Домашняя работа №5:

1. Настроить статическую конфигурацию (без DHCP) в Ubuntu через ip и netplan. Настроить IP, маршрут по умолчанию и DNS-сервера (1.1.1.1 и 8.8.8.8). Проверить работоспособность сети.

Заходим в директорию:

cd /etc/netplan

Смотрим какие файлы есть в директории:

ls -al

Открываем файл с расширением .yaml. В моем случае это 01-network-manager-all.yaml.
Для постоянной конфигурации сети в Ubuntu используется специальная утилита netplan. Файл 01-network-manager-all.yaml. “хранит” ее настройки.

Открываем файл и вносим следующие изменения:

```
network:
  version: 2
  renderer: networkd
  ethernets:
    enp0s3:
      dhcp4: no
      addresses: [192.168.0.8/24]
      routes:
        - to: default
          via: 192.168.0.254
      nameservers:
        addresses:
          - 8.8.8.8
          - 1.1.1.1
```

Проверяем все ли работает:

ping ya.ru

ya.ru – точно ответит

Примечание к решению:

Конфигурация по умолчанию для Ubuntu Desktop:

```
network:
  version: 2
  renderer: NetworkManager
```

version — версия YAML. На момент обновления статьи, была 2.

YAML — это язык для хранения информации в формате понятном человеку. Его название расшифровывается как, «Ещё один язык разметки». Однако, позже расшифровку изменили на — «YAML не язык разметки», чтобы отличать его от настоящих языков разметки.

renderer — менеджер сети (networkd или NetworkManager).

ethernets — настройка сетевых адаптеров ethernet.

enp0s3 — настройки для сетевого адаптера.

dhcp4 — будет ли получать сетевой адаптер IP-адрес автоматически. Возможны варианты yes/true — получать адрес автоматически; no/false — адрес должен быть назначен вручную.

addresses — задает IP-адреса через запятую.

routes — настройка маршрутов.
to — направление маршрута (в какую сеть мы должны попадать).
via — через какой шлюз мы попадаем в сеть to.

Выяснить через какой шлюз попадаем в сеть можно по средством: ip route

Для шлюза по умолчанию используем опцию и значение to: default.

via — через какой шлюз мы попадаем в сеть to.

nameservers — настройка серверов имен (DNS).

addresses — указываем серверы DNS.

Через ip:

sudo ip addr add 192.168.0.9/255.255.255.0 broadcast 192.168.0.255 dev enp0s3

sudo ip addr add 192.168.0.1/24 broadcast 192.168.0.255 dev enp0s3

вообще достаточно:

sudo ip addr add 192.168.0.1/24 dev enp0s3

Добавляем следующий ip адрес 192.168.0.9/24 где /24 - число бит в префиксной части адреса (соответствует маске подсети 255.255.255.0), а enp0s3 - подключаемый сетевой интерфейс.

broadcast добавляет широковещательный адрес

широковещательный адрес — условный (не присвоенный никакому устройству в сети) адрес, который используется для передачи широковещательных пакетов в компьютерных сетях.

Добавить маршрут по умолчанию (default gateway):

sudo ip route add default via 192.168.0.254

Примечание: После перезагрузки все настройки слетят!

Проверяем все ли работает:

ping ya.ru

2 Настроить правила iptables для доступности сервисов на TCP-портах 22, 80 и 443. Также сервер должен иметь возможность устанавливать подключения к серверу обновлений. Остальные подключения запретить.

Netfilter — встроенный в ядро Linux сетевой фильтр. Для управления netfilter служит утилита iptables. Основа iptables — таблицы, в которых содержатся цепочки с правилами

Правила в цепочках создаются следующим образом:
iptables -A имя_цепочки -p протокол --dport порт -j действие

iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -p TCP --dport 22 -j ACCEPT
iptables -A INPUT -p TCP --dport 80 -j ACCEPT
iptables -A INPUT -p TCP --dport 443 -j ACCEPT
iptables -A INPUT -m state --state ESTABLISHED, RELATED -j ACCEPT
iptables -I INPUT DROP

lo (loopback device) – виртуальный интерфейс, присутствующий по умолчанию в любом Linux. Он используется для отладки сетевых программ и запуска серверных приложений на локальной машине

Для чего нужен Loopback ?
В телекоммуникациях loopback (коротко говоря loop) — это аппаратный или программный метод, который направляет полученный сигнал или данные обратно отправителю. Он используется как дополнительное средство в исправлении проблем физического соединения.

established, related, untracked − данное правило разрешает прохождение пакетов, отправленных на маршрутизатор (input) со всех интерфейсов (LAN,WAN) с состоянием connection-state - established, related, untracked.
Оно означает, что пакет будет обработан и пропущен этим правилом дальше только в том случае, если пакет относится к уже установленным (established), зависимым (related) или не отслеживаемым (untracked) соединениям.

-A означает append, то есть добавление правила в конец списка
INPUT — для входящих пакетов, адресованных непосредственно локальному процессу (клиенту или серверу)

3 Запретить любой входящий трафик с IP 3.4.5.6

iptables -I INPUT -s 3.4.5.6 -j DROP

-I - добавления правила в начало списка нужно использовать параметр.
INPUT — для входящих пакетов, адресованных непосредственно локальному процессу (клиенту или серверу)
-s — источник
DROP — выбросить пакет без уведомления отправителя

4 Запросы на порт 8090 перенаправлять на порт 80 (на этом же сервере).

iptables -t nat -I PREROUTING -p tcp --dport 80 -j REDIRECT --to-port 8090

В этой команде мы видим новое действие REDIRECT, которое как раз отвечает за перенаправление портов. В правиле мы работаем с таблицей nat, цепочкой PREROUTING.

5 Разрешить подключение по SSH только из сети 192.168.0.0/24.

Запрещаем подключение всем к SSH:

iptables -I INPUT -p TCP --dport 22 -j DROP

Разрешаем подключение к SSH только 192.168.0.0/24:

iptables -I INPUT -p TCP --dport 22 -s 192.168.0.0/24 -j DROP