

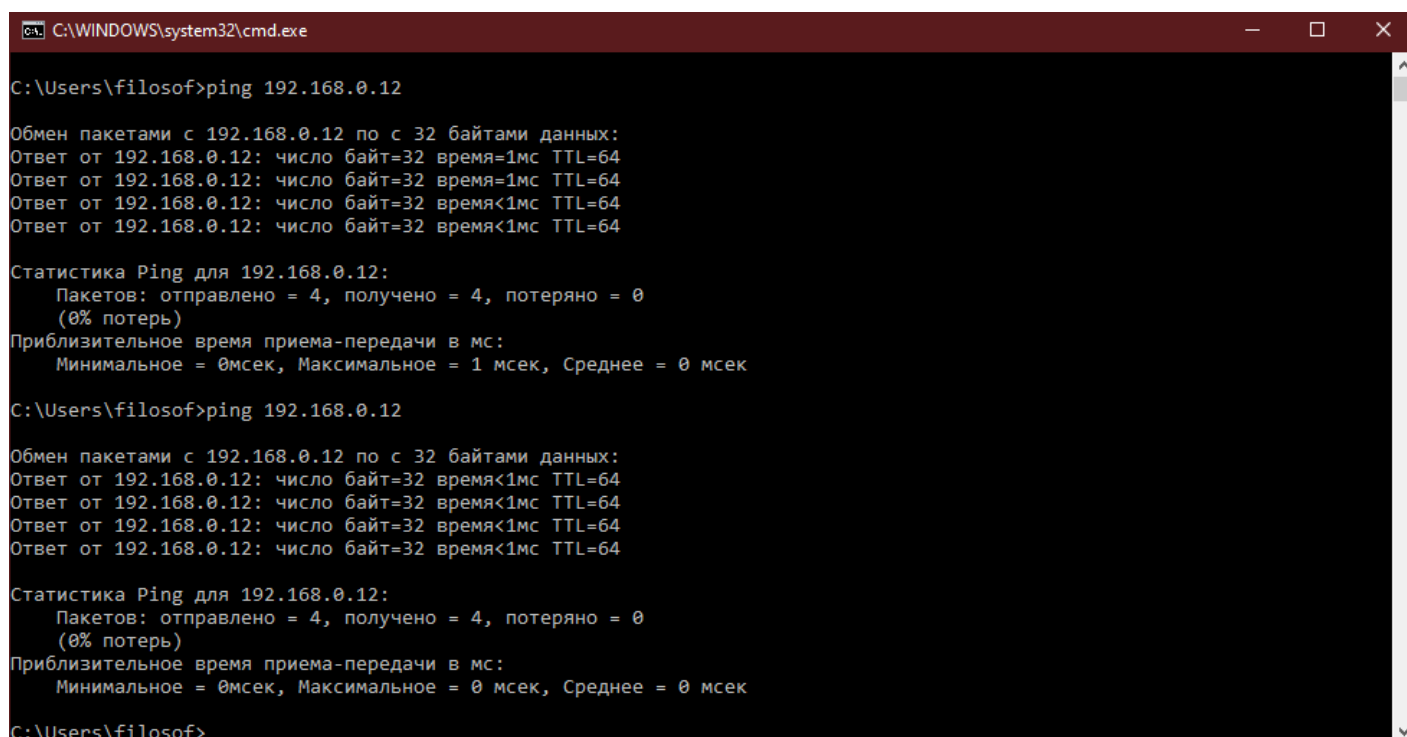
# Операционные системы и виртуализация (Linux) (семинары)

## Урок 5. Настройка сети в Linux. Работа с IPtables

### Задание

- 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.



```
C:\WINDOWS\system32\cmd.exe
C:\Users\filosof>ping 192.168.0.12

Обмен пакетами с 192.168.0.12 по 32 байтами данных:
Ответ от 192.168.0.12: число байт=32 время=1мс TTL=64
Ответ от 192.168.0.12: число байт=32 время=1мс TTL=64
Ответ от 192.168.0.12: число байт=32 время<1мс TTL=64
Ответ от 192.168.0.12: число байт=32 время<1мс TTL=64

Статистика Ping для 192.168.0.12:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 1 мсек, Среднее = 0 мсек

C:\Users\filosof>ping 192.168.0.12

Обмен пакетами с 192.168.0.12 по 32 байтами данных:
Ответ от 192.168.0.12: число байт=32 время<1мс TTL=64
Ответ от 192.168.0.12: число байт=32 время<1мс TTL=64
Ответ от 192.168.0.12: число байт=32 время<1мс TTL=64
Ответ от 192.168.0.12: число байт=32 время<1мс TTL=64

Статистика Ping для 192.168.0.12:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек

C:\Users\filosof>
```

- 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.
- Запретить любой входящий трафик с IP 3.4.5.6.
- Запросы на порт 8090 перенаправлять на порт 80 (на этом же сервере).
- Разрешить подключение по SSH только из сети 192.168.0.0/24.

### Решение

Адрес роутера `ip -c r`

Адрес хоста `ip -c a`

Отредактируем конфигурационный файл netplan (Важны отступы):

```
sudo nano /etc/netplan/01-network-manager-all.yaml
```



## 01-network-manager-all.yaml:

```
15 version: 2
16 renderer: NetworkManager
17 ethernets:
18   enp0s3:
19     dhcp4: no
20     addresses: [192.168.0.12/24] #Адрес хоста
21     routes:
22       - to: default
23       via: 192.168.0.1 #Адрес роутера
24     nameservers:
25       addresses:
26         - 1.1.1.1
27         - 8.8.8.8
```

Применение изменений:

```
sudo netplan apply
```

Проверка работоспособности:

```
tracertpath gb.ru
```

```
[13:01:15]
/home/afilosofof
tracertpath gb.ru
1?: [LOCALHOST] pmtu 1500
1: _gateway 1.228ms
1: _gateway 1.079ms
2: 192.168.101.1 3.062ms
3: atlant.naukanet.ru 15.596ms asymm
4: atlant.naukanet.ru 30.299ms asymm
5: 87-245-229-94.retn.net 16.221ms asymm
6: ae2-6.RT.OK.MSK.retn.ru 23.767ms asymm
7: 139.45.226.166 23.874ms asymm
8: no reply
9: no reply
10: no reply
11: no reply
NC
```

## Просмотр правил

```
sudo iptables -L
```

## Настройка правил iptables

```
sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT  
  
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT  
  
sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT  
  
sudo iptables -A OUTPUT -p tcp --dport 80 -j ACCEPT  
  
sudo iptables -A OUTPUT -p tcp --dport 443 -j ACCEPT
```



- Запретить любой входящий трафик с IP 3.4.5.6.

Запрет остальных соединений. Перед политикой отрабатываются правила, сверху вниз. -A добавление с конца списка (add) -I добавление в начало списка (input)

```
sudo iptables -P INPUT DROP  
  
sudo iptables -A INPUT -s 3.4.5.6 -j DROP
```



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

```
sudo iptables -t nat -A PREROUTING -p tcp --dport 8090 -j REDIRECT --to-port 80
```



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

```
sudo iptables -A INPUT -p tcp -s 192.168.0.0/24 --dport 22 -j ACCEPT
```



## Stack:

```
sudo nano /etc/netplan/

ip a

sudo nano /etc/netplan/

sudo nano /etc/netplan/01-network-manager-all.yaml

sudo netplan apply

sudo nano /etc/netplan/01-network-manager-all.yaml

sudo netplan apply

sudo nano /etc/netplan/01-network-manager-all.yaml

sudo netplan apply

sudo nano /etc/netplan/01-network-manager-all.yaml

sudo netplan apply

ip a

ip

sudo nano /etc/netplan/01-network-manager-all.yaml

sudo netplan apply

sudo nano /etc/netplan/01-network-manager-all.yaml

sudo netplan apply

ping gb.ru

ping ya.ru

exit

ping 192.168.0.233

sudo nano /etc/netplan/01-network-manager-all.yaml

sudo netplan apply

ping 192.168.0.1

tracert gb.ru

sudo iptables -L

clear

sudo iptables -L

sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
```

```
sudo iptables -L

sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT

sudo iptables -L

sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT

sudo iptables -L

sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT

sudo iptables -A OUTPUT -p tcp --dport 80 -j ACCEPT

sudo iptables -A OUTPUT -p tcp --dport 443 -j ACCEPT

sudo iptables -L

sudo iptables -P INPUT DROP

sudo iptables -L

sudo iptables -A INPUT -s 3.4.5.6 -j DROP

sudo iptables -L

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

sudo iptables -L

sudo iptables -A INPUT -p tcp -s 192.168.0.0/24 --dport 22 -j ACCEPT

exit
```