Просмотр всех открытых портов

```
# netstat -na
```

Просмотр всех откры TCP-портов

```
# netstat -nat
```

Просмотр всех откры UDP-портов

```
# netstat -nau
```

Просмотр всех прослушиваемых портов(TCP,UDP,unix-сокеты)

```
# netstat -npl
```

Просмотр всех прослушиваемых портов TCP

```
# netstat -nptl
```

Просмотр всех прослушиваемых портов UDP

```
# netstat -npul
```

Просмотр всех прослушиваемых unix-сокетов

```
# netstat -nplx
```

Просмотр статистики всех протоколов()

```
# netstat -s
```

Просмотр статистики TCP-протокола

```
# netstat -st
```

Просмотр статистики UDP-протокола

```
# netstat -su
```

Просмотр таблицы маршрутизации

```
# netstat -r
```

Просмотр статистики сетевых интерфейсов

```
# netstat -i
```

Просмотр статистики сетевых интерфейсов в режиме реального времени с обновлением каждые 2 секунды.

```
# netstat -ic 2
```

Просмотр расширенной информации о сетевых интерфейсах (аналог ifconfig)

```
# netstat -ie
```

Использование Netstat для определения DoS/DDoS.

Отображение количества подключений на каждый IP-адрес в состоянии ESTABLISHED

```
# netstat -naltp | grep ESTABLISHED | awk '{print $5}' | awk -F:
'{print $1}' | sort -n | uniq -c
```

или

```
# netstat -nalpt | grep ESTABLISHED | awk '{print $5}' | cut -d:
-f1| sort | uniq -c | sort -rn
```

Отобразить все активные Интернет-подключения на 80 порт сервера с их сортировкой
Полезно для определения большого количества запросов с одного IP-адреса(DoS)

```
# netstat -na | grep :80 | sort
```

Подсчет количества подключений с каждого Ip-адреса на 80-порт сервера.

```
# netstat -npla | grep :80 | awk '{print $5}' | cut -d: -f1 |
sort | uniq -c | sort -rn
```

Определение количества запросов на соединение было получено из сети.
Число должно быть достаточно низким(менее 5).Во время DoS/DDoS-атаки такое количество может иметь высокое значение.Однако значение всегда зависит от системы(высокое значение на одном сервере может быть средним на другом)

```
# netstat -np | grep SYN_RECV | wc -l
```

Список всех IP-адресов, с которых поступают соединения со статусом SYN_RECV

```
# netstat -np | grep SYN_RECV | awk '{print $5}' | awk -F:
'{print $1}'
```

Подсчет количества подключений с каждого IP-адреса

```
# netstat -ntu | awk '{print $5}' | cut -d: -f1 | sort | uniq -c
| sort -rn
```

Подсчет количества подключений с каждого IP-адреса по протоколу TCP или UDP.

```
# netstat -nap | grep 'tcp\|udp' | awk '{print $5}' | cut -d: -
f1| sort | uniq -c | sort -rn
```

—
Источник — Использование netstat