

<https://my.oschina.net/foreverich/blog/402252>

摘要：查看mac os x 的网络端口使用情况， `telnet`， `nc`，
`netstat`， `lsof`， 网络实用工具

查看端口是否打开

使用 `netstat` 命令

```
a. `netstat -nat | grep <端口号>` , 如命令 `netstat -nat | grep 3306`  
b. `netstat -nat |grep LISTEN`
```

使用 `lsof` 命令

```
# yongfu-pro at yongfu-pro.local in ~ [22:39:32]  
$ lsof -n -P -i TCP -s TCP:LISTEN  
COMMAND PID      USER      FD  TYPE   DEVICE  SIZE/OFF NODE  
NAME  
php-fpm 387  yongfu-pro    6u  IPv4  0x6d7f5d3c3a615679      0t0  TCP  
127.0.0.1:9000 (LISTEN)  
Dropbox 413  yongfu-pro   26u  IPv4  0x6d7f5d3c445e2c09      0t0  TCP  
*:17500 (LISTEN)  
php-fpm 418  yongfu-pro     0u  IPv4  0x6d7f5d3c3a615679      0t0  TCP  
127.0.0.1:9000 (LISTEN)  
php-fpm 419  yongfu-pro     0u  IPv4  0x6d7f5d3c3a615679      0t0  TCP  
127.0.0.1:9000 (LISTEN)  
php-fpm 420  yongfu-pro     0u  IPv4  0x6d7f5d3c3a615679      0t0  TCP  
127.0.0.1:9000 (LISTEN)  
stunnel 586  yongfu-pro     9u  IPv4  0x6d7f5d3c439ff679      0t0  TCP  
127.0.0.1:1997 (LISTEN)
```

`lsof`命令可以列出当前的所有网络情况， 此命令的解释如下：

- `-n` 表示主机以ip地址显示
- `-P` 表示端口以数字形式显示，默认为端口名称
- `-i` 意义较多，具体 `man lsof`，主要是用来过滤`lsof`的输出结果
- `-s` 和 `-i` 配合使用，用于过滤输出

使用`telnet` 命令

检查本机的3306端口是否打开， 如下

```
telnet 127.0.0.1 3306
```

若该端口没有打开，则会自动退出，并显示如下内容：

```
Trying 127.0.0.1...  
telnet: connect to address 127.0.0.1: Connection refused  
telnet: Unable to connect to remote host
```

若该端口为已打开的状态，则会一直保持连接。

如图

```
# yongfu at yf-mac.local in ~ [9:15:54]
$ telnet 127.0.0.1 1997
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
█
```

退出方法： ctrl +] 再 ctrl + c

```
# yongfu at yf-mac.local in ~ [9:13:26]
$ telnet 127.0.0.1 1997
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
^]
telnet> ^C
```

或者： ctrl + d 再 enter键

```
# yongfu at yf-mac.local in ~ [9:15:31]
$ telnet 127.0.0.1 1997
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
^D
Connection closed by foreign host.
```

使用 nc 命令

```
# yongfu at yf-mac.local in ~ [9:33:14]
$ nc -w 10 -n -z 127.0.0.1 1990-1999
Connection to 127.0.0.1 port 1997 [tcp/*] succeeded!
Connection to 127.0.0.1 port 1998 [tcp/*] succeeded!
```

-w 10 表示等待连接时间为10秒

-n 尽量将端口号名称转换为端口号数字

-z 对需要检查的端口没有输入输出，用于端口扫描模式

127.0.0.1 需要检查的ip地址

1990-1999 可以是一个端口，也可以是一段端口

返回结果为开放的端口，如本例中的 1997 和 1998 端口

使用网络实用工具

网络实用工具是苹果自带的网络分析工具

10.8之前的位于 launchpad --> 其他--> 网络实用工具

10.9之后隐藏了该应用，但可以通过 spotlight 搜索 网络实用工具或者 左上角的苹果标志 --> 关于本机 --> 点按'系统报告' --> 标题栏的'窗口' --> 网络实用工具 --> 点按'端口扫描'