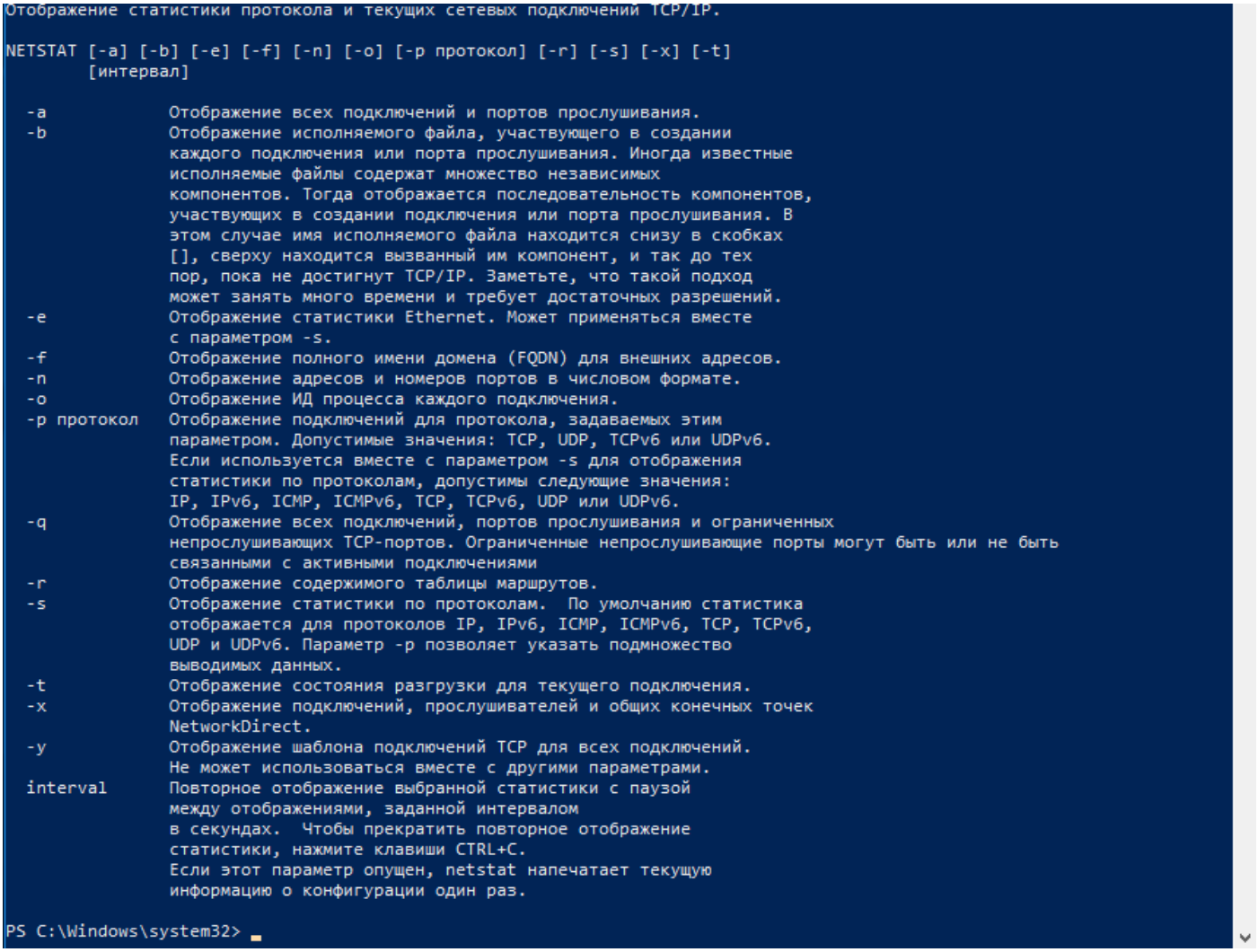


Ключи для команды netstat

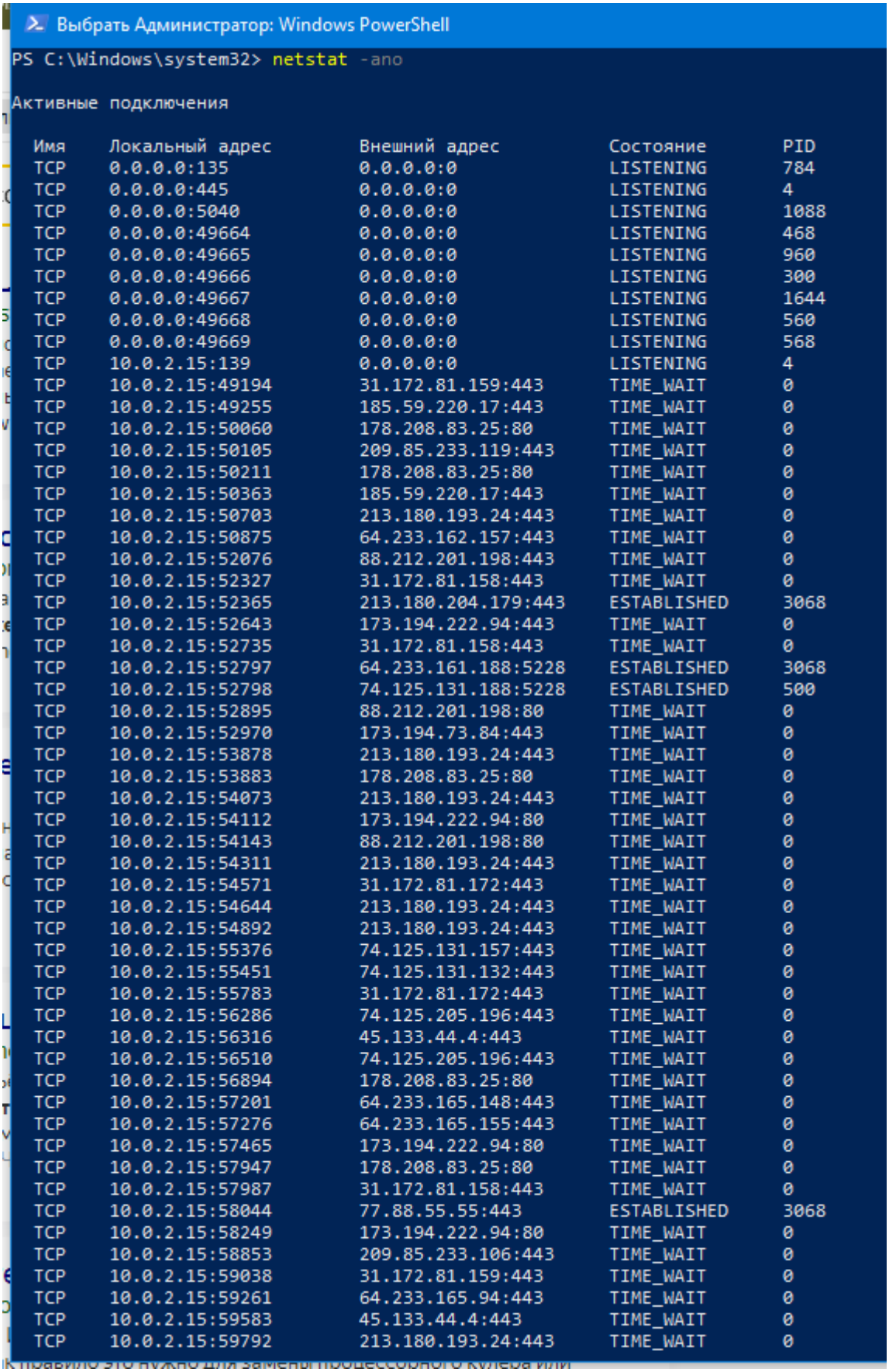
Отчет должен содержать подробное описание 10 произвольных строк:

что это за сокет,

какой протокол, в каком состоянии соединение,

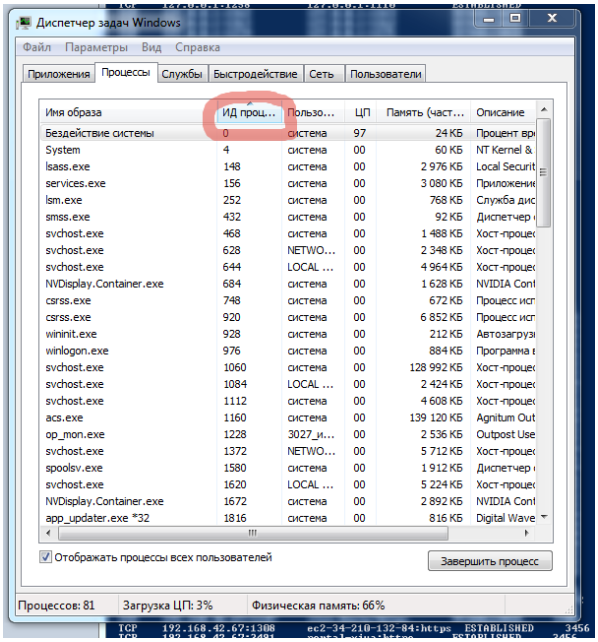
какой сервис или программа его использует,

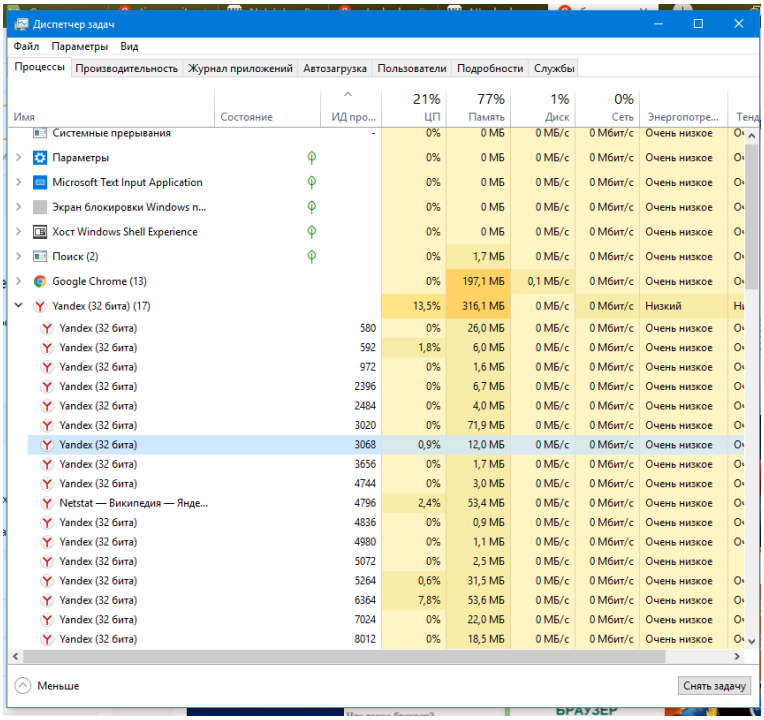
зачем.

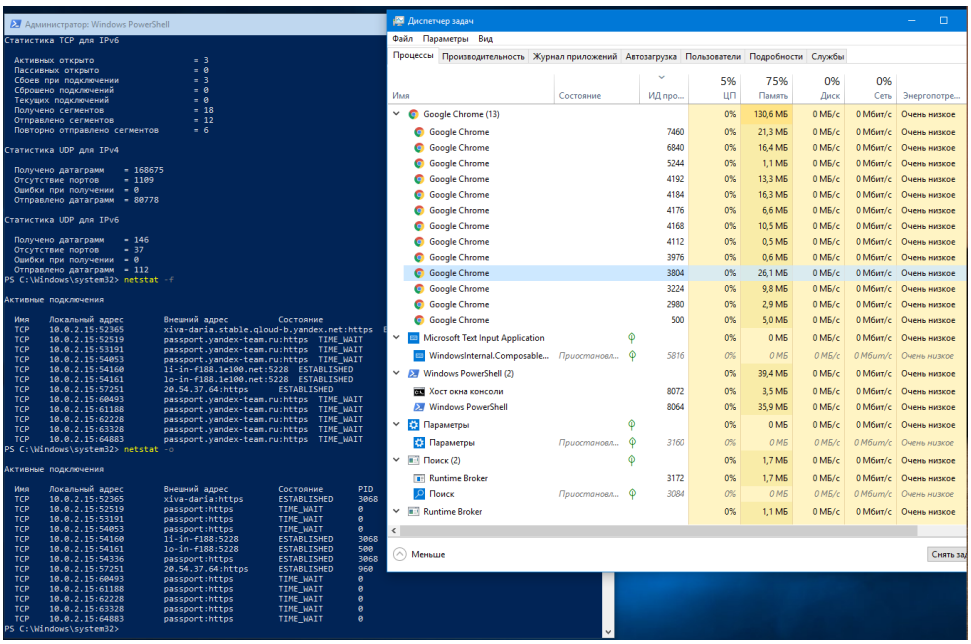

Выбрать Администратор: Windows PowerShell
PS C:\Windows\system32> netstat -ano
Активные подключения
Имя Локальный адрес Внешний адрес Состояние PID
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING 784
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING 4
TCP 0.0.0.0:5040 0.0.0.0:0 LISTENING 1088
TCP 0.0.0.0:49664 0.0.0.0:0 LISTENING 468
TCP 0.0.0.0:49665 0.0.0.0:0 LISTENING 960
TCP 0.0.0.0:49666 0.0.0.0:0 LISTENING 300
TCP 0.0.0.0:49667 0.0.0.0:0 LISTENING 1644
TCP 0.0.0.0:49668 0.0.0.0:0 LISTENING 560
TCP 0.0.0.0:49669 0.0.0.0:0 LISTENING 568
TCP 10.0.2.15:139 0.0.0.0:0 LISTENING 4
TCP 10.0.2.15:49194 31.172.81.159:443 TIME_WAIT 0
TCP 10.0.2.15:49255 185.59.220.17:443 TIME_WAIT 0
TCP 10.0.2.15:50060 178.208.83.25:80 TIME_WAIT 0
TCP 10.0.2.15:50105 209.85.233.119:443 TIME_WAIT 0
TCP 10.0.2.15:50211 178.208.83.25:80 TIME_WAIT 0
TCP 10.0.2.15:50363 185.59.220.17:443 TIME_WAIT 0
TCP 10.0.2.15:50703 213.180.193.24:443 TIME_WAIT 0
TCP 10.0.2.15:50875 64.233.162.157:443 TIME_WAIT 0
TCP 10.0.2.15:52076 88.212.201.198:443 TIME_WAIT 0
TCP 10.0.2.15:52327 31.172.81.158:443 TIME_WAIT 0
TCP 10.0.2.15:52365 213.180.204.179:443 ESTABLISHED 3068
TCP 10.0.2.15:52643 173.194.222.94:443 TIME_WAIT 0
TCP 10.0.2.15:52735 31.172.81.158:443 TIME_WAIT 0
TCP 10.0.2.15:52797 64.233.161.188:5228 ESTABLISHED 3068
TCP 10.0.2.15:52798 74.125.131.188:5228 ESTABLISHED 500
TCP 10.0.2.15:52895 88.212.201.198:80 TIME_WAIT 0
TCP 10.0.2.15:52970 173.194.73.84:443 TIME_WAIT 0
TCP 10.0.2.15:53878 213.180.193.24:443 TIME_WAIT 0
TCP 10.0.2.15:53883 178.208.83.25:80 TIME_WAIT 0
TCP 10.0.2.15:54073 213.180.193.24:443 TIME_WAIT 0
TCP 10.0.2.15:54112 173.194.222.94:80 TIME_WAIT 0
TCP 10.0.2.15:54143 88.212.201.198:80 TIME_WAIT 0
TCP 10.0.2.15:54311 213.180.193.24:443 TIME_WAIT 0
TCP 10.0.2.15:54571 31.172.81.172:443 TIME_WAIT 0
TCP 10.0.2.15:54644 213.180.193.24:443 TIME_WAIT 0
TCP 10.0.2.15:54892 213.180.193.24:443 TIME_WAIT 0
TCP 10.0.2.15:55376 74.125.131.157:443 TIME_WAIT 0
TCP 10.0.2.15:55451 74.125.131.132:443 TIME_WAIT 0
TCP 10.0.2.15:55783 31.172.81.172:443 TIME_WAIT 0
TCP 10.0.2.15:56286 74.125.205.196:443 TIME_WAIT 0
TCP 10.0.2.15:56316 45.133.44.4:443 TIME_WAIT 0
TCP 10.0.2.15:56510 74.125.205.196:443 TIME_WAIT 0
TCP 10.0.2.15:56894 178.208.83.25:80 TIME_WAIT 0
TCP 10.0.2.15:57201 64.233.165.148:443 TIME_WAIT 0
TCP 10.0.2.15:57276 64.233.165.155:443 TIME_WAIT 0
TCP 10.0.2.15:57465 173.194.222.94:80 TIME_WAIT 0
TCP 10.0.2.15:57947 178.208.83.25:80 TIME_WAIT 0
TCP 10.0.2.15:57987 31.172.81.158:443 TIME_WAIT 0
TCP 10.0.2.15:58044 77.88.55.55:443 ESTABLISHED 3068
TCP 10.0.2.15:58249 173.194.222.94:80 TIME_WAIT 0
TCP 10.0.2.15:58853 209.85.233.106:443 TIME_WAIT 0
TCP 10.0.2.15:59038 31.172.81.159:443 TIME_WAIT 0
TCP 10.0.2.15:59261 64.233.165.94:443 TIME_WAIT 0
TCP 10.0.2.15:59583 45.133.44.4:443 TIME_WAIT 0
TCP 10.0.2.15:59792 213.180.193.24:443 TIME_WAIT 0

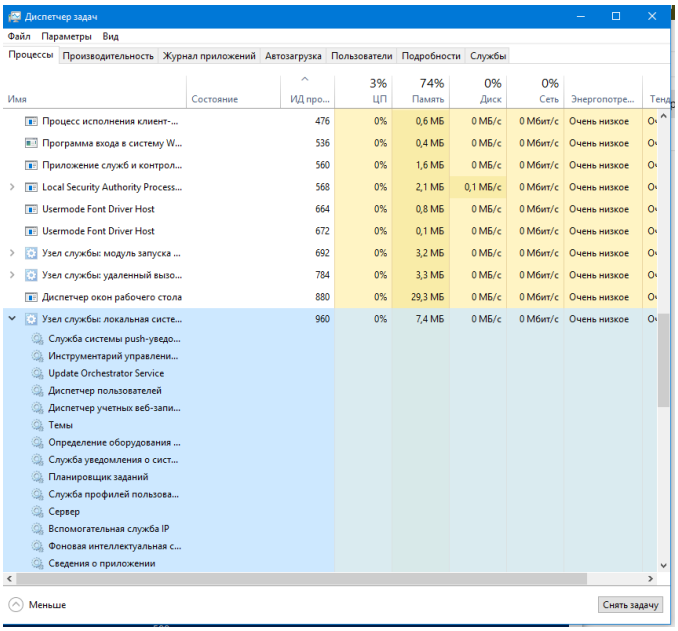
Выбрать Администратор: Windows PowerShell

```
  TCP    10.0.2.15:63770        45.133.44.3:443        TIME_WAIT       0
  TCP    10.0.2.15:64159        195.208.38.26:80       TIME_WAIT       0
  TCP    10.0.2.15:64404        142.251.1.132:443      TIME_WAIT       0
  TCP    10.0.2.15:65178        31.172.81.159:443      TIME_WAIT       0
  TCP    10.0.2.15:65224        87.250.251.42:443      TIME_WAIT       0
  TCP    10.0.2.15:65256        213.180.193.24:443     ESTABLISHED     3068
  TCP    10.0.2.15:65335        178.208.83.25:80       TIME_WAIT       0
  TCP    [::]:135               [::]:0                 LISTENING       784
  TCP    [::]:445               [::]:0                 LISTENING       4
  TCP    [::]:49664             [::]:0                 LISTENING       468
  TCP    [::]:49665             [::]:0                 LISTENING       960
  TCP    [::]:49666             [::]:0                 LISTENING       300
  TCP    [::]:49667             [::]:0                 LISTENING       1644
  TCP    [::]:49668             [::]:0                 LISTENING       560
  TCP    [::]:49669             [::]:0                 LISTENING       568
  UDP    0.0.0.0:5050           *:*                                    1088
  UDP    0.0.0.0:5353           *:*                                    3804
  UDP    0.0.0.0:5353           *:*                                    500
  UDP    0.0.0.0:5353           *:*                                    500
  UDP    0.0.0.0:5353           *:*                                    3804
  UDP    0.0.0.0:5353           *:*                                    1276
  UDP    0.0.0.0:5355           *:*                                    1276
  UDP    0.0.0.0:49280          *:*                                    3068
  UDP    0.0.0.0:56470          *:*                                    3068
  UDP    0.0.0.0:57114          *:*                                    3068
  UDP    0.0.0.0:57575          *:*                                    3068
  UDP    0.0.0.0:57638          *:*                                    3068
  UDP    0.0.0.0:59467          *:*                                    3068
  UDP    0.0.0.0:62972          *:*                                    3068
  UDP    10.0.2.15:137          *:*                                    4
  UDP    10.0.2.15:138          *:*                                    4
  UDP    10.0.2.15:1900         *:*                                    5096
  UDP    10.0.2.15:56170        *:*                                    5096
  UDP    127.0.0.1:1900         *:*                                    5096
  UDP    127.0.0.1:55609        *:*                                    960
  UDP    127.0.0.1:56171        *:*                                    5096
  UDP    [::]:5353              *:*                                    1276
  UDP    [::]:5353              *:*                                    500
  UDP    [::]:5353              *:*                                    3804
  UDP    [::]:5355              *:*                                    1276
  UDP    [::1]:1900             *:*                                    5096
  UDP    [::1]:56169            *:*                                    5096
  UDP    [fe80::e580:c036:3a30:34d2%15]:1900  *:*                                    5096
  UDP    [fe80::e580:c036:3a30:34d2%15]:56168  *:*                                    5096
PS C:\Windows\system32>
```




Диспетчер задач
Файл Параметры Вид
Процессы Производительность Журнал приложений Автозагрузка Пользователи Подробности Службы
Имя Состояние ИД про... 21% ЦП 77% Память 1% Диск 0% Сеть Энергопотре... Тенд
Системные прерывания 0% 0 МБ 0 МБ/с 0 Мбит/с Очень низкое
Параметры 0% 0 МБ 0 МБ/с 0 Мбит/с Очень низкое
Microsoft Text Input Application 0% 0 МБ 0 МБ/с 0 Мбит/с Очень низкое
Экран блокировки Windows п... 0% 0 МБ 0 МБ/с 0 Мбит/с Очень низкое
Хост Windows Shell Experience 0% 0 МБ 0 МБ/с 0 Мбит/с Очень низкое
Поиск (2) 0% 1,7 МБ 0 МБ/с 0 Мбит/с Очень низкое
Google Chrome (13) 0% 197,1 МБ 0,1 МБ/с 0 Мбит/с Очень низкое
Yandex (32 бита) (17) 13,5% 316,1 МБ 0 МБ/с 0 Мбит/с Низкий
Yandex (32 бита) 580 0% 26,0 МБ 0 МБ/с 0 Мбит/с Очень низкое
Yandex (32 бита) 592 1,8% 6,0 МБ 0 МБ/с 0 Мбит/с Очень низкое
Yandex (32 бита) 972 0% 1,6 МБ 0 МБ/с 0 Мбит/с Очень низкое
Yandex (32 бита) 2396 0% 6,7 МБ 0 МБ/с 0 Мбит/с Очень низкое
Yandex (32 бита) 2484 0% 4,0 МБ 0 МБ/с 0 Мбит/с Очень низкое
Yandex (32 бита) 3020 0% 71,9 МБ 0 МБ/с 0 Мбит/с Очень низкое
Yandex (32 бита) 3068 0,9% 12,0 МБ 0 МБ/с 0 Мбит/с Очень низкое
Yandex (32 бита) 3656 0% 1,7 МБ 0 МБ/с 0 Мбит/с Очень низкое
Yandex (32 бита) 4744 0% 3,0 МБ 0 МБ/с 0 Мбит/с Очень низкое
Netstat — Википедия — Янде... 4796 2,4% 53,4 МБ 0 МБ/с 0 Мбит/с Очень низкое
Yandex (32 бита) 4836 0% 0,9 МБ 0 МБ/с 0 Мбит/с Очень низкое
Yandex (32 бита) 4980 0% 1,1 МБ 0 МБ/с 0 Мбит/с Очень низкое
Yandex (32 бита) 5072 0% 2,5 МБ 0 МБ/с 0 Мбит/с Очень низкое
Yandex (32 бита) 5264 0,6% 31,5 МБ 0 МБ/с 0 Мбит/с Очень низкое
Yandex (32 бита) 6364 7,8% 53,6 МБ 0 МБ/с 0 Мбит/с Очень низкое
Yandex (32 бита) 7024 0% 22,0 МБ 0 МБ/с 0 Мбит/с Очень низкое
Yandex (32 бита) 8012 0% 18,5 МБ 0 МБ/с 0 Мбит/с Очень низкое
Меньше
Снять задачу


Администратор: Windows PowerShell
Статистика TCP для IPv6
Активных открыто = 3
Пассивных открыто = 0
Сбоев при подключении = 3
Сброшено подключений = 0
Текущих подключений = 0
Получено сегментов = 10
Отправлено сегментов = 12
Повторно отправлено сегментов = 6
Статистика UDP для IPv4
Получено датаграмм = 168675
Отсутствие портов = 1189
Ошибки при получении = 0
Отправлено датаграмм = 80778
Статистика UDP для IPv6
Получено датаграмм = 146
Отсутствие портов = 37
Ошибки при получении = 0
Отправлено датаграмм = 112
PS C:\Windows\system32> netstat -f
Активные подключения
Имя Локальный адрес Внешний адрес Состояние
TCP 10.0.2.15:52365 xiva-daria.stable.qloud-b.yandex.net:https
TCP 10.0.2.15:52519 passport.yandex-team.ru:https TIME_WAIT
TCP 10.0.2.15:53191 passport.yandex-team.ru:https TIME_WAIT
TCP 10.0.2.15:54053 passport.yandex-team.ru:https TIME_WAIT
TCP 10.0.2.15:54160 li-in-f188.1e100.net:5228 ESTABLISHED
TCP 10.0.2.15:54161 lo-in-f188.1e100.net:5228 ESTABLISHED
TCP 10.0.2.15:57251 20.54.37.64:https ESTABLISHED
TCP 10.0.2.15:60493 passport.yandex-team.ru:https TIME_WAIT
TCP 10.0.2.15:61188 passport.yandex-team.ru:https TIME_WAIT
TCP 10.0.2.15:62228 passport.yandex-team.ru:https TIME_WAIT
TCP 10.0.2.15:63328 passport.yandex-team.ru:https TIME_WAIT
TCP 10.0.2.15:64883 passport.yandex-team.ru:https TIME_WAIT
PS C:\Windows\system32> netstat -o
Активные подключения
Имя Локальный адрес Внешний адрес Состояние PID
TCP 10.0.2.15:52365 xiva-daria:https ESTABLISHED 3068
TCP 10.0.2.15:52519 passport:https TIME_WAIT 0
TCP 10.0.2.15:53191 passport:https TIME_WAIT 0
TCP 10.0.2.15:54053 passport:https TIME_WAIT 0
TCP 10.0.2.15:54160 li-in-f188:5228 ESTABLISHED 3068
TCP 10.0.2.15:54161 lo-in-f188:5228 ESTABLISHED 500
TCP 10.0.2.15:54336 passport:https ESTABLISHED 3068
TCP 10.0.2.15:57251 20.54.37.64:https ESTABLISHED 960
TCP 10.0.2.15:60493 passport:https TIME_WAIT 0
TCP 10.0.2.15:61188 passport:https TIME_WAIT 0
TCP 10.0.2.15:62228 passport:https TIME_WAIT 0
TCP 10.0.2.15:63328 passport:https TIME_WAIT 0
TCP 10.0.2.15:64883 passport:https TIME_WAIT 0
PS C:\Windows\system32>
Диспетчер задач
Файл Параметры Вид
Процессы Производительность Журнал приложений Автозагрузка Пользователи Подробности Службы
Имя Состояние ИД про... 5% ЦП 75% Память 0% Диск 0% Сеть Энергопотре...
Google Chrome (13) 0% 130,6 МБ 0 МБ/с 0 Мбит/с Очень низкое
Google Chrome 7460 0% 21,3 МБ 0 МБ/с 0 Мбит/с Очень низкое
Google Chrome 6840 0% 16,4 МБ 0 МБ/с 0 Мбит/с Очень низкое
Google Chrome 5244 0% 1,1 МБ 0 МБ/с 0 Мбит/с Очень низкое
Google Chrome 4192 0% 13,3 МБ 0 МБ/с 0 Мбит/с Очень низкое
Google Chrome 4184 0% 16,3 МБ 0 МБ/с 0 Мбит/с Очень низкое
Google Chrome 4176 0% 6,6 МБ 0 МБ/с 0 Мбит/с Очень низкое
Google Chrome 4168 0% 10,5 МБ 0 МБ/с 0 Мбит/с Очень низкое
Google Chrome 4112 0% 0,5 МБ 0 МБ/с 0 Мбит/с Очень низкое
Google Chrome 3976 0% 0,6 МБ 0 МБ/с 0 Мбит/с Очень низкое
Google Chrome 3804 0% 26,1 МБ 0 МБ/с 0 Мбит/с Очень низкое
Google Chrome 3224 0% 9,8 МБ 0 МБ/с 0 Мбит/с Очень низкое
Google Chrome 2980 0% 2,9 МБ 0 МБ/с 0 Мбит/с Очень низкое
Google Chrome 500 0% 5,0 МБ 0 МБ/с 0 Мбит/с Очень низкое
Microsoft Text Input Application 0% 0 МБ 0 МБ/с 0 Мбит/с Очень низкое
WindowsInternal.Composable... Приостановл... 5816 0% 0 МБ 0 МБ/с 0 Мбит/с Очень низкое
Windows PowerShell (2) 0% 39,4 МБ 0 МБ/с 0 Мбит/с Очень низкое
Хост окна консоли 8072 0% 3,5 МБ 0 МБ/с 0 Мбит/с Очень низкое
Windows PowerShell 8064 0% 35,9 МБ 0 МБ/с 0 Мбит/с Очень низкое
Параметры 0% 0 МБ 0 МБ/с 0 Мбит/с Очень низкое
Параметры Приостановл... 3160 0% 0 МБ 0 МБ/с 0 Мбит/с Очень низкое
Поиск (2) 0% 1,7 МБ 0 МБ/с 0 Мбит/с Очень низкое
Runtime Broker 3172 0% 1,7 МБ 0 МБ/с 0 Мбит/с Очень низкое
Поиск Приостановл... 3084 0% 0 МБ 0 МБ/с 0 Мбит/с Очень низкое
Runtime Broker 0% 1,1 МБ 0 МБ/с 0 Мбит/с Очень низкое
Меньше
Снять задачу


Диспетчер задач
Файл Параметры Вид
Процессы Производительность Журнал приложений Автозагрузка Пользователи Подробности Службы
Имя Состояние ИД про... 3% ЦП 74% Память 0% Диск 0% Сеть Энергопотре... Тенд
Процесс исполнения клиент-... 476 0% 0,6 МБ 0 МБ/с 0 Мбит/с Очень низкое
Программа входа в систему W... 536 0% 0,4 МБ 0 МБ/с 0 Мбит/с Очень низкое
Приложение служб и контрол... 560 0% 1,6 МБ 0 МБ/с 0 Мбит/с Очень низкое
Local Security Authority Process... 568 0% 2,1 МБ 0,1 МБ/с 0 Мбит/с Очень низкое
Usermode Font Driver Host 664 0% 0,8 МБ 0 МБ/с 0 Мбит/с Очень низкое
Usermode Font Driver Host 672 0% 0,1 МБ 0 МБ/с 0 Мбит/с Очень низкое
Узел службы: модуль запуска ... 692 0% 3,2 МБ 0 МБ/с 0 Мбит/с Очень низкое
Узел службы: удаленный выз... 784 0% 3,3 МБ 0 МБ/с 0 Мбит/с Очень низкое
Диспетчер окон рабочего стола 880 0% 29,3 МБ 0 МБ/с 0 Мбит/с Очень низкое
Узел службы: локальная систе... 960 0% 7,4 МБ 0 МБ/с 0 Мбит/с Очень низкое
Служба системы push-уведо...
Инструментарий управлени...
Update Orchestrator Service
Диспетчер пользователей
Диспетчер учетных веб-запи...
Темы
Определение оборудования ...
Служба уведомления о сист...
Планировщик заданий
Служба профилей пользова...
Сервер
Вспомогательная служба IP
Фоновая интеллектуальная с...
Сведения о приложении
Меньше
Снять задачу

1) TCP 10.0.2.15:49194 31.172.81.159:443 TIME_WAIT 0
   Сокет - 31.172.81.159:443 (https:\\)
   Протокол TCP состояние TIME_WAIT - Сокет закрыт, но ожидает пакеты, ещё находящиеся в сети для обработки
   Приложение 0 – бездействие (это мы определили по PID в диспетчере задач)
2) TCP 0.0.0.0:445 0.0.0.0:0 LISTENING 4
   Сокет - 0.0.0.0:0
   Протокол TCP состояние LISTENING - Ожидает входящих соединений.
   Приложение 4 – System (ntoskrnl.exe - файл ядра операционных систем семейства Windows NT (NT 3.1-3.5, NT 3.51, NT 4.0, 2000, XP, 2003, Vista, 2008, 7, 2008 R2, 8, 2012, 10). Данный файл запускается загрузчиком ядра NTLDR(сокращение от англ. NT Loader) в безопасном режиме. Ядро Windows NT имеет исходные тексты различных сообщений, текст синего экрана смерти и прочую информацию, которую можно увидеть с помощью HEX-редактора.)
3) TCP 10.0.2.15:52365 213.180.204.179:443 ESTABLISHED 3068
   Сокет 213.180.204.179:443 (https:\\)
   Протокол TCP состояние ESTABLISHED - Соединение установлено.
   Приложение 3068 – Яндекс браузер (программа, предназначенная для просмотра сайтов)
4) TCP 10.0.2.15:52797 64.233.161.188:5228 ESTABLISHED 3068
   Сокет 64.233.161.188:5228 Приложение Android для подключения GCM к Интернету 5228 (TCP), 5229 (TCP), 5230 (TCP)
   Протокол TCP состояние ESTABLISHED - Соединение установлено.
   Приложение 3068 – Яндекс браузер (программа, предназначенная для просмотра сайтов)
5) TCP 10.0.2.15:52895 88.212.201.198:80 TIME_WAIT 0
   Сокет - 88.212.201.198:80 (http:\\)
   Протокол TCP состояние TIME_WAIT - Сокет закрыт, но ожидает пакеты, ещё находящиеся в сети для обработки
   Приложение 0 – бездействие (это мы определили по PID в диспетчере задач)
6) UDP 0.0.0.0:5353 *:* 3804
   Сокет *:*
   Протокол UDP состояние не изветсно
   Приложение 3804 – Chrome браузер (программа, предназначенная для просмотра сайтов)
7) TCP 10.0.2.15:52798 74.125.131.188:5228 ESTABLISHED 500
   Сокет 74.125.131.188:5228 Приложение Android для подключения GCM к Интернету 5228 (TCP), 5229 (TCP), 5230 (TCP)
   Протокол TCP состояние ESTABLISHED - Соединение установлено.
   Приложение 500 – Chrome браузер (программа, предназначенная для просмотра сайтов)
8) TCP 10.0.2.15:63636 20.54.37.64:443 ESTABLISHED 960
   Сокет 20.54.37.64:443 (https:\\)
   Протокол TCP состояние ESTABLISHED - Соединение установлено.
   Приложение 960 – svchost.exe в семействе операционных систем Microsoft Windows (2000, XP, Vista, Seven, Windows 8, Windows 10) — главный процесс (англ. Host process) для служб, загружаемых из динамических библиотек. Использование единого процесса для работы нескольких сервисов позволяет существенно уменьшить затраты оперативной памяти и процессорного времени.
9) TCP [::]:135 [::]:0 LISTENING 784
   Сокет [::]:0
   Протокол TCP состояние LISTENING - Ожидает входящих соединений.
   Приложение 784 - svchost.exe в семействе операционных систем Microsoft Windows (2000, XP, Vista, Seven, Windows 8, Windows 10) — главный процесс (англ. Host process) для служб, загружаемых из динамических библиотек. Использование единого процесса для работы нескольких сервисов позволяет существенно уменьшить затраты оперативной памяти и процессорного времени.

10) TCP 10.0.2.15:58044 77.88.55.55:443 ESTABLISHED 3068

Сокет 77.88.55.55:443 (https:\\)

Протокол TCP состояние ESTABLISHED - Соединение установлено.

Приложение 3068 – Яндекс браузер (программа, предназначенная для просмотра сайтов)