浙江财经大学
Zhejiang University of Finance & Economic

09 网络管理

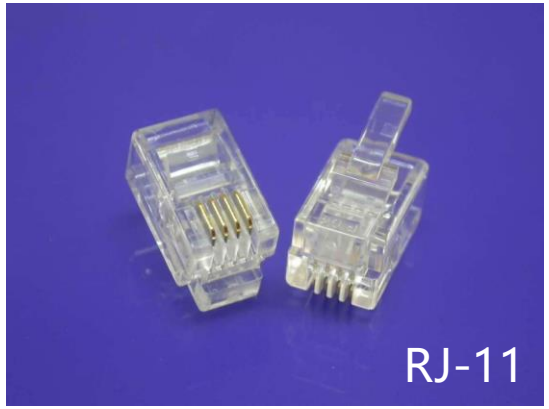
TCP/IP协议

TCP/IP协议是Internet网络的标准协议，采用TCP/IP协议的主机连接到Internet上，就能实现与同在网络上的其他主机进行数据交换。通常把计算机中连接到网络上的设备称为网络接口设备。计算机连接到网络上，需要配置其网络接口信息，包括计算机的IP地址、子网掩码、默认网关，域名解析服务器地址等。本章将介绍如何给计算机配置这些接口信息，以便用户在不同的环境下选择使用。

网络接口

网络接口指的网络设备的各种接口（它主要用于数据的传输），我们现今正在使用的网络接口都为以太网接口。常见的以太网接口类型有RJ-45接口，RJ-11接口，SC光纤接口等。

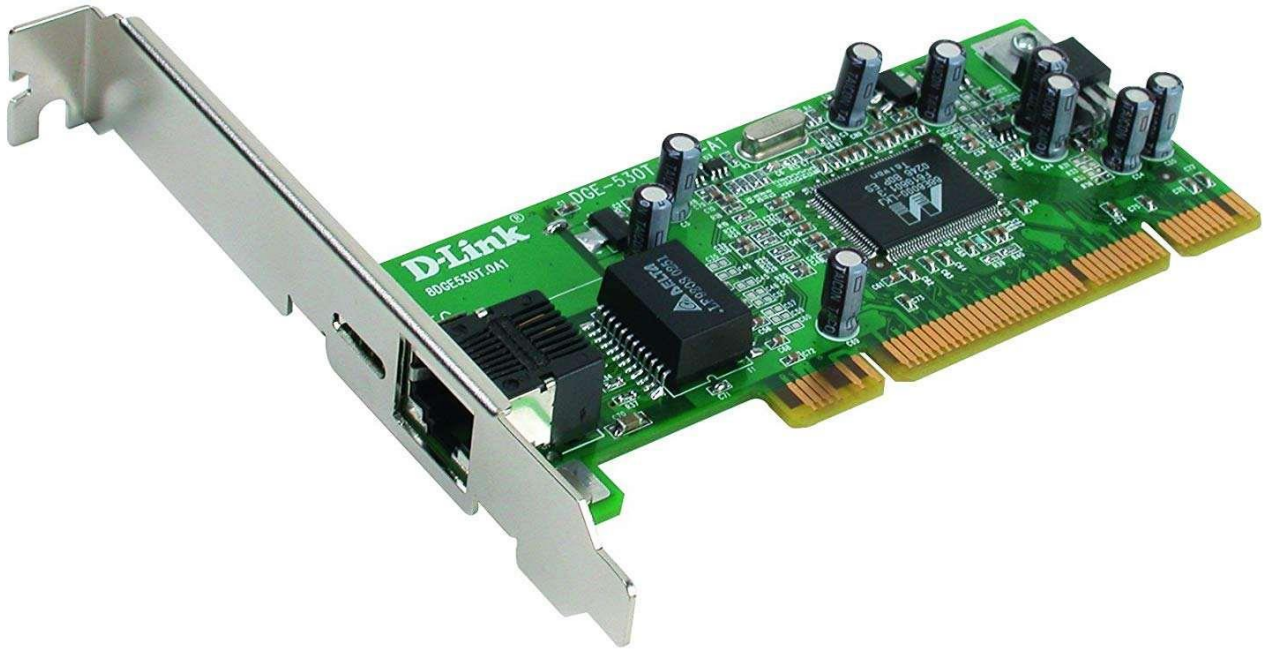
RJ-45


RJ-11


SC光纤

网卡

硬件通过网卡连接上Internet。目前主流的网卡均为以以太网协议所开发出来的以太网卡（Ethernet）。



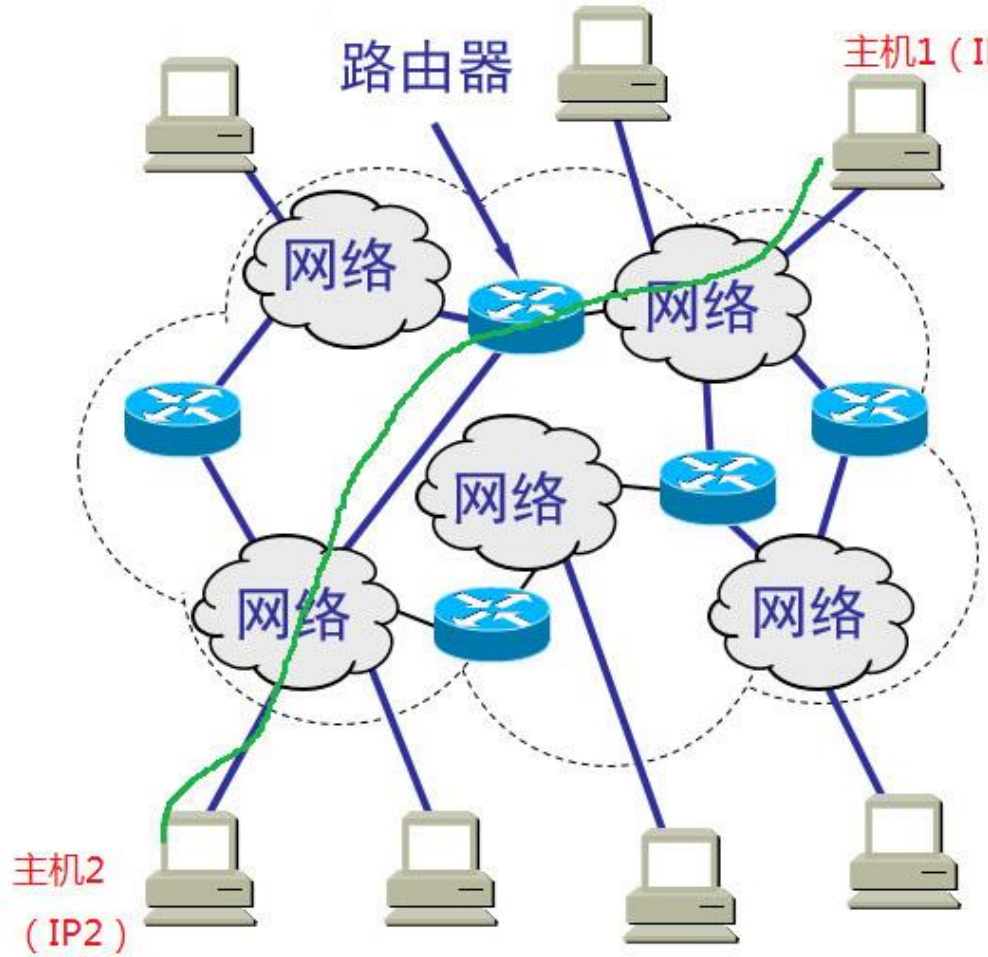
TCP/IP协议

TCP/IP协议主要分为两个部分：传输控制协议（TCP）和网际互联协议（IP）。

1.网际互联协议（IP）

IP协议只负责数据的路由和传输，在源节点与目的节点之间传送数据分组，但并不处理数据内容。数据分组中有目的地址等必要内容，使每个数据分组经过不同的路径也能准确地到达目的地，在目的地重新组合还原成原来发送的数据。

为了能在不同硬件类型和数据分组网络中实现数据的转发，IP需要一种独立于硬件的寻址方式。这种寻址方式是基于IP地址的，在Internet上的每台主机都被设置了一个32位的IP地址。为了方便记忆，IP地址通常被写成点分十进制的结构，即将32位的二进制数利用句点（.）分成4个部分，然后每个部分转换成一个十进制数，例如：192.168.0.45。



网络上的主机都要有IP地址，根据这个地址，找到源节点和目的节点，实现两台PC之间的通信。

传输控制协议（TCP）

传输控制协议（TCP）

虽然IP协议保证了计算机之间可以发送和接收数据报，但它不负责解决数据报传达的可靠性等安全问题，这些安全因素主要由TCP协议负责完成。TCP在两个端点之间建立的连接是可靠的连接，它能够在网络出现错误的时候，通知对应的主机重发该分组。

IP地址分类

IP地址由两部分组成：网络号net_id与主机号host_id，所以IP地址不仅仅表示一个主机的编号，而是指出了连接在某个网络上的某台主机。根据网络号的不同可以将Internet网络的IP地址分为五类，即A类到E类，其中D类作为多路广播地址保留，E类保留今后使用。

- A类网络地址：IP地址的第1个字节表示网络号net_id，其中第一位为0，后面的3个字节表示主机号host_id。A类网络共能容纳的主机数为 $2^{24}-2 = 16777214$ 台。
- B类网络地址：IP地址的前面2个字节表示网络号net_id，其中第1、2位为10，后面的2个字节表示主机号host_id。B类网络共能容纳的主机数为 $2^{16} - 2 = 65534$ 台。
- C类网络地址：IP地址的前面3个字节表示网络号net_id，其中第1、2和3位为110，最后1个字节表示主机号host_id。C类网络共能容纳的主机数为 $2^{8}-2 = 254$ 台。

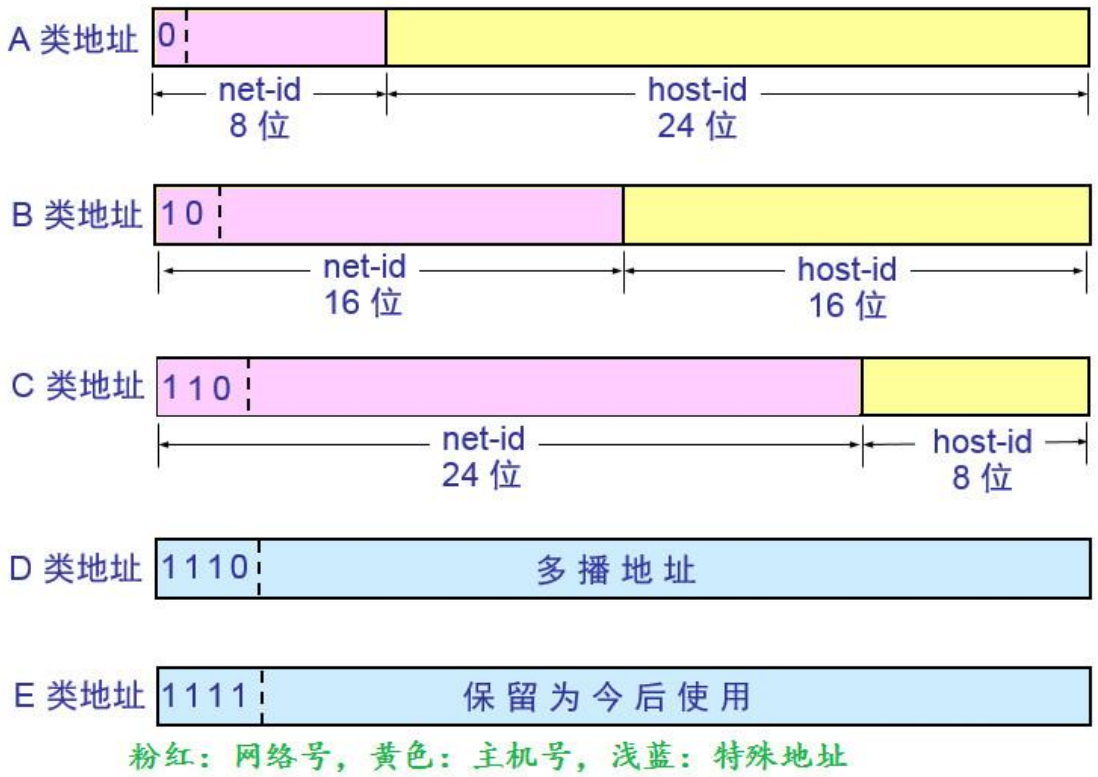
注意减去2是因为主机号全为1时表示该网络广播地址，全为0时表示该网络的网络号。

IP地址结构

每一类地址都由两个固定长度的字段组成，

（1）网络号 net-id：它标志主机（或路由器）所连接到的网络。

（2）主机号 host-id：它标志该主机（或路由器）。



IP地址

同一网络内的所有主机分配相同的网络号，同一网络内的不同主机必须分配不同的主机号，以区分主机

不同网络内的每台主机必须具有不同的网络号，但是可以具有相同的主机号。

按照IP地址的结构和其分配原则，可以在Internet上很方便的寻址：先按IP地址中的网络号找到相应的网络，再在这个网络上利用主机号找到相应的主机。

IP不仅是计算机的代号，还表明了某个网络上的某个计算机。

各类IP地址的范围

类型	范围
A	0.0.0.0~127.255.255.255
B	128.0.0.0~191.255.255.255
C	192.0.0.0~223.255.255.255
D	224.0.0.0~239.255.255.255
E	240.0.0.0~247.255.255.255

网络号和主机号

不同类型IP地址中的网络号net_id和主机号host_id。

IP地址	网络类型	网络号net_id	主机号host_id
60.45.12.40	A类	60	45.12.40
130.50.10.15	B类	130.50	10.15
212.78.42.212	C类	212.78.42	212

子网掩码（NETMASK）

子网掩码是在IPv4地址资源紧缺的背景下为了解决IP地址分配而产生的虚拟IP技术，通过子网掩码将A、B、C三类地址划分为若干子网，从而显著提高了IP地址的分配效率，有效解决了IP地址资源紧张的局面。另一方面，在企业内网中为了更好地管理网络，网管人员也利用子网掩码的作用，人为地将一个较大的企业内部网络划分为更多个小规模的子网，再利用三层交换机的路由功能实现子网互联，从而有效解决了网络广播风暴和网络病毒等诸多网络管理方面的问题。

子网掩码（NETMASK）

子网掩码是一个32位地址，是与IP地址结合使用的一种技术。它的主要作用：

一是用于屏蔽IP地址的一部分以区别网络标识和主机标识，并说明该IP地址是在局域网上，还是在远程网上。

二是用于将一个大的IP网络划分为若干小的子网络。

子网掩码（NETMASK）

默认子网掩码用于不分子网的TCP/IP网络。

类	子网掩码	子网掩码的二进制表示
A	255.0.0.0	11111111.00000000.00000000.00000000
B	255.255.0.0	11111111.11111111.00000000.00000000
C	255.255.255.0	11111111.11111111.11111111.00000000

子网掩码（NETMASK）

有一台主机的IP地址为192.168.101.5，子网掩码为255.255.255.0；有另一台主机的IP地址为192.168.101.250，子网掩码也为255.255.255.0，问这两台主机是否在同一个网段内，如果是请问为什么？它们的主机ID是多少？

192.168.101.5的二进制表示为 11000000 10101000 01100101 00000101；子网掩码为255.255.255.0，其二进制值为11111111 11111111 11111111 00000000，则当192.168.101.5和255.255.255.0进行逻辑与运算

```
11000000 10101000 01100101 00000101

11111111 11111111 11111111 00000000

11000000 10101000 01100101 00000000
```

所得结果为11000000 10101000 01100101 00000000，其中非0的三个字节，即192.168.101为该网络号，剩余的字节为主机号。若该网络的另一台的IP地址为192.168.101.250，子网掩码也为255.255.255.0，则同样会得到网络号为192.168.101，因此这两台主机在同一网段内。

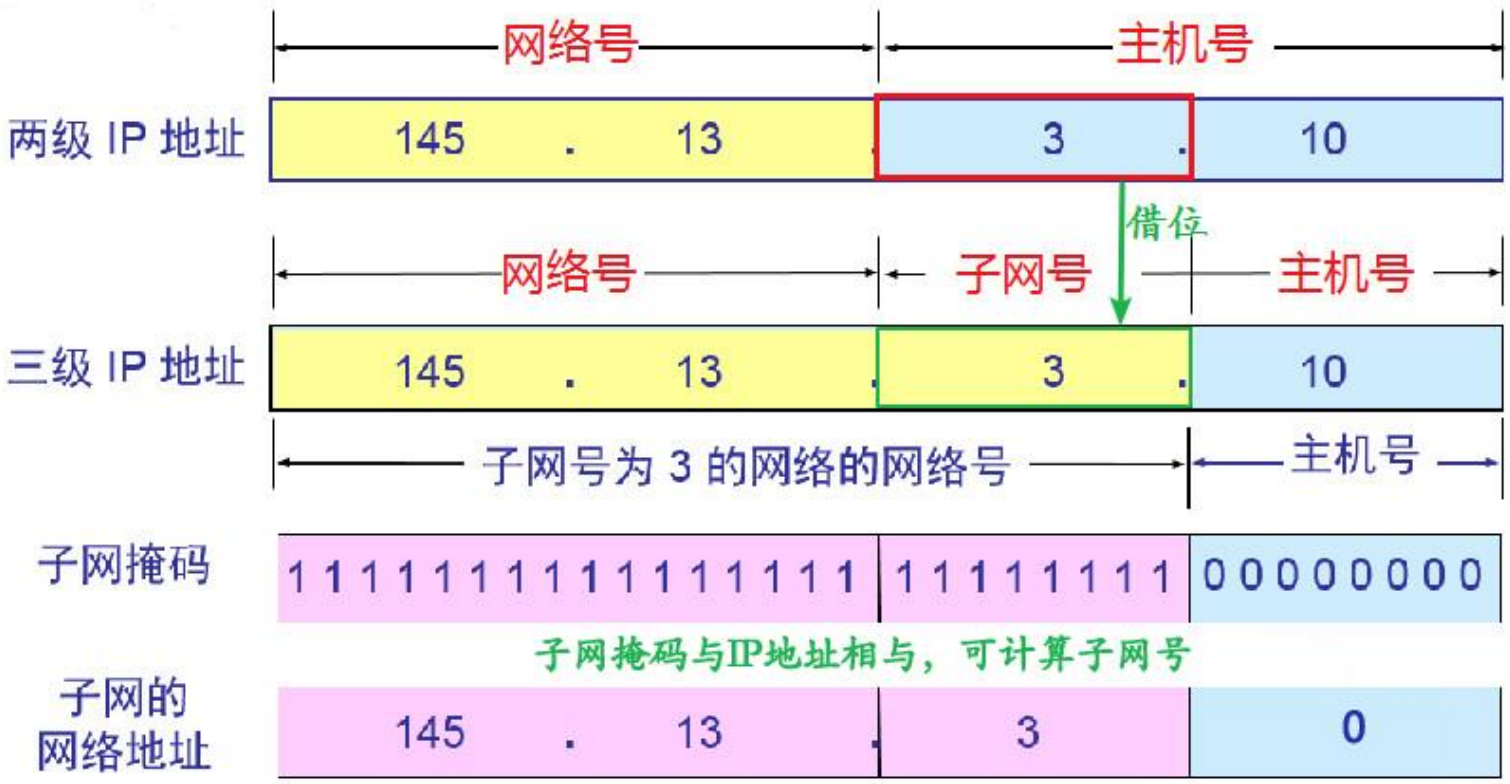
子网掩码

子网掩码机制提供了子网划分的方法。其作用是：减少网络上的通信量；节省IP地址；便于管理；解决物理网络本身的某些问题。使用子网掩码划分子网后，子网内可以通信，跨子网不能通信，子网间通信应该使用路由器，并正确配置静态路由信息。

划分子网就是用连续的1在IP地址中增加表示网络地址，同时减少表示主机地址的位数。
例如，IP地址为145.13.3.10，网络号为145.13.0.0、子网号为145.13.3.0、子网掩码为255.255.255.0，网络地址部分和子网标识部分为“1”所对应，主机标识部分为“0”所对应。

自定义子网掩码，不能通过子网掩码判断IP类型

子网掩码


网络号
主机号
两级 IP 地址
145 . 13 . 3 . 10
借位
网络号
子网号
主机号
三级 IP 地址
145 . 13 . 3 . 10
子网号为 3 的网络的网络号
主机号
子网掩码
11111111 11111111 11111111 00000000
子网掩码与IP地址相与，可计算子网号
子网的
网络地址
145 . 13 . 3 . 0

域名

在Internet上使用主机的IP地址来定位和标识主机，尽管为了方便记忆这些IP地址，采用了4段点分十进制的数字来表示，但是要记住这些枯燥的数字，还是不容易的。为了解决这个问题，提出了网络域名的概念。Internet域名是Internet网络上的一个服务器或一个网络系统的名字，在全世界，域名都是唯一的。通俗的说，域名就相当于每台服务器或主机的别名。

域名是一个层次结构的名称，由若干个引文字母和数字组成，由“.”分隔成几部分，一般的域名格式为：

主机名称.三级域名.二级域名.顶级域名

域名

例如，域名ds.zufe.edu.cn表示浙江财经大学数据科学学院的域名。ds反映的是一台服务器，zufe是浙江财经大学的域名，edu是教育系统域名，cn是顶级域名，代表中国。

顶级域名一般分为两类：组织性顶级域名和地理性顶级域名。组织性顶级域名用于指明网站的属性，而地理性顶级域名用于指明网站的地址属于哪个国家或地区。

组织性顶级域名

域名缩写	机构类型	域名缩写	机构类型
com	商业系统	firm	商业或公司
edu	教育系统	store	提供购买商业的业务部门
gov	政府机关	web	主要活动与www有关的实体
mil	军队系统	arts	以文化为主的实体
net	网管部门	rec	以消遣性娱乐活动为主的实体
org	非盈利性组织	inf	提供信息服务的实体

地理性顶级域名

域名缩写	国家或地区	域名缩写	国家或地区
cn	中国	ca	加拿大
au	澳大利亚	es	西班牙
de	德国	hk	中国香港
fr	法国	tw	中国台湾
jp	日本	sg	新加坡
uk	英国	us	美国

DNS（域名服务器）

当以域名方式访问某台远程主机时，域名系统首先将域名翻译成对应的IP地址（执行域名与IP地址相互转换的网络服务器，被称为DNS），然后使用得到的IP地址作为网络通信地址。因此在网上访问主机时，可以使用域名作为登录地址，也可以使用其IP地址作为登录地址，二者的效果一致。

需要注意的是，域名与IP地址并不是一一对应的，既有多个域名对应一个IP地址的，也有多个IP地址对应一个域名的情况存在。

路由器

由于从物理拓扑来说Internet是一个典型的网状网络，也就是说从一个网络节点（通常是网络主机）到达另一个节点的路径不止一条，那么网络上传输的数据分组是如何选择到达目的主机的路径呢？通常这是靠网络中的特殊主机来完成的，这些特殊主机被称为路由器。路由器负责将到来的数据分组根据其中的路由算法选择一条最有效的路径投递出去。路由器中可选择的一个网络节点到达另一节点的路径，就称为路由。通常，路由器中都设置一个路由表用于缓存系统的路由信息。

由于一个公司或单位的内部网络只通过一个路由器与外部网络建立连接，这个连接外部网络的路由器通常被称为默认网关。当公司内部网络上的主机与外部网络进行连接时，就将数据分组发给默认网关，由该网关负责数据分组的路由选择。

配置网络接口

在Linux系统中，可以使用3种不同的方法来配置网络接口：使用命令工具配置网络参数、直接修改网络配置文件和使用图形工具配置网络参数。

在终端命令模式下，可以首先使用ifconfig工具配置网络接口中的IP地址、网络掩码、广播地址等信息，然后再使用route工具配置网络的默认网关信息。

查看网络接口信息

安装ifconfig

sudo apt install net-tools

ifconfig命令格式如下：

ifconfig [网络接口设备名]

其中网络接口设备名为可选参数，如果没有指定网络接口，ifconfig将返回系统所有的网络设备的TCP/IP参数，包括回环网络接口的信息，否则返回指定的接口参数。

ifconfig命令

```
lei@lei-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::8109:a98a:4d9b:b27  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:29:13:b4  txqueuelen 1000  (Ethernet)
        RX packets 96623  bytes 133930674 (133.9 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 27178  bytes 1845212 (1.8 MB)
        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 309  bytes 28659 (28.6 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 309  bytes 28659 (28.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

enp0s3的IP地址为10.0.2.15，子网掩码为255.255.255.0，广播地址为10.0.2.255。

enp0s3：en表示以太网，p表示网卡位置，s表示网卡所处的槽位。

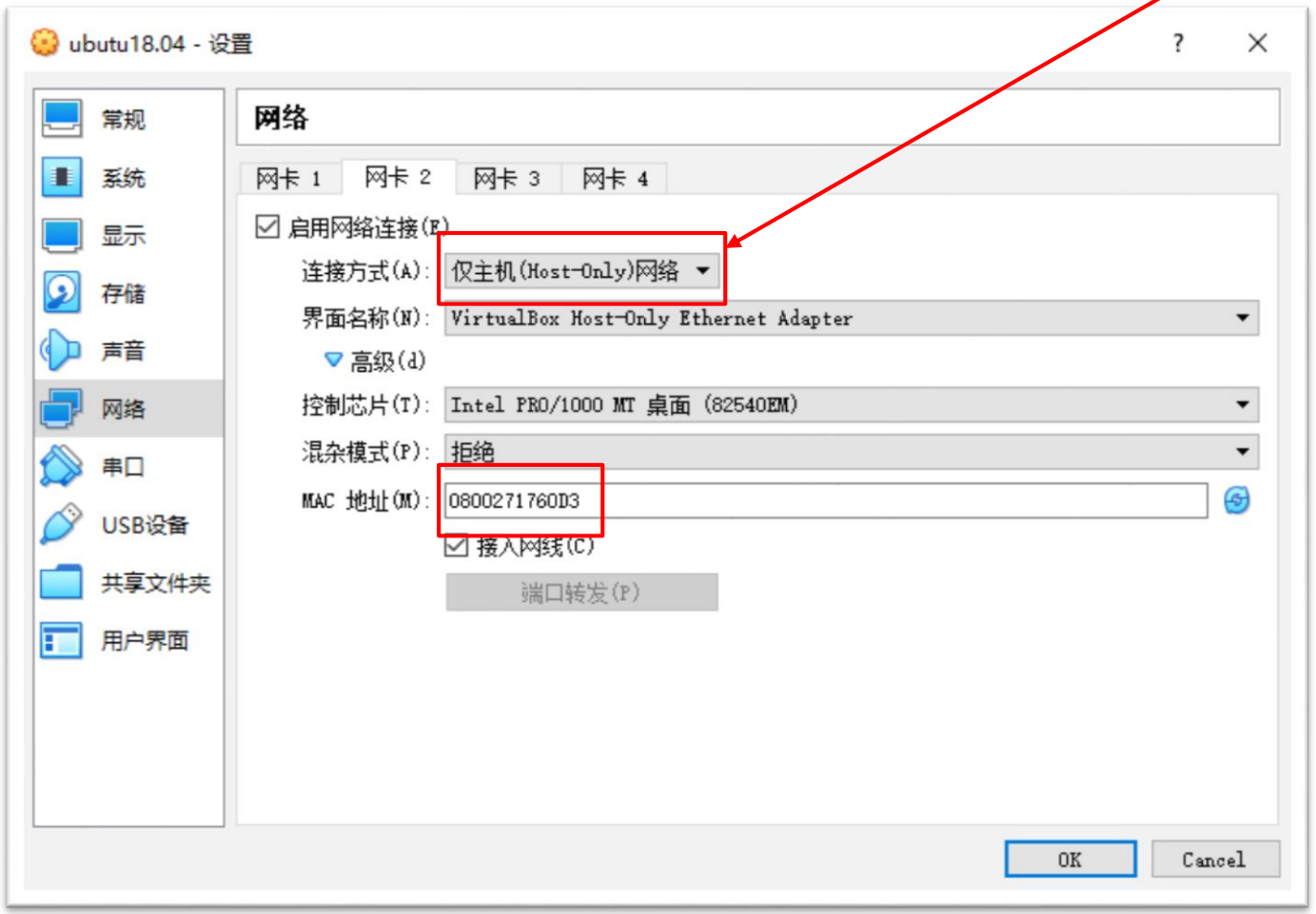
ifconfig命令

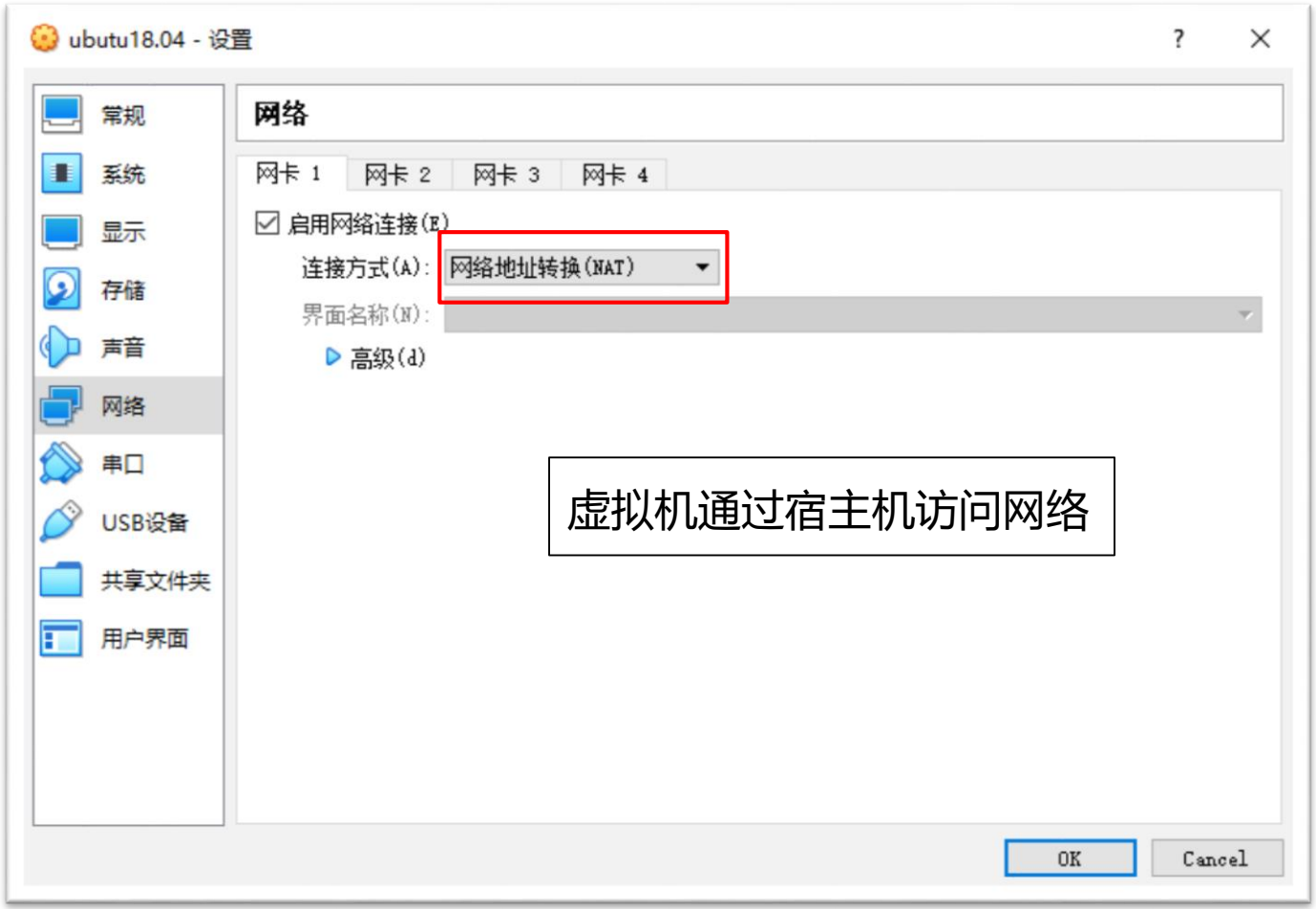
在终端命令提示符中输入如下命令，可以查看网络接口enp0s3的TCP/IP参数信息.

```
lei@lei-VirtualBox:~$ ifconfig enp0s3
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::8109:a98a:4d9b:b27  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:29:13:b4  txqueuelen 1000  (Ethernet)
        RX packets 96647  bytes 133933775 (133.9 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 27202  bytes 1846776 (1.8 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

添加网络接口

Host-only相当于虚拟机和宿主机通过交叉线相连





虚拟机通过宿主机访问网络

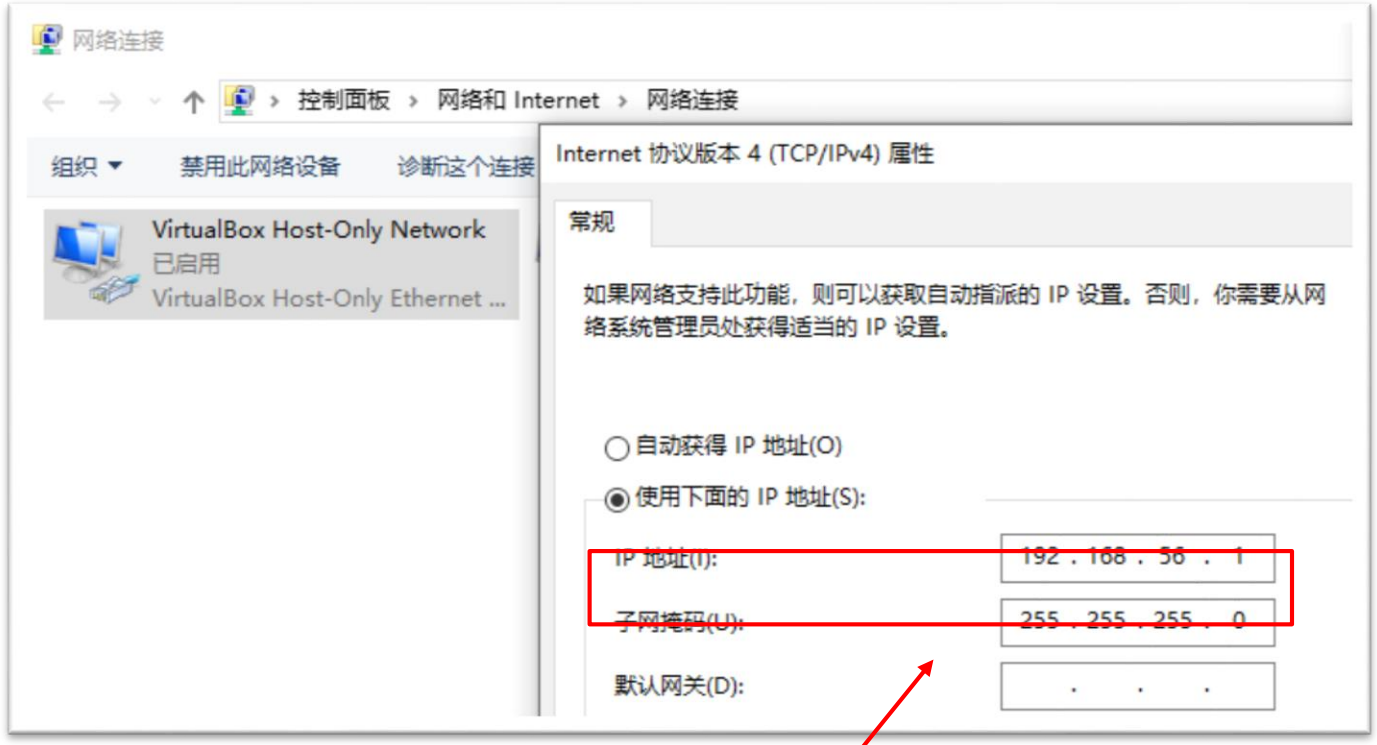
使用ifconfig查看

```
lei@lei-VirtualBox:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::68b4:c1e7:761b:7ee5  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:d3:1b:8f  txqueuelen 1000  (Ethernet)
        RX packets 3991  bytes 4238382 (4.2 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1418  bytes 131623 (131.6 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

enp0s8: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.101  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::341:8cc6:5195:f47b  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:17:60:d3  txqueuelen 1000  (Ethernet)
        RX packets 133  bytes 19469 (19.4 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 139  bytes 56266 (56.2 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 151  bytes 12963 (12.9 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 151  bytes 12963 (12.9 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

宿主机IP



与虚拟机在同一个子网

配置网络信息

ifconfig既可以用于查看网络接口的信息，也可以用于配置网络的TCP/IP参数，还可以用于启动和停用指定的网络接口。

ifconfig配置系统中指定的网络接口的TCP/IP参数信息，其格式如下：

ifconfig 网络接口名 IP地址 [netmask 子网掩码] [broadcast 广播地址]

其中netmask部分和broadcast部分可以任选其一，因为从子网掩码和广播地址可以互相推算。上述命令可以用指定的IP地址和子网掩码来配置命令中指定的网络接口。配置网络接口需要管理员权限。

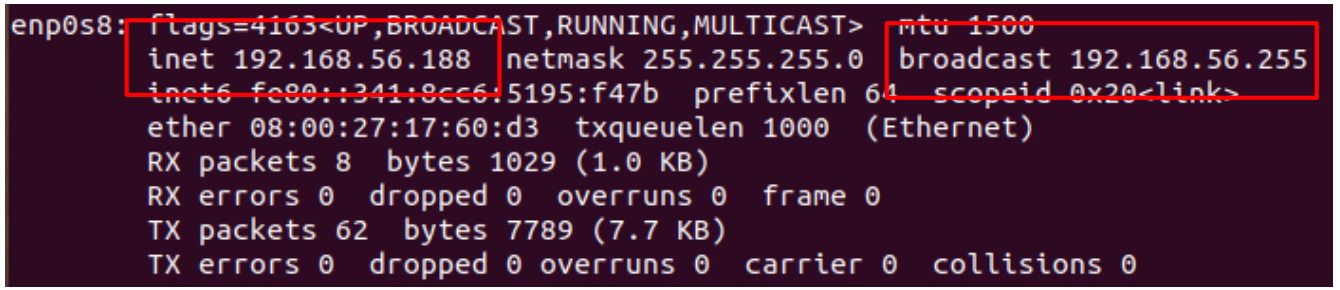
配置网络信息

例如使用ifconfig工具，给当前主机的enp0s8网络接口配置网络参数，其网络IP地址为192.168.56.188，子网掩码为255.255.255.0。

在终端命令提示符中输入如下命令。

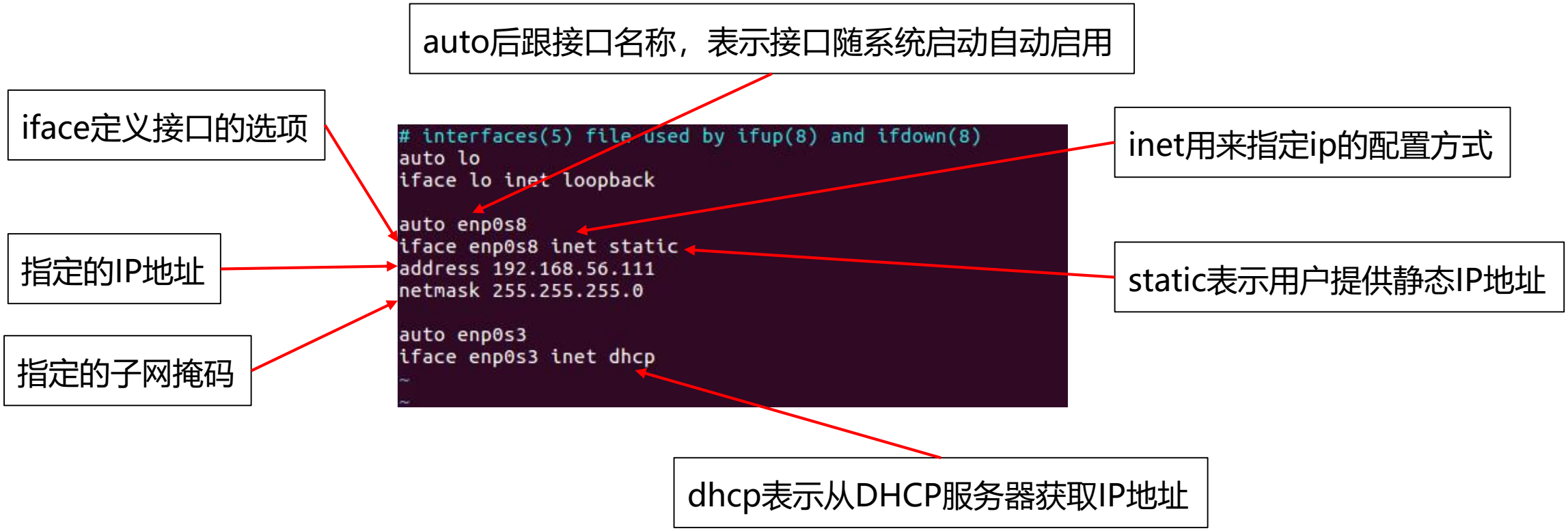
```
sudo ifconfig enp0s8 192.168.56.188 netmask 255.255.255.0
```

设置以后执行ifconfig enp0s8查看



静态IP地址配置

为网络接口指定一个静态IP，需要修改/etc/network/inerfaces配置文件。



设置以后重启系统生效。

网络接口的启用和禁用

启用和禁用指定的网络接口，其格式如下：

Ifconfig 网络接口名 up

ifconfig 网络接口名 down

在终端中使用如下命令禁用enp0s8，然后使用ifconfig enp0s8来查看该网络设备的状态。

sudo ifconfig enp0s8 down

不再包含RUNNING

```
lei@lei-VirtualBox:~$ ifconfig enp0s8
enp0s8: flags=4098<BROADCAST,MULTICAST>  mtu 1500
        inet 192.168.56.188  netmask 255.255.255.0  broadcast 192.168.56.255
        ether 08:00:27:17:60:d3  txqueuelen 1000  (Ethernet)
        RX packets 28  bytes 2828 (2.8 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 70  bytes 8525 (8.5 KB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

route工具的使用

使用ifconfig工具配置了网络接口的IP地址、网络掩码等参数后，该主机就可以在局域网络内和其他主机通信了，但是还不能访问外网的主机。此时需要使用route工具配置网络的路由记录或默认网关。

route工具可以用于查看当前的路由信息，也可以设置网络的默认路由信息。

查看路由信息

route命令在不带任何信息时，系统将返回当前路由表的信息。

```
lei@lei-VirtualBox:~$ route
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
default         _gateway        0.0.0.0         UG    100    0        0 enp0s3
10.0.2.0        0.0.0.0         255.255.255.0   U     100    0        0 enp0s3
link-local      0.0.0.0         255.255.0.0     U     1000   0        0 enp0s3
192.168.56.0    0.0.0.0         255.255.255.0   U     101    0        0 enp0s8
192.168.56.0    0.0.0.0         255.255.255.0   U     101    0        0 enp0s8
```

字 段	说 明
Destination	目标地址，可以是网络地址或主机地址
Gateway	与目标连接时通过的网关地址，*表示没有设置网关
Genmask	目的网络的网络掩码
Flags	路由标记，U表示路由可用，G表示连接目标是一个网关，H表示连接目标是一个主机
Metric	从源网络到达目标网络连接时经过的跳数
Ref	连接路由的参考数据
Use	查找该路由的次数
Iface	连接该路由的网络接口，其中lo表示本地回环设备

路由表

内核把路由归纳到许多个路由表中，并对这些表进行编号1~255。还可以在/etc/iproute2/rt_tables中为路由表命名。

```
#
# reserved values
#
255 local
254 main
253 default
0   unspec
#
# local
#
#1  inr.ruhep
```

默认情况下，所有的路由都会被插入到编号为254的main表中。

路由表

使用ip命令可以显示main路由表的路由信息。

ip route show

```
lei@lei-VirtualBox:~$ ip route show
default via 10.0.2.2 dev enp0s3 proto dhcp metric 100
10.0.2.0/24 dev enp0s3 proto kernel scope link src 10.0.2.15 metric 100
169.254.0.0/16 dev enp0s8 scope link metric 1000
192.168.56.0/24 dev enp0s8 proto kernel scope link src 192.168.56.111
```

第一行由网络接口enp0s3指定默认网关为10.0.2.2。默认网关是必须要有的路由信息，当系统发送数据包的时候，查不到相应的路由信息，便直接从默认路由发送。

第四行定义了一条通过网络接口enp0s8通向网络192.168.56.0/24的路由。

添加/ 删除默认网关

默认网关通常是一个公司或单位内部网络与外部网络通信的唯一通路，当公司内部网络上的主机与外部网络进行连接时，就将数据分组发给默认网关，由该网关负责数据分组的路由选择。可以使用route命令来添加或删除网络中的默认网关，其格式如下：

route add|del default gw 网关地址

参数add表示向路由表中添加一条路由信息，del表示删除路由表中的一条路由信息。gw参数用于指定网关地址。

测试默认网关

使用route命令，删除当前主机默认网关。其中，当前主机的默认网关地址为10.0.2.2。

在终端命令提示符下输入如下命令，为当前主机添加默认网关：

sudo route del default gw 10.0.2.2

```
lei@lei-VirtualBox:~$ ping -c 1 www.baidu.com
PING www.a.shifen.com (180.101.49.12) 56(84) bytes of data.
64 bytes from 180.101.49.12 (180.101.49.12): icmp_seq=1 ttl=48 time=15.8 ms

--- www.a.shifen.com ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 15.841/15.841/15.841/0.000 ms
lei@lei-VirtualBox:~$ sudo route del default gw 10.0.2.2
lei@lei-VirtualBox:~$ ping -c 1 www.baidu.com
connect: Network is unreachable
lei@lei-VirtualBox:~$ sudo route add default gw 10.0.2.2
lei@lei-VirtualBox:~$ ping -c 1 www.baidu.com
PING www.a.shifen.com (180.101.49.12) 56(84) bytes of data.
64 bytes from 180.101.49.12 (180.101.49.12): icmp_seq=1 ttl=48 time=15.2 ms

--- www.a.shifen.com ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 15.218/15.218/15.218/0.000 ms
```

添加/删除路由记录

使用route命令添加或删除一条到达目标网络的路由记录，其格式如下：

route add|del -net 网络地址 netmask 网络掩码 [gw 网关地址] [dev 网络接口]

其中参数add表示向路由表中添加一条路由信息，del表示删除路由表中的一条路由信息。gw参数用于指定网关地址，dev参数用于指定到达目标地址时数据分组投递的网络接口。

使用router命令添加或删除一条到达目标主机的路由记录，其格式如下：

route add|del -host IP地址 [gw 网关地址] [dev 网络接口]

在该命令中无需网络掩码，其中add参数、del参数、gw参数和dev参数含义同上。

其它常用配置文件

在Ubuntu中，具有以下与网络相关的典型配置文件。

① /etc/hostname 配置主机名。

② /etc/hosts 负责在本地将主机名映射到IP地址。hosts文件可用于替代DNS的域名映射，用户可以修改hosts文件，将某些域名映射到某个特定的IP地址上。

③ /etc/resolv.conf 保存域名服务器（DNS）的IP地址。

④ /etc/services 保存Internet网络服务列表，包括服务名、服务使用的端口、协议类型、别名等。

⑤ /etc/network/interfaces 网络接口配置文件，可用于配置IP、子网掩码和网关等。

配置主机名

查看主机名

hostname

```
lei@lei-VirtualBox:~$ hostname
lei-VirtualBox
```

主机名在/etc/hostname 设置

```
lei@lei-Host:~$ cat /etc/hostname
lei-Host
lei@lei-Host:~$
```

将主机名映射到IP地址

/etc/hosts文件可用于替代DNS的域名映射，用户可以修改hosts文件，将某些域名映射到某个特定的IP地址上。

```
lei@master:~$ cat /etc/hosts
127.0.0.1       localhost

# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

192.168.56.111 master
192.168.56.112 slaver1
192.168.56.113 slaver2
```

配置DNS服务器

DNS服务器的信息也是在/etc/network/inerfaces配置文件中指定。

```
# interfaces(5) file used by ifup(8) and ifdown(8)
auto lo
iface lo inet loopback

auto enp0s8
iface enp0s8 inet static
address 192.168.56.111
netmask 255.255.255.0
dns-nameservers 127.0.0.53
```

ping命令

Ping命令是使用ICMP协议来检测整个网络连通情况的。

ICMP是（Internet Control Message Protocol）Internet控制报文协议。它是TCP/IP协议族的一个子协议，用于在IP主机、路由器之间传递控制消息。控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息。这些控制消息虽然并不传输用户数据，但是对于用户数据的传递起着重要的作用。

ping命令是最常用的网络测试命令，该命令通过向被测试的目的主机地址发送ICMP报文并收取回应报文，来测试当前主机到目的主机的网络连接状态。

ping命令

在Linux系统中，ping命令默认会不间断地发送ICMP报文直到用户使用Ctrl+c键来终止该命令，使用“-c”参数可指定发送ICMP报文的数目。该命令的常用格式如下：

ping [选项] 目的主机IP地址/主机名

ping命令

检查域名为www.163.com 的网络连接情况

ping -c 3 www.163.com

查看本机是否安装TCP/IP，网卡是否工作正常。

ping -c 3 127.0.0.1

```
lei@lei-VirtualBox:~$ ping -c 3 127.0.0.1
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.013 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.018 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.018 ms

--- 127.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2055ms
rtt min/avg/max/mdev = 0.013/0.016/0.018/0.004 ms
```

NETSTAT

netstat用于查看网络状态，包括网络连接、路由表及网络接口的各种统计数据。

一般用法如下：

netstat 选项

参 数	含 义
-a	显示所有套接字，包括正在监听的
-c	每个1秒刷新一次结果，直到用户终止
-i	显示所有网络接口信息
-l	显示处于监听状态的套接字信息
-n	显示结果直接使用IP地址，而不使用域名
-t	显示TCP/IP协议的连接状况
-u	显示UDP协议的连接状况
-p	显示使用套接字的进程ID和程序名
-r	显示当前路由表的信息
-v	显示命令执行过程

NETSTAT示例

执行 netstat -tulnp

0.0.0.0表示的是这样一个集合：所有不清楚的主机和目的网络。

不清楚是指在本机的路由表里没有特定条目指明如何到达。

```
lei@lei-VirtualBox:~$ netstat -tulnp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN      -
tcp6       0      0 ::1:631                 :::*                    LISTEN      -
udp        0      0 0.0.0.0:40902           0.0.0.0:*                           -
udp        0      0 127.0.0.53:53           0.0.0.0:*                           -
udp        0      0 0.0.0.0:68              0.0.0.0:*                           -
udp        0      0 0.0.0.0:631             0.0.0.0:*                           -
udp        0      0 0.0.0.0:5353            0.0.0.0:*                           -
udp6       0      0 :::5353                 :::*                                -
udp6       0      0 :::43608                :::*                                -
```

协议

用户未读取的套接字中的数据

远程主机未读取的套接字中的数据

本地地址和端口号

远程地址和端口号

套接字状态

所谓套接字就是使应用程序能够读写与收发通讯协议(protocol)与资料的程序

NETSTAT示例

查看所有网络接口 netstat -i

```
lei@lei-VirtualBox:~$ netstat -i
Kernel Interface table
Iface      MTU    RX-OK RX-ERR RX-DRP RX-OVR    TX-OK TX-ERR TX-DRP TX-OVR Flg
enp0s3    1500     2399      0      0 0          1110      0      0      0 BMRU
enp0s8    1500       31      0      0 0            69      0      0      0 BMRU
lo       65536      170      0      0 0           170      0      0      0 LRU
```

查看路由表信息 netstat -r

```
lei@lei-VirtualBox:~$ netstat -r
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
default         _gateway        0.0.0.0         UG        0 0          0 enp0s3
10.0.2.0        0.0.0.0         255.255.255.0   U         0 0          0 enp0s3
link-local      0.0.0.0         255.255.0.0     U         0 0          0 enp0s8
192.168.56.0    0.0.0.0         255.255.255.0   U         0 0          0 enp0s8
```

防火墙工具ufw

防火墙是保护计算机系统免受网络上其他用户非法访问的一种软件系统。Ubuntu采用ufw作为防火墙管理工具。

启用

```
sudo ufw enable
```

查看防火墙状态

```
sudo ufw status
```

防火墙工具ufw

开启/禁用相应端口或服务

允许外部访问80端口

sudo ufw allow 80

禁止外部访问80 端口

sudo ufw delete allow 80

允许IP 192.168.1.1访问所有的本机端口

sudo ufw allow from 192.168.1.1