

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФГБОУ ВО АЛТАЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Институт цифровых технологий, электроники и физики (ИЦТЭФ)
Кафедра вычислительной техники и электроники (ВТиЭ)

Лабораторная работа № 01

Стек TCP/IP. Сетевые утилиты операционных систем.

Выполнили: студенты 595 гр.

_____ А.В. Осипов

_____ А.В. Лаптев

_____ А.Е. Половинкин

_____ Н.А. Кротов

Проверил: доцент кафедры ВТиЭ

_____ А.В. Калачёв

Лабораторная работа защищена

«___»___сентября_____2022 г.

Оценка _____

1. Постановка задачи

- 1.1. Настроить на 2-4 выбранных компьютерах статические IP адреса в диапазоне 192.168.1.* с маской подсети 255.255.255.0;
- 1.2. при помощи коммутатора и сетевых кабелей соединить ПК с настроенными адресами в сеть;
- 1.3. ознакомиться со способами и параметрами запуска основных сетевых утилит операционных систем: что возвращают, какие ключи имеют, как работают при наличии/отсутствии сети (подключения ПК к коммутатору).

2. Настройка сети

2.1. Физическое соединение компьютеров

Группой было произведено соединение четырёх персональных компьютеров под управлением операционных систем Windows и Debian Linux. Соединение происходило посредством проводного сетевого интерфейса Ethernet и коммутатора. С учётом требований задания было решено присвоить компьютерам следующие IP-адреса:

- ◆ Половинкин: 192.168.1.1
- ◆ Лаптев: 192.168.1.2
- ◆ Кротов: 192.168.1.3
- ◆ Осипов: 192.168.1.4

2.2. Настройка соединения в ОС Windows

Настройка IP-адреса в ОС Windows производилась с помощью пункта «Сетевые подключения» в панели управления. Для этого необходимо открыть данный пункт, выбрать текущий сетевой адаптер и открыть пункт «Свойства» в его контекстном меню. В «Свойствах» содержатся параметры различных сетевых протоколов, включая TCP/IP. Для их изменения необходимо нажать кнопку «Свойства», после чего откроется окно настройки.

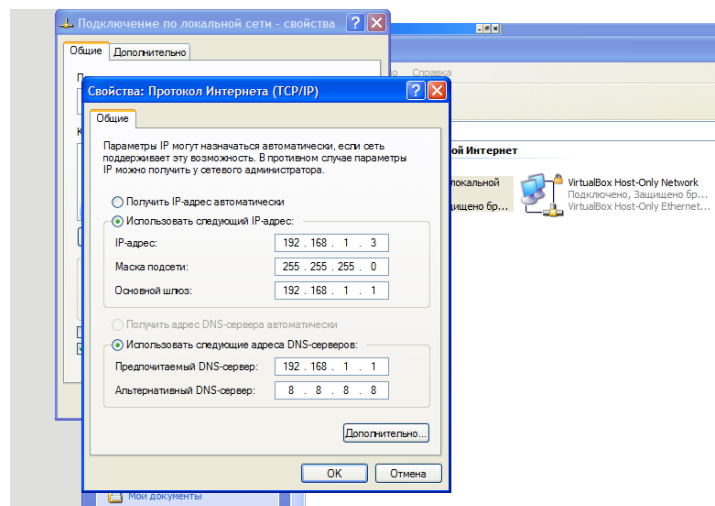
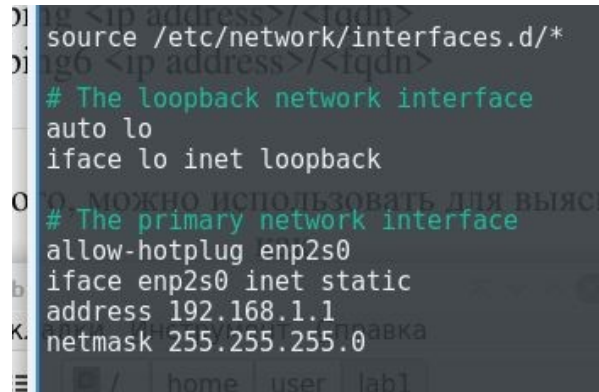


Рис. 1.1. Окно настройки протокола TCP/IP в ОС Windows

В открывшемся окне необходимо включить режим статического IP-адреса и указать его вместе с маской подсети. При включении статической IP-адресации необходимо также вручную указать адрес основного и дополнительного DNS-серверов. Для работы с другими узлами сети необходимо также отключить брандмауэр или разрешить в нём работу в указанной сети, иначе он будет блокировать пакеты, приходящие к нему по сети.

2.3. *Настройка соединения в ОС Linux*

Для ОС на основе ядра Linux существует несколько вариантов настройки параметров сети, однако самым универсальным является редактирование конфигурационного файла `/etc/network/interfaces`, хранящего настройки всех сетевых интерфейсов. Обычно Ethernet-карта со стандартной конфигурацией автоматически добавляется в этот файл, однако эту конфигурацию можно изменить с помощью любого текстового редактора, запущенного от имени пользователя `root`. В качестве примера подойдёт встроенный в Debian консольный текстовый редактор Nano. Перед редактированием необходимо узнать имя редактируемого интерфейса с помощью команды `ip -a` и отключить его.



```

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug enp2s0
iface enp2s0 inet static
address 192.168.1.1
netmask 255.255.255.0

```

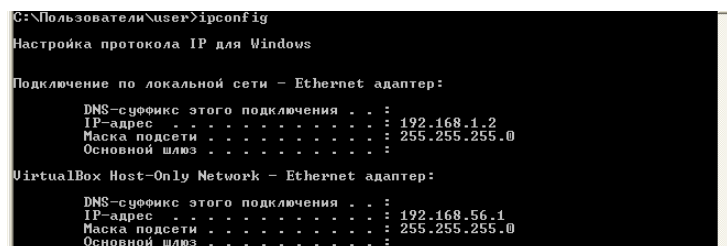
Рис. 1.2. Содержание настроенного файла /etc/network/interfaces в редакторе Nano

В содержании файла необходимо найти строку «iface <интерфейс> inet dhcp» и заменить последнее слово на «static». Следом необходимо строчки «address <IP-адрес>» и «netmask 255.255.255.0», которые указывают IP-адрес компьютера и маску подсети.

3. Проверка сетевых команд в ОС Windows

3.1. IPConfig

Команда IPConfig выводит в консоль информацию о текущих сетевых настройках во всех активных сетях.



```

C:\Пользователи\user>ipconfig

Настройка протокола IP для Windows

Подключение по локальной сети - Ethernet адаптер:

    DNS-суффикс этого подключения . . . : 
    IP-адрес . . . . . : 192.168.1.2
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз . . . . . : 

VirtualBox Host-Only Network - Ethernet адаптер:

    DNS-суффикс этого подключения . . . : 
    IP-адрес . . . . . : 192.168.56.1
    Маска подсети . . . . . : 255.255.255.0
    Основной шлюз . . . . . : 

```

Рис. 1.3. Вывод команды «ipconfig»

Команда может принимать дополнительные аргументы, которые позволяют изменить набор отображаемых параметров или обновить конфигурацию сети при наличии в ней системы DHCP и (или) DNS. Примером аргументов первого типа является аргумент «/all», который выводит расширенную сетевую информацию как о самом компьютере, так и о сетях.

```
C:\Пользователи\user>ipconfig /all

Настройка протокола IP для Windows

Имя компьютера . . . . . : admin-0fa179ebf
Основной DNS-суффикс . . . . . : 
Тип узла . . . . . : неизвестный
IP-маршрутизация включена . . . . . : нет
WINS-прокси включен . . . . . : нет

Подключение по локальной сети - Ethernet адаптер:

DNS-суффикс этого подключения . . : 
Описание . . . . . : Realtek PCIe GBE Family Controller
Физический адрес . . . . . : 00-19-DB-AF-9B-09
DHCP-включен . . . . . : нет
IP-адрес . . . . . : 192.168.1.2
Маска подсети . . . . . : 255.255.255.0
Основной шлюз . . . . . : 

VirtualBox Host-Only Network - Ethernet адаптер:

DNS-суффикс этого подключения . . : 
Описание . . . . . : VirtualBox Host-Only Ethernet Adapter
Физический адрес . . . . . : 08-00-27-00-30-46
DHCP-включен . . . . . : нет
IP-адрес . . . . . : 192.168.56.1
Маска подсети . . . . . : 255.255.255.0
Основной шлюз . . . . . : 

C:\Пользователи\user>
```

Рис. 1.4. Вывод команды «ipconfig /all»

К сожалению, все настроенные не обладают DHCP-сервером, поэтому аргументы «/release» и «/renew», ответственные за удаление и обновление автоматической конфигурации, не будут работать. Однако, аргумент «/flushdns», очищающий локальный кэш DNS, работает исправно, несмотря на отсутствие данной системы в созданной сети.

```
C:\Пользователи\user>ipconfig /release

Настройка протокола IP для Windows

Операция завершена с ошибкой, поскольку ни один адаптер
не находился в состоянии, допустимом для ее выполнения.

C:\Пользователи\user>ipconfig /renew

Настройка протокола IP для Windows

Операция завершена с ошибкой, поскольку ни один адаптер
не находился в состоянии, допустимом для ее выполнения.

C:\Пользователи\user>ipconfig /flushdns

Настройка протокола IP для Windows

Успешно сброшен кэш распознавателя DNS.

C:\Пользователи\user>
```

Рис. 1.5. Вывод команды «ipconfig» с различными аргументами

3.2. Ping

Команда Ping производит попытку получить доступ к указанному в аргументе узлу сети и возвращает статистику по каждому пробному соединению, а также сводную статистику по всем соединениям (время, процент потерь и т. д.).

```

Обмен пакетами с 192.168.1.1 по 32 байт:
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Превышен интервал ожидания для запроса.
Статистика Ping для 192.168.1.1:
  Пакетов: отправлено = 4, получено = 0, потеряно = 4 (100% потерь),
C:\Пользователи\user>ping 192.168.1.2
Обмен пакетами с 192.168.1.2 по 32 байт:
Ответ от 192.168.1.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.1.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.1.2: число байт=32 время<1мс TTL=128
Ответ от 192.168.1.2: число байт=32 время<1мс TTL=128
Статистика Ping для 192.168.1.2:
  Пакетов: отправлено = 4, получено = 4, потеряно = 0 (0% потерь),
  Приблизительное время приема-передачи в мс:
  Минимальное = 0мсек, Максимальное = 0 мсек, Среднее = 0 мсек

```

Рис. 1.6. Вывод команды «ping» при выключенной и включённой сети

По умолчанию команда «Ping» совершает четыре попытки соединения, но можно ограничить работу команды не по количеству повторов, а по времени с помощью аргумента «/t» и количества секунд. Если количество секунд для «/t» не задано, то команда будет работать в течении 60 секунд.

```

C:\Пользователи\user>ping 192.168.1.3 -t
Обмен пакетами с 192.168.1.3 по 32 байт:
Ответ от 192.168.1.3: число байт=32 время<1мс TTL=128
Ответ от 192.168.1.3: число байт=32 время<1мс TTL=128
Ответ от 192.168.1.3: число байт=32 время<1мс TTL=128
Ответ от 192.168.1.3: число байт=32 время<1мс TTL=128
Ответ от 192.168.1.3: число байт=32 время<1мс TTL=128
Ответ от 192.168.1.3: число байт=32 время<1мс TTL=128
Ответ от 192.168.1.3: число байт=32 время<1мс TTL=128
Ответ от 192.168.1.3: число байт=32 время<1мс TTL=128
Ответ от 192.168.1.3: число байт=32 время<1мс TTL=128
Ответ от 192.168.1.3: число байт=32 время<1мс TTL=128
Ответ от 192.168.1.3: число байт=32 время<1мс TTL=128
Ответ от 192.168.1.3: число байт=32 время<1мс TTL=128
Ответ от 192.168.1.3: число байт=32 время<1мс TTL=128
Ответ от 192.168.1.3: число байт=32 время<1мс TTL=128
Ответ от 192.168.1.3: число байт=32 время<1мс TTL=128
Ответ от 192.168.1.3: число байт=32 время<1мс TTL=128
Ответ от 192.168.1.3: число байт=32 время<1мс TTL=128
Ответ от 192.168.1.3: число байт=32 время<1мс TTL=128
Ответ от 192.168.1.3: число байт=32 время<1мс TTL=128
Ответ от 192.168.1.3: число байт=32 время<1мс TTL=128

```

Рис. 1.7. Вывод команды «ping /t»

3.3. Tracert

Команда Tracert выводит полный путь пакетов до указанного узла сети через неё промежуточные узлы. В мелких сетях, наподобие настроенной в рамках этой работы, данное число обычно не превосходит 1-2 (включая конечный узел, но исключая коммутаторы и прочие пассивные узлы), но в крупных составных сетях, наподобие Интернета, данное количество может исчисляться десятками узлов, в зависимости от удалённости конечного узла

сети в её топологии. Максимальное измеряемое число прыжков между узлами обычно равняется 30, однако можно задать своё значение с помощью аргумента «-h».

```
C:\Пользователи\user>tracert 192.168.1.3
Трассировка маршрута к 192.168.1.3 с максимальным числом прыжков 30
 1    <1 мс    <1 мс    <1 мс  192.168.1.3
Трассировка завершена.
C:\Пользователи\user>tracert -h 5 192.168.1.3
Трассировка маршрута к 192.168.1.3 с максимальным числом прыжков 5
 1    <1 мс    <1 мс    <1 мс  192.168.1.3
Трассировка завершена.
```

Рис. 1.8. Вывод команды «tracert»

3.4. Nslookup

Команда Nslookup выводит IP-адрес узла по его доменному имени в системе DNS. Для этого она обращается к одному из двух DNS-серверов, указанных в настройках сети, либо к локальному кэшу. Если ни один из серверов не доступен, а кэш пуст, то команда выдаст сообщение об ошибке разрешения имени.

```
C:\Пользователи\user>nslookup 192.168.1.3
*** Default servers are not available
Server: UnKnown
Address: 127.0.0.1

*** UnKnown can't find 192.168.1.3: No response from server

C:\Пользователи\user>nslookup 172.217.165.142
*** Default servers are not available
Server: UnKnown
Address: 127.0.0.1

*** UnKnown can't find 172.217.165.142: No response from server

C:\Пользователи\user>nslookup google.com
*** Default servers are not available
Server: UnKnown
Address: 127.0.0.1

*** UnKnown can't find google.com: No response from server

C:\Пользователи\user>
```

Рис. 1.9. Вывод команды «nslookup» в сети без DNS и доступа к внешним ресурсам

3.5. NetStat

Команда NetStat выводит информацию об адресах в каждой сети и статус подключения к ним. По умолчанию адреса отображаются в виде имён DNS, однако можно включить отображение IP-адресов с помощью аргумента «-п».

9

```

C:\Пользователи\user>netstat
Активные подключения
    Имя      Локальный адрес      Внешний адрес      Состояние
    TCP      admin-0fa179ebf:1029  localhost:1030     ESTABLISHED
    TCP      admin-0fa179ebf:1030  localhost:1029     ESTABLISHED

C:\Пользователи\user>netstat -n
Активные подключения
    Имя      Локальный адрес      Внешний адрес      Состояние
    TCP      127.0.0.1:1029       127.0.0.1:1030     ESTABLISHED
    TCP      127.0.0.1:1030       127.0.0.1:1029     ESTABLISHED

C:\Пользователи\user>

```

Рис. 1.10. Вывод команды «netstat»

В качестве аргумента команды «netstat» можно задать количество секунд, через которое программа будет обновлять информацию о сети без завершения работы до требования пользователя (комбинация Ctrl + C), что позволяет использовать эту команду для динамического мониторинга сети.

```

C:\Пользователи\user>netstat -n 3
Активные подключения
    Имя      Локальный адрес      Внешний адрес      Состояние
    TCP      127.0.0.1:1029       127.0.0.1:1030     ESTABLISHED
    TCP      127.0.0.1:1030       127.0.0.1:1029     ESTABLISHED

Активные подключения
    Имя      Локальный адрес      Внешний адрес      Состояние
    TCP      127.0.0.1:1029       127.0.0.1:1030     ESTABLISHED
    TCP      127.0.0.1:1030       127.0.0.1:1029     ESTABLISHED

Активные подключения
    Имя      Локальный адрес      Внешний адрес      Состояние
    TCP      127.0.0.1:1029       127.0.0.1:1030     ESTABLISHED
    TCP      127.0.0.1:1030       127.0.0.1:1029     ESTABLISHED
^C
C:\Пользователи\user>arp -a
Не найдены записи в таблице ARP

```

Рис. 1.11. Вывод команды «netstat» с повторением

3.6. ARP

Команда ARP выводит информацию из таблицы адресов протокола разрешения имён ARP или запись из неё по конкретному IP. Данная таблица хранит для каждого IP-адреса в сети его тип и связанный с ним физический адрес устройства.


```

Командная строка
C:\Пользователи\user>arp -a
Интерфейс: 192.168.1.3 --- 0x2
    Адрес      IP               Физический адрес      Тип
    -----
    192.168.1.1  00-19-db-af-9a-b6     динамический
    192.168.1.2  00-19-db-af-9b-09     динамический
    192.168.1.4  00-19-db-af-9b-38     динамический

C:\Пользователи\user>arp -a 192.168.1.2
Интерфейс: 192.168.1.3 --- 0x2
    Адрес      IP               Физический адрес      Тип
    -----
    192.168.1.2  00-19-db-af-9b-09     динамический

C:\Пользователи\user>_

```

Рис. 1.12. Вывод команды «arp»

3.7. Route

Инструмент маршрутизации отображает таблицу маршрутизации, которая позволяет Windows понимать сеть и взаимодействовать с другими устройствами и службами. Инструмент также предлагает некоторые параметры для изменения и очистки таблицы при необходимости.

```

C:\Пользователи\user>arp -a 192.168.1.2
Не найдены записи в таблице ARP

C:\Пользователи\user>route print
=====
Список интерфейсов
0x1 ..... MS TCP Loopback interface
0x2 ...00 19 db af 9b 4b ..... Realtek PCIe GBE Family Controller - [изменяЕС я
решЕт чир ярхСот
0x3 ..08 00 27 00 20 9e ..... VirtualBox Host-Only Ethernet Adapter - [изменяЕС
яррешЕт шыр яррхСот
=====
Активные маршруты:
Сетевой адрес      Маска сети      Адрес шлюза      Интерфейс      Метрика
-----
127.0.0.0          255.0.0.0       127.0.0.1        127.0.0.1      1
192.168.1.0        255.255.255.0   192.168.1.3      192.168.1.3    20
192.168.1.3        255.255.255.255 127.0.0.1        127.0.0.1      20
192.168.1.255     255.255.255.255 192.168.1.3      192.168.1.3    20
192.168.56.0       255.255.255.0   192.168.56.1     192.168.56.1   20
192.168.56.1       255.255.255.255 127.0.0.1        127.0.0.1      20
192.168.56.255    255.255.255.255 192.168.56.1     192.168.56.1   20
224.0.0.0          240.0.0.0       192.168.1.3      192.168.1.3    20
224.0.0.0          240.0.0.0       192.168.56.1     192.168.56.1   20
255.255.255.255    255.255.255.255 192.168.1.3      192.168.1.3    1
255.255.255.255    255.255.255.255 192.168.56.1     192.168.56.1   1
=====
Постоянные маршруты:
Отсутствует

```

Рис. 1.13. Вывод команды «route print»

3.8. NetSh

В Windows 10 NetSh — это инструмент командной строки, который позволяет отображать и изменять практически любую сетевую конфигурацию. Например, вы можете использовать этот инструмент для просмотра текущей конфигурации сети, управления беспроводными соединениями, сброса сетевого стека для устранения наиболее распространённых проблем, включения или отключения брандмауэра и многого другого.

```

C:\Пользователи\user>netsh /?
Использование: netsh [-a <Файла псевдонимов>] [-c <Контекст>]
[<Команда>] [-f <Файл сценария>]

Принимены следующие команды:
Команды в этом контексте:
? - Отображение списка команд.
add - Добавление элемента конфигурации в список элементов.
bridge - Изменения в контексте 'netsh bridge'.
delete - Удаление элемента конфигурации из списка элементов.
diag - Изменения в контексте 'netsh diag'.
dump - Отображение сценария конфигурации.
exec - Запуск файла сценария.
firewall - Изменения в контексте 'netsh firewall'.
help - Отображение списка команд.
interface - Изменения в контексте 'netsh interface'.
lan - Изменения в контексте 'netsh lan'.
ras - Изменения в контексте 'netsh ras'.
routing - Изменения в контексте 'netsh routing'.
set - Обновление параметров конфигурации.
show - Отображение информации.
winsock - Изменения в контексте 'netsh winsock'.

Доступны следующие дочерние контексты:
bridge diag firewall interface lan ras routing winsock

Чтобы получить справку по команде, введите эту команду,
затем пробел и "?".
C:\Пользователи\user>

```

Рис. 1.14. Вывод справочной информации по команде «netsh»

4. Проверка сетевых команд в ОС Linux

4.1. *ping*

В ОС Linux команда *ping* работает аналогично одноимённой команде из Windows: она проверяет доступность узла сети путём отправки проверочных пакетов.

```

user@cs206-05: ~ x
root@cs206-05:~# ping 192.168.1.24
PING 192.168.1.24 (192.168.1.24) 56(84) bytes of data:
64 bytes from 192.168.1.24: icmp_seq=1 ttl=64 time=0.349 ms
64 bytes from 192.168.1.24: icmp_seq=2 ttl=64 time=0.331 ms
64 bytes from 192.168.1.24: icmp_seq=3 ttl=64 time=0.351 ms
64 bytes from 192.168.1.24: icmp_seq=4 ttl=64 time=0.339 ms
^C
--- 192.168.1.24 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3066ms
rtt min/avg/max/mdev = 0.331/0.342/0.351/0.008 ms
root@cs206-05:~#

```

Рис. 2.1. Вывод команды «ping»

4.2. *traceroute*

В ОС Linux команда *traceroute* работает аналогично команде *tracert* из Windows: она отображает полный путь отправки пакетов к указанному узлу сети через другие узлы.

```

root@cs206-05:~# traceroute 192.168.1.2
traceroute to 192.168.1.2 (192.168.1.2), 30 hops max, 60 byte packets
 1 * * *
 2 * * *
 3 192.168.1.2 (192.168.1.2) 0.105 ms 0.154 ms 0.137 ms
root@cs206-05:~#

```

Рис. 2.2. Вывод команды «traceroute»

4.3. *telnet*

Команда *telnet* позволит получить удалённый доступ к другому

компьютеру по протоколу Telnet. Из-за устарелости и незащищённости протокола большинство современных Linux-систем блокирует прямой доступ к управлению по этому протоколу.

4.4. *netstat*

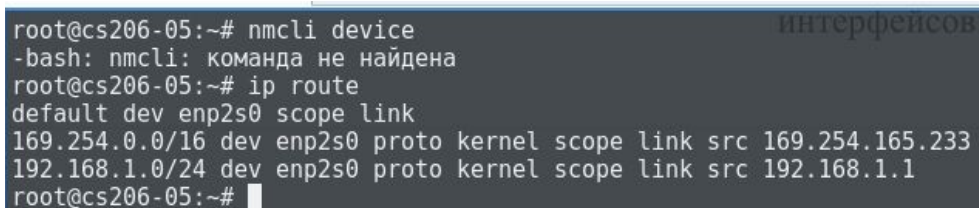
В ОС Linux команда netstat работает аналогично команде traceroute из Windows, но помимо списка адресов (ключ «-r») она может вывести также список всех портов (ключ «-t»), отдельный список «слушающих» портов (ключ «-l») и статистику по каждому протоколу отдельно (ключ «-s»). Все эти режимы работы были проверены на каждой машине отдельно.

4.5. *nmcli*

Возможности команды nmcli проверить не удалось, т. к. в используемом дистрибутиве Linux она отсутствует.

4.6. *ip route*

Команда ip route выводит все установленные маршруты от данного узла к различным подключённым сетям.



```

root@cs206-05:~# nmcli device
-bash: nmcli: команда не найдена
root@cs206-05:~# ip route
default dev enp2s0 scope link
169.254.0.0/16 dev enp2s0 proto kernel scope link src 169.254.165.233
192.168.1.0/24 dev enp2s0 proto kernel scope link src 192.168.1.1
root@cs206-05:~#

```

Рис 2.3. Вывод команды «ip route»

4.7. *route, arp, tcpdump*

Возможности команд route, arp и tcpdump проверить не удалось, т. к. в используемом дистрибутиве Linux они отсутствуют.

4.8. *iptables*

Команда iptables управляет встроенным в систему брандмуэром,

обеспечивая вывод, удаление и установление правил обработки пакетов. Таким образом удалось отрезать один из узлов сети, а затем вернуть ему доступ.

```

root@cs206-05:~# iptables -L
# Warning: iptables-legacy tables present, use iptables-legacy to see them
Chain INPUT (policy ACCEPT)
target    prot opt source                destination
Chain FORWARD (policy ACCEPT)
target    prot opt source                destination
Chain OUTPUT (policy ACCEPT)
target    prot opt source                destination
root@cs206-05:~# iptables -A INPUT -s 192.168.1.2 -j DROP
root@cs206-05:~# iptables -L
# Warning: iptables-legacy tables present, use iptables-legacy to see them
Chain INPUT (policy ACCEPT)
target    prot opt source                destination
DROP      all  --  192.168.1.2            anywhere
Chain FORWARD (policy ACCEPT)
target    prot opt source                destination
Chain OUTPUT (policy ACCEPT)
target    prot opt source                destination
root@cs206-05:~# iptables -A INPUT -s 192.168.1.2 -j ACCEPT
root@cs206-05:~# iptables -L
# Warning: iptables-legacy tables present, use iptables-legacy to see them
Chain INPUT (policy ACCEPT)
target    prot opt source                destination
DROP      all  --  192.168.1.2            anywhere
ACCEPT    all  --  192.168.1.2            anywhere
Chain FORWARD (policy ACCEPT)
target    prot opt source                destination
Chain OUTPUT (policy ACCEPT)
target    prot opt source                destination
root@cs206-05:~# iptables -

```

Рис. 2.4. Вывод команды «iptables» с различными ключами

4.9. nslookup

В ОС Linux команда nslookup работает аналогично одноимённой команде из Windows: она по введённому в собственный командный интерфейс имени DNS выводит IP-адрес связанного с ним узла, либо сообщение о том, что такого имени в сети не существует. В нашем случае система DNS не используется, поэтому любое доменное имя будет считаться несуществующим.

```

root@cs206-05:~# nslookup
> google.com
;; connection timed out; no servers could be reached
>

```

Рис. 2.5. Вывод команды «nslookup» с различными ключами

5. Вывод по выполненной работе

В результате выполненной работы был изучен процесс создания простой компьютерной сети и настройки её узлов под управлением различных ОС. Вместе с тем были изучены основные сетевые возможности и команды этих ОС. Хотя группе и не удалось исследовать некоторые команды из-за

ограничений используемых версий ОС, неисследованные команды могут быть выполнены в других версиях или после установки дополнительных компонентов из сети Интернет.