Команда netstat: получение всевозможной информации о состоянии сети

Команда netstat выдает различную информацию о состоянии сетевого программного обеспечения, включая статистику сетевых интерфейсов, данные о маршрутизации и таблицы соединений. Никакого объединяющего звена во всех этих информационных блоках нет, просто они касаются функционирования сети. Команда netstat включена во все операционные системы, но в каждой из них поддерживаются разные наборы опций.

Мы рассмотрим четыре наиболее распространенных варианта использования команды netstat.

Это:

- проверка состояния сетевых соединений;
- анализ информации о конфигурации интерфейсов;
- изучение таблицы маршрутизации;
- получение статистических данных о различных сетевых протоколах.

Контроль состояния сетевых соединений

Будучи вызванной без аргументов, команда netstat выдает информацию о состоянии активных TCP- и UDP-портов. Неактивные серверы, ожидающие запросов на установление соединений, как правило, не отображаются. О них можно узнать с помощью команды netstat -a . Результат выглядит так:

```
% netstat -a
Active Internet connections (including servers)
Proto Recv-Q Send-Q Local Address Foreign Address (state)
tcp4 0 0 *.6013 *.* LISTEN
tcp46 0 0 *.6013 *.* LISTEN
tcp4 0 0 nimi.ssh xor.com.4105 ESTABLISHED
```

```
tcp4 0 20 nimi.ssh xor.com.1612 ESTABLISHED
tcp4 0 0 *.13500 *.* LISTEN
tcp4 0 0 nimi.ssh 135.197.2.114.883 ESTABLISHED
tcp4 0 0 nimi.1599 xor.com.telnet ESTABLISHED
tcp4 0 0 *.ssh *.* LISTEN
tcp46 0 0 *.ssh *.* LISTEN
tcp4 0 0 nimi.ssh 135.197.2.114.776 ESTABLISHED
tcp4 0 0 *.cvsup *.* LISTEN
udp4 0 0 *.syslog *.*
udp4 0 0 *.ntalk *.*
...
```

Этот результат получен на компьютере nimi. Вывод команды свидетельствует о наличии нескольких входящих соединений по протоколу SSH, одного исходящего telnet-соединения и группы портов, ожидающих установления соединения. Обратите внимание на строки, в которых тип протокола — tcp46. Это сервисы, работающие в соответствии со стандартом IPv6.

Адреса представлены в формате имя_компьютера.сервис, где сервис — номер порта. Для известных сервисов порты указаны в символическом виде (соответствия между номерами портов и их именами определены в файле /etc/services). При наличии опции -n все адреса отображаются в числовом виде. Помните, *что при нефункционирующей службе DNS команда netstat будет выполняться очень медленно, если не указать флаг* ***-n****.*

В колонках Send-Q и Recv-Q показывается, сколько запросов находится во входящих и исходящих очередях на данном компьютере. На другом конце соединения размеры очередей могут быть другими. Желательно, чтобы эти значения были близки к нулю и не были ненулевыми постоянно. Конечно, если команда netstat запускается через сетевой терминал, для ее соединения размер исходящей очереди, скорее всего, никогда не будет равен 0.

Состояние соединения имеет значение только для протокола TCP. Протокол UDP не проверяет факт установления соединения. Наиболее распространенные состояния: ESTABLISHED (установлено)

– для активных соединений, LISTENING (ожидание) – для серверов, ожидающих поступления запросов (при отсутствии опции -a обычно не показываются), TIME_WAIT (ожидание закрытия) – для соединений, находящихся в процессе закрытия.

Эта информация полезна главным образом для устранения проблем на более высоком уровне, если, конечно, базовые сетевые средства работают нормально. Команда netstat позволяет проверить правильность настройки серверов и диагностировать определенные виды нарушений связи, особенно при работе с протоколом TCP. Например, если соединение находится в состоянии SYN_SENT, это означает наличие процесса, который пытается установить контакт с несуществующим или недоступным сервером.

Если команда netstat сообщает о большом количестве соединений, находящихся в состоянии SYN_WAIT, то компьютер, вероятно, не в состоянии обработать запросы на установление соединений. Такая ситуация может быть вызвана ограничениями системного ядра или даже злонамеренными попытками вызвать перегрузку.

Просмотр информации о конфигурации интерфейса

Команда netstat -i сообщает о состоянии сетевых интерфейсов. Вот, к примеру, результаты, полученные на компьютере evolve, работающем под управлением Solaris:

```
% netstat -i
Name Mtu Net/Dest Ipkts Ierrs Opkts Oerrs Collis
lo0 8232 loopback 11650 0 11650 0 0
hme0 1500 evolve 16438 0 18356 0 110
hmel 1500 evolve-bl 94852 7 379410 13 487
```

Указанный компьютер имеет два сетевых интерфейса. В колонках Ipkts и Opkts указывается количество пакетов, принятых и переданных через каждый интерфейс с момента начальной загрузки системы. В колонках Ierrs и Oerrs приводится число ошибок в принимаемых и передаваемых данных: здесь учитывается много разных типов ошибок, и наличие какого-то их числа вполне

нормально.

Количество ошибок должно составлять менее 1% от числа пакетов. Если частота появления ошибок высока, сравните эти показатели на нескольких соседних компьютерах. Большое число ошибок на одном компьютере свидетельствует о наличии проблемы в его интерфейсе или соединении, тогда как высокая частота ошибок, возникающих на всех компьютерах, в большинстве случаев обусловлена наличием проблемы в среде передачи.

Количество коллизий – это показатель степени загруженности сети; наличие ошибок свидетельствует о проблемах с кабелями. Хотя коллизия является одной из разновидностей ошибки, их число команда netstat подсчитывает отдельно. В колонке Collis указывается число конфликтов, произошедших при отправке пакетов. Это число следует использовать для вычисления доли ошибочных пакетов от общего количества отправленных пакетов (Opkts). В приведенном выше примере частота конфликтов в интерфейсе hme0 составляет около 0,6%, а в интерфейсе hme1 – 0,13%. “Нормальным” считается значение менее 5%, а значение выше 15% говорит о серьезной перегрузке сети.

Работу сетевого интерфейса можно контролировать в реальном времени, однако соответствующие опции командной строки различаются в зависимости от системы. Показанные ниже команды выдают статистику с интервалом в одну секунду. Выводные данные взяты из FreeBSD.

```
solaris% netstat -i 1
hp-ux% netstat 1
redhat% netstat -i –c
freebsd% netstat 1
input (Total) output
packets errs packets errs colls
13971549 1216 14757869 16 1431629
512 0 99 1 27
464 1 94 0 40
516 0 101 0 26
452 1 87 0 14
```

```
336 0 71 0 19
```

В этом примере количество коллизий составляет от 20% до 30%. Видимо, сеть передает пакеты очень медленно или вообще не функционирует.

Непрерывный режим работы команды netstat особенно эффективен при выслеживании источника ошибок. Команда *netstat -i* может сообщить о существовании проблем, но она не скажет, какова причина ошибок: то ли это постоянно возникающая аппаратная проблема, то ли кратковременное, но фатальное событие. Наблюдение за сетью при различных уровнях загруженности позволит получить гораздо более полное представление о том, что происходит. Задайте команду *ping с большой длиной пакетов* и наблюдайте за выводом команды netstat.

Проверка таблицы маршрутизации

Команда netstat -r отображает таблицу маршрутизации ядра. Вот пример, полученный на компьютере, который работает под управлением Solaris и имеет два сетевых интерфейса:

```
% netstat -r -n
Routing Table
Destination Gateway Flags Ref Use Interface
192.225.44.0 192.225.44.88 U 3 1841 hme0
192.168.3.0 192.168.3.12 U 2 1317 hmel
10.0.0.0 192.168.3.252 UG 0 4 hmel
default 192.225.44.254 UG 0 91668
127.0.0.1 127.0.0.1 UH 0 543 lo0
```

Пункты назначения и шлюзы могут быть представлены либо доменными именами, либо IP-адресами. Опция -n задает вывод IP-адресов.

В колонке Flags отображаются флаги, характеризующие маршрут: U (up) — активный, G (gateway) — шлюз, H (host) — узловой (связан с конкретным адресом, а не сетью). Флаг D (не показан) обозначает маршрут, полученный в результате переадресации по протоколу ICMP. Флаги G и H вместе обозначают маршрут к

компьютеру, проходящий через промежуточный шлюз. Остальные поля содержат статистические данные о маршруте: текущее число TCP-соединений по этому маршруту, количество отправленных пакетов и имя используемого интерфейса. Точный вид представленных данных зависит от конкретной операционной системы.

Приведенный вариант команды netstat полезен для проверки правильности таблицы маршрутизации. Особенно важно убедиться в наличии и корректности стандартного маршрута. Иногда он обозначается в виде адреса со всеми нулями (0.0.0.0), иногда — словом default.

Просмотр статистики функционирования различных сетевых протоколов

Команда *netstat -s* выдает содержимое всевозможных счетчиков, используемых в сетевых программах. Информация разбивается на разделы в соответствии с протоколами: IP, ICMP, TCP и UDP. Ниже приведены отдельные фрагменты листинга команды netstat -s, полученного на компьютере-шлюзе; они отредактированы так, чтобы были видны только наиболее интересные данные.

```
ip:
2313683 total packets received
0 bad header checksums
1642600 packets for this host
25743 packets sent from this host
0 output packets dropped due to no bufs, etc.
```

Отсутствие ошибок контрольных сумм говорит о том, что аппаратное соединение работает нормально. Также важен тот факт, что пакеты не отбрасывались из-за недостатка свободной памяти (последняя строка).

```
icmp:
57 calls to icmp_error
Output histogram:
echo reply: 157
destination unreachable: 57
```

```
Input histogram:
echo reply: 6
destination unreachable: 4
echo: 157
time exceeded: 14
157 message responses generated
```

Показатели числа эхо-запросов, сгенерированных ответов и эхо-ответов совпадают. Отметим, что сообщения “destination unreachable” (адресат недостижим) могут посылаться даже тогда, когда пакеты, казалось бы, маршрутизируются нормально. Например, дефектные пакеты рано или поздно достигают шлюза, который отклоняет их, и по цепи шлюзов возвращается сообщение об ошибке.

```
tcp:
25087 packets sent
25499 packets received
31 connection requests
30 connection accepts
56 connections established (including accepts)
64 connections closed (including 13 drops)
4 embryonic connections dropped
```

Рекомендуем определить приемлемые диапазоны этих показателей, чтобы можно было сразу же замечать необычное поведение сети.