ФГБОУ ВО “Чувашский государственный университет им. И. Н. Ульянова” Факультет: ИВТ

Кафедра: Вычислительной техники

Предмет: Сети и телекоммуникации

Лабораторная работа 1

**Создание подсети**

Выполнил: студент группы ИВТ-41-20

Галкин Дмитрий

Проверила: Путевская И.В.

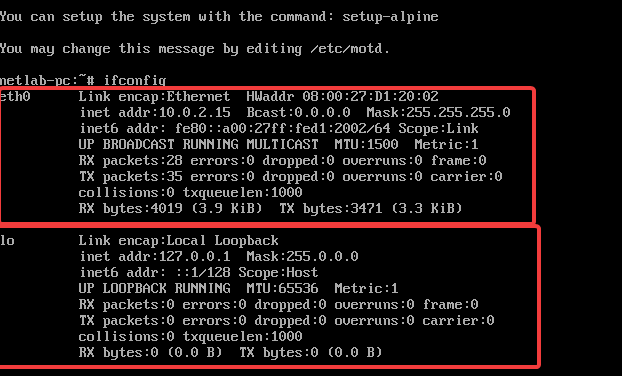
Чебоксары 2023 г.

1. **Анализ сети**

**Цель:** научиться определять настройки сети

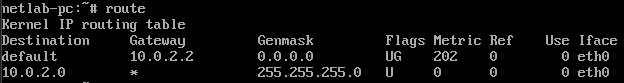
**Задача 1:** изучить ifconfig/ipconfig, arp, route, netstat, ping, traceroute, iftop, ipref, nslookup, wireshark, nmap, whois, ncat, wget.

* ifconfig – Сетевой интерфейс, о котором вы хотите посмотреть информацию или изменить его параметры.
  + up – включить интерфейс
  + down – выключить интерфейс
  + (-)arp – включить или выключить использование протокола ARP для интерфейса
  + (-)promisc – велючить или выключить режим multicast
  + metric – изменить параметр metric
  + mtu – изменить максимальный размер пакета
  + netmask – установить маску сети
  + add – добавить ip адрес для интерфейса
  + del – удалить ip адрес для интерфейса
  + [-]broadcast – установить широковещательный адрес или отключить эту функцию
  + hw – устанвоить MAC адрес для интерфейса
  + txqueuelen – размер очереди интерфейса

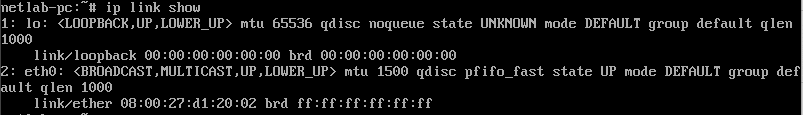




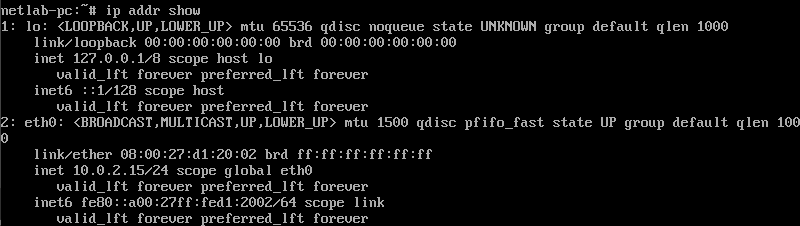
* + route – выводится таблица машрутизации, в достаточно простой форме, которой не всегда достаточно чтобы понять всю суть.



* netstat – печатает сетевых подключений, таблиц машрутизации, статистики интерфейсов.
* link – управляет свойствами сетевого интерфейса
  + -up – устройство подключено и готово принимать, и отправлять фреймы
  + -loopback – интерфейс является локальным и не может взаимодействовать с другими узлами в сети



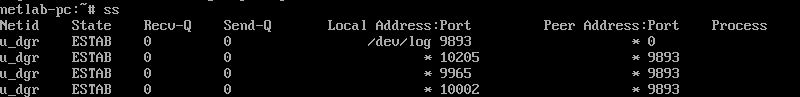
* addr – настройка параметров протокола IP адрес на сетевом интерфейсе



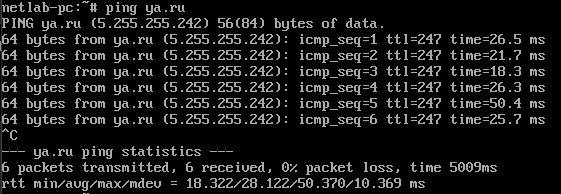
* neigh – управляет ARP-таблицей



* ss – команда для просмотра текущих соединений и открытых портов



* ping – используется для проверки состояния между двумя сетевыми соединениями
  + -4 – использовать только ipv4 (по умолчанию)
  + -6 – использовать только ipv6
  + A – адаптивный режим
  + -b – разрешить ping широковещательного адреса
  + -c – кол-во пакетов, которые нужно отправить
  + -s – размер одного пакета
  + -t – установить TTL вручную
  + -v – более подробный вывод



packets transmitted – отправлено пакетов

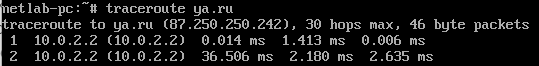
received – получено пакетов

packet loss – процент потерянных пакетов

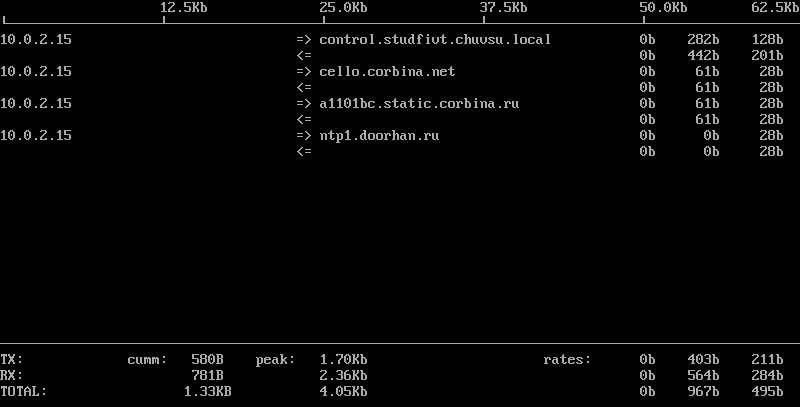
time – общее время работы

rtt min/avg/max/mdev – минимальное время/среднее время/максимальное время/квадратичное отклонение

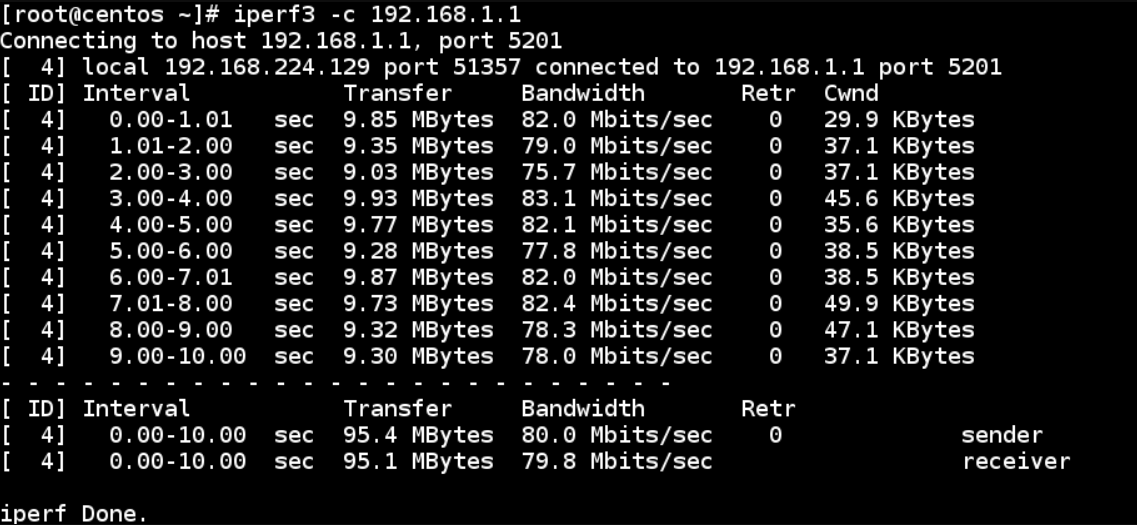
* traceroute – это служебная компьютерная программа, предназначенная для определения машрутов следования данных в сетях TCP/IP
  + -4 или -6 – использовать ipv4 или ipv6 протокол
  + -l – использовать ICMP пакетов вместо UDP
  + -F – не фрагментировать пакеты
  + -f – указать TTL с которого нужно начать
  + -g – передать пакет через уникальный шлюз
  + -i – передать пакет через указанный интерфейс
  + -m – максимальное кол-во узлов, через которые пройдет пакет
  + -q – кол-во пакетов, отправляемых за раз, по умолчанию 3
  + -n – не узнавать доменные имена
  + -p – указать порт вместо порта по умолчанию
  + –mtu – указать размер пакета



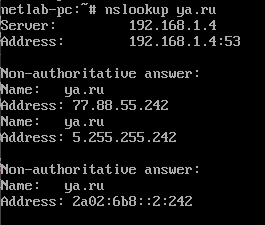
* iftop – инструмент мониторинга пропускной способности сети в режиме реального времени



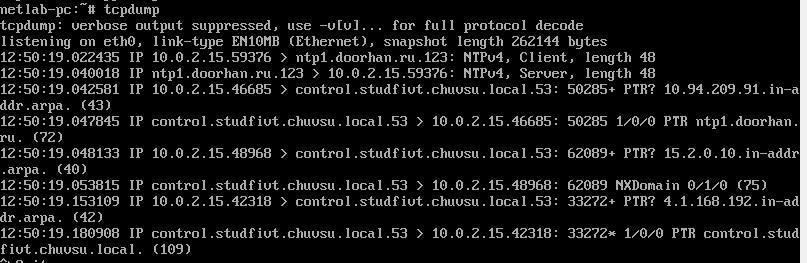
* iperf – предназначена для тестирования пропускной способности сети между двумя узлами. Позволяет генерировать нагрузочной TCP и UDP трафик между хостами.



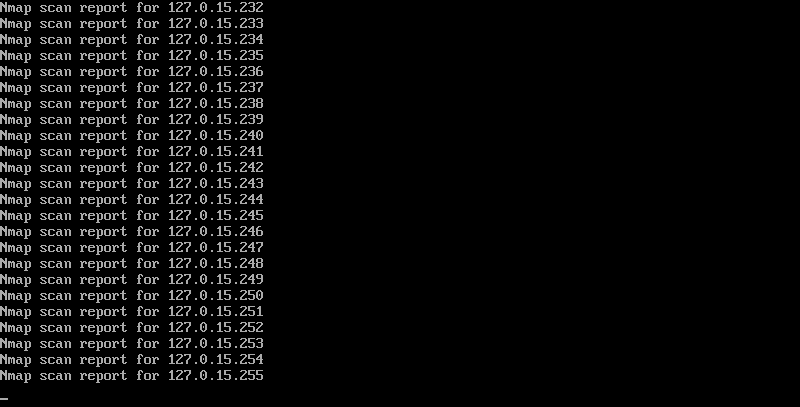
* nslookup – представляет пользователю интерфейс командной строки для обращения к системе DNS
  + -type – тип информации, которую хотим получить
  + -port – другой порт DNS сервера
  + -recurse – использовать другие DNS серверы, если на этом нет ответа
  + -retry – кол-во попыток получить нужную информацию
  + -timeout – время между попытками запросов к серверу
  + -fail – пробовать другой сервер имен, если этот вернул ошибку



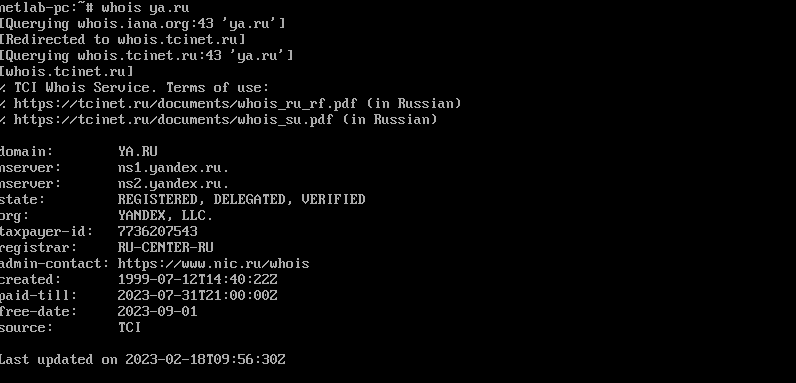
* tcpdump – мощный инструмент для перехвата и анализа сетевых пакетов. Позволяет просматривать все входящие и исходящие из определенного интерфейса пакеты и работает в командной строке.
  + -A – выводит все пакеты в формате ASCII
  + -c – закрыть программу после перехвата n-ого кол-ва пакетов
  + -D – выводит список доступных сетевых интерфейсов
  + -f – выводить доменное имя для ip адресов
  + -F – читать пакеты из файла, а не интерфейса
  + -q – выводит минимум информации



* nmap – предназначена для разнообразного настраиваемого сканирования IP-сетей с любым кол-вом объектов, определения состояния объектов сканируемой сети (портов и соответствующих им служб)
  + sL – просто создать список работающих хостов, но не сканировать порты nmap
  + -sP – только проверять доступен ли хост с помощью ping
  + -O – определять операционную систему
  + -p – указать диапазон портов для проверки
  + -S – изменить свой IP адрес на указанный



* whois – отображает полную информацию о том, кто владеет интернет-доменом



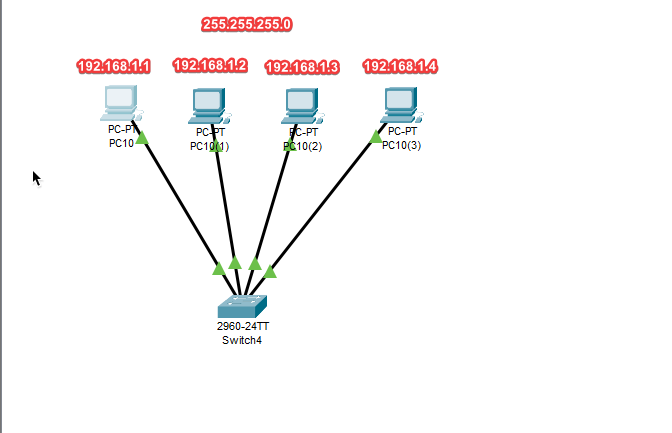
* ncat – многофункциональная утилита, которая считывает и записывает данные в сети из командной строки.
  + -4 – только IPv4
  + -6 - только IPv6
  + -U – использовать доменные сокеты Unix
  + -u – использовать UDP
  + –stcp – использовать SCTP
  + -v – подобный режим. Используется при сканировании портов
  + -z – отключить отправку данных. Используется при сканировании портов
  + -n – Работать с IP-адресами напрямую, не задействует DNS, также отключить поиск портов
  + -l – режим прослушивания. Используется с указанием порта

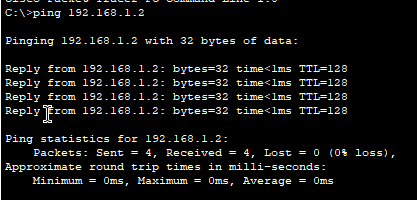


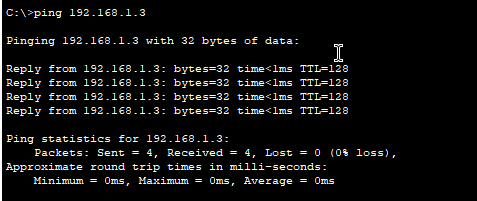
* wget – загрузка файлов из интернета
  + -v – вывод версии программы
  + -h – вывести справку
  + -c – продолжить ранее прерванную загрузку
  + -l – глубина при рекурсивным сканировании
  + -d – включить режим отладки

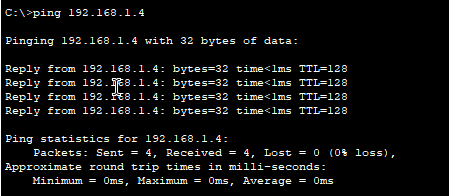


**Задача 2:** построить схему сети в эмуляторе (cisco packettracer)









**Ответы на вопросы:**

1. Для чего используется wget?

Способ загрузки файлов из интерната, посредство url адреса

1. Как правильно остановить ping?

Нажатием на комбинацию клавиш Ctrl+C

1. Как получить сетевые параметры компьютера?

Ввести ifconfig в консоли

1. Какие сетевые данные можно собрать локально, удаленно?

С открытых портов, запущенных служб, о версии операционной системы.

1. Как собрать данные о внешних сетях?

Данные о внешней сети можно получить через команду nmap

1. Чем логическая топология отличается от физической?

Логическая топология делает упор на способ передачи между сетевыми узлами, а не на физическую схему пути, по которому следует.

1. Зачем нужна схема сети?

Потому что графическим путем видно каким образом размещены компоненты сети и как они между собой взаимодействуют

1. Что содержит схема сети?

Содержит компоненты сети, средства взаимодействия (устройства, концентраторы)

1. Какие стандарты обозначений сетевого оборудования существуют?

ISO – Международная организация по стандартизации

W3C – Веб-стандарты

IAB – Протоколы интернета

IEEE – Технология передачи информации