nc

用于设置路由器，是网络工具中的瑞士军刀

补充说明

nc命令 全称**netcat**，用于设置路由器。它能通过 TCP 和 UDP 在网络中读写数据。通过与其他工具结合和重定向，你可以在脚本中以多种方式使用它。使用 netcat 命令所能完成的事情令人惊讶。

语法

```
nc [-hlnruz][-g<网关...>][-G<指向器数目>][-i<延迟秒数>][-o<输出文件>][-p<通信端口>]
[-s<来源位址>][-v...][-w<超时秒数>][主机名称][通信端口...]
```

选项

```
-g<网关> 设置路由器跃程通信网关，最多可设置8个。
-G<指向器数目> 设置来源路由指向器，其数值为4的倍数。
-h 在线帮助。
-i<延迟秒数> 设置时间间隔，以便传送信息及扫描通信端口。
-l 使用监听模式，管控传入的资料。
-n 直接使用IP地址，而不通过域名服务器。
-o<输出文件> 指定文件名称，把往来传输的数据以16进制字码倾倒成该文件保存。
-p<通信端口> 设置本地主机使用的通信端口。
-r 乱数指定本地与远端主机的通信端口。
-s<来源位址> 设置本地主机送出数据包的IP地址。
-u 使用UDP传输协议。
-v 显示指令执行过程。
-w<超时秒数> 设置等待连线的时间。
-z 使用0输入/输出模式，只在扫描通信端口时使用。
```

实例

TCP端口扫描

```
[root@localhost ~]# nc -v -z -w2 192.168.0.3 1-100
192.168.0.3: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.0.3] 80 (http) open
(UNKNOWN) [192.168.0.3] 23 (telnet) open
(UNKNOWN) [192.168.0.3] 22 (ssh) open
```

扫描192.168.0.3 的端口 范围是 1-100 扫描UDP端口

```
[root@localhost ~]# nc -u -z -w2 192.168.0.1 1-1000  # 扫描192.168.0.3 的端口 范围是 1-1000
```

扫描指定端口

```
[root@localhost ~]# nc -nvv 192.168.0.1 80 # 扫描 80端口
(UNKNOWN) [192.168.0.1] 80 (?) open
```

```
y  //用户输入
```

查看从服务器到目的地的出站端口 443 是否被防火墙阻止

```
nc -vz acme-v02.api.letsencrypt.org 443 -w2
# Ncat: Version 7.50 ( https://nmap.org/ncat )
# Ncat: Connected to 23.77.214.183:443.
# Ncat: 0 bytes sent, 0 bytes received in 0.07 seconds.
```

传文件

```
###接受端
nc -l port > your.file

###发送端
nc -w 1 ip port < your.file
```

报错

close: Bad file descriptor

```
$ close: Bad file descriptor
#解决方法: 使用nc -4□强制使用ipv4即可。
```