

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И  
МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ  
ФЕДЕРАЦИИ

«Сибирский государственный университет  
телекоммуникаций и информатики»  
(СибГУТИ)

ОТЧЕТ  
по дисциплине  
«WEB-технологии»

по теме:  
НАСТРОЙКА ШЛЮЗА ЛОКАЛЬНОЙ СЕТИ,  
UBUNTU 24.10

Студент:  
*Группы ИКС-432*

*А.А. Пастухов*

Предподаватель:

*А.В. Андреев*

Новосибирск 2025

## СОДЕРЖАНИЕ

<b>ВВЕДЕНИЕ.....</b>	<b>3</b>
<b>1 ОСНОВЫ РАБОТЫ СЕТИ И НАСТРОЙКА ШЛЮЗА.....</b>	<b>4</b>
<b>2 НАСТРОЙКА ШЛЮЗА ЛОКАЛЬНОЙ СЕТИ .....</b>	<b>8</b>
<b>ЗАКЛЮЧЕНИЕ .....</b>	<b>18</b>

## ВВЕДЕНИЕ

В современных локальных сетях подключение к глобальной сети Интернет является неотъемлемой частью как для частных пользователей, так и для организаций. Для обеспечения доступа к внешним ресурсам используется шлюз – специализированное устройство или сервер, которое выполняет функции маршрутизации данных между локальной сетью (LAN) и внешними узлами (WAN). Шлюз выступает в роли посредника, который позволяет устройствам внутри сети взаимодействовать с внешними серверами и ресурсами.

Шлюз играет ключевую роль в организации сетевой инфраструктуры. Он не только обеспечивает доступ в Интернет, но и выполняет ряд дополнительных функций:

1. **Маршрутизация трафика:** Шлюз определяет оптимальные пути для передачи данных между локальной сетью и внешними узлами.
2. **Управление трафиком:** Он позволяет контролировать объем и тип передаваемых данных, что особенно важно для предотвращения перегрузок сети.
3. **Фильтрация пакетов:** Шлюз может блокировать нежелательный или вредоносный трафик, повышая безопасность сети.
4. **Обеспечение безопасности:** С помощью встроенных механизмов, таких как брандмауэры, шлюз предотвращает несанкционированный доступ и защищает локальную сеть от внешних угроз.

Настройка шлюза является важным этапом развертывания сети, особенно в корпоративной среде, где требуется высокая степень защиты данных и стабильность работы. В данной работе рассматривается процесс конфигурации шлюза на основе операционной системы Ubuntu 24.10. Будут подробно описаны этапы настройки сетевых интерфейсов, активация маршрутизации, а также использование брандмауэра iptables для управления трафиком и обеспечения безопасности. Эти методы помогут создать надежную и защищенную сетевую инфраструктуру.

## 1 ОСНОВЫ РАБОТЫ СЕТИ И НАСТРОЙКА ШЛЮЗА

Основой функционирования любых сетей, от небольших локальных до глобальных, являются ключевые механизмы, обеспечивающие передачу информации. Среди них центральное место занимают IP-адресация, порты TCP/IP и процессы создания сетевых пакетов. Эти элементы позволяют устройствам находить друг друга, устанавливать соединения и обмениваться данными. В этом разделе мы подробно изучим их назначение и принципы работы.

Каждое устройство, подключенное к сети, должно иметь уникальный идентификатор, чтобы участвовать в обмене данными. Таким идентификатором является IP-адрес — числовое значение, которое позволяет устройствам находить друг друга и взаимодействовать. Существует две основные версии IP-адресов: IPv4 и IPv6, каждая из которых имеет свои особенности.

IPv4 — это классическая версия, которая использует 32-битную систему адресации. Адрес записывается в виде четырех чисел от 0 до 255, разделенных точками, например, 192.168.0.1. Такая система позволяет создать около 4,3 миллиарда уникальных адресов, что долгое время было достаточным. Однако с ростом числа устройств, подключаемых к Интернету, IPv4-адреса стали заканчиваться, что потребовало перехода на более современную версию.

IPv6 — это усовершенствованный стандарт, использующий 128-битную адресацию. Адреса записываются в виде восьми групп шестнадцатеричных чисел, разделенных двоеточиями, например, 2001:0db8:85a3:0000:0000:8a2e:0370:7334. Благодаря такой системе IPv6 поддерживает практически неограниченное количество уникальных адресов, что делает его идеальным решением для современных сетей с огромным количеством устройств.

Некоторые IP-адреса имеют специальное назначение и используются для определенных целей в сетях:

127.0.0.1 — это локальный адрес устройства, также известный как localhost. Он используется для тестирования сетевых приложений на самом устройстве без передачи данных в сеть.

192.168.x.x, 10.x.x.x, 172.16.x.x – 172.31.x.x — это частные диапазоны IP-адресов, которые используются в локальных сетях. Эти адреса не маршрутизируются в Интернете и предназначены для внутреннего использования.

xxx.xxx.xxx.0 — это адрес сети, который используется для идентификации всей подсети.

xxx.xxx.xxx.255 — это широковещательный адрес, который используется для отправки данных всем устройствам в подсети.

Шлюз (Gateway) — это устройство, которое соединяет разные сети и передает трафик между ними. Шлюз может быть как физическим устройством, например, роутером или маршрутизатором, так и программным решением, например, сервером с настроенным сетевым интерфейсом.

Маска подсети — это параметр, который определяет границу между адресом сети и адресом устройства в этой сети. Маска подсети используется для разделения IP-адреса на две части: сетевую и хостовую. Например, маска подсети /24 (255.255.255.0) означает, что первые три октета IP-адреса относятся к сети, а последний октет — к устройству. Это позволяет создать сеть на 256 адресов. Маска подсети /23 (255.255.254.0) позволяет создать сеть на 512 адресов.

NAT (Network Address Translation) — это технология, которая используется для преобразования IP-адресов в сети. NAT позволяет устройствам с частными IP-адресами выходить в Интернет через один общий публичный IP-адрес. Это особенно полезно в локальных сетях, где используется множество устройств, но количество доступных публичных IP-адресов ограничено.

Существует несколько видов NAT:

Статический NAT — один внутренний IP-адрес сопоставляется с одним внешним IP-адресом. Это используется, когда необходимо обеспечить постоянное сопоставление между внутренним и внешним адресом.

Динамический NAT — внешний IP-адрес назначается из пула доступных адресов. Это позволяет использовать несколько внешних адресов для множества внутренних устройств.

PAT (Port Address Translation) — это наиболее распространенный вид NAT, при котором один внешний IP-адрес используется для множества внутренних устройств. В этом случае для различения устройств используются порты.

NAT не только экономит глобальные IP-адреса, но и обеспечивает дополнительную безопасность, скрывая внутренние адреса устройств от внешнего мира.

DHCP (Dynamic Host Configuration Protocol) — это протокол, который позволяет автоматически назначать IP-адреса устройствам в сети. Это значительно упрощает процесс настройки сети, так как администратору не нужно вручную назначать IP-адреса каждому устройству.

Существует несколько способов распределения IP-адресов с помощью DHCP:

Ручное распределение — администратор вручную назначает IP-адреса устройствам. Это используется, когда необходимо закрепить за устройством определенный IP-адрес.

Автоматическое распределение — IP-адреса назначаются из заданного диапазона и закрепляются за устройствами на постоянной основе.

Динамическое распределение — IP-адреса выдаются на определенное время (аренда), после чего могут быть перераспределены другим устройствам.

DHCP реализован в большинстве современных роутеров и сетевых устройств. В Linux для настройки DHCP-сервера часто используется ISC DHCP Server, а в Windows — встроенный DHCP Server.

## 2 НАСТРОЙКА ШЛЮЗА ЛОКАЛЬНОЙ СЕТИ

Для выполнения работы были подготовлены две виртуальные машины:  
VM gate — выполняет роль шлюза.

VM Ubuntu Desktop — используется для тестирования работы шлюза.

Обе виртуальные машины были клонированы из заранее подготовленных шаблонов. При клонировании было уделено внимание указанию имен VM и выбору политики MAC-адресов. После завершения клонирования были настроены сетевые адаптеры для каждой VM. На рисунке 1 представлена настройка сетевого адаптера для виртуальной машины, выполняющей роль шлюза.

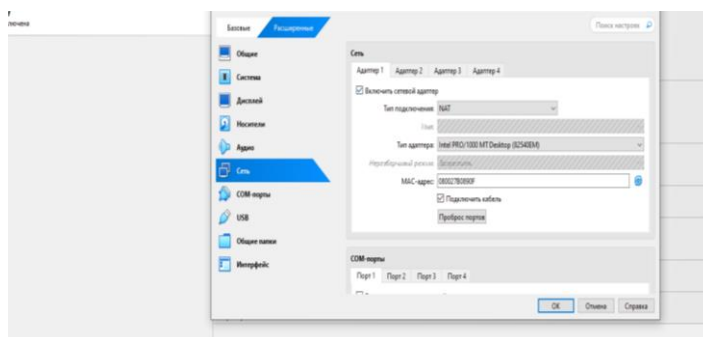


Рисунок 1 – Настройка адаптера 1 для сервера

На рисунке 2 представлена настройка второго сетевого адаптера, отвечающего за внутреннюю сеть.

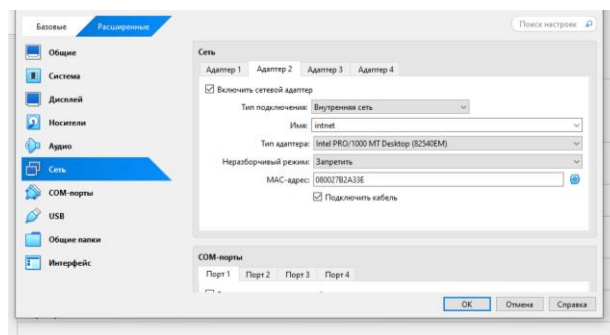


Рисунок 2 – Настройка адаптера 2 для сервера



Для виртуальной машины, выполняющей роль клиента, сетевой адаптер настроен аналогично адаптеру 2 сервера.

На рисунке 3 представлена схема дальнейшей настройки внутренней сети.

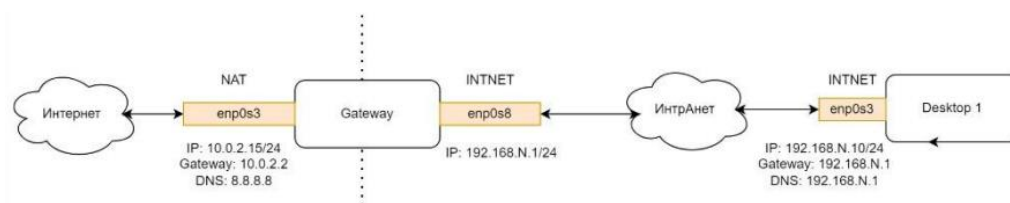


Рисунок 3 – настройка внутренней сети

Были получены права суперпользователя и выполнена проверка сетевых интерфейсов. В результате был определен внешний интерфейс enp0s3 (для связи с Интернетом) и внутренний enp0s8 (для локальной сети). Использованные команды и результат их выполнения представлены на рисунке 4. В ответ получаем список сетевых интерфейсов в системе и их параметры, они также представлены на рисунке 4.

```
Пн, 3 марта 23:00
root@server: /home/arown

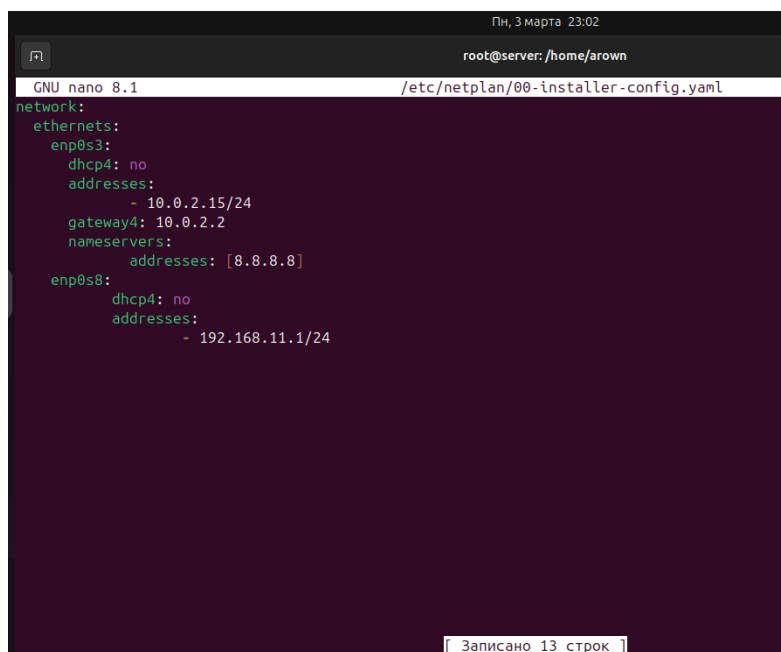
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

arown@server:~$ sudo su
[sudo] пароль для arown:
root@server:/home/arown# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 10
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
    link/ether 08:00:27:bd:35:b1 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3
        valid_lft 86281sec preferred_lft 86281sec
    inet6 fd00::780d:891e:36a1:6c24/64 scope global temporary dynamic
        valid_lft 86282sec preferred_lft 14282sec
    inet6 fd00::a00:27ff:febd:35b1/64 scope global dynamic mngtppaddr proto kernel_r
        valid_lft 86282sec preferred_lft 14282sec
    inet6 fe80::a00:27ff:febd:35b1/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
    link/ether 08:00:27:ba:7d:c4 brd ff:ff:ff:ff:ff:ff
    inet6 fe80::2588:4b8:f3b7:891/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
root@server:/home/arown#
```

Рисунок 4 – результаты выполнения команд *sudo su* и *ip a*

enp0s3 – является внешним интерфейсом для связи с Интернетом, а enp0s8 внутренним для построения Интранет сети.

Следующим этапом были изменены настройки сетевых устройств в конфигурационном файле 00-installer-config.yaml. Содержимое файла после редактирования настроек сети представлено на рисунке 5.



```
Пн, 3 марта 23:02
root@server: /home/arown
GNU nano 8.1 /etc/netplan/00-installer-config.yaml
network:
  ethernets:
    enp0s3:
      dhcp4: no
      addresses:
        - 10.0.2.15/24
      gateway4: 10.0.2.2
      nameservers:
        addresses: [8.8.8.8]
    enp0s8:
      dhcp4: no
      addresses:
        - 192.168.11.1/24
[ Записано 13 строк ]
```

Рисунок 5 – настройка 00-installer-config.yaml

После настройки конфигурационного файла изменения были применены с помощью команды *netplan apply*. Также проверяем результат при помощи *ip a*. Результат представлен на рисунке 6.

```
Пн, 3 марта 23:03
root@server: /home/arown

** (process:3853): WARNING **: 23:03:17.627: Permissions for /etc/netplan/00-installer-co
configuration should NOT be accessible by others.

** (process:3853): WARNING **: 23:03:17.628: 'gateway4' has been deprecated, use default
See the 'Default routes' section of the documentation for more details.

** (process:3853): WARNING **: 23:03:17.629: Permissions for /etc/netplan/01-network-mana
lan configuration should NOT be accessible by others.
root@server: /home/arown# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 10
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group defau
    link/ether 08:00:27:bd:35:b1 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global noprefixroute enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:febd:35b1/64 scope global temporary dynamic
        valid_lft 86390sec preferred_lft 14390sec
    inet6 fe80::a00:27ff:febd:35b1/64 scope global dynamic mngtmpaddr proto kernel_ra
        valid_lft 86390sec preferred_lft 14390sec
    inet6 fe80::a00:27ff:febd:35b1/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group defau
    link/ether 08:00:27:ba:7d:c4 brd ff:ff:ff:ff:ff:ff
    inet 192.168.11.1/24 brd 192.168.11.255 scope global noprefixroute enp0s8
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:feba:7dc4/64 scope link proto kernel_ll
        valid_lft forever preferred_lft forever
root@server: /home/arown#
```

Рисунок 6 – информация о сетевых интерфейсах после изменения параметров

На рисунке видно, что ip-адрес внутренней сети был изменён на 192.168.22.1, что соответствует заданию. Проверим доступ в интернет при помощи команды *ping ya.ru*. Результат выполнения команды *ping* представлен на рисунке 7.

```
PING ya.ru (77.88.55.242) 56(84) bytes of data.
64 bytes from ya.ru (77.88.55.242): icmp_seq=1 ttl=255 time=1.40 ms
64 bytes from ya.ru (77.88.55.242): icmp_seq=2 ttl=255 time=0.890 ms
64 bytes from ya.ru (77.88.55.242): icmp_seq=3 ttl=255 time=0.804 ms
64 bytes from ya.ru (77.88.55.242): icmp_seq=4 ttl=255 time=0.563 ms
64 bytes from ya.ru (77.88.55.242): icmp_seq=5 ttl=255 time=0.585 ms
64 bytes from ya.ru (77.88.55.242): icmp_seq=6 ttl=255 time=0.652 ms
64 bytes from ya.ru (77.88.55.242): icmp_seq=7 ttl=255 time=0.682 ms
```

Рисунок 7 – результат выполнения команды *ping ya.ru*

На клиентской машине вручную выполнена настройка статического ip-адреса локальной сети. Заданы параметры:

ip-адрес: 192.168.11.10

Маска подсети: 255.255.255.0

Шлюз: 192.168.11.1

DNS: 192.168.11.1

Отменить Проводное подключение Применить

Сведения о системе Идентификация IPv4 IPv6 Безопасность

Метод IPv4

☐ Автоматический (DHCP) ☐ Только для локальной сети

☒ Вручную ☐ Выключить

☐ Общий доступ другим компьютерам

Адреса

Адрес	Маска сети	Шлюз	
192.168.11.10	255.255.255.0	192.168.11.1	

DNS

Автоматически ☒

192.168.11.1

Отделяйте IP-адреса запятыми

Маршруты

Автоматически ☒

Адрес	Маска сети	Шлюз	Метрика	

Рисунок 8 – настройка клиентской машины

Проверяем настройку сети при помощи команды `ping 192.168.11.1`.  
Результат выполнения представлен на рисунке 9.

```
root@server:/home/argown# ping 192.168.11.1
PING 192.168.11.1 (192.168.11.1) 56(84) bytes of data.
64 bytes from 192.168.11.1: icmp_seq=1 ttl=64 time=0.091 ms
64 bytes from 192.168.11.1: icmp_seq=2 ttl=64 time=0.040 ms
64 bytes from 192.168.11.1: icmp_seq=3 ttl=64 time=0.039 ms
z^Z
[3]+  Остановлен    ping 192.168.11.1
```

Рисунок 9 – Результат ping 192.168.11.1

На основном шлюзе путем редактирования файла `sysctl.conf` разрешаем перенаправление пакетов, для этого была раскомментирована строка `net.ipv4.ip_forward=1`. Данные изменения представлены на рисунке 10.

```
GNU nano 7.2 /etc/sysctl.conf *
#####
# Functions previously found in netbase
#
# Uncomment the next two lines to enable Spoof protection (reverse-path filter)
# Turn on Source Address Verification in all interfaces to
# prevent some spoofing attacks
#net.ipv4.conf.default.rp_filter=1
#net.ipv4.conf.all.rp_filter=1
#
# Uncomment the next line to enable TCP/IP SYN cookies
# See http://lwn.net/Articles/277146/
# Note: This may impact IPv6 TCP sessions too
#net.ipv4.tcp_syncookies=1
#
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
#
# Uncomment the next line to enable packet forwarding for IPv6
# Enabling this option disables Stateless Address Autoconfiguration
#####
^G Справка ^O Записать ^W Поиск ^K Вырезать ^T Выполнить ^С Позиция
^X Выход ^R ЧитФайл ^\ Замена ^U Вставить ^J Выводить ^/_ К строке
```

Рисунок 10 – Изменения sysctl.conf

Следующим этапом был установлен пакет *iptables-persistent*, позволяющий сохранять настройки сетевого экрана после перезагрузки.

Сначала была обновлена информация о пакетах с помощью команды:

*apt-get update*

Затем был установлен сам пакет:

*apt install iptables-persistent*

Во время установки дважды появлялись сообщения с предложением сохранить текущие настройки, и в обоих случаях было выбрано подтверждение.

Принцип работы *iptables-persistent* заключается в том, что при перезагрузке системы автоматически применяются правила, сохраненные в файлах */etc/iptables/rules.v4* и */etc/iptables/rules.v6*.

После установки пакета были созданы следующие правила:

*iptables -F*

*iptables -t nat -A POSTROUTING -o enp0s3 -j MASQUERADE*

*iptables -A FORWARD -i enp0s3 -o enp0s3 -j REJECT*

```
iptables -I FORWARD -p tcp --tcp-flags SYN,RST SYN -j TCPMSS --clamp-  
mss-to-pmtu
```

```
iptables -t nat -A PREROUTING -i enp0s8 -p tcp -m tcp --dport 53 -j DNAT  
--to-destination 8.8.8.8:53
```

```
iptables -t nat -A PREROUTING -i enp0s8 -p udp -m udp --dport 53 -j  
DNAT --to-destination 8.8.8.8:53
```

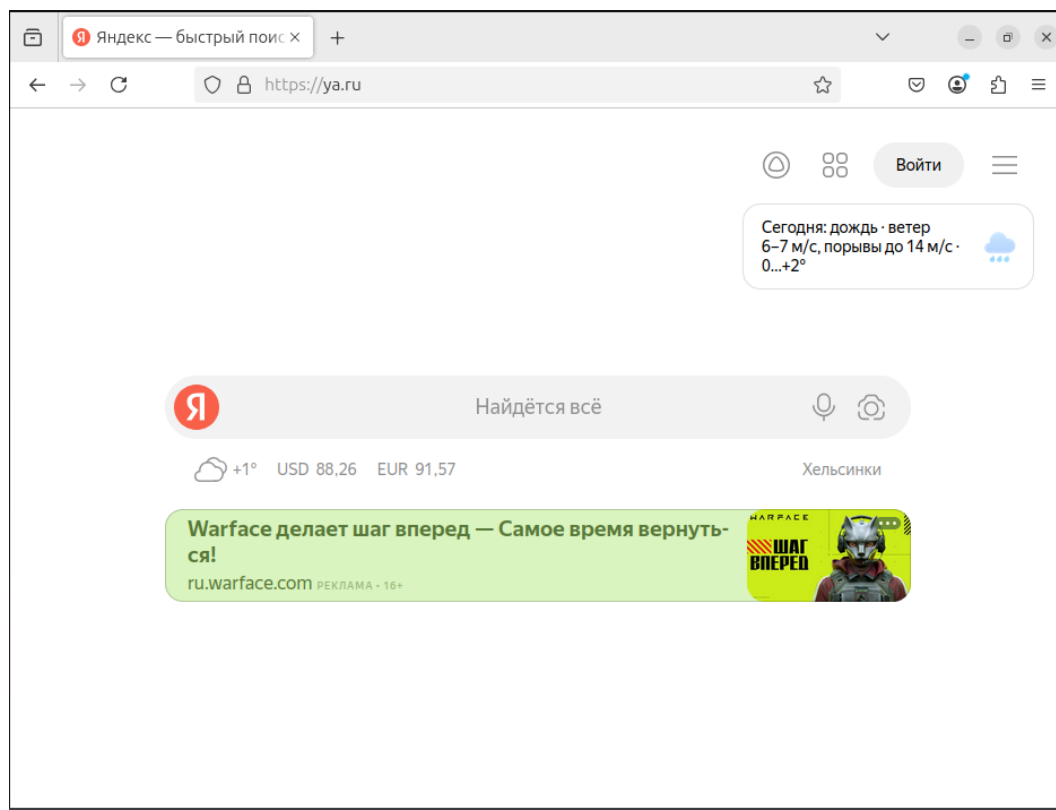
После создания правил они были сохранены в файл /etc/iptables/rules.v4:

```
iptables-save > /etc/iptables/rules.v4
```

Результаты выполнения данных команд представлен на рисунке 11.

В завершение была выполнена перезагрузка сервера для применения настроек.

Настройки успешно сохранились, и после перезагрузки сервера правила были автоматически применены. На рисунке 12 представлен пример доступа к сайту с клиентской машины после настройки.



### 2.3 Выполнение настройки DHCP

Перед выполнение данной части задания был создан снимок состояния виртуальной машины (VM snapshot) под названием "Lab4". Это позволило сохранить текущее состояние и конфигурацию VM.

Следующем этапе установлен пакет DHCP-сервера при помощи команд: `apt-get update` и `apt install isc-dhcp-server`.

Определен интерфейс, на котором будет работать DHCP-сервер (`enp0s8`).

Файл `/etc/default/isc-dhcp-server` был отредактирован, в строке `INTERFACESv4` указано:

```
INTERFACESv4="enp0s8"
```

Сделана резервная копия конфигурационного файла:

```
cp /etc/dhcp/dhcpd.conf /etc/dhcp/dhcpd.conf.example echo && "" > /etc/dhcp/dhcpd.conf
```

Далее был настроен конфигурационный файл `dhcpd.conf` в котором установлен авторитарный режим (`authoritative;`), настроена подсеть `192.168.11.0/24`, диапазон IP-адресов `192.168.11.10 – 192.168.11.254`, маска `255.255.255.0`, шлюз и DNS-сервер `192.168.11.1`. Конфигурационные настройки представлены на рисунке 13.

```
authoritative;
subnet 192.168.11.0 netmask 255.255.255.0 {
range 192.168.11.10 192.168.11.254;
option domain-name-servers 192.168.11.1;
option routers 192.168.11.1;
option broadcast-address 192.168.11.255;
default-lease-time 604800;
max-lease-time 720000;
}
host testhost {
hardware ethernet 00:01:8a:e3:s8:92;
fixed-address 192.168.11.51;
}
```

Рисунок 13 – dhcpd.conf

Запущен сервис DHCP при помощи команды `service isc-dhcp-server start`

и проверен статус сервиса: `service isc-dhcp-server status`. Результат выполнения команды для проверки представлен на рисунке 14.

```
root@server: /home/arown
root@server:/home/arown# service isc-dhcp-server status
● isc-dhcp-server.service - ISC DHCP IPv4 server
   Loaded: loaded (/usr/lib/systemd/system/isc-dhcp-server.servi
   Active: active (running) since Tue 2025-03-18 17:14:17 +07; 1
   Invocation: 575f96758c82465484ea3715646f9537
   Docs: man:dhcpd(8)
   Main PID: 4120 (dhcpd)
   Tasks: 1 (limit: 1887)
   Memory: 4.2M (peak: 4.4M)
   CPU: 42ms
   CGroup: /system.slice/isc-dhcp-server.service
           └─4120 dhcpd -user dhcpd -group dhcpd -f -4 -pf /run/

map 18 17:14:17 sanya sh[4120]: Wrote 0 new dynamic host decls to
map 18 17:14:17 sanya dhcpd[4120]: Wrote 1 leases to leases file.
map 18 17:14:17 sanya sh[4120]: Wrote 1 leases to leases file.
map 18 17:14:17 sanya dhcpd[4120]: Listening on LPF/enp0s8/08:00:2
map 18 17:14:17 sanya sh[4120]: Listening on LPF/enp0s8/08:00:27:6
map 18 17:14:17 sanya dhcpd[4120]: Sending on  LPF/enp0s8/08:00:2
map 18 17:14:17 sanya sh[4120]: Sending on  LPF/enp0s8/08:00:27:6
map 18 17:14:17 sanya sh[4120]: Sending on  Socket/fallback/fallb
map 18 17:14:17 sanya dhcpd[4120]: Sending on  Socket/fallback/fa
map 18 17:14:17 sanya dhcpd[4120]: Server starting service.
lines 1-22/22 (END)
```

Рисунок 14 – Статус сервера DHCP



После настройки Проверена связь между сервером и клиентом командой: `ping 192.168.11.1`. Настройка DHCP-сервера завершена успешно. DHCP-сервер работает корректно, клиентские машины получают IP-адреса, связь и доступ в интернет подтверждены.

## **ЗАКЛЮЧЕНИЕ**

В ходе данной работы был успешно настроен шлюз локальной сети на базе Ubuntu Server 24.10. Были реализованы основные сетевые функции, обеспечивающие взаимодействие локальных клиентов с интернетом, включая настройку сетевых интерфейсов, маршрутизацию трафика и применение правил NAT с использованием iptables.

Дополнительно был развернут DHCP-сервер, позволяющий автоматически раздавать IP-адреса клиентам в локальной сети. Проведено тестирование работы шлюза и DHCP-сервера, подтверждающее корректную настройку сети, доступ в интернет и работоспособность механизмов динамического распределения IP-адресов.

Настроенный шлюз обеспечивает безопасное и эффективное управление сетевым трафиком, что является важным элементом организации локальных сетей. В процессе выполнения работы были закреплены навыки администрирования сети на базе Linux, конфигурирования сетевых интерфейсов, настройки iptables и работы с DHCP-сервером.