Федеральное государственное автономное образовательное учреждение высшего образования

«Национальный исследовательский университет ИТМО»

Факультет Информационных технологий и программирования

Работа: Лабораторная работа 3

Мониторинг сетевого трафика на хосте на примере работы с

утилитами диагностики и мониторинга сетевых соединений в Linux

Выполнил: Петровский Андрей M3302

Крючкова Александра М3302

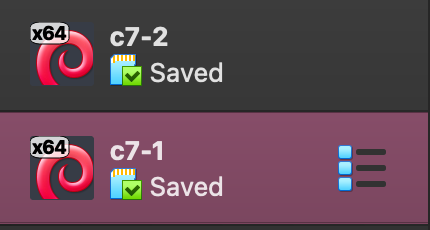
Миловацкий Никита M3302

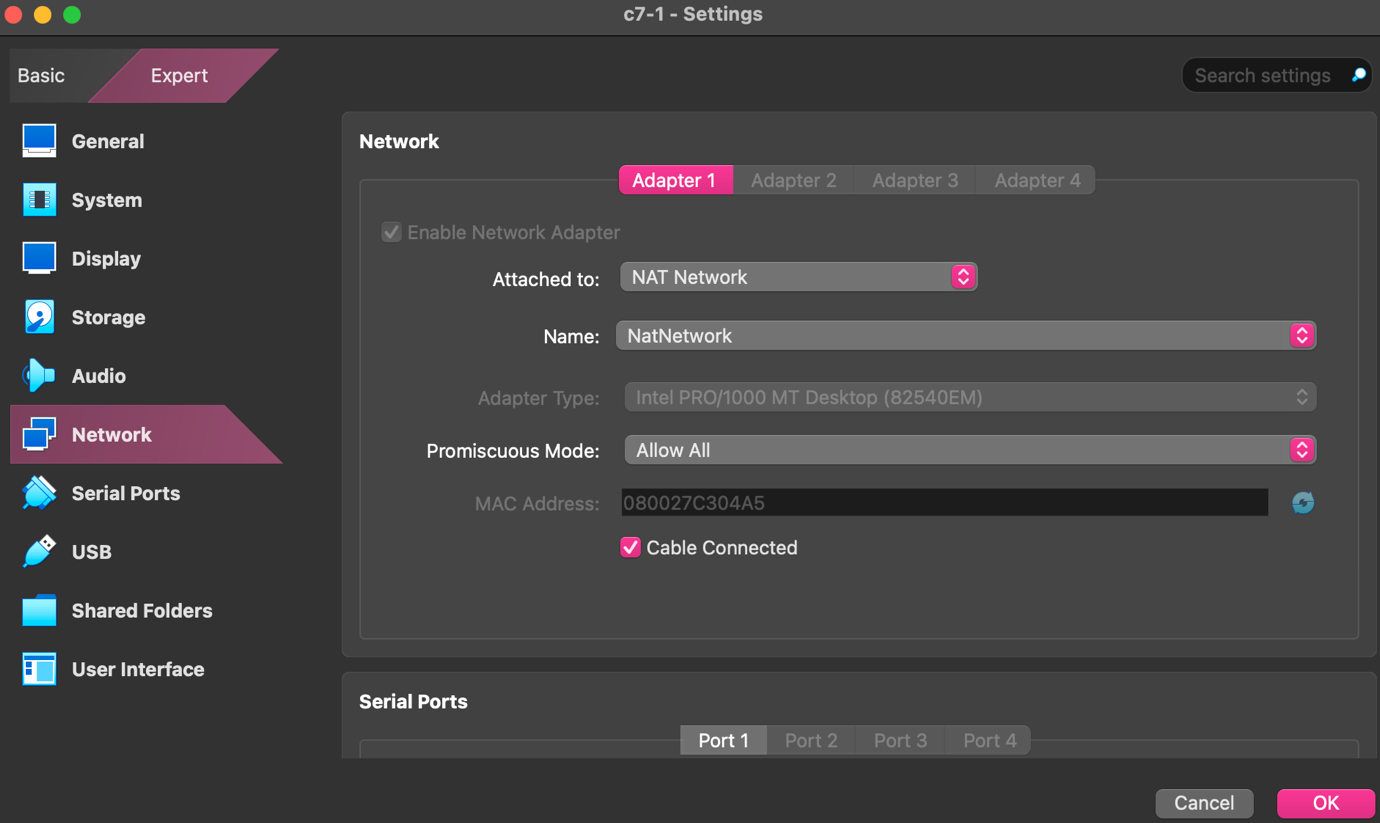
Санкт-Петербург

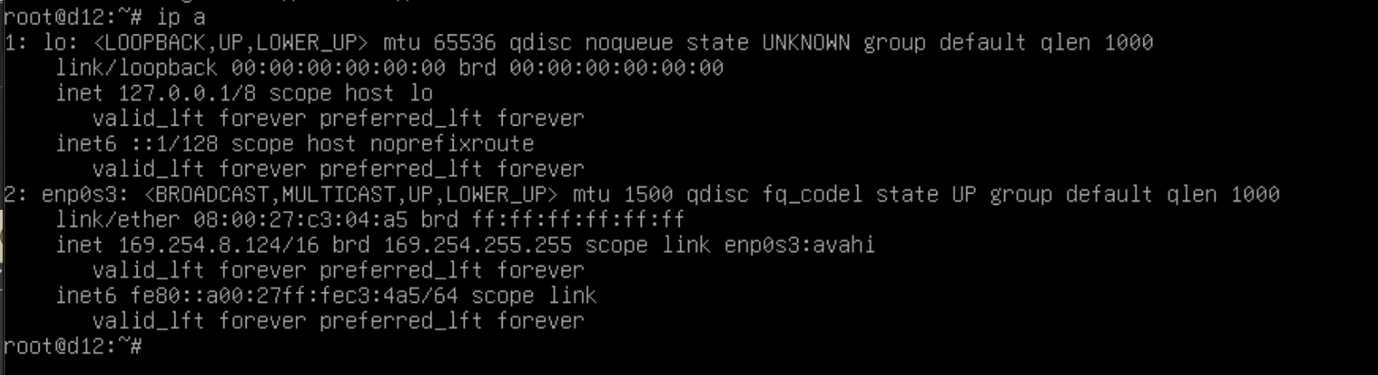
2024 г.

Часть 1. Настройка инфраструктуры

1. Подготовьте две виртуальные машины c ОС Linux. Одну машину назовите c7-1, другой с7-2



1. На обоих машинах сетевые интерфейсы настройте в режим Сеть NAT с включенным неразборчивым режимом, внутри машин получение адресов – автоматически с DHCP сервера VirtualBox.
2. Определите полученные адреса для машин с7-1 и c7-2



1. Установите на реальном хосте программу Wireshark (https://www.wireshark.org). Если вы используете WiFi при инсталляции npcap включите поддержку IEEE 802.11 .
2. На хосте c7-1 с помощью утилиты ping проверьте доступность внешней сети.
3. Проверьте на c7-1 наличие перечисленных утилит. В случае, если утилиты, упомянутые в работе отсутствуют на хосте, их следует установить. a. bmon (еще есть аналоги nload, iftop) b. nethogs c. mtr d. traceroute e. vnstat f. nc

Часть 2. Диагностика соединения

1. Познакомитесь с ключами утилиты ping.

2. На машине c7-2 напишите команду ping, которая (!) интервалом 10 секунд отправляет 5 пакетов размером 1500 байт на машину с7-1

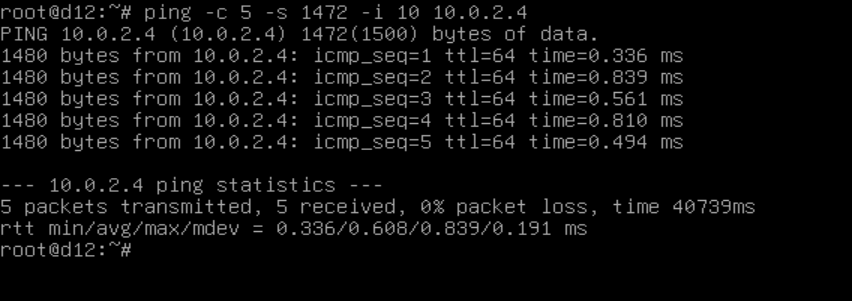
3. Выясните что означат использование ключа -f (используйте его только при использовании утилиты ping между хостами c7-1 и c7-2)

4. Познакомитесь с ключами утилиты mtr. С ее помощью с хоста c7-1 соберите статистику соединения с хостом [www.itmo.ru](http://www.itmo.ru).

5. Определите значение всех параметров, выводимых утилитой mtr.

6. Напишите команду, которая сохранит в файл расширенную статистику работы mtr при отправке 40 пакетов (!)

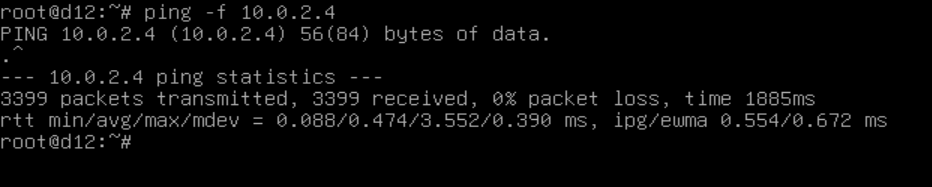
2.



3.

Ключ -f команды ping означает режим flood. При его использовании пакеты отправляются без задержек. Используется, например, для тестирования производительности сети

Пример использования:



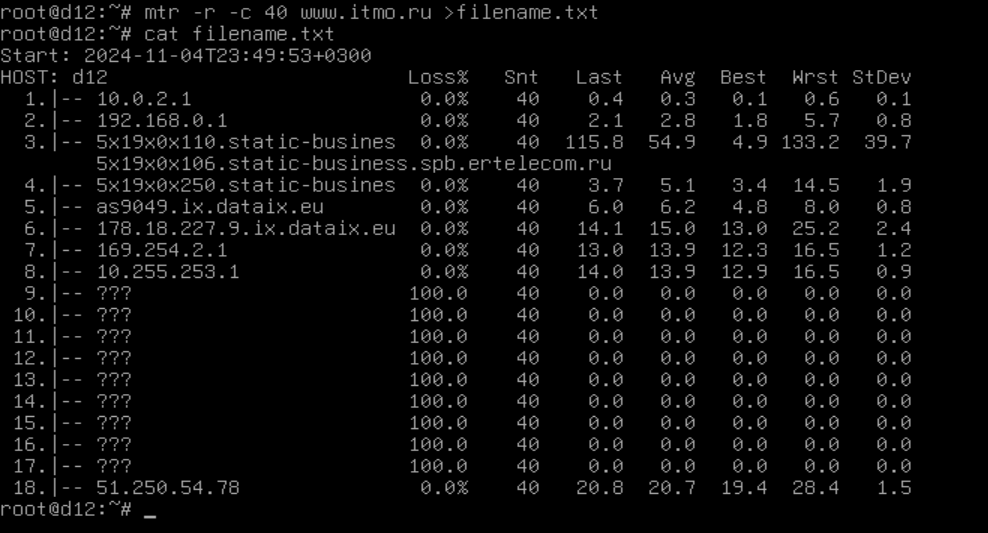
4.



5.

host - ip-адрес или название хоста, loss% - процент потерянных пакетов, snt - общее количество отправленных пакетов, avg - среднее арифметическое, best - лучшее, wrst - худшее, stdev - среднеквадратическое отклонение - времен задержки

6.



Часть 3. Работа с Wireshark

1. Настройте перехват трафика на реальном интерфейсе, так чтобы он завершился после сбора 5 Мб (для увеличения интенсивности генерации кадров открыть любой сайт в браузере).

2. Используя инструментарий статистики, определите (!): a. Узел с максимальной активностью (по объему переданных данных), b. Узел, осуществивший наибольшее количество широковещательных рассылок, c. Самый активный TCP-порт на хосте (по количеству переданных пакетов) d. Постройте на одной координатной сетке постройте графики интенсивности TCP и UDP трафика (пункт Io Graphs). e. Постройте диаграмму связей только для пакетов, содержащих сообщения протокола HTTPS (пункт Flow Graph)

3. Напишите фильтры, которые выделяют из общего числа пакеты (!): a. Отбирающие сообщения протокола DNS (53 порт udp и tcp) относящиеся только к взаимодействию DNS клиента на хосте и внешних серверов. То есть в случае, если на вашем компьютере будет запущен и DNS-сервер, фильтр должен отбирать только трафик от и к DNSклиенту, игнорируя трафик от и к DNS-сервера. Для генерации DNS запросов на виртуальной машине можно использовать утилиту dig (dig www.itmo.ru). b. Все кадры Ethernet, отправленные с сетевого интерфейса хоста. c. Напишите фильтр, отбирающий только широковещательные сообщения. Определите назначение 3-х широковещательных рассылок разных протоколов (или тех, которые удалось обнаружить).

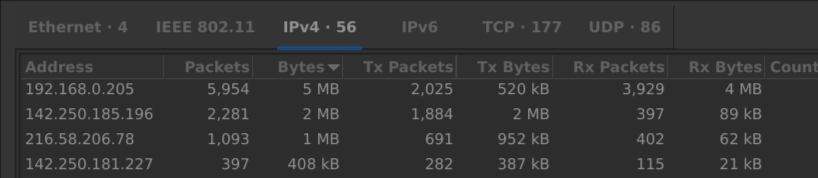
4. На основании анализа адресов отправителя и получателя в перехваченных пакетах, их вида и распределения, определите к какому типу коммутационного оборудования подключен используемый компьютер (концентратор, коммутатор или маршрутизатор)

1.

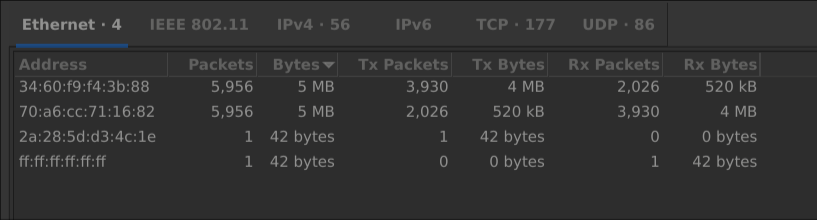


2.

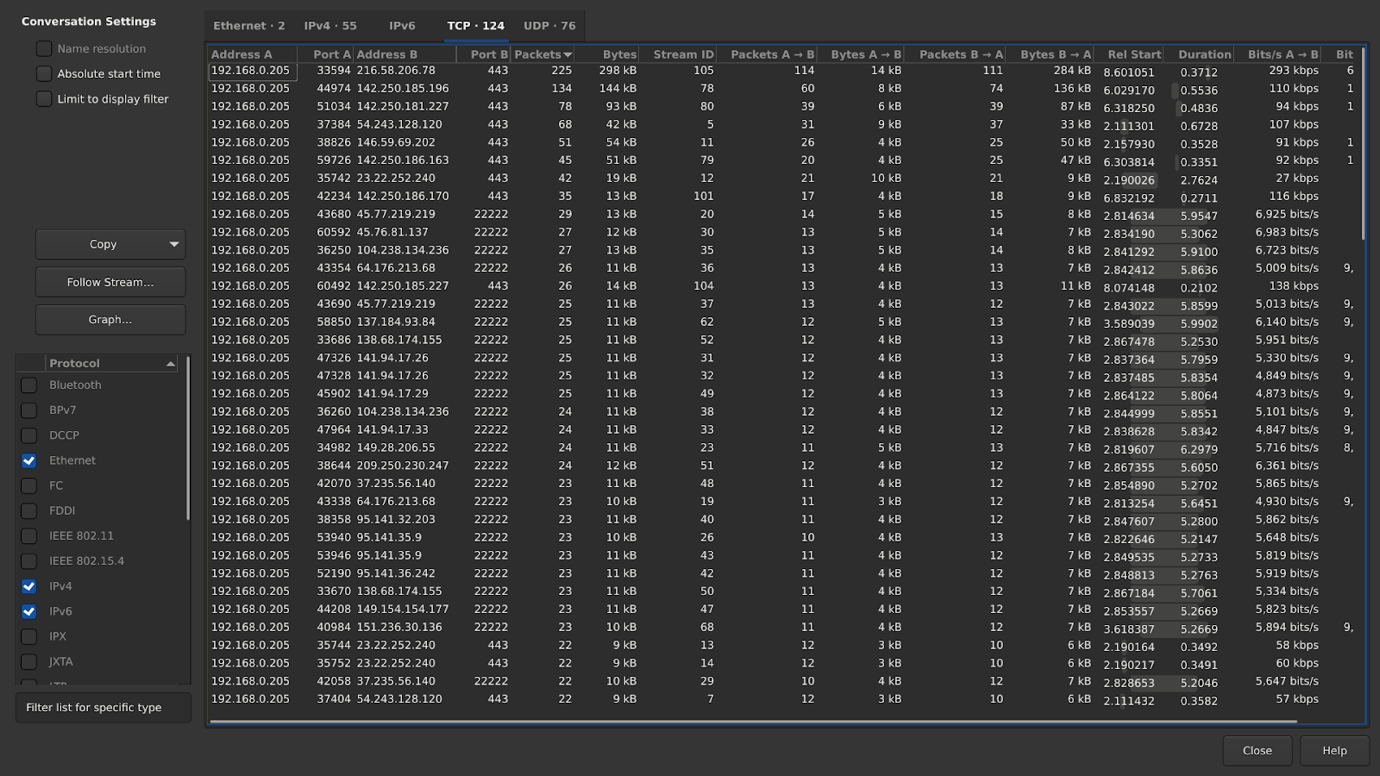
a.



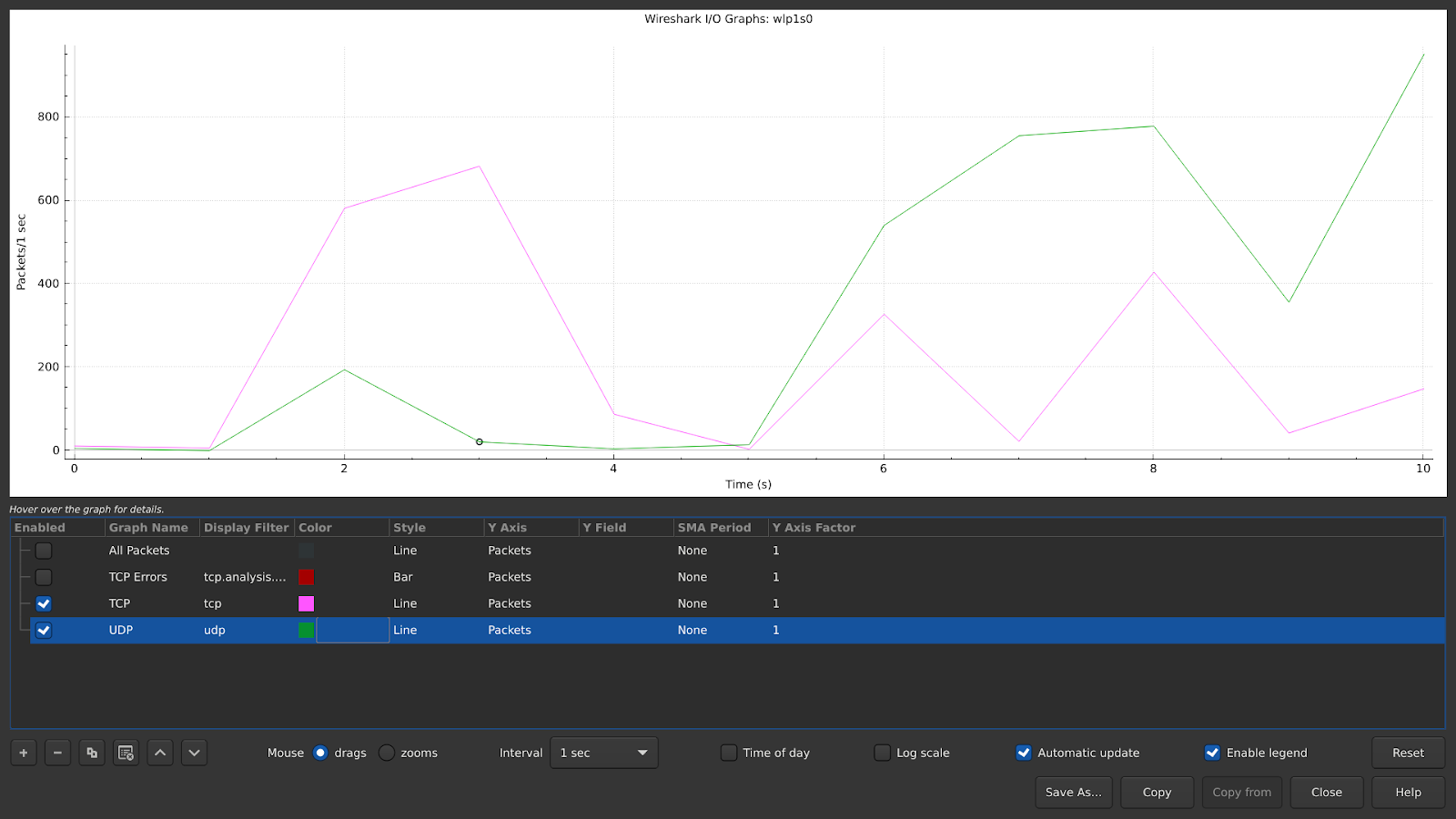
b.



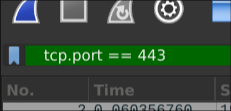
c.

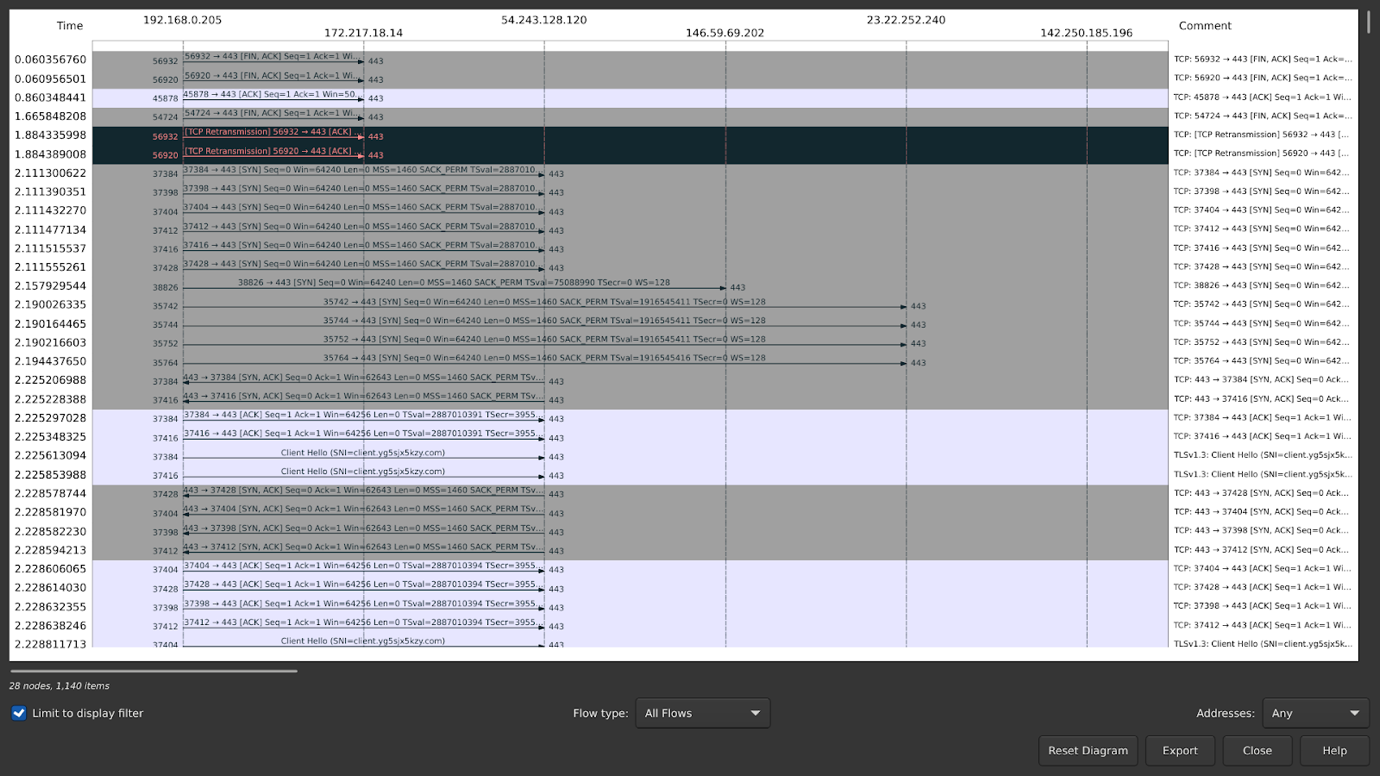


d.



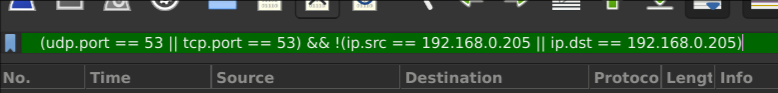
e.



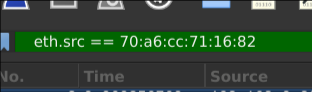


3.

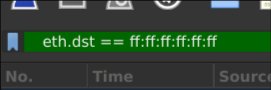
a.



b.



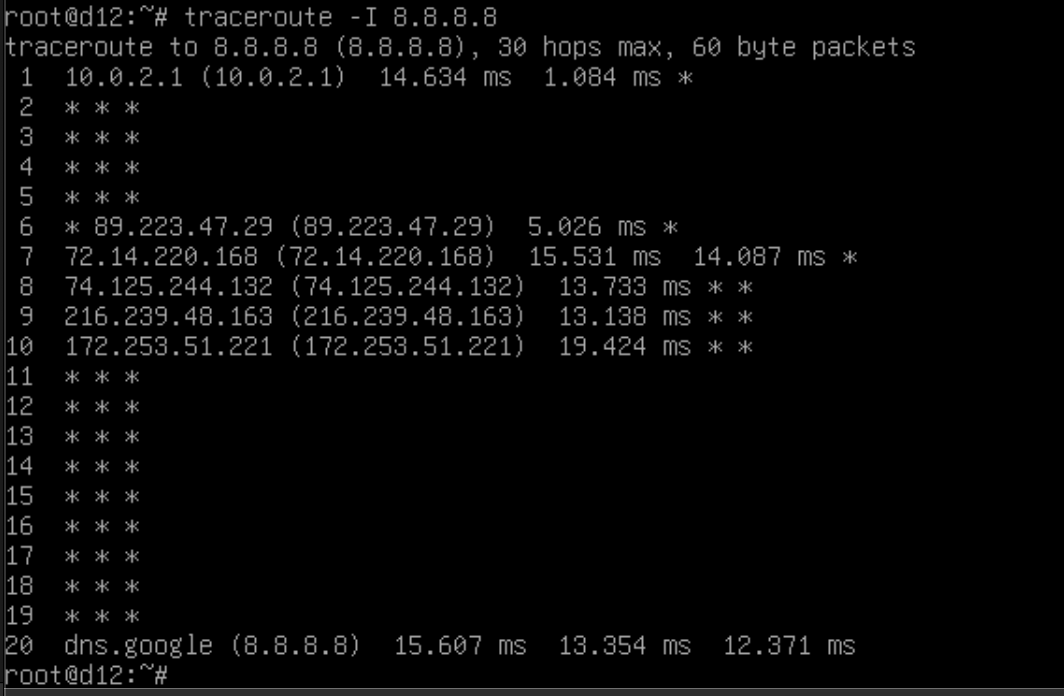
c.

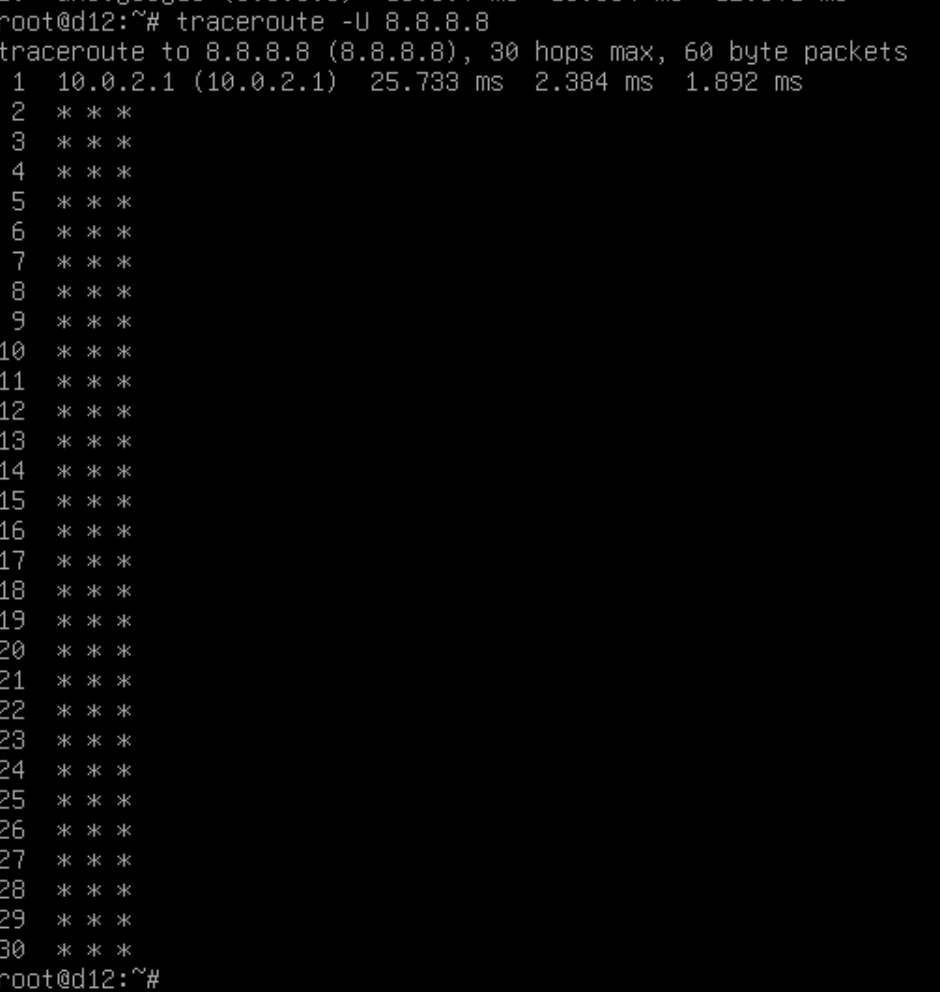


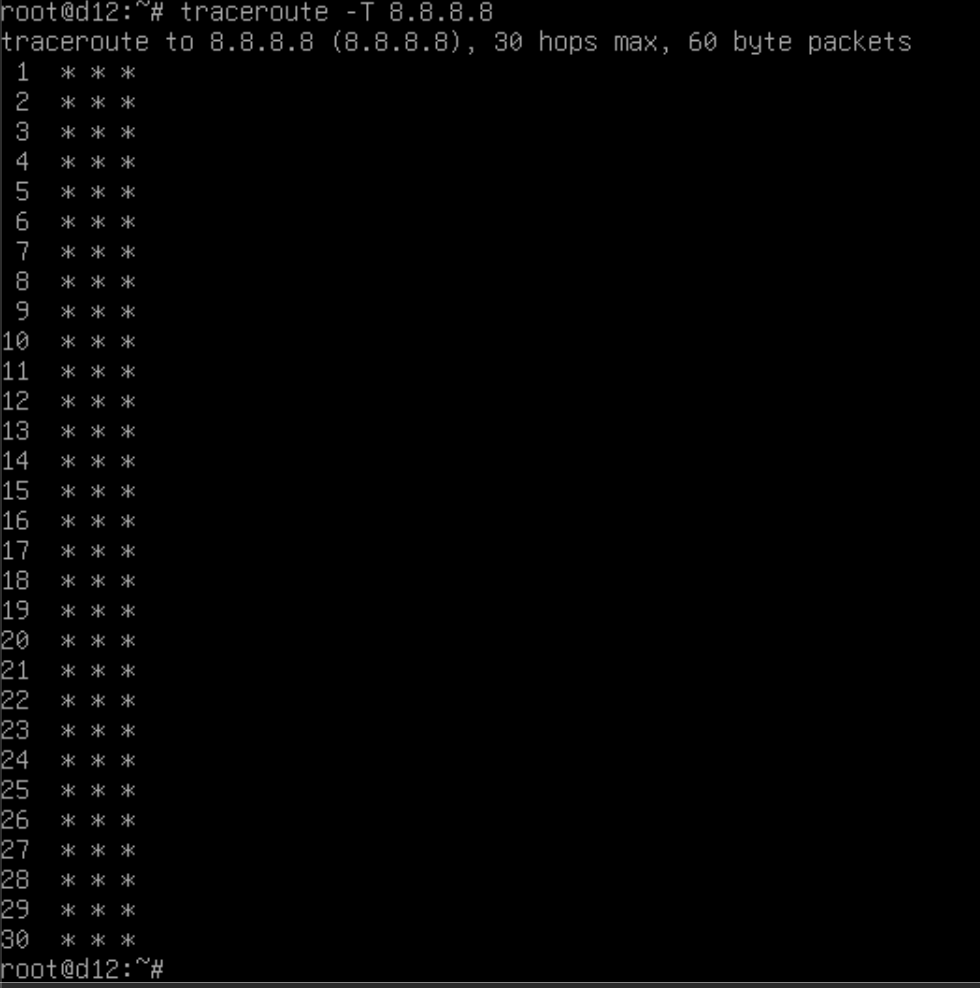
Часть 4. Определение маршрута прохождения пакета

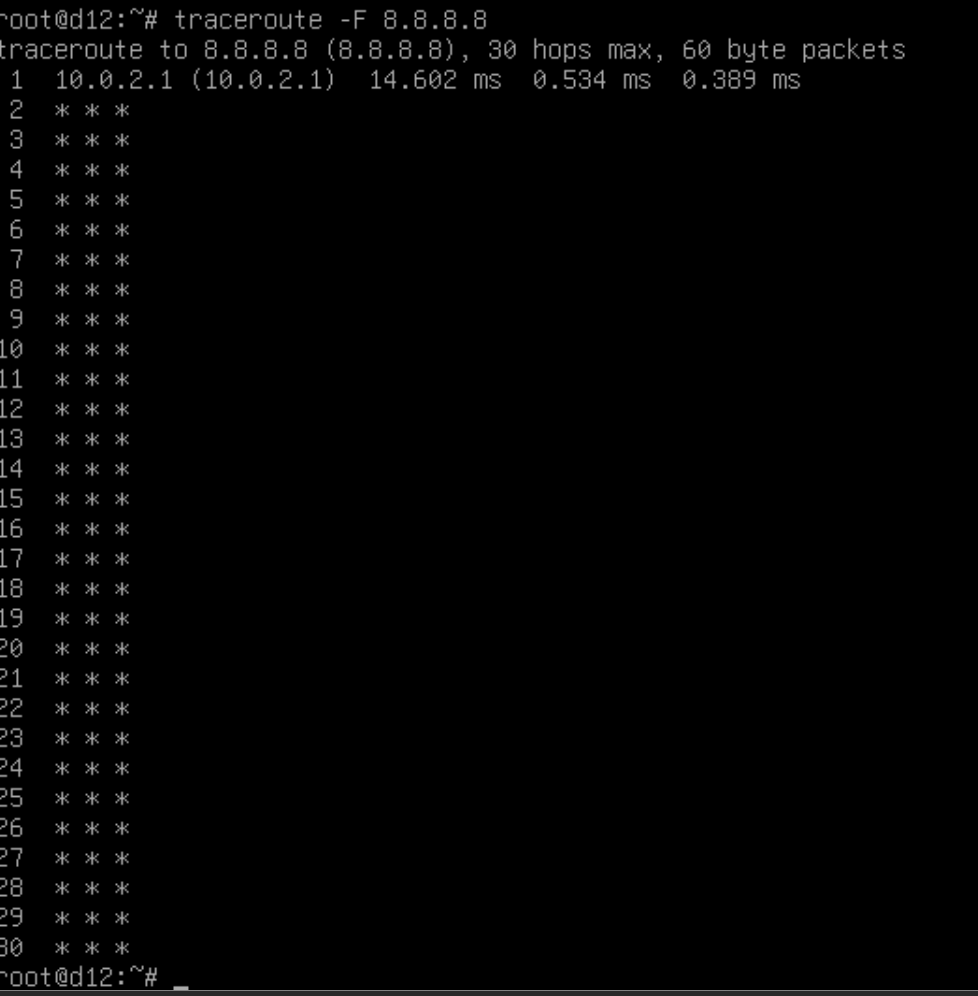
1. Познакомитесь с ключами утилиты traceroute.

2. На машине c7-1 напишите команды traceroute, которые (!):

a. определяют маршрут до хоста 8.8.8.8 с помощью ICMP 

b. определяют маршрут до хоста 8.8.8.8 с помощью UDP 

c. определяют маршрут до хоста 8.8.8.8 с помощью TCP 

d. позволяют определить используется ли по маршруту фрагментация IPv4

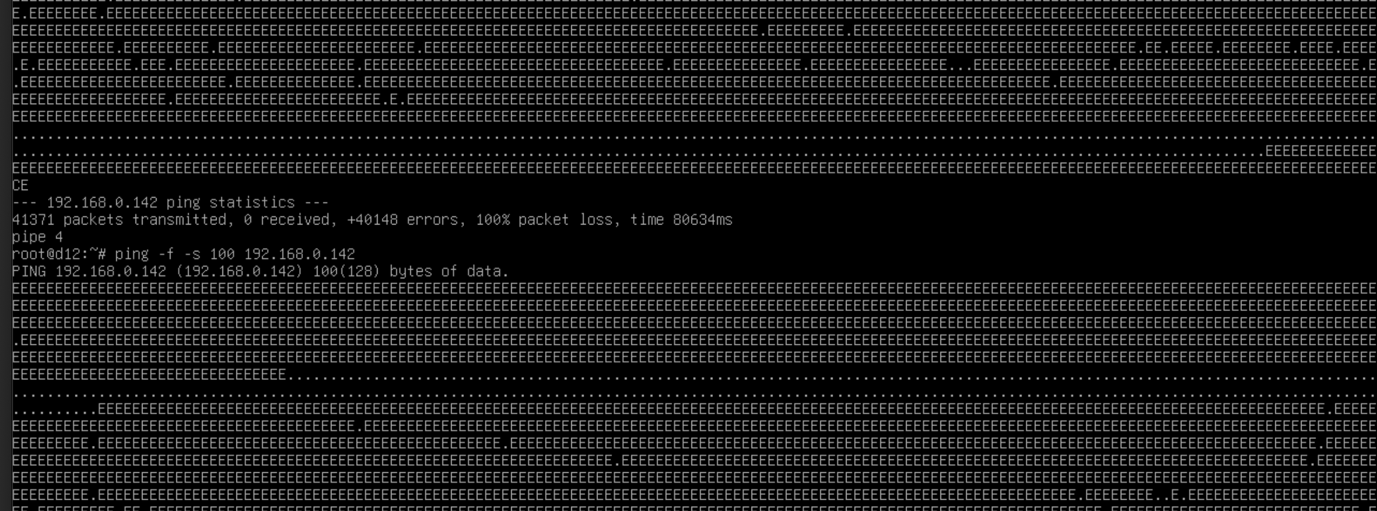
Часть 5. Текущий мониторинг сетевых интерфейсов

1. С хоста c7-2 запустите отправку запросов утилитой ping в режиме flood на внутренний интерфейс c7- 1. 

2. На хосте c7-1 последовательно с помощью утилиты bmon или ее аналогов получите данные о загрузке интерфейса, на который отправляет трафик хост c7-2 (!).

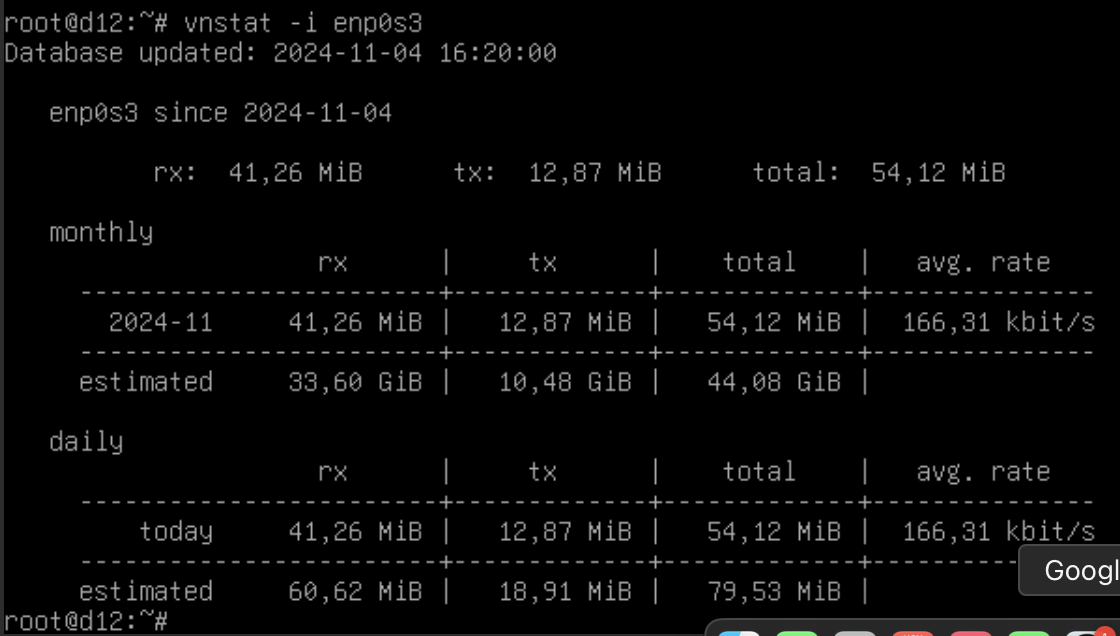


3. Изменяйте размер пакета, передаваемой утилитой ping пакета от 100 до 60100 с шагом 10000. Определите, как меняется загрузка на сетевом интерфейсе (!).

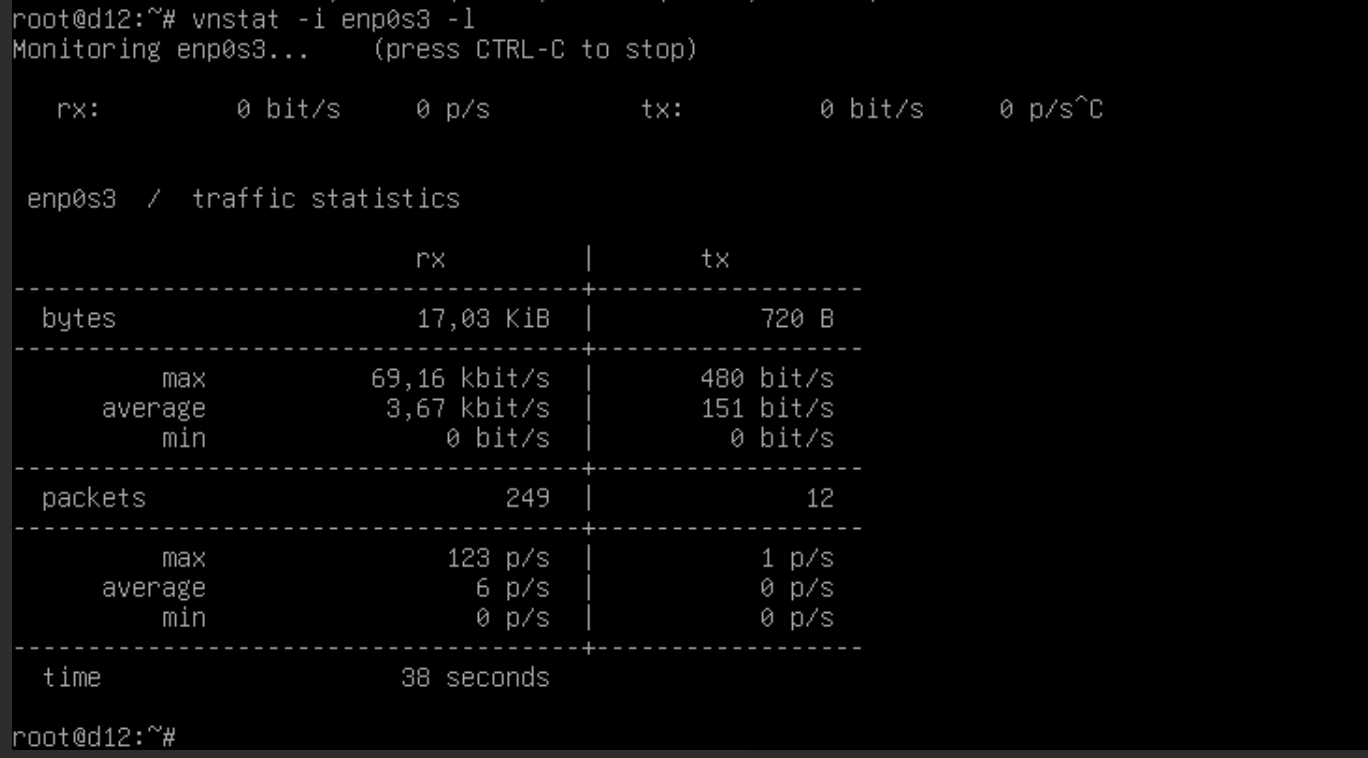


Часть 6. Сбор статистики о загрузки сетевого интерфейса

1. На хосте с7-1 запустите демон vnstat.

2. Поставите на мониторинг интерфейс, через который машина c7-1 подключена к c7-2 

3. С хоста c7-2 запустите отправку запросов утилитой ping в режиме flood, так чтобы работа утилиты прекратилась после отправки 500 пакетов. 

4. Выведите статистику собранного трафика 

Часть 7. Диагностика работы приложений через сеть

1. Установите несколько соединений с SSH сервером на хосте c7-1 с хоста c7-2. Для простоты можно открыть несколько физических консолей или запускать ssh клиент в скрипте, передавая пароль в явном виде с помощью утилиты sshpass (sshpass -p МуPlainPassword\_DontBeatMeSecurityMamager ssh username@host\_address ). Никогда не поступайте так в реальной жизни! Если нужно используйте аутентификацию по ключам.

2. Используя утилиту netstat или lsof на c7-1 вывести все активные (прослушиваемые) порты. (!)

3. Используя утилиту netstat или ss все установленные соединения (!).

4. Напишите скрипт, которой выводит список IP-адресов и количество подключений с них к нашему хосту через порт, задаваемый параметрами скрипта (значение по умолчанию 22). Список упорядочить по количеству соединений с IP адреса. Ради большей наглядности результатов вы можете дополнительно подключиться по SSH к c7-1 с основного хоста или с дополнительных виртуальных машин. Для выполнения задания вам могут понадобиться утилиты grep, awk, cut, sort и uniq, но в выборе инструментов вы не ограничены. (!)

5. Закройте все соединения по ssh с хостом c7-1.

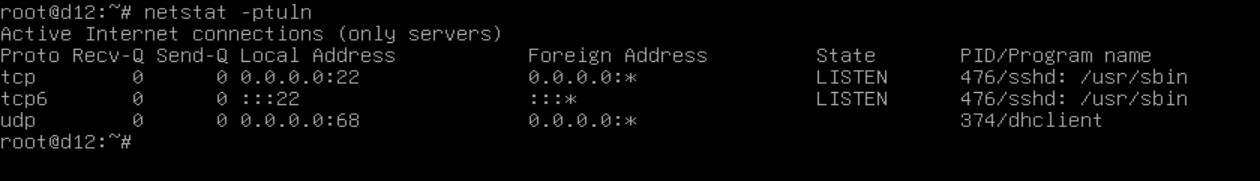
6. Познакомитесь с ключами утилиты nethogs.

7. С хоста c7-2 подключитесь по ssh к машине с7-1. В терминале ssh запустите утилиту top.

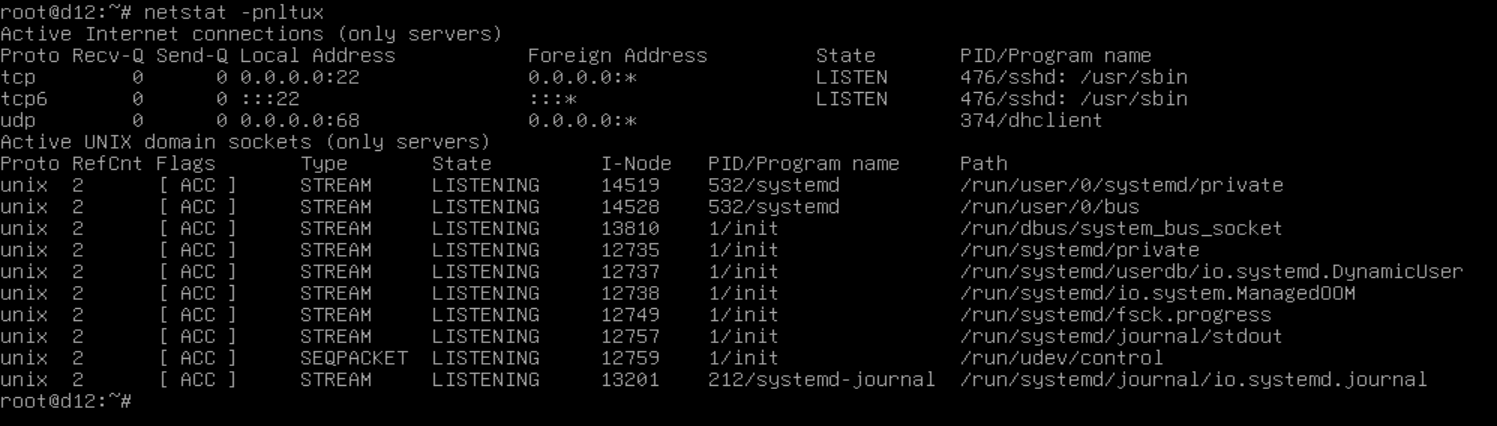
8. На хосте c7-1 с помощью утилиты nethogs определите (!) a. Среднюю скорость передачи данных до sshd. b. PID процесса sshd.



2.



3.



4.

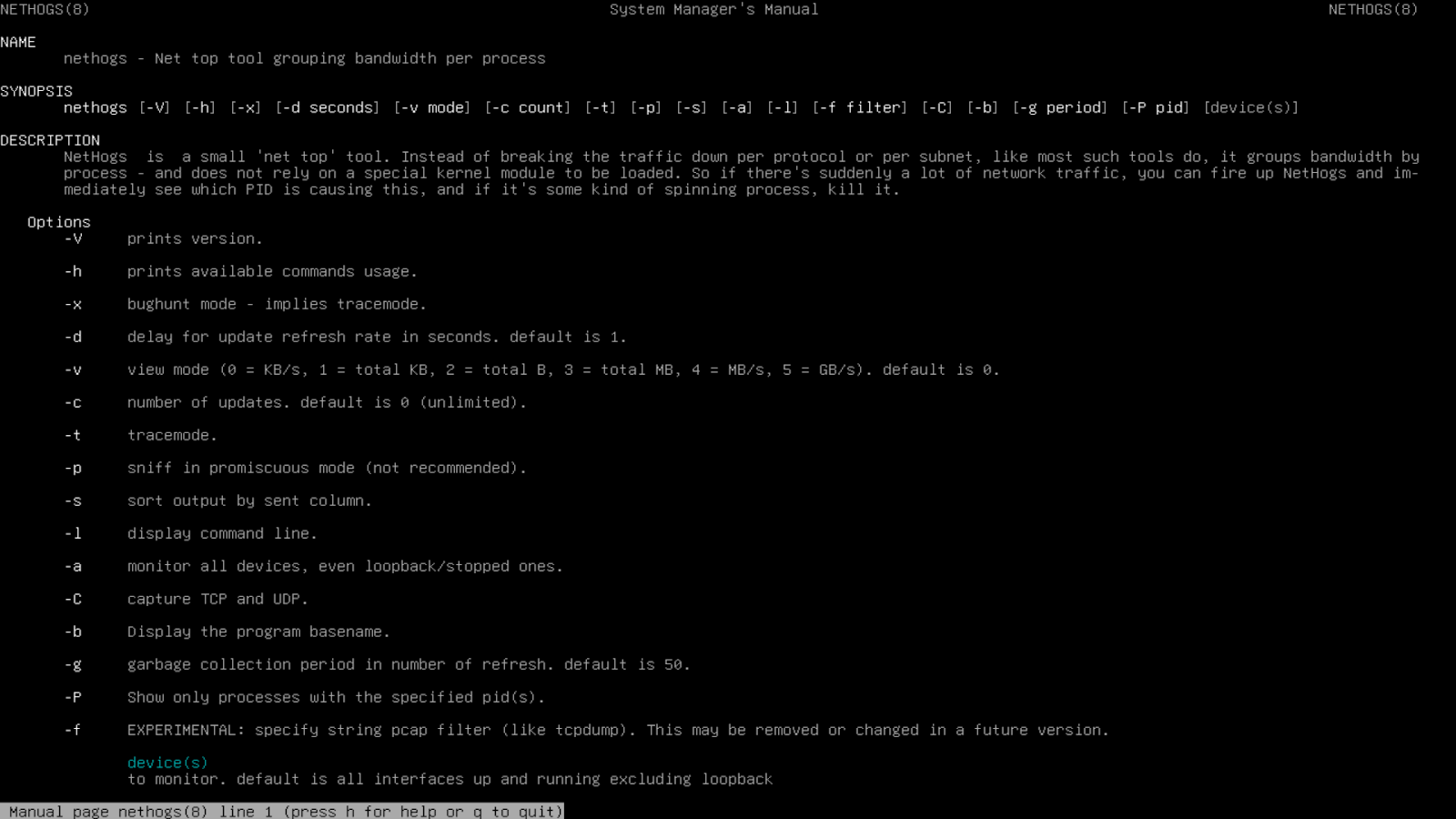


5.



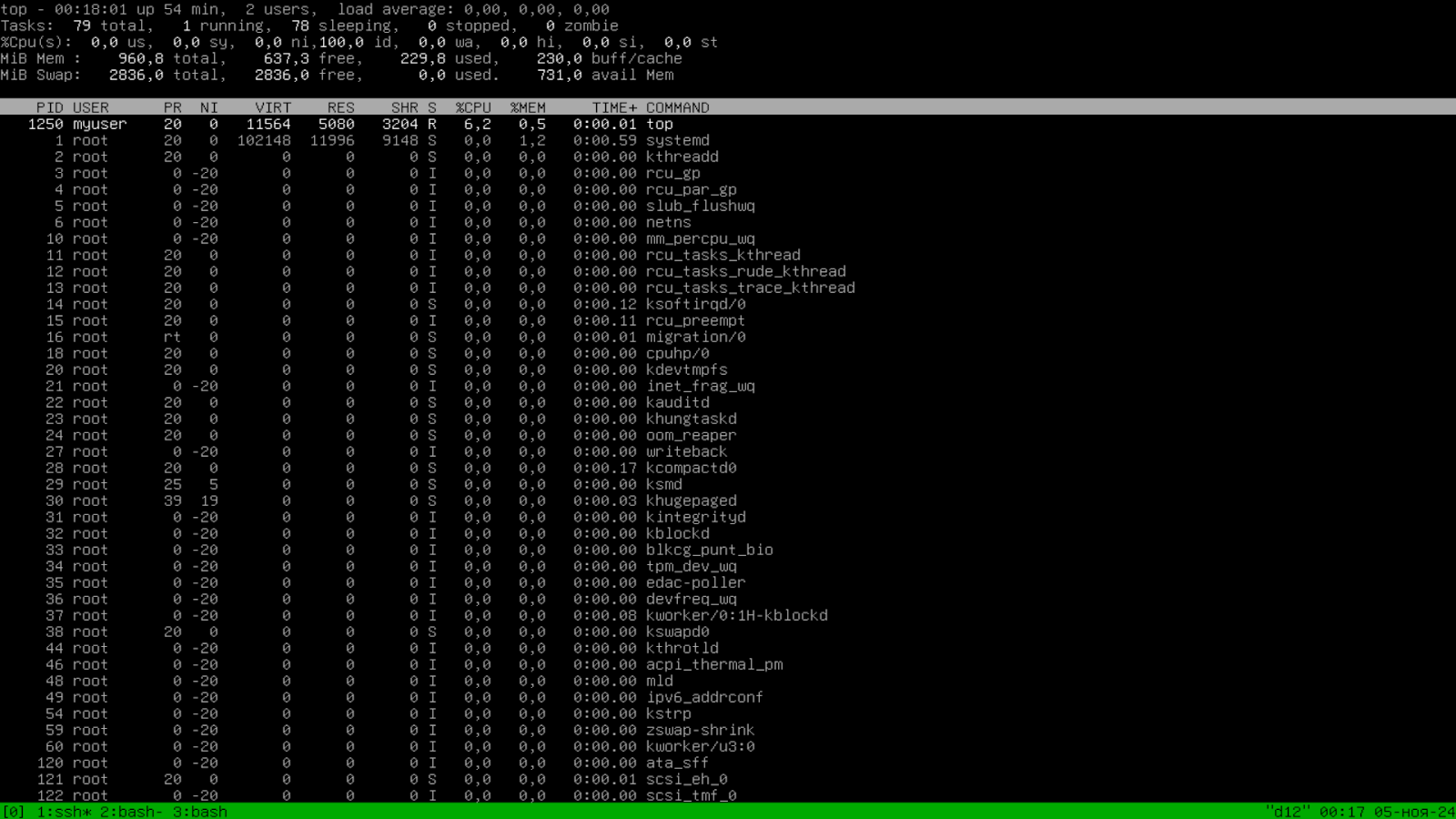
или pkill sshd :)

6.



7.





8.



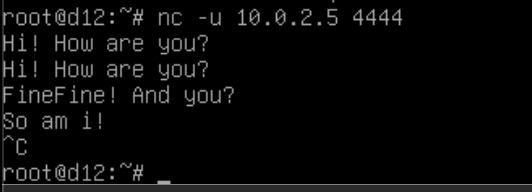
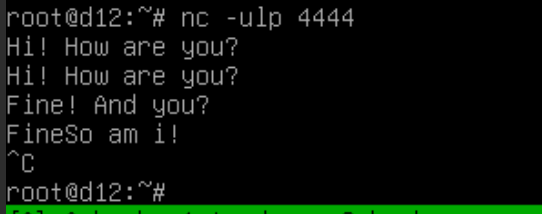
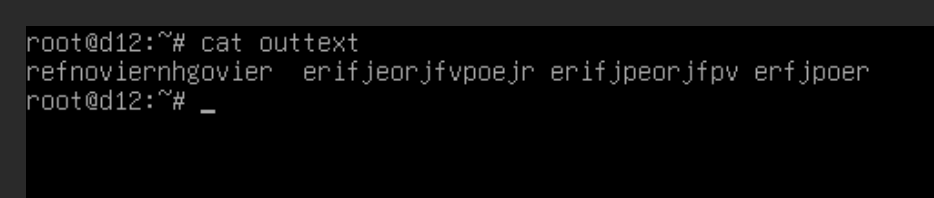
Часть 8. Работа с утилитой nc (NetCat)

1. На машине c7-1 на отдельной консоли запустите tcpdump для сбора всего трафика с портов 9999 и 4444, так, чтобы на консоль выводилось содержимое сообщения, а не только информация из служебных заголовков (!).

2. Используя утилиту nc на обоих машинах передайте текстовый файл с произвольным текстовым содержимым (не мнее 20 слов) принимая файл на порту tcp 9999 (!).

3. Используя утилиту nc на обоих машинах организовать текстовый чат между машинами через порт udp 4444. a. Hi! How are you? b. Fine! And You? c. So am i! Завершите сессию (Cntrl+C)

4. Остановите работу tcpdump, проанализируйте перехваченные сообщения. Какие выводы можно сделать? Примечание: вывод tcpdump можно направить в файл с помощью ключа -w. Это будет файл стандарта pcap, который можно открыть в Wireshark для удобного анализа.



5. Этот пункт выполняется по желанию. С помощью nc можно организовать reverse shell. На машине с Linux Centos 7 с помощью ключа -e запустите команду /bin/bash с перенаправлением вывода-ввода на порт tcp 4445, так же как вы делали для организации чата. Со второй Linux машине подключитесь к порту 4445 и позадавайте команды bash, например получите версию ядра, адрес или hostname.

Вопросы и задания:

1. По какому протоколу работает утилита mtr?
   1. Утилита mtr (My Traceroute) работает по протоколу ICMP (Internet Control Message Protocol) для трассировки маршрута. В некоторых случаях она может использовать UDP (User Datagram Protocol) для обхода ограничений, наложенных на ICMP-трафик.
2. Как это можно определить?
   1. Это можно определить, запустив mtr и проверив тип пакетов, передаваемых в сети, либо отслеживая трафик в сетевом анализаторе (например, Wireshark), где будет видно использование ICMP
3. Опишите значения столбцов статистики, выводимой утилитой mtr. Какие еще статистики доступны в mtr кроме основных?
   1. Основные столбцы в выводе mtr:
      1. Loss% — процент потерь пакетов, показывает стабильность связи.
      2. Snt — количество отправленных пакетов к каждому узлу.
      3. Last — время отклика на последний пакет.
      4. Avg — среднее время отклика.
      5. Best — минимальное время отклика.
      6. Wrst — максимальное время отклика.

Помимо основных, mtr может предоставлять статистику по TCP и UDP, а также может включать такие данные, как время перехода через каждый узел и данные о jitter (колебания задержки).

1. Какие типы кадров Ethernet бывают, в чем их отличия?
   1. Ethernet II: Использует поле "Type" для указания типа протокола высшего уровня.
   2. IEEE 802.3: Использует поле "Length" для указания длины данных.
   3. IEEE 802.3 с SNAP: Использует поле "Length" и дополнительный заголовок SNAP для указания типа протокола высшего уровня.
   4. IEEE 802.3 с LLC: Использует поле "Length" и заголовок LLC для указания типа протокола высшего уровня.
2. Какой тип кадров Ethernet используется в анализируемой сети? Почему именно его применение позволяет сети функционировать?
   1. В большинстве современных сетей используется тип кадров Ethernet II. Этот тип кадров позволяет сети функционировать благодаря своей простоте и эффективности. Поле "Type" в Ethernet II кадрах позволяет легко определить тип протокола высшего уровня, что упрощает обработку пакетов и повышает производительность сети.
3. Как можно определить тип используемого коммутационного оборудования, используя сетевую статистику? Сделайте предположения о типе коммутационного оборудования использовался в сети на основании собранного трафика.
   1. Определить тип используемого коммутационного оборудования можно, анализируя сетевую статистику и трафик:
      1. MAC-адреса: Анализ MAC-адресов устройств может дать информацию о производителе оборудования.
      2. Протоколы управления: Наличие протоколов управления, таких как LLDP (Link Layer Discovery Protocol) или CDP (Cisco Discovery Protocol), может указывать на конкретные производители и модели оборудования.
      3. Типы кадров: Анализ типов кадров Ethernet может дать информацию о поддерживаемых протоколах и функциях оборудования.
      4. Производительность: Анализ задержек, потерь пакетов и других характеристик производительности может дать представление о типе и качестве оборудования.
4. На какие адреса сетевого уровня осуществляются широковещательные рассылки?
   1. Широковещательные рассылки на сетевом уровне (IP) осуществляются на адрес 255.255.255.255 для IPv4 и на адрес ff02::1 для IPv6.
5. На какой канальный адрес осуществляются широковещательные рассылки?
   1. На канальном уровне (уровне Ethernet) широковещательные рассылки осуществляются на специальный широковещательный MAC-адрес: FF:FF:FF:FF:FF:FF
6. Для чего применяются перехваченные широковещательные рассылки в Части 3?
   1. для получения mac-адреса устройства зная его ip-адрес (ARP), для идентификации устройств
7. В Части 4 при разном использовании утилиты traceroute вы получили разные данные. Почему?
   1. При использовании разных протоколов (ICMP, UDP, TCP) для трассировки маршрута можно получить разные данные по нескольким причинам:
      1. Фильтрация трафика: Некоторые сетевые устройства (например, межсетевые экраны или маршрутизаторы) могут фильтровать или блокировать определенные типы трафика. Например, ICMP-трафик может быть заблокирован, тогда как UDP или TCP-трафик будет пропущен.
      2. Приоритеты трафика: Разные типы трафика могут обрабатываться с разными приоритетами, что может влиять на задержки и маршрутизацию.
      3. Протоколы и порты: Некоторые сетевые устройства могут обрабатывать разные протоколы и порты по-разному. Например, TCP-трафик на определенный порт может быть пропущен, тогда как UDP-трафик на тот же порт может быть заблокирован.
      4. Фрагментация: Использование разных протоколов может привести к различной фрагментации пакетов, что может влиять на маршрутизацию и задержки.
      5. Пути маршрутизации: Некоторые сети могут использовать разные пути маршрутизации для разных типов трафика, что может привести к различным результатам трассировки.
8. Как изменяется загрузка интерфейса в Части 5. п. 3? Почему?
   1. Увеличение загрузки сетевого интерфейса
      1. Увеличение объема данных: При увеличении размера пакета увеличивается объем данных, передаваемых по сети. Это приводит к увеличению загрузки сетевого интерфейса, так как больше данных проходит через интерфейс за единицу времени.
      2. Увеличение количества байт в секунду: В режиме flood ping отправляет пакеты с максимальной скоростью. Увеличение размера пакета приводит к увеличению количества байт, передаваемых в секунду, что увеличивает загрузку сетевого интерфейса.
   2. Увеличение использования пропускной способности
      1. Пропускная способность: Увеличение размера пакета приводит к увеличению использования пропускной способности сетевого интерфейса. Если размер пакета становится слишком большим, это может привести к перегрузке сетевого интерфейса и, возможно, к потере пакетов.
      2. Фрагментация: Если размер пакета превышает MTU (Maximum Transmission Unit) сети, пакеты будут фрагментироваться. Это может добавить накладные расходы на обработку фрагментов и увеличить загрузку сетевого интерфейса.
   3. Увеличение задержек
      1. Задержки: Увеличение размера пакета может привести к увеличению задержек, особенно если сетевой интерфейс или маршрутизаторы не могут обрабатывать большие пакеты так же быстро, как маленькие.
      2. Очереди: Увеличение размера пакета может привести к увеличению очередей на сетевых устройствах, что также может увеличить задержки.
   4. Увеличение потерь пакетов
      1. Потери пакетов: Если сетевой интерфейс или маршрутизаторы не могут обрабатывать большие пакеты, это может привести к потере пакетов. Потери пакетов могут быть вызваны перегрузкой сетевого интерфейса или необходимостью фрагментации пакетов.
9. Какие выводы вы сделали в Части 7, п.4?
   1. :::22 и 0.0.0.0:22 означают, что SSH-сервер прослушивает порт 22 на всех интерфейсах -ipv6 (:::) и ipv4 (0.0.0.0). количество соединений 1 означает то, что несмотря на некоторое количество активных подключений по ssh, единственной программой, слушающей порт 22 является локальный sshd
10. На каком уровне модели OSI работает vnstat?
    1. vnstat ведет лог по выбранному сеетвому интерфейсу, поэтому задействуется 2-ой уровень OSI - канальный