

Сколько записей результата было возвращено? Укажите целое число цифрой.

```
[root@c7 ~]# dig AAAA ifmo.ru
; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7 <<>> AAAA ifmo.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 65523
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 13, ADDITIONAL: 13
;; QUESTION SECTION:
;ifmo.ru.                IN      AAAA
;; AUTHORITY SECTION:
.                9999    IN      NS      i.root-servers.net.
.                9999    IN      NS      j.root-servers.net.
.                9999    IN      NS      k.root-servers.net.
.                9999    IN      NS      l.root-servers.net.
.                9999    IN      NS      m.root-servers.net.
.                9999    IN      NS      b.root-servers.net.
.                9999    IN      NS      c.root-servers.net.
.                9999    IN      NS      d.root-servers.net.
.                9999    IN      NS      e.root-servers.net.
.                9999    IN      NS      f.root-servers.net.
.                9999    IN      NS      g.root-servers.net.
.                9999    IN      NS      h.root-servers.net.
.                9999    IN      NS      a.root-servers.net.
;; ADDITIONAL SECTION:
i.root-servers.net.  592687 IN      A      192.36.148.17
j.root-servers.net.  592687 IN      A      192.58.128.30
k.root-servers.net.  592687 IN      A      193.0.14.129
l.root-servers.net.  592687 IN      A      199.7.83.42
m.root-servers.net.  592687 IN      A      202.12.27.33
b.root-servers.net.  592687 IN      A      199.9.14.201
c.root-servers.net.  592687 IN      A      192.33.4.12
d.root-servers.net.  592687 IN      A      199.7.91.13
e.root-servers.net.  592687 IN      A      192.203.230.10
f.root-servers.net.  592687 IN      A      192.5.5.241
g.root-servers.net.  592687 IN      A      192.112.36.4
h.root-servers.net.  592687 IN      A      198.97.190.53
a.root-servers.net.  592687 IN      A      198.41.0.4
;; Query time: 19 msec
;; SERVER: 192.168.0.1#53(192.168.0.1)
;; WHEN: Wed Nov 18 09:27:28 EST 2020
;; MSG SIZE rcvd: 444
```

2

На роутере задана таблица маршрутизации:

АДРЕС	МАСКА	ШЛЮЗ	ПОРТ
10.0.0.0	255.0.0.0	10.0.0.100	eth0
10.0.1.0	255.255.255.0	10.0.0.101	eth1
10.0.1.17	255.255.255.255	10.0.0.102	eth1
0.0.0.0	0.0.0.0	10.0.0.103	eth0

Все метрики одинаковые.

Выберите все верные утверждения

- ☒ Пакет на адрес 10.0.1.17 будет направлен на 10.0.0.0.102
- ☐ Пакет на адрес 10.0.1.17 будет направлен на 10.0.0.0.101
- ☐ Пакет на адрес 10.0.0.5 будет направлен на 10.0.0.0.103
- ☒ Пакет на адрес 10.134.240.9 будет направлен на 10.0.0.0.103

3

Выберите верные утверждения о файерволе с проверками по цепочкам (например iptables).

- ☐ Порядок правил в цепочке не важен
- ☒ Правила объединяются в цепочки и каждый пакет проверяется по цепочке правил по порядку, до первого срабатывания
- ☒ У цепочки есть политика по умолчанию, которую можно менять
- ☐ Правила объединяются в цепочки и каждый пакет проверяется по всем правилам в любом случае

4

Выберите верные утверждения о DMZ

- ☐ в DMZ помещают узлы приватной сети без доступа к ним из Интернет
- ☐ правила фильтрации между DMZ и приватной сетью и Интернетом и приватной сетью должны отличаться незначительно
- ☐ DMZ предназначен для регуляции клиентского доступа из LAN в Интернет
- ☒ в DMZ помещают узлы приватной сети с доступом к их сервисам из Интернет

5

Поле метрика в таблицах маршрутизации IP содержит

- ☐ Показатель качества маршрута, который чем больше, тем маршрут предпочтительнее.
- ☐ Всегда количество промежуточных маршрутизаторов
- ☒ Показатель качества маршрута, который чем меньше, тем маршрут предпочтительнее.
- ☐ Число, пропорциональное количеству бит в адресе сети

6

Существует программный шлюз Linux, через который настроен доступ в интернет из локальной сети, с использованием NAT.

На программном шлюзе с Linux были последовательно введены команды:

```
iptables -I INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

```
iptables -P INPUT DROP
```

```
iptables -P OUTPUT ACCEPT
```

Выберите все верные утверждения, считая, что не существует других правил блокирующих заданные выше правила, а ключ -P задает политику по умолчанию

- ☐ Обеспечена возможность для всех внешних клиентов устанавливать соединения с сервисами на этом хосте
- ☐ Будет заблокирован и входящий и исходящий трафик
- ☒ Обеспечена возможность для всех клиентских приложений, работающих на хосте соединяться со внешними сервисами
- ☐ первое правило работать не будет, так как оно противоречит политике по умолчанию

7

Выберите верные утверждения о DNS

- ☒ DNS позволяет хранить конфигурационные данные приложения
- ☐ Распределенность хранения подразумевает, что информация о домене может храниться на нескольких DNS серверах
- ☒ Распределенность администрирования подразумевает, что отдельные ресурсные записи управляются их владельцами
- ☒ Кэширование подразумевает временное хранение результатов запросов разрешения имен

8

**Выберите верные утверждения**

- ☐ Номер порта клиента должен быть известен серверу перед началом соединения
- ☐ Номер порта сервера обычно больше 1024
- ☒ Номер порта сервера должен быть известен клиенту перед началом соединения
- ☒ Номер порта клиента обычно больше 1024

9

**Выберите верные утверждения о DNS**

- ☒ Рекурсивный DNS сервер возвращает конечному клиенту IP адрес ресурсной записи
- ☒ DNS клиент должен заранее знать IP адрес DNS сервера
- ☒ DNS сервер может вернуть ответ на запрос клиента без полного обхода дерева имен
- ☐ Корневые DNS сервера – рекурсивные

10

**Выберите верные утверждения**

- ☐ Программная маршрутизация невозможна в операционных системах общего назначения, например Linux.
- ☒ Маршрутизаторы могут быть как программными, так и аппаратными
- ☒ Маршрутизаторы должны работать по идентичному канальному протоколу на всех его портах
- ☒ Маршрутизатор обрабатывает каждый IPv4 пакет в отдельности

11

**Существует программный шлюз Linux, через который надо настроить доступ в интернет из локальной сети, с использованием NAT.**

**На программном шлюзе с Linux была введена команда:**

**`iptables -t nat -A POSTROUTING -o ens33 -s 192.168.100.0/24 -j MASQUERADE`**

**Выберите все верные утверждения, считая, что не существует других правил блокирующих заданное выше правило**

- ☐ Внутренняя сеть подключена к интерфейсу ens33
- ☒ Если в локальной сети используется подсеть 192.168.100.0/24, то из нее возможен клиентский доступ во внешнюю сеть
- ☒ Внешняя сеть подключена к интерфейсу ens33
- ☐ Правило не верно, поскольку не задан внешний IP, который надо использовать при трансляции адресов

12

**Выберите верные утверждения про стек TCP/IP**

- ☐ стек TCP/IP предполагает не строгий порядок инкапсуляции, сетевой уровень может инкапсулировать сетевой пакет и т.п.
- ☐ тек TCP/IP регламентирует работу канальных протоколов, т.е. содержит спецификации форматов заголовков канального уровня, длительность IPG и т.д.
- ☐
- ☒ стек TCP/IP предполагает строгий порядок инкапсуляции, прикладной уровень строго в транспортный, транспортный строго в сетевой уровень.
- ☒ устройство стека TCP/IP регулируется документами RFC

13

**Выберите верные утверждения о протоколе BGP**

- ☐ BGP маршрутизатор всегда хранит один и только один маршрут до сети назначения
- ☐ Это протокол динамической трансляции метрик
- ☐ Это протокол внутренней маршрутизации
- ☒ В этом протоколе на маршрутизаторе надо явно указывать соседние маршрутизаторы для обеспечения взаимодействия

14

Существует программный шлюз Linux (host) с адресами 195.0.0.1 и 10.0.0.1, через который настроен доступ в интернет из локальной сети (10.0.0.0/24), с использованием NAT.

В локальной сети существует еще один программный шлюз с Linux (host2), с адресами 10.0.0.2 и 10.1.0.1, за которым работает еще одна сеть 10.1.0.0/24

На программном шлюзе host1 была введена команда:

```
iptables -t nat -A PREROUTING --dst 195.0.0.1 -p tcp --dport 14080 -j DNAT --to-destination 10.0.0.2:222
```

На программном шлюзе host2 была введена команда:

```
iptables -t nat -A PREROUTING --dst 10.0.0.2 -p tcp --dport 222 -j DNAT --to-destination 10.1.0.2:22
```

Выберите все верные утверждения, считая, что не существует других правил блокирующих заданные выше правила и существуют правила SNAT, а на хосте 10.1.0.2 (host3) работает ssh сервер по порту tcp 22.

- ☒ К ssh серверу на host3 можно подключиться с host1 командой  
ssh 10.1.0.2 -p 22
- ☐ К ssh серверу на host3 можно подключиться из Интернет командой  
ssh 195.0.0.1 -p 1408
- ☐ К ssh серверу на host3 можно подключиться из Интернет командой  
ssh 195.0.0.1 -p 22
- ☒ К ssh серверу на host3 можно подключиться с host2 командой  
ssh 10.1.0.2 -p 22

15

Выберите верные утверждения о публикации порта через NAT (DNAT)

- ☒ Для каждого серверного приложения, к которому требуется доступ извне, должен быть назначен статический внешний порт
- ☐ Если в локальной сети на разных хостах есть несколько ssh серверов, то на шлюзе может быть «опубликован» только один из них
- ☐ Для каждого клиентского приложения в локальной сети для доступа в Интернет должен быть назначен статический внешний порт
- ☐ DNAT позволяет всем клиентским приложениям получать доступ во внешнюю сеть из локальной сети

16

Выберите верные утверждения об Congestion window (окне перегрузки)

- ☐ не может быть больше окна передачи
- ☒ значение постепенно увеличивается по мере накопления положительного опыта передачи сегментов сеанса
- ☒ регулирует скорость передачи данных по TCP
- ☐ зависит целиком от прикладного протокола

17

**Выберите верные утверждения о клиентском NAT (SNAT)**

- ☐ Для каждого локального приложения, работающего с внешней сетью, будет уникальный внешний сокет, причем это отображение создается вручную
- ☒ Для каждого локального приложения, работающего с внешней сетью, будет уникальный внешний сокет
- ☐ У исходящего из локальной сети пакета меняется только IP адрес получателя
- ☒ У исходящего из локальной сети пакета меняется IP адрес отправителя и порт отправителя

18

**Выберите верные утверждения**

- ☒ Контрольная сумма UDP рассчитывается по заголовку
- ☐ Заголовок UDP содержит как IP адрес отправителя, так и IP адрес получателя
- ☒ В случае повреждения поля данных UDP сбрасывает сообщение
- ☐ Длина UDP сообщения фиксирована и определена RFC

19

**Выберите верные утверждения о TCP**

- ☒ Флаг ACK указывает, что надо обрабатывать поле «Номер октета, который должен прийти следующим» (иначе «Номер подтверждения»)
- ☐ Флаг SYN указывает, что надо обрабатывать поле «Номер октета, который должен прийти следующим» (иначе «Номер подтверждения»)
- ☐ Флаг UGT указывает, что надо обрабатывать поле «Номер октета, который должен прийти следующим» (иначе «Номер подтверждения»)
- ☐ Флаг PSH указывает, что надо обрабатывать поле «Номер октета, который должен прийти следующим» (иначе «Номер подтверждения»)

20

**Выберите верные утверждения**

- ☒ Для каждого входящего соединения от клиента сервер запускает отдельный процесс на отдельном номере порта.
- ☒ Номера портов серверов определены в RFC, но могут быть изменены
- ☐ Порт с номером 0 запрещен к использованию как TCP, так и UDP.
- ☐ На одном хосте в один момент времени не должно быть совпадающих портов UDP и TCP

21

**Выберите верные утверждения о клиентском NAT (SNAT)**

- ☒ Для каждого локального приложения, работающего с внешней сетью, будет уникальный внешний socket
- ☐ Для каждого локального приложения, работающего с внешней сетью, будет уникальный внешний socket, причем это отображение создается вручную
- ☐ У исходящего из локальной сети пакета меняется только IP адрес получателя
- ☒ У исходящего из локальной сети пакета меняется IP адрес отправителя и порт отправителя

22

**Название протокола RIP означает:**

- ☐ Rest In Peace
- ☐ Round Independent Protocol
- ☒ Routing Information Protocol
- ☐ Routing Interactive Protocol

23

**В TCP/IP socket это**

- ☒ IP : Порт
- ☐ URL : Порт
- ☐ IP : PID
- ☐ IP : MAC

24

**Для IPv4 выберите все адреса, которые могут быть адресом компьютера**

- ☒ 250.168.96.2/27
- ☐ 192.168.0.127/27
- ☐ 192.168.96.0/18
- ☐ 192.168.96.0/19



25

**Выберите верные утверждения о TCP**

- ☐ Используется метод сбалансированного соединения
- ☒ Используется метод тройного рукопожатия
- ☐ Для установки соединения необходимо предать только 2 сегмента – запрос соединения (SYN) и один сегмент подтверждения (ACK)
- ☒ Для установления соединения используется флаги SYN и ACK

26

**В локальной сети у вас установлен роутер, подключенный к Интернет. На нем настроен клиентский нат. В локальной сети серые IP адреса. На вашем компьютере нет доступа в Интернет (например команда ping 8.8.8.8 показывает недоступность сервиса). Вы убедились с помощью команды ping, что внутренний адрес маршрутизатора доступен.**

**Выберите возможные причины неисправности**

- ☐ На вашем компьютере не назначен адрес DNS сервера
- ☒ На маршрутизаторе ваш адрес отфильтровывается фаерволом
- ☐ На вашем сетевом интерфейсе не назначен IP адрес
- ☒ На вашем компьютере не указан default gateway, равный внутреннему IP адресу маршрутизатора
- ☐ Не включен NAT на вашем компьютере

27

**Выберите верные утверждения**

- ☒ DNS позволяет по IP адресу определять доменное имя
- ☐ DNS клиент взаимодействует с DNS сервером по протоколу TCP
- ☒ DNS позволяет по доменному имени определять IP адрес
- ☐ DNS служит для назначения IP адресов хостам.

28

**Выберите верные утверждения**

- ☒ Протокол TCP обеспечивает надежную доставку данных
- ☒ Протокол UDP не обеспечивает надежной доставки данных.
- ☐ Протокол TCP может передавать сообщения протоколу UDP и наоборот
- ☐ Все протоколы транспортного уровня TCP/IP устанавливают соединения

29

Существует программный шлюз Linux, через который настроен доступ в интернет из локальной сети, с использованием NAT.

На программном шлюзе с Linux были введены команды:

```
iptables -A INPUT -p tcp --sport 80 -j ACCEPT
```

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

Выберите все верные утверждения, считая, что не существует других правил блокирующих заданные выше правила.

- ☐ Эти команды выдадут ошибку, так как в правилах не указаны IP адреса
- ☒ Эти правила разрешают все обращения из локальной сети через программный шлюз на внешние сервисы, работающие по порту tcp 80
- ☒ Эти правила разрешают подключение с программного шлюза к внешнему сервису, работающему по порту tcp 80
- ☐ Эти правила разрешают подключение к сервису, работающему на этой же Linux по порту tcp 80

30

Выберите верные утверждения о DNS

- ☒ MX записи содержат численное значение предпочтительности почтового сервера
- ☒ SOA записи нужны для конфигурации доменов
- ☐ SRV записи используются для создания записей на Web сервер
- ☒ AAAA записи нужны для поддержки IPv6

31

Выберите верные утверждения о публикации порта через NAT (DNAT)

- ☐ Если в локальной сети на разных хостах есть несколько ssh серверов, то на шлюзе может быть «опубликован» только один из них
- ☒ Для каждого серверного приложения, к которому требуется доступ извне, должен быть назначен статический внешний порт
- ☐ Для каждого клиентского приложения в локальной сети для доступа в Интернет должен быть назначен статический внешний порт
- ☐ DNAT позволяет всем клиентским приложениям получать доступ во внешнюю сеть из локальной сети

32

Как ой командой можно определить e-mail администратора домена?

- ☐ dig MX itmo.ru
- ☐ dig EMAIL itmo.ru
- ☐ dig TXT itmo.ru
- ☒ dig SOA itmo.ru

33

Выберите верные утверждения о внешней маршрутизации

- ☒ Это динамическая маршрутизация между автономными системами
- ☒ Эта маршрутизация может реализовываться с помощью протокола BGP
- ☐ Это статическая маршрутизация автономной системы
- ☐ Эта маршрутизация может реализовываться с помощью протокола RIP2

34

У вас из корпоративной сети (192.168.100.0/24) есть доступ через NAT в Интернет через программный шлюз. Вы определили что IP адрес на внешнем интерфейсе eth0 = 198.51.100.1 и он получен от провайдера по DHCP. Выберите самый верный вариант команды iptables для настройки.

- ☒ iptables -t nat -A POSTROUTING -o eth0 -s 192.168.100.0/24 -j MASQUERADE
- ☐ iptables -t nat -A PREROUTING -o eth0 -s 192.168.100.0/24 -j SNAT
- ☐ iptables -t nat -A POSTROUTING -o eth0 -s 192.168.100.0/24 -j ACCEPT
- ☐ eth0

35

Выберите условия, необходимые для работы маршрутизации IPv4

- ☒ все IP адреса должны быть уникальными
- ☐ общий IP адрес сети для всех соединенных локальных сетей
- ☐ необходим идентичный протокол канального уровня во всех соединенных локальных сетях
- ☒ необходимо непротиворечивое, единое пространство адресов во всех объединенных сетях

@ Не знаете как сохранить результат? [Отправьте его на email](#)