Министерство науки и высшего образования Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО

Факультет ФТИИ

Дисциплина: «Сетевые технологии»

ПРАКТИЧЕСКАЯ РАБОТА № 2

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

Выполнил:
Тиганов Вадим Игоревич, студент группы J3212
ИСУ: 467701

Проверила:
Шиманская Галина Станиславовна

Санкт-Петербург
2025

Содержание

1 Цель работы

Получить практические навыки мониторинга сетевого трафика и диагностирования сетевых соединений на хосте Linux с использованием консольных утилит: `ss`, `lsof`, `tcpdump`/`tshark`, `iftop`/`nload`/`bmon`, а также базовых средств `ip` и `ethtool`.

2 Артефакты выполнения

2.1 Часть 1. Настройка инфраструктуры

ВМ c7-1/c7-2, NAT в VirtualBox, DHCP-адреса, проверка ping внешней сети, установка утилит (bmon/nload/iftop, nethogs, mtr, traceroute, vnstat, nc)

2.2 Часть 2. Диагностика соединения

Команды и выводы по `ping`, запуск `mtr` к `www.itmo.ru`, сохранение расширенной статистики на 40 пакетов:

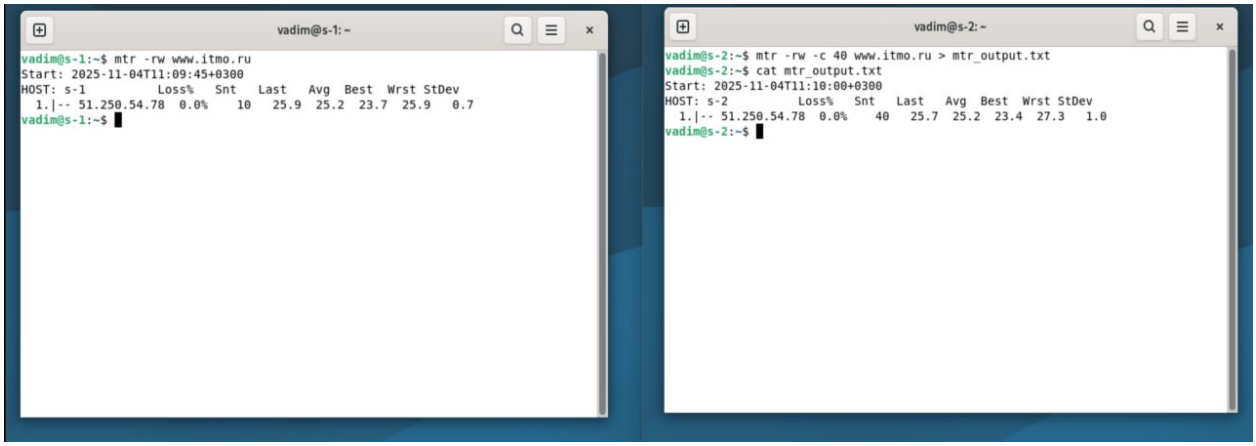
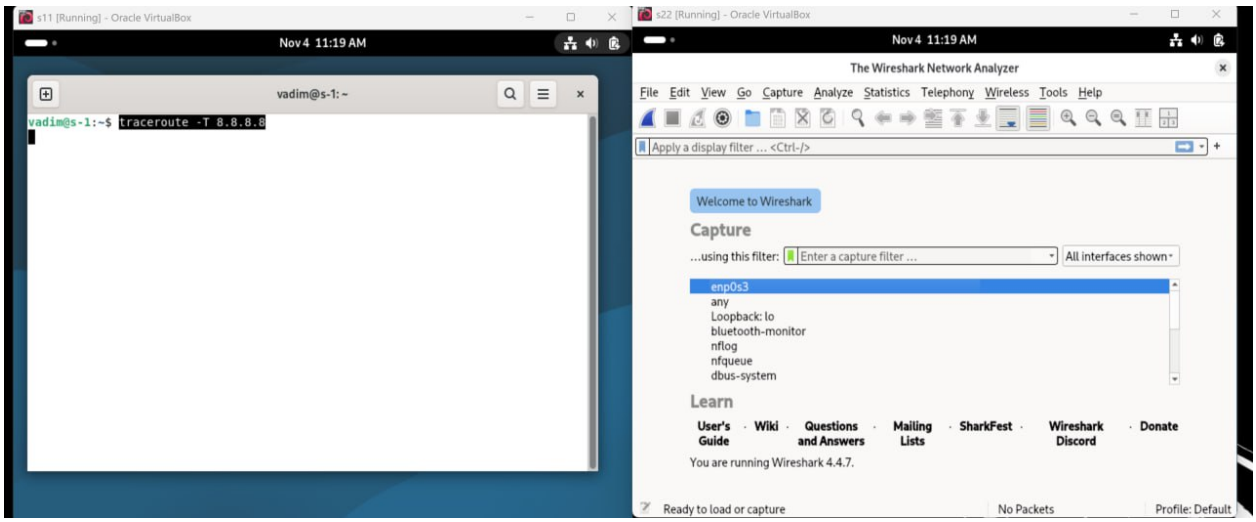


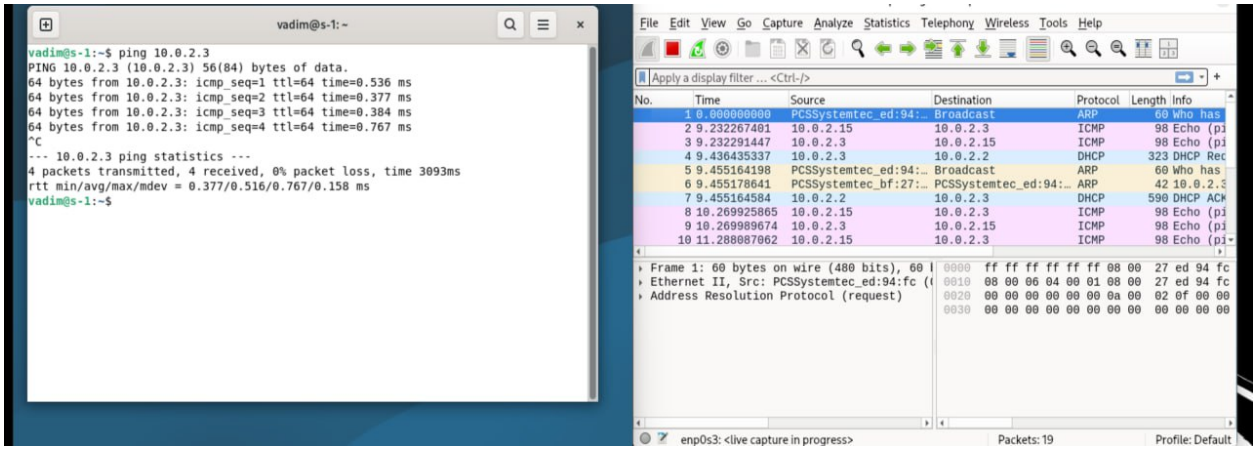
Рис. 1: Вывод команды `ping`

2.3 Часть 3. Работа с Wireshark

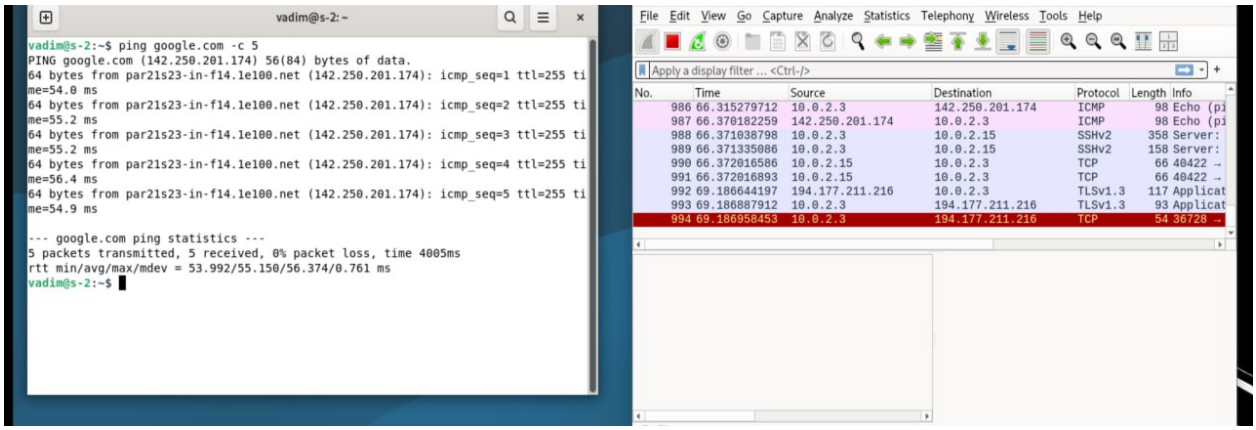
Настройка захвата (ограничение 5 МБ), статистика — самый активный узел, широковещательный «говорун», самый активный TCP-порт; графики Io Graphs (TCP/UDP вместе); Flow Graph по HTTPS; фильтры отображения для DNS/кадров хоста/широковещаний:



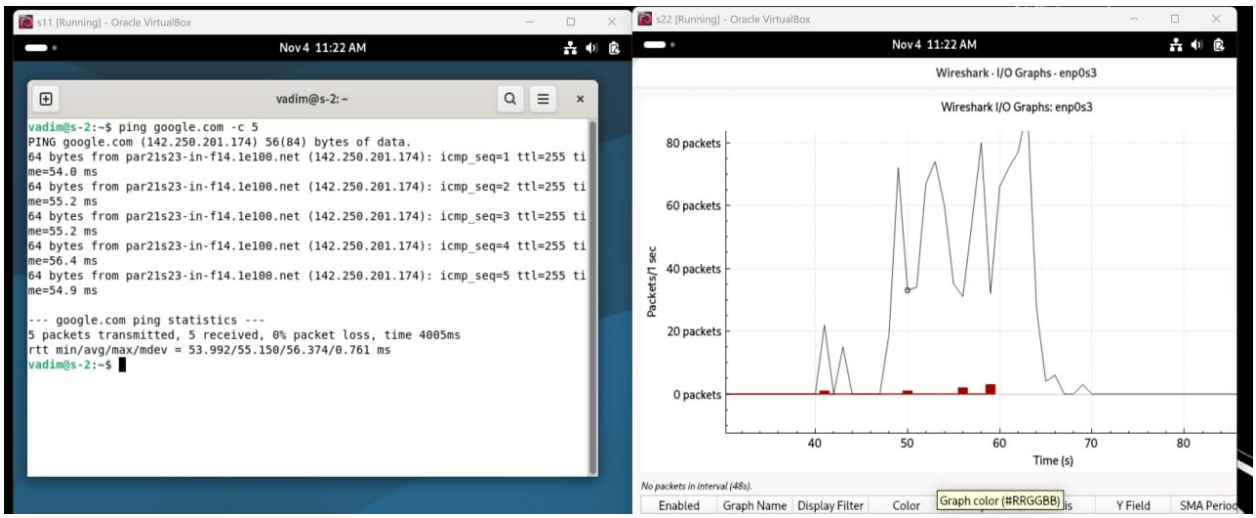
wireshark 1



wireshark 2



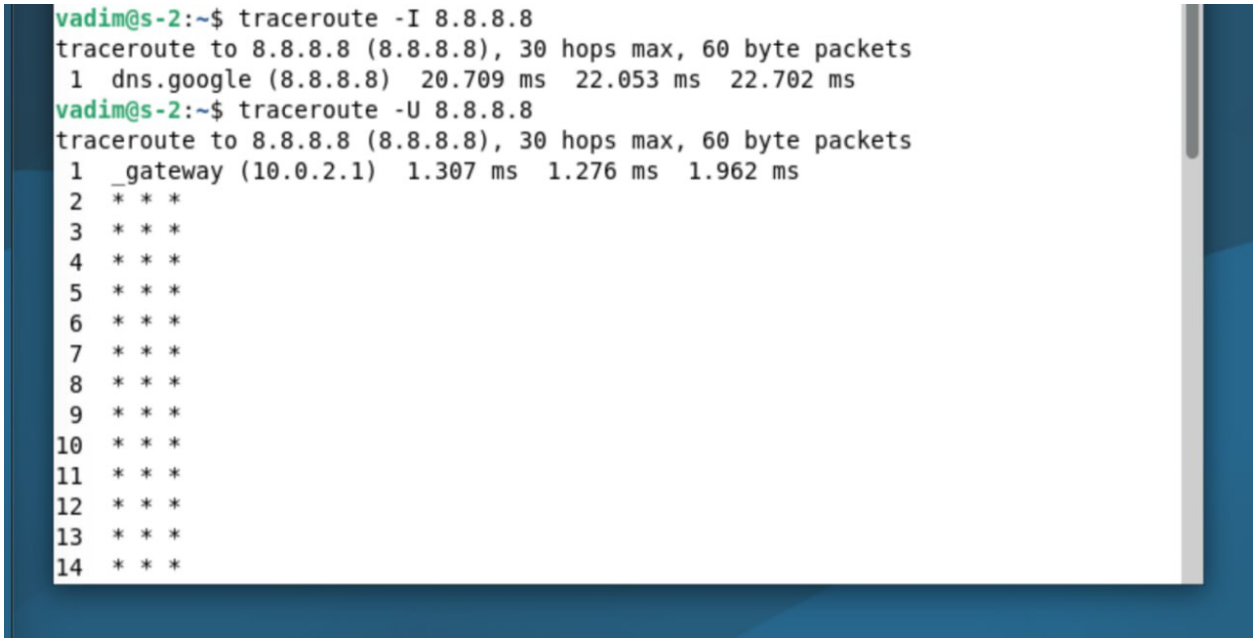
wireshark 3



wireshark 4

2.4 Часть 4. Определение маршрута прохождения пакета

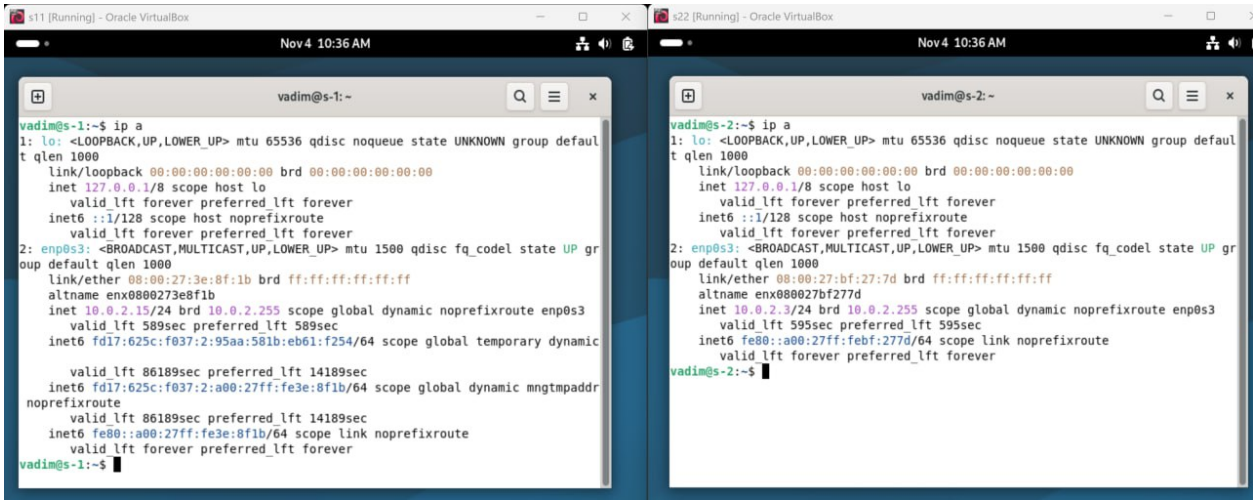
Место для: команды `traceroute` *с ICMP/UDP/TCP до 8.8.8.8 и проверка фрагментации IPv4 — команды и выводы*



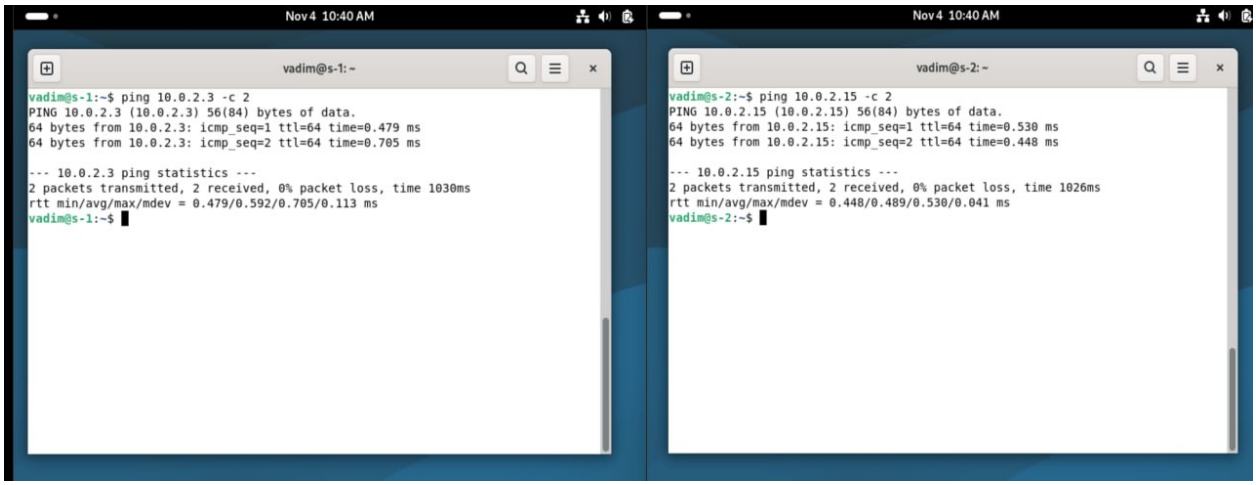
traceroute 8.8.8.8

2.5 Часть 5. Текущий мониторинг сетевых интерфейсов

Место для: `ping -f` с c7-2 на внутренний интерфейс c7-1;



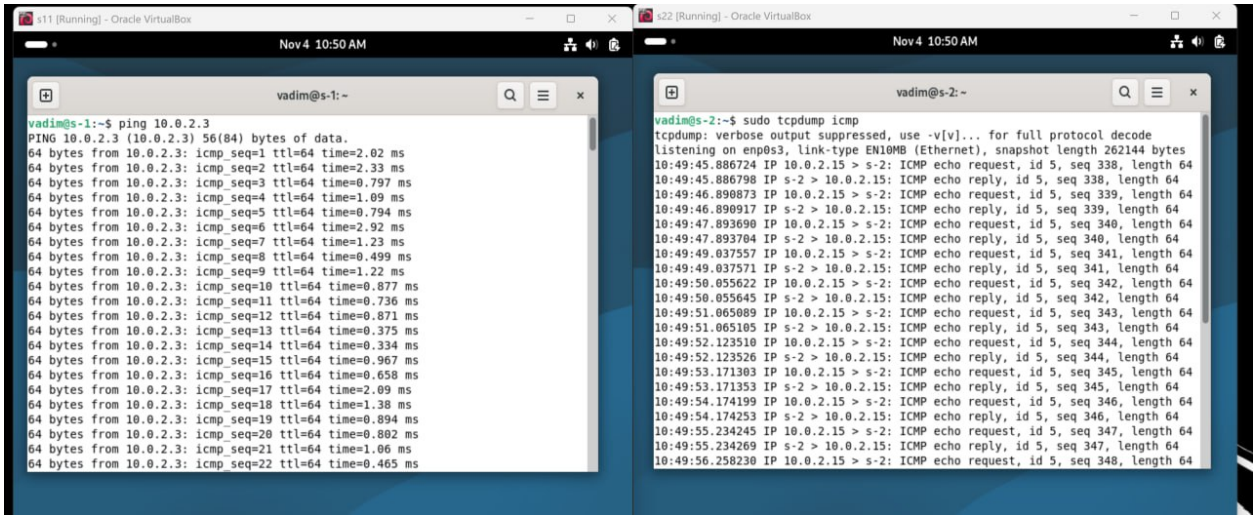
Проверим ip адреса



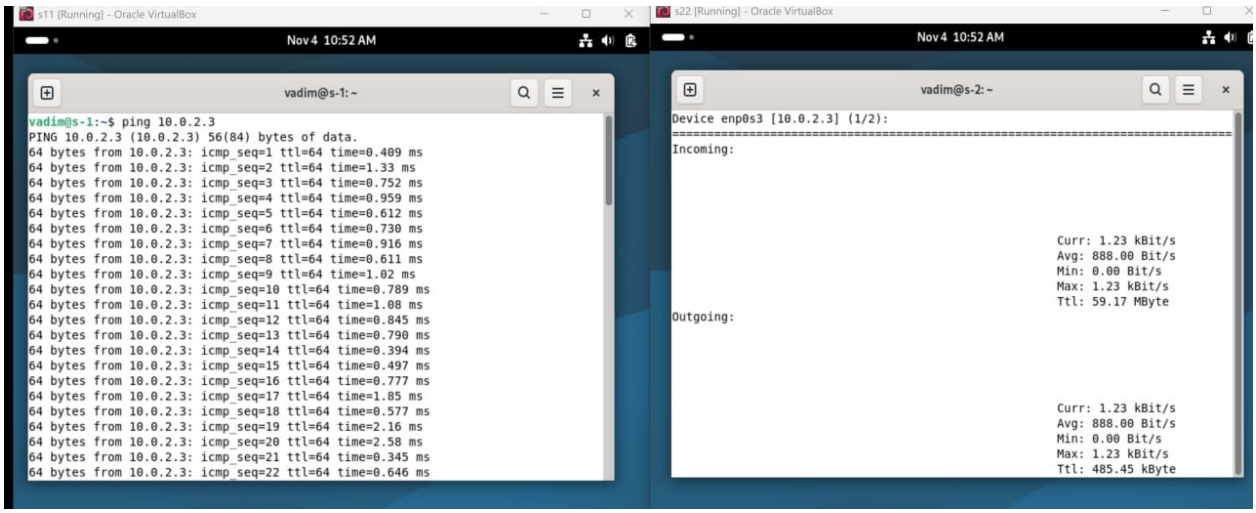
Пингуем для проверки соединения

2.6 Часть 6. Диагностика работы приложений через сеть

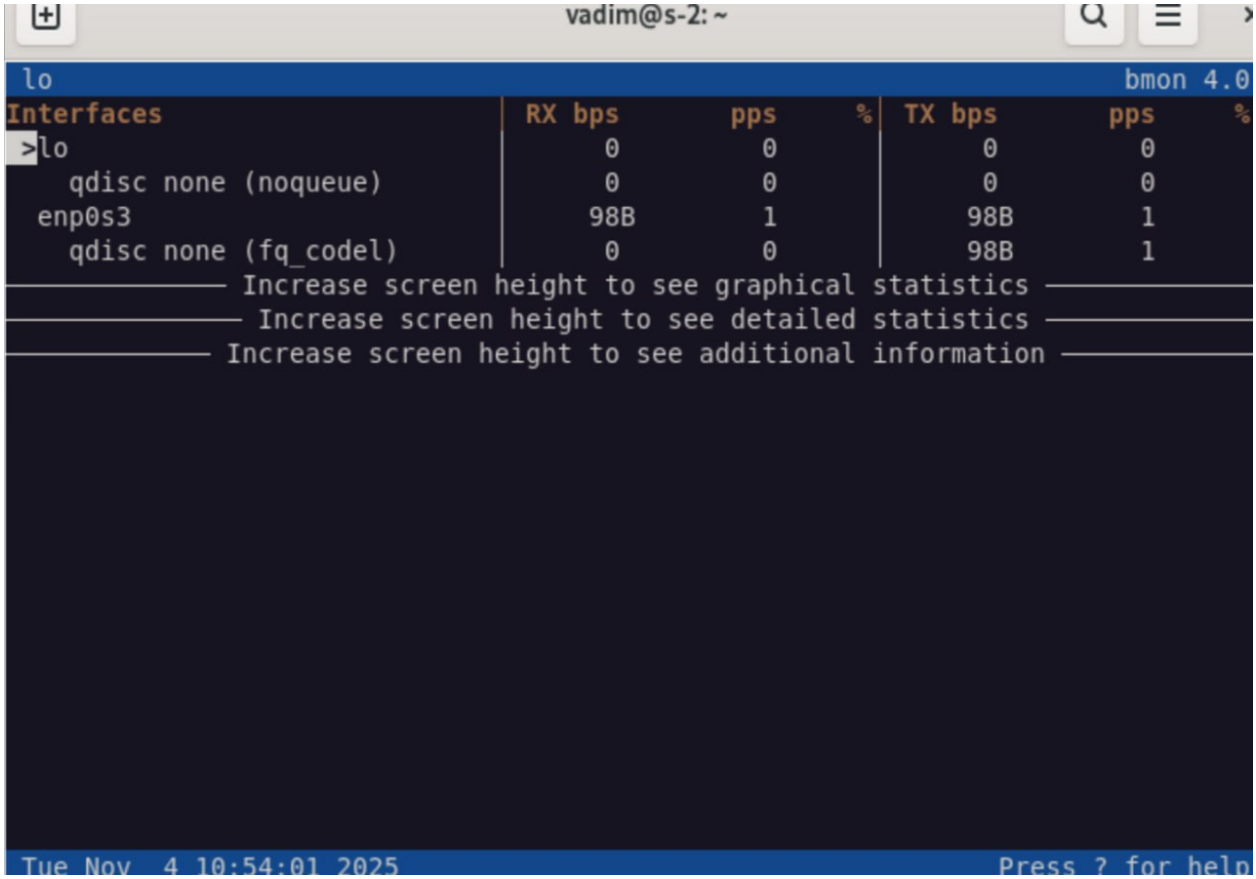
SSH-сессии; вывод `netstat/ss` — прослушиваемые порты и установленные соединения; скрипт агрегации соединений по порту (по умолчанию 22); закрытие сессий — вывод:



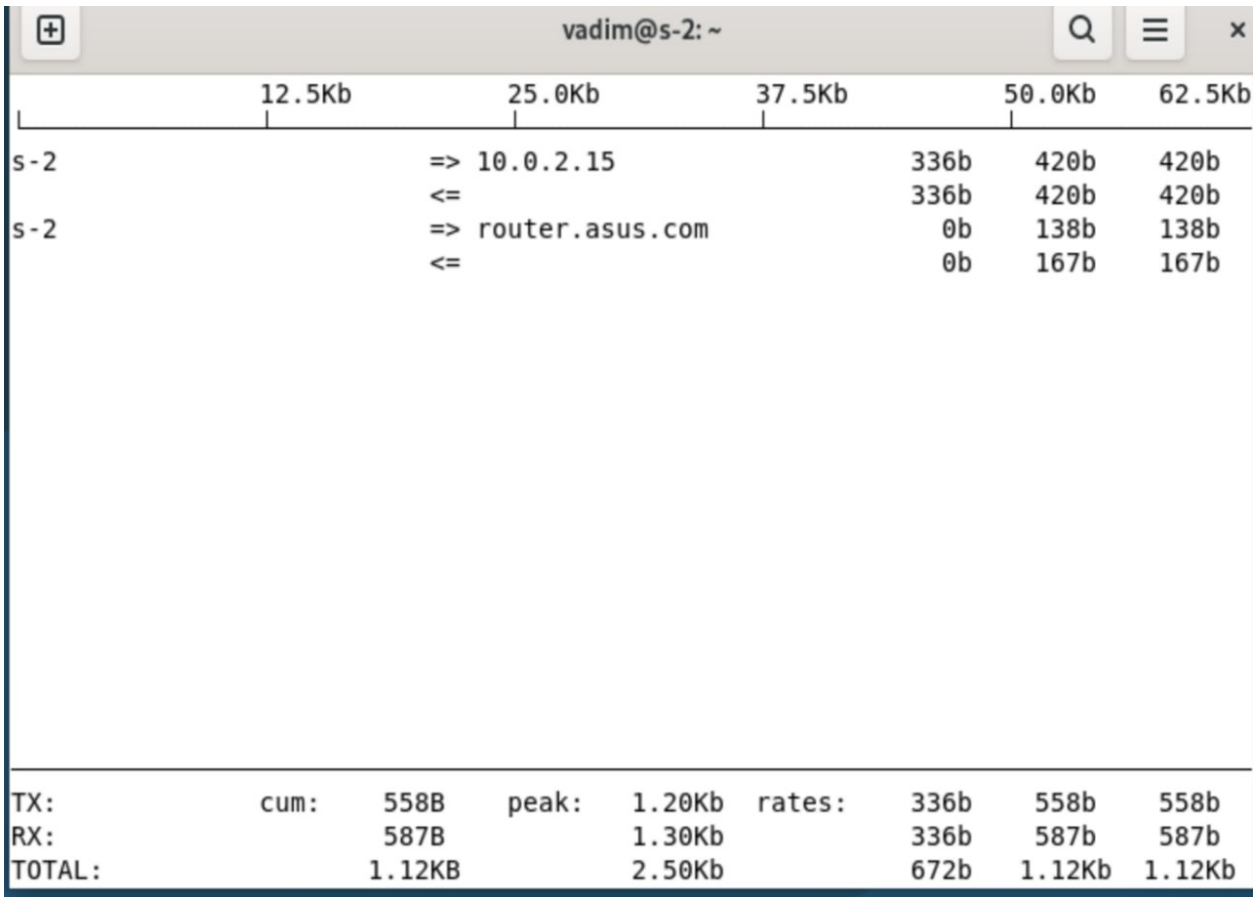
tcpdump



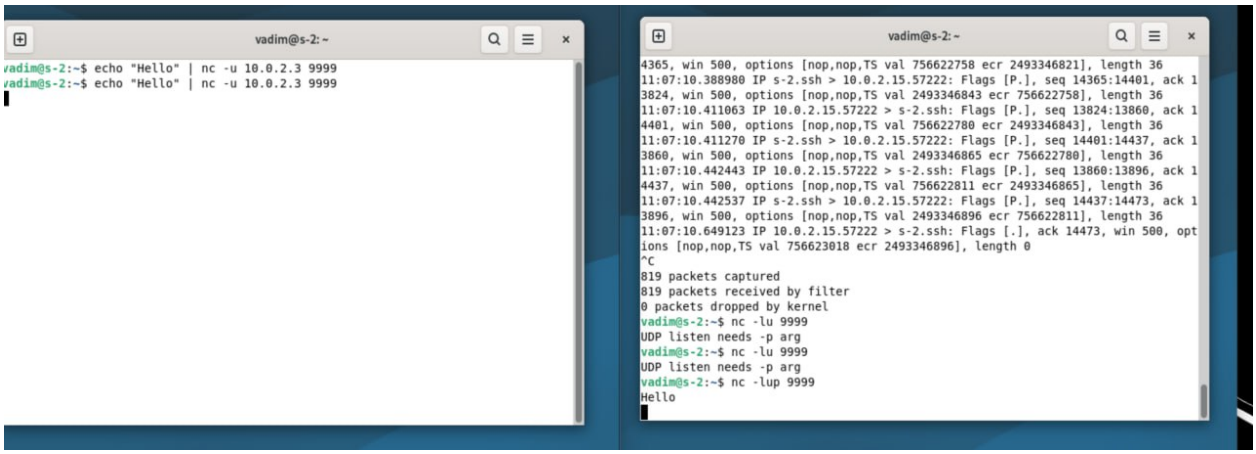
netstat



bmon



Дополнительный мониторинг



Отправим Hello World по SSH

3 Ответы на вопросы и задания

1. **По какому протоколу работает утилита mtr? Как это можно определить?**

   По умолчанию `mtr` в Linux использует **ICMP Echo** (Echo Request/Reply) аналогично `traceroute -I`. Определить можно по захвату `tcpdump/wireshark` (видны ICMP Echo), либо явно переключая режимы `-u` (UDP) и `-T` (TCP) и наблюдая изменение типа пакетов.

2. **Опишите значения столбцов статистики, выводимой утилитой mtr. Какие еще статистики доступны в mtr кроме основных?**
   Базовые столбцы: *Loss%* — потери по хопу; *Snt* — число зондов; *Last* — время последнего ответа; *Avg* — средняя RTT; *Best* — минимальная RTT; *Wrst* — максимальная RTT; *StDev* — стандартное отклонение. Дополнительно доступны отчеты (`-report`, `-report-cycles`), форматы `-json`/`-xml`, отображение `-show-ips`/AS/GeoIP, а также *Jitter* в некоторых сборках.

3. **Какие типы кадров Ethernet бывают, в чем их отличия?**
   Ethernet II (поле EtherType, наиболее распространен); *IEEE 802.3 LLC* (длина + LLC заголовок); *802.3 SNAP* (LLC+SNAP для индикации протокола); *802.1Q VLAN*/QinQ (теги VLAN); служебные кадры типа *PAUSE 802.3x*, *LLDP*. Отличаются форматом полей заголовка и наличием тегов/LLC.

4. **На какие адреса сетевого уровня осуществляются широковещательные рассылки?**
   В IPv4: **255.255.255.255** (ограниченный широковещательный) и **направленный широковещательный** адрес сети (например, 192.168.1.255/24). В IPv6 широковещания нет — используется многоадресная рассылка (`ff00::/8`).

5. **На какой канальный адрес осуществляются широковещательные рассылки?**
   На MAC-адрес **ff:ff:ff:ff:ff:ff**.

6. **Для чего применяются перехваченные широковещательные рассылки в Части 3?**
   Примеры: *ARP Request* (разрешение IP→MAC), *DHCP Discover/Offer* (получение параметров IP-сети), *mDNS/LLMNR/NBNS* (локальное разрешение имён), а также сервисные рассылки (например, *STP/LLDP*). Требовалось определить назначение минимум трёх таких рассылок.

7. **Как изменяется загрузка интерфейса в Части 5. п. 3? Почему?**
   При увеличении размера ICMP-пакета (100→60100 байт) **доля заголовочного оверхеда уменьшается**, а **битовая загрузка** интерфейса при flood растёт до упора в пропускную способность/ограничения ядра; частота пакетов (pps) падает. Итог: использование канала увеличивается примерно пропорционально полезной нагрузке до достижения пределов CPU/линейной скорости.

8. **На каком уровне модели OSI работает vnstat?**
   `vnstat` собирает счётчики интерфейсов из ядра (`/proc/net/dev`), то есть оперирует **на канальном уровне (L2)** независимо от протоколов L3/L4.

4 Использование GAI

Был ли использован в ходе выполнения практической работы GAI (ChatGPT, YandexGPT и др.)?

Да, для помощи в структуре отчета, формулировках теоретических ответов и оформления LaTeX.

Цели использования:

- Подготовка шаблона разделов и заглушек под артефакты
- Вычитка и сжатие теоретических формулировок

Оценка качества ответов моделей:

Качество ответов ChatGPT было высоким. Модель:

- Помогла структурировать материал и сделать листинг более читаемым
- Дала корректные примеры фильтров и ключей для утилит (особенно для wireshark)

5 Рефлексия

Что вы узнали нового из работы? Как, по-вашему, эти знания или навыки могут пригодиться в будущей профессиональной деятельности?

В ходе выполнения данной лабораторной работы я приобрел следующие знания и навыки:

Новые знания:

- Различия между инвентаризацией сокетов (`ss`/`lsof`) и пакетным анализом (`tcpdump`/`tshark`)
- Интерпретация состояний TCP и счетчиков интерфейса
- Подходы к фильтрации трафика с помощью BPF-выражений

Практические навыки:

- Быстрая диагностика «что слушает порт» и «кто держит соединение»
- Прицельный захват и разбор трафика, запись/чтение PCAP
- Анализ пропускной способности и выявление узких мест по интерфейсам

Применение в профессиональной деятельности:

- **Системное администрирование**: оперативная диагностика сетевых инцидентов
- **DevOps/SRE**: воспроизведение проблем, профилирование сетевых зависимостей сервисов
- **Безопасность**: сетевой Threat Hunting и анализ аномалий

6 Список использованных источников

1. man-pages: `ss(8)`, `tcpdump(8)`, `tshark(1)`, `lsof(8)`, `ip-link(8)`, `ethtool(8)`
2. https://www.tcpdump.org/manpages/tcpdump.1.html
3. https://www.wireshark.org/docs/wsug_html_chunked/
4. https://www.kernel.org/doc/Documentation/networking/