ЛАБОРАТОРНАЯ РАБОТА № 14

**Протоколы транспортного уровня TCP/IP, TCP и UDP**

**Цель работы.** Провести анализ работы протоколов транспортного уровня TCP/IP(TCP, UDP) с использованием Netstat.

**Краткие теоретические сведения**

**Netstat** – отображает активные подключения TCP, портов, прослушиваемых компьютером, статистики Ethernet, таблицы маршрутизации IP, статистики IPv4 (для протоколов IP, ICMP, TCP и UDP) и IPv6 (для протоколов IPv6, ICMPv6, TCP через IPv6 и UDP через IPv6). Запущенная без параметров, команда **nbtstat** отображает подключения TCP.

### Синтаксис

netstat [-Aan] [-f семейство\_адресов] [-I интерфейс] [-p имя\_протокола] [система] [core]

netstat [-n] [-s] [-i | -r] [-f семейство\_адресов] [-I интерфейс] [-p имя\_протокола] [система] [core]

netstat [-n] [-I интерфейс] интервал [система] [core]

Первая форма команды показывает список активных сокетов ([sockets](http://ru.wikipedia.org/wiki/Socket" \o "Socket)) для каждого протокола. Вторая форма выбирает одну из нескольких других сетевых структур данных. Третья форма показывает динамическую статистику пересылки пакетов по сконфигурированным сетевым интерфейсам; аргумент интервал задает, сколько секунд собирается информация между последовательными показами.

**Опции**

|  |  |
| --- | --- |
| -a | Показывать состояние всех сокетов; обычно сокеты, используемые серверными процессами, не показываются. |
| -A | Показывать адреса любых управляющих блоков протокола, связанных с сокетами; используется для отладки. |
| -i | Показывать состояние автоматически сконфигурированных (auto-configured) интерфейсов. Интерфейсы, статически сконфигурированные в системе, но не найденные во время загрузки, не показываются. |
| -n | Показывать сетевые адреса как числа. netstat обычно показывает адреса как символы. Эту опцию можно использовать с любым форматом показа. |
| -r | Показать таблицы маршрутизации. При использовании с опцией -s, показывает статистику маршрутизации. |
| -s | Показать статистическую информацию по протоколам. При использовании с опцией -r, показывает статистику маршрутизации. |
| -f семейство\_адресов | Ограничить показ статистики или адресов управляющих блоков только указанным семейством\_адресов, в качестве которого можно указывать: **inet** Для семейства адресов **AF\_INET**, или **unix** Для семейства адресов **AF\_UNIX**. |
| -I интерфейс | Выделить информацию об указанном интерфейсе в отдельный столбец; по умолчанию (для третьей формы команды) используется интерфейс с наибольшим объёмом переданной информации с момента последней перезагрузки системы. В качестве интерфейса можно указывать любой из интерфейсов, перечисленных в файле конфигурации системы, например, emd1 или lo0. |
| -p имя\_протокола | Ограничить показ статистики или адресов управляющих блоков только протоколом с указанным именем\_протокола, например, tcp. |

**Активные сокеты**

Для каждого активного сокета показывается протокол, размер очередей приема и получения (в байтах), локальный и удаленный адрес, а также внутреннее состояние протокола. Символьный формат, обычно используемый для показа адресов сокетов, — это либо:

имя\_хоста.порт

если имя хоста указано, либо:

сеть.порт

если адрес сокета задает сеть, но не конкретный хост. Имена хостов и сетей берутся из соответствующих записей в файле /etc/hosts или /etc/networks.

Если имя сети или хоста для адреса неизвестно (или если указана опция -n), адрес показывается числами. Не указанные или «обобщенные» адреса и порты показываются как «\*».

**Сокеты TCP**

Для сокетов TCP допустимы следующие значения состояния:

|  |  |
| --- | --- |
| CLOSED | Закрыт. Сокет не используется. |
| LISTEN | Ожидает входящих соединений. |
| SYN\_SENT | Активно пытается установить соединение. |
| SYN\_RECEIVED | Идет начальная синхронизация соединения. |
| ESTABLISHED | Соединение установлено. |
| CLOSE\_WAIT | Удаленная сторона отключилась; ожидание закрытия сокета. |
| FIN\_WAIT\_1 | Сокет закрыт; отключение соединения. |
| CLOSING | Сокет закрыт, затем удаленная сторона отключилась; ожидание подтверждения. |
| LAST\_ACK | Удаленная сторона отключилась, затем сокет закрыт; ожидание подтверждения. |
| FIN\_WAIT\_2 | Сокет закрыт; ожидание отключения удаленной стороны. |
| TIME\_WAIT | Сокет закрыт, но ожидает пакеты, ещё находящиеся в сети для обработки |

**Показ таблицы маршрутизации**

Таблица маршрутизации показывает все имеющиеся маршруты (routes) и статус каждого из них. Каждый маршрут состоит из целевого хоста или сети и шлюза (gateway), который используется для пересылки пакетов. Столбец flags (флаги) показывает статус маршрута (U, если он включен), ведет ли маршрут на шлюз (G), был ли маршрут создан динамически при помощи перенаправления (D) и используется ли адрес индивидуального хоста (H) вместо адреса сети. Например, интерфейс закольцовывания (loopback transport provider), lo0, всегда имеет флаг H.

Прямые маршруты создаются для каждого интерфейса, подключенного к локальному хосту; поле gateway (шлюз) для таких записей показывает адрес выходного интерфейса.

Столбец refcnt показывает текущее количество активных использований для маршрута. Протоколы, ориентированные на соединение, обычно используют в ходе соединения один маршрут, тогда как протоколы без соединения получают маршрут для каждой посылки одному и тому же адресату.

Столбец use показывает количество пакетов, посланных по маршруту.

Столбец interface показывает сетевой интерфейс, используемый маршрутом.

**Суммарная статистика передачи данных**

Когда задан аргумент интервал, netstat показывает таблицу суммарной статистической информации о переданных пакетах, ошибках и коллизиях. Первая показываемая строка данных, а также каждая последующая 24-я строка содержит суммарную статистическую информацию с момента последней перезагрузки системы. Каждая последующая строка показывает данные, накопленные за очередной указанный в командной строке интервал с момента последнего показа.

**ВЫПОЛЕНИЕ**

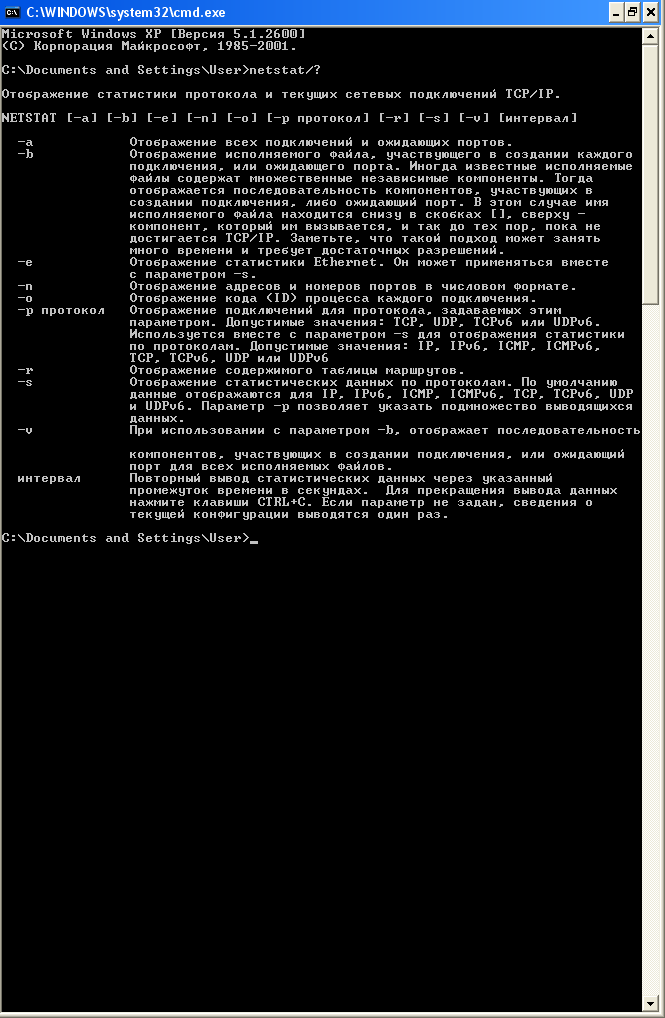


Рисунок 1 – Вывод справки (netstat/?)



Рисунок 2 – Использование Netstat для просмотра имеющихся соединений (netstat -a):

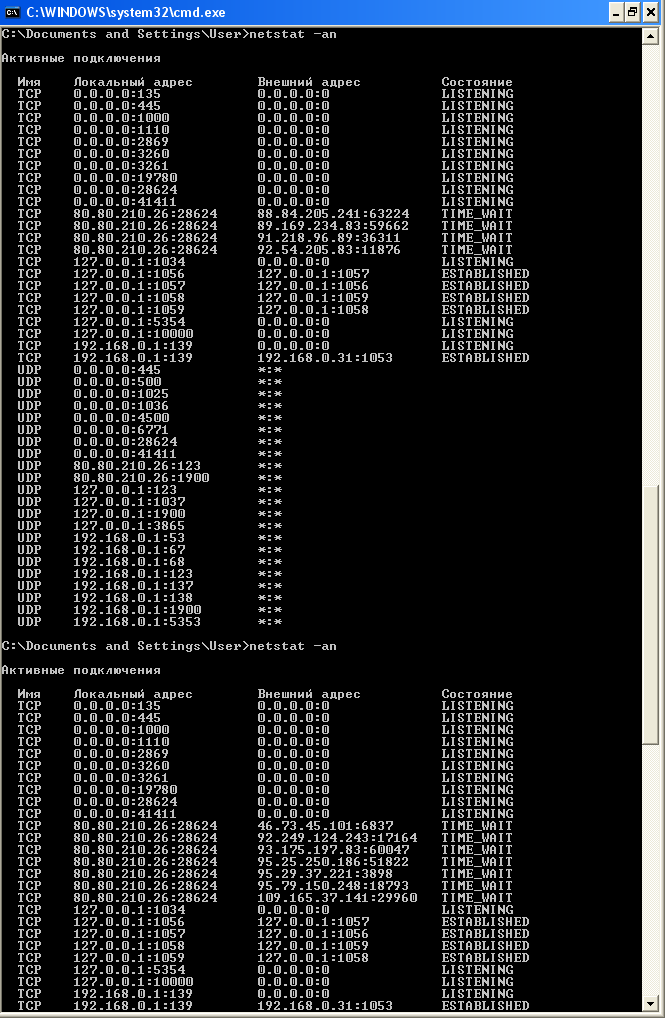
****

Рисунок 3 – Вывод соединений в числовом формате (netstat -an)

В процессе выполнения команд Netstat компьютер клиента имел выход в Интернет. При этом выполнялся запрос на сайт [www.rambler.ru](http://www.rambler.ru) через браузер Mozilla Firefox. Через определенные интервалы времени компьютер находился в режиме ожидания для установления соединения (состояние TIME\_WAIT). После успешного выполнения соединения на экран выводилось состояние ESTABLISHED.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Соединение | Имя | Локальный адрес | Внешний адрес | Состояние |
| 1. | TCP | pc: 10499 | [www.rambler.ru: http](http://www.rambler.ru:%20http) | TIME\_WAIT |
| TCP | 80.80.210.26:28624 | 88.84.205.241: 63224 | TIME\_WAIT |
| 2. | TCP | pc: 10502 | [www.rambler.ru: http](http://www.rambler.ru:%20http) | TIME\_WAIT |
| TCP | 80.80.210.26:28624 | 89.169.234.83: 59662 | TIME\_WAIT |
| 3. | TCP | pc: 28624 | Host-77-81-205-101.ucanet.ru: 6426 | TIME\_WAIT |
| TCP | 80.80.210.26:28624 | 91.218.96.89: 36311 | TIME\_WAIT |
| 4. | UDP | pc: ntp | \*:\* |  |
| UDP | 80.80.210.26:123 | \*:\* |  |
| 5. | UDP | pc:1037 | \*:\* |  |
| UDP | 80.80.210.26:1900 | \*:\* |  |
| 6. | UDP | pc: 1900 | \*:\* |  |
| UDP | 127.0.0.1:123 | \*:\* |  |

**Содержание отчета**

1. Краткие теоретические сведения.
2. Основные команды утилиты Netstat.
3. Основные состояния, выводимые утилитой Netstat.
4. Результаты анализа выполнения запросов к сети Интернет.
5. Анализ полученных результатов.

**Контрольные вопросы**

1. Функции сокетов TCP.
2. Что такое локальный адрес?
3. Для чего нужна таблица маршрутизации?
4. Функции утилиты Netstat.
5. Таблица маршрутизаций.
6. Выполнения запросов к сети Интернет