**ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ ИВАНОВСКОЙ ОБЛАСТИ**

Областное государственное бюджетное

профессиональное образовательное учреждения

«Ивановский промышленно-экономический колледж»

**ОТЧЕТ**

**практической подготовки**

**УП.03** Эксплуатация объектов сетевой инфраструктуры

База практики:

ОГБПОУ «Ивановский промышленно-экономический колледж»

наименование базы согласно договору

Сроки прохождения практической подготовки: 08.10.2024-21.12.2024

Специальность: 09.02.06 Сетевое и системное администрирование

код и наименование специальности

Курс 3 Группа № 309

Обучающаяся Бродин Егор Эдуардович

Фамилия, Имя, Отчество студента (*полностью*)

Руководитель практики \_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_ /\_\_Букин Д.А.\_\_/

от Организации оценка  подпись Ф.И.О.

**ДНЕВНИК**

**практической подготовки**

**УП.03** Выполнение работ по проектированию сетевой инфраструктуры

База практики:

ОГБПОУ «Ивановский промышленно-экономический колледж»

наименование базы согласно договору

Сроки прохождения практической подготовки: 08.10.2024-21.12.2024

Специальность: 09.02.06 Сетевое и системное администрирование

код и наименование специальности

Курс 3 Группа № 309

Обучающаяся Бродин Егор Эдуардович

Фамилия, Имя, Отчество студента (*полностью*)

Руководитель практики \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ /Букин Д.А./

подпись Ф.И.О.

г. Иваново 2024

|  |  |  |
| --- | --- | --- |
| **Дата** | **Краткое описание выполняемых работ** | **Количество часов** |
| 8.10.2024 | Основы проектирования сетевой инфраструктуры  Инструктаж по охране труда при работе на персональном компьютере. Требования охраны труда во время работы. Требования охраны труда в аварийных ситуациях. | 6 |
| 10.10.2024 | Практическая работа № 1. Анализ полученного задания | 6 |
| 16.10.2024 | Практическая работа № 2. Построение физической карты локальной сети с помощью Visio | 6 |
| 17.10.2024 | Оформление технической документации, правила оформления документов. | 6 |
| 22.10.2024 | Практическая работа № 3. Изучение и написание технической документации сети. | 6 |
| 25.10.2024 | Разработка схемы сети в эмуляторе Cisco Packet Tracer.  Практическая работа № 4. Создание схемы сети в эмуляторе Cisco Packet Tracer, подключение сетевого оборудования. | 6 |
| 6.11.2024 | Практическая работа №5. Создание виртуальных локальных сетей в соответствии с подразделениями предприятия, настройка NAT (Network Address Translation). | 6 |
| 12.11.2024 | Практическая работа №6. Настройка IP-маршрутизации протокола OSPF(Open Shortest Path First для созданной локально-вычислительной сети. | 6 |
| 15.11.2024 | Практическая работа №7. Настройка туннеля для связи между сетями. Проверка его работоспособности. | 6 |
| 20.11.2024 | Администрирование сетевых ресурсов на базе OC Windows Server 2016. Практическая работа №8. Установка и базовая настройка ОС Windows Server 2016. | 6 |
| 22.11.2024 | Практическая работа №9. Развертывание службы AD DS. Настройка службы динамической выдачи IP-адресов, настройка DNS. | 6 |
| 27.11.2024 | Практическая работа №10. Настройка протокола NTP (Network Time Protocol) и NFS (Network File System) | 6 |
| 28.11.2024 | Практическая работа №11. Настройка web-сервера IIS на базе ОС Windows Server 2016. | 6 |
| 29.11.2024 | Администрирование сетевых ресурсов на базе OC Linux. Практическая работа №12.Настройка служб DNS (Domain Name System) и DHCP (Dynamic Host Configuration Protocol) | 6 |
| 30.11.2024 | Практическая работа №13. Настройка протокола NTP и удаленного доступа при помощи SSH. | 6 |
| 3.12.2024 | Практическая работа №14. Настройка web-сервера Apache на базе ОС Linux Debian 11. | 6 |
| 6.12.2024 | Практическая работа №15. Настройка связи между сетями при помощи VPN. Настройка протокола NAT. | 6 |
| 9.12.2024 | Выполнение действий по устранению неисправностей.  Практическая работа №16. Диагностика неисправностей сети с помощью команд-утилит. Аппаратная диагностика неисправностей сети. | 6 |
| 10.12.2024 | Практическая работа №17. Поиск неисправностей технических средств. Выполнение действий по устранению неисправностей ОС Linux Debian 11. | 6 |
| 12.12.2024 | Практическая работа №18. Выполнение действий по устранению неисправностей Cisco IOS. | 6 |
| 17.12.2024 | Практическая работа №19. Обжим патч-панели. | 6 |
| 19.12.2024 | Практическая работа №20. Обжим витой пары по стандартам EIA/TIA-568B и EIA/TIA-568А.  Практическая работа №21.Обжим компьютерной розетки RJ-45. | 6 |
| 20.12.2024 | Оформление отчета. Подготовка к защите. | 6 |
|  | Дифференцированный зачет | 6 |
| **ИТОГО часов** | | **144** |

Содержание

[Модуль 1 6](#_Toc185935511)

[1.1 Настройка имён устройств согласно топологии 6](#_Toc185935512)

[1.2. Настройка ISP 11](#_Toc185935513)

[1.3. Создание локальных учетных записей 13](#_Toc185935514)

[1.4 Настройте на интерфейсе HQ-SW в сторону офиса HQ виртуальный коммутатор 15](#_Toc185935515)

[1.5 Настройка безопасного удаленного доступа 18](#_Toc185935516)

[1.6 Между офисами HQ и BR необходимо сконфигурировать ip GRE туннель 20](#_Toc185935517)

[1.7 Обеспечьте динамическую маршрутизацию: ресурсы одного офиса должны быть доступны из другого офиса. 22](#_Toc185935518)

[1.8 Настройка протокола динамической конфигурации хостов. 24](#_Toc185935519)

[1.9 Настройка DNS для офисов HQ и BR. 25](#_Toc185935520)

[1.10 Настройте часовой пояс на всех устройствах, согласно месту проведения экзамена. 28](#_Toc185935521)

[Модуль 2 30](#_Toc185935522)

[2.1 Настройте доменный контроллер Samba на машине BR-SRV. 30](#_Toc185935523)

[2.2 Сконфигурируйте файловое хранилище 35](#_Toc185935524)

[2.3. Сконфигурируйте Ansible на сервере BR-SRV 38](#_Toc185935525)

[2.4 Развертывание приложений в Docker на сервере BR-SRV 40](#_Toc185935526)

[2.5 На маршрутизаторах сконфигурируйте статическую трансляцию портов 44](#_Toc185935527)

[2.6 Запустите сервис moodle на сервере BR-SRV 45](#_Toc185935528)

[2.7 Настройте веб-сервер nginx как обратный прокси-сервер на ISP 50](#_Toc185935529)

[Приложение Б. Пример заполнения таблицы адресов 54](#_Toc185935530)

[Приложение В. Файл users.csv 54](#_Toc185935531)

Модуль 1

Топология сети

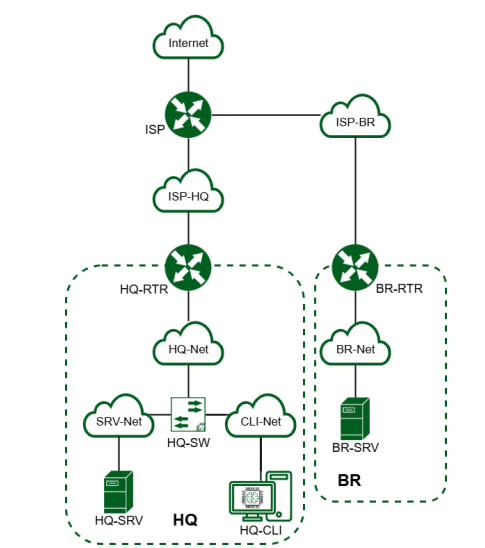


Таблица 1 - IP-адресации

|  |  |  |
| --- | --- | --- |
| Имя устройства | IP-адрес | Шлюз по умолчанию |
| ISP |  |  |
| BR-RTR | 192.168.5.1/28 | 192.168.5.1 |
| BR-SRV | 192.168.3.1/27 | 192.168.3.30 |
| HQ-RTR | 192.168.4.1/28 | 192.168.4.14 |
| HQ-SRV | 192.168.100.1/26 | 192.168.100.62 |
| HQ-SW | 192.168.9.5/29 | 192.168.9.6 |
| HQ-CLI | 192.168.200.1/28 | 192.168.200.14 |

1.Настройка устройств

1.1 Настройка имён устройств согласно топологии

Перед началом работы необходимо сделать базовую настройку устройств: имя и ip адрес. Сменить имя устройства на Debian можно в файле /etc/hostname.



Рисунок 1 – hostname ISP



Рисунок 2 – hostname HQ-SW



Рисунок 3 – hostname BR-RTR



Рисунок 4 – hostname HQ-SRV



Рисунок 5 – hostname BR-SRV



Рисунок 6 – hostname HQ-RTR



Рисунок 7 – hostname HQ-CLI

На всех устройствах необходимо сконфигурировать IPv4.

Поставить на ISP ip address в файле /etc/network/interfaces.

*172.16.4.0/28* – для сети HQ

*172.16.5.0/28* – для сети BR

**Настройка IP-адресации в ALT Linux** — это процесс определения уникального адреса компьютера в формате четырёх трёхзначных десятичных чисел, разделённых точками.  Как правило, каждый сетевой интерфейс имеет не менее одного IP-адреса.

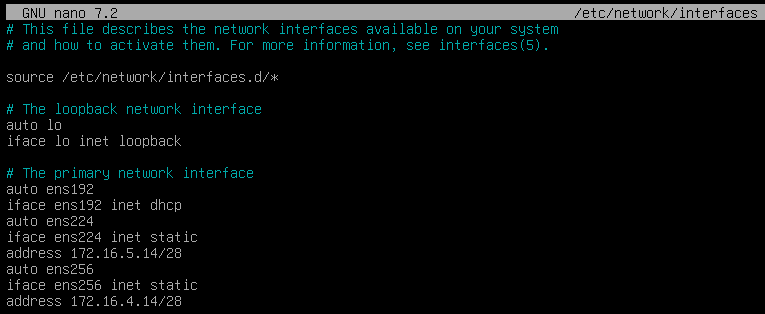


Рисунок 8 – IP-Адреса на ISP

Чтобы все изменения, что мы прописали в файле вступили в силу нам нужно прописать команду systemctl restart networking.

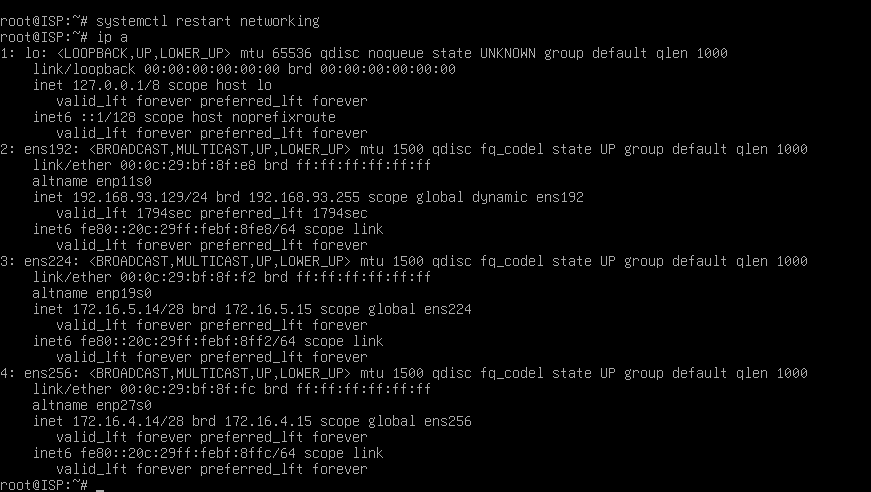


Рисунок 9 – Проверка адресации

Для просмотра интерфейсов мы используем команду ip address. Далее настроим субинтерфейсы на EcoRouter. Service instance является логическим субинтерфейсом, работающим между L2 и L3 уровнями. Данный вид интерфейса необходим для соединения физического порта с интерфейсами L3, интерфейсами bridge, портами.

Vl100 – для hq-srv

Vl200 – для hq-cli

Vl999 – для управления

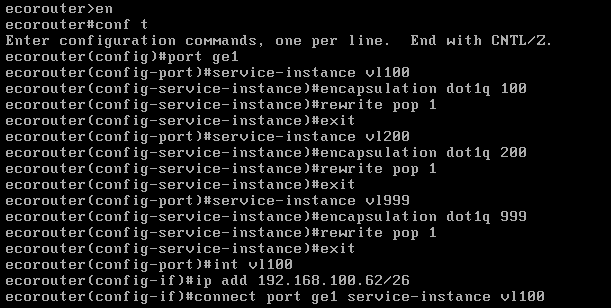


Рисунок 10 – Настройка субинтерфейсов

*192.168.100.0/26* – для hq-srv

*192.168.200.0/28* – для hq-cli

*192.168.9.0/29* – для управления

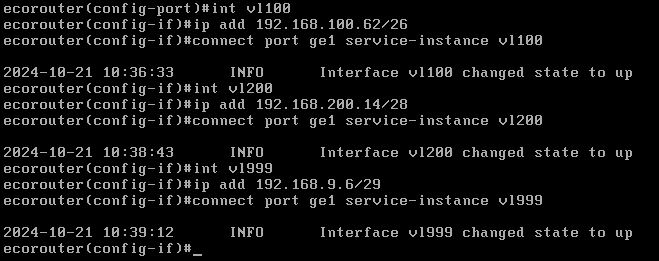


Рисунок 11 – Конфигурация IP

*192.168.3.0/27* – для сети BR

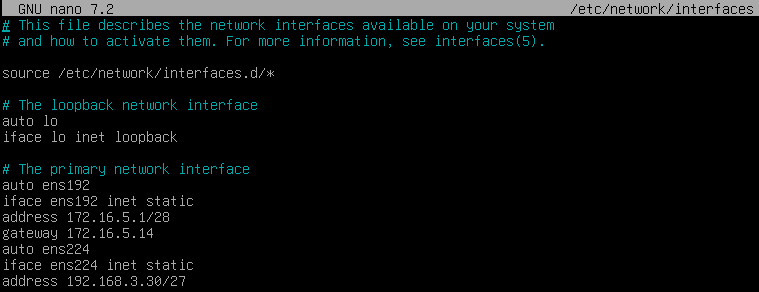


Рисунок 12 – Конфигурация IP

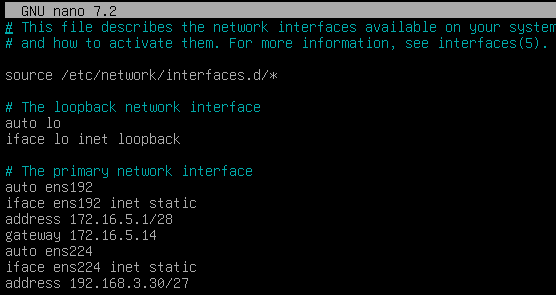


Рисунок 13 – IP-Адреса на BR-RTR

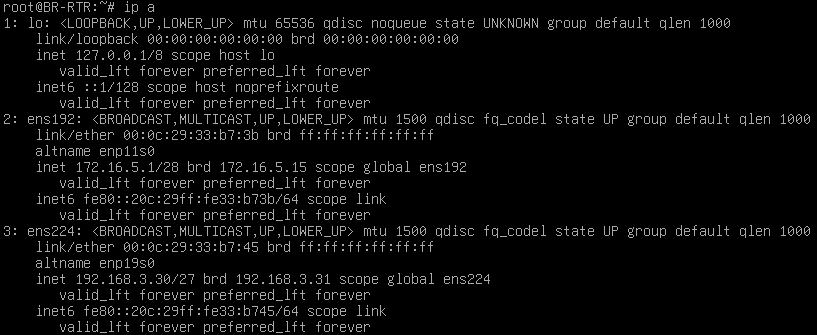


Рисунок 14 – Проверка IP

Смена ip адреса на серверах BR-SRV и HQ-SRV (ALT Linux) происходит следующим образом:

Просматриваем подключения nmcli connection show на рисунке 15.



Рисунок 15 – Просмотр подключений

Удаляем имеющееся соединение, nmcli connection del ‘Проводное соединение’



Рисунок 16 – Удаление соединения

Теперь создадим своё соединение nmcli connection add con-name “[Имя соединения]” type ethernet ifname [интерфейс] connection.autoconnect yes ipv4.method manual ipv4.address [ip address/префикс] ipv4.gateway [шлюз] ipv4.dns [ip address dns сервера]

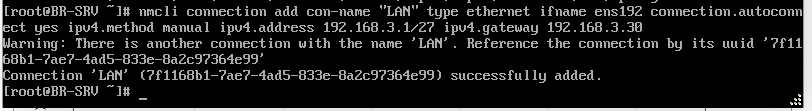


Рисунок 17 – Создание нового подключения

Далее включаем соединение nmcli connection up “имя соединения” и проверяем nmcli connection show.

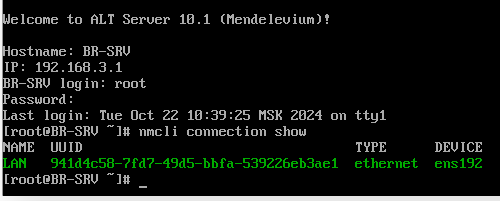


Рисунок 18 – Проверка подключения

1.2. Настройка ISP

Для доступа в сеть интернета нужно настроить PAT.

Для начала следует включить пакеты для доступа на другие интерфейсы, для этого необходимо сначала перейти в файл /etc/sysctl.conf, и в строку net.ipv4.ip\_forward=1 (аналогично тому делаем на HQ-SW).

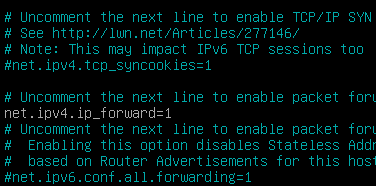


Рисунок 19 – Включение форвардинга

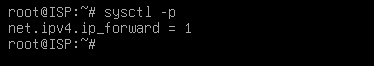


Рисунок 20 – Применение настроек

Для того, чтобы устанавливать дополнительное ПО, необходимо настроить репозитории в файле /etc/apt/sources.list, то же нужно сделать на HQ-SW.

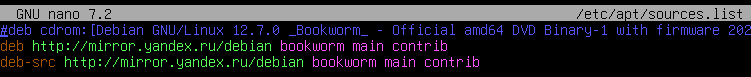


Рисунок 21 - Настройка репозиторий

Далее устанавливаем пакеты iptables и создаём правила PAT.

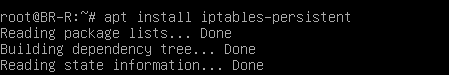


Рисунок 22 – Установка iptables

Правило PAT следует сохранить в файл /etc/iptables/rules.v4.



Рисунок 23 – Настройка PAT

На EcoRouter создаём пулы NAT и привязываем их к внешнему интерфейсу, как показано на рисунках 24-27.

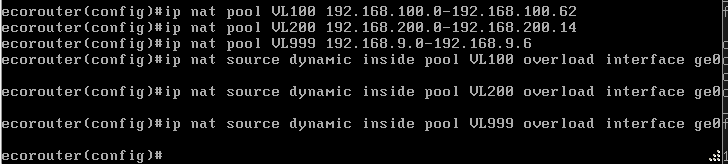


Рисунок 24 – Настройка NAT на HQ-RTR

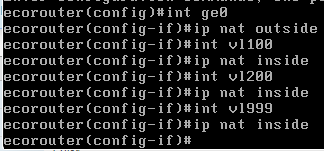


Рисунок 25 – Внешняя и внутренние интерфейсы

Так как правило iptables не установлено на машину, для начала нужна установка этого правила, как показано на рисунке 26.

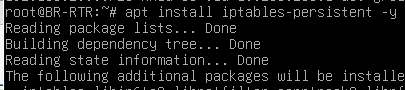


Рисунок 26 – Установка iptables



Рисунок 27 – Создание правила

1.3. Создание локальных учетных записей

useradd -u [ id ] [имя ]- создание пользователя

passwd [пользователя] – смена пароля

**SSH (Secure Shell) на Linux** ‒ сетевой протокол прикладного уровня, предназначенный для безопасного удалённого доступа к различным системам. В основном он нужен для удалённого управления данными пользователя на сервере, запуска служебных команд, работы в консольном режиме с базами данных.

Производим настройку SSH и создадем нового пользователя на HQ-SRV и BR-SR, как показано на рисунке 28.



Рисунок 28 – Создание пользователя

Настройка ранее созданного пользователя sshuser, как показано на рисунке 29.

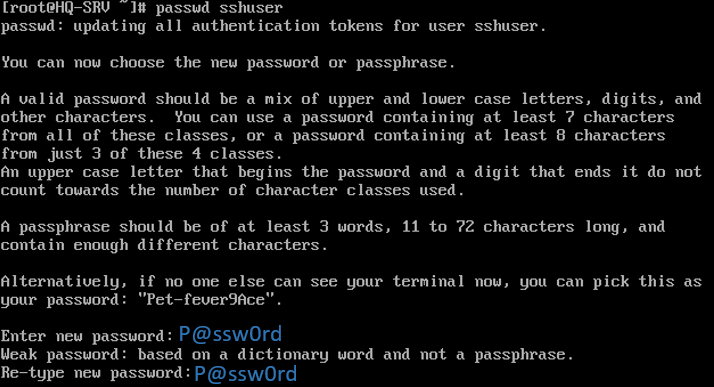


Рисунок 29 – Создание локальной учетной записи на серверах

Пользователь sshuser должен иметь возможность запускать sudo без дополнительной аутентификации, для этого можно сделать в visudo /etc/sudoers. Редактирование так же как VI (наводим курсор – переходим в режим редактирования клавишей I – редактируем – нажимаем ESC – Вводим : wq - Enter). Те же действия нужно выполнить на BR-SRV.

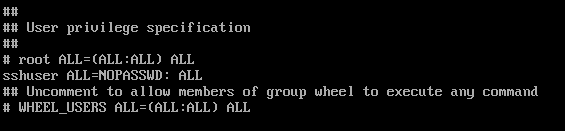


Рисунок 30 – Выдача прав на исполнения sudo без запроса пароля



Рисунок 31 – Проверка

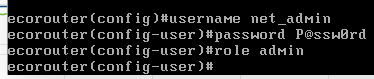


Рисунок 32 – Создание пользователя на маршрутизаторах

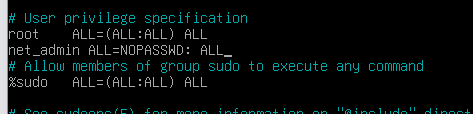


Рисунок 33 – Выдача прав на исполнения sudo без запроса пароля

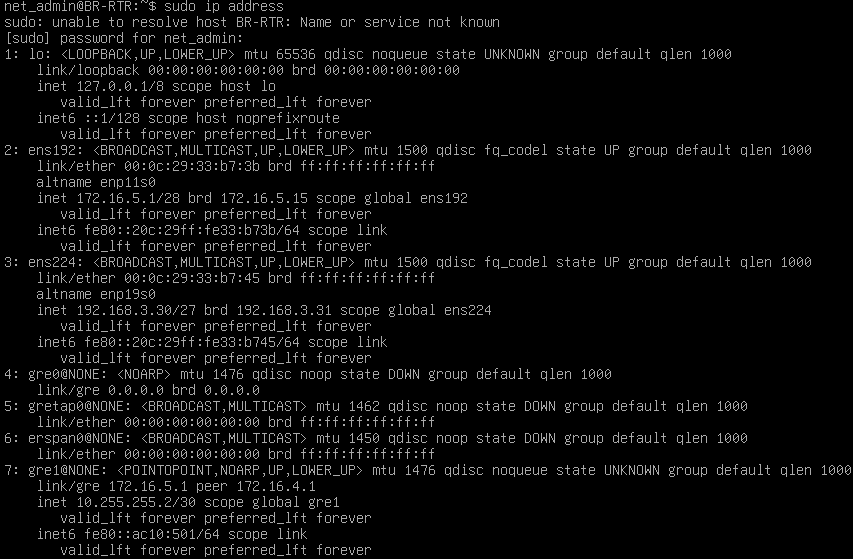


Рисунок 34 – Проверка

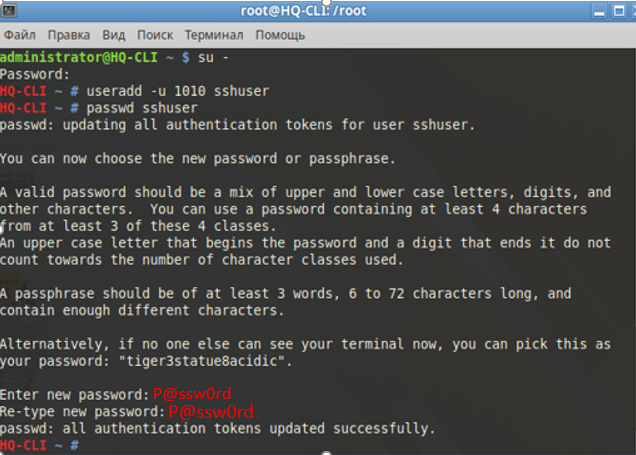


Рисунок 35 – Создание пользователя на HQ-CLI

1.4 Настройте на интерфейсе HQ-SW в сторону офиса HQ виртуальный коммутатор

На ISP нужно настроить репозитории для установки дополнительных ПО.

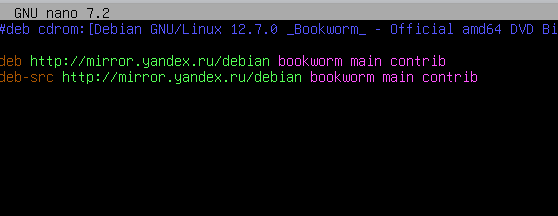


Рисунок 36 – Запись репозиторий



Рисунок 37 – Включение форвардинга



Рисунок 38 – Применение настроек

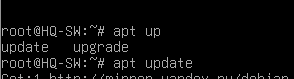


Рисунок 39 – Обновление репозиторий

**Open vSwitch — программный многоуровневый коммутатор с открытым исходным текстом**, предназначенный для работы с гипервизорами.

Теперь установка и настройка openvswitch.



Рисунок 40 – Установка Openvswitch

Произведём добавление коммутатора HQ-SW в ПО openvswitch и настроим режимы доступа и trunk соединение на данном коммутаторе.

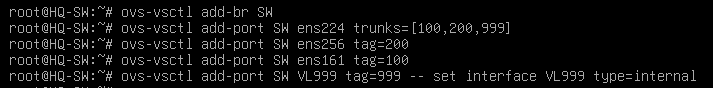


Рисунок 41 – Добавление виртуального коммутатора и портов

Далее настройка интерфейсов HQ-SW в файле конфигурации: /etc/network/interfaces.

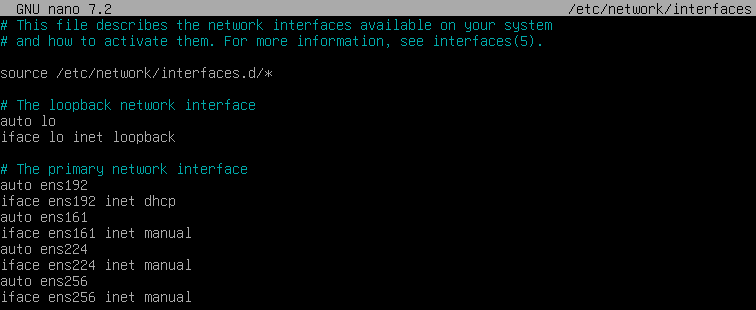


Рисунок 42 – Настройка интерфейсов

Создаём скрипт OVS.SH, который используется для управления Open vSwitch.



Рисунок 43 – Создание файла со скриптом автозагрузки

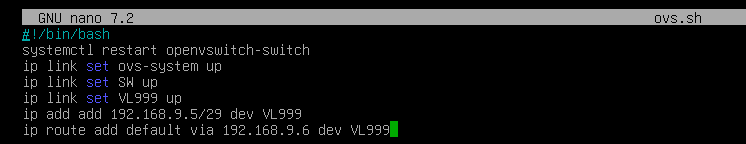


Рисунок 44 – Редактирование файла ovs.sh

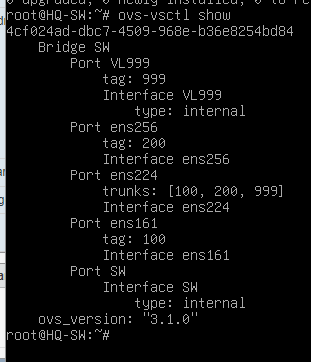


Рисунок 45 – Проверка конфигурации

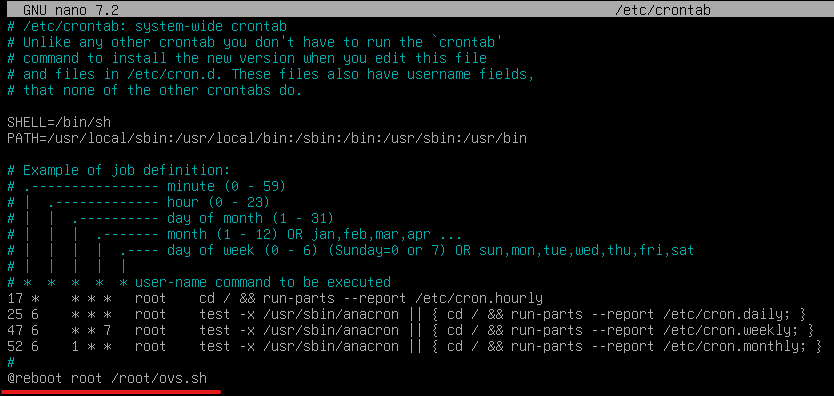


Рисунок 46 – Добавление в автозагрузку

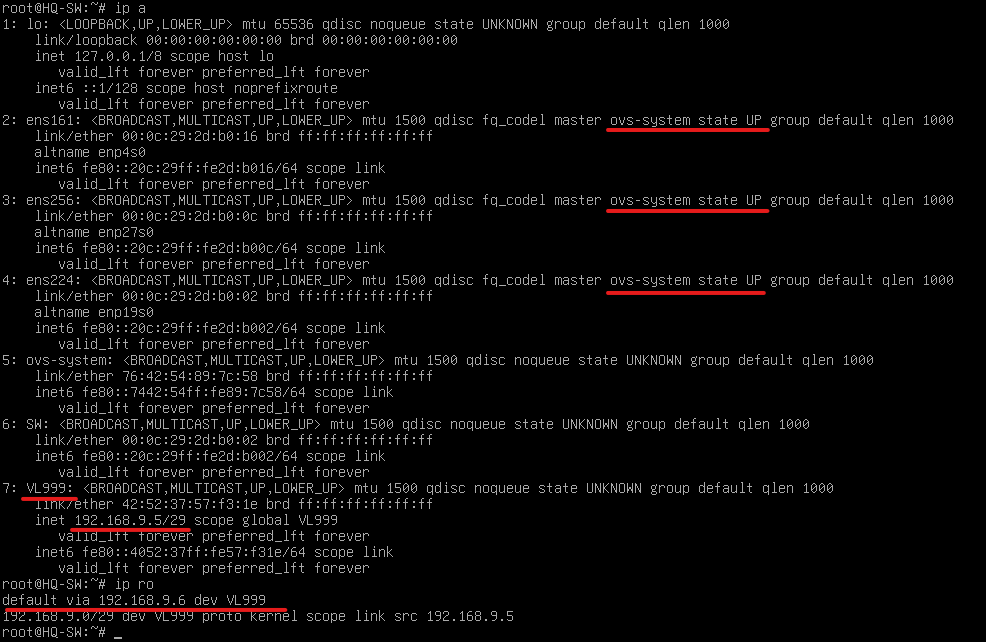


Рисунок 47 – Проверка адресации

1.5 Настройка безопасного удаленного доступа

Для того. чтобы безопасно и удаленно подключиться к устройствам нужно настроить ssh. Настройка включает в себя: подключение по порту 2024(22), разрешение подключения только пользователю sshuser(net\_admin), ограничение количества попыток входа до двух и настройка баннер «Authorized access only».



Рисунок 48 – Установка SSH



Рисунок 49 – Перезагрузка daemon

В файле конфигурации /etc/openssh/sshd\_config прописываем: по какому порту будет подключение, максимальное количество попыток входа, аутентификация по паролю, какому пользователю разрешено подключение и путь до баннера.

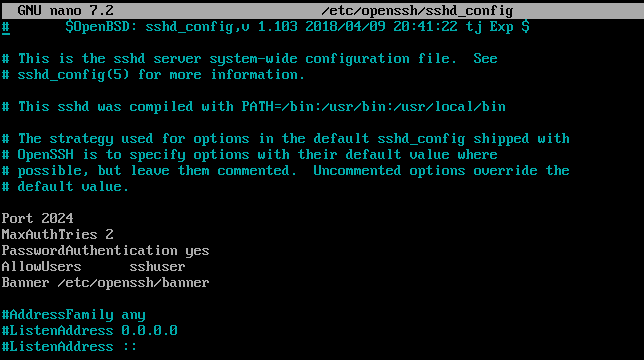


Рисунок 50 – Конфигурация файла sshd\_config



Рисунок 51 – Запись баннера

Подключаемся к ssh командой: ssh полизователь@ip\_address -p порт

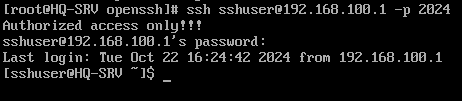


Рисунок 52 – Проверка подключения

На BR-SRV и других устройствах настройка осуществляется аналогично тому как мы производили настройку до этого.

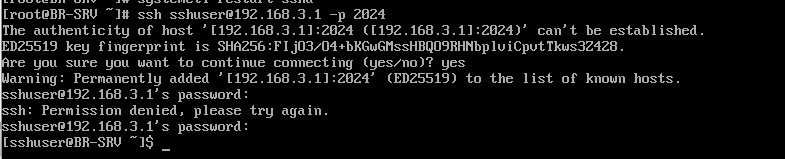


Рисунок 53 – Проверка подключения

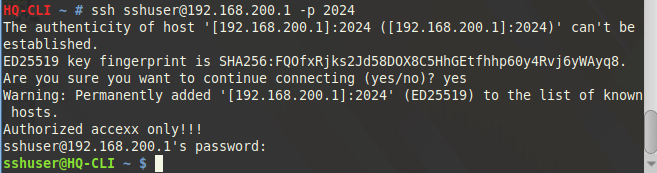


Рисунок 54 – Проверка подключения

На BR-RTR ssh подключается под пользователем net\_admin и по порту 22.

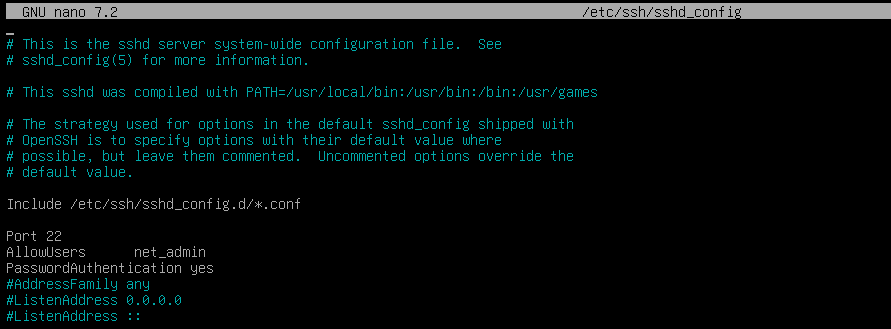


Рисунок 55 – Конфигурация файла sshd\_config



Рисунок 56 – Проверка подключения

1.6 Между офисами HQ и BR необходимо сконфигурировать ip GRE туннель

**GRE-туннели в Linux —** это**простейшие туннели для соединения двух Linux-станций,** поддерживающие инкапсуляцию в том числе и широковещательного трафика.

Производим настройка туннеля GRE, как показано на рисунках 57-61.

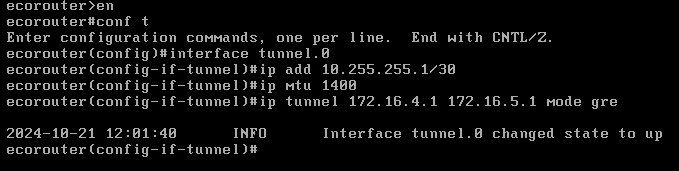


Рисунок 57 – Настройка туннеля на HQ-RTR

*touch gre.up* – создание файла

*chmod + x gre.up* – изменение прав доступа к файлу

*nano ./gre.up* – редактирование файла

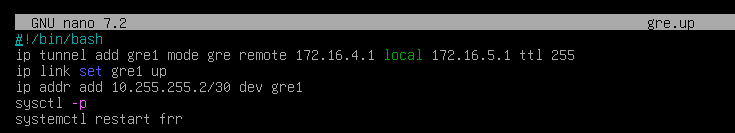


Рисунок 58 – Настройка туннеля на BR-RTR

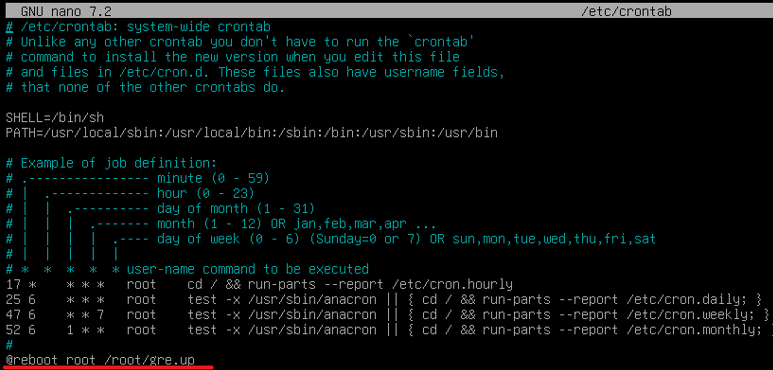


Рисунок 59 – Добавление в автозагрузку

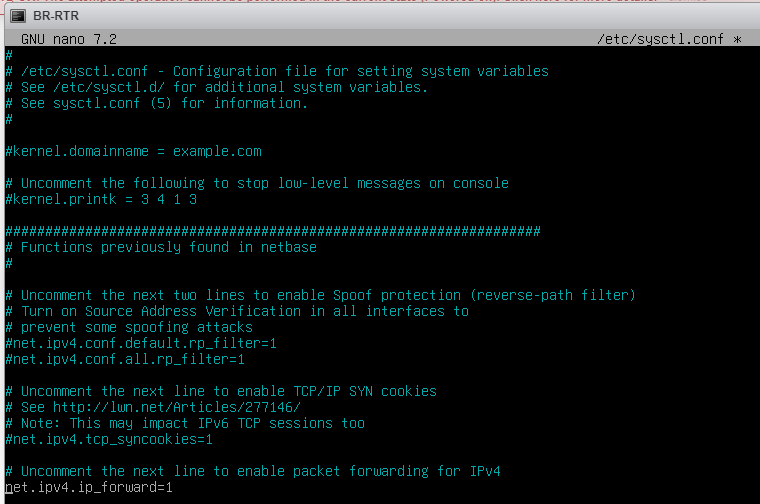


Рисунок 60 - Включение форвардинга



Рисунок 61 – Применение настроек

Чтобы настройки forward применялись вместе с GRE, добавляем в файл gre.up команду sysctl –p.

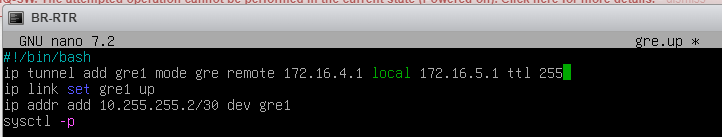


Рисунок 62 – Изменение файла

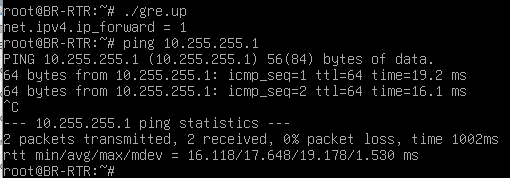


Рисунок 63 – Запуск скрипта

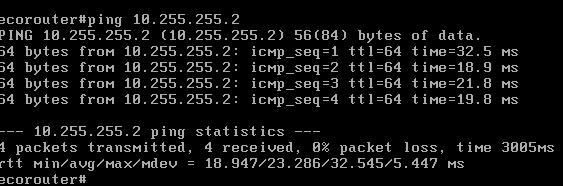


Рисунок 64 – Проверка связи с BR-RTR

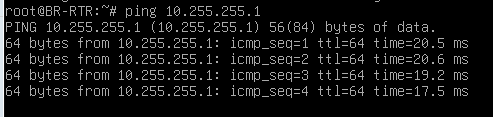


Рисунок 65 – Проверка связи с HQ-RTR

1.7 Обеспечьте динамическую маршрутизацию: ресурсы одного офиса должны быть доступны из другого офиса.

Динамическая маршрутизация OSPF будет осуществляться на интерфейсах туннелей. Туннель использует подключение точка-точка, поэтому на его интерфейсе обязательно нужно прописать команду: ip ospf network point-to-point. Настройка OSPF показана на рисунках 66–67.

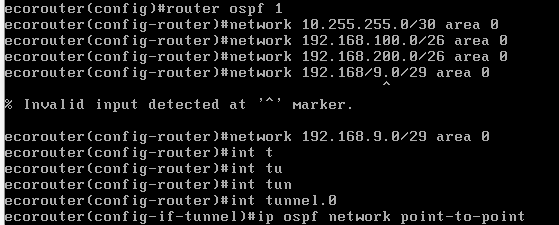




Рисунок 66 – Настройка ospf на HQ-RTR

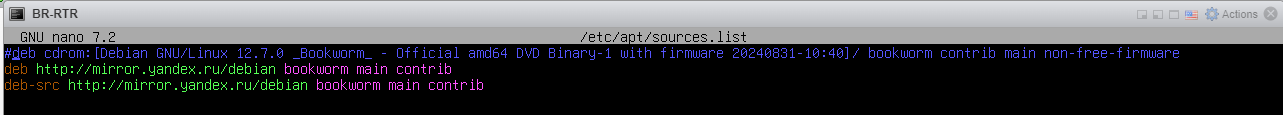


Рисунок 67 – Настройка репозиториев

На RB-RTR нужно установить FRR.

Free Range Routing или FRRouting или FRR — это программный пакет сетевой маршрутизации, работающий на Unix-подобных платформах, в частности, Linux.

Настройка показана на рисунках 68 – 74.

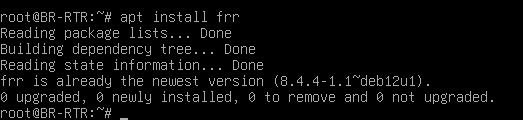


Рисунок 68 – Установка пакета frr

В файле /etc/frr/daemons включаем ospfd. И перезагружаем Systemctl restart frr.

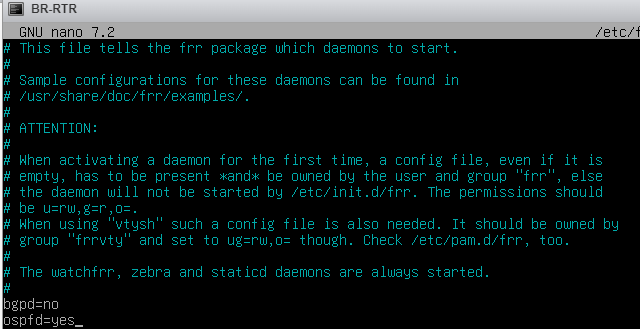


Рисунок 69 – Включение ospf

Переходим в редактор vtysh для настройки ospf.

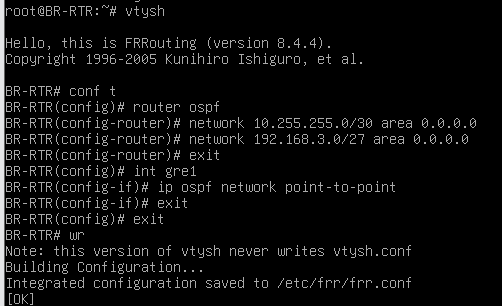


Рисунок 70 – Настройка ospf на BR-RTR

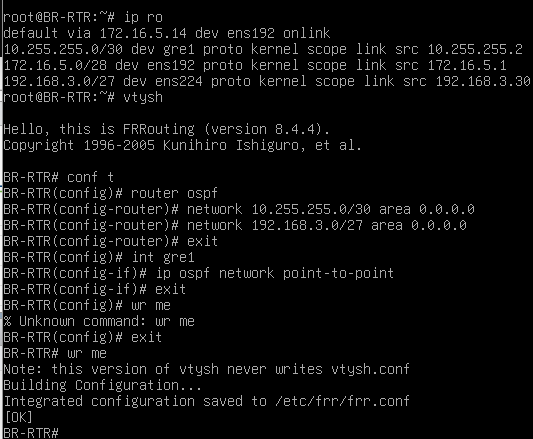


Рисунок 71 – Настройка ospf на BR-RTR

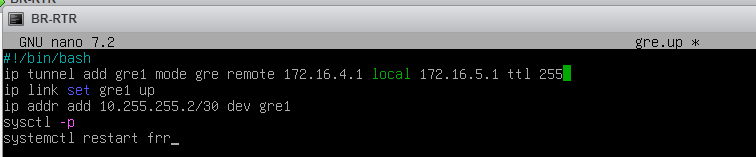


Рисунок 72 – Добавление в автозапуск



Рисунок 73 – Проверка работоспособности на HQ-RTR



Рисунок 74 – Проверка работоспособности на BR-RTR

1.8 Настройка протокола динамической конфигурации хостов.

Для сети клиента 192.168.200.0/28 нужно на EcoRoutere настроить DHCP.

В параметрах dhcp указываем:

Pool VL200 – пул адресов

Mask 28 - префикс

Gateway *192.168.200.14* – шлюз

Dns *8.8.8.8* – dns-server

Domain-mane au-team.irpo – имя домена

Domain-search au-team.irpo – второе имя домена

После привязываем dhcp-server к субинтерфейсу клиента.

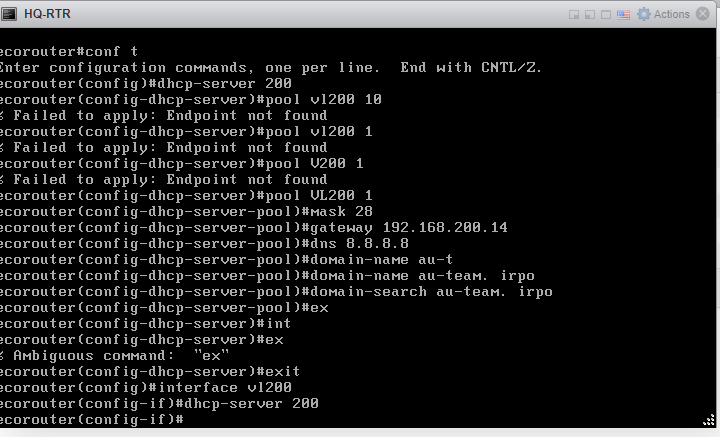


Рисунок 75 – Настройка DHCP

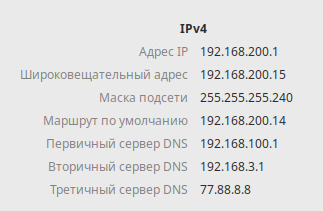


Рисунок 76 – Проверка работоспособности DHCP

1.9 Настройка DNS для офисов HQ и BR.

Чтобы иметь возможность обращаться по имени, необходимо настроить DNS сервер.

Bind — открытая и наиболее распространённая реализация DNS-сервера, обеспечивающая выполнение преобразования DNS-имени в IP-адрес и наоборот.



Рисунок 77 – Установка Bind



Рисунок 78 – Установка nano

В файле /etc/bind/options.conf прописываем локальный ip address сервера, адрес сервера пересылки и разрешаем запросы.

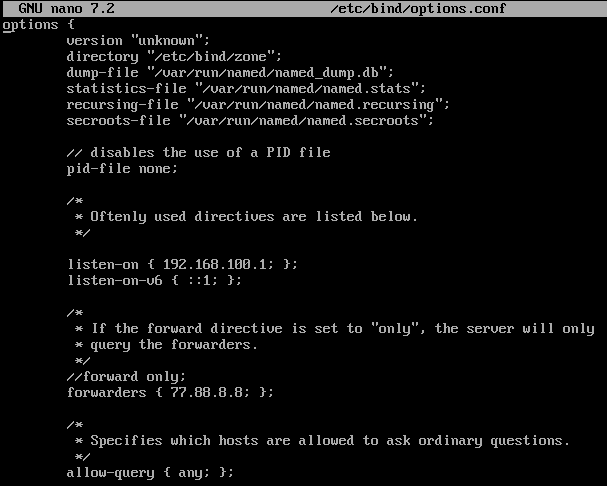


Рисунок 79 – Выбор DNS сервера

В файле /etc/bind/rfc1912.conf пишем имена зон и названия файлов, в которых они находятся.

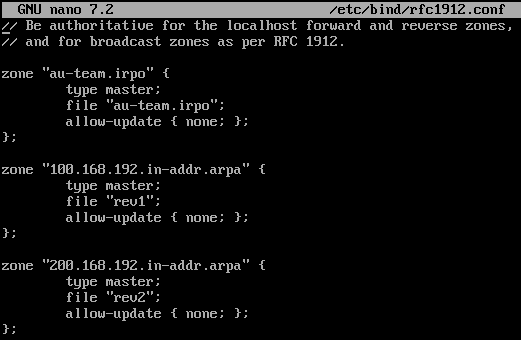


Рисунок 80 – Создание DNS зон

Копируем и переименовываем, созданные по умолчанию зоны.

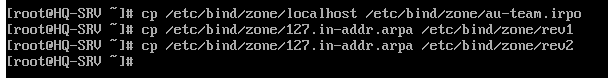


Рисунок 81 – Копирование зон

Заполняем зоны прямого и обратного просмотра.

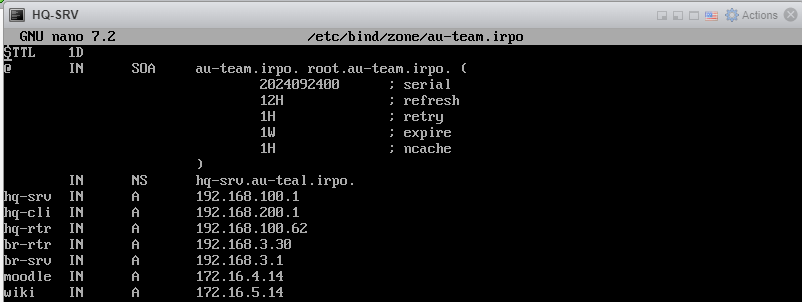


Рисунок 82 – Редактирование прямой зоны

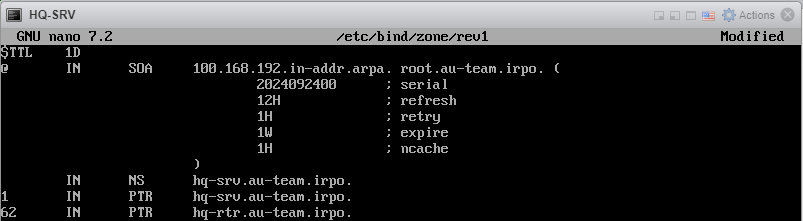


Рисунок 83 – Редактирование обратной зоны rev1

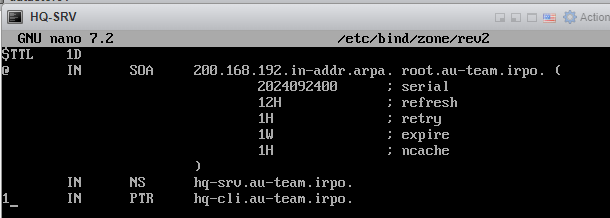


Рисунок 84 – Редактирование обратной зоны rev2

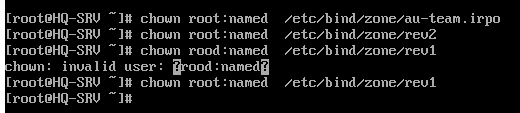


Рисунок 85 – Редактирование прав



Рисунок 86 – Перезапуск службы bind

Проверяем работоспособность bind командой nslookup.



Рисунок 87 – Проверка работоспособности DNS

1.10 Настройте часовой пояс на всех устройствах, согласно месту проведения экзамена.

Для того, чтобы настроить часовой пояс используется команда timedatectl set-timezone [ZONE]. Перед этим нужно посмотреть доступные зоны timedatectl list-timezones.

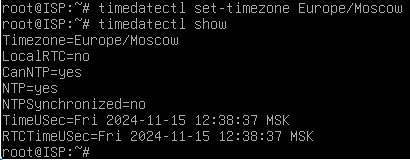


Рисунок 88 – Часовой пояс на ISP

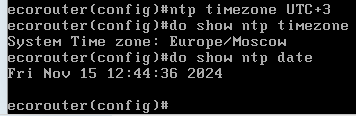


Рисунок 89 – Часовой пояс на EcoRouter

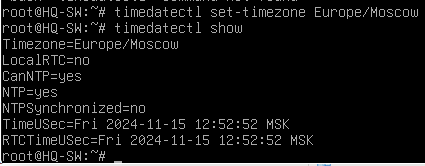


Рисунок 90 – Часовой пояс на HQ-SW

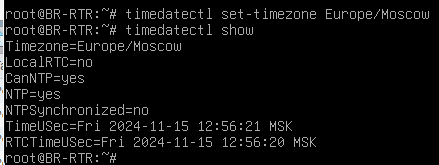


Рисунок 91 – Часовой пояс на BR-RTR

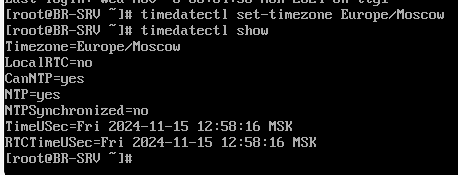


Рисунок 92 – Часовой пояс на BR-SRV

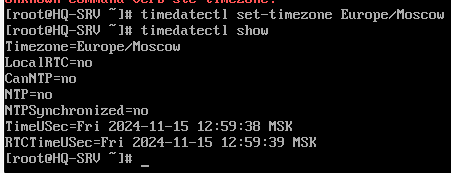


Рисунок 93 – Часовой пояс на HQ-SRV

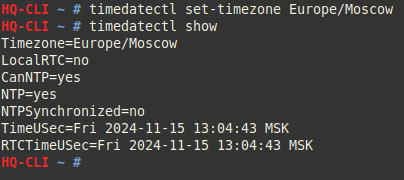


Рисунок 94 – Часовой пояс на HQ-CLI

# Модуль 2

# 2.1 Настройте доменный контроллер Samba на машине BR-SRV.

Настройка Samba в Linux включает в себя **установку и настройку файлового сервера**с общим доступом и гибкими настройками прав для пользователей.

Устанавливаем Samba.

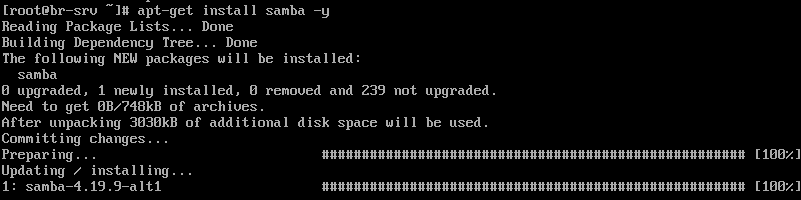


Рисунок 95 – Установка Samba

Для сервера должно быть установлено правильное имя узла и домена. Для этого в файл /etc/sysconfig/network необходимо добавить строку:

HOSTNAME=br-srv.au-team.irpo

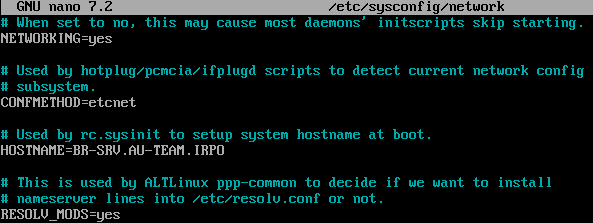


Рисунок 96 – Замена имени с добавлением домена

Очищаем базы и конфигурацию Samba, как показано на рисунке 96.

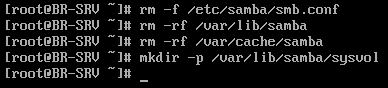


Рисунок 97 – Очищение базы данных Samba

Далее необходимо настроить контроллер домена samba, как показано на рисунках 98-100.



Рисунок 98 – Настройка котроллера домена

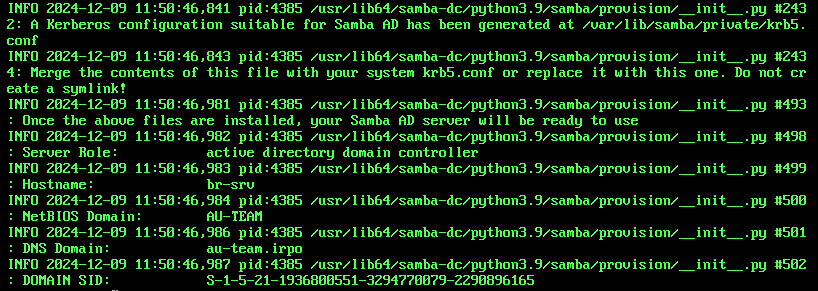


Рисунок 99 – Настройка котроллера домена

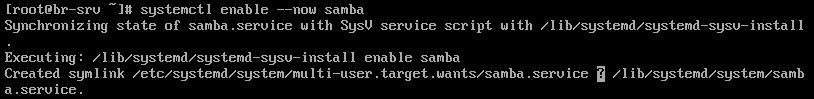


Рисунок 100 – Настройка котроллера домена

В файле /etc/krb5.conf нужно раскомментировать строку default\_realm и содержимое разделов realms и domain\_realm и указать название домена, в строке dns\_lookup\_realm должно быть установлено значение false.

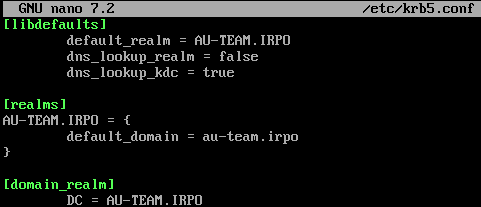


Рисунок 101 – Настройка Kerberos

Теперь проверяем работоспособность домена.

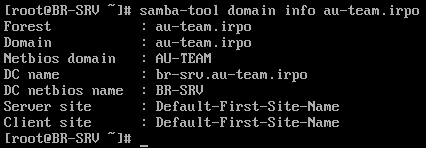


Рисунок 102 – Просмотр информации о домене

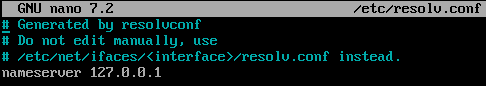


Рисунок 103 – Проверка конфигурации DNS  


Рисунок 104 – Проверка имени хостов

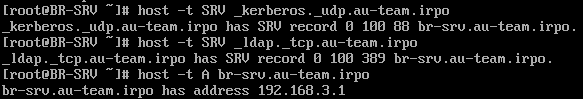


Рисунок 105 – Проверка имени хостов

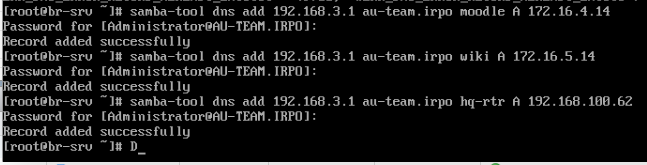


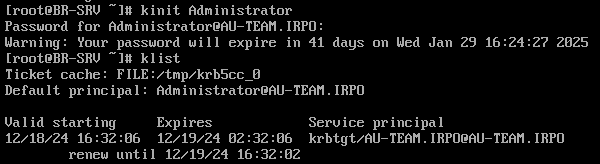
Рисунок 106 – Записи прямой зоны DNS

Рисунок 107 – Выдача билeта Kerberos

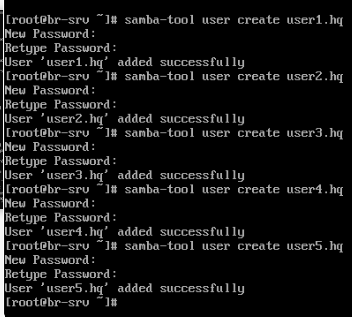


Рисунок 108 – Создание пользователей

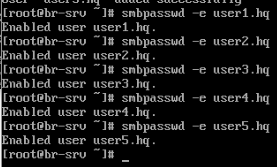


Рисунок 109 – Включение



Рисунок 110 – Создание группы

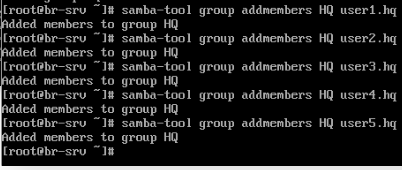


Рисунок 111 – Добавление пользователей в группу

Далее необходимо выполнить проверку Kerberos, как показано на рисунке 112.

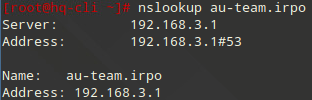


Рисунок 112 – Проверка доступа по dns

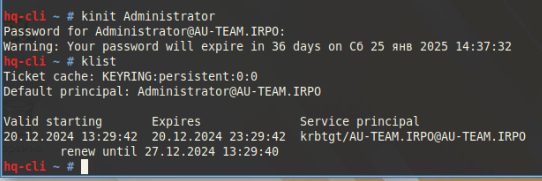


Рисунок 113 – Билет Kerberos

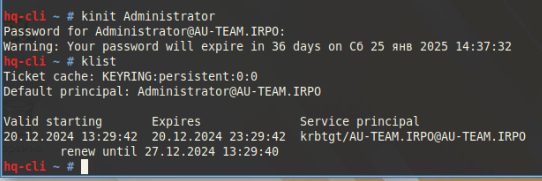


Рисунок 114 – Билет Kerberos

После этого необходимо ввести клиента в домен. Процесс показан на рисунках 115-117.

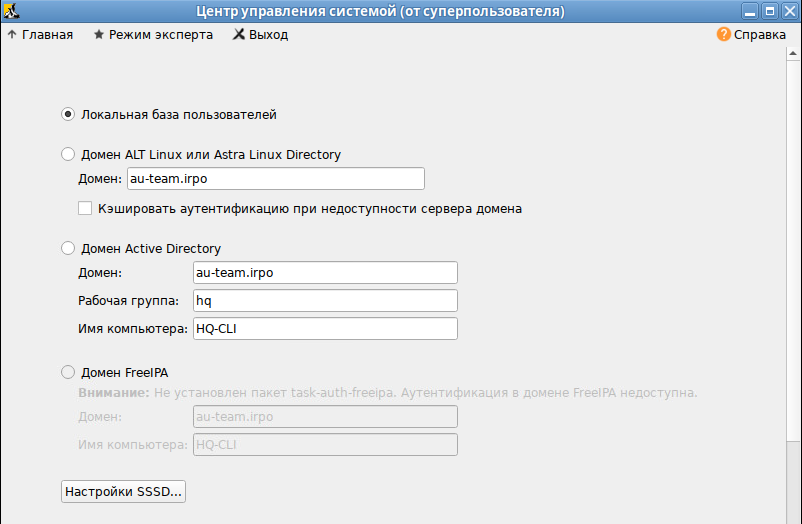


Рисунок 115 – Ввод клиента в домен

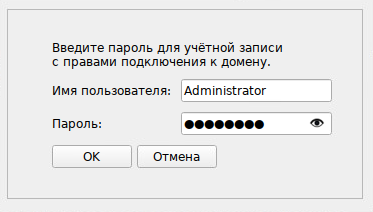


Рисунок 116 – Подтверждение учетной записи

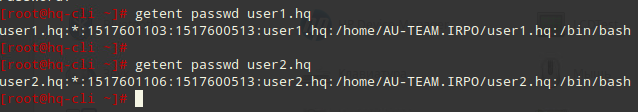


Рисунок 117 – Проверка доменного пользователя

Проверим возможность аутентификации пользователя на клиенте, как показано на рисунке 118.

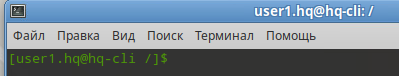


Рисунок 118 – Проверка возможности аутентификации

Пользователи группы HQ должны иметь возможность повышать

привилегии для выполнения ограниченного набора команд: cat, grep, id.

Запускать другие команды с повышенными привилегиями пользователи

группы не имеют права.

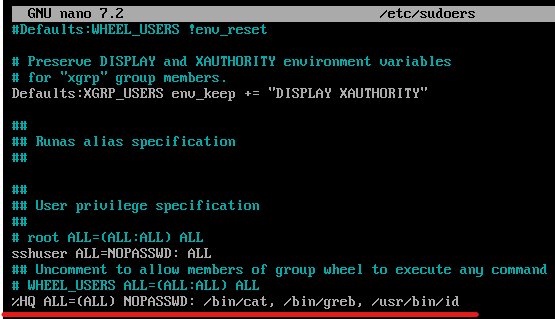
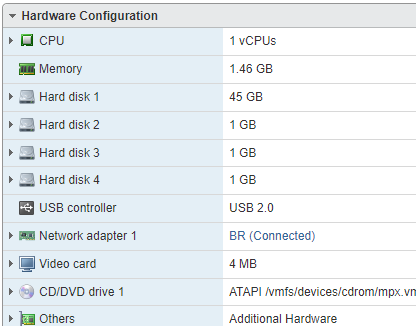


Рисунок 119 – Повышение привилегий

2.2 Сконфигурируйте файловое хранилище

Добавим дисков на HQ-SRV:

  
Рисунок 120 – Добавление дисков

Диски должны быть видны в каталоге /dev на HQ-SRV

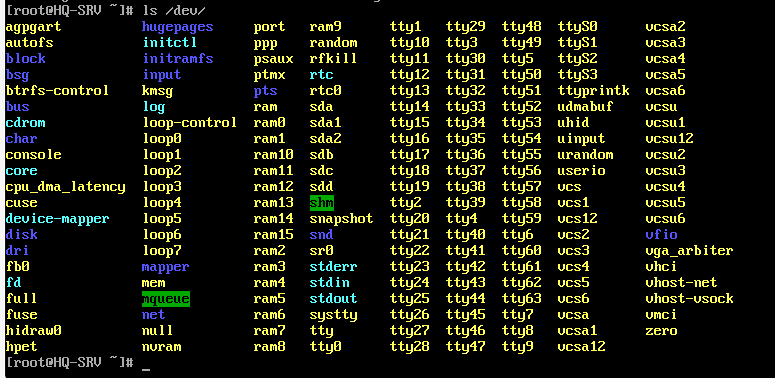


Рисунок 121 – Просмотр дисков

Диски должны быть видны в каталоге /dev на HQ-SRV.

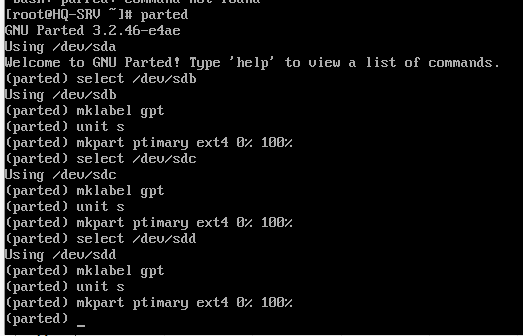


Рисунок 122 – Подготовка дисков

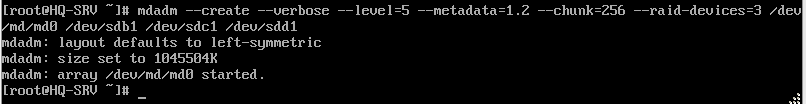


Рисунок 123 – Создание массива

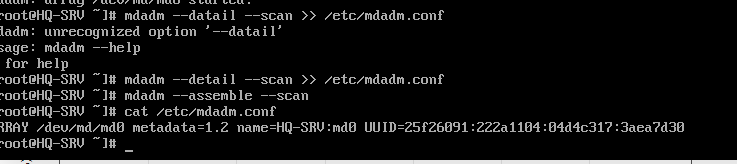


Рисунок 124 – Сбор компонентов в массив

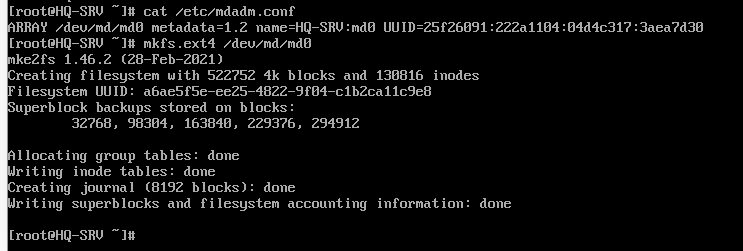


Рисунок 125 – Форматирование RAID

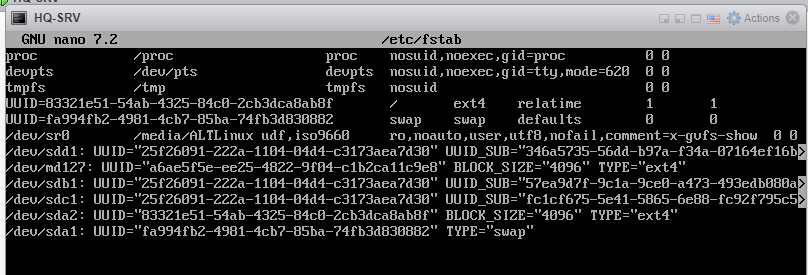


Рисунок 126 – Таблица файловых систем



Рисунок 127 – Редактирование таблицы

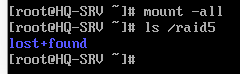


Рисунок 128 – Монтирование и проверка

NFS обеспечивает пользователям доступ к файлам, расположенным на удаленных компьютерах, и позволяет работать с этими файлами точно так же, как и с локальными.



Рисунок 129 – Установка NFS сервера



Рисунок 130 – Создание папки

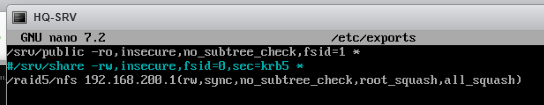


Рисунок 131 – Экспортируемый каталог

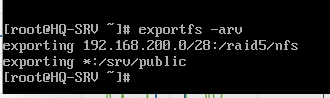


Рисунок 132 – Экспорт

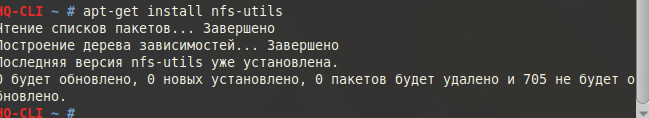


Рисунок 133 – Установка утилит NFS



Рисунок 134 – Создание папки



Рисунок 135 – Монтирование общей папки



Рисунок 136 – Автомонтирование



Рисунок 137 – Создание файла для проверки



Рисунок 138 – Проверка

2.3. Сконфигурируйте Ansible на сервере BR-SRV

Ansible помогает автоматизировать настройку удалённых серверов в сети и управление ими. Он позволяет управлять конфигурациями машин, доставлять и развёртывать приложения, а также выполнять другие задачи администрирования без ручного вмешательства. Настройка показана на рисунках 139 – 142.



Рисунок 139 – Установка ansible



Рисунок 140 – Смена mtu

sshpass — утилита, которая позволяет выполнять команды на удалённом сервере по SSH без ввода пароля вручную



Рисунок 141 – Установка sshpass

Чтобы при подключении по SSH проверка ключей была отключена, нужно в файле /etc/ansible/ansible.cfg раскомментировать строку: host\_key\_checking=False.

Это полезно, когда с управляющего хоста Ansible надо подключиться к большому количеству устройств первый раз.

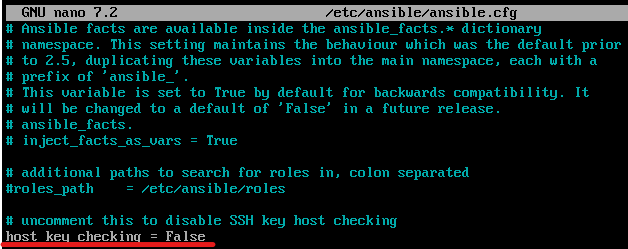


Рисунок 142 - Host в конфигурации ansible

Далее необходимо отредактировать файл Host чтобы суметь зайти на HQ-CLI под пользователем root. Процесс показан на рисунке 143.

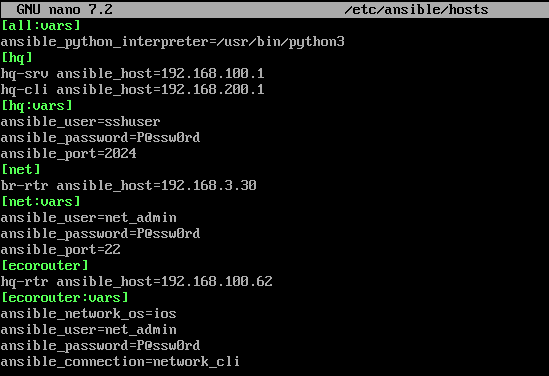


Рисунок 143 – Конфигурация файла hosts

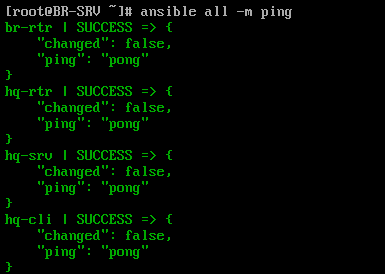


Рисунок 144 – Проверка работоспособности

2.4 Развертывание приложений в Docker на сервере BR-SRV

Docker на ALT Linux — это**технология контейнеризации с открытым исходным кодом для построения и контейнеризации приложений.** Она позволяет упаковывать приложения и все их зависимости в контейнеры, что обеспечивает их стабильную работу в любых средах. Настройка Wiki с помощью docker показана на рисунке 145.



Рисунок 145 – Установка Docker

Далее необходимо отредактировать /etc/docker/daemon.json, как показано на рисунке 146.



Рисунок 146 – Конфигурация daemon.json

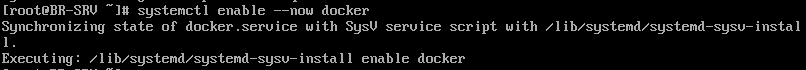


Рисунок 147 – Включение Docker

Далее необходимо подготовить файл конфигураций для mediawiki, как показано на рисунке 148.

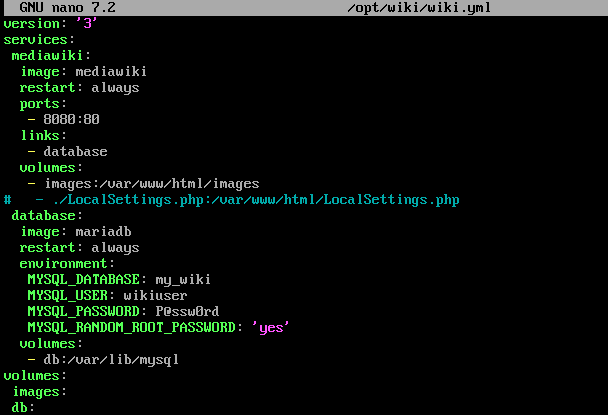


Рисунок 148 - Файл конфигураций

После этого необходимо поднять docker, чтобы все изменения вступили в силу. Делается это при помощи следующих команд:

cd /opt/wiki

docker-compose –f wiki.yml up

Будет происходить долгое включение сервиса, поэтому для перехода во вторую консоль используем комбинацию клавиш Ctrl+Alt+F2.

Для отображения списка запущенных контейнеров используется команда docker ps. Применение этой команды представлено на рисунке 149.

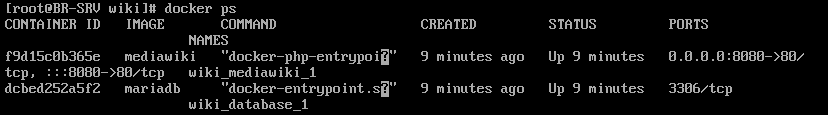


Рисунок 149 - Команда docker ps

Далее с клиента HQ-CLI запускаем браузер и до настраиваем mediawiki, как показано на рисунках 150-153.

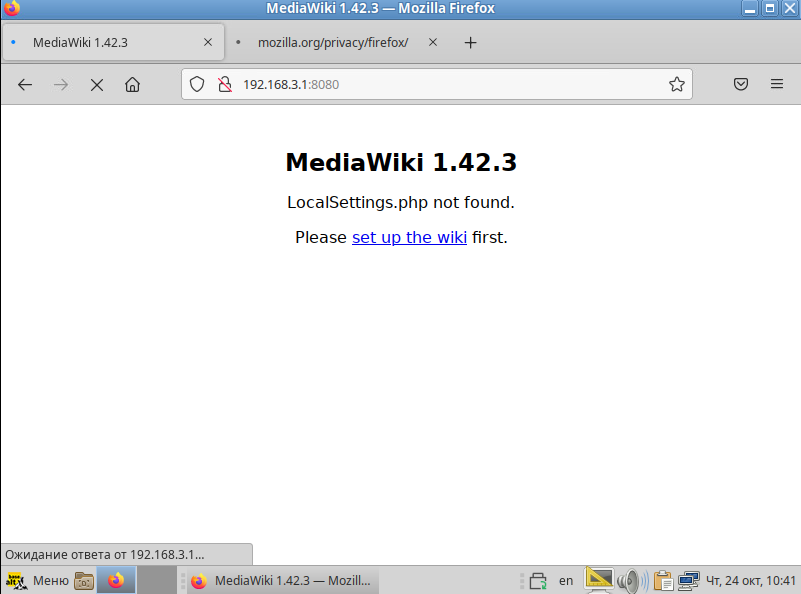


Рисунок 150 – Настройка mediawiki

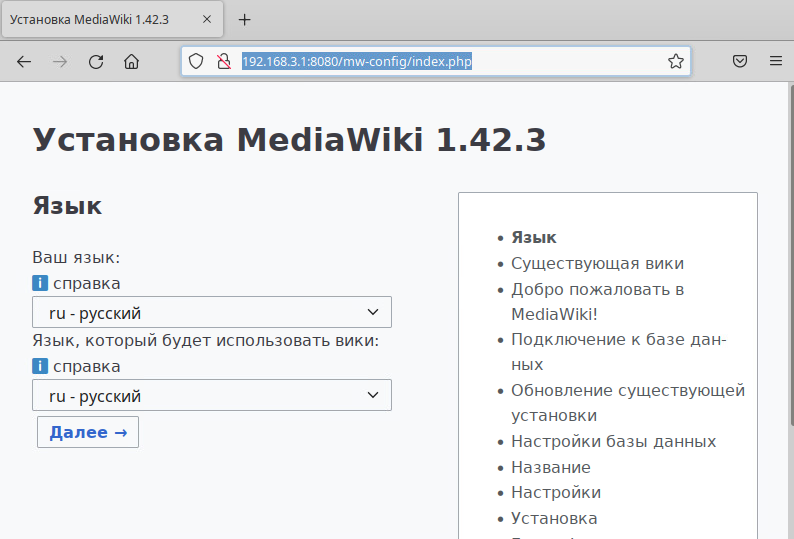


Рисунок 151 – Настройка mediawiki

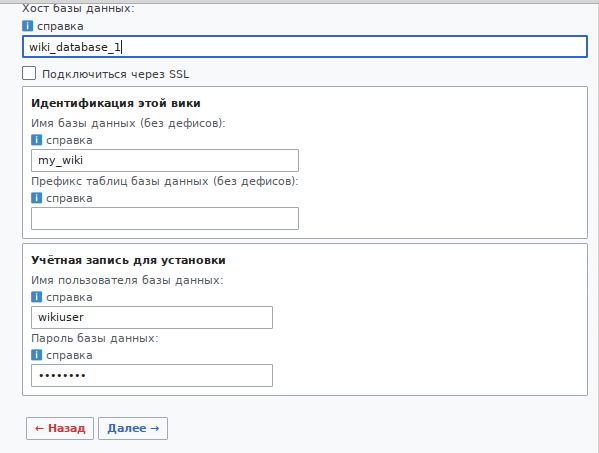


Рисунок 152 – Настройка mediawiki

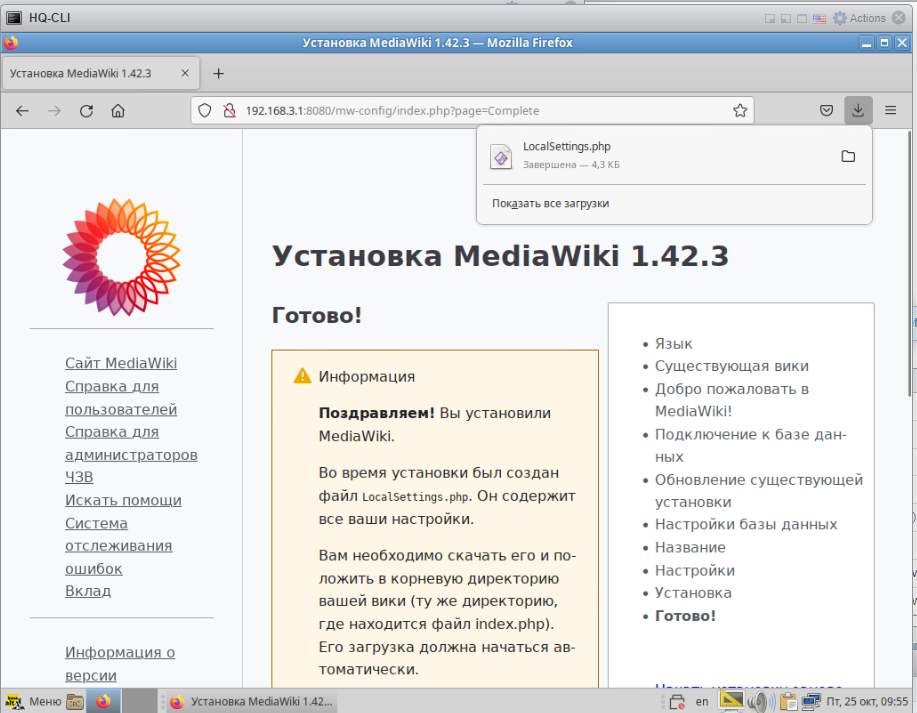


Рисунок 153 – Завершение установки

Далее скопируем файл на BR-SRV с HQ-CLI, как показано на рисунках 154-159.



Рисунок 154 – Копирование файла

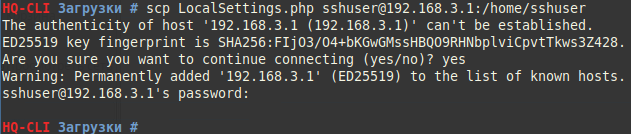


Рисунок 155 – Копирование файла



Рисунок 156 – Копирование файла

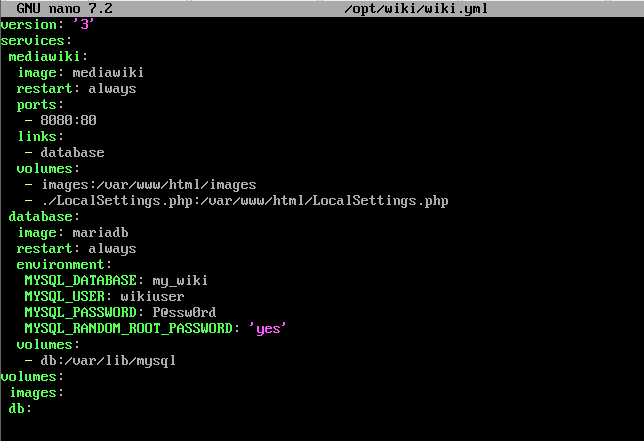


Рисунок 157 – Копирование файла

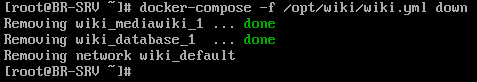


Рисунок 158 – Копирование файла

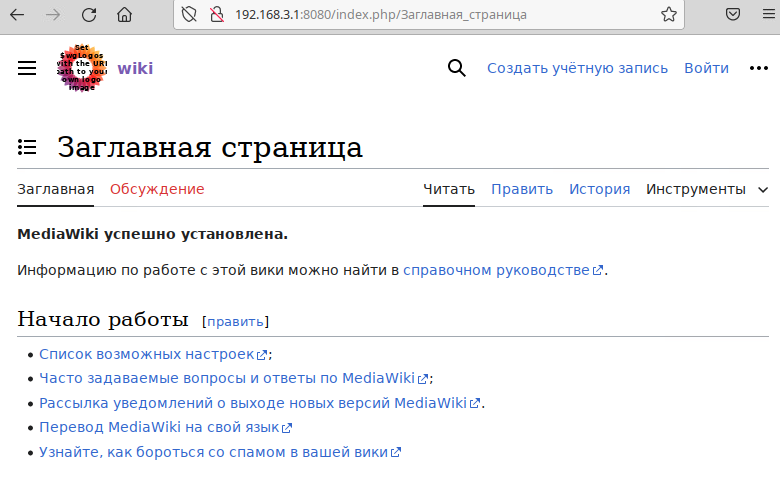


Рисунок 159 – Копирование файла

2.5 На маршрутизаторах сконфигурируйте статическую трансляцию портов

Для доступа к серверам, находящимся за межсетевым экраном, можно настроить переадресацию портов (проброс портов, port forwarding). Это позволяет получать доступ к серверу, не зная внутреннего IP-адреса сервера. Пользователи также могут подключаться, используя только те порты, которые были выбраны. Настройка показана на рисунках 160 – 162.



Рисунок 160 – Проброс для HQ-SRV



Рисунок 161 – Проброс для BR-SRV wiki



Рисунок 162 – Проброс для BR-SRV

2.6 Запустите сервис moodle на сервере BR-SRV

Moodle (модульная объектно-ориентированная динамическая учебная среда) – это веб-система для организации дистанционного обучения и управления им.



Рисунок 163 - Установка Apache2

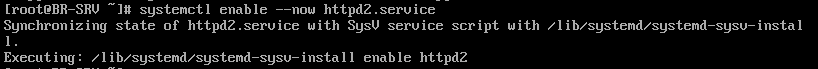


Рисунок 164 – Включение http сервиса

Indexes: позволяет отображать список файлов в каталоге, если нет файла по умолчанию. Это полезно, если вы хотите, чтобы пользователи могли видеть содержимое каталога.

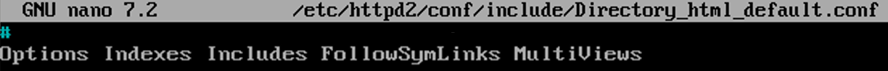


Рисунок 165 – Добавление Indexes

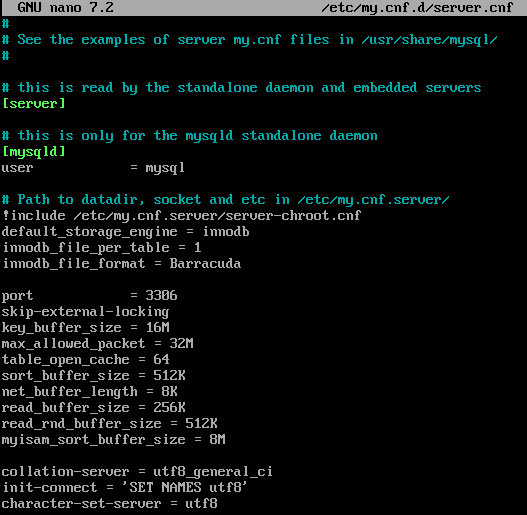


Рисунок 166 – Конфигурация MariaDB



Рисунок 167 – Перезагрузка mariadb

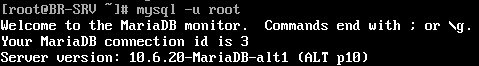


Рисунок 168 – Подключение к MySQL

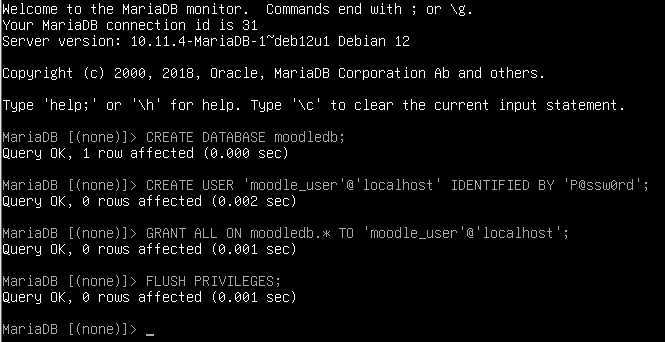


Рисунок 169 – Создание базы данных

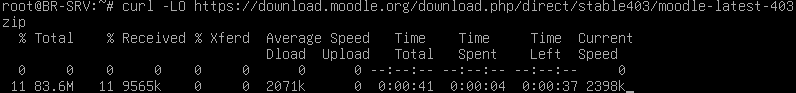


Рисунок 170 – Установка zip-пакета php8.1



Рисунок 171 – Распаковка

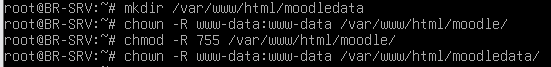


Рисунок 172 – Выдача прав

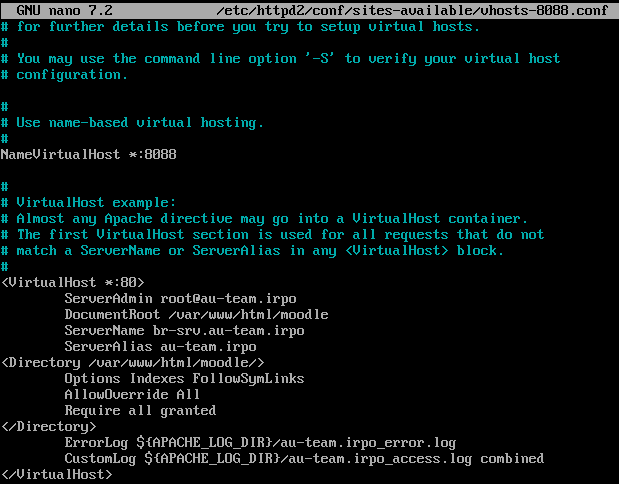


Рисунок 173 – Редактирование файла httpd2



Рисунок 174 – Перезагрузка файла httpd2

С клиентской машины необходимо произвести обращение к сайту LMS для дальнейшей настройки через браузер, как показано на рисунке 175.

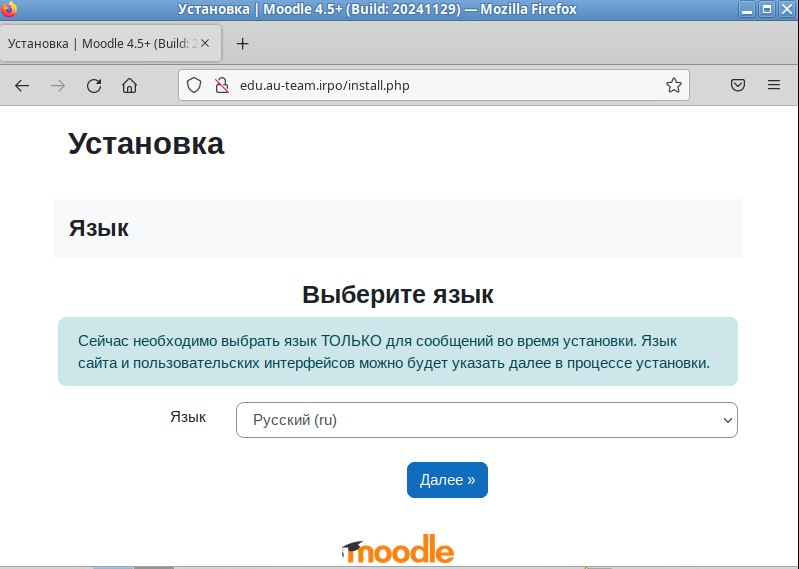


Рисунок 175 – Обращение к сайту

Необходимо произвести установку LMS через web интерфейс, как показано на рисунках 176-178.

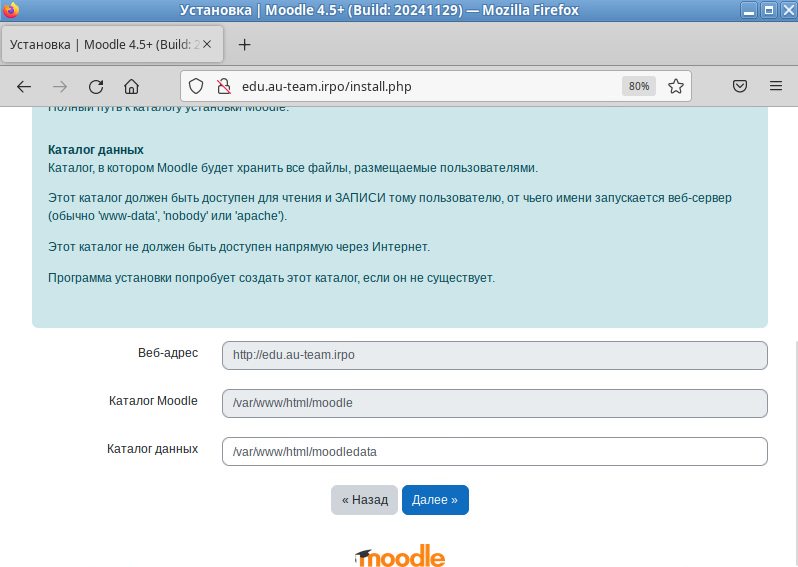


Рисунок 176 – Установка LMS через web интерфейс

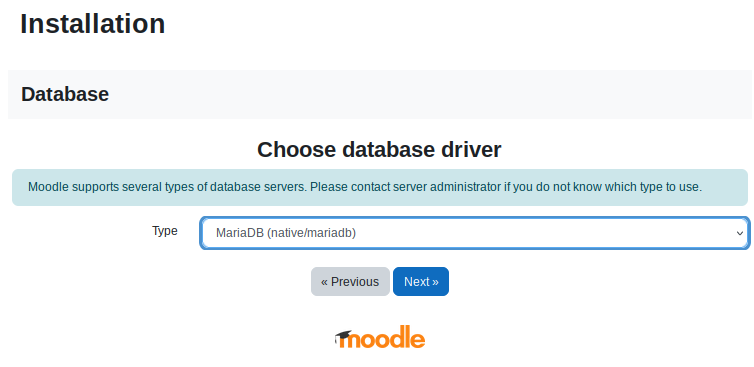


Рисунок 177 - Установка LMS через web интерфейс

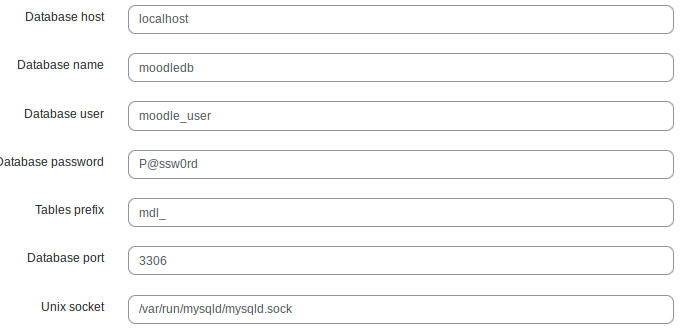


Рисунок 178 - Установка LMS через web интерфейс

Далее запускаем процесс установки и дожидаемся положительного результата, результат показан на рисунке 179.

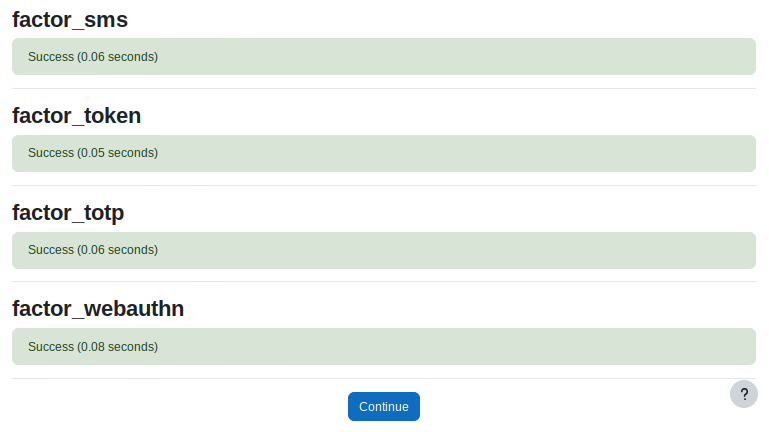


Рисунок 179 – Положительный результат

После создаём аккаунт администратора системы LMS, как показано на рисунке 180-182.

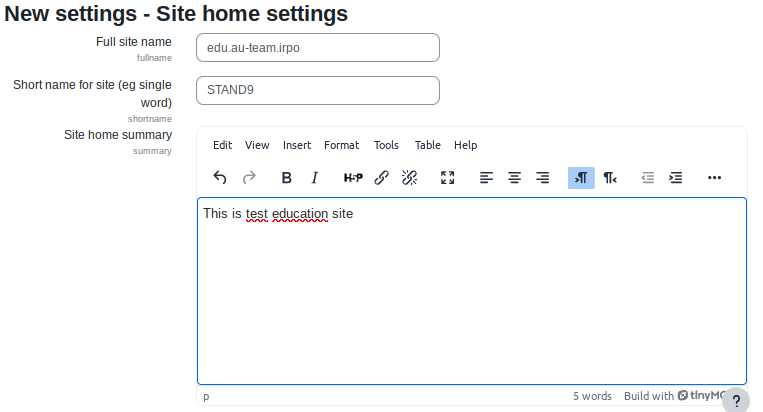


Рисунок 180– Создание аккаунта

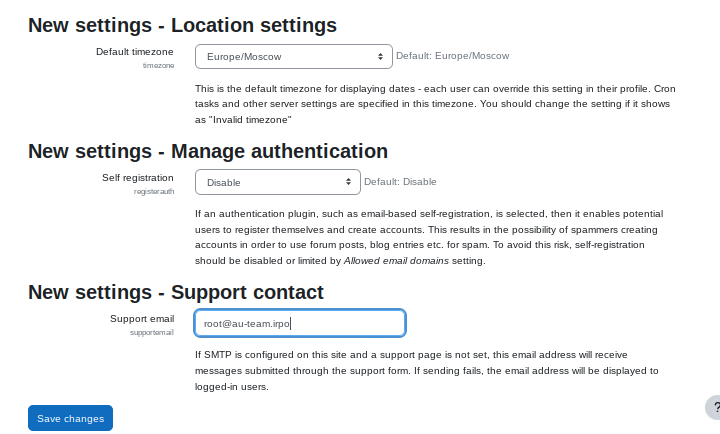


Рисунок 181 – Создание аккаунта

На этом процесс установки системы LMS считается завершённым, показано на рисунке 182.

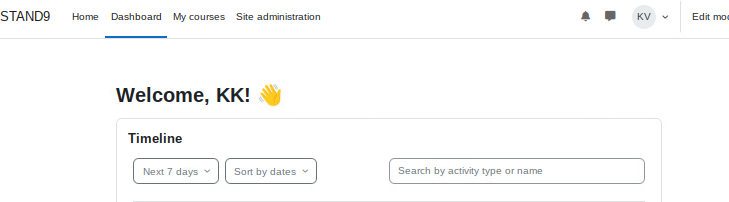


Рисунок 182 – Процесс установки завершен

2.7 Настройте веб-сервер nginx как обратный прокси-сервер на ISP

Nginx ― это программное обеспечение с открытым исходным кодом, которое позволяет создавать веб-сервер. Также его используют как почтовый сервер или обратный прокси-сервер. Установка показана на рисунке 183.

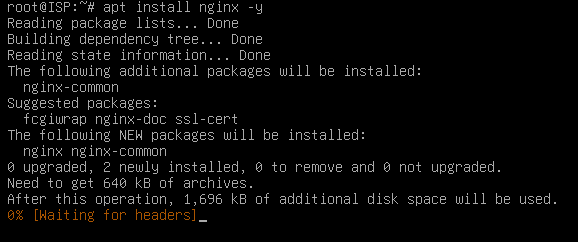


Рисунок 183 – Обратное проксикопирование

Необходимо перенаправить запросы к сайтам moodle и wiki, как показано на рисунке 184.

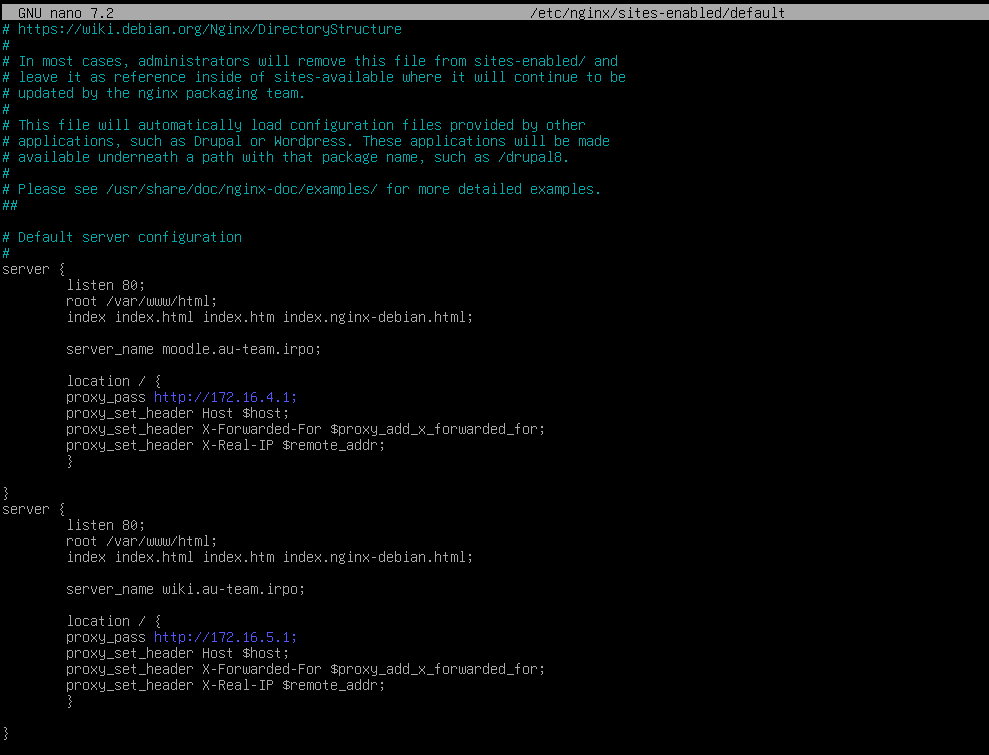


Рисунок 184 – Настройка nginx

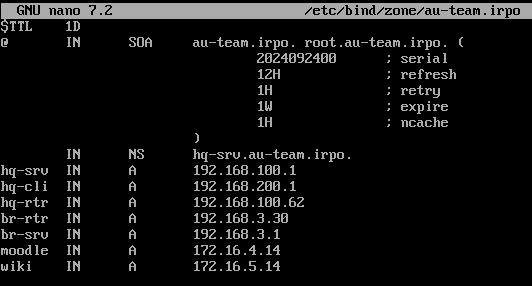


Рисунок 185 – Редактирование DNS

Далее пробрасываем порт на BR-RTR для сайта wiki, как показано на рисунке 186.



Рисунок 186 - Порт на BR-RTR

Далее необходимо проверить доступ к сайту по имени с HQ-CLI, как показано на рисунке 187.



Рисунок 187 – Доступ к сайту

Далее нас перенаправит прокси на 172.16.5.1:80, откуда произойдёт проброс на 192.168.3.1:8080. В результате откроется сайт wiki, как показано на рисунке 188.

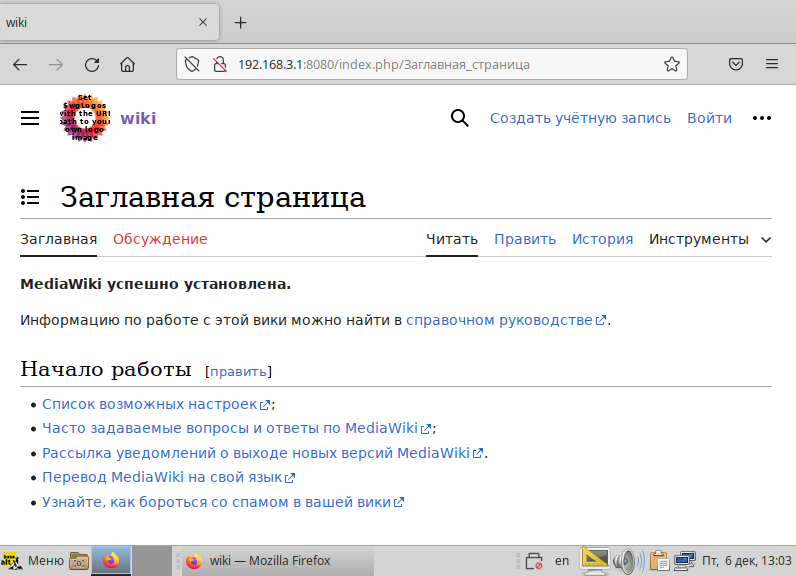


Рисунок 188 – Сайт wiki

Далее произведём установку браузера на HQ-CLI. Для этого изменяем файл инвентаря на BR-SRV, до настраиваем ssh на HQ-CLI и пишем playbook на BR-SRV, как показано на рисунках 189-195.

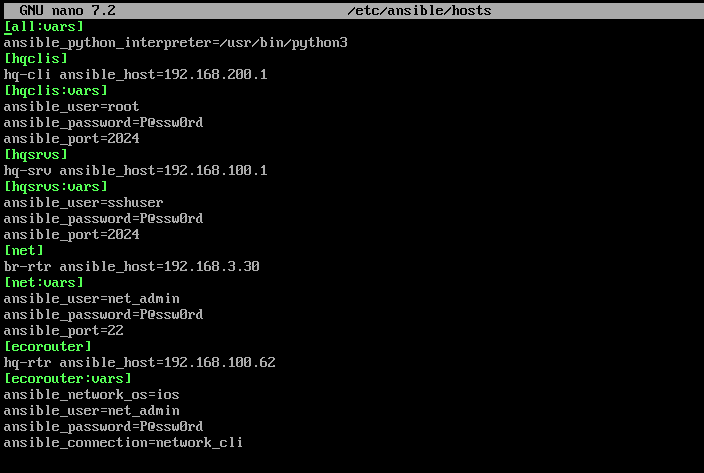


Рисунок 189 – Запись Host

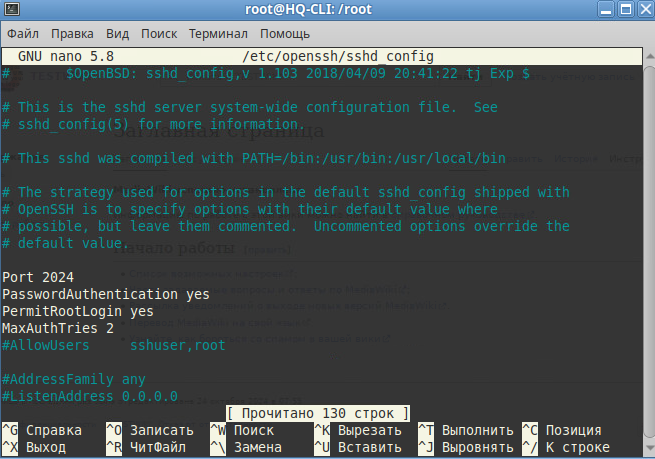


Рисунок 190 – Донастройка ssh на HQ-CLI

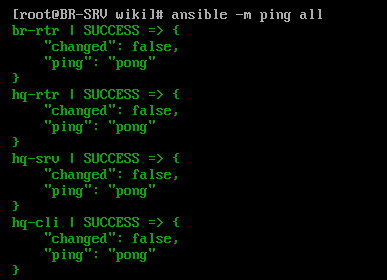


Рисунок 191 – Проверка доступности всех хостов



Рисунок 192 – playbook



Рисунок 193 – playbook

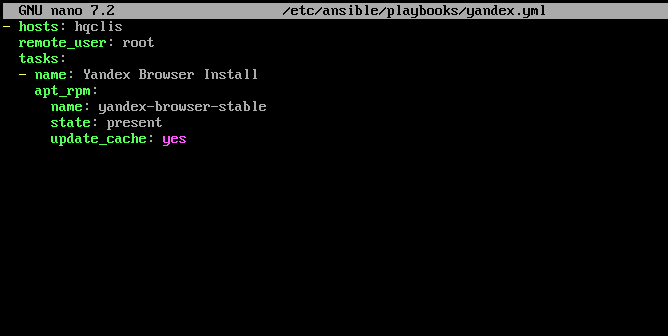


Рисунок 194 – playbook

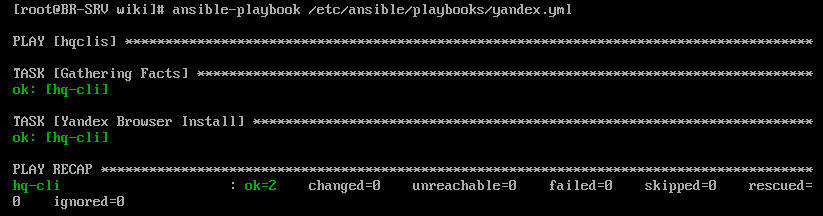


Рисунок 195 – playbook

Необходимо проверить на HQ-CLI, что браузер яндекс теперь присутствует, рисунок 196.

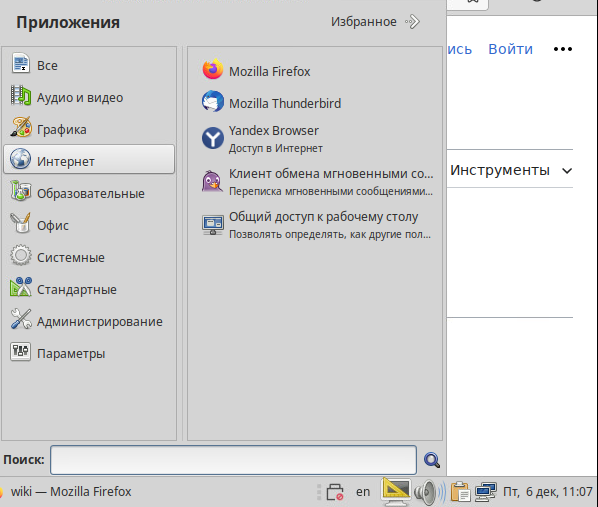


Рисунок 196 – Яндекс

Приложение Б. Пример заполнения таблицы адресов

Приложение В. Файл users.csv

Таблица 2 – DNS записи устройств

|  |  |  |
| --- | --- | --- |
| Устройство | Запись | Тип |
| HQ-RTR | hq-rtr.au-team.irpo | A,PTR |
| BR-RTR | br-rtr.au-team.irpo | A |
| HQ-SRV | hq-srv.au-team.irpo | A,PTR |
| HQ-CLI | hq-cli.au-team.irpo | A,PTR |
| BR-SRV | br-srv.au-team.irpo | A |
| HQ-RTR | moodle.au-team.irpo | CNAME |
| HQ-RTR | wiki.au-team.irpo | CNAME |

Таблица 3 – Таблица IP адресов.

|  |  |  |
| --- | --- | --- |
| Имя устройства | IP адрес | Шлюз по умолчанию |
| BR- SRV | Ens192 192.168.3.1/27 | 192.168.3.30 |
| HQ-RTR | Tunnel.0 10.255.255.1/30 |  |
| Ge0 172.16.4.1/28 |  |
| Vl100 192.168.100.62/26 |  |
| Vl200 192.168.200.14/28 |  |
| Vl999 192.168.9./26 |  |
| HQ-SRV | 192.168.100.1/26 | 192.168.100.62 |
| HQ-CLI | DHCP | 192.168.200.14 |
| BR-RTR | Ge1 10.255.255.2/30 |  |
| Ens192 172.16.5.1/28 |  |
| Ens224 192.168.3.30/27 |  |
| HQ-SW |  |  |
| ISP | ens192 192.168.194.129/24 | 192.168.254 |
| Ens224 172.16.5.14/28 |  |
| Ens256 172.16.4.14/28 |  |