

Сетевые ВОЗМОЖНОСТИ Linux

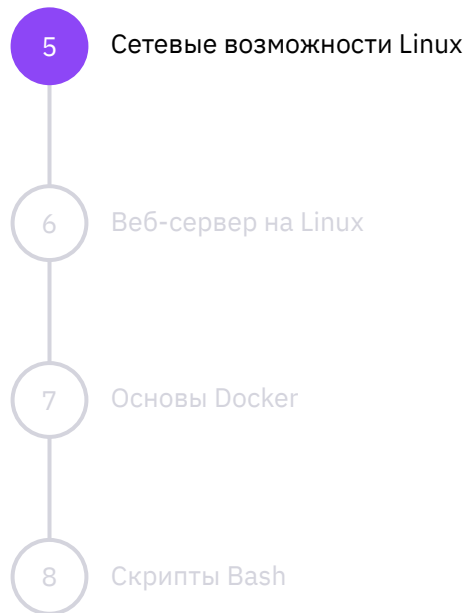
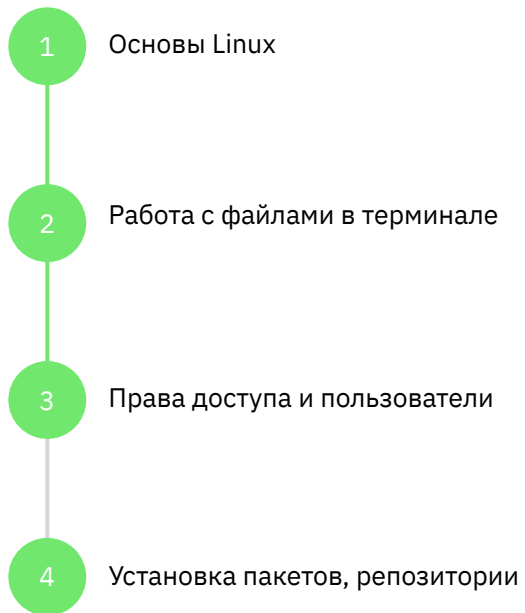




Содержание урока







План курса





Что будет на уроке сегодня

-  Узнаем, как устроена работа с сетью
-  Научимся настраивать сетевые интерфейсы
-  Узнаем, как можно диагностировать проблемы
-  Научимся настраивать фильтрацию пакетов



Сетевая подсистема в Linux

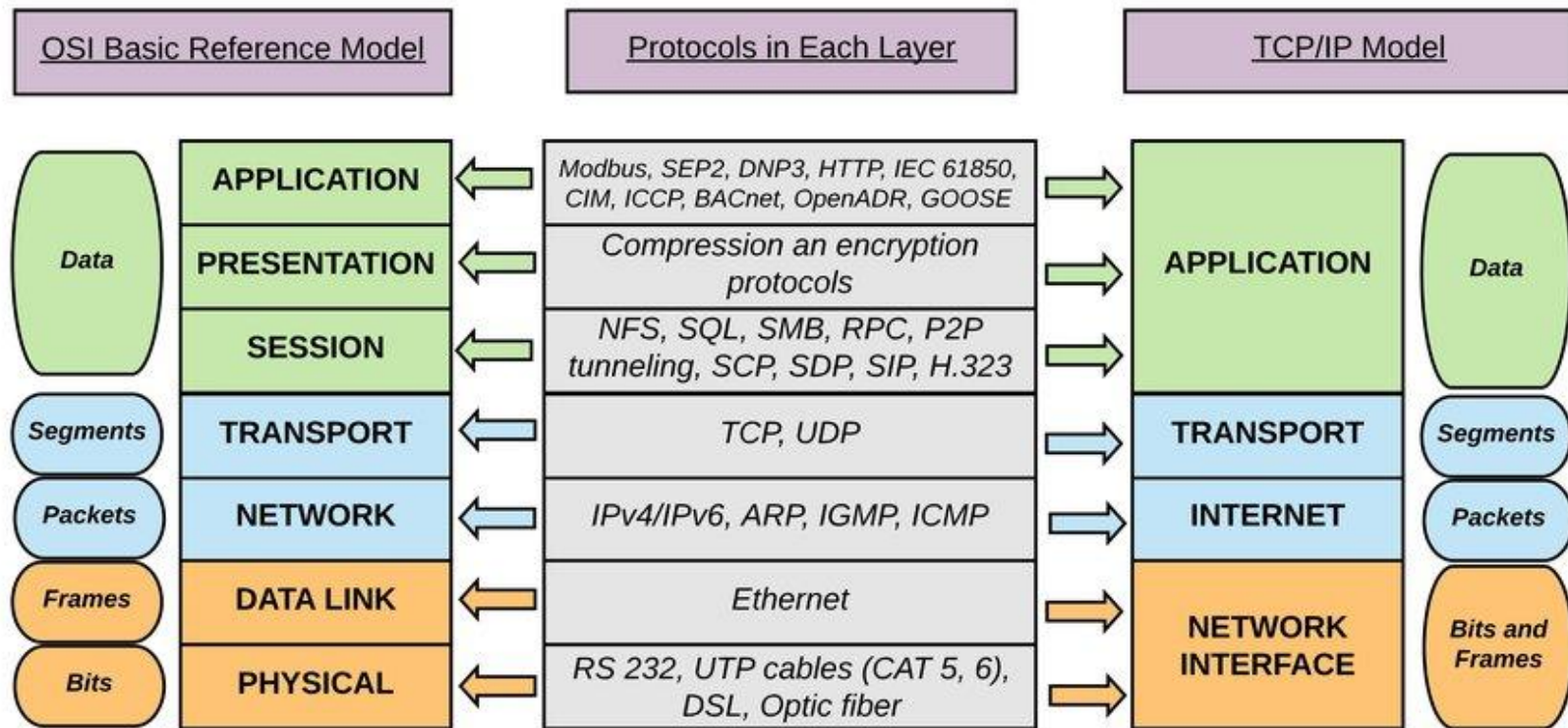


Архитектура сетевой подсистемы





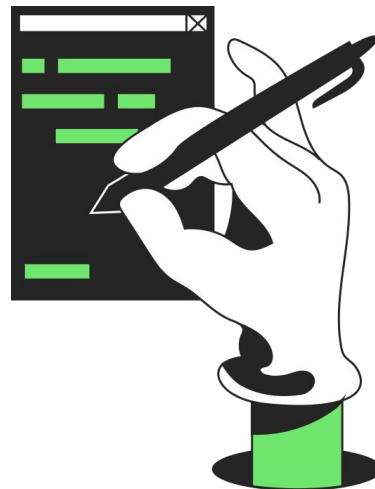
Сетевые уровни и протоколы





Сетевые интерфейсы и команда ip

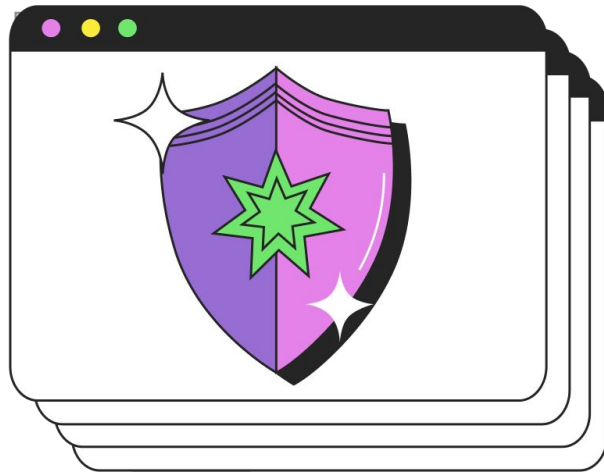
- `ip a` – список всех интерфейсов
- `ip -s a` – показ статистики
- `ip -c -s a` – включение подсветки
- `ip a show enp0s3` – данные по одному интерфейсу
- `ip link show enp0s3` – данные уровня L2 (link)
- `ip r` – просмотр информации о маршрутах





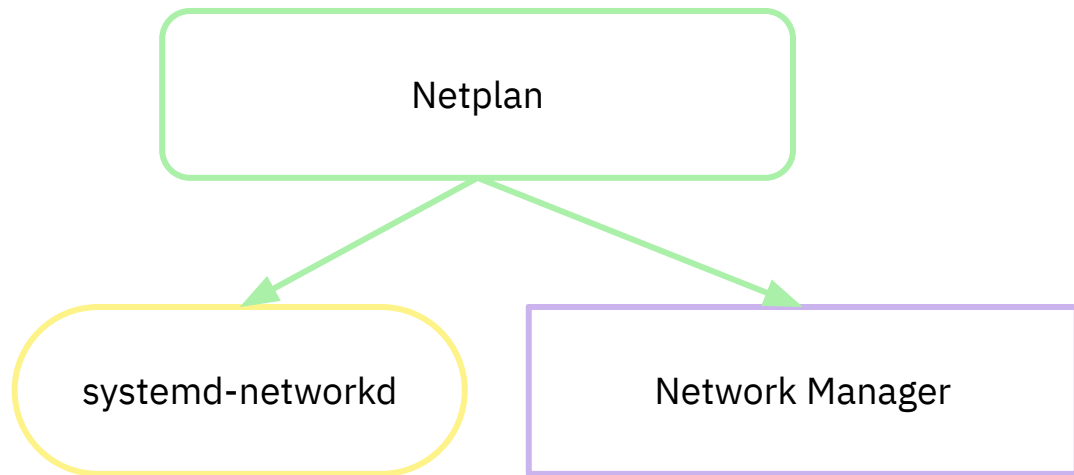
Сокеты и порты

- `ss - socket stat`
- `ss -ntlp` – TCP-сокеты в состоянии `LISTEN`
- `ss -ntulp` – TCP и UDP-сокеты в состоянии `LISTEN`
- `ss -tulpan` – Все TCP и UDP-сокеты

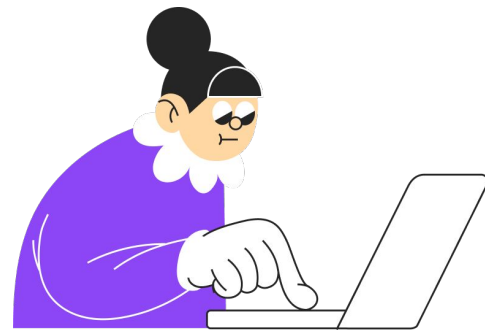




Конфигурация сети в Ubuntu



<https://netplan.io/>

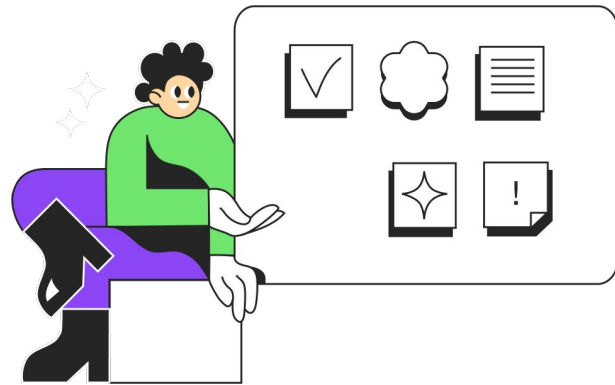




Netplan

- `/etc/netplan/*.yaml` – конфигурационные файлы
- `netplan try` – тестирование и применение конфигурации
- `netplan apply` – применение конфигурации
- Конфигурация по умолчанию:

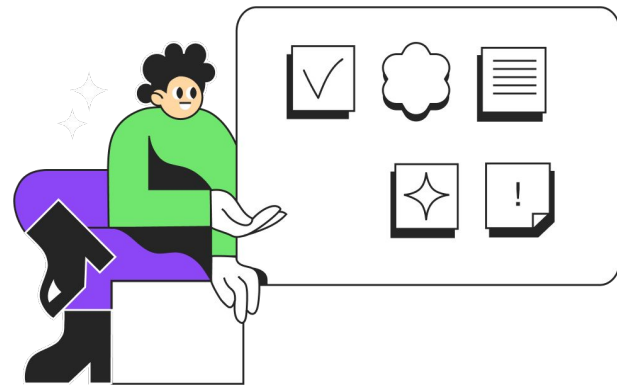
```
# Let NetworkManager manage all devices on this system
network:
  version: 2
  renderer: NetworkManager
```





Netplan – конфигурация с DHCP

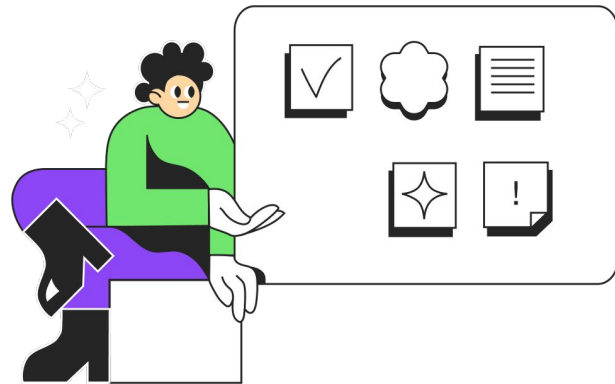
```
network:  
  version: 2  
  renderer: networkd  
  ethernets:  
    enp0s3:  
      dhcp4: yes  
      nameservers:  
        addresses:  
          - 8.8.8.8  
          - 8.8.4.4
```





Netplan – статическая конфигурация

```
network:  
  version: 2  
  renderer: networkd  
  ethernets:  
    enp0s3:  
      dhcp4: no  
      addresses: [192.168.0.8/24]  
      gateway4: 192.168.0.1  
      nameservers:  
        addresses:  
          - 8.8.8.8  
          - 8.8.4.4
```





Диагностика сети

- `ping 8.8.8.8` – доступность хоста (ICMP протокол)
- `ping ya.ru` – проверка DNS и доступности
- `host -t a yandex.ru` – проверка DNS
- `host -t a yandex.ru 8.8.8.8` – другой DNS-сервер
- `dig @8.8.8.8 google.com` – подробная информация по DNS
- `tracert ya.ru` – просмотр маршрута прохождения пакетов
- `tracert ya.ru` – альтернатива
- `mtr ya.ru` – постоянный мониторинг доступности хостов

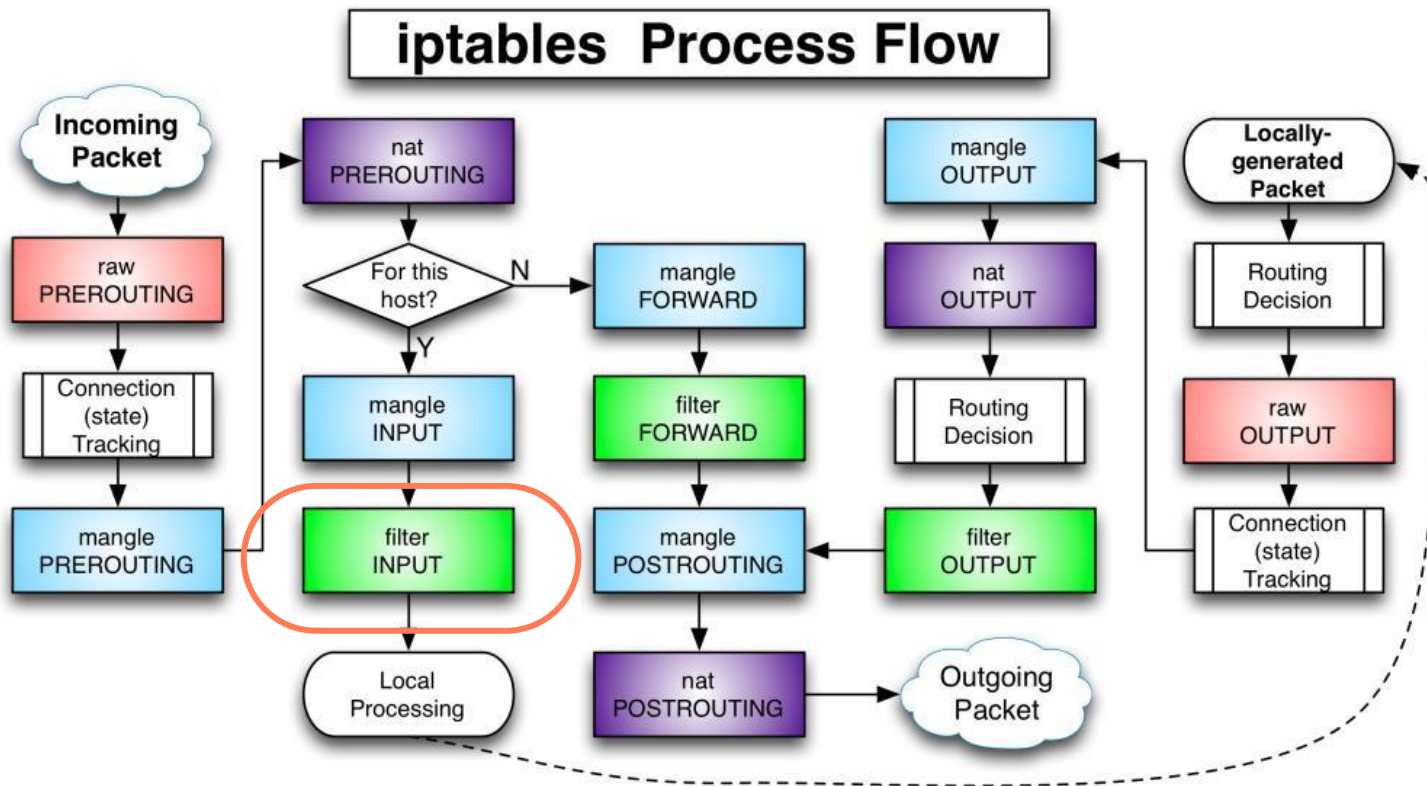




Фильтрация пакетов

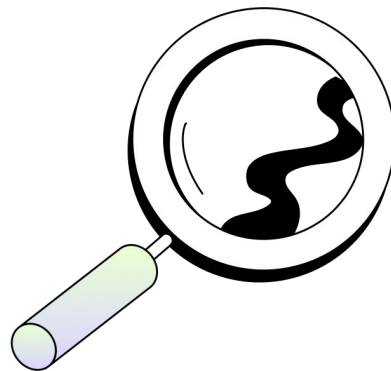


Путь пакета в ядре





Правила фильтрации



- Просмотр таблицы
 - `iptables -L -nv`
 - `iptables -L -nv -t nat`
- Политика по умолчанию
 - `iptables -P INPUT DROP`
- Добавление правил
 - `iptables -A INPUT -p tcp --dport 80 -j ACCEPT`
 - `iptables -I INPUT -p tcp --dport 80 -j ACCEPT`
 - `iptables -A INPUT -p tcp -s 192.168.0.100 --dport 80 -j DROP`
- Удаление правил
 - `iptables -D INPUT 3`
 - `iptables -D INPUT -p tcp --dport 80 -j ACCEPT`
- Сброс правил
 - `iptables -F`



Пример конфигурации сервера

```
# SSH allow
iptables -A INPUT -p tcp --dport=22 -j ACCEPT
# HTTP, HTTPS allow
iptables -A INPUT -p tcp -m multiport --dport 80,443 -j ACCEPT
# loopback allow
iptables -A INPUT -i lo -j ACCEPT
# ICMP
iptables -A INPUT -p icmp -j ACCEPT
# established connections allow
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
# policy drop
iptables -P INPUT DROP
```





Перенаправление портов

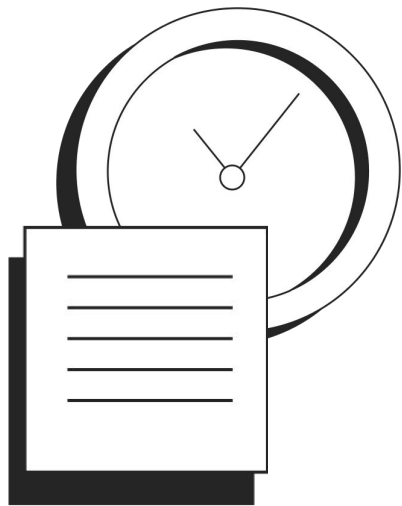
- Редирект с 80 на 8080 порт (TCP):
 - `iptables -t nat -I PREROUTING -p tcp --dport 80 -j REDIRECT --to-port 8080`
- Проверка:
 - `iptables -L -nv -t nat`





Сохранение конфигурации iptables

- Сохранение и восстановление из файла
 - `iptables-save > iptables.rules`
 - `iptables-restore < iptables.rules`
- Сервис `netfilter-persistent`
 - `apt install iptables-persistent netfilter-persistent`
 - `netfilter-persistent save`
 - Конфигурация в `/etc/iptables`





Итоги занятия

На этом уроке мы

- 📌 Посмотрели на реализацию сетевой подсистемы
- 📌 Научились настраивать сетевые интерфейсы
- 📌 Узнали, как можно протестировать сеть
- 📌 Разобрали настройку межсетевого экрана с iptables
- 📌 Научились сохранять конфигурацию правил iptables





Спасибо за внимание!