tcpdump

一款sniffer工具，是Linux上的抓包工具，嗅探器

补充说明

tcpdump命令 是一款抓包，嗅探器工具，它可以打印所有经过网络接口的数据包的头信息，也可以使用-w选项将数据包保存到文件中，方便以后分析。

语法

```
tcpdump(选项)
```

选项

```
-a□尝试将网络和广播地址转换成名称；
-c<数据包数目>：收到指定的数据包数目后，就停止进行倾倒操作；
-d□把编译过的数据包编码转换成可阅读的格式，并倾倒到标准输出；
-dd□把编译过的数据包编码转换成C语言的格式，并倾倒到标准输出；
-ddd□把编译过的数据包编码转换成十进制数字的格式，并倾倒到标准输出；
-e□在每列倾倒资料上显示连接层级的文件头；
-f□用数字显示网际网络地址；
-F<表达文件>：指定内含表达方式的文件；
-i<网络界面>：使用指定的网络截面送出数据包；
-l□使用标准输出列的缓冲区；
-n□不把主机的网络地址转换成名字；
-N□不列出域名；
-O□不将数据包编码最佳化；
-p□不让网络界面进入混杂模式；
-q □快速输出，仅列出少数的传输协议信息；
-r<数据包文件>：从指定的文件读取数据包数据；
-s<数据包大小>：设置每个数据包的大小；
-S□用绝对而非相对数值列出TCP关联数；
-t□在每列倾倒资料上不显示时间戳记；
-tt□ 在每列倾倒资料上显示未经格式化的时间戳记；
-T<数据包类型>：强制将表达方式所指定的数据包转译成设置的数据包类型；
-v□详细显示指令执行过程；
-vv□更详细显示指令执行过程；
-x□用十六进制字码列出数据包资料；
-w<数据包文件>：把数据包数据写入指定的文件。
```

实例

直接启动tcpdump将监视第一个网络接口上所有流过的数据包

```
tcpdump
```

监视指定网络接口的数据包

```
tcpdump -i eth1
```

如果不指定网卡，默认tcpdump只会监视第一个网络接口，一般是eth0□下面的例子都没有指定网络接口。

监视指定主机的数据包

打印所有进入或离开sundown的数据包。

```
tcpdump host sundown
```

也可以指定ip,例如截获所有210.27.48.1 的主机收到的和发出的所有的数据包

```
tcpdump host 210.27.48.1
```

打印helios 与 hot 或者与 ace 之间通信的数据包

```
tcpdump host helios and \( hot or ace \)
```

截获主机210.27.48.1 和主机210.27.48.2 或210.27.48.3的通信

```
tcpdump host 210.27.48.1 and \ (210.27.48.2 or 210.27.48.3 \)
```

打印ace与任何其他主机之间通信的IP 数据包, 但不包括与helios之间的数据包.

```
tcpdump ip host ace and not helios
```

如果想要获取主机210.27.48.1除了和主机210.27.48.2之外所有主机通信的ip包，使用命令：

```
tcpdump ip host 210.27.48.1 and ! 210.27.48.2
```

抓取eth0网卡上的包，使用:

```
sudo tcpdump -i eth0
```

截获主机hostname发送的所有数据

```
tcpdump -i eth0 src host hostname
```

监视所有送到主机hostname的数据包

```
tcpdump -i eth0 dst host hostname
```

监视指定主机和端口的数据包

如果想要获取主机210.27.48.1接收或发出的telnet包，使用如下命令

```
tcpdump tcp port 23 and host 210.27.48.1
```

对本机的udp 123 端口进行监视 123 为ntp的服务端口

```
tcpdump udp port 123
```

监视指定网络的数据包

打印本地主机与Berkeley网络上的主机之间的所有通信数据包

```
tcpdump net ucb-ether
```

ucb-ether此处可理解为“Berkeley网络 ” 的网络地址，此表达式最原始的含义可表达为：打印网络地址为ucb-ether的所有数据包

打印所有通过网关snup的

```
tcpdump 'gateway snup and (port ftp or ftp-data)'
```

注意：表达式被单引号括起来了，这可以防止shell对其中的括号进行错误解析

打印所有源地址或目标地址是本地主机的IP数据包

```
tcpdump ip and not net localnet
```

如果本地网络通过网关连到了另一网络，则另一网络并不能算作本地网络。

抓取80端口的HTTP报文，以文本形式展示：

```
sudo tcpdump -i any port 80 -A
```