

Сеть и сетевые протоколы: Траблшутинг



Александр
Гришин



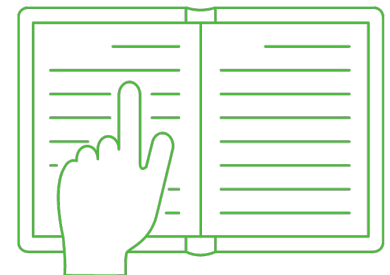
Александр Гришин

Инженер, компания YADRO

Предисловие

На этом занятии мы рассмотрим основные **инструменты анализа проблем в сетевом стеке**, в том числе на уровнях

- L2;
- L3;
- L4.



План занятия

1. [Предисловие](#)
2. [Troubleshooting](#)
3. [Физические проблемы](#)
4. [Проблемы с connectivity](#)
5. [Некорректная настройка \(L2, L3, L4\)](#)
6. [Некорректная работа ПО \(L5-L7\)](#)
7. [Загрузка канала](#)
8. [«Проблемы не на нашей стороне»](#)
9. [Итоги](#)
10. [Домашнее задание](#)



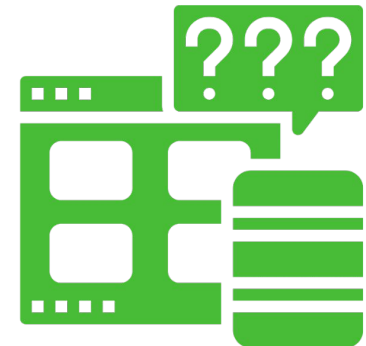
Troubleshooting

Определение

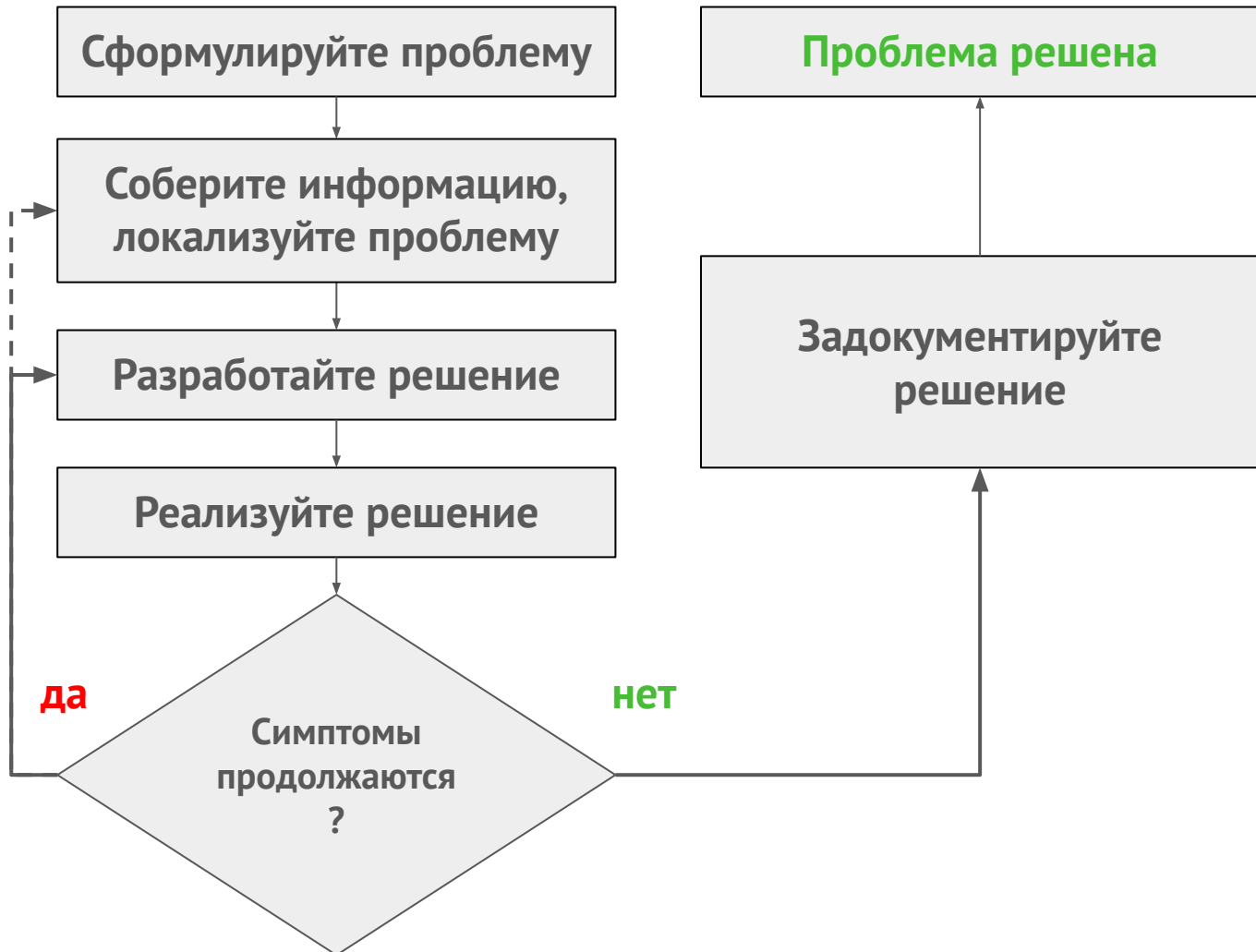
Troubleshooting (устранение неполадок, работа над проблемой) — форма решения проблем, часто применяемая к ремонту неработающих устройств или процессов.

Представляет собой **систематический**, опосредованный **определённой логикой поиск источника проблемы с целью её решения**.

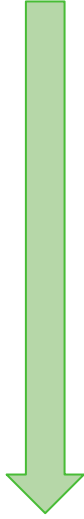
Траблшутинг как поиск и устранение неисправностей **необходим для поддержания и развития сложных систем**, где проблема может иметь множество различных причин.



Базовая логика



Основные проблемы в сетях

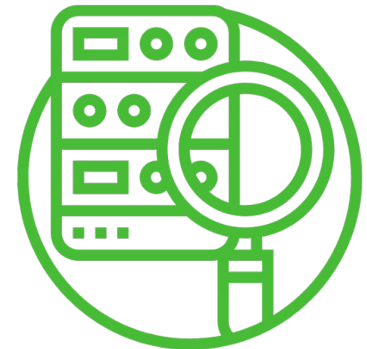
- 
- **физические** (L1) – кабель отключен или повреждён;
 - **connectivity** (L1, L2) – порт на оборудовании может быть не настроен, заблокирован или отключен;
 - **некорректная настройка** (L2, L3, L4) – некорректный IP-адрес, маршрут, шлюз, блокировка на стороне **firewall**'а, и т.д.;
 - **некорректная работа ПО** (L5-L7) – несоответствие версий ПО, выключенное ПО, неправильно настроенный порт, и т.д.;
-
- **загрузка канала** – попытка передать через канал большее количество информации, чем возможно;
 - **проблема на стороне провайдера**;
 - и многое-многое другое...

Л – логика. Л – локализация проблемы.

Если **один** клиент жалуется на отсутствие доступа к **разным** сервисам – скорее всего проблема только у него (компьютер, IP-адрес, сеть, ПО).

Если **много** клиентов жалуется на отсутствие доступа к **одному** сервису – скорее всего проблема в сервисе.

Если **много** клиентов жалуется на отсутствие доступа к **разным** сервисам – скорее всего или глобальные проблемы в локальной сети, или проблемы у провайдера.






Физические проблемы

Физические проблемы

Здесь всё достаточно просто – что бы ни случилось, для работы всего остального должна быть **связность на физическом уровне модели OSI (Layer 1)**.

 **Если не работает физическое подключение – не будет работать ничего!**

Вопросы, на которые нужно иметь положительный ответ:

- Есть ли электричество на оборудовании? Включена ли **VM**?
- Подключен ли кабель?
- Если подключен – уверены ли вы, что он целый?



Проблемы с connectivity

Проблемы с connectivity (L1, L2)

Здесь всё ещё достаточно просто, хотя немного сложнее – всё может быть подключено, но всё равно не работать. 🙄

Вопросы, на которые нужно иметь положительный ответ:

- Если кабель подключен и в порядке – горит ли лампочка (есть ли «линк»)?
- Не заблокирован ли порт в настройках коммутатора / сервера?
- Не заблокирован ли [MAC-адрес](#) на коммутаторе?

Команды поиска проблем на L1, L2

```
osboxes@osboxes:~$ ip link
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group
default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode
DEFAULT group default qlen 1000
    link/ether 08:00:27:f4:39:49 brd ff:ff:ff:ff:ff:ff
3: eth1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN mode
DEFAULT group default qlen 1000
    link/ether 08:00:27:f4:39:50 brd ff:ff:ff:ff:ff:ff
```

eth0 – **LOWER_UP** – физический (аппаратный) уровень сети (L1) также в состоянии UP.

UP/state UP – интерфейс работает / подключён.


Команды поиска проблем на L1, L2

```
osboxes@osboxes:~$ ip link
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode DEFAULT group
default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode
DEFAULT group default qlen 1000
    link/ether 08:00:27:f4:39:49 brd ff:ff:ff:ff:ff:ff
3: eth1: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN mode
DEFAULT group default qlen 1000
    link/ether 08:00:27:f4:39:50 brd ff:ff:ff:ff:ff:ff
```

eth1 – **NO-CARRIER** означает, что сетевой разъем не обнаруживает сигнал на линии.

➡ Обычно это происходит потому, что сетевой кабель отключён или повреждён. В редких случаях это также может быть аппаратный сбой или ошибка драйвера.

UP / state DOWN – интерфейс работает / не подключён (LOWER_UP отсутствует).



Некорректная настройка (L2, L3, L4)

Некорректная настройка (L2, L3, L4)

Здесь начинается самое интересное – проблема может быть много где – иногда локализовать проблему здесь сложнее всего.

Вопросы, на которые нужно иметь положительный ответ:

- Есть ли связь на L2?
Видю ли я компьютеры внутри локальной сети
- Есть ли связь на L3?
- Много что работает, не работает связь именно с этим IP-адресом.
Тестируем с помощью arp, ping, trace.
- ...

Некорректная настройка (L2, L3, L4)

Вопросы, на которые нужно иметь положительный ответ:

- ...

- Есть ли связь на L4?

Хост доступен, однако не работает конкретный сервис. Тестируем с помощью `telnet` со стороны клиента, `ss` / `netstat` со стороны сервера, просматриваем правила `firewall`'а

Команды поиска проблем на L2 (arp, arping)

Просмотр arp (связь L2 и L3)

```
# ip neigh show dev eth1
192.168.11.12 lladdr 08:00:27:23:22:97 REACHABLE

# arp -i eth1
Address HWtype HWaddress Flags Mask Iface
192.168.11.100 ether 00:00:00:00:00:aa CM eth1
```

Опрос устройства на L2

```
$ sudo arping -c 1 10.0.2.3
60 bytes from 52:54:00:12:35:03 (10.0.2.3): index=0 time=7.346 usec
--- 10.0.2.3 statistics ---
1 packets transmitted, 1 packets received, 0% unanswered (0 extra)
rtt min/avg/max/std-dev = 0.007/0.007/0.007/0.000 ms
```

Команды поиска проблем на L2 (tcpdump)

Просмотр трафика L2

```
# sudo tcpdump -i any arp -nn -A -e
```

- С опцией `-e` программа `tcpdump` будет печатать заголовки канального уровня в каждой выведенной строке.
- ➔ Это может использоваться, например, для показа аппаратных адресов `MAC` для таких протоколов как `Ethernet` и `IEEE 802.11`.
- С опцией `-A` команда `tcpdump` будет отображать на экране содержимое пакетов в формате `ASCII`.
- Опция `-nn` отображает порты и `IP`-адреса цифрами вместо имён (localhost, ssh, http, и т.д.)

Команды поиска проблем L3 (ip addr, route)

Проверка корректности настройки своего устройства

```
osboxes@osboxes:~$ ip -4 address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    inet 192.168.12.15/24 brd 192.168.12.255 scope global dynamic noprefixroute eth0
        valid_lft 86328sec preferred_lft 86328sec

# ip route list
192.168.12.0/24 dev eth0  proto kernel  scope link  src 192.168.12.15
default via 192.168.12.1 dev eth0
```

Команды поиска проблем на L3 (ping, trace)

Опрос хоста на L3 – ping (ICMP echo request + ICMP echo reply)

```
osboxes@osboxes:~$ ping -c 1 netology.ru
PING netology.ru (104.26.8.143) 56(84) bytes of data.
64 bytes from 104.26.8.143 (104.26.8.143): icmp_seq=1 ttl=63 time=3.88 ms
--- netology.ru ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 3.877/3.877/3.877/0.000 ms
```

Проверка маршрута до хоста L3 – trace

```
# traceroute -n ya.ru
traceroute to ya.ru (87.250.250.242), 30 hops max, 60 byte packets
 1  172.11.111.1  8.044 ms  7.967 ms  8.020 ms
 2  195.201.66.111  0.122 ms  0.091 ms  0.066 ms
 3  * * *
 4  85.10.243.237  0.734 ms  1.083 ms  1.028 ms
 5  85.10.228.85  0.384 ms  85.10.250.213  0.353 ms  0.318 ms
 6  213.239.252.21  3.470 ms  213.239.245.33  7.857 ms  7.821 ms
 7  * 213.239.245.126  3.991 ms *
 8  5.45.200.40  4.415 ms  4.314 ms  3.868 ms
 9  * * *
10  87.250.250.242  28.153 ms  28.110 ms  28.083 ms
```

Команды поиска проблем на L3 (ping, trace)

Ломаем сеть – добавляем некорректный маршрут

```
# ip r add 8.8.4.4/32 dev eth0
```

Неудачный опрос хоста на L3

```
# ping -c1 8.8.4.4
PING 8.8.4.4 (8.8.4.4) 56(84) bytes of data.
From 157.90.168.222 icmp_seq=1 Destination Host Unreachable
--- 8.8.4.4 ping statistics ---
1 packets transmitted, 0 received, +1 errors, 100% packet loss, time 0ms
```

Неудачный trace

```
# traceroute -n 8.8.4.4
traceroute to 8.8.4.4 (8.8.4.4), 30 hops max, 60 byte packets
 1  157.90.168.111  3077.514 ms !H  3077.483 ms !H  3077.480 ms !H
```

Команды поиска проблем на L3 (IP route)

Поиск проблемы с маршрутизацией

```
# ip route list
default via 172.31.1.1 dev eth0 proto dhcp src 157.90.168.111 metric 100
8.8.4.4 dev eth0 scope link
172.31.1.1 dev eth0 proto dhcp scope link src 157.90.168.111 metric 100
```

Устраняем проблему с маршрутизацией

```
# ip r del 8.8.4.4/32 dev eth0

# ip route list
default via 172.31.111.1 dev eth0 proto dhcp src 157.90.168.111 metric 100
172.31.111.1 dev eth0 proto dhcp scope link src 157.90.168.111 metric 100
```

Очень важно, чтобы на хосте был маршрут до конечной точки, либо маршрут по-умолчанию + маршрут до конечной точки на роутере.

Команды поиска проблем с DNS

Ломаем DNS – добавляем некорректный DNS

```
# nameserver 8.8.8.7 -> /etc/resolv.conf
```

Неудачный опрос хоста

```
root@vagrant:~# ping ya.ru  
ping: ya.ru: Temporary failure in name resolution
```

Расследуем проблему

```
# cat /etc/resolv.conf  
nameserver 8.8.8.7
```

С настройкой DNS в ОС Linux можно детальнее ознакомиться по ссылкам: [1](#) и [2](#).

Команды поиска проблем на L4/L7 (telnet)

Поиск проблемы на L4 (проблемы нет)

```
$ telnet ya.ru 80
Trying 87.250.250.242...
Connected to ya.ru.
Escape character is '^]'.
```

Поиск проблемы на L4 (проблема есть)

```
$ telnet ya.ru 81
Trying 87.250.250.242...
```

```
telnet: Unable to connect to remote host: Network is unreachable
```

Команды поиска проблем на L4/L7 (curl)

Поиск проблемы на L4 (проблемы нет)

```
* Rebuilt URL to: http://ya.ru/
* Trying 87.250.250.242...
* TCP_NODELAY set
* Connected to ya.ru (87.250.250.242) port 80 (#0)
> GET / HTTP/1.1
> Host: ya.ru
> User-Agent: curl/7.58.0
> Accept: */*
< Content-Length: 0
< Date: Sun, 14 Mar 2021 23:19:39 GMT
< Expires: Sun, 14 Mar 2021 23:19:40 GMT
< Last-Modified: Sun, 14 Mar 2021 23:19:40 GMT
< Location: https://ya.ru/
<
* Connection #0 to host ya.ru left intact
```

Поиск проблемы на L4 (проблема есть)

```
vah@VAH-ZEN:~$ curl -v http://ya.ru:81
* Rebuilt URL to: http://ya.ru:81/
* Trying 87.250.250.242...
* TCP_NODELAY set
* Trying 2a02:6b8::2:242...
* TCP_NODELAY set
* connect to 2a02:6b8::2:242 port 81 failed: Connection refused
```

Некорректная настройка (L4)

Если нет связи по нужному нам порту, при том что хост доступен, пытаемся подключиться ещё куда-то **по тому же порту** (TCP / UDP), чтобы понять, не блокируется ли подключение нашим сетевым администратором на пограничном роутере.

Также просматриваем правила нашего **firewall**'а.

```
[root@localhost ~]# sudo iptables -L -v
Chain INPUT (policy ACCEPT 31 packets, 3913 bytes)
  pkts bytes target    prot opt in     out     source         destination
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
  pkts bytes target    prot opt in     out     source         destination
Chain OUTPUT (policy ACCEPT 28 packets, 4640 bytes)
  pkts bytes target    prot opt in     out     source         destination
[root@localhost ~]#
```

Как tcpdump поможет при проблемах?

В зависимости от того что покажет `tcpdump` на разных хостах, мы сможем делать дальнейшие выводы о локализации проблемы:


```
root@netology1:~# tcpdump -nn -i eth1
10:34:38.393610 IP 172.28.128.10.50700 > 172.28.128.60.80: Flags [S]...
10:34:39.423744 IP 172.28.128.10.50700 > 172.28.128.60.80: Flags [S]...

root@netology2:~# tcpdump -nn -i eth1 # (вариант 1)
10:34:37.621593 IP 172.28.128.10.50700 > 172.28.128.60.80: Flags [S]...
10:34:38.652240 IP 172.28.128.10.50700 > 172.28.128.60.80: Flags [S]...

root@netology2:~# tcpdump -nn -i eth1 # (вариант 2)
...
```

Вариант 1 говорит о том, что **TCP** сегменты на хост `netology2` приходят, но не генерируются ответные.

Вариант 2 говорит о том, что сегменты до хоста `netology2` не доходят.



Некорректная работа ПО (L5-L7)

Некорректная работа ПО (L5-L7)

Здесь многое аналогично L4, т.к. если диагностировать проблему выше 3-го уровня, то со стороны клиента это будет выглядеть как *«связь в принципе есть, однако ответ на мой запрос по порту 80 не приходит»*. И понять, в чём именно причина, не имея доступа к серверной части, иногда сложно.

Вопросы, на которые нужно иметь положительный ответ:

- Есть ли связь на L4 по тем же портам с другими хостами?
- Корректно ли работает ПО со стороны клиента?
- Корректно ли работает ПО со стороны сервера?

Есть ли связь на L4/L7 с другими хостами?

Если связь у клиента по тем же популярным портам (80, 443, 22, 23, и т. д.) с другими хостами есть, это означает, что с клиентской стороны **скорее всего** всё в порядке.

При этом без доступа к серверу понять причину будет невозможно, но попробовать можно.

Если речь идёт о подключении к высокодоступным сервисам (Yandex, Google, и т.д.) – проблема чаще на стороне пользователя или провайдера. Можно попробовать изменить внешний IP-адрес и проверить ещё раз.

Если нет доступа к серверу

Если связь у клиента по тем же популярным портам (80, 443, 22, 23, и т. д.) с другими хостами есть, это означает, что с клиентской стороны **скорее всего** всё в порядке.

При этом без доступа к серверу понять причину будет невозможно, но попробовать можно.

Если речь идёт о подключении к высокодоступным сервисам (Yandex, Google, и т.д.) – проблема чаще на стороне пользователя или провайдера. Можно попробовать изменить внешний IP-адрес и проверить ещё раз.

Если есть доступ к серверу

Необходимо проверить:

- запущена ли служба (`ps aux`);
- слушает ли она нужный порт (`ss, netstat`);
- какие ошибки есть в логах (`/var/log/*.log`, файл зависит от сервиса)



Если есть доступ к серверу (ps)

ps – утилита для сбора информации о запущенных процессах

```
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.8  77616  8604 ?        Ss   19:47   0:01 /sbin/init
root         2  0.0  0.0      0      0 ?        S    19:47   0:00 [kthreadd]
...
```

Если есть доступ к серверу (ss)

socket statistics – наиболее актуальная утилита для сбора информации о сокетах, в частности сетевых сокетах. Аналог **netstat**.

```
osboxes@osboxes:~$ ss -4 state listening state unconnected -n | column -t
Netid  State   Recv-Q  Send-Q  Local        Address:Port  Peer  Address:Port  Process
udp    UNCONN  0        0       127.0.0.53%lo:53  0.0.0.0:*
udp    UNCONN  0        0       0.0.0.0:5353    0.0.0.0:*
tcp    LISTEN  0        4096    127.0.0.53%lo:53  0.0.0.0:*
tcp    LISTEN  0        5       127.0.0.1:631    0.0.0.0:*
```

А так посмотрим установленные TCP соединения не на порт SSH:

```
osboxes@osboxes:~$ ss state connected sport != :ssh -t | column -t
State  Recv-Q  Send-Q  Local        Address:Port  Peer  Address:Port
Process
ESTAB  0        0       10.0.2.15:48668  104.26.8.143:http
```

Если есть доступ к серверу (lsof)

lsof – мощная утилита, в том числе для получения информации по сети.

Среди прочего он поможет вам узнать, какому процессу принадлежит прослушиваемый порт:

```
osboxes@osboxes:~$ sudo lsof -ni :22
COMMAND  PID    USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
sshd     722    root    3u   IPv4  21337      0t0  TCP *:ssh (LISTEN)
sshd     722    root    4u   IPv6  21348      0t0  TCP *:ssh (LISTEN)
sshd     778    root    4u   IPv4  22479      0t0  TCP 10.0.2.15:ssh->10.0.2.2:52115
(ESTABLISHED)
sshd    1179  osboxes  4u   IPv4  22479      0t0  TCP 10.0.2.15:ssh->10.0.2.2:52115
(ESTABLISHED)
sshd    1538    root    4u   IPv4  30466      0t0  TCP 10.0.2.15:ssh->10.0.2.2:52283
(ESTABLISHED)
sshd    1607  osboxes  4u   IPv4  30466      0t0  TCP 10.0.2.15:ssh->10.0.2.2:52283
(ESTABLISHED)
```

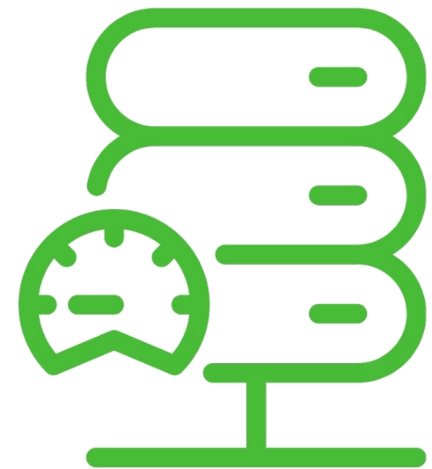


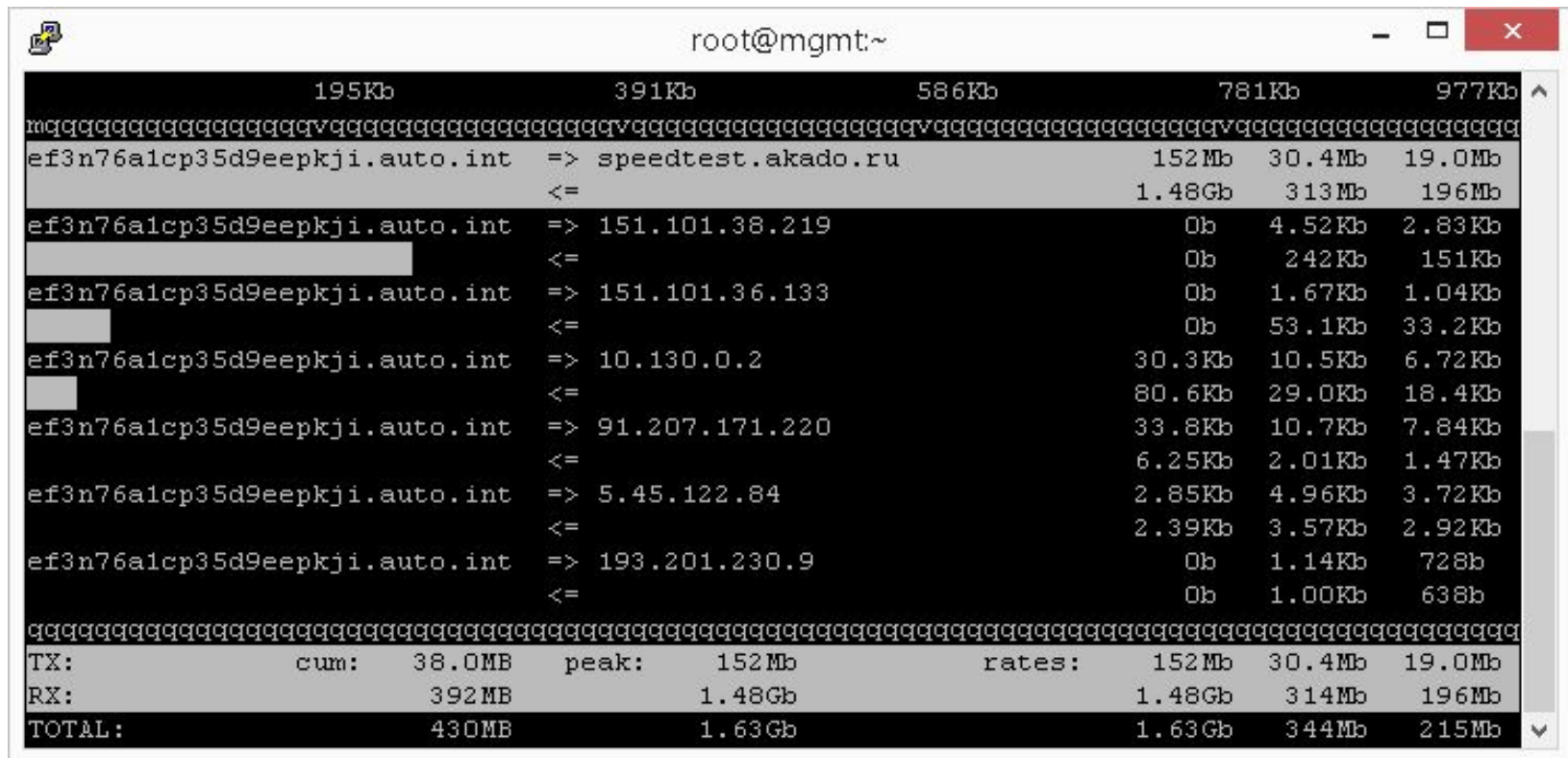
Загрузка канала

Загрузка канала

Если пинг от клиента к серверу стабильно высокий, плюс «тормозит» не только этот сервис – можем попробовать сделать вывод о том, что канал загружен.


Если же медленно работает только один сервис – проблема на стороне сервиса.





Загрузка канала (bmon)

```
root@mgmt:~  
lo bmon 3.6  
Interfaces      x RX bps      pps      %x TX bps      pps      %  
-lo             x      0      0      x      0      0  
  qdisc none (noqueue) x      0      0      x      0      0  
  eth0          x 603.85KiB   332      x   3.09MiB   221  
    qdisc none (mq)    x      0      0      x   3.22MiB  2.27K  
      class :1 (mq)    x      0      0      x   3.22MiB  2.27K  
    qdisc none (pfifo_fast)x      0      0      x   3.22MiB  2.27K  
B  
(RX Bytes/second)  
100.00 .....|.....  
83.33 .....|.....  
66.67 .....|.....  
50.00 .....|.....  
33.33 .....|.....  
16.67 .....|.....  
1  5  10  15  20  25  30  35  40  45  50  55  60  
B  
(TX Bytes/second)  
100.00 .....|.....  
83.33 .....|.....  
66.67 .....|.....  
50.00 .....|.....  
33.33 .....|.....  
16.67 .....|.....  
1  5  10  15  20  25  30  35  40  45  50  55  60  
Increase screen height to see detailed statistics  
MTU             65536 x Flags      loopback, up, running, lo  
Operstate       unknown x IfIndex      1  
Address         00:00:00:00:00:00 x Broadcast 00:00:00:00:00:00  
Mode            default x TXQlen      1000  
Family          unspec x Alias  
Qdisc           noqueue x
```



**«Проблема не на нашей
стороне»**

Проблема не на нашей стороне

Если **trace** показывает потери или сильное увеличение задержек на каком-то узле вне нашей зоны ответственности – мы ничего сделать не можем.

Если не можем подключиться только к конкретному серверу, к остальным **по тем же портам** подключаемся.

Рекомендации – попробовать подключение с другого оператора (с 4g роутера, резервного канала, и т.д.) + пообщаться с сетевым администратором и / или коллегами, может быть недавно вносили какие-то изменения в конфигурационные файлы.



Итоги

Итоги

Сегодня мы познакомились с базовыми алгоритмами и командами траблштинга в ОС Linux





Домашнее задание

Домашнее задание

Давайте посмотрим ваше [домашнее задание](#).

Настоятельно рекомендуем вам выполнять ДЗ в том же ритме, что и просмотр лекций.

- Вопросы по домашней работе задавайте **в чате** мессенджера .
- Задачи можно сдавать **по частям**.
- Зачёт по домашней работе проставляется после того, как **приняты все задачи**.

**Задавайте вопросы и
пишите отзыв о лекции!**

Александр Гришин