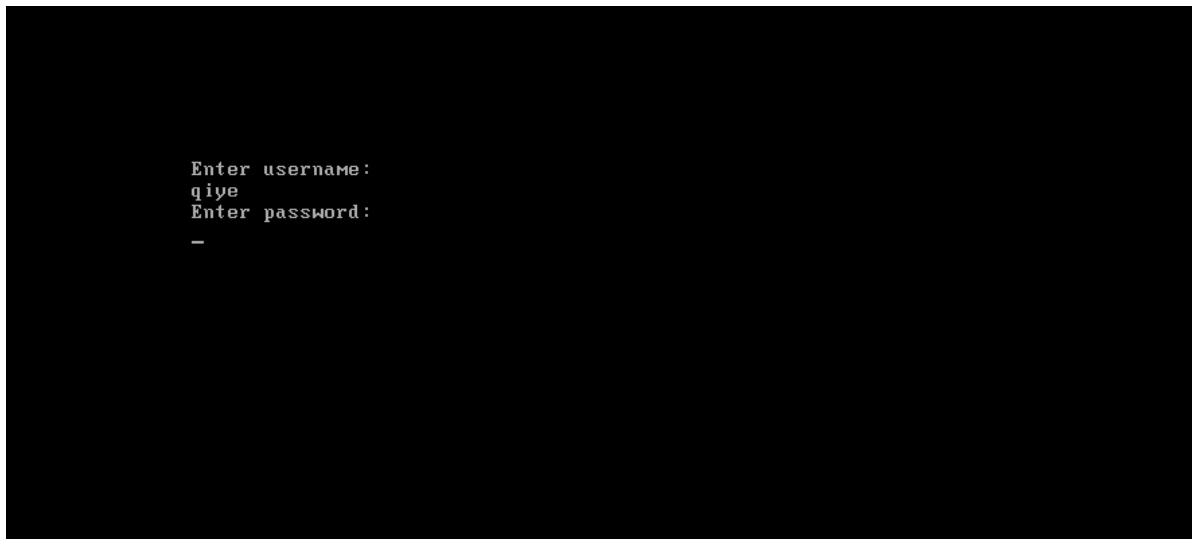
```

# unavailable.
else
    set timeout=5
fi
### END /etc/grub.d/00_header ###

### BEGIN /etc/grub.d/10_linux ###
set superusers="qiye"
password_pbkdf2 qiye grub.pbkdf2.sha512.10000.3D4FFC21A4D44D1B2431F432DB4CF66DA0
84DDD74B993391FC9A180E80C721EFBD08DFA053F523B9327BD681FCC93234E340BEE4AFDBFD22FE
11C015C1A529E0.43D70C0A2973F87652326D5F39C9783383A7EA09C06E2776B8CC4C51BAAF54662
44C3172C84C893343925695B97C622137CFAAF309CF6281AA275BEB03717738
menuentry 'CentOS Linux, with Linux 3.10.0-123.el7.x86_64' --class centos --clas
s gnu-linux --class gnu --class os --unrestricted $menuentry_id_option 'gnulinux
-3.10.0-123.el7.x86_64-advanced-ea4f0718-db92-4c4c-bb69-3ad522c637b1' {
    load_video
    set gtxpayload=keep
    insmod gzio
    insmod part_msdos
    insmod xfs
    set root='hd0,msdos1'
    if [ x$feature_platform_search_hint = xy ]; then
@
73.303 58%

```

保存退出，一样reboot重启，再次进入gurb2界面



- 输入用户: qiye
- 密码: qiye

发现可以打开GURB2界面，ya☆da☆ze!

3.修复MBR

主引导记录，也叫主引导扇区

Linux是文件型的操作系统，所有的信息和数据都以文件形式保存于系统中，但是并不是所有的数据，主

引导记录就不是以文件的形式保存，无法进行备份，只能通过 dd 命令备份

- **先进行备份，再破坏**

使用 dd 命令，将 sda 的 MBR 进行备份
 用 zero设备生成 446 字节的“0”写入 MBR
 重启后发现系统已坏

```
#备份
[root@localhost ~]# dd if=/dev/sda of=/root/mbr.bak count=1 bs=512
1+0 records in
1+0 records out
512 bytes (512 B) copied, 0.000676292 s, 757 kB/s

#破坏
[root@localhost ~]# dd if=/dev/zero of=/dev/sda count=1 bs=446
1+0 records in
1+0 records out
446 bytes (446 B) copied, 0.000305554 s, 1.5 MB/s
```

重启后，发现无法正常启动

```
Network boot from Intel E1000
Copyright (C) 2003-2018 VMware, Inc.
Copyright (C) 1997-2000 Intel Corporation
```

- 连接镜像光盘，在光盘引导界面选择 Troubleshooting

| 设备 | 摘要 |
|----------------|---------------------|
| 内存 | 1 GB |
| 处理器 | 1 |
| 硬盘 (SCSI) | 20 GB |
| CD/DVD (IDE) | 正在使用文件 D:\迅雷下载\C... |
| CD/DVD 2 (IDE) | 自动检测 |
| 网络适配器 | NAT |
| USB 控制器 | 存在 |
| 声卡 | 自动检测 |
| 打印机 | 存在 |
| 显示器 | 自动检测 |

设备状态

☒ 已连接(C)

☒ 启动时连接(O)

连接

☐ 使用物理驱动器(P):

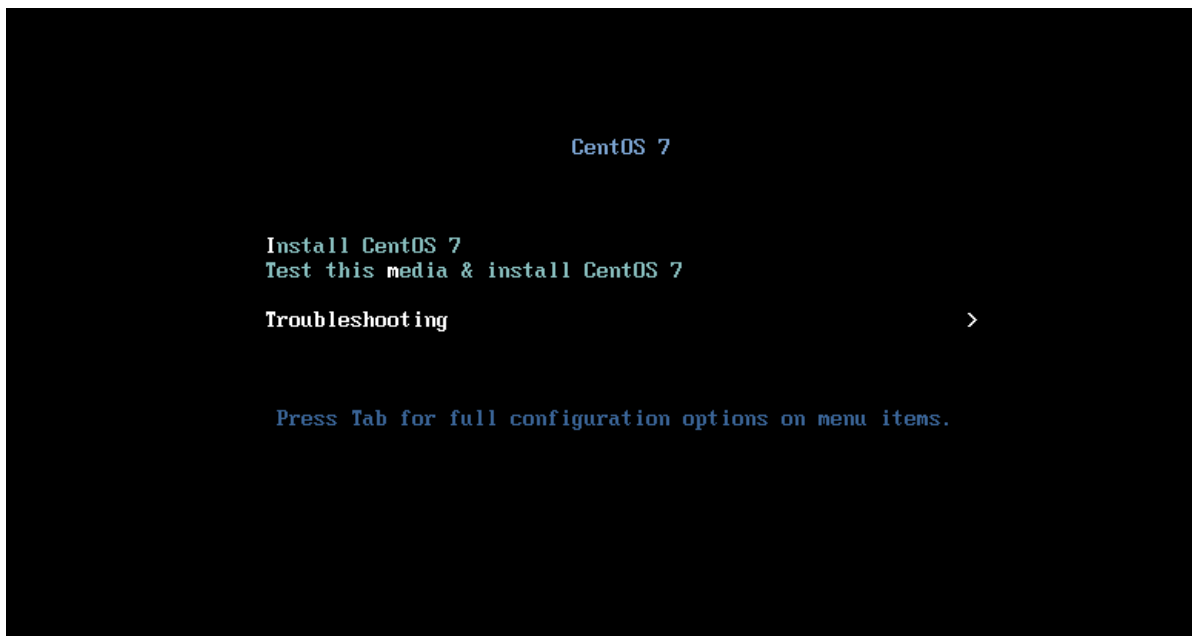
自动检测

☒ 使用 ISO 映像文件(M):

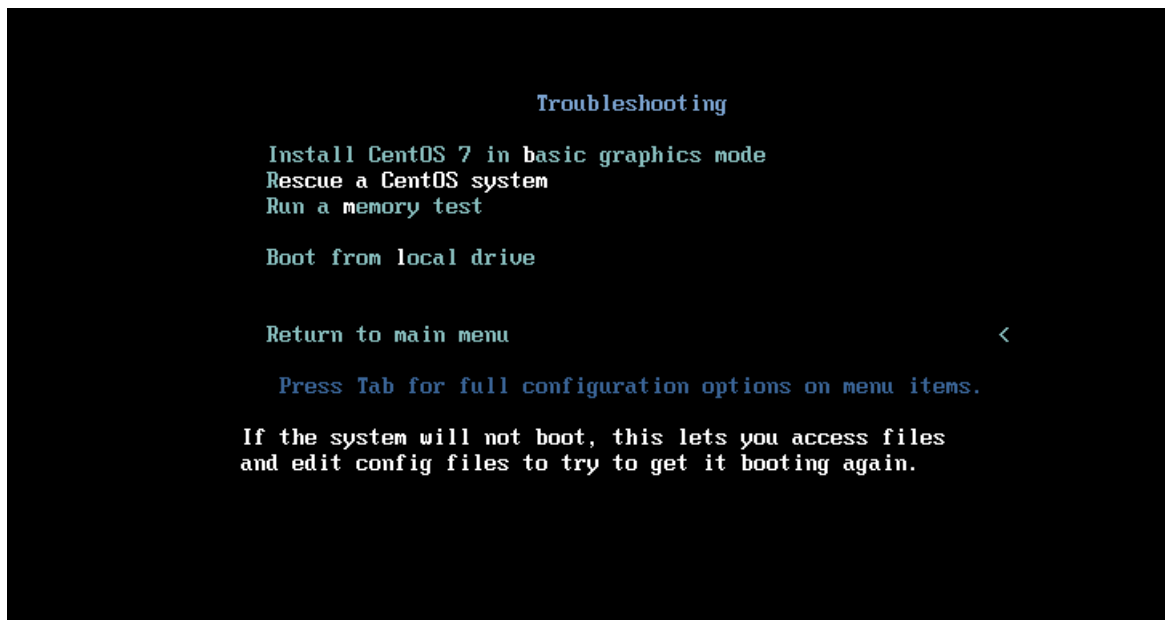
D:\迅雷下载\CentOS-7.0-1406

浏览(B)...

高级(V)...



- 选择救援模式 Rescue a Centos system



- 选择Continue, 以 rw 模式挂载分区



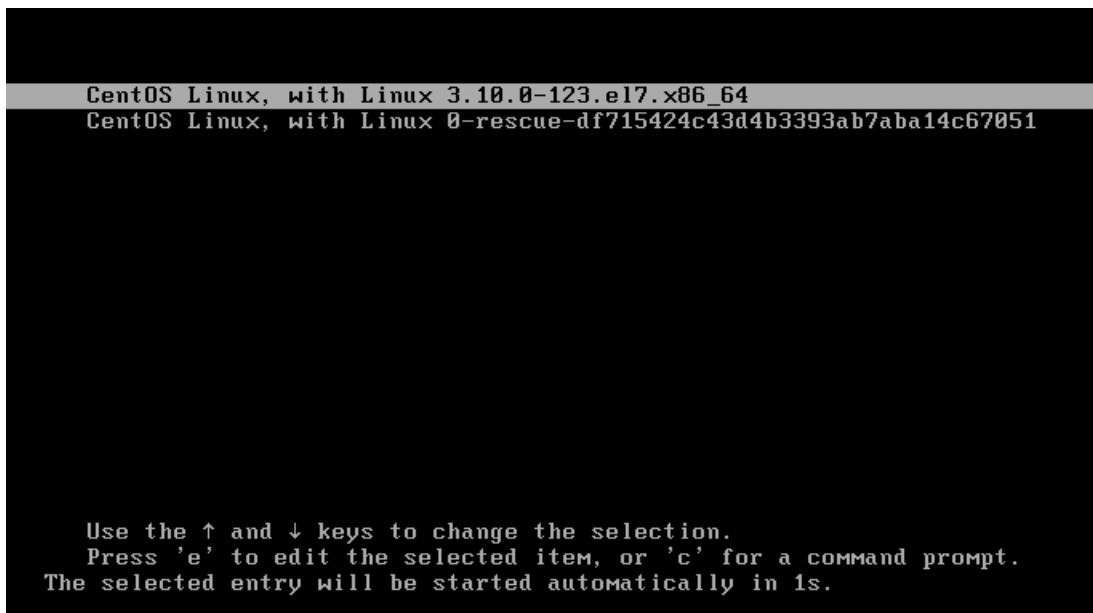
grub2-install 命令重建 Bootloader, 随后 sync 写入硬盘, reboot 重启系统

```
egfs on /mnt/sysimage/egfs type egfs (rw,relatime)
selinuxfs on /mnt/sysimage/sys/fs/selinux type selinuxfs (rw,relatime)
sh-4.2# chroot /mnt/sysimage
bash-4.2# grub2-install /dev/sda
Installing for i386-pc platform.
Installation finished. No error reported.
bash-4.2# sync
bash-4.2# exit
exit
sh-4.2# reboot
anaconda] 1:main* 2:shell 3:log 4:storage-log 5:program-log
```

进入挂载文档, 重新安装 Bootloader, sync写入硬盘, reboot重启system

```
sh-4.2# chroot /mnt/sysimage
sh-4.2# grub2-install /dev/sda
sh-4.2# sync
sh-4.2# exit
sh-4.2# reboot
```

完成! (我好菜, 都是跟着文档来着)



4.修复GRUB

我们设想，有没有一种可能，grub配置文件丢失，开机直接登录，显然这是不可能的，它会直接进入grub界面，直接让你调试解决

总之，乱来前能快照就快照（不能过度依靠），然后必须备份

```
#备份
[root@localhost ~]# mkdir grub2.bak
[root@localhost ~]# chmod 777 grub2.bak/
[root@localhost ~]# cp -rp /boot/grub2/* ./grub2.bak/
[root@localhost ~]# ls grub2.bak/
device.map  fonts  grub.cfg  grubenv  i386-pc  locale  themes
[root@localhost ~]#
#删除
[root@localhost ~]# rm /boot/grub2/grub.cfg
rm: remove regular file '/boot/grub2/grub.cfg'? y
[root@localhost ~]# reboot
```

最好在确认一下，磁盘分区：

```
df -h
```

```
[qiye@localhost 桌面]$ df -h
文件系统      容量  已用  可用  已用% 挂载点
/dev/sda3      18G   3.4G   15G   20% /
devtmpfs       482M    0   482M    0% /dev
tmpfs          490M   148K   490M    1% /dev/shm
tmpfs          490M    7.0M   483M    2% /run
tmpfs          490M    0   490M    0% /sys/fs/cgroup
/dev/sda1      297M  106M   192M   36% /boot
/dev/sr0       6.6G   6.6G    0  100% /run/media/qiye/CentOS 7 x86_64
[qiye@localhost 桌面]$
```

开始重启：

```
Minimal BASH-like line editing is supported. For the first word,
TAB lists possible command completions. Anywhere else TAB lists
possible device or file completions.
```

```
grub> _
```

重启后，进入grub状态，一下调试参数：

小心版本问题啊，建议linux16 /vm 直接Tab出来就行

initrd16 /init 也一样

```
grub> insmod xfs

grub> set root='hd0,msdos1'      #你的/boot分区/dev/sda1,没错hd0对于sda, msdos1对
应/dev/sda1

grub> linux16 /vmlinuz-3.10.0-123.el7.x86_64

root=/dev/sda3

grub> initrd16 /initramfs-3.10.0-123.el7.x86_64.img

grub> boot
```

关于root=/dev/sda3:

我的系统分区位于/dev/sda3,不能搞错绝对路径！！！！

恢复Grub

```
[root@localhost ~]# cp ./grub2.bak/grub.cfg /boot/grub2/

[root@localhost ~]# reboot
```

能够正常重启！

DHCP服务器的配置与使用

1.安装DHCP服务

检查是否有安装DHCP，若无提示，则未安装

```
rpm -qa dhcp
```

关闭防火墙及SELinux策略

```
[root@localhost ~]# systemctl stop firewalld.service
```

```
[root@localhost ~]# setenforce 0
```

安装dhcp服务

#挂载镜像

```
[root@localhost ~]# mkdir /mnt/cdrom
```

```
[root@localhost ~]# mount /dev/cdrom /mnt/cdrom/
```

mount: /dev/sr0 is write-protected, mounting read-only

```
[root@localhost ~]# cd /mnt/cdrom/
```

```
[root@localhost cdrom]# ls
```

```
CentOS_BuildTag  GPL          LiveOS       RPM-GPG-KEY-CentOS-7
EFI              images      Packages    RPM-GPG-KEY-CentOS-Testing-7
EULA             isolinux   repodata    TRANS.TBL
```

```
[root@localhost cdrom]# cd Packages/
```

#在包内查找dhcp安装包

```
[root@localhost Packages]# ls | grep dhcp
```

```
dhcp-4.2.5-27.el7.centos.x86_64.rpm
dhcp-common-4.2.5-27.el7.centos.x86_64.rpm
dhcp-devel-4.2.5-27.el7.centos.i686.rpm
dhcp-devel-4.2.5-27.el7.centos.x86_64.rpm
dhcp-libs-4.2.5-27.el7.centos.i686.rpm
dhcp-libs-4.2.5-27.el7.centos.x86_64.rpm
```

#安装dhcp

```
[root@localhost Packages]# rpm -ivh dhcp-4.2.5-27.el7.centos.x86_64.rpm
```

warning: dhcp-4.2.5-27.el7.centos.x86_64.rpm: Header V3 RSA/SHA256 Signature, key ID f4a80eb5: NOKEY

```
Preparing... ##### [100%]
```

```
Updating / installing...
```

```
1:dhcp-12:4.2.5-27.el7.centos ##### [100%]
```

```
[root@localhost Packages]# rpm -qa dhcp
```

```
dhcp-4.2.5-27.el7.centos.x86_64
```

#yum下载安装也行

```
wget -o /etc/yum.repos.d/CentOS-Base.repo
```

```
https://mirrors.aliyun.com/repo/Centos-7.repo
```

```
yum install dhcp
```

再次检查dhcp

```
[root@localhost Packages]# rpm -qa dhcp
```

```
dhcp-4.2.5-27.el7.centos.x86_64
```

2.DHCP的配置

更新本地网卡ip配置（我这网卡名就很离谱。）

```
[root@localhost Packages]# dhclient
```

```
[root@localhost Packages]# ifconfig
```

```
eno16777736: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.241.144 netmask 255.255.255.0 broadcast 192.168.241.255
    ether 00:0c:29:e0:c1:21 txqueuelen 1000 (Ethernet)
```

```
RX packets 631 bytes 40374 (39.4 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 18 bytes 3110 (3.0 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

```
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 0 (Local Loopback)
    RX packets 930 bytes 80828 (78.9 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 930 bytes 80828 (78.9 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

找到dhcp配置文件

```
[root@localhost Packages]# find /* -name dhcpd.conf
/etc/dhcp/dhcpd.conf
```

然后出了一堆问题，解决起来真的是。。。怀疑人生啊

1.配置静态ip

```
vim /etc/sysconfig/network-scripts/ifcfg-eno16777736
```

```
HWADDR=00:0C:29:E0:C1:21
TYPE=Ethernet
BOOTPROTO=static
DEFROUTE=yes
PEERDNS=yes
PEERROUTES=yes
IPV4_FAILURE_FATAL=no
IPV6_INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_PEERDNS=yes
IPV6_PEERROUTES=yes
IPV6_FAILURE_FATAL=no
NAME=eno16777736
UUID=118af5e5-92de-42b0-a1c6-619c8d9d6c81
DEVICE=eno16777736
ONBOOT=yes
IPADDR=192.168.111.111
NETMASK=255.255.255.0
GATEWAY=192.168.111.2
DNS1=114.114.114.144
DNS2=8.8.8.8
~
"/etc/sysconfig/network-scripts/ifcfg-eno16777736" 22L, 416C
```

#检查ip是否正确

```
[root@localhost ~]# ifconfig
eno16777736: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.111.111 netmask 255.255.255.0 broadcast 192.168.111.255
    inet6 fe80::20c:29ff:fee0:c121 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:e0:c1:21 txqueuelen 1000 (Ethernet)
    RX packets 34 bytes 2994 (2.9 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 34 bytes 4361 (4.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

2.配置dhcp文件

在/etc/dhcp/dhcpd.conf增加以下:

```
vim /etc/dhcp/dhcpd.conf
```

```
subnet 192.168.111.0 netmask 255.255.255.0 {  
    range 192.168.111.100 192.168.111.200;  
    option domain-name-servers 192.168.111.1;  
    option domain-name "qiye";  
    option routers 192.168.111.1;  
    option broadcast-address 192.168.111.255;  
    default-lease-time 600;  
    max-lease-time 7200;  
}
```

subnet 后面接的是你ip的网段，不是你的ip，且后面数值都应该是跟你同个网段的ip

```
#启动dhcp服务
```

```
systemctl status dhcpd
```

```
# 重启DHCP服务
```

```
[root@localhost ~]# systemctl restart dhcpd.service
```

```
# 查看DHCP状态
```

```
[root@localhost ~]# netstat -luntp | grep dhcp
```

```
udp          0      0 0.0.0.0:67          0.0.0.0:*  
12514/dhcpd
```

修改虚拟网络配置

| 名称 | 类型 | 外部连接 | 主机连接 | DHCP | 子网地址 |
|--------|--------|--------|------|------|---------------|
| VMnet0 | 自定义... | - | - | - | 192.168.106.0 |
| VMnet1 | 仅主机... | - | 已连接 | 已启用 | 192.168.141.0 |
| VMnet8 | NAT 模式 | NAT 模式 | 已连接 | - | 192.168.111.0 |

添加网络(E)...
移除网络(O)
重命名网络(W)...

VMnet 信息

☐ 桥接模式(将虚拟机直接连接到外部网络)(B)
已桥接至(G): 自动设置(U)...

☒ NAT 模式(与虚拟机共享主机的 IP 地址)(N) NAT 设置(S)...

☐ 仅主机模式(在专用网络内连接虚拟机)(H)

☒ 将主机虚拟适配器连接到此网络(V)
主机虚拟适配器名称: **VMware 网络适配器 VMnet8**

☐ 使用本地 DHCP 服务将 IP 地址分配给虚拟机(D) DHCP 设置(P)...

子网 IP (I): 192.168.111.0
子网掩码(M): 255.255.255.0

⚠ 需要具备管理员特权才能修改网络配置。
更改设置(C)

在一台被我渗透了无数遍的靶机win7上，终于。。。。。

```
以太网适配器 Bluetooth 网络连接:

    媒体状态 . . . . . : 媒体已断开
    连接特定的 DNS 后缀 . . . . . :

以太网适配器 本地连接:

    连接特定的 DNS 后缀 . . . . . : qiye
    本地链接 IPv6 地址 . . . . . : fe80::e4d7:c67e:c7ff:268az11
    IPv4 地址 . . . . . : 192.168.111.100
    子网掩码 . . . . . : 255.255.255.0
    默认网关 . . . . . : 192.168.111.1

隧道适配器 isatap.{C4E1DEAB-944C-421F-9166-98868058E78A}:

    媒体状态 . . . . . : 媒体已断开
    连接特定的 DNS 后缀 . . . . . :

隧道适配器 isatap.qiye:

    媒体状态 . . . . . : 媒体已断开
    连接特定的 DNS 后缀 . . . . . : qiye

C:\Users\qiye>
```

给win7配置一个nice的IP地址 (192.168.111.114)

```
vim /etc/dhcp/dhcpd.conf
```

```
subnet 192.168.111.0 netmask 255.255.255.0 {
    range 192.168.111.100 192.168.111.200;
    option domain-name-servers 192.168.111.1;
```

```

option domain-name "qiye";
option routers 192.168.111.1;
option broadcast-address 192.168.111.255;
default-lease-time 600;
max-lease-time 7200;
}

# 增加一行
host boss {
    hardware ethernet 00:0C:29:5A:D5:EB;
    fixed-address 192.168.111.144;
}

```

重启服务

```
[root@localhost ~]# systemctl restart dhcpd.service
```

```

以太网适配器 Bluetooth 网络连接:

    媒体状态 . . . . . : 媒体已断开
    连接特定的 DNS 后缀 . . . . . :

以太网适配器 本地连接:

    连接特定的 DNS 后缀 . . . . . : qiye
    本地链接 IPv6 地址 . . . . . : fe80::e4d7:c67e:c7ff:268a%11
    IPv4 地址 . . . . . : 192.168.111.144
    子网掩码 . . . . . : 255.255.255.0
    默认网关 . . . . . : 192.168.111.1

隧道适配器 isatap.{C4E1DEAB-944C-421F-9166-98868058E78A}:

    媒体状态 . . . . . : 媒体已断开
    连接特定的 DNS 后缀 . . . . . :

隧道适配器 isatap.qiye:

    媒体状态 . . . . . : 媒体已断开
    连接特定的 DNS 后缀 . . . . . :

```

Linux发送，给我的ubuntu配置ip和主机名

```

host qiye {
    hardware ethernet 00:0c:29:2d:61:0b;
    fixed-address 192.168.111.141;
    option host-name "qiye_handsome_boy";
}

```

```

subnet 192.168.111.0 netmask 255.255.255.0 {
    range 192.168.111.100 192.168.111.200;
    option domain-name-servers 192.168.111.1;
    option domain-name "qiye";
    option routers 192.168.111.1;
    option broadcast-address 192.168.111.255;
    default-lease-time 600;
    max-lease-time 7200;
}

host win7 {
    hardware ethernet 00:0C:29:5A:D5:EB;
    fixed-address 192.168.111.144;
}

host qiye {
    hardware ethernet 00:0c:29:2d:61:0b;
    fixed-address 192.168.111.141;
    option host-name "qiye_handsome_boy";
}

```

```

[root@localhost ~]# dhclient -d eno16777736
Internet Systems Consortium DHCP Client 4.2.5
Copyright 2004-2013 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

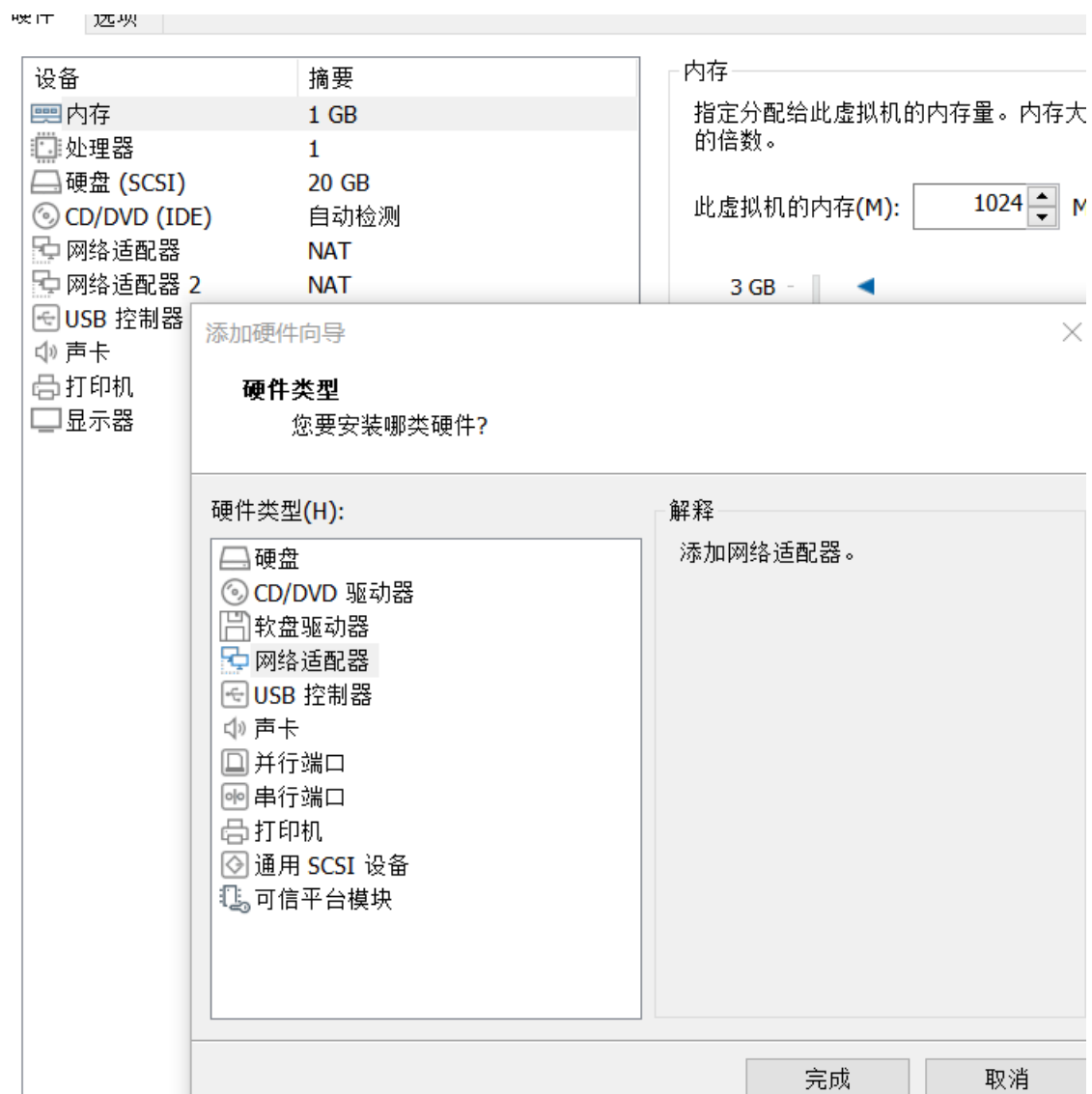
Listening on LPF/eno16777736/00:0c:29:e0:c1:21
Sending on   LPF/eno16777736/00:0c:29:e0:c1:21
Sending on   Socket/fallback
DHCPDISCOVER on eno16777736 to 255.255.255.255 port 67 interval 4
(xid=0xa56da87)
DHCPREQUEST on eno16777736 to 255.255.255.255 port 67 (xid=0xa56da87)
DHCPOFFER from 192.168.111.111
DHCPACK from 192.168.111.111 (xid=0xa56da87)
hostname: the specified hostname is invalid
See -nc option in dhclient(8) man page.
bound to 192.168.111.141 -- renewal in 245 seconds.

```

ip能成功，主机名硬是改不出来。。

3.超级作用域

新增网卡



新建一个网卡静态配置文件（建议拷过来）

修改网卡mac地址、注释UUID，把新网卡的配置内容更新过来

```
HWADDR=00:0c:29:e0:c1:2b
TYPE=Ethernet
BOOTPROTO=static
DEFROUTE=yes
PEERDNS=yes
PEERROUTES=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_PEERDNS=yes
IPV6_PEERROUTES=yes
IPV6_FAILURE_FATAL=no
NAME=eno33554984
UUID=118af5e5-92de-42b0-a1c6-619c8d9d6c81
DEVICE=eno33554984
ONBOOT=yes
IPADDR=192.168.112.111
NETMASK=255.255.255.0
GATEWAY=192.168.111.2
DNS1=114.114.114.144
DNS2=8.8.8.8
```

```
"ifcfg-eno33554984" 23L, 418C
```

重启网络服务

```
[root@localhost dhcp]# systemctl restart network.service
```

```
[root@localhost ~]# systemctl restart network.service
[root@localhost ~]# ifconfig
eno16777736: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.111.111 netmask 255.255.255.0 broadcast 192.168.111.255
    inet6 fe80::20c:29ff:fee0:c121 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:e0:c1:21 txqueuelen 1000 (Ethernet)
    RX packets 247 bytes 45094 (44.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 185 bytes 20921 (20.4 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eno33554984: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.112.111 netmask 255.255.255.0 broadcast 192.168.112.255
    inet6 fe80::20c:29ff:fee0:c12b prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:e0:c1:2b txqueuelen 1000 (Ethernet)
    RX packets 85 bytes 23056 (22.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 54 bytes 9468 (9.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

修改dhcp配置 (最好不要重复的mac地址, 不然配置生效的是后一个)

```
vim /etc/dhcp/dhcpd.conf
```

新增

```

subnet 192.168.112.0 netmask 255.255.255.0 {
    range 192.168.112.100 192.168.112.200;
    option domain-name-servers 192.168.112.1;
    option domain-name "qiye";
    option routers 192.168.112.1;
    option broadcast-address 192.168.112.255;
    default-lease-time 600;
    max-lease-time 7200;
}

host ubuntu {
    hardware ethernet 00:0c:29:2d:61:0b;
    fixed-address 192.168.112.144;
}

```

可以发现，ubuntu已经跟换到112段

```

root@ubuntu:/home/qiye/Desktop# ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.112.144 netmask 255.255.255.0 broadcast 192.168.112.255
    inet6 fe80::7e36:1937:20a6:7902 prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:2d:61:0b txqueuelen 1000 (Ethernet)
    RX packets 225 bytes 34704 (34.7 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1169 bytes 125832 (125.8 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 9309 bytes 670887 (670.8 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 9309 bytes 670887 (670.8 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

未完待续~~