# Мониторинг сетевого трафика на хосте на примере работы с утилитами диагностики и мониторинга сетевых соединений в Linux

Выполнил: Михалев Никита Романович М3311

## Часть 1. Настройка инфраструктуры

1. Проверка доступности внешней сети

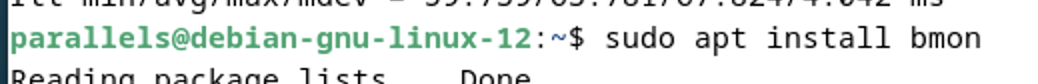
Изображение выглядит как текст, Шрифт, снимок экрана, алгебра

Автоматически созданное описание

Изображение выглядит как текст, Шрифт, снимок экрана

Автоматически созданное описание

1. Установка зависимостей:





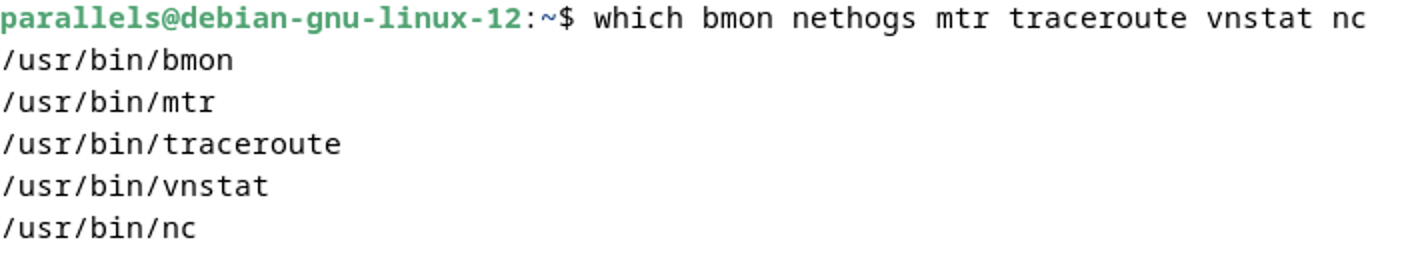








1. Проверка установленных пакетов:



## Часть 2. Диагностика соединения

1. Флаги, используемые в задании для ping:
   1. -c – кол-во пакетов для отправки
   2. -i – интервал между отправкой пакетов
   3. -s – размер отправляемого пакета (в байтах)
   4. -f – «flood ping» отправляет пакеты с максимальной скоростью
   5. -q – «тихий режим» выводит только итоговую статистику
2. Использование ping:

Изображение выглядит как текст, снимок экрана, Шрифт, документ

Автоматически созданное описание

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

Ключ -f в утилите ping включает **flood ping** — режим, при котором пакеты отправляются с максимальной скоростью без ожидания ответов. Этот режим может генерировать большое количество пакетов за короткий промежуток времени и обычно используется для тестирования производительности сети.

1. Флаги, используемые в задании для mtr:
   1. -c – кол-во пакетов для отправки
   2. -r – запустить в отчетном режиме (без интерактивного интерфейса)
   3. -i – интервал между отправкой пакетов
   4. -w – включить расширенные тайминги
   5. -o – позволяет указать параметры для вывода (по умолчанию выводится LSDRN, где L – потеря пакетов, S – скорость, D – задержка, R – джиттер, N – узел)
2. Использование mtr:

Изображение выглядит как текст, Шрифт, число, линия

Автоматически созданное описание

1. Значение всех параметров, выводимых утилитой mtr:

Loss% – процент потерянных пакетов.

Snt – количество отправленных пакетов.

Last – задержка для последнего пакета.

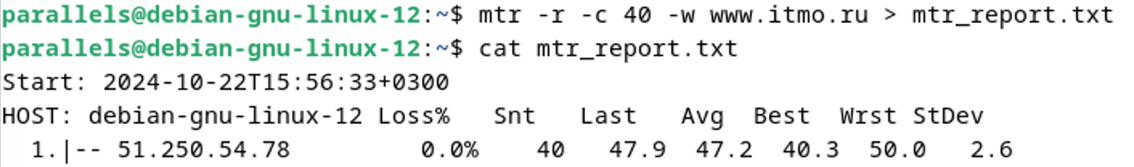
Avg – средняя задержка.

Best – минимальная задержка.

Wrst – максимальная задержка.

StDev – стандартное отклонение (джиттер). В сетях джиттер измеряет, насколько изменяется задержка (время между отправкой и получением пакета) между последовательными пакетами.

1. Команда, которая сохранит в файл расширенную статистику работы mtr при отправке 40 пакетов.

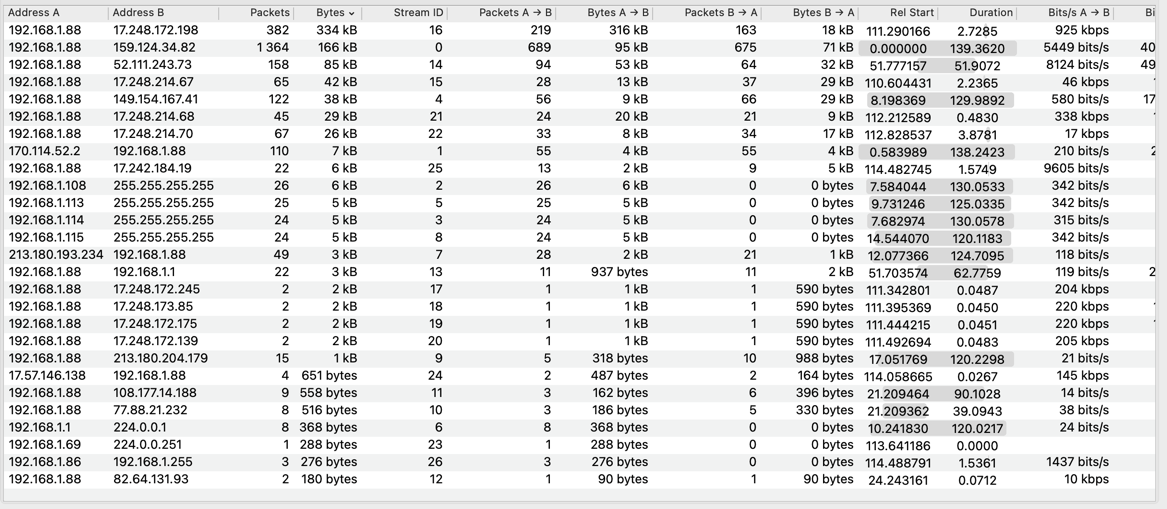


## Часть 3. Работа с Wireshark

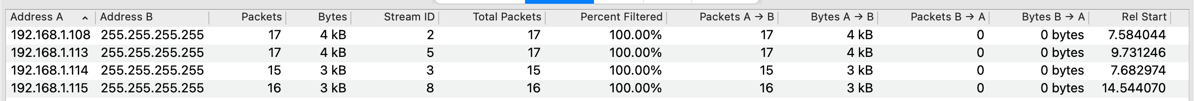
1. (Capture-> Option->Option)

## Изображение выглядит как текст, программное обеспечение, Значок на компьютере, число Автоматически созданное описание

1. Используя инструментарий статистики, определил:
   1. Узел с максимальной активностью (по объему переданных данных)



* 1. Узел, осуществивший наибольшее количество широковещательных рассылок



* 1. Самый активный TCP-порт на хосте (по количеству переданных пакетов)

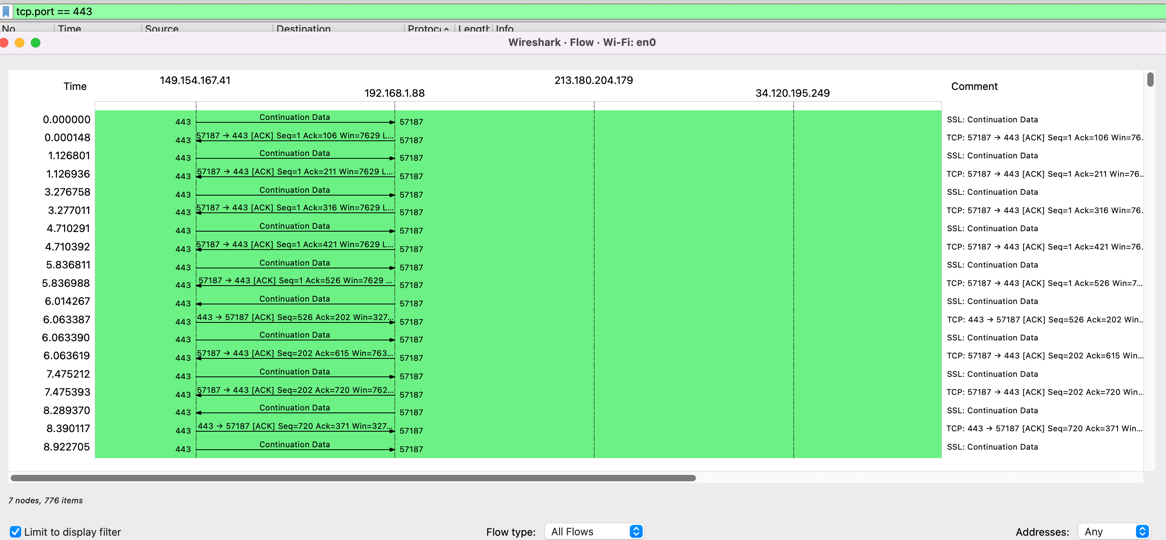
Изображение выглядит как текст, снимок экрана, чек, Шрифт

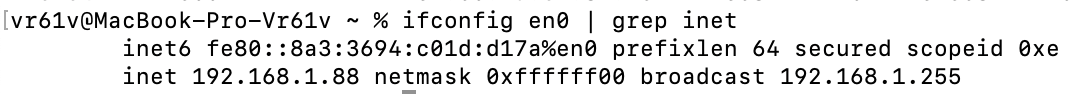
Автоматически созданное описание

* 1. Построил на одной координатной сетке постройте графики интенсивности TCP и UDP трафика (пункт Io Graphs).

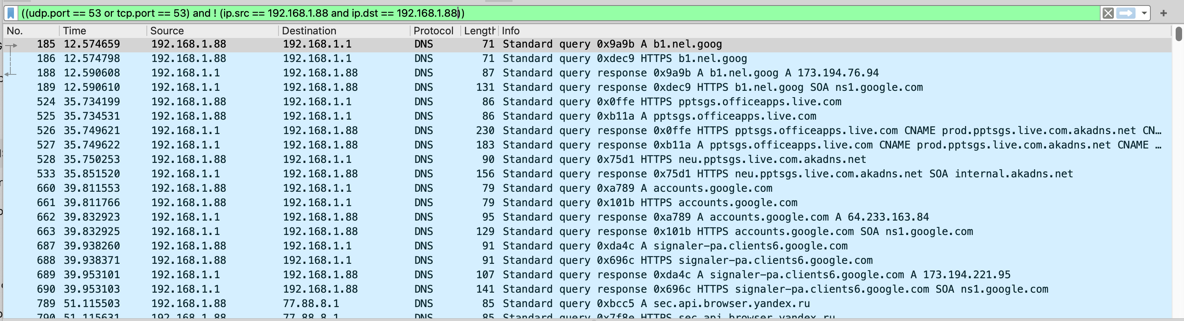


* 1. Построил диаграмму связей только для пакетов, содержащих сообщения протокола HTTPS (пункт Flow Graph)



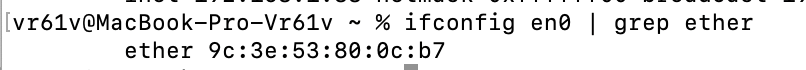
1. Написал фильтры, которые выделяют из общего числа пакеты
   1. Отбирающие сообщения протокола DNS (53 порт udp и tcp) относящиеся только к взаимодействию DNS клиента на хосте и внешних серверов.

Подставив адреса в фильтр, получил следующее:

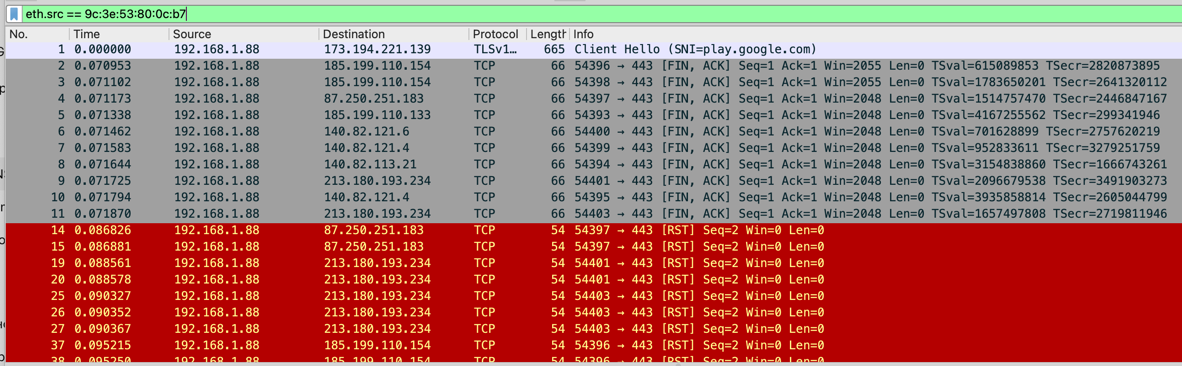


* 1. Все кадры Ethernet, отправленные с сетевого интерфейса хоста.

Для получения mac-адреса устройства воспользовался ipconfig:



Подставив адрес в фильтр, получил следующее:



* 1. Фильтр, отбирающий только широковещательные сообщения. Определил назначение 4-х широковещательных рассылок.

Изображение выглядит как текст, снимок экрана, число, Шрифт

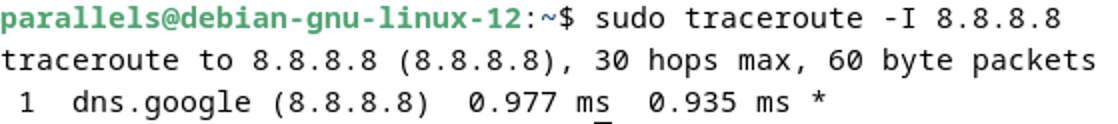
Автоматически созданное описание

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

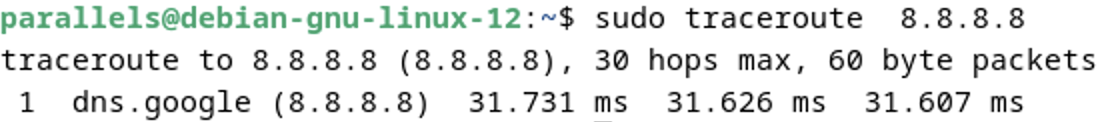
Используемый компьютер подключен к роутеру. Такой вывод можно сделать, основываясь на том, что большинство пакетов адресованы другим сетям, а широковещательные запросы почти отсутствуют (на фоне основного трафика).

## Часть 4. Определение маршрута прохождения пакета

1. Флаги, используемые в задании для traceroute:
   1. -I – использует ICMP
   2. -U – использует UDP (по умолчанию используется именно он)
   3. -T – использует TCP
   4. -f <number> - указывает первый TTL, с которого следует начать
   5. -m <max TTL> - указывает максимальное количество хостов
   6. -p <port number> - указывает номер порта для UDP или TCP
   7. -n – показывает IP-адреса вместо разрешенных имен хостов
2. На машине c7-1 написал команды traceroute, которые:
   1. Определяют маршрут до хоста 8.8.8.8 с помощью ICMP



* 1. Определяют маршрут до хоста 8.8.8.8 с помощью UDP

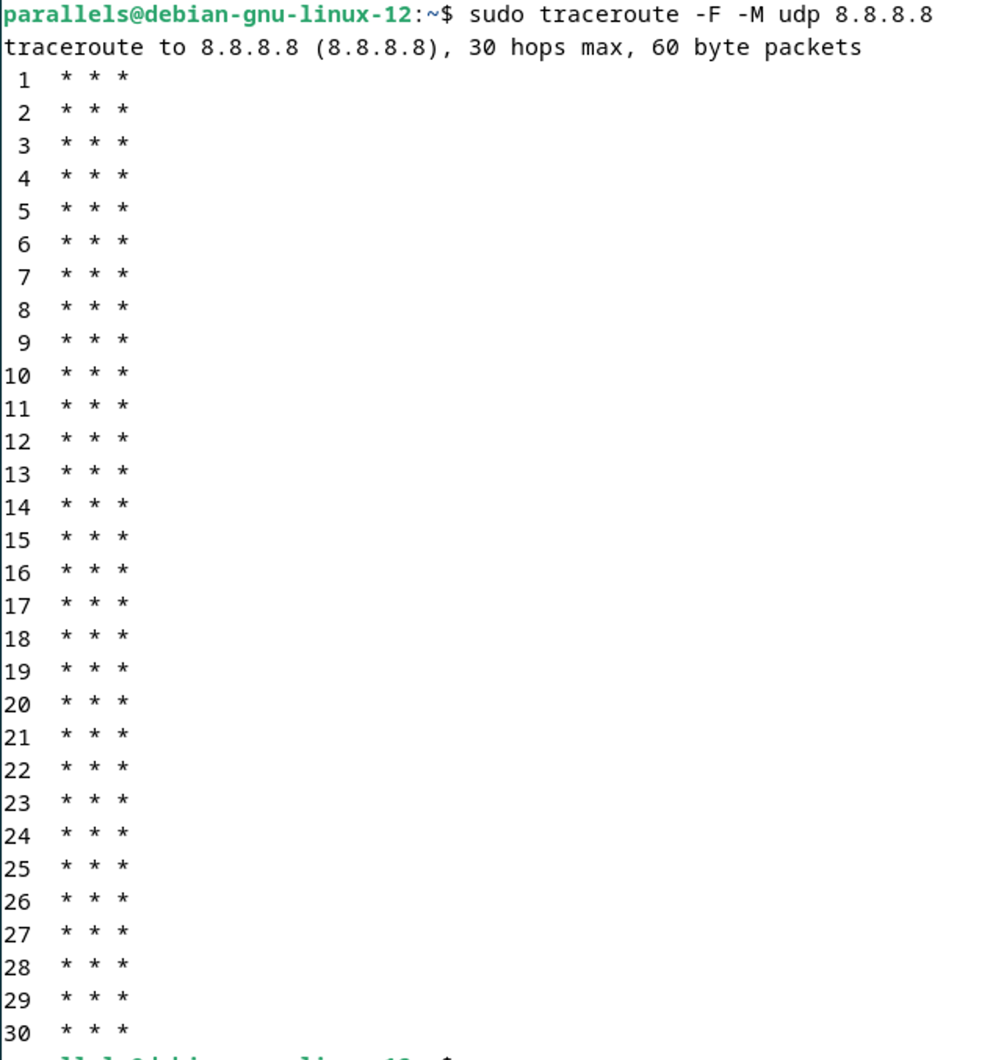


* 1. Определяют маршрут до хоста 8.8.8.8 с помощью TCP

Изображение выглядит как текст, снимок экрана, число

Автоматически созданное описание

* 1. Позволяют определить используется ли по маршруту фрагментация IPv4



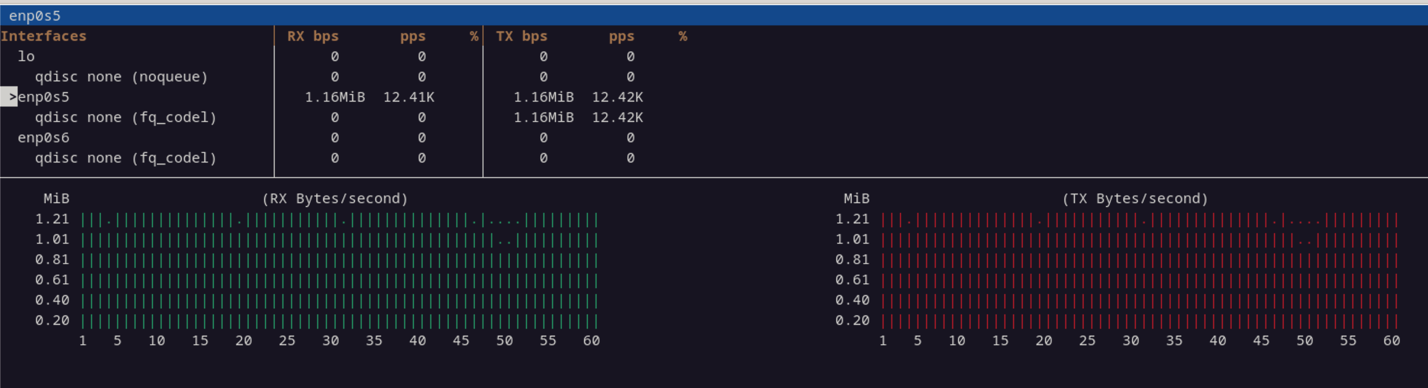
Такое поведение означает, что пакеты невозможно отправить без фрагментации, а следовательно она необходима.

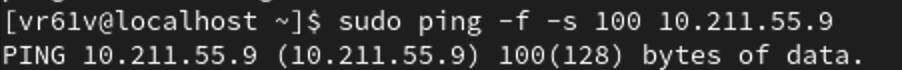
## Часть 5. Текущий мониторинг сетевых интерфейсов

На машине с7-2(CentOS) запустил ping -f машины с7-1(Debian), а на c7-1 запустил bmon:

Изображение выглядит как текст, Шрифт, снимок экрана

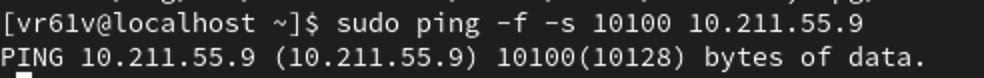
Автоматически созданное описание

  
Из показателей bmon можно сделать вывод, что на enp0s5 (который пингуется из c7-2) идет нагрузка.



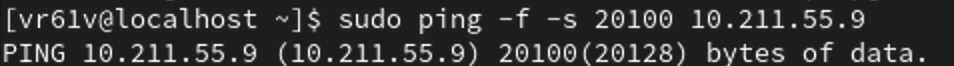
Изображение выглядит как снимок экрана, текст

Автоматически созданное описание



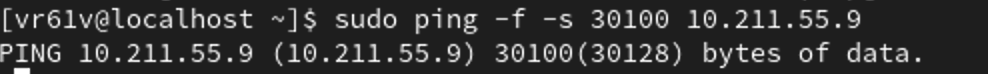
Изображение выглядит как снимок экрана, текст

Автоматически созданное описание



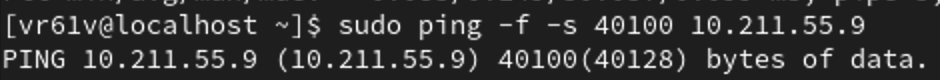
Изображение выглядит как текст, снимок экрана

Автоматически созданное описание



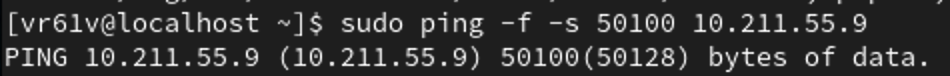
Изображение выглядит как снимок экрана, текст

Автоматически созданное описание



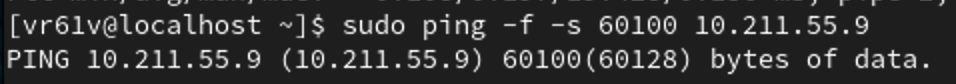
Изображение выглядит как снимок экрана, текст

Автоматически созданное описание



Изображение выглядит как снимок экрана, текст

Автоматически созданное описание

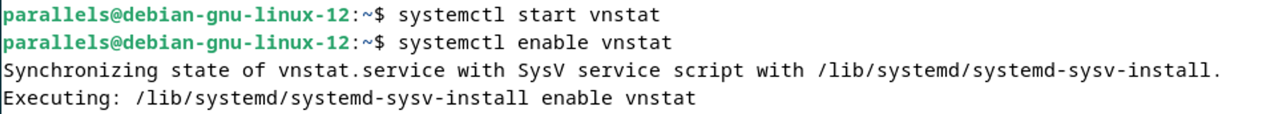


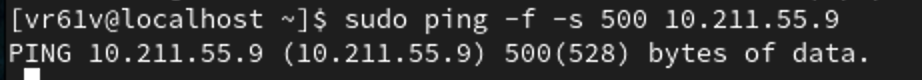
Изображение выглядит как снимок экрана, текст

Автоматически созданное описание

## Часть 6. Сбор статистики о загрузки сетевого интерфейса

1. На хосте с7-1 запустите демон vnstat.





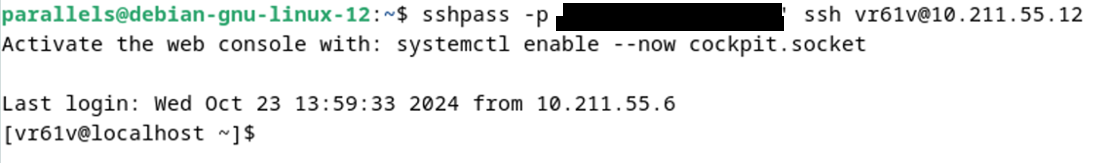
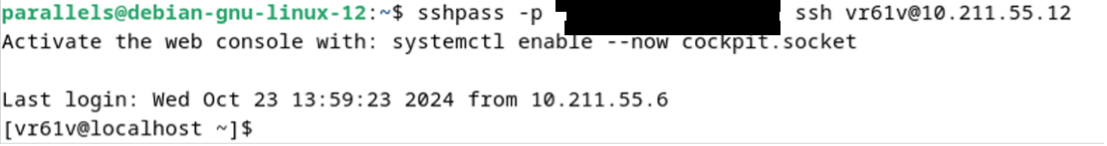
1. Поставите на мониторинг интерфейс, через который машина c7-1 подключена к c7-2

Изображение выглядит как текст, снимок экрана, Шрифт, число

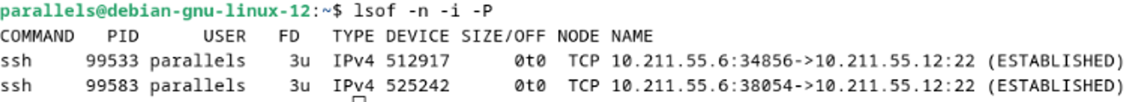
Автоматически созданное описание

## Часть 7. Диагностика работы приложений через сеть

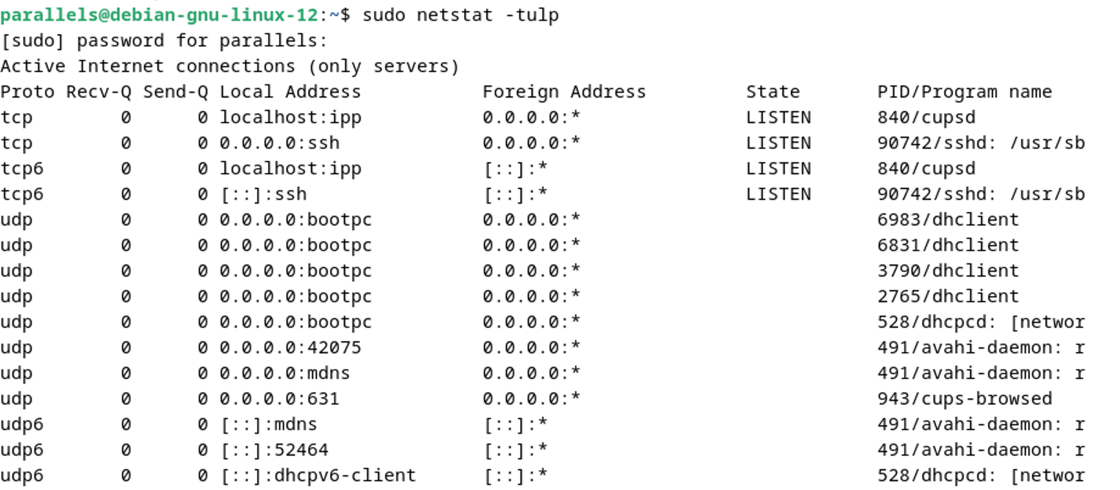
1. Установил несколько соединений с SSH сервером на хосте c7-1 с хоста c7-2:



1. Просмотр активных портов

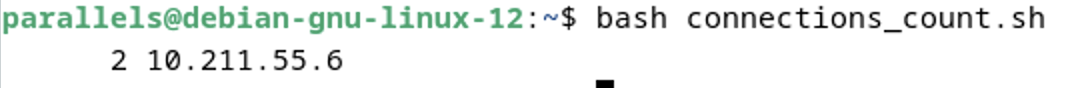


1. Вывод всех установленных соединений



1. Скрипт для получения количества подключений к IP адресам





1. Nethogs –утилита, которая показывает использование сети по процессам. В nethogs используются следующие ключи:
2. -d <seconds> – обновляет вывод каждую секунду
3. -t – выводит в текстовом формате
4. -p <pid> – фильтрует по PID
5. -v – выводит более подробную информаци

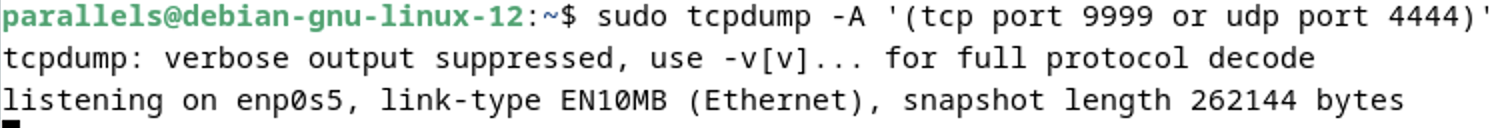


После запуска top:



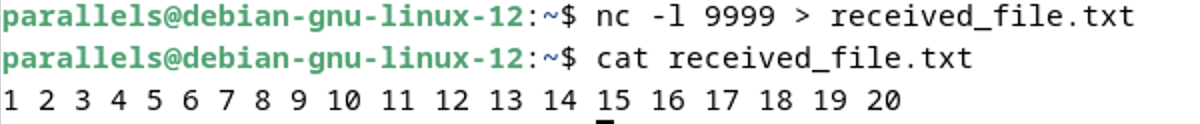
## Часть 8. Работа с утилитой nc (NetCat)

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

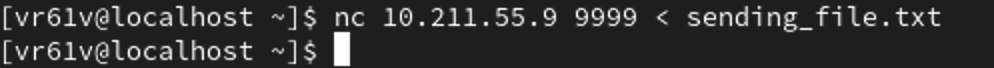


1. Используя утилиту nc на обоих машинах, передал текстовый файл с произвольным текстовым содержимым (не мнее 20 слов) принимая файл на порту tcp 9999 (!).

Ожидание и вывод файла с сообщением:



Отправка файла:



Вывод tcpdump

Изображение выглядит как текст, снимок экрана, чек

Автоматически созданное описание

1. Используя утилиту nc на обоих машинах организовать текстовый чат между машинами через порт udp 4444.

Изображение выглядит как текст, Шрифт, снимок экрана, линия

Автоматически созданное описание

Изображение выглядит как текст, Шрифт, снимок экрана, черный

Автоматически созданное описание

Изображение выглядит как текст, Шрифт, снимок экрана

Автоматически созданное описание

Тут видно, как шло общение между хостами. Выводятся адреса, направления отправки и сами сообщения

## Вопросы и задания

1. **Протокол, по которому работает утилита** mtr: Утилита mtr (My Traceroute) использует **ICMP**, **UDP**, или **TCP** протоколы в зависимости от настроек. По умолчанию, она использует ICMP, который является частью протокола IP и предназначен для передачи сообщений об ошибках и другой информации о работе сети
2. Отображать такие параметры как детализация RTT (время отклика) для разных протоколов (UDP, TCP)
3. Типы кадров Ethernet
   1. Ethernet II: самый распространенный тип кадров, используется в современных сетях. Использует 2-байтовое поле для указания типа протокола верхнего уровня (например, IPv4, IPv6).
   2. IEEE 802.3: включает длину данных вместо типа протокола (максимум 1500 байт данных). Часто используется в сочетании с 802.2 LLC (Logical Link Control).
   3. Ethernet SNAP: расширение IEEE 802.3 для поддержки большего количества протоколов, включающее дополнительные заголовки.
4. Используется **Ethernet II**, так как это стандарт для современных сетей, который поддерживает IPv4 и IPv6. Его применение позволяет корректно передавать сетевые протоколы, такие как IP.
5. Определение типа коммутационного оборудования по сетевой статистике:
   1. Используя такие утилиты как mtr, traceroute, можно определить задержки и маршруты пакетов, которые помогут понять, используется ли в сети оборудование уровня Layer 2 (коммутаторы) или Layer 3 (маршрутизаторы).
   2. Если обнаружены высокие задержки между узлами или промежуточные шаги, это может указывать на наличие маршрутизаторов, а низкие задержки обычно говорят о коммутаторах.
6. На уровне IP широковещательные рассылки осуществляются на адрес **255.255.255.255** или на широковещательный адрес подсети, например, **192.168.1.255** для сети 192.168.1.0/24.
7. Широковещательный MAC-адрес: FF:FF:FF:FF:FF. Все устройства в локальной сети принимают кадры с этим адресом.
8. Широковещательные рассылки могут использоваться для:
   1. Протоколов ARP (Address Resolution Protocol) для определения MAC-адресов устройств.
   2. Протоколов DHCP для назначения IP-адресов.
9. Разные данные при использовании traceroute могут быть связаны с:
   1. Использованием разных протоколов (ICMP, UDP, TCP), которые могут по-разному обрабатываться сетевыми устройствами.
   2. Нагрузкой на сеть, маршрутизацией или конфигурацией сетевых фильтров.
10. **При увеличении размера пакета** (от 100 до 60100 байт) будет увеличиваться объем данных, передаваемых по сети. Это приведет к увеличению загрузки интерфейса, поскольку каждое отправляемое сообщение занимает больше места в канале передачи данных. При отправке большого объема трафика (например, с размером пакета 60100) возможно, что интерфейс достигнет своей предельной пропускной способности, что приведет к увеличению задержек
11. **К одному порту может быть много подключений с разных IP адресов**
12. Утилита **vnstat** работает на **канальном уровне** (уровень 2 модели OSI). Она отслеживает трафик на сетевом интерфейсе, анализируя кадры и пакеты без интерпретации данных на более высоких уровнях.