ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ ИВАНОВСКОЙ ОБЛАСТИ
ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«КИНЕШЕМСКИЙ ТЕХНОЛОГИЧЕСКИЙ КОЛЛЕДЖ»

УТВЕРЖДАЮ
Директор ОГБПОУ КТК
_____/И.А. Смирнов/
«31» августа 2022г.

Фонд оценочных средств
по ПМ.02 Организация сетевого администрирования
по специальности среднего профессионального образования
программа подготовки специалистов среднего звена
технологического профиля
09.02.06 Сетевое и системное администрирование

Срок обучения 3 года 10 месяцев

Кинешма, 2022

Фонд оценочных средств по ПМ.02 Организация сетевого администрирования разработан в соответствии с Федеральным государственным образовательным стандартом среднего профессионального образования по специальности 09.02.06 Сетевое и системное администрирование.

Разработчик: Ветюгов Александр Викторович – преподаватель ОГБПОУ «Кинешемский технологический колледж»

Фонд оценочных средств по ПМ.02 Организация сетевого администрирования рассмотрен и одобрен на заседании методической комиссии учебно-методического объединения по укрупненным группам специальностей 09.00.00 Информатика и вычислительная техника, 13.00.00 Электро - и теплоэнергетика, 15.00.00 Машиностроение, 18.00.00 Химические технологии

Протокол № 1 от «31» августа 2022г.

Председатель _____ Киселева Е.В.

Паспорт
фонда оценочных средств по ПМ 02. Организация сетевого администрирования

1.2. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля студент должен освоить основной вид деятельности Организация сетевого администрирования и соответствующие ему общие компетенции и профессиональные компетенции:

1.2.1 Перечень общих компетенций

Код	Наименование общих компетенций
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 2	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 3	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 4	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 5	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 6	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК 7	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 8	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.
ОК 9	Использовать информационные технологии в профессиональной деятельности.
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языке.
ОК 11	Планировать предпринимательскую деятельность в профессиональной сфере

1.2.2 Перечень профессиональных компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ВД 2.	*Организация сетевого администрирования*
ПК 2.1	Администрировать локальные вычислительные сети и принимать меры по устранению возможных сбоев.
ПК 2.2	Администрировать сетевые ресурсы в информационных системах.
ПК 2.3	Обеспечивать сбор данных для анализа использования и функционирования программно-технических средств компьютерных сетей
ПК 2.4	Взаимодействовать со специалистами смежного профиля при разработке методов, средств и технологий применения объектов профессиональной деятельности.

Контролируемые разделы (темы) дисциплины*	Код формируемой компетенции	Результат освоения (умения и знания)		Оценочные средства
		уметь	знать	

Раздел 1. Администрирование сетевых операционных систем	ОК 01-11 ПК 2.1 - 2.4	администрировать локальные вычислительные сети; принимать меры по устранению возможных сбоев; обеспечивать защиту при подключении к информационно-телекоммуникационной сети "Интернет".	основные направления администрирования компьютерных сетей; утилиты, функции, удаленное управление сервером; технологию безопасности, протоколов авторизации, конфиденциальности и безопасности при работе с сетевыми ресурсами.	Вопросы для подготовки к дифференцированному зачету Реферат Тестирование
Раздел 2. Программное обеспечение компьютерных сетей	ОК 01-11 ПК 2.1 - 2.4	администрировать локальные вычислительные сети; принимать меры по устранению возможных сбоев; обеспечивать защиту при подключении к информационно-телекоммуникационной сети "Интернет".	основные направления администрирования компьютерных сетей; утилиты, функции, удаленное управление сервером; технологию безопасности, протоколов авторизации, конфиденциальности и безопасности при работе с сетевыми ресурсами.	Вопросы для подготовки к дифференцированному зачету Реферат Тестирование
Раздел 3. Организация администрирования компьютерных систем	ОК 01-11 ПК 2.1 - 2.4	администрировать локальные вычислительные сети; принимать меры по устранению возможных сбоев; обеспечивать защиту при подключении к информационно-телекоммуникационной сети "Интернет".	основные направления администрирования компьютерных сетей; утилиты, функции, удаленное управление сервером; технологию безопасности, протоколов авторизации, конфиденциальности и безопасности при работе с сетевыми ресурсами.	Вопросы для подготовки к дифференцированному зачету Реферат Тестирование

Приложение 1

ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ ИВАНОВСКОЙ ОБЛАСТИ

ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

«КИНЕШЕМСКИЙ ТЕХНОЛОГИЧЕСКИЙ КОЛЛЕДЖ»

ВОПРОСЫ К ЭКЗАМЕНУ

МДК 02.01 Администрирование сетевых операционных систем

специальность **09.02.06 Сетевое и системное администрирование**

Раздел 1. Администрирование сетевых операционных систем

Тема 1.1. Тема 1.1 Установка и настройка Windows Server 2012 R2

1. Развертывание и управление Windows Server 2012 R2.бзор Windows Server 2012 R2. Установк 2012 R2.
2. Настройка Windows Server 2012 R2 после установки. Обзор задач по управлению Windows Введение в Windows PowerShell.
3. **Управление объектами доменных служб Службы Каталога**
4. Управление учетными записями пользователей.

Тема 1.2Администрирование Windows Server 2012 R2

5. Настройка и устранение неполадок службы DNS. Настройка серверной роли DNS. Наст Настройка передачи зоны DNS. Управление службой DNS и устранение неполадок
6. Поддержка доменных служб Службы Каталога
7. Обзор AD DS. Использование виртуализированных контроллеров домена. Применение контроллеров домена с доступом только на чтение (RODC). Администрирование AD DS. Управление базой данных AD DS
8. Внедрение инфраструктуры Групповых политик
9. Обзор Групповой политики. Внедрение и администрирование Групповых политик. Область действия и порядок обработки Групповых политик
10. Управление пользовательским рабочим столом через Групповую политику
11. Применение Административных шаблонов. Настройка применения скриптов и перенаправления папок Установка, настройка и устранение неполадок роли Сервер Сетевой политики.
12. Установка и настройка роли Сервер Сетевой политики. Настройка клиентов и серверов RADIUS.
13. Настройка NAP. Настройка применения NAP через принудительные IPSec взаимодействия. Мониторинг и устранение неполадок NAP
14. Шифрование дисков с использованием BitLocker. Шифрование файлов с использованием EFS. Настройка расширенного аудита.
15. Шифрование дисков с использованием BitLocker. Шифрование файлов с использованием EFS. Настройка расширенного аудита.
16. Шифрование дисков с использованием BitLocker. Шифрование файлов с использованием EFS. Настройка расширенного аудита.
17. Управление пользовательскими и служебными учетными записями
18. Внедрение Web Application Proxy
19. . Применение защиты доступа к сети

Тема 1.3. Основы Linux.

20. Файловые системы ОС Linux
21. Создание и разметка жесткого диска
22. Настройка web-серверов в ОС Linux

23. Протокол HTTP. Веб-сервер Nginx.
24. Обратное проксирование в Nginx.
25. Настройка сервера DNS в ОС Linux
26. Протокол DNS
27. Настройка сервера DHCP в ОС Linux
28. Протокол DHCP
29. Настройка файловых серверов в ОС Linux
30. Протокол FTP. Файловая система NFS. Файловый сервер Samba.
31. Разворачивание домена на операционной системе ОС «Альт Сервер». Создание первого кон
32. Присоединение к домену в роли контроллера домена
33. Контроллер домена на чтение (RODC
34. Редактирование существующего домена
35. Настройка аутентификации доменных пользователей на контроллере домена
36. Инструменты управления объектами домена и групповыми политиками
37. Настройка серверов БД в ОС Linux СУБД MySQL. СУБД MongoDB
38. Контейнеры Docker
39. Контейнеры Docker.Способы связи контейнеров Docker.
40. Реализация системы. Составление документации

Приложение 2

ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ ИВАНОВСКОЙ ОБЛАСТИ

ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

«КИНЕШЕМСКИЙ ТЕХНОЛОГИЧЕСКИЙ КОЛЛЕДЖ»

БИЛЕТЫ К ЭКЗАМЕНУ
МДК 02.01 Администрирование сетевых операционных систем
специальность **09.02.06 Сетевое и системное администрирование**

Экзаменационный билет №1

1. Развертывание и управление Windows Server 2019
2. Настройка Windows Server 2019 после установки. Обзор задач по управлению Windows Server 2019.
3. Нстроить proxy squid на Debian.

Экзаменационный билет №2

1. Управление объектами доменных служб Службы Каталога
2. Управление учетными записями пользователей.
3. Определить находятся ли два узла A и B в одной подсети, если адреса компьютеров A и B 26.219.123.6 и 26.218.102.31. Маска подсети 255.255.192.0

Экзаменационный билет №3

1. Настройка и устранение неполадок службы DNS. Настройка серверной роли DNS. Настройка зон DNS. Настройка передачи зоны DNS. Управление службой DNS и устранение неполадок
2. Поддержка доменных служб Службы Каталога
3. Определить количество и диапазон ip адресов подсети, если номер подсети - 26.219.128.0, маска подсети – 255.255.192.0

Экзаменационный билет №4

1. Обзор AD DS. Использование виртуализированных контроллеров домена. Применение контроллеров домена с доступом только на чтение (RODC). Администрирование AD DS. Управление базой данных AD DS
2. Внедрение инфраструктуры Групповых политик
3. Разделить сеть класса C на четыре подсети с количеством узлов не менее пятидесяти. Определить маски и количество возможных адресов новых подсетей. Настроить сеть на базе Debian.

Экзаменационный билет №5

1. Обзор Групповой политики. Внедрение и администрирование Групповых политик. Область действия и порядок обработки Групповых политик
2. Управление пользовательским рабочим столом через Групповую политику
3. Настроить сеть в Vmware.

Экзаменационный билет №6

1. Применение Административных шаблонов. Настройка применения скриптов и перенаправления папок Установка, настройка и устранение неполадок роли Сервер Сетевой политики.

2. Установка и настройка роли Сервер Сетевой политики. Настройка клиентов и серверов RADIUS.
3. Настроить виртуальную машину с Windows Server 2019 в качестве маршрутизатора для сети 192.168.1.0.

Экзаменационный билет №7

1. Настройка NAP. Настройка применения NAP через принудительные IPSec взаимодействия. Мониторинг и устранение неполадок NAP
2. Шифрование дисков с использованием BitLocker. Шифрование файлов с использованием EFS. Настройка расширенного аудита.
3. *Создать Active Directory на виртуальной машине.

Экзаменационный билет №8

1. Файловые системы ОС Linux
2. Создание и разметка жесткого диска
3. Выполнить в командной строке команду IPconfig с ключом /all. Определить параметры сети.

Экзаменационный билет №9

1. Файловые системы ОС Linux
2. Создание и разметка жесткого диска
3. Выполнить в командной строке команду IPconfig с ключом /all. Определить параметры сети.

Экзаменационный билет №10

1. Шифрование дисков с использованием BitLocker. Шифрование файлов с использованием EFS. Настройка расширенного аудита.
2. Настройка web-серверов в ОС Linux
3. Изменить имя виртуальной машины и ввести ее в рабочую группу. Проверить имя с помощью утилиты hostname.

Экзаменационный билет №11

1. Шифрование дисков с использованием BitLocker. Шифрование файлов с использованием EFS. Настройка расширенного аудита.
2. Управление пользовательскими и служебными учетными записями
3. Отобразить информацию о текущих сетевых параметрах и активности сети.

Экзаменационный билет №12

1. Протокол HTTP. Веб-сервер Nginx.
2. Обратное проксирование в Nginx.
3. Создать учетную запись пользователя в Debian с правами администратора.

Экзаменационный билет №13

1. Внедрение Web Application Proxy
2. Применение защиты доступа к сети
3. *Создать домен DC1 (Windows Server 2019) Включить рабочую станцию CLI1в домен.

Экзаменационный билет №14

1. Настройка сервера DNS в ОС Linux
2. Протокол DNS
3. Установить DNS сервер в Windows Server 2019.

Экзаменационный билет №15

1. Настройка сервера DHCP в ОС Linux
2. Протокол DHCP
3. Установить DNS сервер в Windows Server 2019.

Экзаменационный билет №16

1. Настройка файловых серверов в ОС Linux

2. Протокол FTP. Файловая система NFS. Файловый сервер Samba.
3. Присвоить шлюз по умолчанию 192.168.0.10 серверу в Debian.

Экзаменационный билет №17

1. Разворачивание домена на операционной системе ОС «Альт Сервер». Создание первого контроллера домена
2. Присоединение к домену в роли контроллера домена
3. Установить DHCP сервер в Debian. Подключить рабочую станцию HQ.

Экзаменационный билет №18

1. Контроллер домена на чтение (RODC)
2. Редактирование существующего домена
3. Установить DHCP сервер в Windows Server 2019. Подключить рабочую станцию HQ.

Экзаменационный билет №19

1. ACL-список. Виды списков и их задачи.
2. Технология Port security. Функции и назначение.
3. Создать доменную учетную запись пользователя, имеющего доступ ко всем компьютерам в сети в любое время.

Экзаменационный билет №20

1 *Технология NAT.
2. Настройка аутентификации доменных пользователей на контроллере домена
3. Определить количество и диапазон ip адресов подсети, если номер подсети - 26.219.128.168, маска подсети – 255.255.255.128

Экзаменационный билет №21

1. Утилиты диагностики TCP/IP. Утилита Ping. Ключи утилиты.
2. Утилиты диагностики TCP/IP. Утилита Tracert. Ключи утилиты.
3. Разбить на 10 подсетей блок адресов 192.168.1.0/25. Указать первый и последний IP-адрес в 10 подсети.

Экзаменационный билет №22

1. Основные понятия и виды виртуальных частных сетей.
2. Инструменты управления объектами домена и групповыми политиками
3. Создать поддомен в доменном пространстве Exam.

Экзаменационный билет №23

1. Внедрение Web Application Proxy
2. Применение защиты доступа к сети
3. *Создать домен DC1 (Windows Server 2019) Включить рабочую станцию CLI1в домен.

Экзаменационный билет №24

1. Настройка сервера DNS в ОС Linux
2. Протокол DNS
3. Установить DNS сервер в Windows Server 2019.

Экзаменационный билет №25

1. Настройка сервера DHCP в ОС Linux
2. Протокол DHCP
3. Установить DNS сервер в Windows Server 2019.

Экзаменационный билет №26

1. Настройка файловых серверов в ОС Linux
2. Протокол FTP. Файловая система NFS. Файловый сервер Samba.
3. Присвоить шлюз по умолчанию 192.168.0.10 серверу в Debian.

Экзаменационный билет №27

1. Разворачивание домена на операционной системе ОС «Альт Сервер». Создание первого контроллера домена

2. Присоединение к домену в роли контроллера домена
3. Установить DHCP сервер в Debian. Подключить рабочую станцию HQ.

Приложение 3

ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ ИВАНОВСКОЙ ОБЛАСТИ

ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

«КИНЕШЕМСКИЙ ТЕХНОЛОГИЧЕСКИЙ КОЛЛЕДЖ»

ВОПРОСЫ К ЭКЗАМЕНУ
МДК 02.01 Программное обеспечение компьютерных сетей
специальность **09.02.06 Сетевое и системное администрирование**

Раздел 2. Программное обеспечение компьютерных сетей
Тема 2.1. Реализация клиентской инфраструктуры

1. Оценка и определение параметров развертывания клиентских ОС.
2. Обзор жизненного цикла клиентских компьютеров предприятия. Оценка оборудования и готовности инфраструктуры к развертыванию клиентских ОС.
3. Обзор методов развертывания клиентских ОС в среде организации. Технологии лицензионной активации для клиентских компьютеров в организации.
4. Планирование стратегии развертывания клиентских ОС. Сбор данных об инфраструктуре. Реализация решения лицензионной активации
5. Планирование стратегии управления образами. Обзор форматов образа Windows.
6. Обзор средств управления образами (Image Management).
7. Оценка бизнес-требований для поддержки стратегии управления образами.
8. Реализация безопасности клиентских систем. Реализация централизованного решения по безопасности клиентских ОС. Планирование и реализация BitLocker.
9. Планирование и реализация шифрования с помощью EFS. Настройка безопасности клиентских ОС с помощью групповой политики. Настройка шифрования диска с помощью BitLocker.
10. Реализация решения централизованного управления EFS. Реализация решения для восстановления файлов, защищенных EFS.
11. Захват и управление образами клиентских ОС. Обзор Windows ADK. Управление средой предустановки Windows (Windows PE). Создание исходного образа с помощью Windows SIM и Sysprep. Захват и обслуживанию эталонного образа.
12. Настройка и управление службой развертывания Windows (Windows Deployment Services). Настройка Windows PE. Установка эталонного компьютера с помощью файла ответов. Обработка эталонного компьютера с помощью Sysprep.
13. Создание файла ответов с помощью Windows SIM. Установка эталонного компьютера с помощью файла ответов. Обработка эталонного компьютера с помощью Sysprep. Services
14. Планирование среды Windows Deployment Services. Установка и настройка серверной роли WDS. Захват эталонного образа с помощью WDS. Развертывание образа с помощью WDS

15. Планирование и реализация миграции пользовательской среды
16. Обзор способов миграции пользовательской среды. Планирование миграции пользовательской среды с помощью USMT.
17. Миграция состояния пользователя с помощью USMT. Планирование миграции пользовательской среды. Создание и настройка XML-файлов USMT.
18. Сбор данных и восстановления профиля пользователя с помощью USMT. Выполнение миграции с созданием жестких ссылок

19. Планирование и развертывание клиентских ОС с помощью Microsoft Deployment Toolkit
20. Планирование среды Lite Touch Installation.
21. Реализация MDT 2012 для Lite Touch Installation. Интеграция служб развертывания Windows с MDT. Планирование среды Lite Touch Installation.
22. Установка MDT 2012 и необходимых компонентов. Создание и настройка MDT 2012 Deployment Share. Развертывание и захват образа эталонной ОС.
23. Интеграция WDS с MDT 2012 для обеспечения возможностей загрузки PXE.

24. Планирование и развертывание клиентских ОС с помощью System Center Configuration Manager 2012
25. Планирование среды Zero Touch Installation. Подготовка сайта для развертывания ОС. Построение эталонного образа на основе последовательности задач Configuration Manager.
26. Использование последовательности задач MDT для развертывания клиентских образов. Планирование инфраструктуры развертывания операционной системы.
27. Подготовка среды Zero Touch Installation. Настройка пакетов развертывания и образов системы. Подготовка среды ZeroTouchInstallation

28. Планирование и реализация служб удаленного доступа (Remote Desktop Services)
29. Обзор службы удаленного рабочего стола. Планирование среды Remote Desktop Services.
30. Настройка развертывания инфраструктуры виртуальных рабочих столов. Настройка доступа к клиентам на основе сеансов (Session-Based Desktop).
31. Расширение среды Remote Desktop Services в Интернет. Планирование среды Remote Desktop Services. Настройка сценария инфраструктуры виртуальных рабочих столов.
32. Настройка сценария доступа на основе сеансов. Проектирование политик шлюзов RDS. Настройка шлюзов RDS
33. Управление виртуализацией пользовательского состояния для клиентских ОС организации**.** Обзор виртуализации профиля пользователя. Планирование виртуализации профиля пользователя.
34. Настройка перемещаемых профилей, перенаправления папок и автономных (offline) файлов. Реализация виртуализации работы пользователя от Microsoft (Microsoft User Experience Virtualization).
35. Планирование виртуализации профиля пользователя. Реализация виртуализации профиля пользователя.
36. Планирование и реализация инфраструктуры обновлений для поддержки клиентских ОС организаци
37. Реализация поддержки обновлений программного обеспечения с помощью Configuration Manager 2012. Управление обновлениями для виртуальных машин и образов.
38. Использование Windows Intune для управления обновление программного обеспечения. Планирование инфраструктуры обновления.
39. Реализация обновлений программного обеспечения с помощью Configuration Manager 2012.
40. Реализация обновлений программного обеспечения для библиотек виртуальных машин.
41. Защита компьютеров предприятия от вредоносных программ и потерь данных
42. Обзор System Center 2012 Endpoint Protection. Настройка Endpoint Protection Client Settings и мониторинга состояния. Использование Windows Intune Endpoint Protection.
43. Защита клиентских ОС с помощью System Center 2012 Data Protection Manager. Настройка и развертывание политик EndpointProtection.
44. Настройка параметров клиента для поддержки Endpoint Protection. Мониторинг защиты конечных точек. Настройка и проверка защиты данных клиента
45. Мониторинг производительности и работоспособности инфраструктуры клиентских ОС
46. Производительность и работоспособность инфраструктуры клиентских ОС.
47. Мониторинг инфраструктуры виртуальных клиентов. Настройка Operations Manager для мониторинга виртуальных сред.
48. Планирование инфраструктуры обновлений для организации
49. Защита компьютеров предприятия от вредоносных программ и потерь данных
50. Обзор System Center 2012 Endpoint Protection.

Тема 2.2. Реализация среды настольных приложений.

51. Разработка стратегии развертывания приложений
52. Определение бизнес-требований для развертывания приложений. Обзор стратегии развертывания приложений. Выбор подходящей стратегии развертывания приложений для офиса.
53. Диагностика и обеспечение совместимости приложений. Диагностика проблем совместимости приложений. Оценка и реализация решений по восстановлению. Решение проблемы совместимости с помощью Application Compatibility Toolkit.
54. Установка и настройка ACT. Анализ потенциальных проблем совместимости
55. Решение проблем совместимости приложений. Автоматизация развертывания программных средств обеспечения совместимости (shims)
56. Развертывание приложений с помощью групповых политик. Развертывание приложений с помощью Windows Intune.
57. Развертывание приложений с помощью групповых политик. Запуск симуляции Windows Intune.
58. Развертывание приложений с помощью System Center Configuration Manager/ Концепции развертывания приложений с помощью Configuration Manager 2012. Развертывание приложений с помощью Configuration Manager 2012.
59. Создание запросов Configuration Manager 2012. Создание коллекций пользователей и устройств Configuration Manager 2012.
60. Развертывания самообслуживаемых приложений. Концепции развертывания самообслуживаемых приложений.
61. Настройка самообслуживаемых приложений с Windows Intune. Развертывания самообслуживаемых приложений с Configuration Manager 2012. Развертывания самообслуживаемых приложений с Service Manager 2012.
62. Подготовка System Center Configuration Manager 2012 для поддержки Service Manager 2012 Self-Service Portal. Настройка ServiceManager 2012 Self-ServicePortal. Проверка возможности предоставления приложений пользователям с помощью Self-Service Portal.
63. Проектирование и реализация инфраструктуры виртуализации представлений. Оценка требований виртуализации представлений.
64. Планирование инфраструктуры виртуализации представлений. Развертывание инфраструктуры виртуализации представлений. Развертывание инфраструктуры высокой готовности для виртуализации представлений
65. Подготовка, настройка и развертывание представлений виртуализации приложений
66. Определение стратегии представлений виртуализации приложений. Развертывание удален ного рабочего стола, RemoteApp, и RD Web Access.
67. Развертывание приложений на RD Session Host. Настройка и развертывание приложений RemoteApp. Проверка возможности использования приложений с помощью RD Web Access.

68. Проектирование и развертывание среды виртуализации приложений
69. Обзор моделей виртуализации приложений. Развертывание компонентов инфраструктуры виртуализации приложений.
70. Настройка клиентской поддержки виртуализации приложений. Планирование развертывания App-V ролей и компонентов. Развертывание инфраструктуры App-V. Настройка клиента App-V
71. Подготовка к виртуализации и развертывание виртуальных приложений
72. Подготовка приложений для выполнения в среде App-V. Развертывание приложений App-V.
73. Установка и настройка App-V Sequencer. Подготовка приложений к виртуализации. Развертывание App-V приложений с помощью Configuration Manager.
74. Планирование и реализация безопасности и обновления приложений. Планирование обновления приложений. Развертывание обновлений с помощью WSUS. Развертывание обновлений с помощью Configuration Manager 2012.
75. Реализация безопасности приложений. Обновление развернутых приложений. Обновление приложений App-V. Развертывание политик AppLocker для управления запуском приложений.
76. Планирование и реализация обновления и замены приложений. Планирование и реализация обновления приложений и замещения приложений. Планирование и реализация сосуществования приложений.

Преподаватель А.В. Ветюгов

Приложение 4

ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ ИВАНОВСКОЙ ОБЛАСТИ

ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

«КИНЕШЕМСКИЙ ТЕХНОЛОГИЧЕСКИЙ КОЛЛЕДЖ»

БИЛЕТЫ К ЭКЗАМЕНУ
МДК 02.01 Программное обеспечение компьютерных сетей
специальность **09.02.06 Сетевое и системное администрирование**

Экзаменационный билет №1

1 Оценка и определение параметров развертывания клиентских ОС
2 Обзор жизненного цикла клиентских компьютеров предприятия. Оценка оборудования и готовности инфраструктуры к развертыванию клиентских ОС.
3 Задание

Экзаменационный билет №2

1 Обзор методов развертывания клиентских ОС в среде организации. Технологии лицензионной активации для клиентских компьютеров в организации.
2 Планирование стратегии развертывания клиентских ОС. Сбор данных об инфраструктуре. Реализация решения лицензионной активации
3 Задание

Экзаменационный билет №3

1 Планирование стратегии управления образами. Обзор форматов образа Windows.
2 Планирование и реализация инфраструктуры обновлений для поддержки клиентских ОС организации.
3 Задание

Экзаменационный билет №4

1 Развертывание приложений с помощью групповых политик. Развертывание приложений с помощью Windows Intune.
2 Развертывания самообслуживаемых приложений. Концепции развертывания самообслуживаемых приложений.
3 Задание

Экзаменационный билет №5

1 Установка и настройка App-V Sequencer. Подготовка приложений к виртуализации. Развертывание App-V приложений с помощью Configuration Manager.

2 Планирование и реализация обновления и замены приложений. Планирование и реализация обновления приложений и замещения приложений. Планирование и реализация сосуществования приложений.

3 Задание

Экзаменационный билет №6

1 Реализация безопасности приложений. Обновление развернутых приложений. Обновление приложений App-V. Развертывание политик AppLocker для управления запуском приложений.

2 Диагностика и обеспечение совместимости приложений. Диагностика проблем совместимости приложений. Оценка и реализация решений по восстановлению. Решение проблемы совместимости с помощью Application Compatibility Toolkit.

3 Задание

Экзаменационный билет №7

1 Защита компьютеров предприятия от вредоносных программ и потерь данных

2 Настройка самообслуживаемых приложений с Windows Intune. Развертывания самообслуживаемых приложений с Configuration Manager 2012. Развертывания самообслуживаемых приложений с Service Manager 2012.

3 Задание

Экзаменационный билет №8

1 Настройка параметров клиента для поддержки Endpoint Protection. Мониторинг защиты конечных точек. Настройка и проверка защиты данных клиента

2 Мониторинг инфраструктуры виртуальных клиентов. Настройка Operations Manager для мониторинга виртуальных сред.

3 Задание.

Экзаменационный билет №9

1 Производительность и работоспособность инфраструктуры клиентских ОС.

2 Планирование инфраструктуры виртуализации представлений. Развертывание инфраструктуры виртуализации представлений. Развертывание инфраструктуры высокой готовности для виртуализации представлений

3 Задание.

Экзаменационный билет №10

1 Создание запросов Configuration Manager 2012. Создание коллекций пользователей и устройств Configuration Manager 2012.

2 Развертывание приложений с помощью групповых политик. Запуск симуляции Windows Intune.

3 Задание.

Экзаменационный билет №11

1 Развертывание приложений с помощью System Center Configuration Manager/ Концепции развертывания приложений с помощью Configuration Manager 2012. Развертывание приложений с помощью Configuration Manager 2012.

2 Решение проблем совместимости приложений. Автоматизация развертывания программных средств обеспечения совместимости (shims)

3 Задание.

Экзаменационный билет №12

1 Создание запросов Configuration Manager 2012. Создание коллекций пользователей и устройств Configuration Manager 2012.

2 Развертывание приложений с помощью групповых политик. Запуск симуляции Windows Intune.

3 Задание.

Экзаменационный билет №13

1 Разработка стратегии развертывания приложений

2 Подготовка System Center Configuration Manager 2012 для поддержки Service Manager 2012 Self-Service Portal. Настройка ServiceManager 2012 Self-ServicePortal. Проверка возможности предоставления приложений пользователям с помощью Self-Service Portal.

3 Задание.

Экзаменационный билет №14

1 Проектирование и реализация инфраструктуры виртуализации представлений. Оценка требований виртуализации представлений.

2 Проектирование и развертывание среды виртуализации приложений

3 Задание.

Экзаменационный билет №15

1 Планирование и реализация безопасности и обновления приложений. Планирование обновления приложений. Развертывание обновлений с помощью WSUS. Развертывание обновлений с помощью Configuration Manager 2012.

2 Обзор моделей виртуализации приложений. Развертывание компонентов инфраструктуры виртуализации приложений.

3 Задание.

Экзаменационный билет №16

1 Мониторинг производительности и работоспособности инфраструктуры клиентских ОС

2 Определение бизнес-требований для развертывания приложений. Обзор стратегии развертывания приложений. Выбор подходящей стратегии развертывания приложений для офиса.

3 Задание.

Экзаменационный билет №17

1 Реализация поддержки обновлений программного обеспечения с помощью Configuration Manager 2012. Управление обновлениями для виртуальных машин и образов.

2 Настройка перемещаемых профилей, перенаправления папок и автономных (offline) файлов. Реализация виртуализации работы пользователя от Microsoft (Microsoft User Experience Virtualization).

3 Задание.

Экзаменационный билет №18

1 Использование Windows Intune для управления обновление программного обеспечения. Планирование инфраструктуры обновления.

2 Управление виртуализацией пользовательского состояния для клиентских ОС организации**.** Обзор виртуализации профиля пользователя. Планирование виртуализации профиля пользователя.

3 Задание.

Экзаменационный билет №19

1 Планирование и реализация служб удаленного доступа (Remote Desktop Services)

2 Подготовка среды Zero Touch Installation. Настройка пакетов развертывания и образов системы. Подготовка среды ZeroTouchInstallation

3 Задание.

Экзаменационный билет №20

1 Захват и управление образами клиентских ОС. Обзор Windows ADK. Управление средой предустановки Windows (Windows PE). Создание исходного образа с помощью Windows SIM и Sysprep. Захват и обслуживанию эталонного образа.

2 Настройка и управление службой развертывания Windows (Windows Deployment Services). Настройка Windows PE. Установка эталонного компьютера с помощью файла ответов. Обработка эталонного компьютера с помощью Sysprep.

3 Задание.

\

Экзаменационный билет №21

1 Реализация безопасности клиентских систем. Реализация централизованного решения по безопасности клиентских ОС. Планирование и реализация BitLocker.

2 Обзор средств управления образами (Image Management).

3 Задание.

Экзаменационный билет №22

1 Планирование среды Windows Deployment Services. Установка и настройка серверной роли WDS. Захват эталонного образа с помощью WDS. Развертывание образа с помощью WDS

2 Оценка бизнес-требований для поддержки стратегии управления образами.

3 Задание.

Экзаменационный билет №23

1 Реализация решения централизованного управления EFS. Реализация решения для восстановления файлов, защищенных EFS.

2 Планирование и реализация шифрования с помощью EFS. Настройка безопасности клиентских ОС с помощью групповой политики. Настройка шифрования диска с помощью BitLocker.

3 Задание.

Приложение 4

ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ ИВАНОВСКОЙ ОБЛАСТИ

ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

«КИНЕШЕМСКИЙ ТЕХНОЛОГИЧЕСКИЙ КОЛЛЕДЖ»

ПРАКТИЧЕКИЕ РАБОТЫ

Междисциплинарный курс 02.01 Администрирование компьютерных сетей

Междисциплинарный курс 02.02 Программное обеспечение компьютерных сетей

специальность **09.02.06 Сетевое и системное администрирование**

Содержание

Введение

Задачи сетевого администрирования состоят в обеспечении надежной, бесперебойной и безопасной работы корпоративной сети. Слово «корпорация» означает объединение предприятий, работающих под централизованным управлением и решающих общие задачи. Корпорация является сложной, многопрофильной структурой и вследствие этого имеет распределенную иерархическую систему управления. Для централизованного управления таким объединением предприятий используется корпоративная сеть.

Основная задача корпоративной сети заключается в обеспечении передачи информации между различными приложениями, используемыми в организации. Под приложением понимается программное обеспечение, которое непосредственно нужно пользователю.

Будем рассматривать корпоративную сеть как совокупность программных, аппаратных и коммуникационных средств, обеспечивающих эффективное распределение вычислительных ресурсов. Все сети можно условно разделить на 3 категории: локальные сети (LAN, Local Area Network), глобальные сети (WAN, Wide Area Network), городские сети (MAN, Metropolitan Area Network).

Обязательным компонентом корпоративной сети являются локальные сети, связанные между собой. Основное назначение LAN состоит в объединении пользователей (как правило, одной организации) для совместной работы. LAN обеспечивают наивысшую скорость обмена информацией между компьютерами.

Инфраструктура сети - это набор физических и логических компонентов, которые обеспечивают связь, безопасность, маршрутизацию, управление, доступ и другие обязательные свойства сети.

Сетевая инфраструктура строится из различных компонентов, которые условно можно разнести по следующим уровням:

1. кабельная система и средства коммуникаций;
2. активное сетевое оборудование;

3. сетевые протоколы;
4. сетевые службы;
5. сетевые приложения.

Каждый из этих уровней может состоять из различных подуровней и компонент. Например, кабельные системы могут быть построены на основе коаксиального кабеля («толстого» или «тонкого»), витой пары (экранированной и неэкранированной), оптоволокна. Активное сетевое оборудование включает в себя такие виды устройств, как повторители (репитеры), мосты, концентраторы, коммутаторы, маршрутизаторы.

В корпоративной сети может быть использован богатый набор сетевых протоколов: TCP/IP, SPX/IPX, NetBEUI, AppleTalk и др.

Основу работы сети составляют сетевые службы (сервисы). Базовый набор сетевых служб любой корпоративной сети состоит из следующих служб:

- службы сетевой инфраструктуры DNS, DHCP, WINS;
- службы файлов и печати;
- службы каталогов (например, Novell NDS, MS Active Directory);
- службы обмена сообщениями;
- службы доступа к базам данных.

Самый верхний уровень функционирования сети — сетевые приложения.

Сопровождение, администрирование и управление логической инфраструктурой существующей сети требует глубокого знания многих сетевых технологий. Администратор сети даже в небольшой организации должен уметь создавать различные типы сетевых подключений, устанавливать и конфигурировать необходимые сетевые протоколы, знать методы ручной и автоматической адресации и методы разрешения имен и, наконец, устранять неполадки связи, адресации, доступа, безопасности и разрешения имен.

В средних и крупных сетях у администраторов более сложные задачи:

- настройка виртуальных частных сетей (VPN);

- создание, настройка и устранение неполадок интерфейсов и таблиц маршрутизации;

- создание и поддержка подсистемы безопасности на основе открытых ключей;

- обслуживание смешанных сетей с разными ОС, в том числе Microsoft Windows и UNIX.

Сеть позволяет легко взаимодействовать друг с другом самым различным видам компьютерных систем благодаря стандартизованным методам передачи данных, которые позволяют скрыть от пользователя все многообразие сетей и машин.

Для описания работы сети разработаны специальные модели. В настоящее время общепринятыми моделями являются модель OSI (Open System Interconnection) и модель TCP/IP.

Задачи сетевого администрирования:

Планирование сети - добавление или удаление рабочих станций, добавление или удаление сетевых протоколов, добавление или удаление сетевых служб, установка серверов, разбиение сети на сегменты, чтобы новые устройства, узлы или протоколы включались в сеть или исключались из нее без нарушения целостности сети, без снижения производительности, без нарушения инфраструктуры сетевых протоколов, служб и приложений.

Установка и настройка сетевых узлов (устройств активного сетевого оборудования, персональных компьютеров, серверов, средств коммуникаций) - замену сетевого адаптера в ПК с соответствующими настройками компьютера, перенос сетевого узла (ПК, сервера, активного оборудования) в другую подсеть с соответствующим изменениями сетевых параметров узла, добавление или замена сетевого принтера с соответствующей настройкой рабочих мест.

Установка и настройка сетевых протоколов - планирование и настройка базовых сетевых протоколов корпоративной сети, тестирование работы сетевых протоколов, определение оптимальных конфигураций протоколов.

Установка и настройка сетевых служб:

- установка и настройка служб сетевой инфраструктуры (службы DNS, DHCP, WINS, службы маршрутизации, удаленного доступа и виртуальных частных сетей); установка и настройка служб файлов и печати, которые в настоящее время составляют значительную часть всех сетевых служб;

- администрирование служб каталогов (Novell NDS, Microsoft Active Directory), составляющих основу корпоративной системы безопасности и управления доступом к сетевым ресурсам;

- администрирование служб обмена сообщениями (системы электронной почты);

- администрирование служб доступа к базам данных.

Поиск неисправностей. От неисправного сетевого адаптера на рабочей станции пользователя до сбоев отдельных портов коммутаторов и маршрутизаторов, а также неправильные настройки сетевых протоколов и служб.

Поиск узких мест сети и повышения эффективности работы сети - анализ работы сети и определение наиболее узких мест, требующих либо замены сетевого оборудования, либо модернизации рабочих мест, либо изменения конфигурации отдельных сегментов сети.

Мониторинг сетевых узлов - наблюдение за функционированием сетевых узлов и корректностью выполнения возложенных на данные узлы функций.

Мониторинг сетевого трафика позволяет обнаружить и ликвидировать: высокую загруженность отдельных сетевых сегментов, чрезмерную загруженность отдельных сетевых устройств, сбои в работе сетевых адаптеров или портов сетевых устройств, нежелательную активность или атаки злоумышленников (распространение вирусов, атаки хакеров и др.) Обеспечение защиты данных:

- резервное копирование и восстановление данных;

- разработка и осуществление политик безопасности учетных записей

пользователей и сетевых служб (требования к сложности паролей, частота смены паролей);

- построение защищенных коммуникаций (применение протокола IPSec, построение виртуальных частных сетей, защита беспроводных сетей);
- планирование, внедрение и обслуживание инфраструктуры открытых ключей (PKI).

Моделирование сети

Моделирование сети является обязательной частью любого проекта (модернизации) корпоративной сети.

Целями моделирования могут являться:

- определение оптимальной топологии;
- выбор сетевого оборудования;
- определение рабочих характеристик сети;
- проверка характеристик новых протоколов.

На модели можно проверить влияние всплесков загрузки, воздействие большого потока широковещательных запросов, что вряд ли кто-то может себе позволить в работающей сети.

Перечисленные задачи предъявляют различные требования к программам, моделирующим функционирование сети. При этом определение характеристик сети до того, как она будет введена в эксплуатацию, имеет первостепенное значение, та как позволяет отрегулировать характеристики локальной сети на стадии проектирования (модернизации). Решение этой проблемы возможно путем аналитического или статистического моделирования.

Аналитическое моделирование сети представляет собой совокупность математических соотношений, связывающих между собой входные и выходные характеристики сети. При выводе таких соотношений приходится пренебрегать малосущественными деталями или обстоятельствами.

Симуляционное (статистическое) моделирование служит для анализа системы с целью выявления критических элементов сети. Этот тип моделирования используется также для предсказания будущих характеристик системы. Процесс моделирования включат в себя формирование модели, отладку моделирующей программы и проверку корректности выбранной модели. Последний этап обычно состоит из сравнения расчетных результатов с экспериментальными данными, полученными для реальной сети.

Возможны разные подходы к моделированию. Классический подход заключается в воспроизведении событий в сети как можно точнее и поэтапном моделировании последствий этих событий.

Другим подходом может стать метод, где для каждого логического сегмента (зоны столкновений) сначала моделируется очередь событий.

Полное моделирование сети с учетом рабочих приложений предполагает использование следующих характеристик:

- характеристики узла;
- характеристики соединений;
- используемые протоколы;
- характеристики отправляемых пакетов.

Характеристики протоколов:

- длина пакета, посылаемого каждым узлом (длина сообщения + длина адресной части + длина дополнительной присоединяемой информации);
- длина сообщения;
- временное распределение моментов посылки пакетов.

Структура описания каждого из узлов включает в себя:

- номер узла (идентификатор);
- код типа узла;
- MAC-адрес; IP-адрес;
- байт статуса (узел ведет передачу; до узла дошел чужой пакет);
- код используемого протокола (IPv4 или IPv6; TCP, UDP, ICMP и т.д.);
- объем входного/выходного буфера. Тип буфера (FIFO, LIFO и

т.д.).

В каждом из существующих способов моделирования есть свои недостатки. Осуществляя построение сети, необходимо помнить к каким результатам должна привести данная модель.

Для более детального анализа было решено использовать статистическое представление модели. Результаты, полученные с помощью моделирования всех процессов в сети, будут достаточным основанием для оценки качества построенной сети. Данная модель предполагает моделирование процессов в сети при помощи специальных программных средств.

VMware Workstation Pro: Мощный инструмент виртуализации для профессионалов

В середине 1990-х годов стандартные серверы и персональные компьютеры были невероятно неэффективными. Большую часть времени процессоры простаивали, ожидая задач. Проблема изоляции приложений и сред также была острой: сбой одной программы мог "положить" всю операционную систему.

В это время группа талантливых инженеров и исследователей из Калифорнийского университета в Беркли и Стэнфорда работала над концепцией виртуализации на платформе x86, которая тогда считалась практически невозможной для этого из-за архитектурных ограничений.

В 1998 году Мендель Розенблюм, Диана Грин (ставшая CEO), Скотт Девлин, Эдвард Ванг и Эд Бугонь основали компанию **VMware, Inc.** Название отражало суть технологии: "VM" — Virtual Machine (виртуальная машина), а "ware" — от software (ПО).

Их первой целью был рынок настольных ПК. Разработчики, тестировщики и IT-администраторы остро нуждались в инструменте для создания изолированных сред на своих рабочих станциях.

В **1999 году** свет увидела первая публичная версия **VMware**

Workstation 1.0 для Linux. Это был настоящий технологический шедевр. Она позволяла запускать на одном Linux-компьютере несколько экземпляров Windows 95, 98 и даже NT. Это произвело эффект разорвавшейся бомбы в IT-сообществе. Вскоре вышла и версия для Windows.

Эволюция и становление "Pro"

Первые версии VMware Workstation были бесплатными для некоммерческого использования. Однако технология была настолько передовой и востребованной в бизнесе, что компания быстро осознала необходимость коммерческого продукта с расширенной функциональностью и поддержкой.

2000-2001: Появляются VMware Workstation 2.0 с поддержкой большего количества гостевых ОС и VMware Workstation 3.0, которая уже четко разделяется на две линии: бесплатную **VMware GSX Server** (для рабочих групп) и платную **VMware ESX Server** (для корпоративных серверов). Сама Workstation продолжала развиваться как флагманский настольный продукт.

Ключевые инновации: С каждой версией добавлялись функции, которые стали отраслевым стандартом:

Снимки (Snapshots): Появились как "машина времени" для ВМ.

Виртуальные сети: Продвинутые возможности настройки виртуальных сетей (NAT, Host-only, Bridged).

Клонирование: Быстрое создание копий ВМ.

Поддержка USB и 3D-графики: Интеграция с периферийными устройствами и ускоренная графика.

Формирование линейки "Pro": Со временем, чтобы подчеркнуть профессиональную ориентацию продукта и отличать его от бесплатного аналога (который позже стал называться VMware Workstation Player), за продуктом закрепилось название **VMware Workstation Pro**.

Приобретение и дальнейшее развитие

В 2004 году VMware была приобретена корпорацией EMC, а позже, в 2016 году, стала частью Dell Technologies. Это дало компании огромные

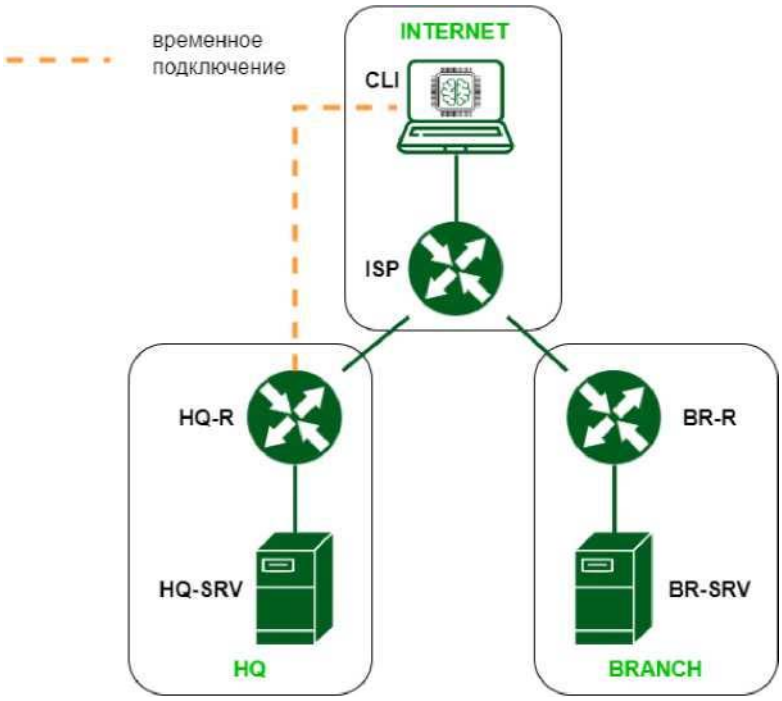
ресурсы для развития.

VMware Workstation Pro — это настольный гипервизор типа 2 (работающий поверх установленной операционной системы), который позволяет создавать и запускать несколько виртуальных машин (ВМ) одновременно на одном физическом компьютере под управлением Windows или Linux.

1 Задание

1.1 Модуль 1: Выполнение работ по проектированию сетевой инфраструктуры

Топология сети



1. Выполните базовую настройку всех устройств:

Присвоить имена в соответствии с топологией

Рассчитайте IP-адресацию IPv4 и IPv6. Необходимо заполнить таблицу №1, чтобы эксперты могли проверить ваше рабочее место.

Пул адресов для сети офиса BRANCH - не более 16

Пул адресов для сети офиса HQ - не более 64

Таблица 1.1

Имя устройства	**IP**
CLI	
ISP	
HQ-R	
HQ-SRV	
BR-R	

BR-SRV	
HQ-CLI	
HQ-AD	

2 Настройте внутреннюю динамическую маршрутизацию по средствам FRR. Выберите и обоснуйте выбор протокола динамической маршрутизации из расчёта, что в дальнейшем сеть будет масштабироваться.

a. Составьте топологию сети L3.

3 Настройте автоматическое распределение IP-адресов на роутере HQ-R.

a. Учтите, что у сервера должен быть зарезервирован адрес.

4 Настройте локальные учётные записи на всех устройствах в соответствии с таблицей 1.2.

Таблица 1.2

Учётная запись	**Пароль**	**Примечание**
Admin	P@ssw0rd	CLI HQ-SRV HQ-R
Branch admin	P@ssw0rd	BR-SRV BR-R
Network admin	P@ssw0rd	HQ-R BR-R BR-SRV

5 Измерьте пропускную способность сети между двумя узлами HQ-R-ISP по средствам утилиты iperf 3. Предоставьте описание пропускной способности канала со скриншотами.

6 Составьте backup скрипты для сохранения конфигурации сетевых устройств, а именно HQ-R BR-R. Продемонстрируйте их работу.

7 Настройте подключение по SSH для удалённого конфигурирования устройства HQ-SRV по порту 2222. Учтите, что вам необходимо перенаправить трафик на этот порт по средствам контролирования трафика.

8 Настройте контроль доступа до HQ-SRV по SSH со всех устройств, кроме CLI.

1.2 Модуль 2: Организация сетевого администрирования

Задание модуля 2 ГИА/ДЭ БУ,
1. Настройте DNS-сервер на сервере HQ-SRV: ГИА/ДЭ ПУ
a. На DNS сервере необходимо настроить 2 зоны
Зона hq.work, также не забудьте настроить обратную зону.

Имя	Тип записи	Адрес
hq-r.hq.work	A, PTR	IP-адрес
hq-srv.hq.work	A, PTR	IP-адрес

Зона branch.work

Имя	Тип записи	Адрес
br-r.branch.work	A, PTR	IP-адрес
r-srv.branch.work	A	IP-адрес

2. Настройте синхронизацию времени между сетевыми устройствами по протоколу NTP.
    a. В качестве сервера должен выступать роутер HQ-R со стратумом 5
    b. Используйте Loopback интерфейс на HQ-R, как источник сервера времени
    c. Все остальные устройства и сервера должны синхронизировать свое время с роутером HQ-R
    d. Все устройства и сервера настроены на московский часовой пояс (UTC +3)
3. Настройте сервер домена, выбор его типа обоснуйте, на базе HQ-SRV через web интерфейс, выбор технологий обоснуйте.
    a. Введите машины BR-SRV и CLI в данный домен
    b. Организуйте отслеживание подключения к домену
4. Реализуйте файловый SMB или NFS (выбор обоснуйте) сервер на базе сервера HQ-SRV.
    a. Должны быть опубликованы общие папки по названиям:
        i. Branch_Files - только для пользователя Branch admin;
        ii. Network - только для пользователя Network admin;
        iii. Admin_Files - только для пользователя Admin;
    b. Каждая папка должна монтироваться на всех серверах в папку /mnt/<name_folder> (например, /mnt/All_files) автоматически при входе доменного пользователя в систему и отключаться при его выходе из сессии. Монтироваться должны только доступные пользователю каталоги.

5. Сконфигурируйте веб-сервер LMS Apache на сервере BR- SRV:
    a. На главной странице должен отражаться номер места
    b. Используйте базу данных mySQL

Создайте пользователей в соответствии с таблицей, пароли у всех пользователей «P@ssw0rd»

Пользователь	Группа
Admin	**Admin**
Managerl	**Manager**
Manager2	**Manager**
Manager3	**Manager**
Userl	**WS**
User2	**WS**
User3	**WS**

User4	WS
User5	TEAM
User6	TEAM
User7	TEAM

h. Установите авторизацию по сертификату выданным HQ-SRV

4. Реализуйте антивирусную защиту по средствам ClamAV на устройствах HQ-SRV и BR-SRV:

   a. Настройте сканирование системы раз в сутки с сохранением отчёта

   i. Учтите, что сканирование должно проводится при условии, что от пользователей нет нагрузки

5. Настройте систему управления трафиком на роутере BR-R для контроля входящего трафика в соответствии со следующими правилами:
   a. Разрешите подключения к портам DNS (порт 53), HTTP (порт 80) и HTTPS (порт 443) для всех клиентов. Эти порты необходимы для работы настраиваемых служб.
   b. Разрешите работу выбранного протокола организации защищенной связи. Разрешение портов должно быть выполнено по принципу "необходимо и достаточно".
   c. Разрешите работу протоколов ICMP (протокол управления сообщениями Internet).
   d. Разрешите работу протокола SSH (Secure Shell) (SSH используется для безопасного удаленного доступа и управления устройствами).
   e. Запретите все прочие подключения.
   f. Все другие подключения должны быть запрещены для обеспечения безопасности сети.
6. Настройте виртуальный принтер с помощью CUPS для возможности печати документов из Linux-системы на сервере BR-SRV.
7. Между офисами HQ и BRANCH установите защищенный туннель, позволяющий осуществлять связь между регионами с применением внутренних адресов.
8. По средствам уже настроенного мониторинга установите следующие параметры:
   a. Warning
      i. Нагрузка процессора больше или равна 70%
      ii. Заполненность оперативной памяти больше или равна 80%
      iii. Заполненность диска больше или равна 85%
   b. Напишите план действия при получении Warning сообщений
9. Настройте программный RAID 5 из дисков по 1 Гб, которые подключены к машине BR-SRV.
10. Настройте Bacula на сервере HQ-SRV для резервного копирования etc на сервере BR-SRV.

2 Топология . Предварительная настройка VMware Workstation Pro

Разбиение сетей на подсети

Название устройства	NIC	Сеть (подсеть)	IP-адрес	Шлюз
BR-R	ISP <-> BR-RTR	172.16.5.0/28	172.16.5.2/28	172.16.5.1
	BR-R <-> BR-SRV	192.168.2.0/28	192.168.200.1/28	-
	Tunnel (GRE)	10.10.10.0/30	10.10.10.1/30	-
BR-SRV	BR-SRV<-> BR-R	192.168.2.0/28	192.168.2.2/28	192.168.2.1/28
HQ-R	ISP <-> HQ-R	172.16.4.0/28	172.16.4.2/28	172.16.4.1
	HQ-R <-> HQ -SRV	192.168.1.0/26	192.168.1.1/26	-
	Tunnel (GRE)	10.10.10.0/30	10.10.10.2/30	-
HQ-CLI	ISP	192.168.3.0/24	192.168.3.2/24	192.168.3.1/24
HQ-SRV	HQ-R	192.168.1.0/26	192.168.1.2/26	192.168.1.1

255.255.255.0 /24 маска — 1 сеть в которой 256 адресов от 0 до 255

255.255.255.128 /25 маска — 2 сети в каждой из которых по 128 адресов от 0 до 127 и от 128 до 256

255.255.255.192 /26 маска — 4 сети в каждой из которых по 64 адреса

255.255.255.224 /27 маска — 8 сетей по 32 адреса

255.255.255.240 /28 маска — 16 сетей по 16 адресов

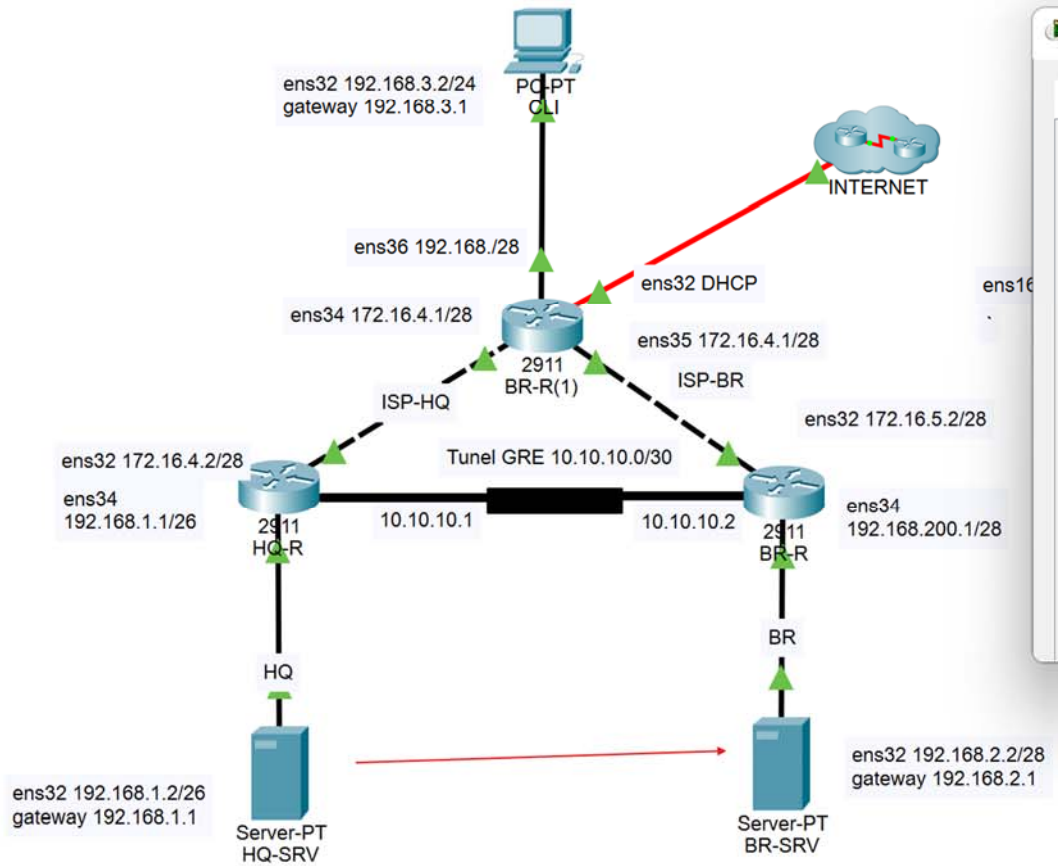
255.255.255. 248 /29 маска — 32 сети по 8 адресов

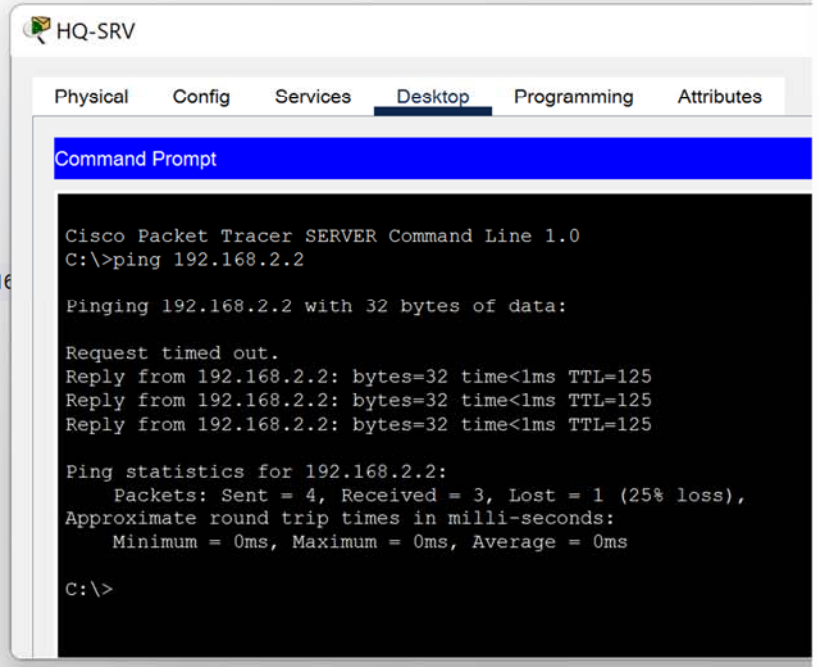
255.255.255.252 /30 маска — 64 сети по 4 адреса

255.255.255.254 /31 маска — 128 сетей по 2 адреса

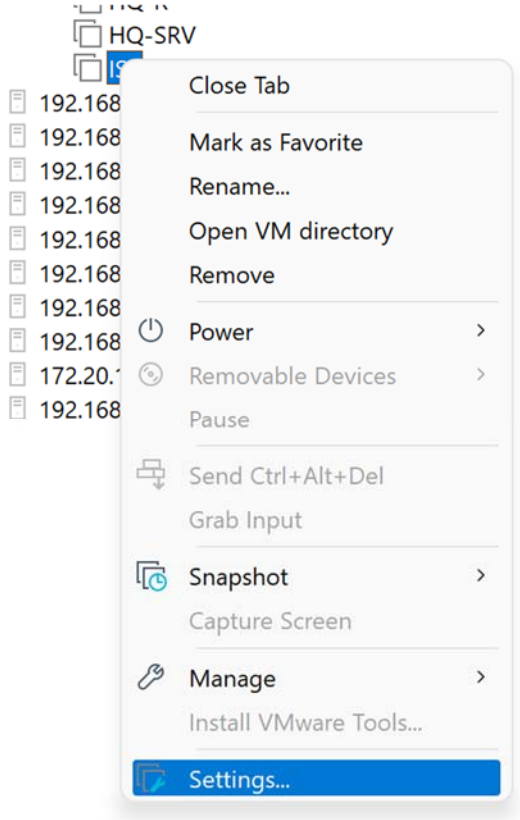
255.255.255.255 /32 маска — 256 сетей по 1 адресу

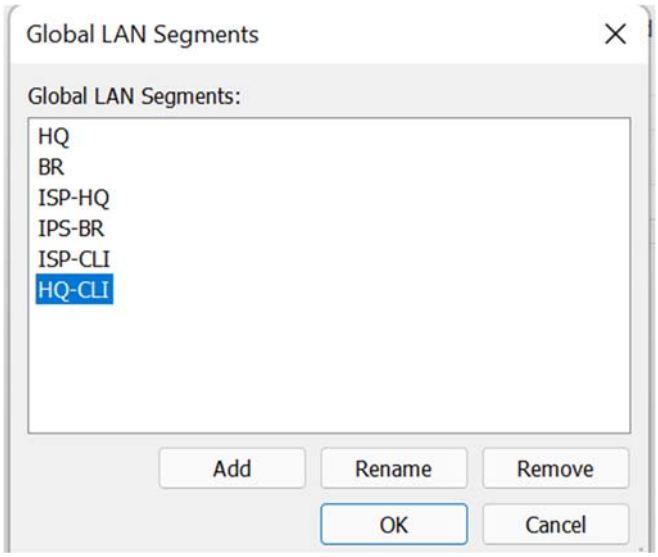
Разработаем схему сети в Cisco Packet Tracer


ens32 192.168.3.2/24
gateway 192.168.3.1
PC-PT
CLI
INTERNET
ens36 192.168./28
ens32 DHCP
ens34 172.16.4.1/28
ens35 172.16.4.1/28
2911
BR-R(1)
ISP-HQ
ISP-BR
ens32 172.16.5.2/28
ens32 172.16.4.2/28
Tunel GRE 10.10.10.0/30
ens34
192.168.1.1/26
2911
HQ-R
10.10.10.1
10.10.10.2
2911
BR-R
ens34
192.168.200.1/28
BR
HQ
ens32 192.168.1.2/26
gateway 192.168.1.1
Server-PT
HQ-SRV
Server-PT
BR-SRV
ens32 192.168.2.2/28
gateway 192.168.2.1

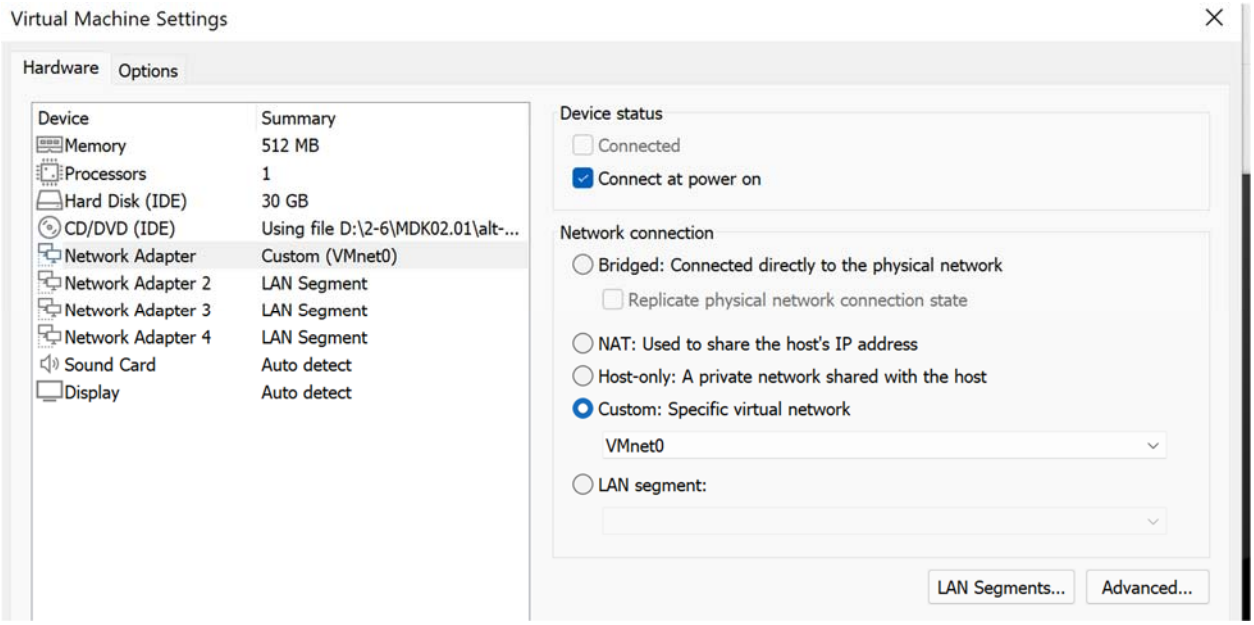

HQ-SRV
Physical
Config
Services
Desktop
Programming
Attributes
Command Prompt
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ping 192.168.2.2
Pinging 192.168.2.2 with 32 bytes of data:
Request timed out.
Reply from 192.168.2.2: bytes=32 time<1ms TTL=125
Reply from 192.168.2.2: bytes=32 time<1ms TTL=125
Reply from 192.168.2.2: bytes=32 time<1ms TTL=125
Ping statistics for 192.168.2.2:
Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>

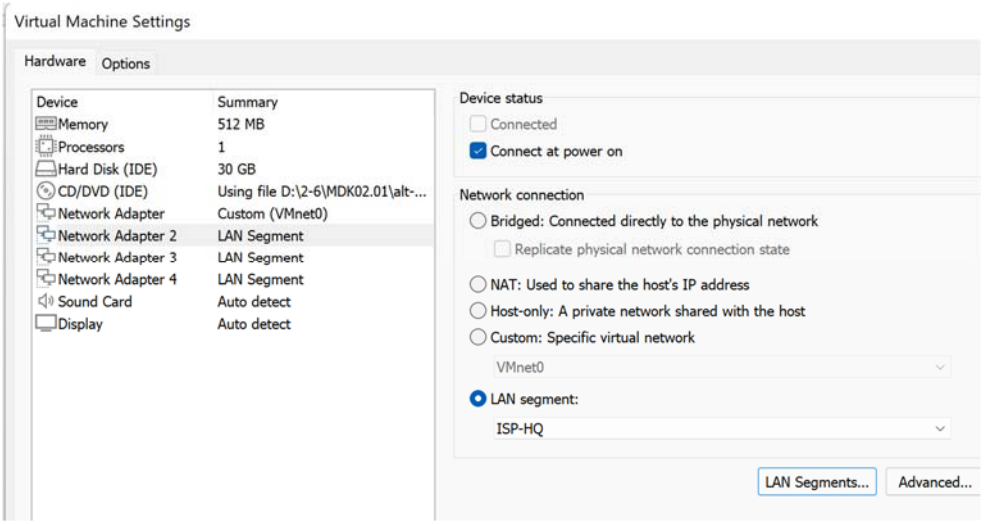
Необходимо создать виртуальные коммутаторы

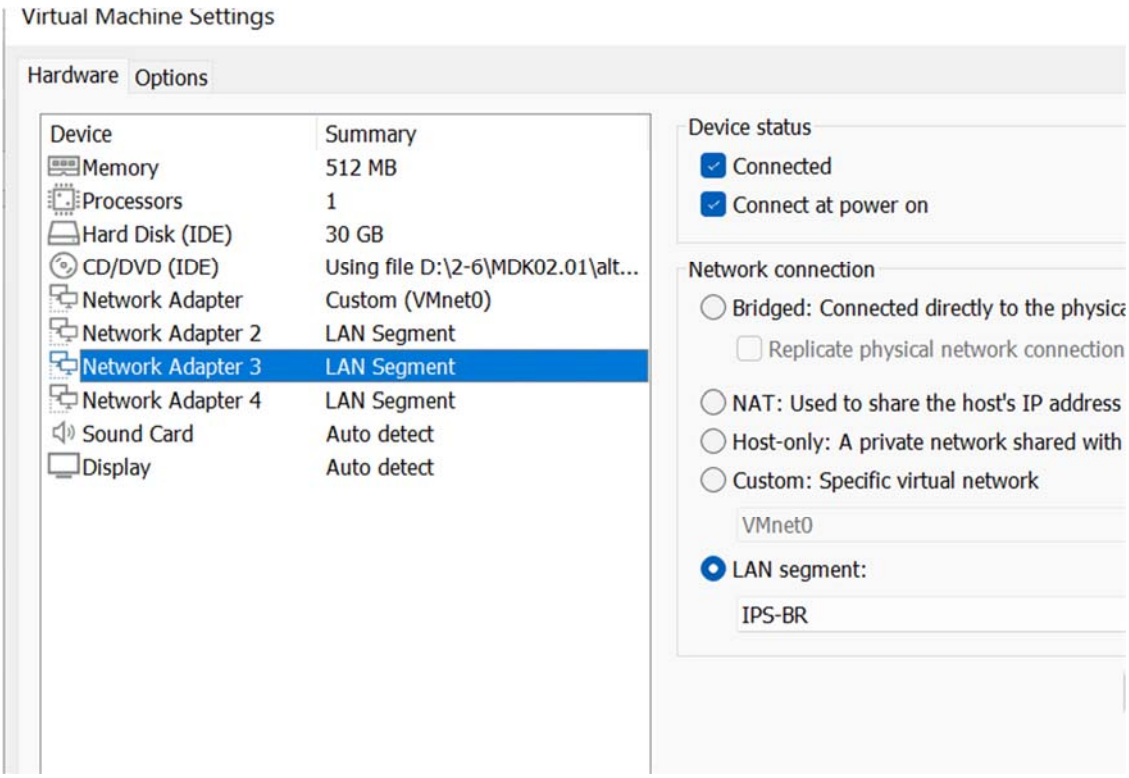


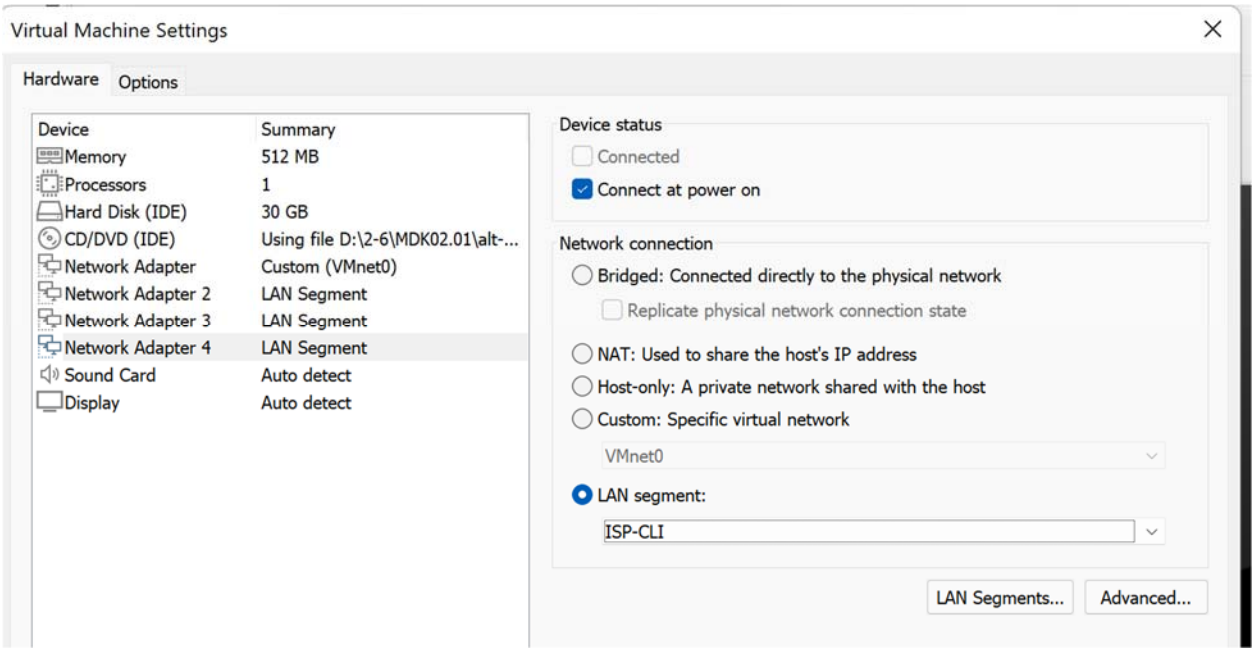


Настройка ISP

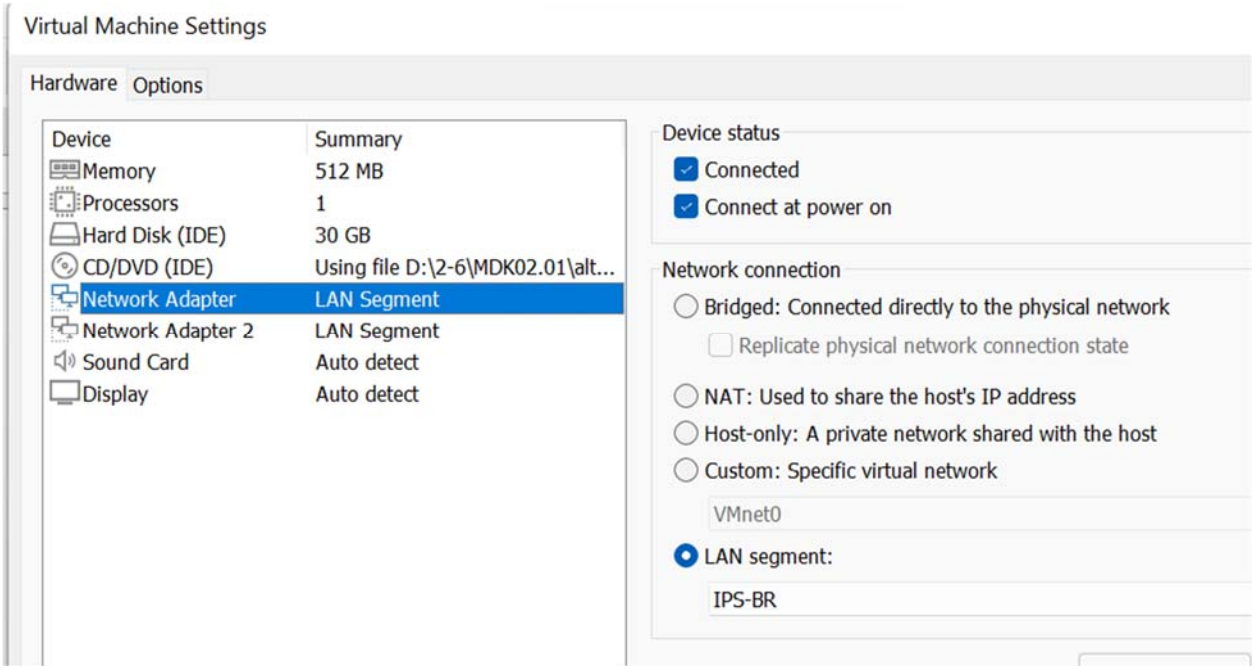

Virtual Machine Settings
Hardware
Options
Device
Summary
Memory
512 MB
Processors
1
Hard Disk (IDE)
30 GB
CD/DVD (IDE)
Using file D:\2-6\MDK02.01\alt-...
Network Adapter
Custom (VMnet0)
Network Adapter 2
LAN Segment
Network Adapter 3
LAN Segment
Network Adapter 4
LAN Segment
Sound Card
Auto detect
Display
Auto detect
Device status
Connected
Connect at power on
Network connection
Bridged: Connected directly to the physical network
Replicate physical network connection state
NAT: Used to share the host's IP address
Host-only: A private network shared with the host
Custom: Specific virtual network
VMnet0
LAN segment:
LAN Segments...
Advanced...

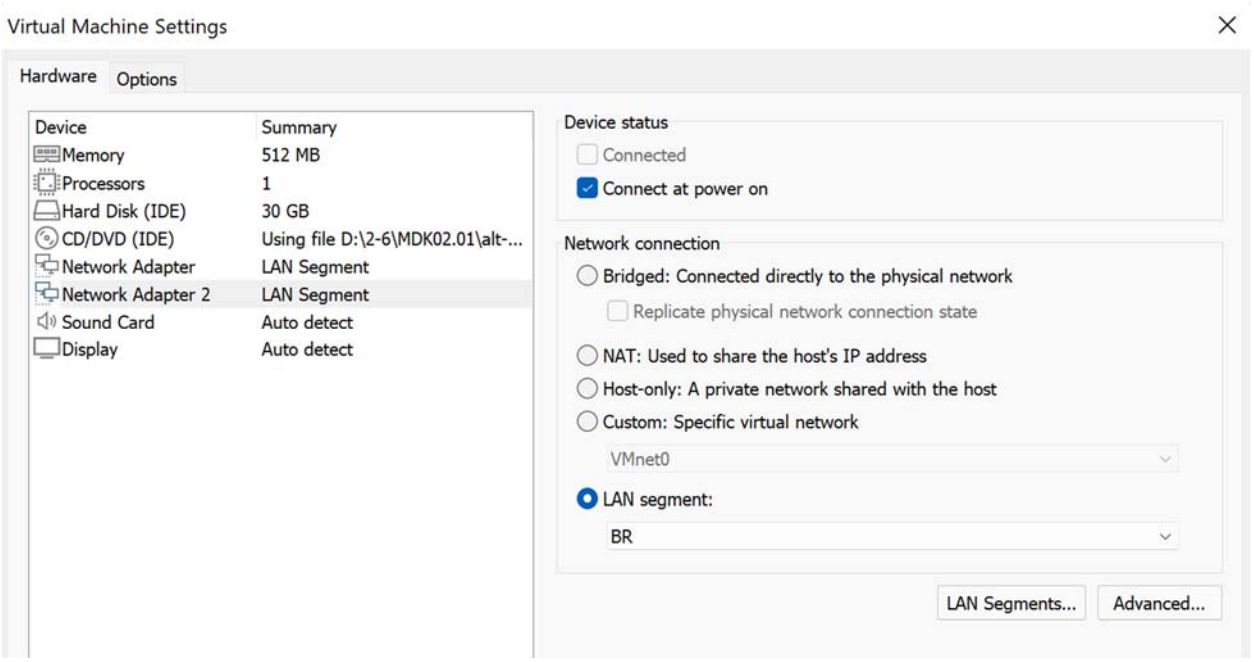

Virtual Machine Settings
Hardware
Options
Device
Summary
Memory
512 MB
Processors
1
Hard Disk (IDE)
30 GB
CD/DVD (IDE)
Using file D:\2-6\MDK02.01\alt-...
Network Adapter
Custom (VMnet0)
Network Adapter 2
LAN Segment
Network Adapter 3
LAN Segment
Network Adapter 4
LAN Segment
Sound Card
Auto detect
Display
Auto detect
Device status
Connected
Connect at power on
Network connection
Bridged: Connected directly to the physical network
Replicate physical network connection state
NAT: Used to share the host's IP address
Host-only: A private network shared with the host
Custom: Specific virtual network
VMnet0
LAN segment:
ISP-HQ
LAN Segments...
Advanced...


Virtual Machine Settings
Hardware
Options
Device
Summary
Memory
512 MB
Processors
1
Hard Disk (IDE)
30 GB
CD/DVD (IDE)
Using file D:\2-6\MDK02.01\alt...
Network Adapter
Custom (VMnet0)
Network Adapter 2
LAN Segment
Network Adapter 3
LAN Segment
Network Adapter 4
LAN Segment
Sound Card
Auto detect
Display
Auto detect
Device status
Connected
Connect at power on
Network connection
Bridged: Connected directly to the physica
Replicate physical network connection
NAT: Used to share the host's IP address
Host-only: A private network shared with
Custom: Specific virtual network
VMnet0
LAN segment:
IPS-BR

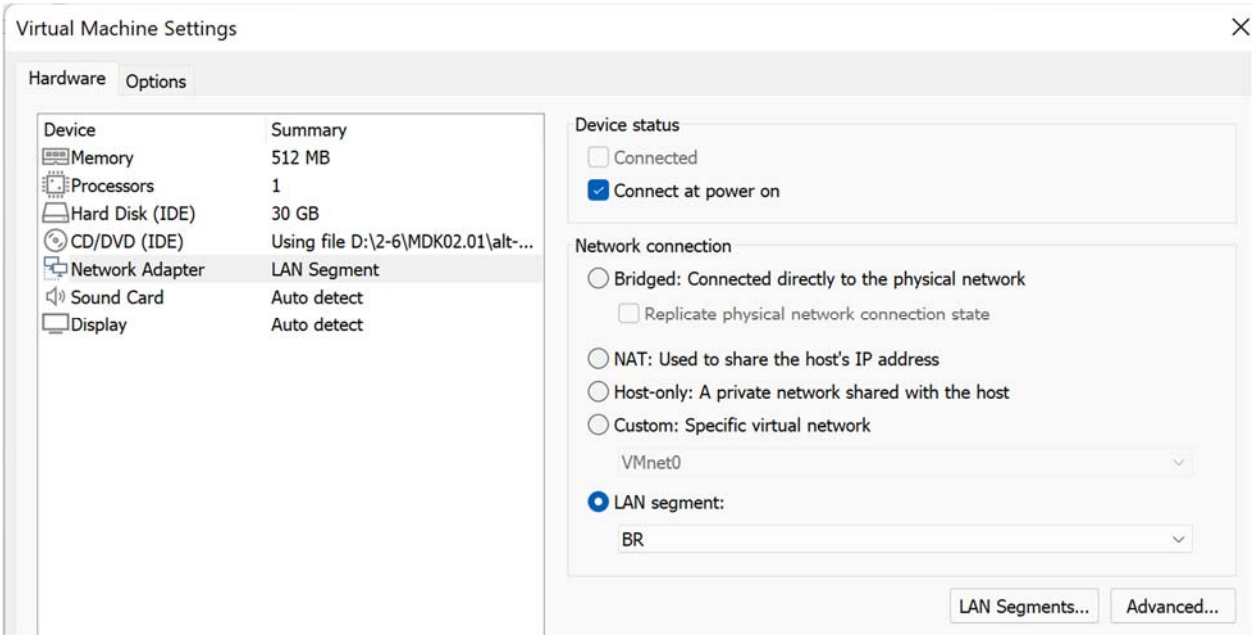

Virtual Machine Settings
Hardware
Options
Device
Summary
Memory
512 MB
Processors
1
Hard Disk (IDE)
30 GB
CD/DVD (IDE)
Using file D:\2-6\MDK02.01\alt-...
Network Adapter
Custom (VMnet0)
Network Adapter 2
LAN Segment
Network Adapter 3
LAN Segment
Network Adapter 4
LAN Segment
Sound Card
Auto detect
Display
Auto detect
Device status
Connected
Connect at power on
Network connection
Bridged: Connected directly to the physical network
Replicate physical network connection state
NAT: Used to share the host's IP address
Host-only: A private network shared with the host
Custom: Specific virtual network
VMnet0
LAN segment:
ISP-CLI
LAN Segments...
Advanced...

BR-R

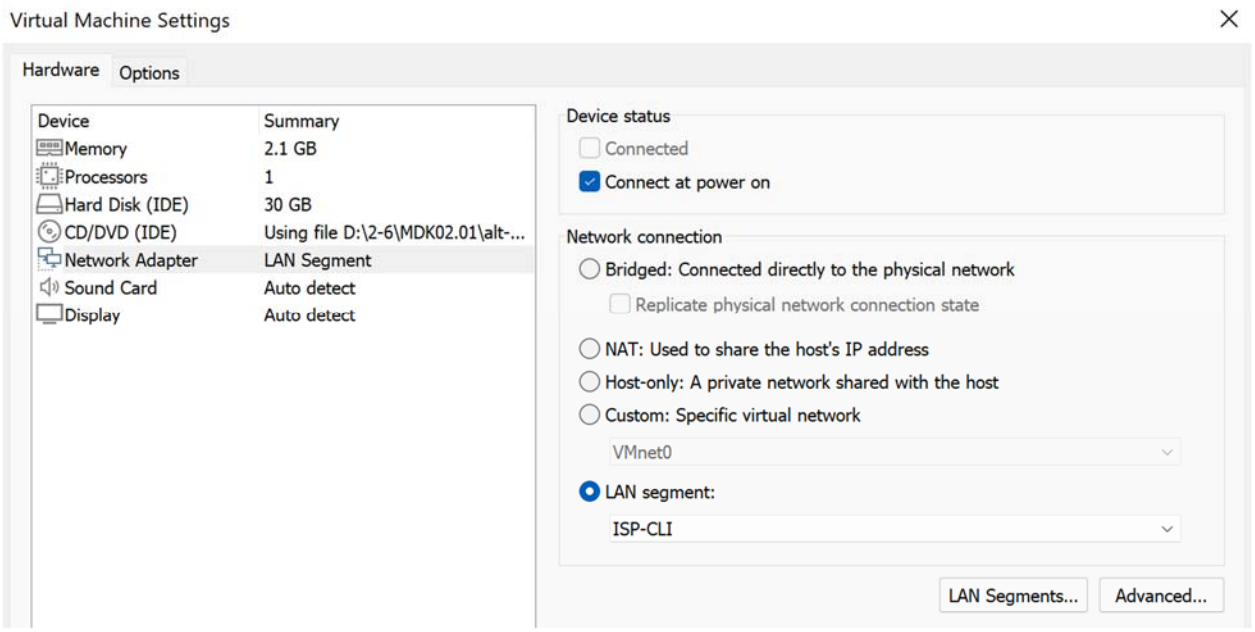

Virtual Machine Settings
Hardware
Options
Device
Summary
Memory
512 MB
Processors
1
Hard Disk (IDE)
30 GB
CD/DVD (IDE)
Using file D:\2-6\MDK02.01\alt...
Network Adapter
LAN Segment
Network Adapter 2
LAN Segment
Sound Card
Auto detect
Display
Auto detect
Device status
Connected
Connect at power on
Network connection
Bridged: Connected directly to the physical network
Replicate physical network connection state
NAT: Used to share the host's IP address
Host-only: A private network shared with the host
Custom: Specific virtual network
VMnet0
LAN segment:
IPS-BR

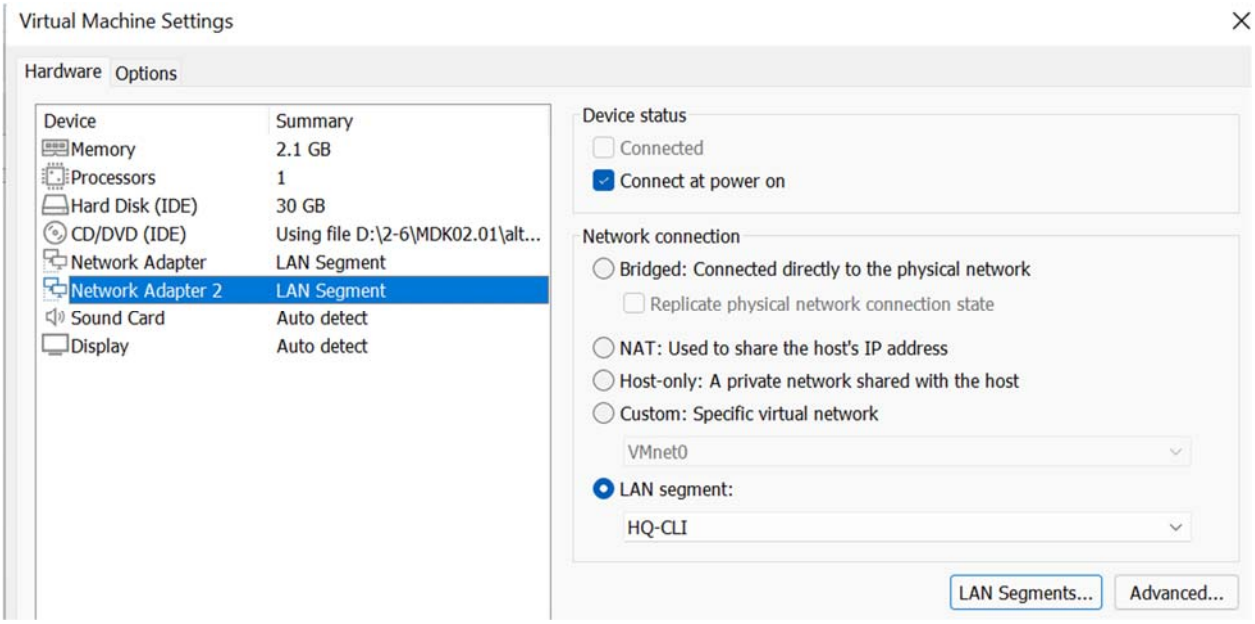

Virtual Machine Settings
Hardware
Options
Device
Summary
Memory
512 MB
Processors
1
Hard Disk (IDE)
30 GB
CD/DVD (IDE)
Using file D:\2-6\MDK02.01\alt-...
Network Adapter
LAN Segment
Network Adapter 2
LAN Segment
Sound Card
Auto detect
Display
Auto detect
Device status
Connected
Connect at power on
Network connection
Bridged: Connected directly to the physical network
Replicate physical network connection state
NAT: Used to share the host's IP address
Host-only: A private network shared with the host
Custom: Specific virtual network
VMnet0
LAN segment:
BR
LAN Segments...
Advanced...

BR-SRV

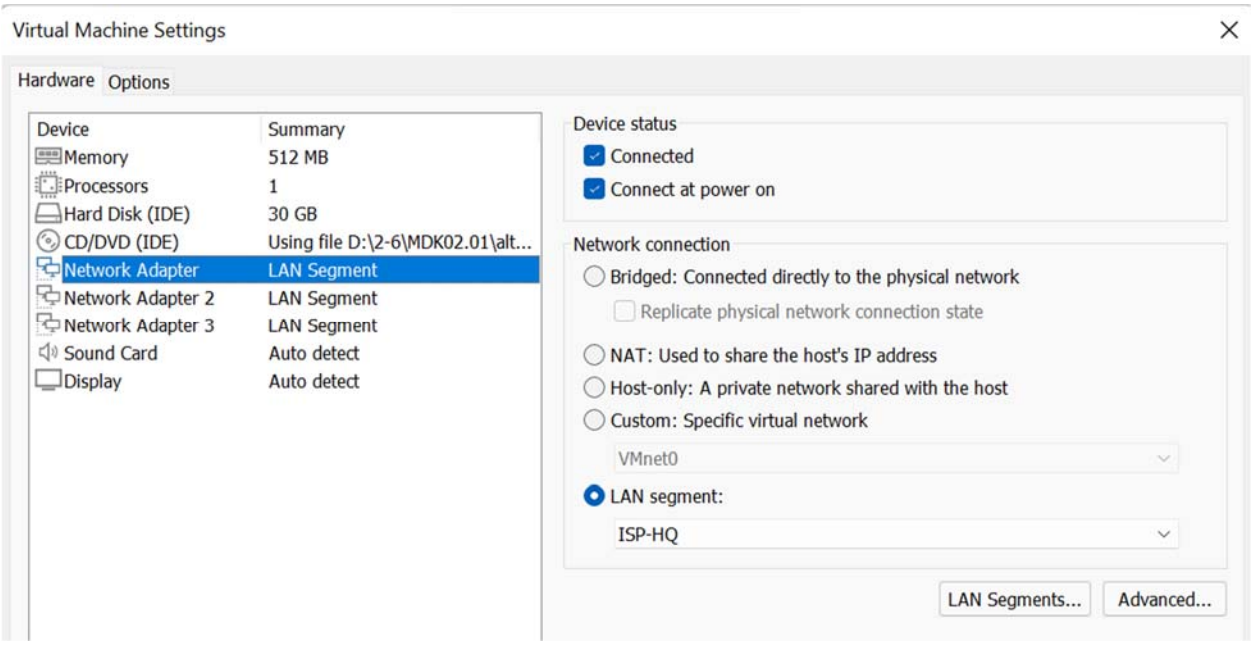

Virtual Machine Settings
Hardware
Options
Device
Summary
Memory
512 MB
Processors
1
Hard Disk (IDE)
30 GB
CD/DVD (IDE)
Using file D:\2-6\MDK02.01\alt-...
Network Adapter
LAN Segment
Sound Card
Auto detect
Display
Auto detect
Device status
Connected
Connect at power on
Network connection
Bridged: Connected directly to the physical network
Replicate physical network connection state
NAT: Used to share the host's IP address
Host-only: A private network shared with the host
Custom: Specific virtual network
VMnet0
LAN segment:
BR
LAN Segments...
Advanced...

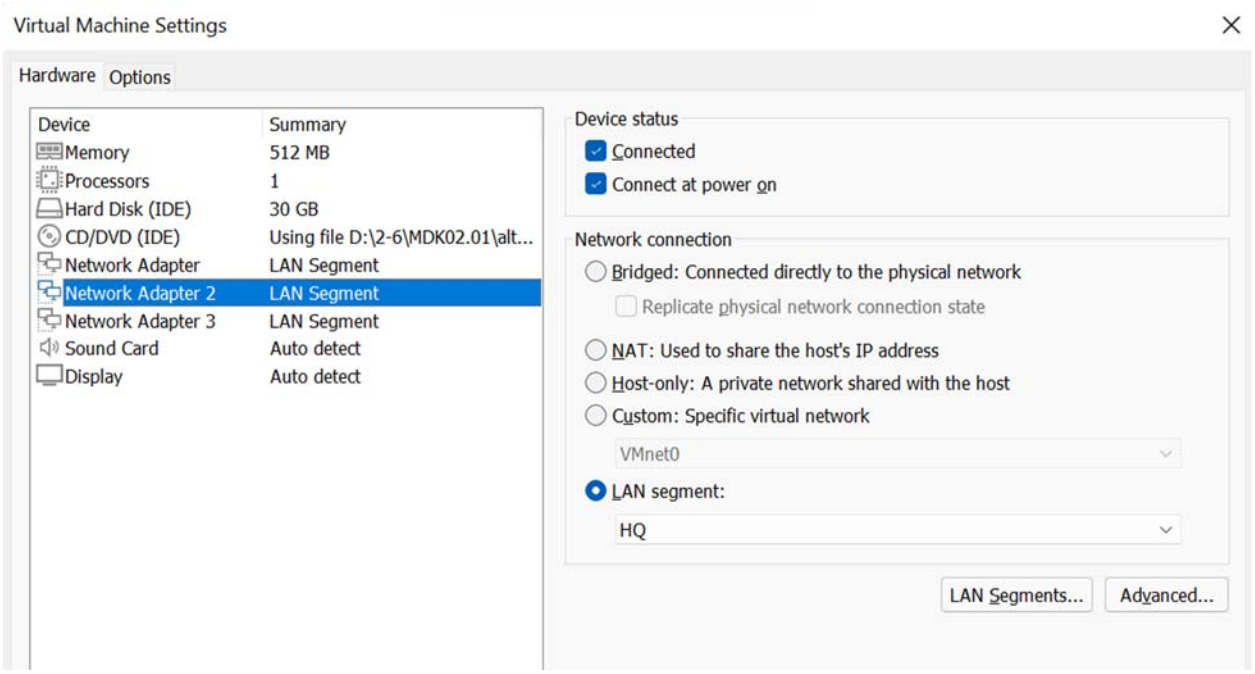
CLI

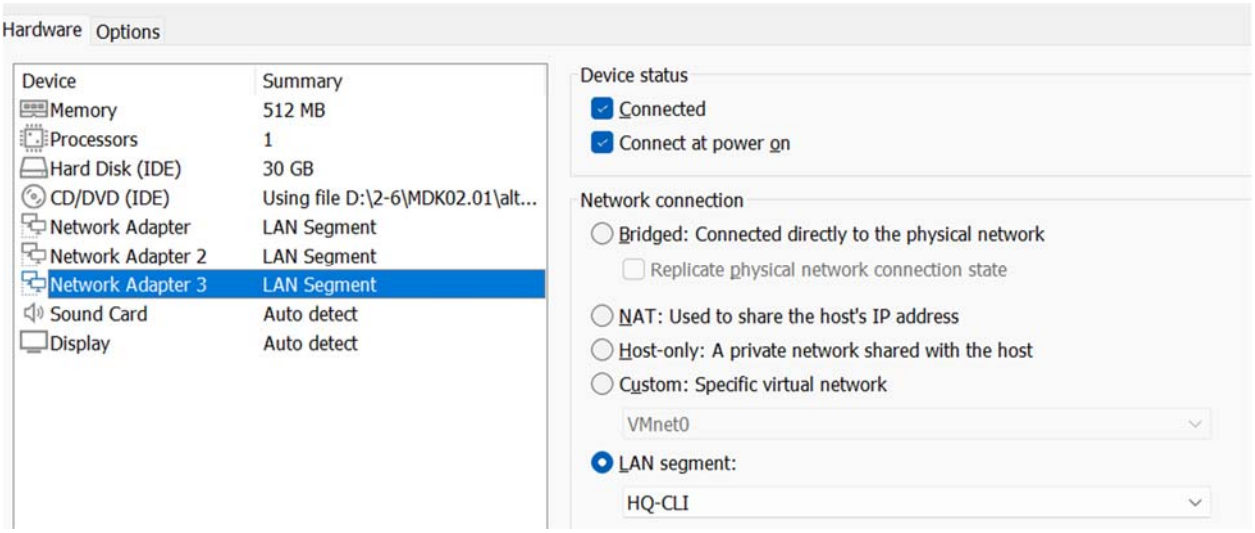

Virtual Machine Settings
Hardware
Options
Device
Summary
Memory
2.1 GB
Processors
1
Hard Disk (IDE)
30 GB
CD/DVD (IDE)
Using file D:\2-6\MDK02.01\alt-...
Network Adapter
LAN Segment
Sound Card
Auto detect
Display
Auto detect
Device status
Connected
Connect at power on
Network connection
Bridged: Connected directly to the physical network
Replicate physical network connection state
NAT: Used to share the host's IP address
Host-only: A private network shared with the host
Custom: Specific virtual network
VMnet0
LAN segment:
ISP-CLI
LAN Segments...
Advanced...


Virtual Machine Settings
Hardware
Options
Device
Summary
Memory
2.1 GB
Processors
1
Hard Disk (IDE)
30 GB
CD/DVD (IDE)
Using file D:\2-6\MDK02.01\alt...
Network Adapter
LAN Segment
Network Adapter 2
LAN Segment
Sound Card
Auto detect
Display
Auto detect
Device status
Connected
Connect at power on
Network connection
Bridged: Connected directly to the physical network
Replicate physical network connection state
NAT: Used to share the host's IP address
Host-only: A private network shared with the host
Custom: Specific virtual network
VMnet0
LAN segment:
HQ-CLI
LAN Segments...
Advanced...

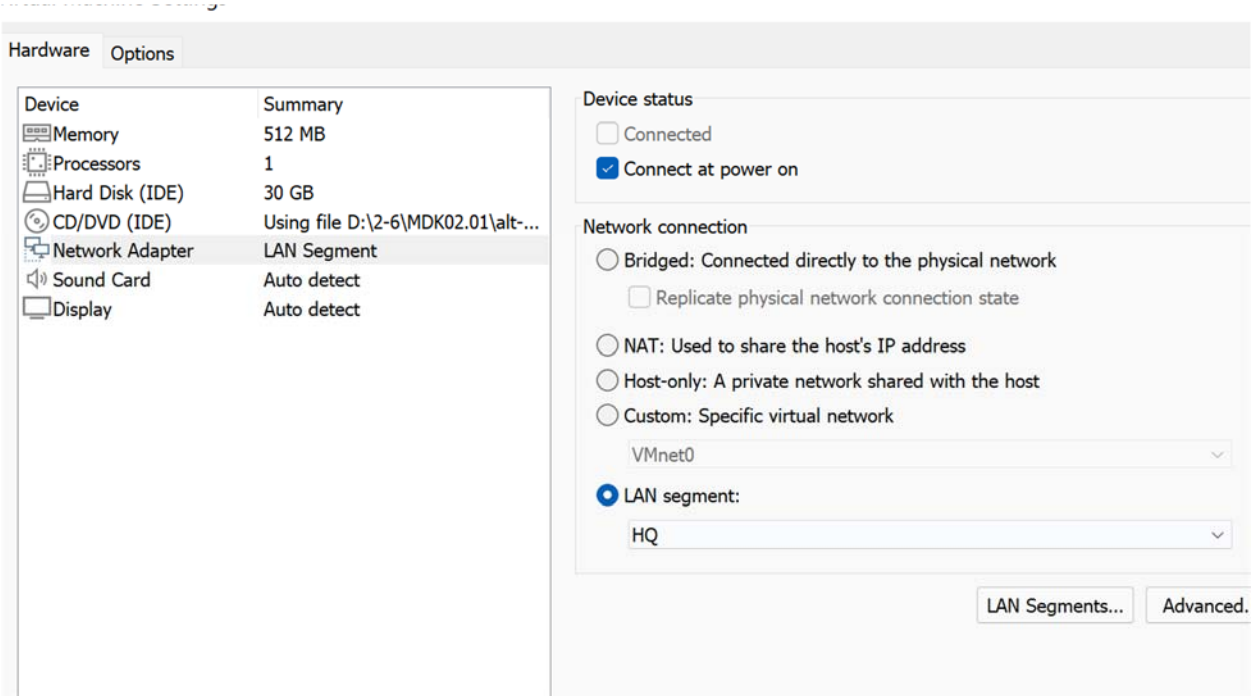
HQ-R

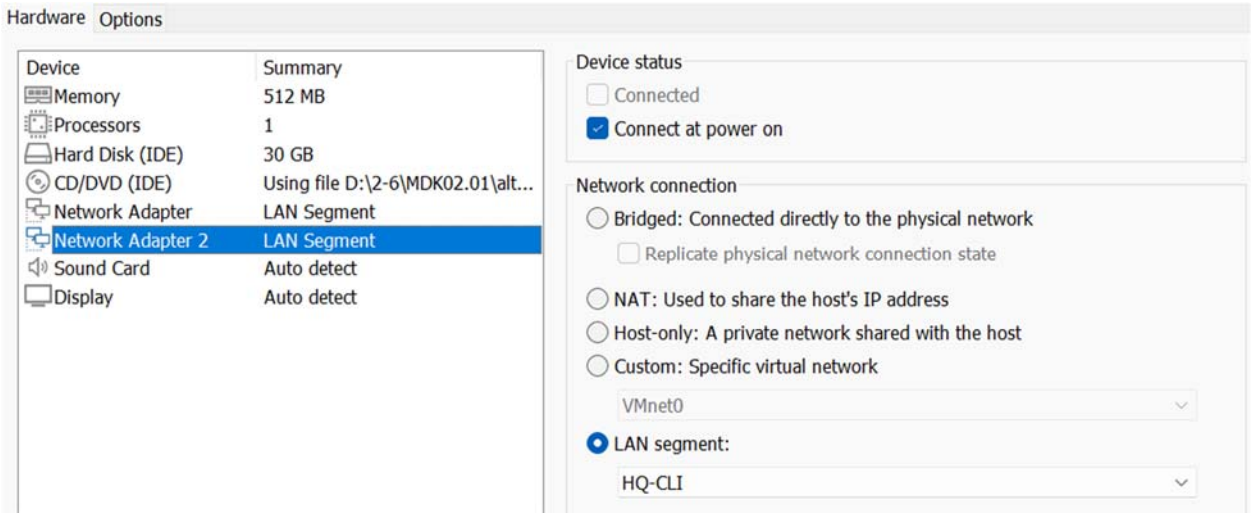

Virtual Machine Settings
Hardware
Options
Device
Summary
Memory
512 MB
Processors
1
Hard Disk (IDE)
30 GB
CD/DVD (IDE)
Using file D:\2-6\MDK02.01\alt...
Network Adapter
LAN Segment
Network Adapter 2
LAN Segment
Network Adapter 3
LAN Segment
Sound Card
Auto detect
Display
Auto detect
Device status
Connected
Connect at power on
Network connection
Bridged: Connected directly to the physical network
Replicate physical network connection state
NAT: Used to share the host's IP address
Host-only: A private network shared with the host
Custom: Specific virtual network
VMnet0
LAN segment:
ISP-HQ
LAN Segments...
Advanced...


Virtual Machine Settings
Hardware
Options
Device
Summary
Memory
512 MB
Processors
1
Hard Disk (IDE)
30 GB
CD/DVD (IDE)
Using file D:\2-6\MDK02.01\alt...
Network Adapter
LAN Segment
Network Adapter 2
LAN Segment
Network Adapter 3
LAN Segment
Sound Card
Auto detect
Display
Auto detect
Device status
Connected
Connect at power on
Network connection
Bridged: Connected directly to the physical network
Replicate physical network connection state
NAT: Used to share the host's IP address
Host-only: A private network shared with the host
Custom: Specific virtual network
VMnet0
LAN segment:
HQ
LAN Segments...
Advanced...


Hardware
Options
Device
Summary
Memory
512 MB
Processors
1
Hard Disk (IDE)
30 GB
CD/DVD (IDE)
Using file D:\2-6\MDK02.01\alt...
Network Adapter
LAN Segment
Network Adapter 2
LAN Segment
Network Adapter 3
LAN Segment
Sound Card
Auto detect
Display
Auto detect
Device status
Connected
Connect at power on
Network connection
Bridged: Connected directly to the physical network
Replicate physical network connection state
NAT: Used to share the host's IP address
Host-only: A private network shared with the host
Custom: Specific virtual network
VMnet0
LAN segment:
HQ-CLI

HQ-SRV


Hardware
Options
Device
Summary
Memory
512 MB
Processors
1
Hard Disk (IDE)
30 GB
CD/DVD (IDE)
Using file D:\2-6\MDK02.01\alt-...
Network Adapter
LAN Segment
Sound Card
Auto detect
Display
Auto detect
Device status
Connected
Connect at power on
Network connection
Bridged: Connected directly to the physical network
Replicate physical network connection state
NAT: Used to share the host's IP address
Host-only: A private network shared with the host
Custom: Specific virtual network
VMnet0
LAN segment:
HQ
LAN Segments...
Advanced.


Hardware
Options
Device
Summary
Memory
512 MB
Processors
1
Hard Disk (IDE)
30 GB
CD/DVD (IDE)
Using file D:\2-6\MDK02.01\alt...
Network Adapter
LAN Segment
Network Adapter 2
LAN Segment
Sound Card
Auto detect
Display
Auto detect
Device status
Connected
Connect at power on
Network connection
Bridged: Connected directly to the physical network
Replicate physical network connection state
NAT: Used to share the host's IP address
Host-only: A private network shared with the host
Custom: Specific virtual network
VMnet0
LAN segment:
HQ-CLI

3 Вариант преднастройки ISP

Настройте адресацию на интерфейсах:

- Интерфейс, подключенный к **магистральному провайдеру**, получает адрес по **DHCP**
- Настройте маршруты по умолчанию там, где это необходимо
- Интерфейс, к которому подключен **HQ-R**, подключен к сети **172.16.4.0/28**
- Интерфейс, к которому подключен **BR-R**, подключен к сети **172.16.5.0/28**
- На ISP настройте **динамическую сетевую трансляцию** в сторону HQ-R и BR-R для доступа к сети Интернет

3.1 Базовая настройка, адресация и маршрутизация

Изменяем имя

#hostnamectl set-hostname ips.au-team.irpo ; exec bash

- Настроим интернет в сети ISP-HQ и ISP-BR.
- Для этого на ISP настраиваем интерфейс ens32 для получения адреса по DHCP
  #nano /etc/net/ifaces/ens32/options

Ctrl+o -> Enter (сохраняем изменения в файле)

Ctrl+x (выходим из редактирования файла)

Сетевые интерфейсы подключённые к ISP:

- **ens32** - сеть Интернет;
- **ens34** - сеть в сторону офиса HQ;
- **ens35** - сеть в сторону офиса BRANCH;
- **ens36** - сеть в сторону CLI;

- cp /etc/net/ifaces/ens34/options /etc/net/ifaces/ens35/

cp /etc/net/ifaces/ens34/options /etc/net/ifaces/ens36/

Или можно простым bash-скриптом сразу записать все опции для всех сетевых интерфейсов:

```
 for i in {4..6}; do
  cat <<EOF > /etc/net/ifaces/ens3$i/options
  TYPE=eth
  DISABLED=no
  NM_CONTROLLED=no
  BOOTPROTO=static
  CONFIG_IPV4=yes
  EOF
done
```

теперь назначаем IPv4 -адреса на сетевые интерфейсы:

- **ens34** - сеть в сторону офиса HQ

echo 172.16.4.1/28 > /etc/net/ifaces/ens34/ipv4address

- **ens35** - сеть в сторону офиса BRANCH;

echo 172.16.5.1/28 > /etc/net/ifaces/ens35/ipv4address

- **ens36** - сеть в сторону CLI;

echo 192.168.3.1/24 > /etc/net/ifaces/ens36/ipv4address

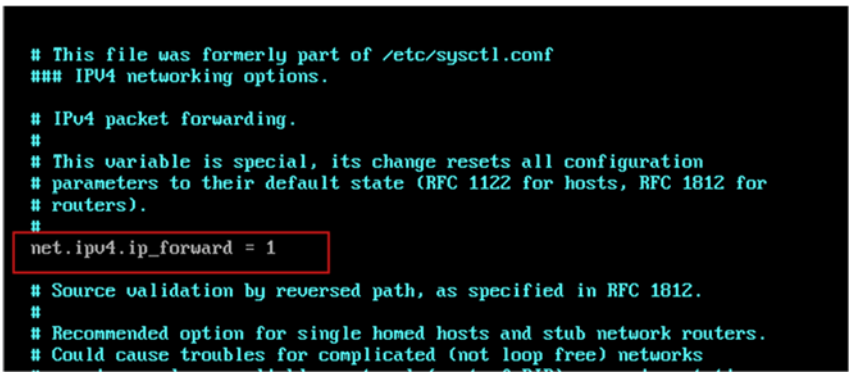
Таким образом, должна получиться следующая структура в директориях сетевых интерфейсов:

Tree — программа рекурсивного вывода каталогов, которая отображает содержимое каталогов в виде дерева. Она выводит пути и файлы каталогов в каждом подкаталоге, а также предоставляет сводку общего количества подкаталогов и файлов.

Включаем forwarding – маршрутизацию (На ALT Linux включить forwarding (маршрутизацию) (IP-форвардинг) можно через файл sysctl.conf или с помощью утилиты iptables. По умолчанию IP-форвардинг отключён, и его нужно включить, чтобы система могла пересылать пакеты между сетевыми интерфейсами.):

Включаем forwarding для IPv4 посредством редактирования файла по пути **/etc/net/sysctl.conf**

#vim /etc/net/sysctl.conf



Для применения всех сетевых настроек перезагружаем службу "network"

#systemctl restart network

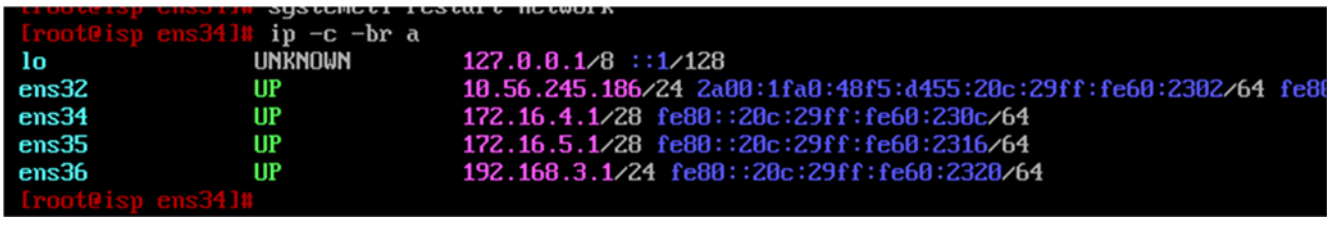


Рисунок -2.7

3.2 Настройка динамической трансляции адресов

Iptables в Alt Linux— это инструмент, который позволяет сохранять правила iptables на постоянной основе. Это гарантирует, что правила брандмауэра останутся неизменными даже после перезагрузки системы.

Iptables — утилита для настройки программного Firewall (межсетевого экрана) в Linux. Она предустанавливается по умолчанию во все сборки Linux, начиная с версии 2.4. с помощью iptables администраторы создают и изменяют правила, управляющие фильтрацией и перенаправлением пакетов. Некоторые возможности утилиты:

Настройка фильтрации пакетов. Есть два вида фильтрации: stateless (проверка статических параметров одного пакета, например IP-адреса источника и получателя, порта) и statefull (анализ потоков трафика, с помощью которого можно определить параметры целой TCP-сессии или UDP-потока). Настройка трансляции IP-адресов и портов. Можно настроить NAT, PAT, NAPT.

Настройка политик QoS. Манипуляции с пакетами, например изменение полей в заголовке IP.

Выполнятеся для настройки доступа в Интернет из сетей:

- HQ
- BRANCH
- CLI

Установка iptables:

- Устанавливаем **iptables**:

apt-get update && apt-get install -y iptables

Настройка iptables:

Далее создаём необходимую структуру для **iptables** (семейство, таблица, цепочка) для настройки NAT:

Напишем правило NAT для предоставления доступа в сеть интернет через интерфейс ens32 сетям ISP-HQ и ISP-BR:

```
[root@isp /]# iptables -t nat -A POSTROUTING -o ens32 -j MASQUERADE
[root@isp /]# iptables-save >
bash: syntax error near unexpected token `newline'

[root@isp etc]# iptables-save > /etc/sysconfig/iptables
[root@isp etc]# _
```

- Включаем и добавляем в автозагрузку службу **iptables**:

```
[root@isp sysconfig]# systemctl enable --now iptables
Synchronizing state of iptables.service with SysV service scri
Executing: /usr/lib/systemd/systemd-sysv-install enable iptabl
```

3.3 Установка утилиты iperf 3

Установка утилиты iperf 3

Необходимо установить пакет "iperf3" для проверки пропускной способности сети между серверами

#apt-get install -y iperf3

Выполнить запуск службы iperf3:

#systemctl enable --now iperf3

Проверяем:

```
[root@isp ens34]# systemctl status iperf3
● iperf3.service - Iperf3 Server
     Loaded: loaded (/usr/lib/systemd/system/iperf3.service; enabled; preset: disabled)
     Active: active (running) since Sat 2025-10-04 13:15:44 MSK; 34s ago
    Process: 8035 ExecStart=/usr/bin/iperf3 $ARGS (code=exited, status=0/SUCCESS)
   Main PID: 8037 (iperf3)
      Tasks: 1 (limit: 534)
     Memory: 696.0K (peak: 1.4M)
        CPU: 48ms
     CGroup: /system.slice/iperf3.service
             └─8037 /usr/bin/iperf3 -s -D

Oct 04 13:15:44 isp.au-team.irpo systemd[1]: Starting iperf3.service - Iperf3 Server...
Oct 04 13:15:44 isp.au-team.irpo systemd[1]: Started iperf3.service - Iperf3 Server.
[root@isp ens34]# _
```

3.4 Настройка протокола динамической конфигурации хостов

Установка DHCP:

- Установим пакет **dhcp-server**:

#apt-get install -y dhcp-server

Настройка DHCP-сервера:

- Укажем сетевой интерефейс, через который будет работать DHCP-сервер:

sed -i "s/DHCPDARGS=/DHCPDARGS=ens34 ens35 ens36/g" /etc/sysconfig/dhcpd

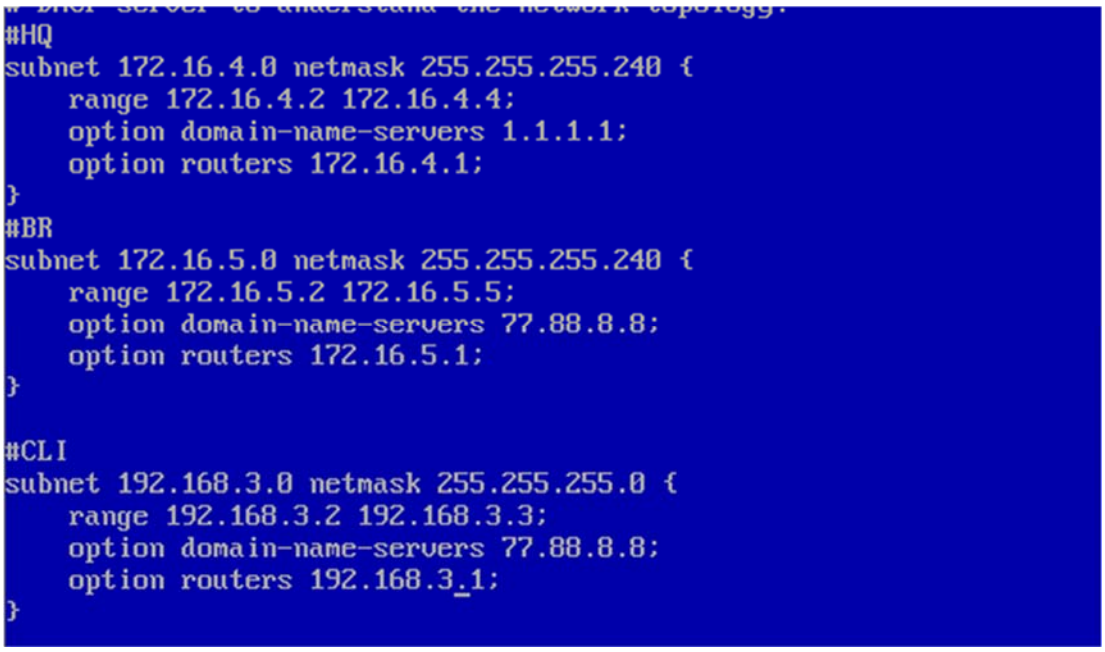
```
dhcpd             [----] 27 L:[  1+ 2   3/  5] *(70  / 169b) 0010 0x00A
# The following variables are recognized:

DHCPDARGS=ens34 ens35 ens36
# Default value if chroot mode disabled.
#CHROOT="-j / -lf /var/lib/dhcp/dhcpd/state/dhcpd.leases"
```

- Пример конфигурационного файла с настройкой DHCP - сервера - расположен по пути "**/etc/dhcp/dhcpd.conf.example**"

cp /etc/dhcp/dhcpd.conf{.example,}

- После чего, необходимо привести файл "**/etc/dhcp/dhcpd.conf**" к следующему виду:

vim /etc/dhcp/dhcpd.conf

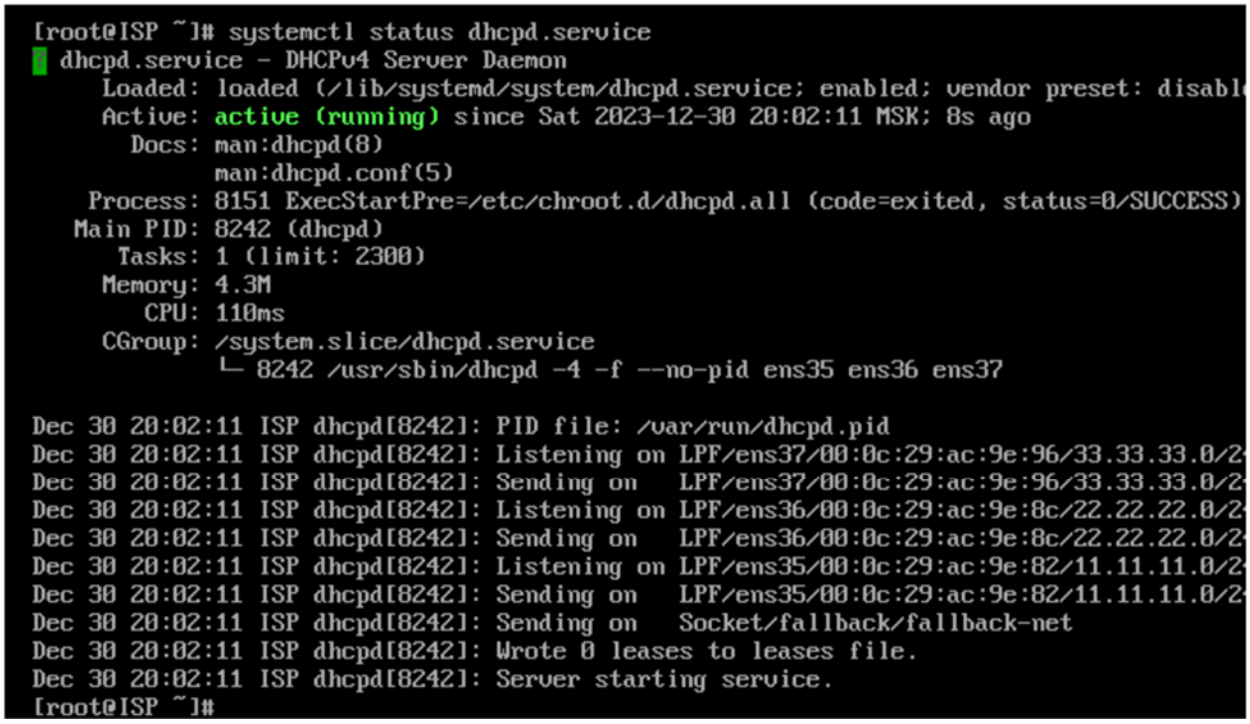


- если планируется далее развёртывать и DNS-сервер, то выдаём в качестве **option domain-name-servers** соответствующие адреса;
- в противном случае, можно расскомментировать строку "**option domain-name-servers 77.88.8.8 77.88.8.88;**"
- Включаем и добавляем в автозагрузку службу **dhcpd**:

#systemctl enable --now dhcpd

- Проверить работоспособность службы **dhcpd**:

#systemctl status dhcpd



4 Модуль 1: Выполнение работ по проектированию сетевой инфраструктуры

4.1 Базовая настройка всех устройств

Задание:

1. Выполните базовую настройку всех устройств:

- a. Присвоить имена в соответствии с топологией
- b. Рассчитайте IP-адресацию IPv4 и. Необходимо заполнить таблицу №1, чтобы эксперты могли проверить ваше рабочее место.
- c. Пул адресов для сети офиса BRANCH - не более 16
- d. Пул адресов для сети офиса HQ - не более 64

Выполнение:

a. Присвоить имена в соответствии с топологией

Таблица 4.1

Устройство	Запись	Тип

HQ-R	**hq-r.au-team.irpo**	**A,PTR**
BR-R	**br-r.au-team.irpo**	**A**
HQ-SRV	**hq-srv.au-team.irpo**	**A,PTR**
CLI	**cli. au-team.irpo**	**A,PTR**
BR-SRV	**br-srv.au-team.irpo**	**A**
HQ-R	**moodle.au-team.irpo**	**CNAME**
HQ-R	**wiki.au-team.irpo**	**CNAME**

#hostnamectl set-hostname <NAME>; exec bash

где:

- **<NAME>** - имя устройства
- **exec bash** — перезапуск оболочки bash для отображения нового хостнейма

Выполняем на всех хостах.

Пример:

#hostnamectl set-hostname isp.au-team.irpo; exec bash

Таблица 4.2

Название устройства	**NIC**	**Сеть (подсеть)**	**IP-адрес**	**Шлюз**
ISP	ISP <-> BR-R	172.16.5.0/28	172.16.5.1/28	-
	WLAN	DHCP		
	ISP <-> HQ-R	172.16.4.0/28	172.16.4.1/28	-

	ISP <-> CLI	172.16.3.0/24	172.16.3.1/24	-
BR-R	ISP <-> BR-R	172.16.5.0/28	172.16.5.2/28 (DHCP)	172.16.5.1
	BR-R <-> BR-SRV	192.168.2.0/28	192.168.2.1/28	-
	Tunnel (GRE)	10.10.10.0/30	10.10.10.1/30	-
BR-SRV	BR-SRV<-> BR-R	192.168.2.0/28	192.168.2.2/28	192.168.2.1/28
HQ-R	ISP <-> HQ-R	172.16.4.0/28	172.16.4.2/28 (DHCP)	172.16.4.1
	HQ-R <-> HQ -SRV	192.168.1.0/26	192.168.1.1/26	-
	HQ-R <-> CLI	192.168.4.0/24	192.168.4.2/24	-
	Tunnel (GRE)	10.10.10.0/30	10.10.10.2/30	-
CLI	CLI<-> ISP	192.168.3.0/24	192.168.3.2/24	192.168.3.1/24
	CLI<-> HQ-R	192.168.4.0/24	192.168.4.1/24	-
HQ-SRV	HQ-R	192.168.1.0/26	192.168.1.2/26	192.168.1.1
	HQ-SRV <-> CLI	192.168.4.0/24	192.168.4.3/24	-

Важно помнить о **недопустимых** диапазонах IPv4 и IPv6 адресов:

- **IPv4**

Таблица 4.3

Сеть	**Диапазон**	**Назначание**
0.0.0.0/8	0.0.0.0 - 0.255.255.255	спец. назначение
127.0.0.0/8	127.0.0.0 - 127.255.255.255	localhost (самотестирование)
169.254.0.0/16	169.254.0.0 - 169.254.255.255	APIPA (Automatic Private Internet Protocol Addressing)
192.88.99.0/24	192.88.99.0 - 192.88.99.255	Используются для рассылки ближайшему узлу
192.88.99.1/32		применяется в качестве ретранслятора при инкапсуляции IPv6 в IPv4
224.0.0.0 /2	224.0.0.0 - 255.255.255.255	multicast

Назначение IPv4 адресов:

В качестве системы конфигурации сети используется **etcnet**

- подробнее о **etcnet в Альт**

Для каждого сетевого интерфейса необходимо создать директорию по пути **/etc/net/ifaces/<NAME_INTERFACE>/options**:

- где - **<NAME_INTERFACE>** имя сетевого интерфейса

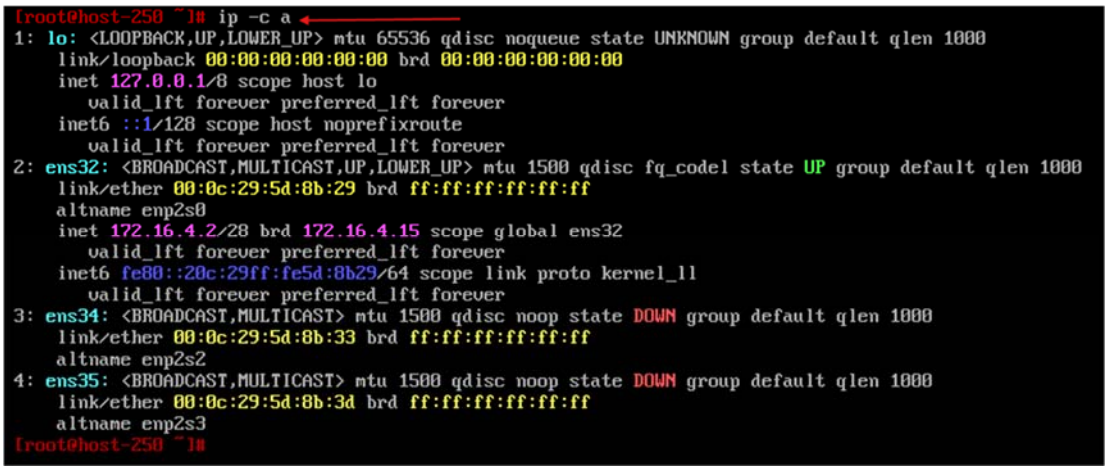
Подразумевается, что доступ к ISP не предусмотрен, а ISP является преднастроенной ВМ и организовавыет доступ в сеть Интернет

4.1.1 HQ-R:

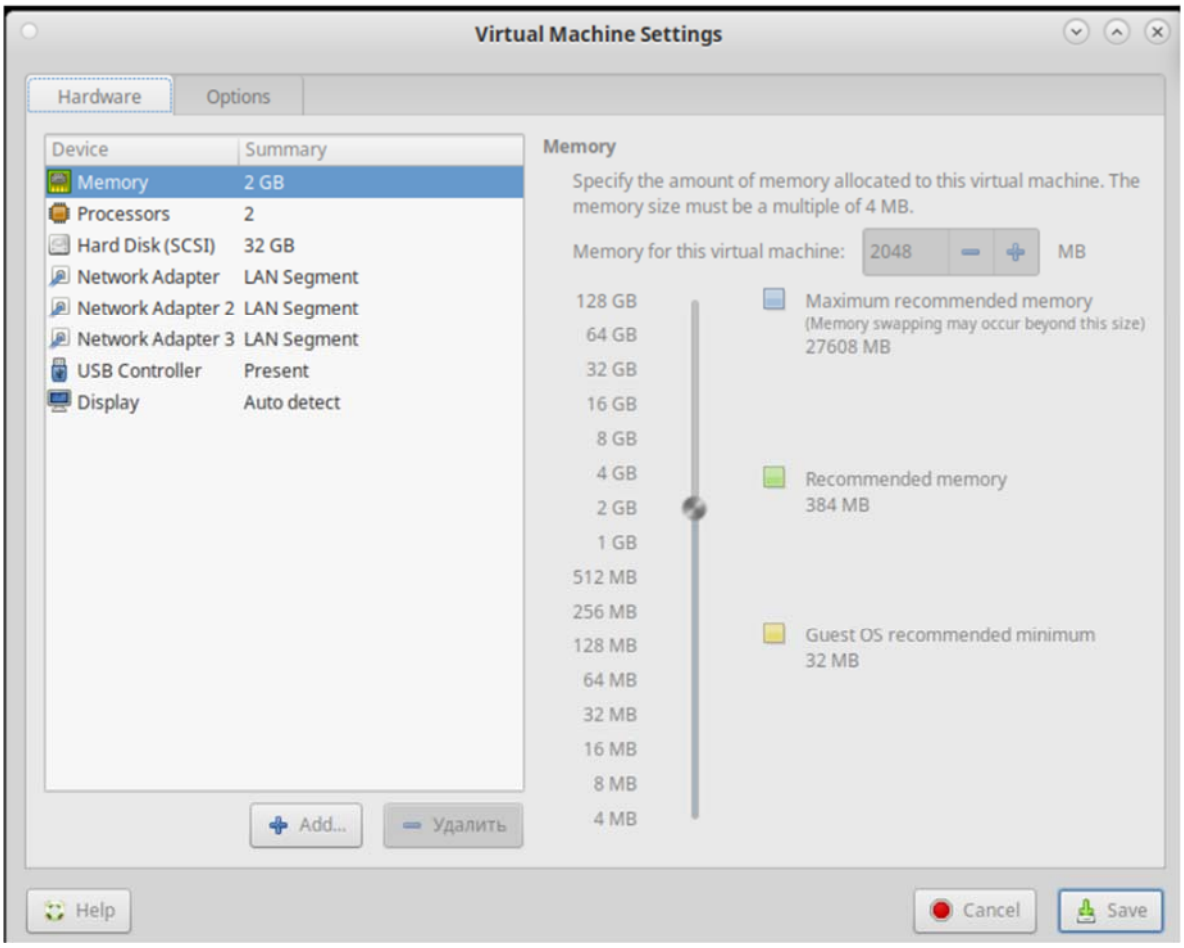
1. Определяемся какой интерфейс в какую сторону смотит:

- для этого выводим информацию о сетевых интерфейсах:

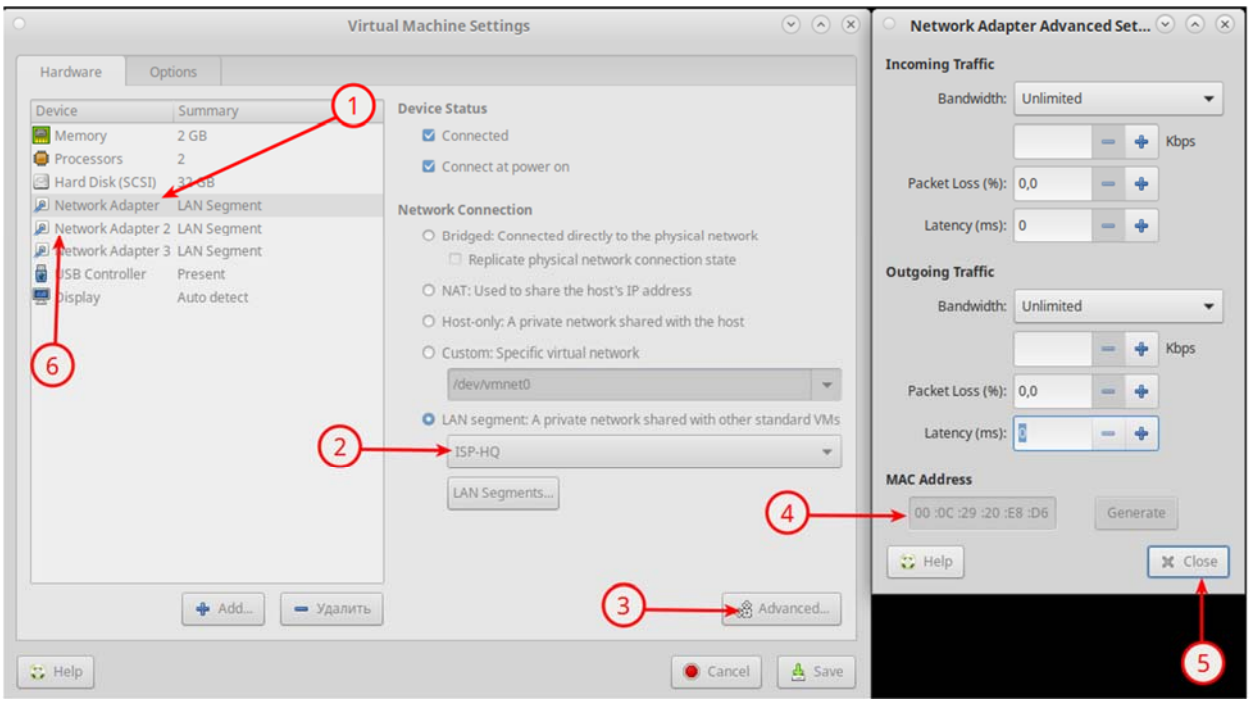
#ip -c a



- после чего открываем настройки виртуальной машины - нажимаем ПКМ на ВМ -> выбираем "Settings"



- 1 - выбираем "Network Adapter"
- 2 - смотрим название LAN Segment
- 3 - нажимаем "Advanced"
- 4 - смотрим на MAC - адрес сетевого интерфейса, запоминаем - фиксируем для себя
- 5 - нажимаем "Close"
- 6 - выполняем аналогичные действия (1-5) для другого сетевого интерфейса



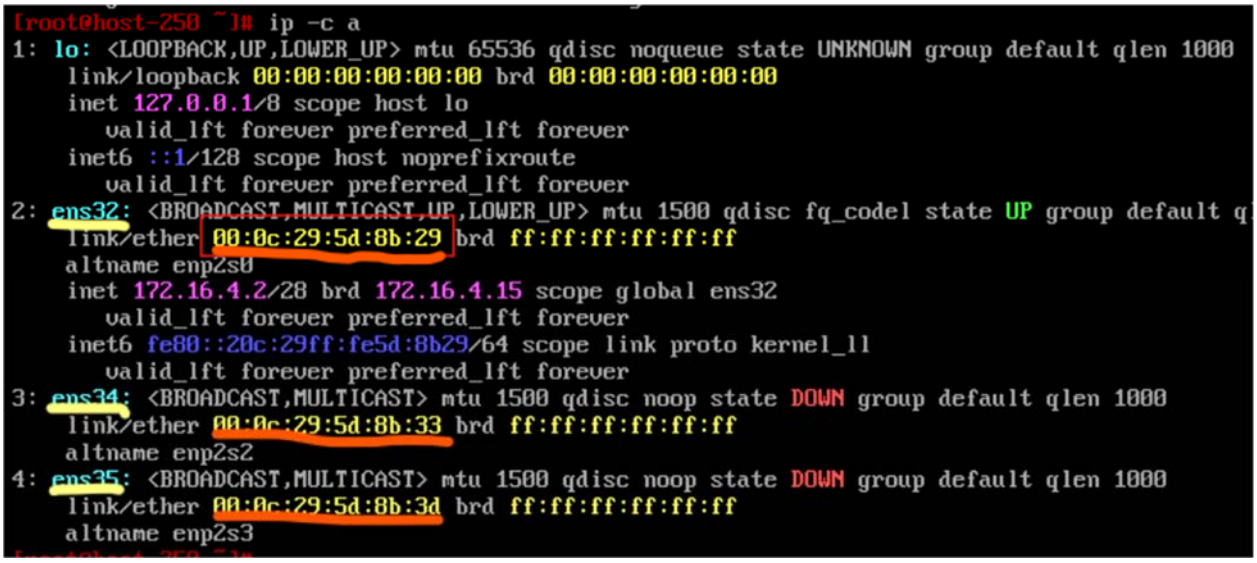
- Сравниваем зафиксированные MAC - адреса с полученные с настроек Виртуальной машины и с результатом вывода команды "**ip -c a**", где также присутствуют MAC - адреса

  где:

- красным - показаны MAC - адреса;
- жёлтым - имена интерфейсов

  Таким образом, получаем следующую информацию:

- **ens32** - интерфейс в сторону **ISP (DHCP)**;
- **ens34** - интерфейс в локальную сеть офиса **HQ (static)**;
- **ens35** - интерфейс для временного подключения **CLI** с офисом **HQ (static);**



Аналогичные действия необходимо выполнять для каждой ВМ!

- создаём для каждого интерфейса директорию по пути "**/etc/net/ifaces/**":

  mkdir /etc/net/ifaces/ens3{4,5}

  или

  mkdir /etc/net/ifaces/ens34

  mkdir /etc/net/ifaces/ens35

- Теперь необходимо описать файл **options** для каждого интерфейса в директории **/etc/net/ifaces/<NAME_INTERFACE>**
  - содержимое для DHCP:

  TYPE=eth

  DISABLED=no

  NM_CONTROLLED=no

BOOTPROTO=dhcp

CONFIG_IPV4=YES

- содержимое для Static:

TYPE=eth

DISABLED=no

NM_CONTROLLED=no

BOOTPROTO=static

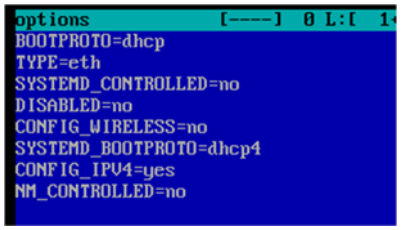
CONFIG_IPV4=YES

где:

- **TYPE** - Эта опция определяет тип интерфейса;
- **DISABLED** - Если установить значение "yes", то интерфейс будет игнорироваться;
- **NM_CONTROLLED** - В сочитание с **DISABLED=no** получается чистый Etcnet;
- **BOOTPROTO** - Может быть любым из следующих: static, dhcp, ipv4ll. * "static": использует ipv4address/ipv6address;

Описываем файл "**options**" для интерфейса **ens32** в сторону **ISP:**

#vim /etc/net/ifaces/ens32/options

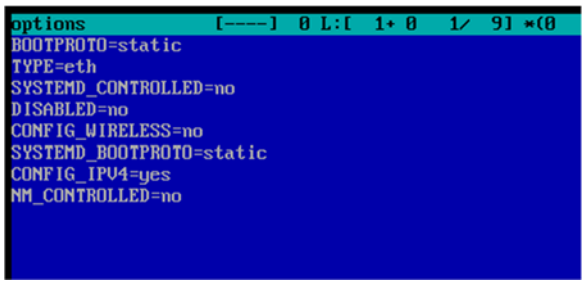


также можно получить параметры автоматически и зафиксировать их статически, или назначить статическими сразу (в соответствие с заданием);

Описываем файл "**options**" для интерфейсов **ens34** и **ens35**:

- т.к. файл одинаков в **данном случае** для двух интерфейсов, то описываем один и копируем его:

  #vim /etc/net/ifaces/ens34/options



- т.к. файл одинаков в **данном случае** для двух интерфейсов, то описываем один и копируем его:

- `cp /etc/net/ifaces/ens34/options /etc/net/ifaces/ens35/`

или можно простым bash-скриптом сразу записать все опции для всех сетевых интерфейсов:

```
for i in 4 5; do
  cat <<EOF > /etc/net/ifaces/ens3$i/options
  TYPE=eth
  DISABLED=no
  NM_CONTROLLED=no
  BOOTPROTO=static
  CONFIG_IPV4=YES
  CONFIG_IPV6=YES
  EOF
done
```

Назначаем IPv4 адреса согласно Таблице №4.2

- для **ens32** - в сторону **ISP,** сетевые параметры будут получены автоматически, т.к. на ISP преднастроен DHCP сервер

- для **ens34** - в сторону локальной сети офиса **HQ**

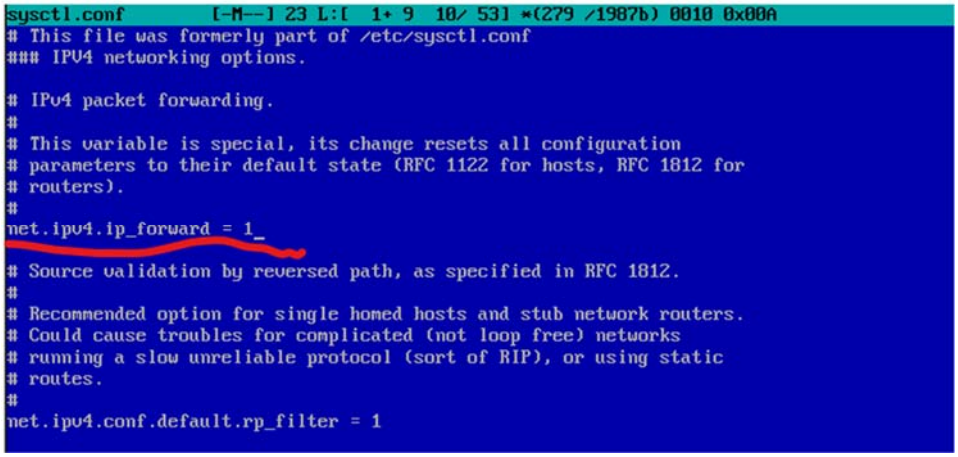
  echo 192.168.1.1/26 > /etc/net/ifaces/ens34/ipv4address

- для **ens35** - для временного подключения **CLI** с офисом **HQ**

  echo 192.168.4.2/24 > /etc/net/ifaces/ens35/ipv4address

`Также, поскольку HQ-R является маршрутизатором для офиса HQ - необходимо включить forwarding для IPv4 - пакетов:

#vim /etc/net/sysctl.conf



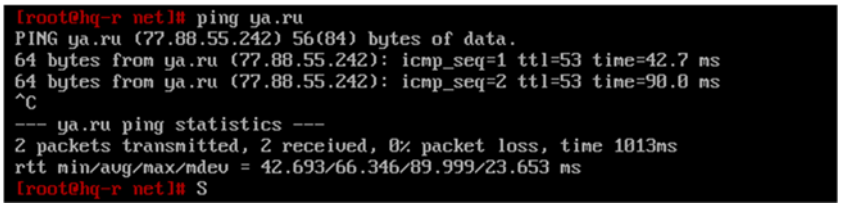
Для применения всех сетевых настроек перезагружаем службу "**network**"

systemctl restart network

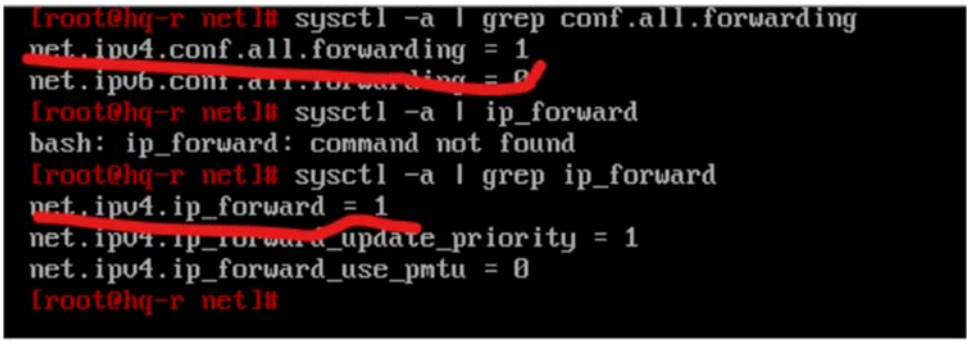
Проверяем (и меняем host)

- IPv4 - адресация

- Проверяем доступ в Интернет

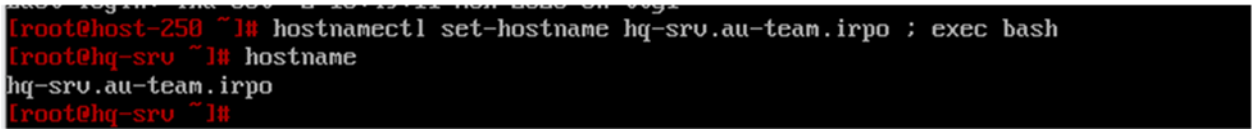


- forwarding



4.1.2 HQ-SRV

По заданию сетевые параметры должны быть получены **автоматически** после настройки DHCP-сервера на **HQ-R**



В качестве сетевой подсистемы будем использовать **NetworkManager**, т.к. у **etcnet** наблюдаются проблемы при одновременной работе **dhcp-клиента** для **IPv4** и **IPv6:**

Так как все ВМ в минимальной установке, то нет необходимых пакетов, а также и локального репозитория, поэтому назначаем средствами "**iproute2**" временный IPv4 адрес, шлюз по умолчанию и DNS, чтобы установить необходимые пакеты:

- назначаем IPv4-адрес:

  ip addr add 192.168.1.2/2 dev ens32

- назначаем адрес шлюза:

  ip route add 0.0.0.0/0 via 192.168.1.1

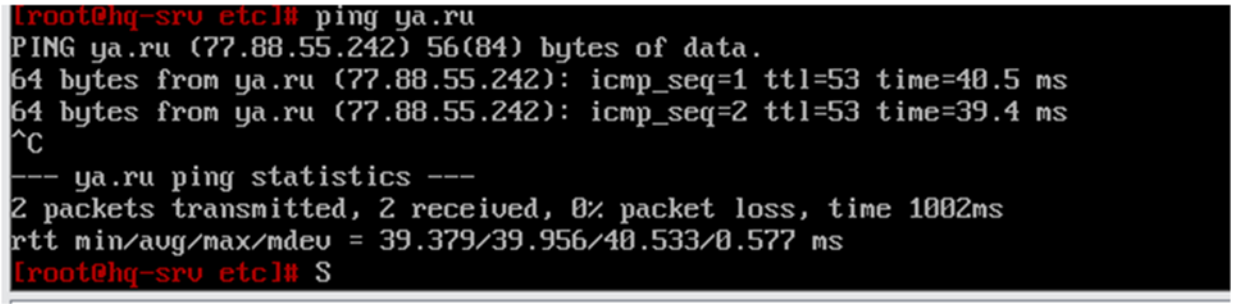
- назначаем DNS:

  echo ‘nameserver 77.88.8.8’ > /etc/resolv.conf

После чего, на **HR-R** - необходимо временно разрешить доступ в Интернет (т.к. потом будет выполнено на постоянной основе, посредством **iptables**):

HQ-R:

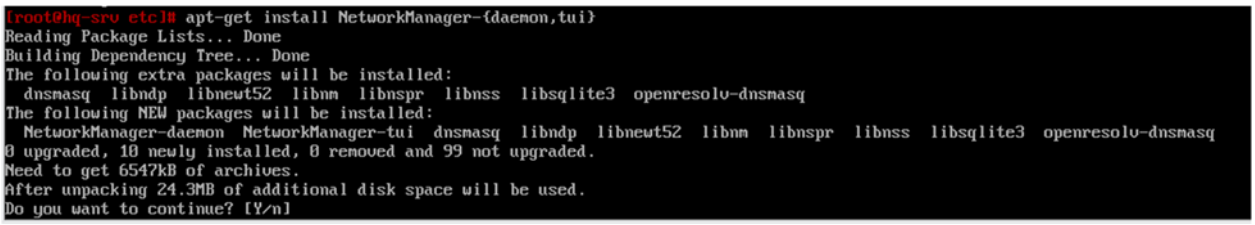
iptables -t nat -A POSTROUTING -s 192.168.1.0/26 -o ens32 -j MASQUERADE



Далее на **HQ-SRV** устанавливанием необходимые пакеты:

HQ-SRV:

apt-get update && apt-get install -y NetworkManager-{daemon,tui}



Настраиваем интерфейсы для работы с **NetworkManager**:

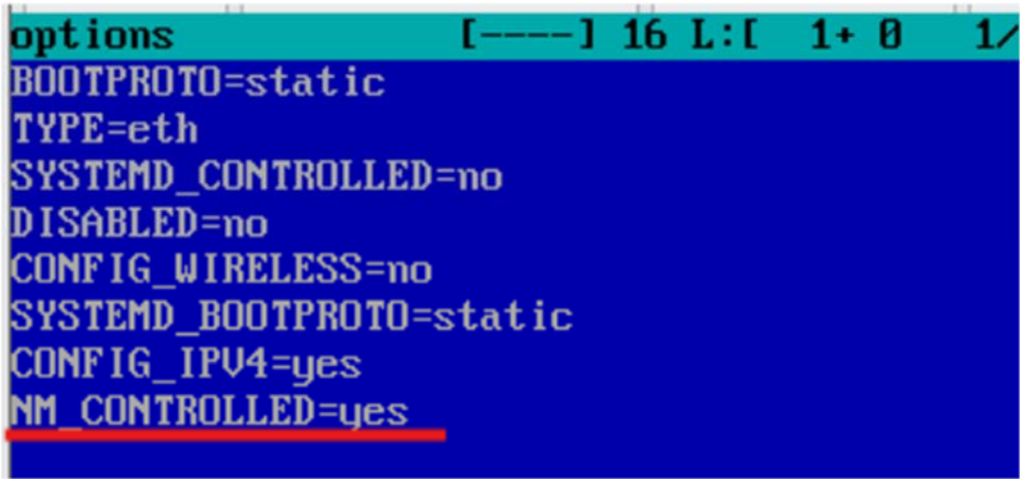
- **ens32** - интерфейс в локальную сеть офиса **HQ;**
- **ens34** - интерфейс для временного подключения **CLI** с офисом **HQ**

Запускаем и добавляем в автозагрузку службу "**NetworkManager**":

systemctl enable --now NetworkManager

Для того, чтобы интерфейсы стали видимы в **nmtui** или **nmcli** - необходимо поправить параметр в файле **/etc/net/ifaces/<ИМЯ_ИНТЕРФЕЙСА/options**

sed -i "s/NM_CONTROLLED=no/NM_CONTROLLED=yes/g" /etc/net/ifaces/ens32/options



Перезапускаем службы "**network**" и "**NetworkManager**":

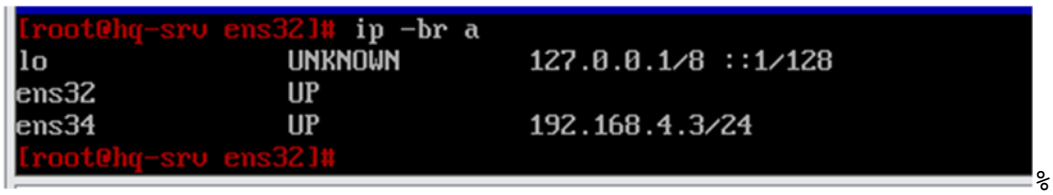
#systemctl restart network

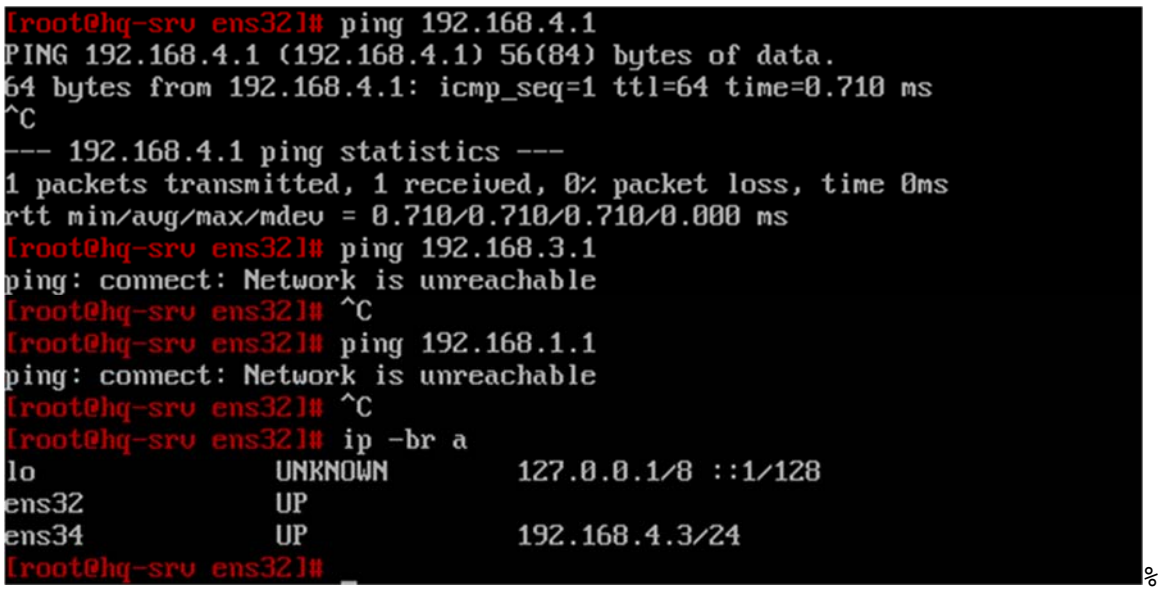
#systemctl restart NetworkManager

Переходим в **nmtui**:

#nmtui

Проверяем:




[root@hq-srv ens32]# ping 192.168.4.1
PING 192.168.4.1 (192.168.4.1) 56(84) bytes of data.
64 bytes from 192.168.4.1: icmp_seq=1 ttl=64 time=0.710 ms
^C
--- 192.168.4.1 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.710/0.710/0.710/0.000 ms
[root@hq-srv ens32]# ping 192.168.3.1
ping: connect: Network is unreachable
[root@hq-srv ens32]# ^C
[root@hq-srv ens32]# ping 192.168.1.1
ping: connect: Network is unreachable
[root@hq-srv ens32]# ^C
[root@hq-srv ens32]# ip -br a
lo UNKNOWN 127.0.0.1/8 ::1/128
ens32 UP
ens34 UP 192.168.4.3/24
[root@hq-srv ens32]#
%

%

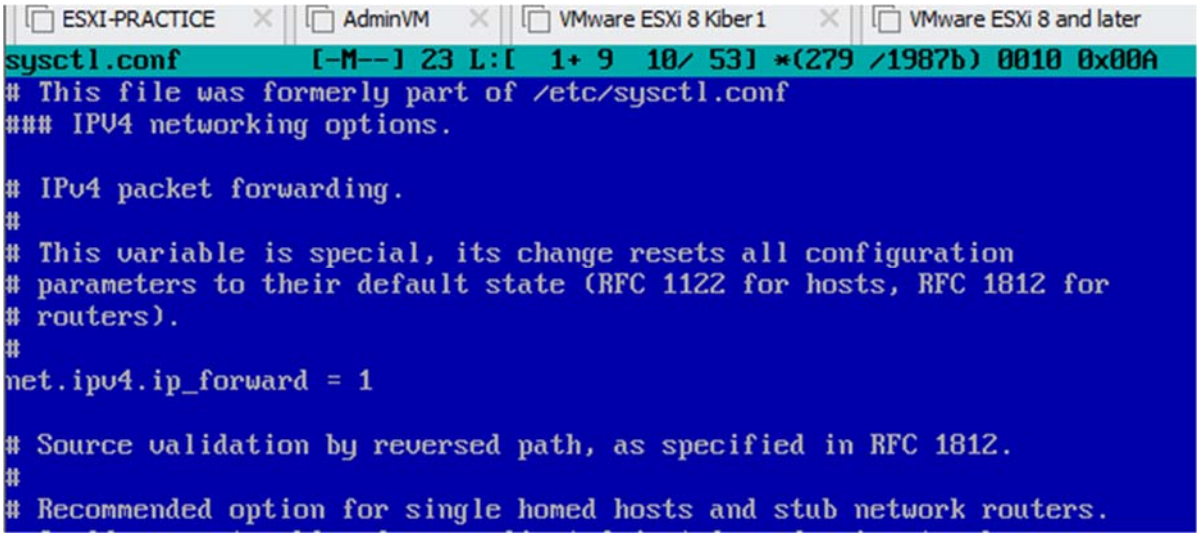
4.1.3 BR-R

```
[root@host-250 ~]# hostnamectl set-hostname br-r.au-team.irpo ;exec bash
[root@br-r ~]#
```

Настройка аналогична HQ-R, за исключением:

ens32 - в сторону ISP для доступа в сеть Интернет (DHCP;

ens34 - в сторону локальной сети офиса BR static



Результат:

IPv4 адресация доступ в Интернет

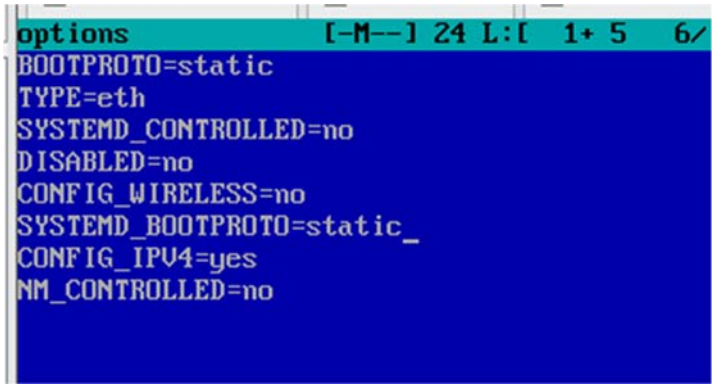
```
[root@br-r net]# systemctl restart network
[root@br-r net]# ip -c -br a
lo               UNKNOWN        127.0.0.1/8 ::1/128
ens32            UP             172.16.5.2/28 fe80::20c:29ff:fefe:1881/64
ens34            UP             192.168.2.1/28 fe80::20c:29ff:fefe:188b/64
[root@br-r net]# ip -c -br r
default via 172.16.5.1 dev ens32 proto dhcp src 172.16.5.2 metric 1002
172.16.5.0/28 dev ens32 proto dhcp scope link src 172.16.5.2 metric 1002
192.168.2.0/28 dev ens34 proto kernel scope link src 192.168.2.1
[root@br-r net]# ping ya.ru
PING ya.ru (5.255.255.242) 56(84) bytes of data.
64 bytes from ya.ru (5.255.255.242): icmp_seq=1 ttl=246 time=28.1 ms
64 bytes from ya.ru (5.255.255.242): icmp_seq=2 ttl=246 time=29.8 ms
^C
--- ya.ru ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 28.064/28.912/29.760/0.848 ms
[root@br-r net]#
```

forwarding

```
[root@br-r ~]# sysctl -a | grep conf.all.forwarding
net.ipv4.conf.all.forwarding = 1
net.ipv6.conf.all.forwarding = 1
[root@br-r ~]# sysctl -a | grep ip_forward
net.ipv4.ip_forward = 1
```

4.1.4 BR-SRV

```
root@host-250 ~]# hostnamectl set-hostname br-srv.au-team.irpo ; exec bash
root@br-srv ~]#
```



Задаём IPv4 адрес на интерфейс **ens32** согласно Таблице №4.2

echo ‘192.168.2.2/28’ > /etc/net/ifaces/ens32/ipv4address

Задаём адрес шлюза по умолчанию для IPv4 :

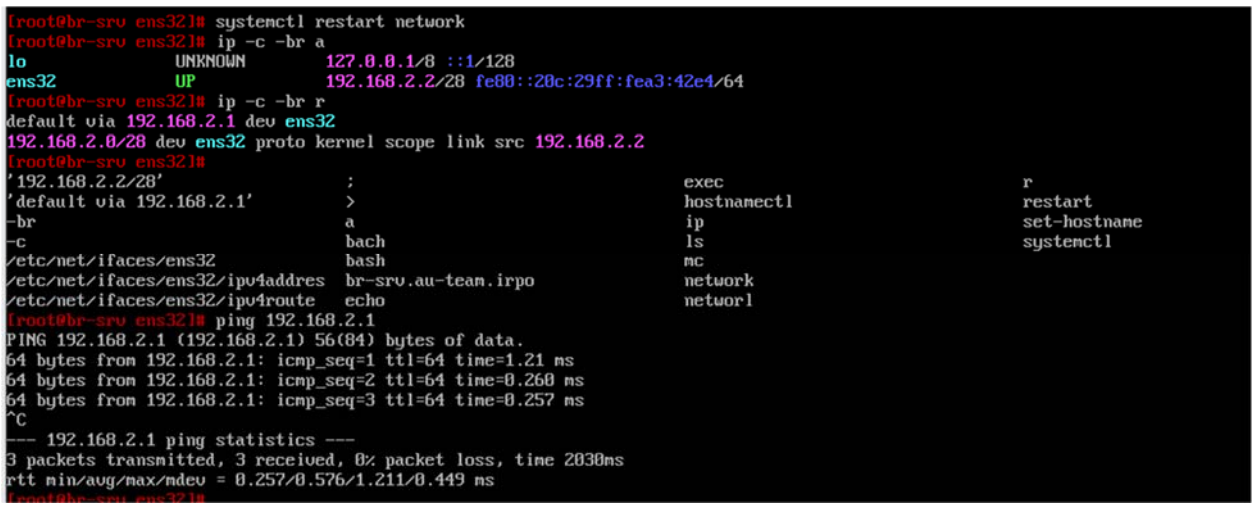
echo ‘default via 192.168.2.1’ > /etc/net/ifaces/ens33/ipv4route

перезапускаем службу "**network**"

systemctl restart network

Проверяем:

IPv4 адресация:



4.1.5 CLI

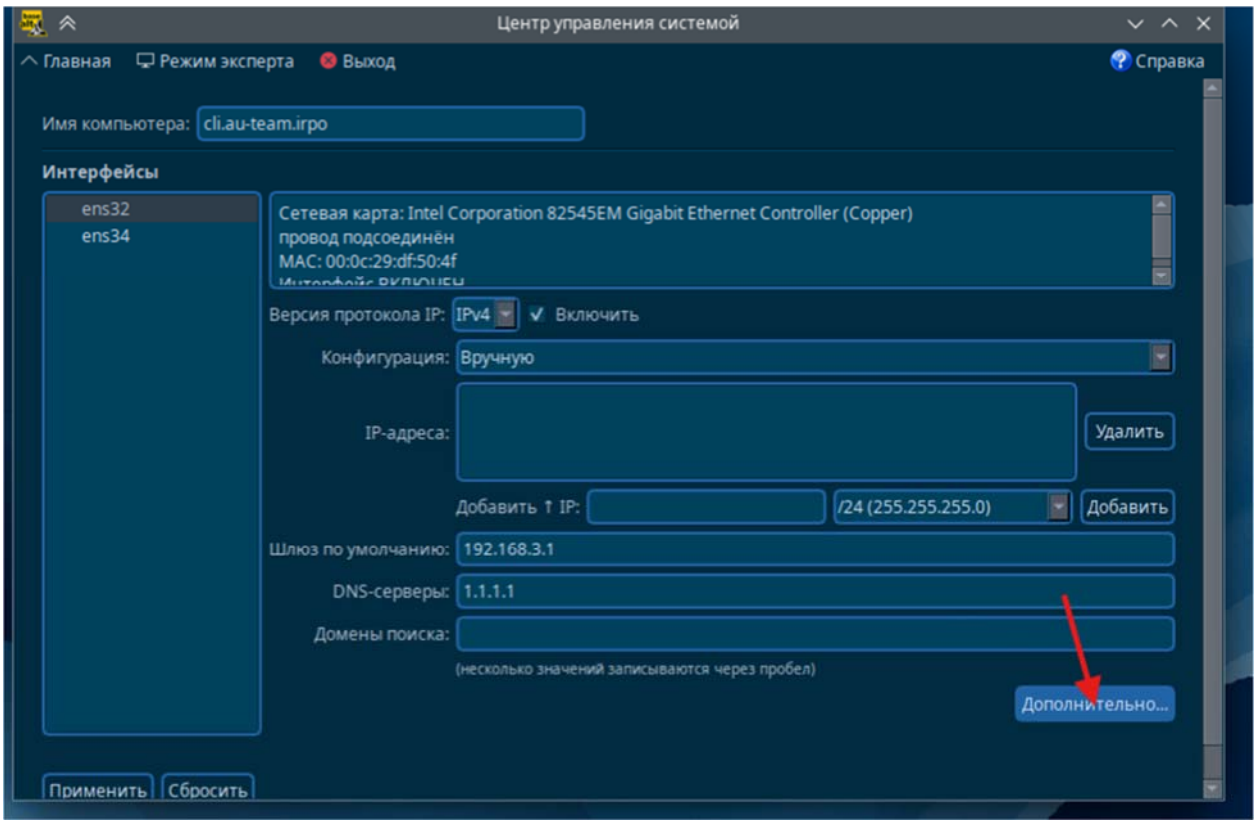
Либо статически, либо автоматически в зависимости от задания:

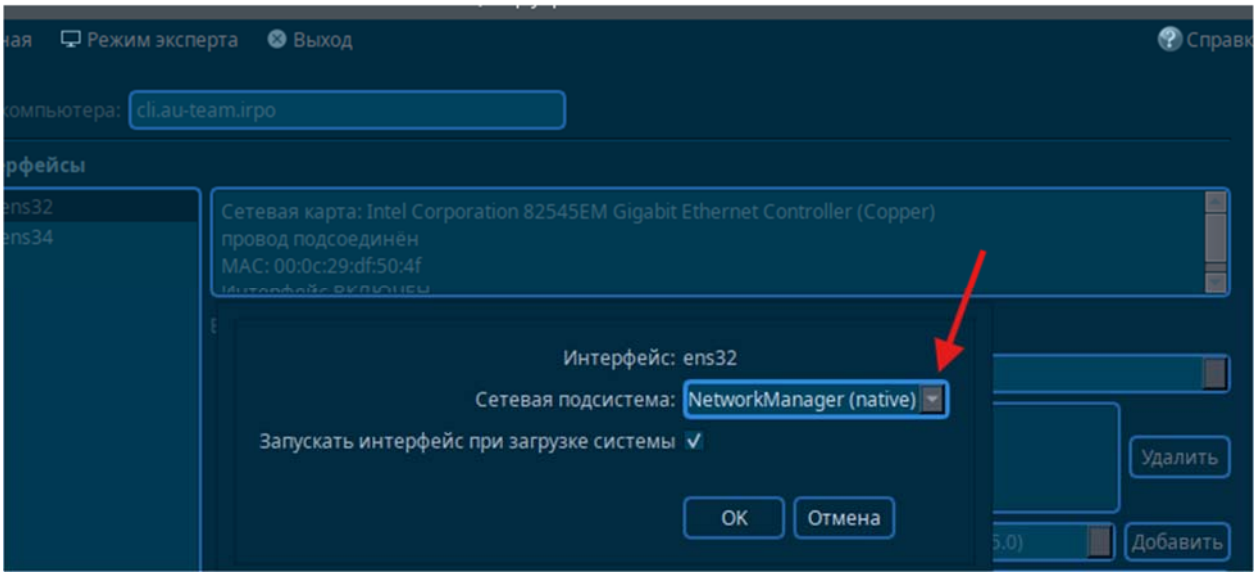
В текущих настольных дистрибутивах ОС Альт в качестве штатного средства управления сетевыми интерфейсами по умолчанию применяется NetworkManager; при этом обеспечено его взаимодействие с etcnet, а средствами alterator-net-eth при необходимости возможно выбрать, какой именно интерфейс какой подсистемой обслуживается.

Для настройки сети в MATE/Cinnamon/Xfce используется апплет NetworkManager. Он отображается в трее.

Также в alterator необходимо указать, что в качестве сетевой подсистемы будет использываться именно он:

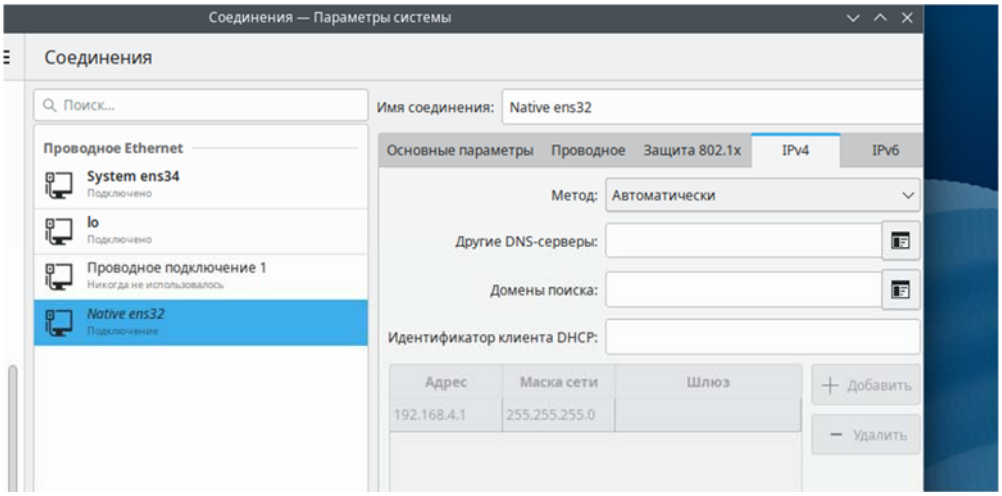
Открываем "Пуск" -> открываем "Центр управления"

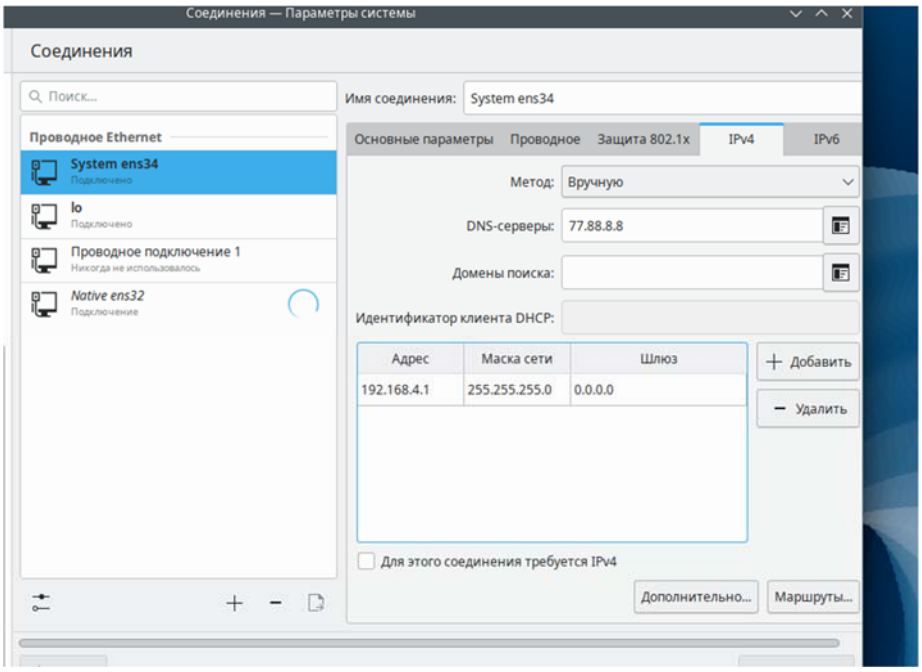




далее настройки выполняются, через иконку в трее:

ПКМ нажимаем на иконку в трее -> выбираем "Параметры соединений"






```
root@cli ens32]# systemctl restart network
root@cli ens32]# ip -br a
o               UNKNOWN        127.0.0.1/8 ::1/128
ns32            UP             192.168.3.2/24 fe80::d559:6cf6:b650:82f9/64
ns34            UP             192.168.4.1/24 fe80::20c:29ff:fedf:5059/64
root@cli ens32]#
```

```
ens34            UP             192.168.4.1/24 fe80::20c:29ff:fedf:5059/64
[root@cli ens32]# ping ya.ru
PING ya.ru (77.88.44.242) 56(84) bytes of data.
64 bytes from ya.ru (77.88.44.242): icmp_seq=1 ttl=55 time=40.8 ms
64 bytes from ya.ru (77.88.44.242): icmp_seq=2 ttl=55 time=42.4 ms
64 bytes from ya.ru (77.88.44.242): icmp_seq=3 ttl=55 time=45.1 ms

--- ya.ru ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 40.754/42.771/45.149/1.812 ms
^C[root@cli ens32]#
```

4.2 Настройка внутренней динамической маршрутизации по средствам FRR

4.2.1 Задание:

2. Настройте внутреннюю динамическую маршрутизацию по средствам FRR. Выберите и обоснуйте выбор протокола динамической маршрутизации из расчёта, что в дальнейшем сеть будет масштабироваться.

- a. Составьте топологию сети L3

4.2.2 Выполнение:

Поскольку маршрутизация внешних сетей по заданию не описана, то на HQ-R и на BR-R достаточно настроить статическую маршрутизацию, а именно на стадии настройки IP-адресации в качестве шлюза были заданы соответствующие адреса маршрутизатора провайдера ISP

А вот маршрутизация внутренних сетей (динамическая) нужно связать HQ-R и BR-R туннелем, чтобы обмен внутренними сетями происходил строго между маршрутизаторами подразделений **HQ** и **BRANCH** а **ISP** не имел к ним прямого доступа.

- на данном этапе достаточно реализовать простой туннель **GRE**, т.к. в базовом уровне нет явного требования о реализации защищённого тунеля, а значит и нет за это баллов

- а в **Модуле 3** -> пункте задания **№ 7**, где требуется реализовать защищённый тунель, просто выполнить шифрование **GRE** туннеля по средством **IPSec** (strongswan)

4.2.3 Поднимаем GRE-туннель между HQ-R и BR-R

HQ-R:

Forwarding IPv4 и **IPv6** был включён в базовой настройке.

Напоминаю что тут используется "etcnet"

- подробнее о туннелях в etcnet

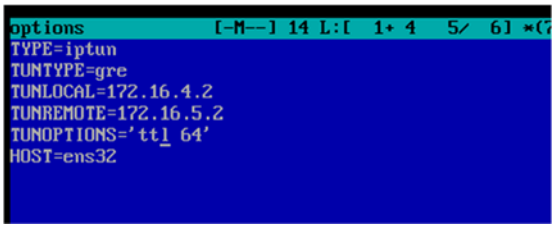
Необходимо создать директорию для туннельного интерфейса:

- Стоит помнить, что имена tunl0, gre0 и sit0 являются зарезервированными в iproute2 ("base devices") и имеют особое поведение:

#mkdir /etc/net/ifaces/tun1

- затем описываем файл **options**

  #vim /etc/net/ifaces/tun1/options



  где:

  - **TUNLOCAL** - IP-адрес ens32 на HQ-R
  - **TUNREMOTE** - IP-адрес ens32 на BR-R

  назначаем IPv4 адрес на туннельный интерфейс:

  echo '10.10.10.1/30' > /etc/net/ifaces/tun1/ipv4address

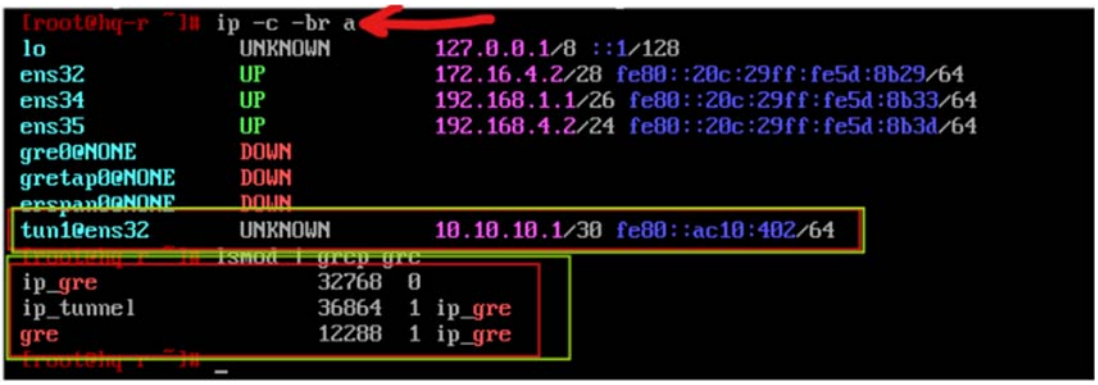
  Перезапускаем службу "**network**":

  #systemctl restart network

  Включаем модуль ядра для **gre**:

  #modprobe gre

  Проверяем:

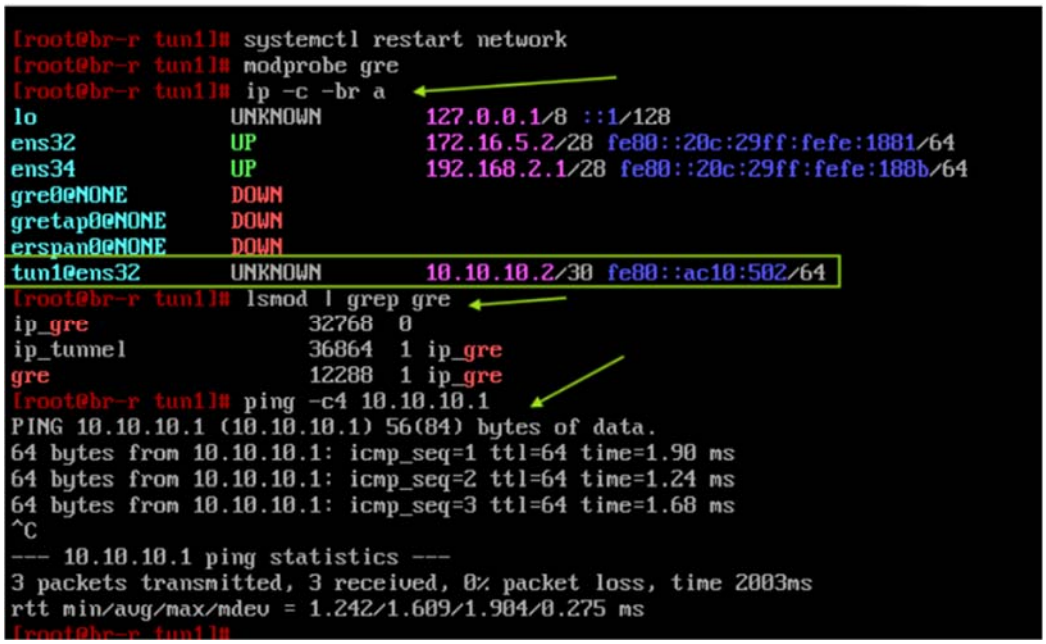


  #lsmod | grep gre

  BR-R:

  Настройки аналогичны **HR-R** за исключением:

- параметров **TUNLOCAL** и **TUNREMOTE** в файле **options**;
- а также **IPv4** адресов назначаемых на **tun1**



4.2.4 Настройка динамической (внутренней) маршрутизации средствами frr

FRRouting (FRR) — это бесплатный набор протоколов интернет-маршрутизации с открытым исходным кодом для платформ Linux и Unix. Он реализует протоколы BGP, OSPF, RIP, IS-IS, PIM, LDP, BFD, Babel, PBR, OpenFabric и VRRP, а также альфа-версию протоколов EIGRP и NHRP.

Благодаря полной интеграции FRR с собственными сетевыми стеками IP для Linux/Unix он представляет собой универсальный стек маршрутизации, применимый в самых разных случаях, включая подключение хостов/виртуальных машин/контейнеров к сети, рекламу сетевых сервисов, коммутацию и маршрутизацию в локальной сети, маршрутизацию доступа в Интернет и пиринг в Интернете.

FRR уходит корнями в проект Quagga. На самом деле он был создан многими разработчиками Quagga, которые объединили свои усилия, чтобы усовершенствовать хорошо зарекомендовавшую себя основу Quagga и создать лучший из доступных стеков протоколов маршрутизации. Мы приглашаем вас присоединиться к сообществу FRRouting и помочь сформировать будущее сетевых технологий.

4.2.4.1 HQ-R

Установим пакет frr:

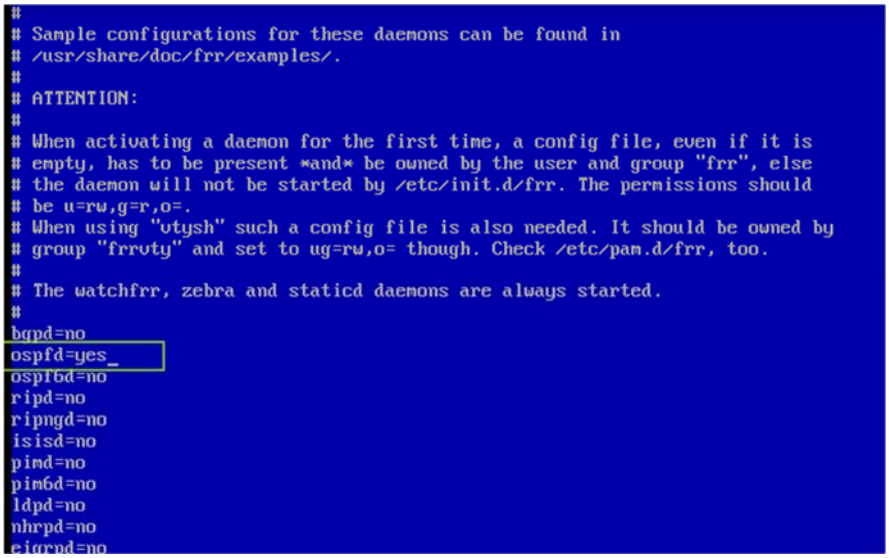
#apt-get update && apt-get install -y frr

- для настройки внутренней динамической маршрутизации для IPv4 и IPv6 будет использован протокол OSPFv2 и OSPFv3

В конфигурационном файле "**/etc/frr/daemons**" необходимо активировать выбранный протокол для дальнейшей реализации его настройки:

#vim /etc/frr/daemons

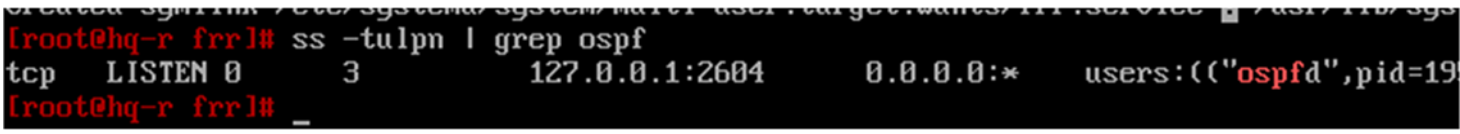
- переводим **ospfd=no** в **ospfd=yes** - для OSPFv2 (IPv4)



Включаем и добавляем в автозагрузку службу **frr**:

#systemctl enable --now frr

Проверяем:



Настраиваем **OSPFv2** - переходим в интерфейс **frr** при помощи "**vtysh**":

```
[root@hq-r frr]# vtysh

Hello, this is FRRouting (version 10.2.2).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

hq-r.au-team.irpo# conf t
hq-r.au-team.irpo(config)# router ospf
hq-r.au-team.irpo(config-router)# passive-interface default
hq-r.au-team.irpo(config-router)# network 192.168.1.0/26 area 0
hq-r.au-team.irpo(config-router)# network 10.10.10.0/30 area 0
hq-r.au-team.irpo(config-router)# exit
hq-r.au-team.irpo(config)# interface tun1
hq-r.au-team.irpo(config-if)# no ip ospf network broadcast
hq-r.au-team.irpo(config-if)# no ip ospf passive
hq-r.au-team.irpo(config-if)# do write memory
Note: this version of vtysh never writes vtysh.conf
Building Configuration...
Integrated configuration saved to /etc/frr/frr.conf
[OK]
hq-r.au-team.irpo(config-if)# _
```

Также если у вас есть gre туннель тут вы можете настроить его парольную защиту, в моем примере он есть, так что вот настройка:

int tun1

ip ospf authentication message-digest

ip ospf message-digest-key 1 md5 P@ssw0rd

do wr mem

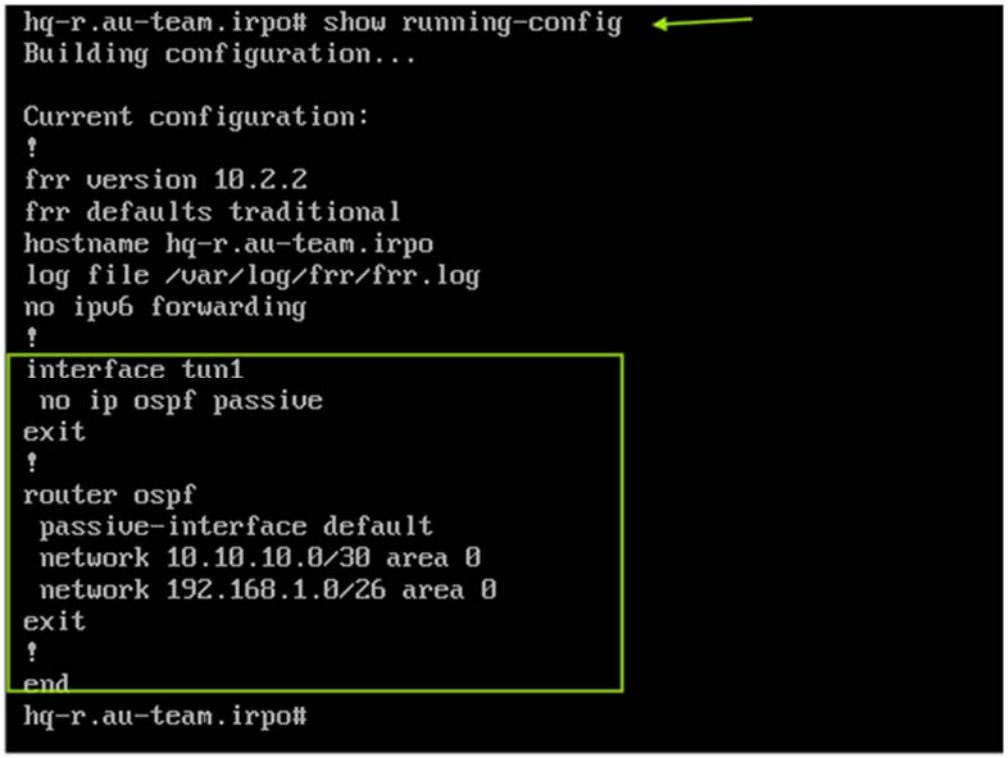
где:

- **configure terminal** - переход в режим глобальной конфигурации
- **router ospf** - переход в режим конфигурации OSPFv2
- **passive-interface default** - перевод всех интерфейсов в пассивный режим:
- далее туннельный интерфейс "tun1" будет сделать активным, для того чтобы устанавливать соседство с BR-R и обмениваться внутренними маршрутами
- **network** - объявляем локальную сеть офиса HQ и туннельную сеть

после чего переводим интерфейс tun1 в активный режим

сохраняем текущую конфигурацию

Проверяем:



4.2.4.2 BR-R:

Настройки аналогичны HR-R за исключением:

объявляемых сетей в OSPFv2;

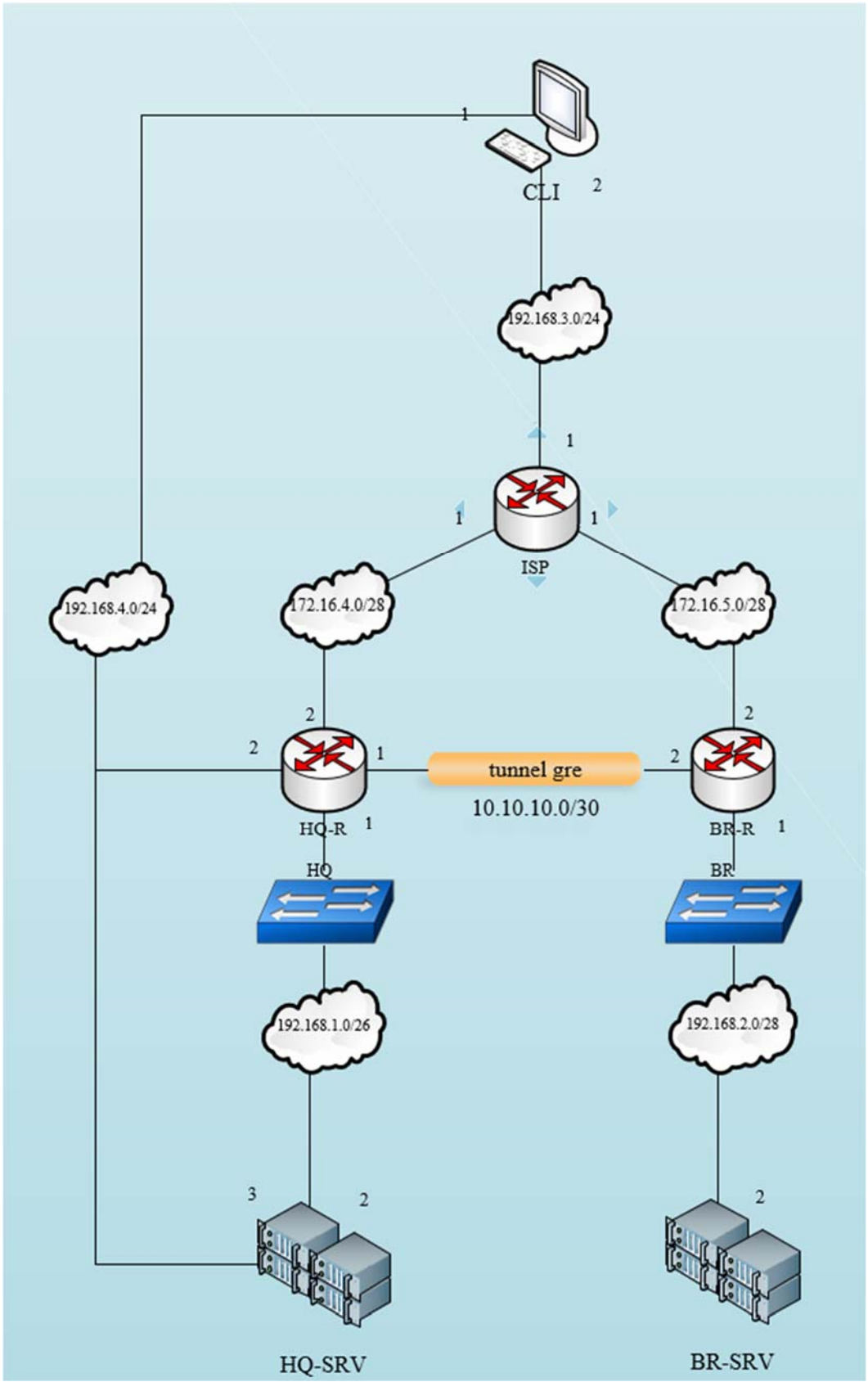
```
br-r.au-team.irpo# show running-config
Building configuration...

Current configuration:
!
frr version 10.2.2
frr defaults traditional
hostname br-r.au-team.irpo
log file /var/log/frr/frr.log
no ipv6 forwarding
!
interface tun1
 no ip ospf passive
exit
!
router ospf
 passive-interface default
 network 10.10.10.0/30 area 0
 network 192.168.2.0/28 area 0
exit
!
end
```

Проверяем:

OSPFv2:

HQ-R

```
hq-r.au-team.irpo# show ip ospf neighbor

Neighbor ID     Pri State           Up Time         Dead Time Address         Interface
192.168.2.1       1 Full/-          2m14s             35.004s 10.10.10.2      tun1:10.10.10.1

hq-r.au-team.irpo# show ip ro
ro         route      router-id
hq-r.au-team.irpo# show ip route ospf
Codes: K - kernel route, C - connected, L - local, S - static,
       R - RIP, O - OSPF, I - IS-IS, B - BGP, E - EIGRP, N - NHRP,
       T - Table, v - VNC, V - VNC-Direct, A - Babel, F - PBR,
       f - OpenFabric, t - Table-Direct,
       > - selected route, * - FIB route, q - queued, r - rejected, b - backup
       t - trapped, o - offload failure

O   10.10.10.0/30 [110/10] is directly connected, tun1, weight 1, 00:15:43
O   192.168.1.0/26 [110/100] is directly connected, ens34, weight 1, 00:16:12
O>* 192.168.2.0/28 [110/110] via 10.10.10.2, tun1, weight 1, 00:02:42
hq-r.au-team.irpo# _
```



Топология L3

4.3 Настройка автоматического распределения IP-адресов на роутере HQ-R

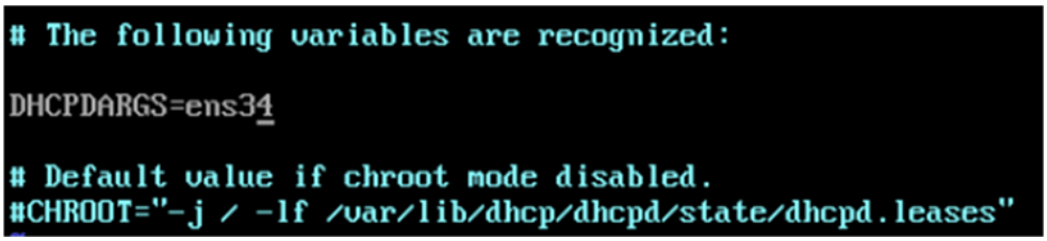
Установим пакет "dhcp-server":

apt-get update && apt-get install -y dhcp-server

Укажим сетевой интерефейс, через который будет работать DHCP-сервер:

/etc/sysconfig/dhcpd - для dhcpd.service

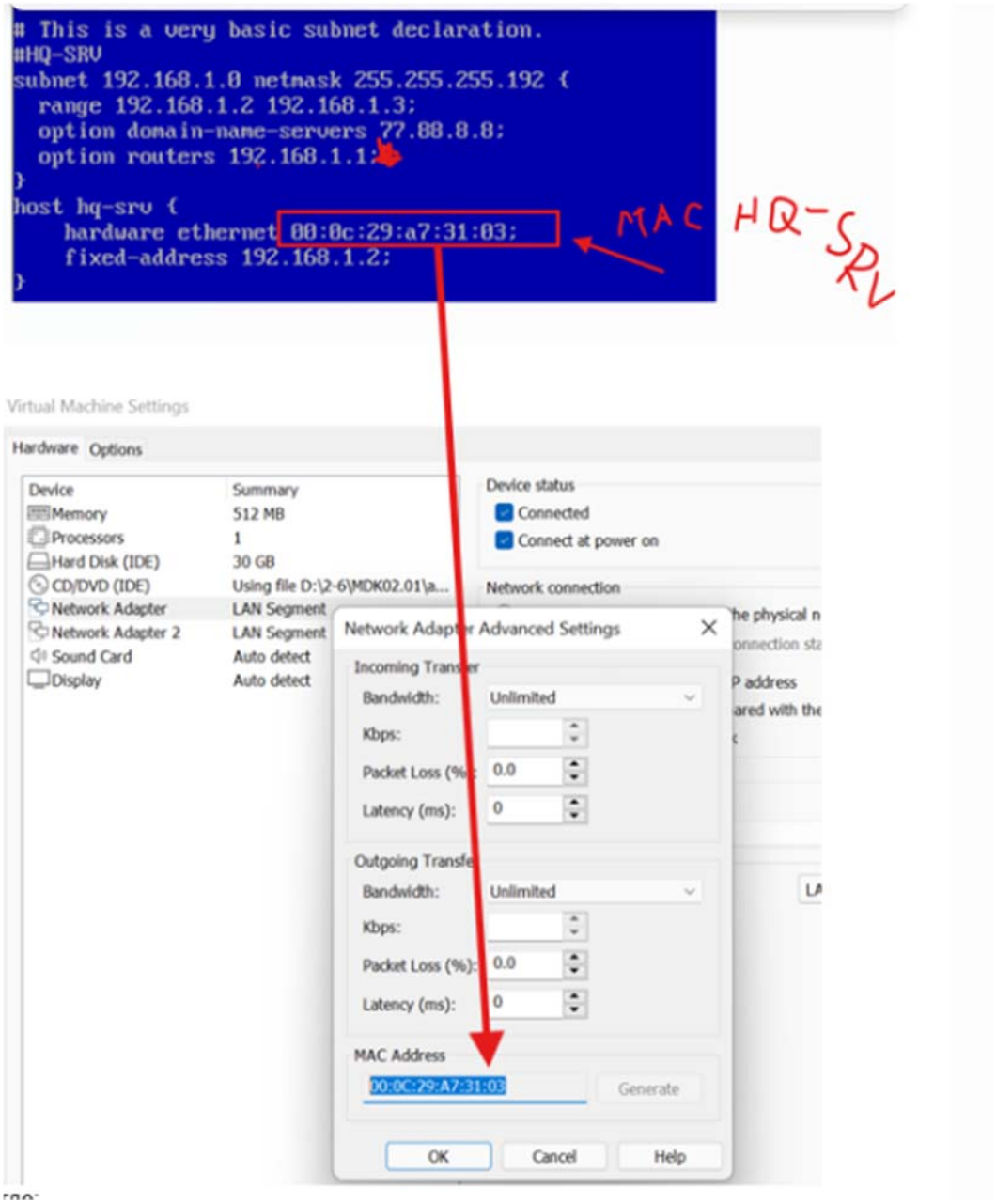
где: ens34 - интерфейс смотрящий в локальную сеть офиса HQ



cp /etc/dhcp/dhcpd.conf{.example,}

vim /etc/dhcp/dhcpd.conf

после удаления лишних строк из файла с шаблоном - конфигурационный файл выглядит следующим образом:



где:

default и max - leases-time - стандартное и максимальное время аренды (в секундах)

authoritative - только этот сервер можем выдавать IP адреса

блок subnet {} - сеть, маска сети и диапазон выдаваемых IP

блок host {} - чтобы выдать IP-адрес, исходя из MAC-адреса сетевого интерфейса для того, чей MAC-адрес описан в секции "hardware ethernet"

в данном случае MAC-адрес сетевого интерфейса ens33 на HQ-SRV, т.к. у сервера по заданию должен быть зарезервирован адрес

После чего пожно проверить данный конфигурационный файл через утилиту "dhcpd"

dhcpd -t -cf /etc/dhcp/dhcpd.conf

в случае ошибки в описании конфигурационного файла - в выводе данной утилиты будет написано что не так

Запускаем и добавляем в автозагрузку службу dhcpd (для IPv4):

#systemctl enable --now dhcpd

Проверяем:

Проверим статус службы dhcpd:

#systemctl status dhcpd

```
root@hq-r dhcp]# systemctl restart dhcpd
root@hq-r dhcp]# systemctl status dhcpd
● dhcpd.service - DHCPv4 Server Daemon
     Loaded: loaded (/usr/lib/systemd/system/dhcpd.service; enabled; preset: disabled)
     Active: active (running) since Sat 2025-10-11 17:05:22 MSK; 1s ago
       Docs: man:dhcpd(8)
             man:dhcpd.conf(5)
    Process: 2372 ExecStartPre=/etc/chroot.d/dhcpd.all (code=exited, status=0/SUCCESS)
   Main PID: 2462 (dhcpd)
      Tasks: 1 (limit: 534)
     Memory: 5.0M (peak: 5.3M)
        CPU: 43ms
     CGroup: /system.slice/dhcpd.service
             └─2462 /usr/sbin/dhcpd -4 -f --no-pid ens34

Oct 11 17:05:22 hq-r.au-team.irpo dhcpd[2462]: All rights reserved.
Oct 11 17:05:22 hq-r.au-team.irpo dhcpd[2462]: For info, please visit https://www.isc.org/software/dhcp/
Oct 11 17:05:22 hq-r.au-team.irpo dhcpd[2462]: Listening on LPF/ens34/00:0c:29:5d:8b:33/192.168.1.0/26
Oct 11 17:05:22 hq-r.au-team.irpo dhcpd[2462]: Sending on   LPF/ens34/00:0c:29:5d:8b:33/192.168.1.0/26
Oct 11 17:05:22 hq-r.au-team.irpo dhcpd[2462]: Sending on   Socket/fallback/fallback-net
Oct 11 17:05:22 hq-r.au-team.irpo dhcpd[2462]: Wrote 0 class decls to leases file.
Oct 11 17:05:22 hq-r.au-team.irpo dhcpd[2462]: Wrote 0 deleted host decls to leases file.
Oct 11 17:05:22 hq-r.au-team.irpo dhcpd[2462]: Wrote 0 new dynamic host decls to leases file.
Oct 11 17:05:22 hq-r.au-team.irpo dhcpd[2462]: Wrote 0 leases to leases file.
Oct 11 17:05:22 hq-r.au-team.irpo dhcpd[2462]: Server starting service.
root@hq-r dhcp]#
```

Проверка HQ-SRV

```
[root@hq-srv ~]# systemctl restart network
[root@hq-srv ~]# ip -c -br a
lo               UNKNOWN        127.0.0.1/8 ::1/128
ens32            UP             192.168.1.2/26
ens34            UP             192.168.4.3/24
[root@hq-srv ~]#
```

4.4 Настраиваем доступ в Интернет из локальных сетей офисов HQ и BRANCH через iptables

Настраиваем NAT - через iptables:

HQ-R | BR-R

В Альт iptables установлен по умолчанию:

добавляем правило в таблицу nat в цепочку postrouting (после маршрутизации):

apt-get update

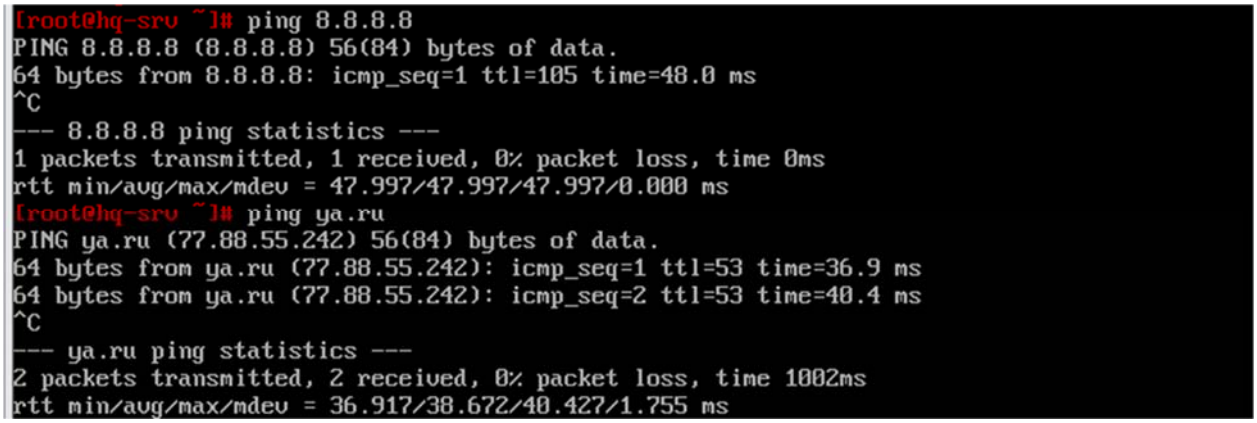
#apt-get install iptables

#iptables -t nat -A POSTROUTING -o ens32 -j MASQUERADE

```
[root@isp etc]# iptables-save > /etc/sysconfig/iptables
```

Проверка:

HQ-SRV



HQ-BR

%

4.5 Настройте локальные учётные записи на всех устройствах

Задание:

4. Настройте локальные учётные записи на всех устройствах в соответствии с таблицей 4.3.

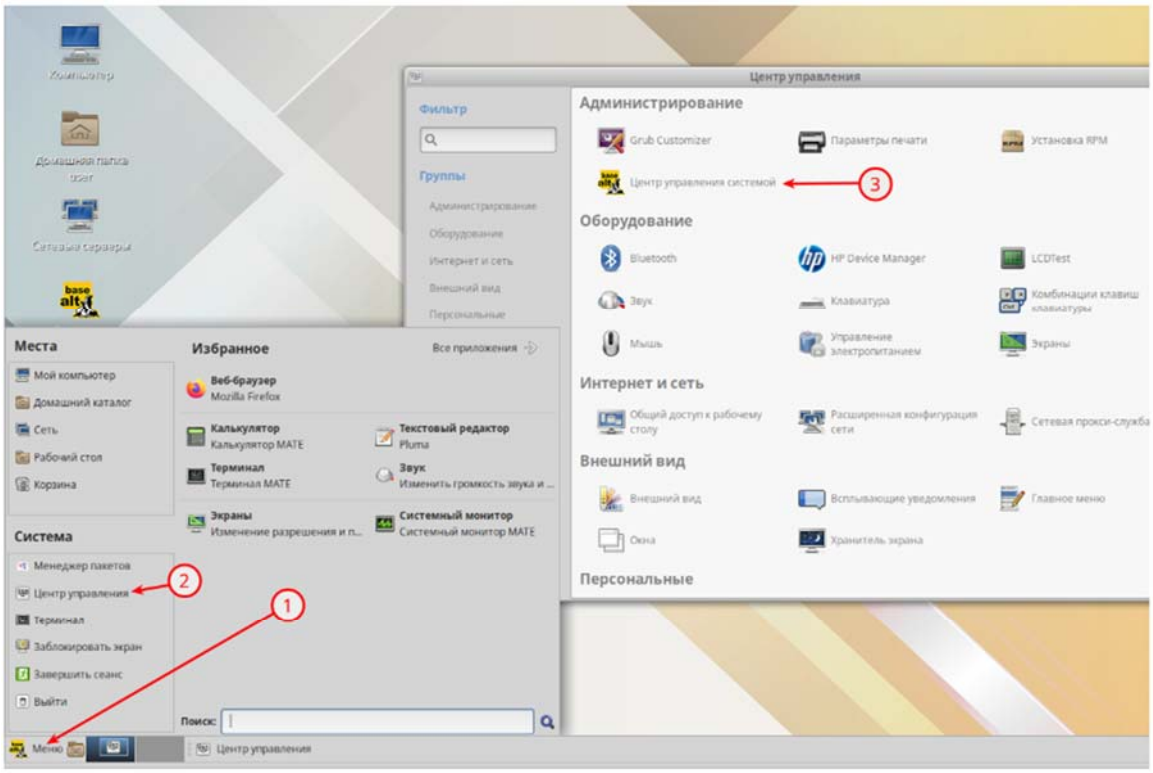
Учётная запись	Пароль	Примечание
Admin	P@ssw0rd	CLI HQ-SRV HQ-R
Branch admin	P@ssw0rd	BR-SRV BR-R
Network admin	P@ssw0rd	HQ-R BR-R BR-SRV

Выполнение:

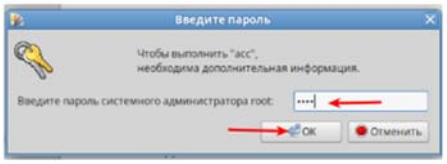
CLI:

На клиенте создать необходимого пользователя можно через ЦУС -> выбрав вкладку "Локальные учётные записи"

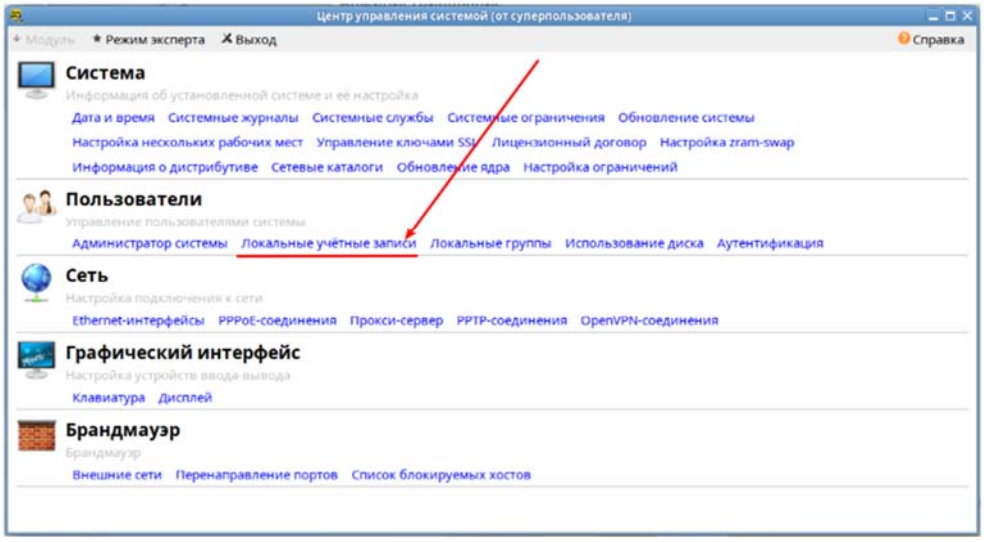
"Пуск" -> "Центр управления" -> "Центр управления системой (ЦУС)":



- вводим пароль пользователя "**root**" -> нажимаем "**OK**":

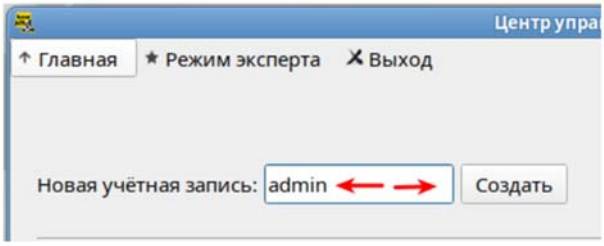


- Переходим "**Локальные учётные записи**":

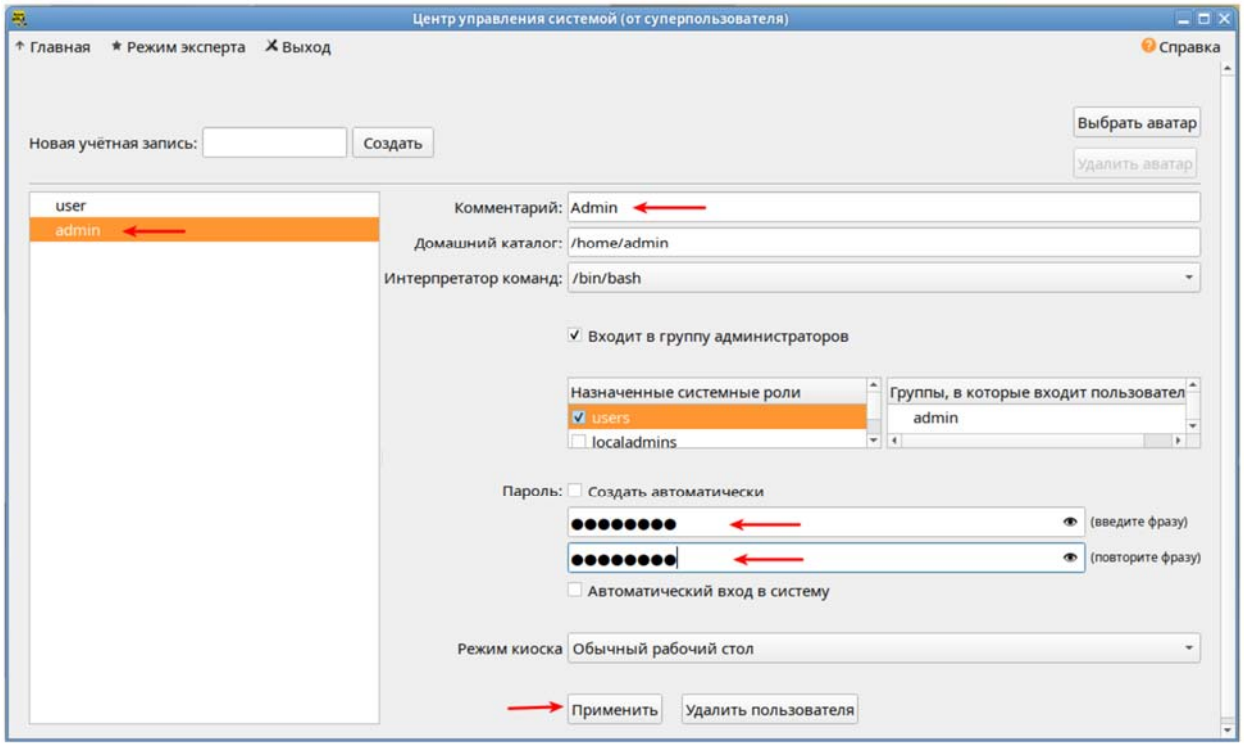


\

В качестве "Новая учётная запись" пишим имя пользователя -> нажимаем "Создать"



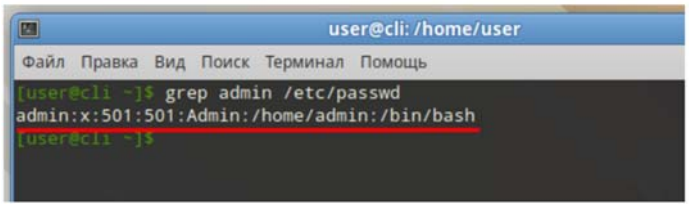
т.к. нельзя создать пользователя с загланой буквы как указано в таблице 2 -> в "Комментарий:" можно указать "Admin" как в таблице 2 -> также задаём пароль и подтверждаем его -> нажимаем "Применить":



Проверяем:

Нажимаем "Ctrl + Alt + T" для открытия терминала и вводим команду:

grep admin /etc/passwd



BR-SRV | BR-R:

Для добавления пользователя используется утилита useradd

useradd branch-admin -m -c "Branch admin" -U

где:

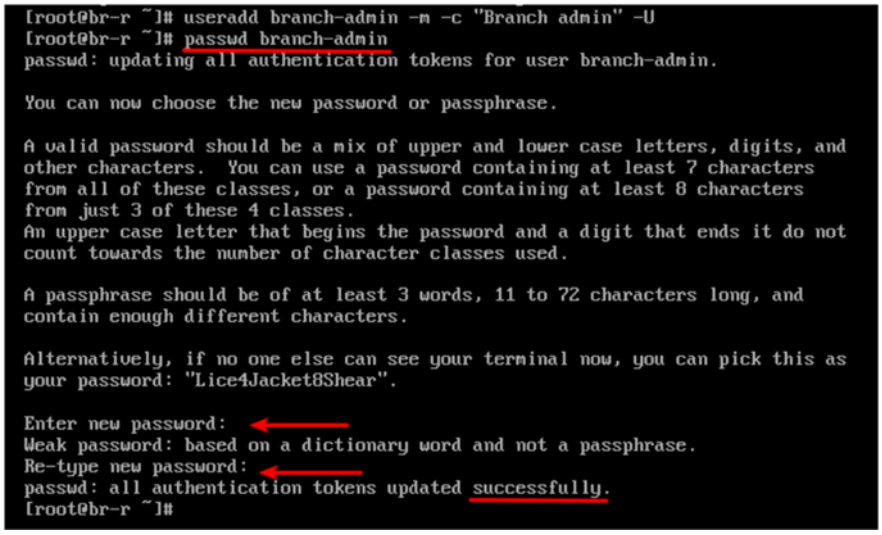
- **branch-admin** - имя пользователя

- **-m** - если домашнего каталога пользователя не существует, то он будет создан
- **-c "Branch admin"** - любая текстовая строка. Обычно, здесь коротко описывается учётная запись, и в настоящее время используется как поле для имени и фамилии пользователя
- **-U** - создайтся группа с тем же именем, что и у пользователя, и добавляеется пользователь в эту группу

после добавления пользователя - ему необходимо задать пароль:

- необходимо дважды указать в качестве пароля - "P@ssw0rd"

passwd branch-admin



HQ-SRV | HQ-R:

useradd admin -m -c "Admin" -U

passwd admin

HQ-R | BR-R | BR-SRV:

useradd network-admin -m -c "Network admin" -U

passwd network-admin

Проверяем:

- HQ-R:

```
admin:x:501:501:Admin:/home/admin:/bin/bash
network-admin:x:502:502:Network admin:/home/network-admin:/bin/bash
```

- HR-SRV:

```
admin:x:501:501:Admin:/home/admin:/bin/bash
```

- BR-R:

```
branch-admin:x:501:501:Branch admin:/home/branch-admin:/bin/bash
network-admin:x:502:502:Network admin:/home/network-admin:/bin/bash
```

- BR-SRV:

```
branch-admin:x:501:501:Branch admin:/home/branch-admin:/bin/bash
network-admin:x:502:502:Network admin:/home/network-admin:/bin/bash
```

4.6 Измерьте пропускную способность сети между двумя узлами

Задание:

Измерьте пропускную способность сети между двумя узлами HQ-R-ISP по средствам утилиты iperf 3. Предоставьте описание пропускной способности канала со скриншотами.

Выполнение:

HQ-R:

Необходимо установить пакет "iperf3" для проверки пропускной способности сети между серверами:

#apt-get install -y iperf3

Выполнить запуск службы iperf3:

#systemctl enable --now iperf3

запустим iperf3 в режиме клиента, используя флаг -c, и укажем хост, на котором работает сервер -> ISP (172.16.4.1):

#iperf3 -c 172.16.4.1

при помощи параметра "--get-server-output" - можно получить более детальный результат:

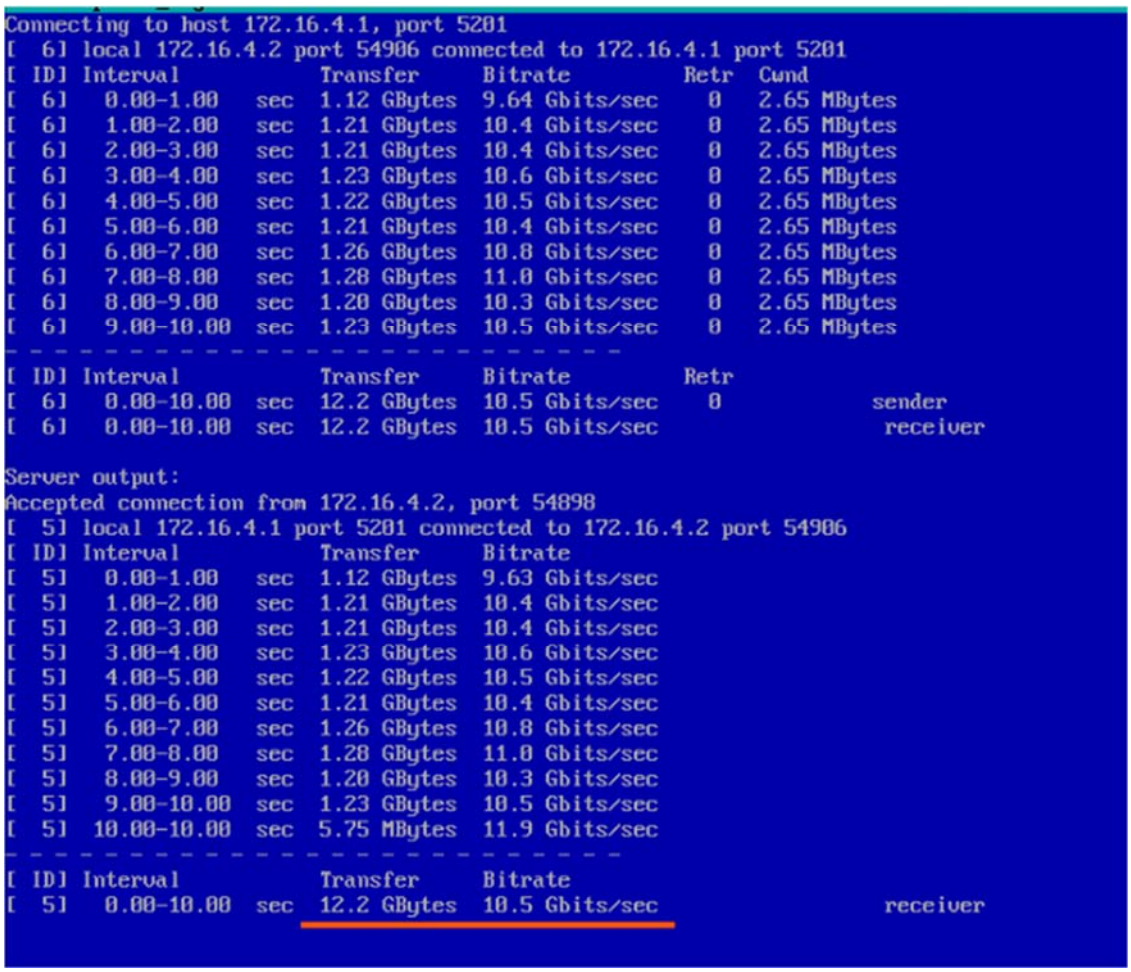
```
[root@hq-r ~]# iperf3 -c 172.16.4.1
Connecting to host 172.16.4.1, port 5201
[  5] local 172.16.4.2 port 45590 connected to 172.16.4.1 port 5201
[ ID] Interval           Transfer     Bitrate         Retr  Cwnd
[  5]   0.00-1.00   sec  1.16 GBytes  9.96 Gbits/sec    0   2.56 MBytes
[  5]   1.00-2.00   sec  1.25 GBytes  10.8 Gbits/sec    0   2.56 MBytes
[  5]   2.00-3.00   sec  1.24 GBytes  10.6 Gbits/sec    0   2.56 MBytes
[  5]   3.00-4.00   sec  1.23 GBytes  10.6 Gbits/sec    0   2.56 MBytes
[  5]   4.00-5.00   sec  1.26 GBytes  10.8 Gbits/sec    0   2.56 MBytes
[  5]   5.00-6.00   sec  1.24 GBytes  10.7 Gbits/sec    0   2.56 MBytes
[  5]   6.00-7.00   sec  1.24 GBytes  10.6 Gbits/sec    0   2.56 MBytes
[  5]   7.00-8.00   sec  1.25 GBytes  10.7 Gbits/sec    0   2.56 MBytes
[  5]   8.00-9.00   sec  1.25 GBytes  10.7 Gbits/sec    0   2.56 MBytes
[  5]   9.00-10.00  sec  1.23 GBytes  10.6 Gbits/sec    0   2.56 MBytes
- - - - - - - - - - - - - - - - - - - - - - - - -
[ ID] Interval           Transfer     Bitrate         Retr
[  5]   0.00-10.00  sec  12.3 GBytes  10.6 Gbits/sec    0             sender
[  5]   0.00-10.00  sec  12.3 GBytes  10.6 Gbits/sec                  receiver

iperf Done.
```

если необходимо получить результаты сервера в выводе клиента

при помощи параметра "--logfile /path/to/file" - можно указать путь к файлу в который записать вывод данной каманды в качестве отчёта

```
#iperf3 -c 11.11.11.1 --get-server-output --logfile ~/iperf3_logfile.txt
```

```
[root@hq-r ~]# iperf3 -c 172.16.4.1 --get-server-output --logfile ~/iperf3_logfile.txt
[root@hq-r ~]# ls
iperf3_logfile.txt  ipv4address  ipv4route  options  resolv.conf  tmp
[root@hq-r ~]#
```



Таким образом, пропускная способность канала между HQ-R -> ISP составляет 10.5 Гбит/с на отправку данных и 10.5 Гбит/с на получение данных. Также за 10 секунд тестирования было передано 12.2 ГБ данных.

4.7 Составьте backup скрипты для сохранения конфигурации сетевых устройств

Задание:

6. Составьте backup скрипты для сохранения конфигурации сетевых устройств, а именно HQ-R BR-R. Продемонстрируйте их работу.

Выполнение:

HQ-R | BR-R:

Создадим простой bash-скрипт:

vim backup-script.sh

```
#!/bin/bash

echo "Start backup!"

backup_dir="/etc"
dest_dir="/opt/backup"

mkdir -p $dest_dir
tar -czf $dest_dir/$(hostname -s)-$(date +"%d.%m.%y").tgz $backup_dir

echo "Done!"
```

Назначаем права на исполнения для данного файла:

chmod +x backup-script.sh

```
[root@hq-r ~]# ls -l
total 12
-rw-r--r-- 1 root root  178 Jan  6 16:56 backup-script.sh
-rw-r--r-- 1 root root 2380 Jan  6 16:42 iperf3_logfile.txt
drwx------ 2 root root 4096 Jan  6 16:35 tmp
[root@hq-r ~]# chmod +x backup-script.sh
[root@hq-r ~]# ls -l
total 12
-rwxr-xr-x 1 root root  178 Jan  6 16:56 backup-script.sh
-rw-r--r-- 1 root root 2380 Jan  6 16:42 iperf3_logfile.txt
drwx------ 2 root root 4096 Jan  6 16:35 tmp
[root@hq-r ~]#
```

где:

#!/bin/bash: Эта строка - это шебанг (shebang), она указывает на то, какую оболочку следует использовать для выполнения скрипта. В данном случае, скрипт выполняется с использованием оболочки Bash.

echo "Start backup!": Эта команда выводит текст "Start backup!" в стандартный вывод (обычно в терминал).

backup_dir="/etc"": Эта строка определяет переменную backup_dir и устанавливает ей значение "/etc". Эта переменная будет использоваться для указания каталога, который будет архивироваться.

в случае если необходимо указать несколько директорий для резервного копирования они указываются в "кавычках" через пробел, например backup_dir="/etc /var /home"

dest_dir="/opt/backup": Здесь определяется переменная dest_dir и устанавливается значение "/opt/backup". Эта переменная будет использоваться для указания каталога, в который будет сохранен архив.

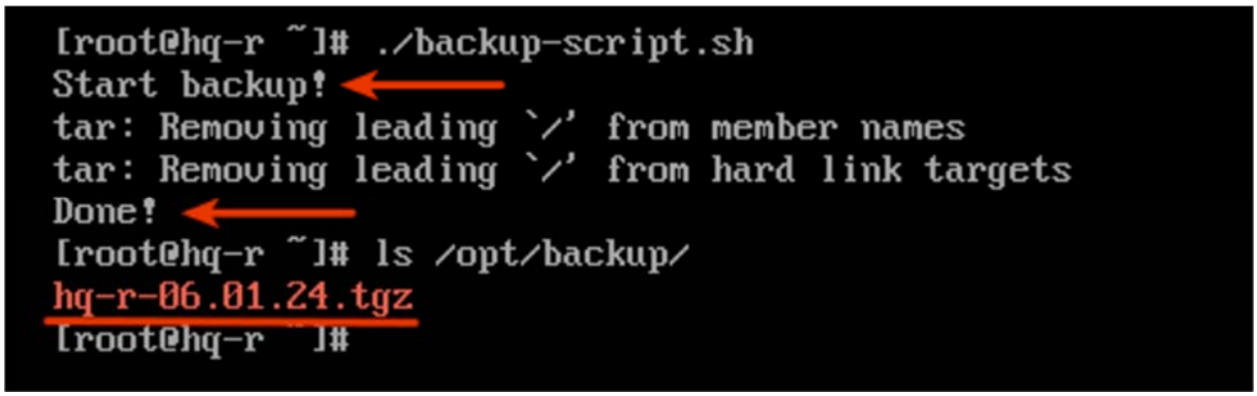
mkdir -p $dest_dir: Эта команда создает каталог, указанный в переменной dest_dir с опцией -p, которая позволяет создать каталог, а также все родительские каталоги, если они не существуют.

tar -czf $dest_dir/$(hostname -s)-$(date +"%d.%m.%y").tgz $backup_dir: Эта команда использует tar для создания архива файлов из каталога, указанного в переменной backup_dir. Архив сохраняется в каталоге, указанном в переменной dest_dir, с именем, которое включает имя хоста (hostname), текущую дату и расширение ".tgz". Опции -czf указывают на то, что архив должен быть сжат в формате gzip.

echo "Done!": Эта команда выводит текст "Done!" в стандартный вывод после завершения создания архива.

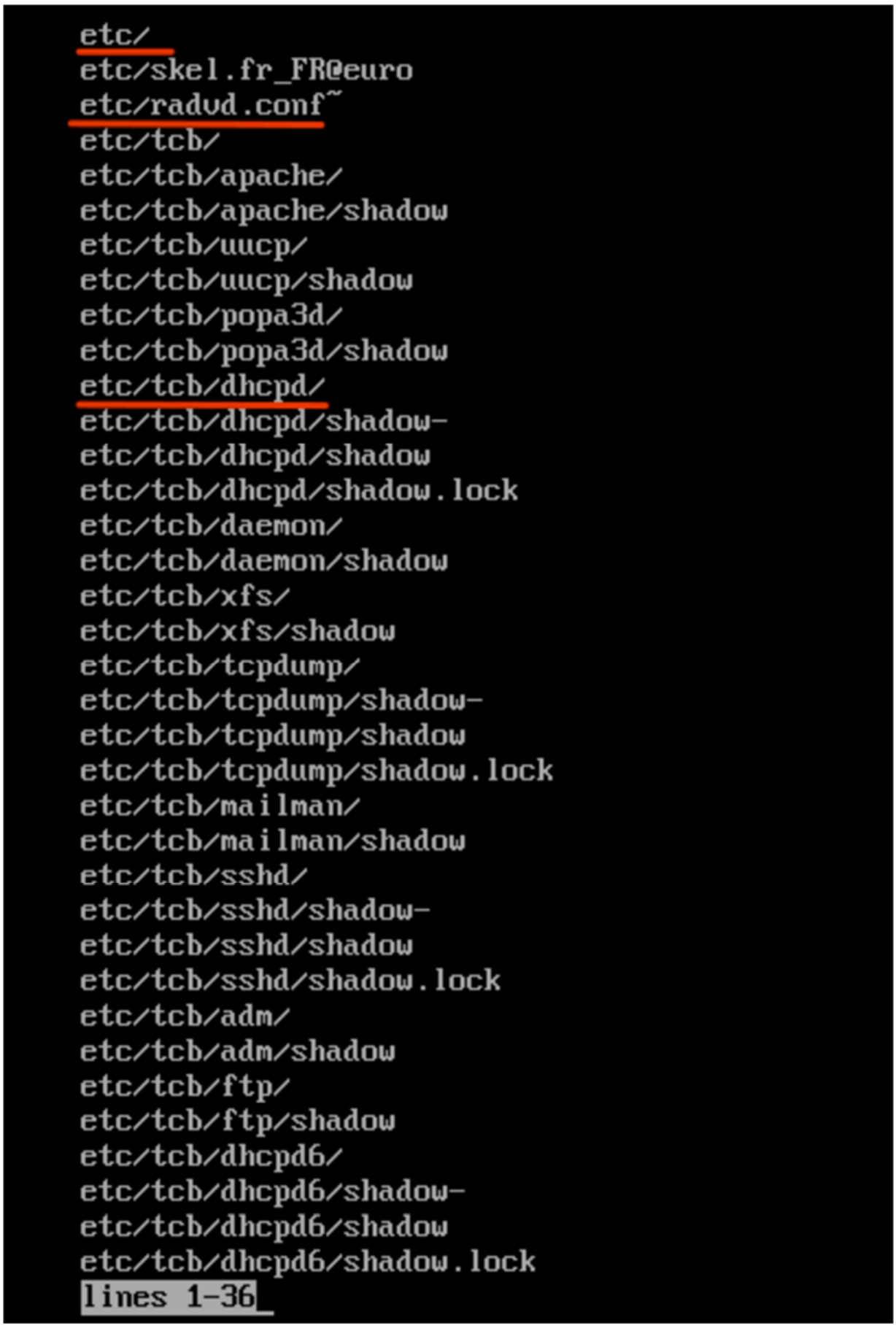
Выполняем запуск скрипта:

./backup-script.sh



Просмотрим содержание архива:

tar -tf /opt/backup/hq-r-06.01.24.tgz | less



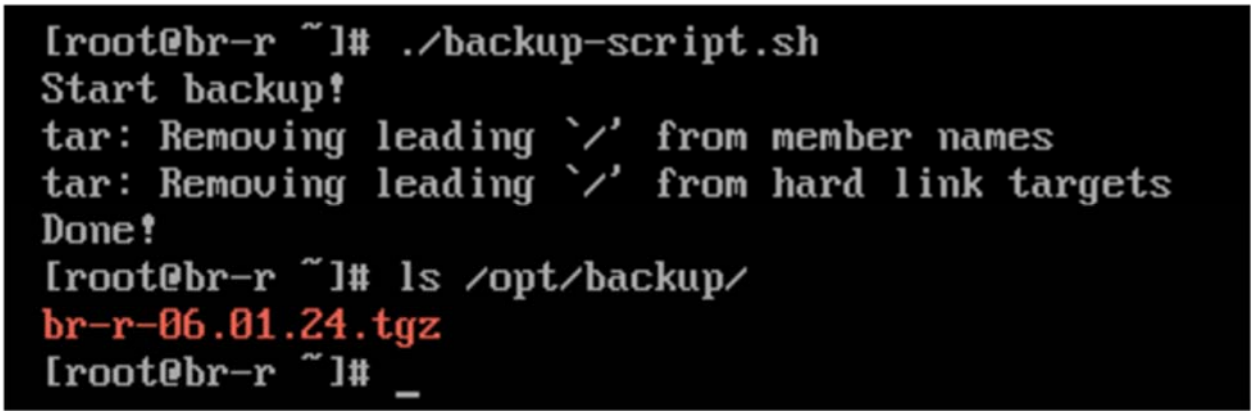
таким образом, скрипт записал в архив всё содержимое директории /etc

также есть возможность архивировать не одну, а несколько директорий с целью резевного копирования, необходимо всеголишь в переменную backup_dir скрипта передать необходимые директории через пробел, например:

backup_dir="/etc /var /home"

Аналогичный скрипт запускаем и на BR-R

для ускорения процесса, передать скрипт с HQ-R на BR-R или наоборот можно по scp



4.8 Настройка подключения по SSH для удалённого конфигурирования устройства HQ-SRV по порту 2222.

Учтите, что вам необходимо перенаправить трафик на этот порт по средствам контролирования трафика.

HQ-SRV:

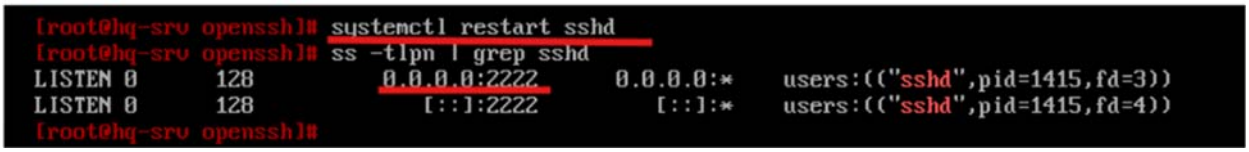
меняем стандартный порт **ssh (22)** на **2222** согласно заданию:

sed -i "s/#Port 22/Port 2222/g" /etc/openssh/sshd_config

перезапускаем службу **sshd**:

systemctl restart sshd

Проверяем:



HQ-R

через iptables:

в Альт установлен по умолчанию;

Создадим следующее правило, которое будет перенаправлять **внешние** подключения на порт **22** -> на порт **2222** сервера **HQ-SRV**:

в таблицу **nat** в цепочку **prerouting** (до маршрутизации) добавляем правило:

iptables -t nat -A PREROUTING -i ens32 -p tcp --dport 22 -j DNAT --to-destination 192.168.1.2:2222

где:

-t nat - таблица nat;

-A PREROUTING - добавить правило в цепочку prerouting, выполняющееся до маршрутизации;

-i ens32 - внешний интерфейс;

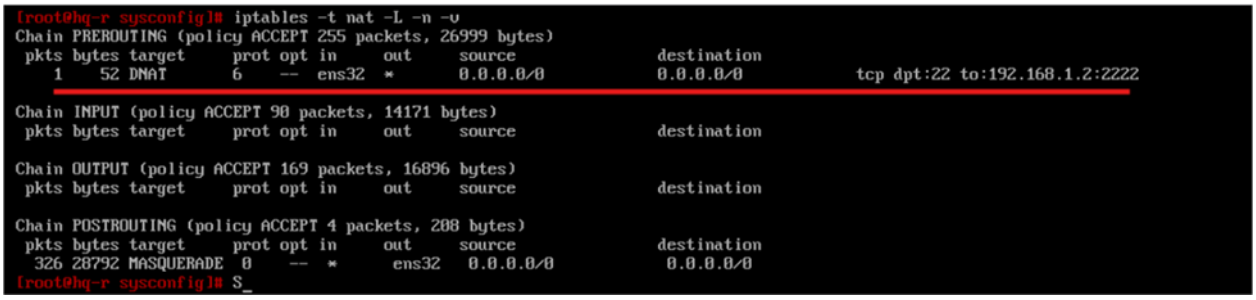
-p tcp - порт TCP;

--dport 22 - порт назначения;

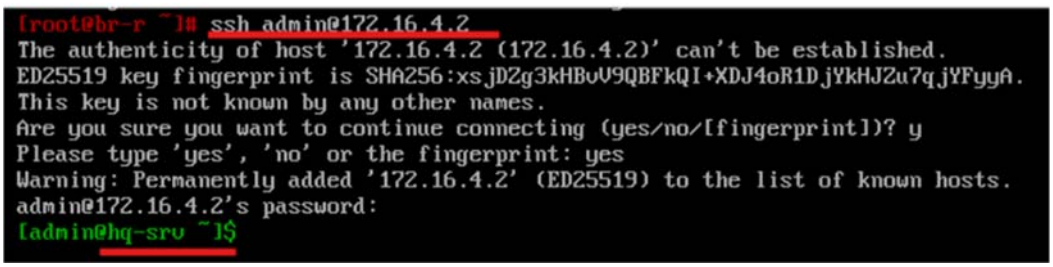
-j DNAT - "обратный" nat;

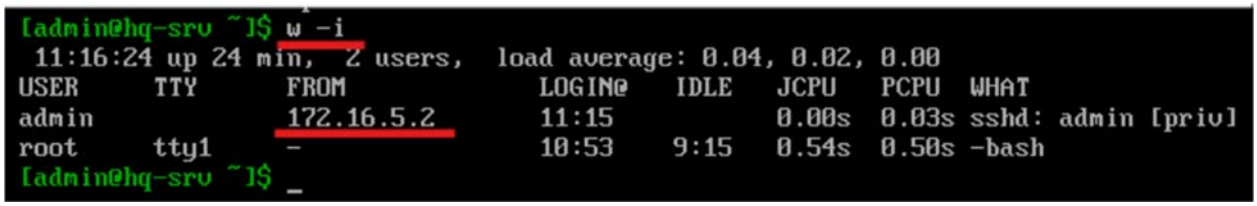
--to-destination - куда перенаправлять;

проверяем:



проверяем подключение с **BR-R** к **HQ-SRV**, через внешний адрес **HQ-R** (172.16.4.2):





сохраняем правила **iptables** и **ip6tables**:

iptables:

iptables-save >> /etc/sysconfig/iptables

systemctl enable --now iptables

Модуль 2: Организация сетевого администрирования

Настройте DNS-сервер на сервере HQ-SRV

Задание:

1. Настройте DNS-сервер на сервере HQ-SRV (dhcp УБРАТЬ СЕТЬ ПО STATIC)

a. На DNS сервере необходимо настроить 2 зоны

Зона au-team.irpo , также не забудьте настроить обратную зону

Имя	Тип записи	Адрес
hq-r.au-team.irpo	A, PTR	192.168.1.1
hq-srv.au-team.irpo	A, PTR	192.168.1.2
br-r.au-team.irpo	A, PTR	192.168.0.1
br-srv.au-team.irpo	A	192.168.0.2

Выполнение:

HQ-SRV:

Устанавливаем пакеты bind и bind-utils:

apt-get install -y bind bind-utils

Во избежании появлении ошибки при запуске bind:

не следует, при установке системы, задавать полное (FQDN) имя для hq-srv;

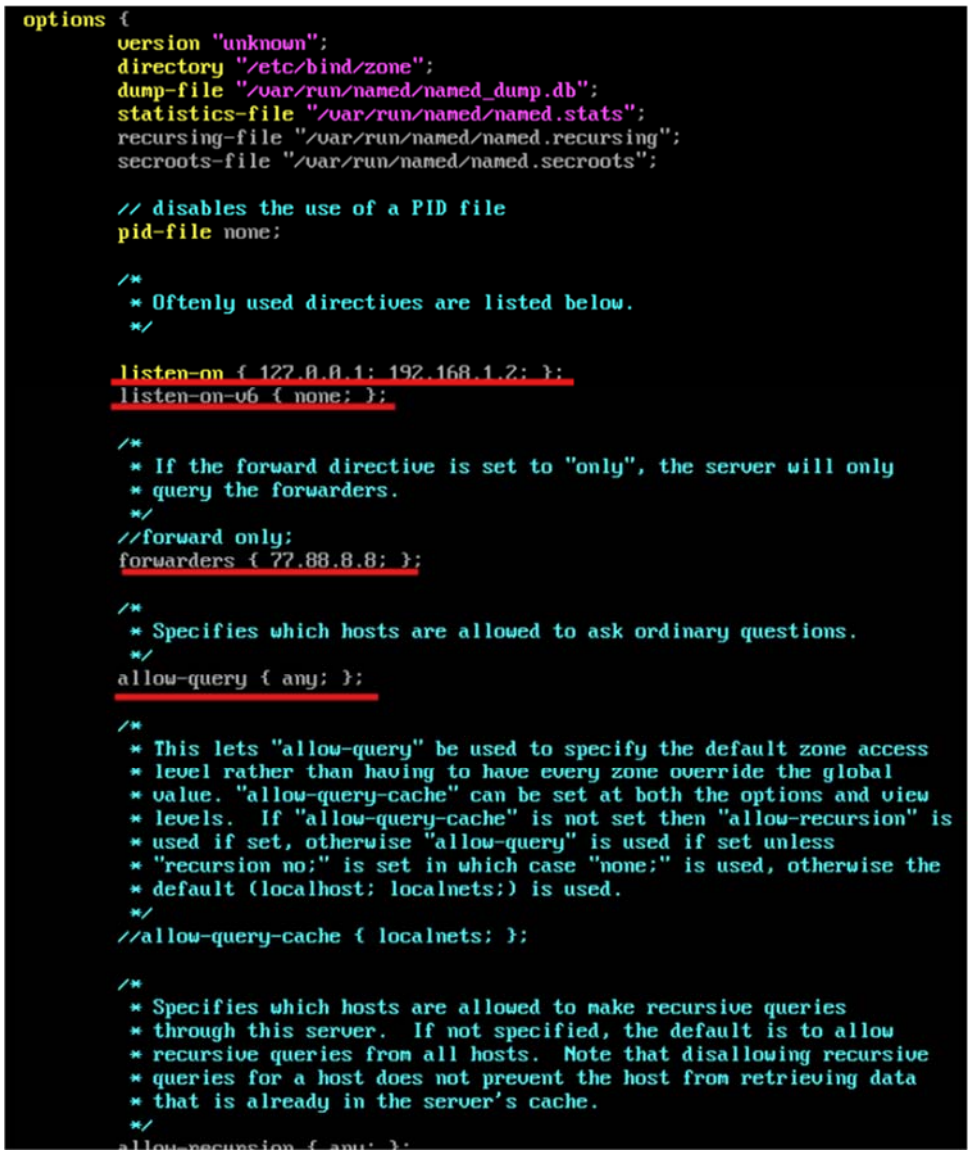
В конфигурационном файле /etc/bind/options.conf - правим следующие параметры:

vim /etc/bind/options.conf

listen-on параметр определяет адреса и порты, на которых DNS-сервер будет слушать запросы. Значение any означает, что сервер будет прослушивать запросы на всех доступных интерфейсах и IP-адресах (IPv4 | IPv6);

в параметре forwarders указать сервера, куда будут перенаправляться запросы, на которые нет информации в локальной зоне;

раскомментировать параметр allow-query и указать в нём подсети из которых разрешено подавать запросы;

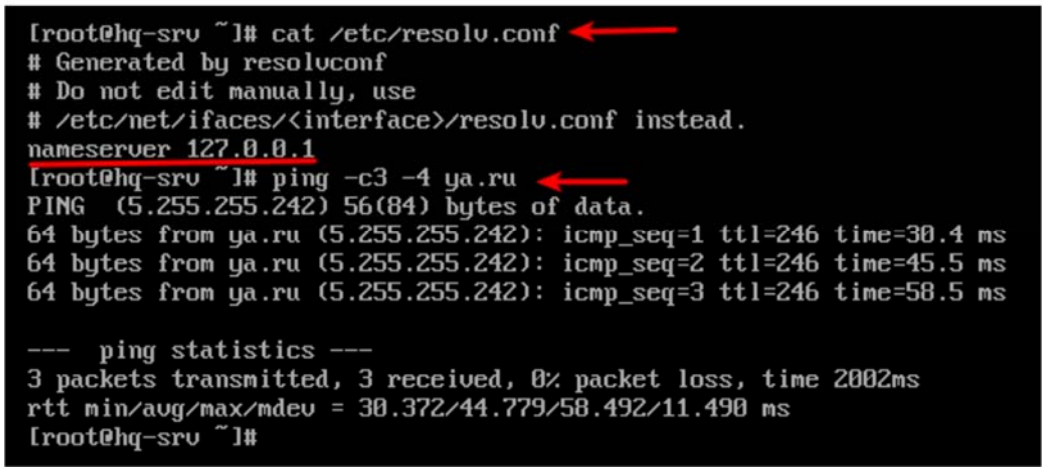


В качестве DNS-сервера для hq-srv должен быть 127.0.0.1:

echo “nameserver 127.0.0.1” >> /etc/resolv.conf

resolvconf -u

Проверяем доступ в Интернет:



В конфигурационной файле vim /var/lib/bind/etc/rfc1912.conf

описываем необходимые зоны согласно требованию задания:

au-team.irpo - зона прямого просмотра;

1.168.192.in-addr.arpa - зона обратного просмотра HQ;

0.168.192.in-addr.arpa - зона обратного просмотра BR;

vim /var/lib/bind/etc/rfc1912.conf

Добавляем следующее содержимое:

```
zone "au-team.irpo" {
        type master;
        file "au-team.irpo";
};
zone "1.168.192.in-addr.arpa" {
        type master;
        file "1.168.192.in-addr.arpa";
};
zone "0.168.192.in-addr.arpa" {
        type master;
        file "0.168.192.in-addr.arpa";
};
```

Необходимо перейти в директорию /var/lib/bind/etc/zone и путем копирования создать файлы зон:

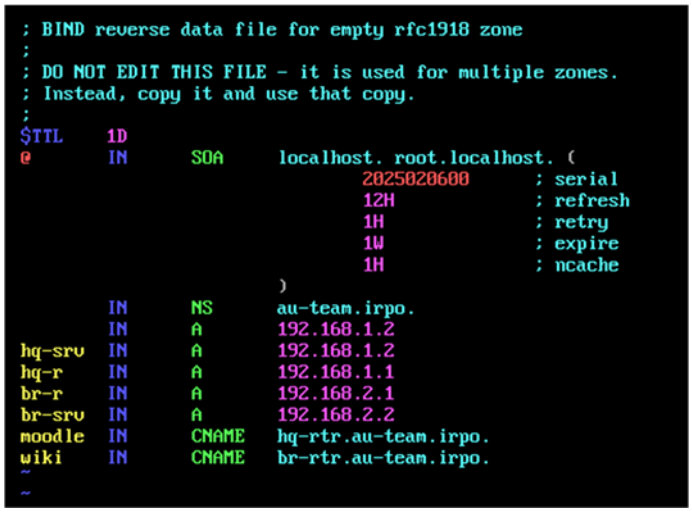
```
[root@hq-srv ~]# cd /var/lib/bind/etc/zone/
[root@hq-srv zone]# cp empty au-team.irpo
[root@hq-srv zone]# cp empty 100.168.192.in-addr.arpa
[root@hq-srv zone]#
```

Необходимо сконфигурировать файл **au-team.irpo**:

vim au-team.irpo

который является прямой зоной следующим образом:

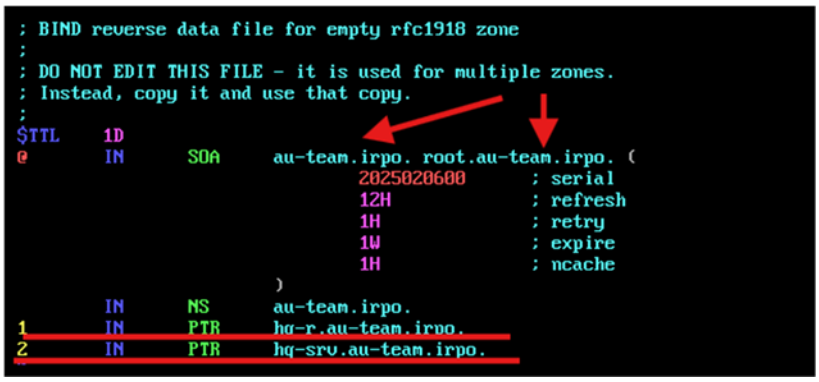
приводим файл к следующему виду - добавляя записи типа A для зоны au-team.irpo:



Далее необходимо настроить обратную зону и привести файл **1.168.192.in-addr.arpa**:

vim 1.168.192.in-addr.arpa

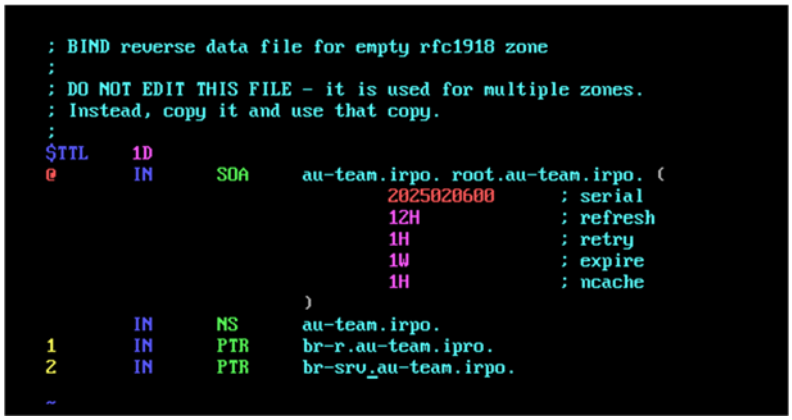
к следующему виду:



Далее необходимо настроить обратную зону и привести файл **1.168.192.in-addr.arpa**:

vim 0.168.192.in-addr.arpa

к следующему виду:



Запускаем и добавляем в автозагрузку службу bind:

systemctl enable --now bind

Для DNS-сервиса важно обеспечить непрерывный аптайм, не допуская даже минутных простоев.

Если вы попытаетесь перезапустить systemd-юнит обычной командой systemctl, а в конфигурации будут ошибки, то BIND не запустится.

Чтобы избежать столь неприятных последствий, всего-то надо правильно настроить утилиту **rndc**, которая позволяет обойти эти сложности.

После того, как конфигурация зон была завершена, для корректной работы службы bind необходимо выполнить команду:

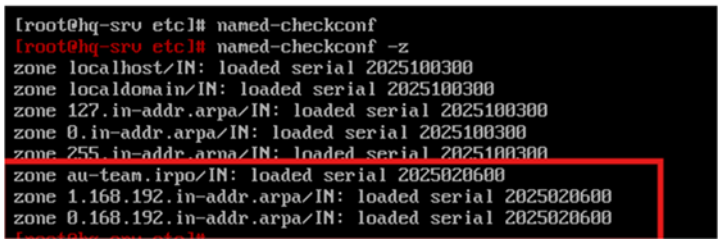
rndc-confgen > /var/lib/bind/etc/rndc.key

Затем выполнить команду:

sed -i ‘6,$d’ /var/lib/bind/etc/rndc.key

Перед запуском службы остается поменять группу у файлов зон, которые были созданы ранее, на named

а также проверить конфигурационные файлы и файлы зон командами **named-checkconf** и **named-checkconf -z** соответственно:



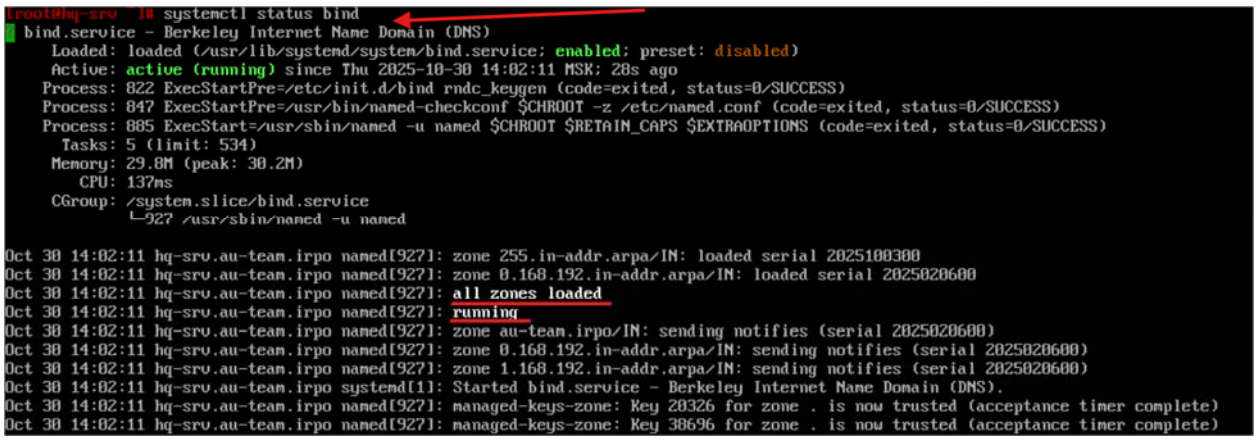
Проверяем файл /etc/resolv.conf

После этого можно запустить службу **bind**:

systemctl enable --now bind.service

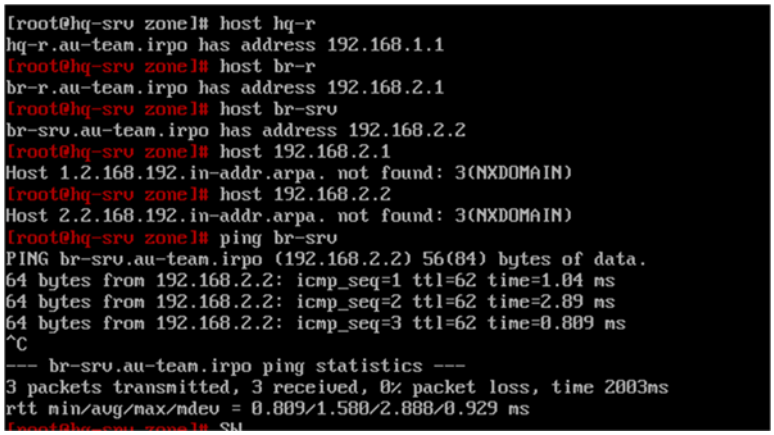
Перезапускаем службу bind:

systemctl restart bind



Проверяем:

зона au-team.irpo



. Настройте синхронизацию времени между сетевыми устройствами по протоколу NTP

Задание:

2. Настройте синхронизацию времени между сетевыми устройствами по протоколу NTP

a. В качестве сервера должен выступать роутер HQ-R со стратумом 5

b. Используйте Loopback интерфейс на HQ-R, как источник сервера времени

c. Все остальные устройства и сервера должны синхронизировать свое время с роутером HQ-R

d. Все устройства и сервера настроены на московский часовой пояс (UTC +3)

Выполнение:

HQ-R:

timedatectl set-timezone Europe/Moscow

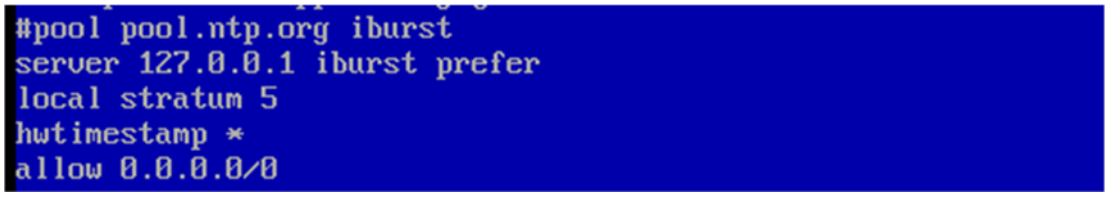
Настройка NTP сервера:

Установим пакет chrony:

apt-get install -y chrony

Приводим конфигурационный файл "chrony.conf" к следующему виду:

vim /etc/chrony.conf



где:

server 127.0.0.1 iburst prefer - указываем сервером синхронизации самого себя, опция «iburst» принудительно отправляет сразу несколько пакетов для точности синхронизации, опция «prefer» говорит о том, что это будет предпочитаемый сервер;

hwtimestamp * - опция, чтобы сетевой интерфейс считал собственный источник времени верным и синхронизировал клиентов с ним;

local stratum 5 - устанавливаем для себя значение по stratum = 5;

Stratum — это класс сервера, который указывает на его точность. Число после названия класса (от 1 до 16) показывает уровень сервера по отношению к самому точному времени.

allow - кому разрешается подключаться к серверу и запрашивать время: чтобы не перечеслять все используемые в задании IPv4 и IPv6 сети, используется 0/0 и ::/0; (закомментированный блок писать не надо, как пример описание всех используемых в задании сетей)

Запускаем и добавляем в автозагрузку службу chronyd:

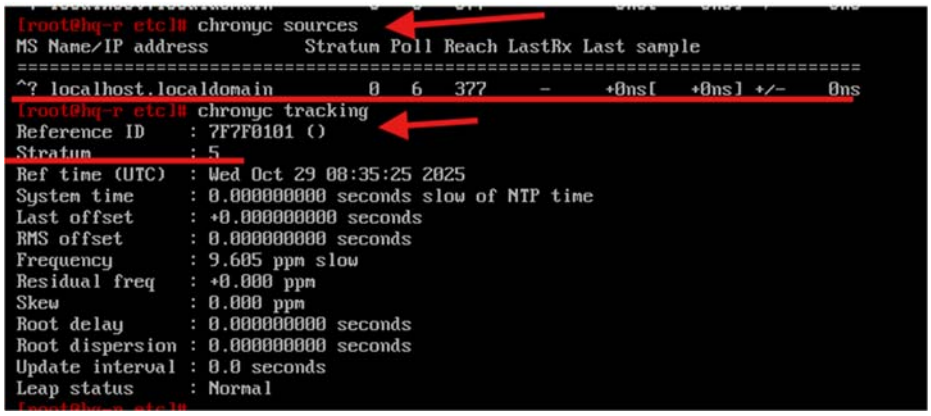
systemctl enable --now chronyd

Перезагружаем службу chronyd для применения изменений:

systemctl restart chronyd

Проверяем:

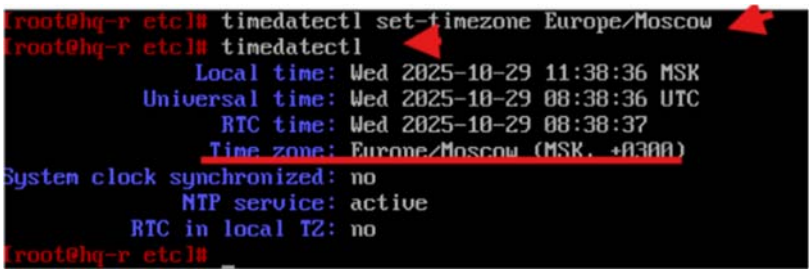
Проверяем:



Настроим московский часовой пояс (UTC +3):

timedatectl set-timezone Europe/Moscow

Проверяем:



Настройка NTP клиентов:

HQ-SRV:

Настроим московский часовой пояс (UTC +3):

timedatectl set-timezone Europe/Moscow

Установим пакет chrony:

apt-get install -y chrony

Приводим конфигурационный файл "chrony.conf" к следующему виду:

vim /etc/chrony.conf

где:

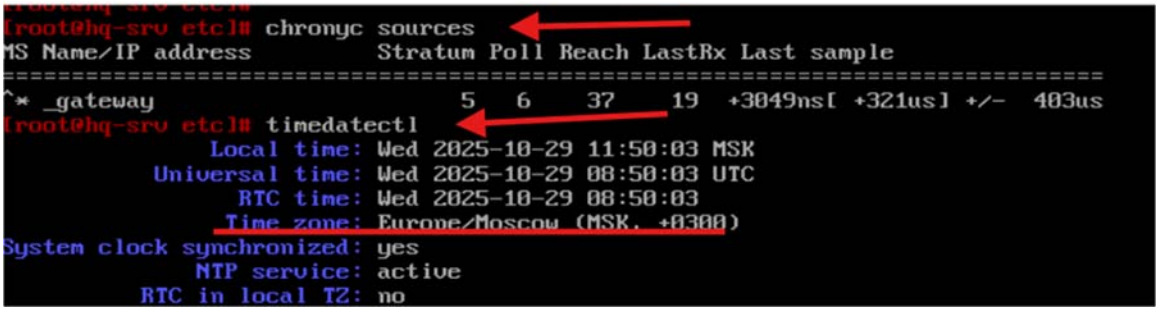
192.168.1.1 - IPv4 адрес HQ-R;

Запускаем и добавляем в автозагрузку службу chronyd:

systemctl enable --now chronyd

Проверяем:

с клиента HQ-SRV:



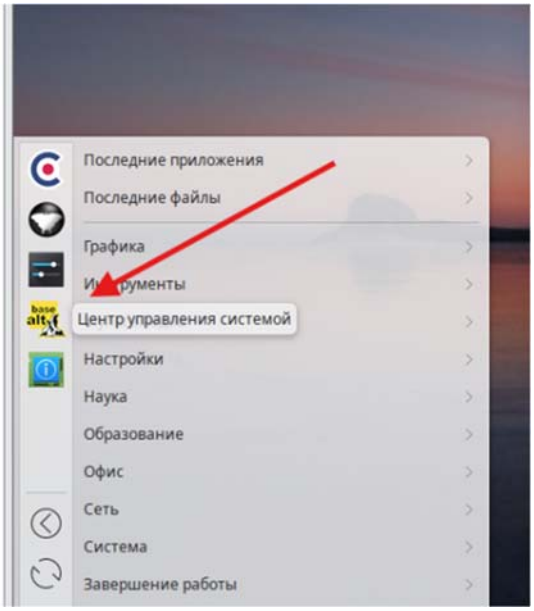
с сервера HQ-R:

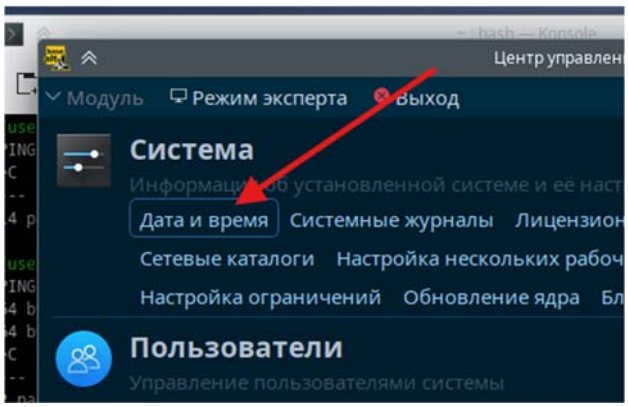
```
[root@hq-r etc]# chronyc clients
Hostname                      NTP   Drop Int IntL Last     Cmd   Drop Int  Last
===============================================================================
localhost.localdomain          16      0   7   -   119       0      0   -     -
hq-srv.au-team.irpo             7      0   6   -    11       0      0   -     -
[root@hq-r etc]# _
```

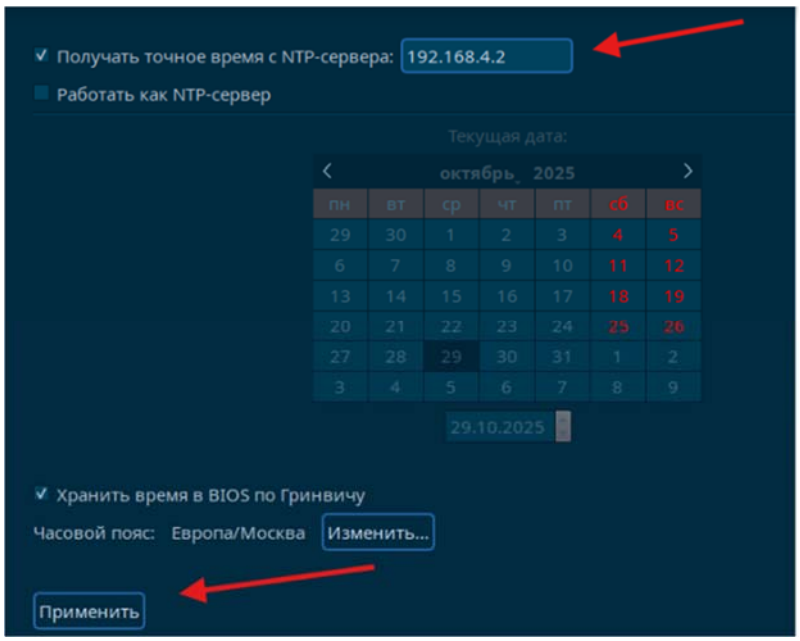
BR-R | BR-SRV

Настройка аналогична HQ-SRV - за исключением указания соответствующих адресов IPv4 HQ-R

CLI:







Проверяем: с HQ-R

- С **HQ-R** проверяем клиентов, должны быть все ВМ как по **IPv4** так и

```
[root@hq-r etc]# chronyc clients
Hostname                      NTP   Drop Int IntL Last     Cmd   Drop Int  Last
===============================================================================
localhost.localdomain          31      0   8   -   320       0      0   -     -
hq-srv.au-team.irpo            30      0   9   -   343       0      0   -     -
192.168.4.1                    22      0   7   -    10       0      0   -     -
10.10.10.2                      6      0   5   -    20       0      0   -     -
192.168.2.2                     2      0   1   -     1       0      0   -     -
[root@hq-r etc]# _
```

где:

- 192.168.1.2 - HQ-SRV;
- 10.10.10.2 - BR-R;
- 192.168.2.2 - BR-SRV;
- 192.168.4.1 - CLI

5.1 Настройте контроллер домена Samba DC на сервере BR-SRV

Задание:

- Имя домена au-team.irpo
- Введите в созданный домен машину CLI
- Создайте 5 пользователей для офиса HQ: имена пользователей формата hquser№ (например hquser1, hquser2 и т.д.)
- Создайте группу hq, введите в группу созданных пользователей

- Убедитесь, что пользователи группы hq имеют право аутентифицироваться на CLI
- Пользователи группы hq должны иметь возможность повышать привилегии для выполнения ограниченного набора команд: cat, grep, id. Запускать другие команды с повышенными привилегиями пользователи группы права не имеют.

Вариант реализации:

5.1.1 BR-SRV:

- Для Samba DC на базе Heimdal Kerberos необходимо установить пакет **task-samba-dc**, который установит все необходимое:

```
apt-get update && apt-get install -y task-samba-dc
```

- Так как Samba в режиме контроллера домена (Domain Controller, DC) использует свой сервер LDAP, свой центр распределения ключей Kerberos и свой сервер DNS (если не включен плагин BIND9_DLZ), перед установкой необходимо остановить конфликтующие службы **krb5kdc** и **slapd**, а также **bind**:

```
for service in smb nmb krb5kdc slapd bind;
do
  systemctl disable $service --now;
done
```

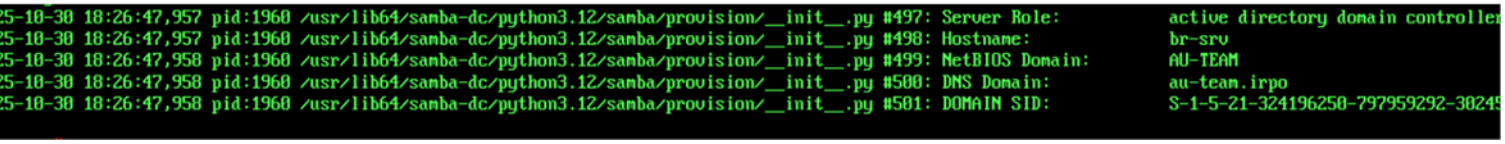
- Восстановление к начальному состоянию Samba:
  - Необходимо очистить базы и конфигурацию Samba (домен, если он создавался до этого, будет удалён):

```
rm -f /etc/samba/smb.conf
rm -rf /var/lib/samba
rm -rf /var/cache/samba
mkdir -p /var/lib/samba/sysvol
```

- Для интерактивного развертывания запустите **samba-tool domain provision**, это запустит утилиту развертывания, которая будет задавать различные вопросы о требованиях к установке:

- У Samba свой собственный DNS-сервер. В DNS forwarder IP address нужно указать внешний DNS-сервер, чтобы DC мог разрешать внешние доменные имена
- При запросе ввода нажимайте Enter за исключением запроса пароля администратора («Administrator password:» и «Retype password:»)
- Пароль администратора должен быть не менее 7 символов и содержать символы как минимум трёх групп из четырёх возможных: латинских букв в верхнем и нижнем регистрах, чисел и других небуквенно-цифровых символов
- Пароль, не полностью соответствующий требованиям, это одна из причин завершения развертывания домена ошибкой.
- При правильной базовой настройки устройства, все параметры подставятся атоматически

- Результат успешного интерактивного развертывания домена Samba DC:



- Включаем и добавляем в автозагрузку службу **samba**:

```
systemctl enable --now samba
```

- Настройка Kerberos:

```
cp /var/lib/samba/private/krb5.conf /etc/krb5.conf
```

- Перезагружаем службу **samba**:

```
systemctl restart samba
```

Проверка работоспособности домена:

Просмотр общей информации о домене

Просмотр предоставляемых служб

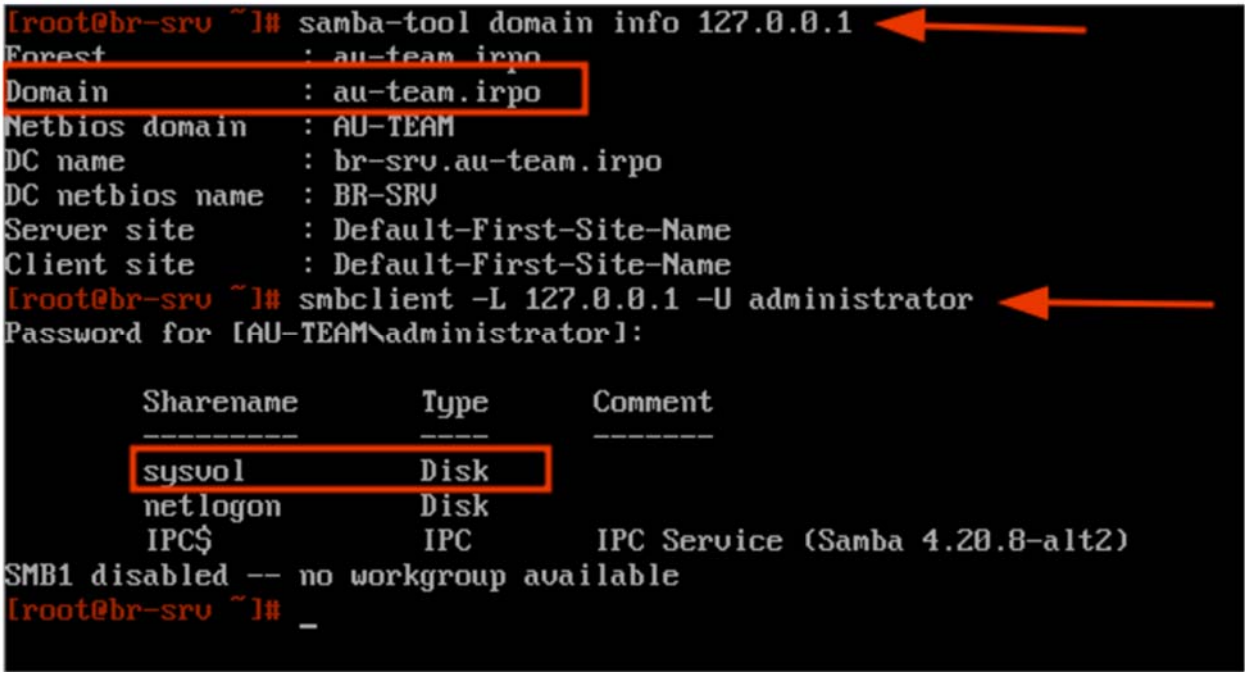
Перезагружаем службу samba:

systemctl restart samba

Проверка работоспособности домена:

Просмотр общей информации о домене

Просмотр предоставляемых служб



Проверка конфигурации DNS:

Убедиться в наличии nameserver 127.0.0.1 в /etc/resolv.conf:

echo "search au-team.irpo" > /etc/net/ifaces/ens32/resolv.conf

echo "nameserver 127.0.0.1" >> /etc/net/ifaces/ens32/resolv.conf

systemctl restart network

Утилита host в пакете bind-utils

Проверить имена хостов:

```
[root@br-srv ~]# host au-team.irpo
au-team.irpo has address 192.168.2.2
[root@br-srv ~]# host -t SRV _kerberos
_kerberos has no SRV record
[root@br-srv ~]# host -t SRV _kerberos._udp.au-team.irpo.
_kerberos._udp.au-team.irpo has SRV record 0 100 88 br-srv.au-team.irpo.
[root@br-srv ~]# host au-team.irpo
au-team.irpo has address 192.168.2.2
[root@br-srv ~]# host -t SRV _kerberos._udp.au-team.irpo.
_kerberos._udp.au-team.irpo has SRV record 0 100 88 br-srv.au-team.irpo.
[root@br-srv ~]# host -t SRV _ldap._tcp.au-team.irpo.
_ldap._tcp.au-team.irpo has SRV record 0 100 389 br-srv.au-team.irpo.
[root@br-srv ~]# host br-srv.au-team.irpo
br-srv.au-team.irpo has address 192.168.2.2
[root@br-srv ~]#
```

Проверка Kerberos (имя домена должно быть в верхнем регистре):

kinit administrator@AU-TEAM.IRPO

Просмотр полученного билета:

```
[root@br-srv ~]# kinit Administrator@AU-TEAM.IRPO
Password for Administrator@AU-TEAM.IRPO:
Warning: Your password will expire in 41 days on Fri Oct 17 08:33:35 2025
[root@br-srv ~]# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: Administrator@AU-TEAM.IRPO

Valid starting     Expires            Service principal
09/05/25 08:38:43  09/05/25 18:38:43  krbtgt/AU-TEAM.IRPO@AU-TEAM.IRPO
        renew until 09/06/25 08:38:41
[root@br-srv ~]#
```

Добавление всех необходимые записей типа A, PTR и CNAME средствами samba-tool

BR-SRV:

Добавляем все необходимые записи типа **A, PTR** и **CNAME** средствами **samba-tool**

Добавляем записи типа **A**:

samba-tool dns add 127.0.0.1 au-team.irpo br-r A 192.168.2.1 -U Administrator

samba-tool dns add 127.0.0.1 au-team.irpo hq-r A 192.168.1.1 -U Administrator

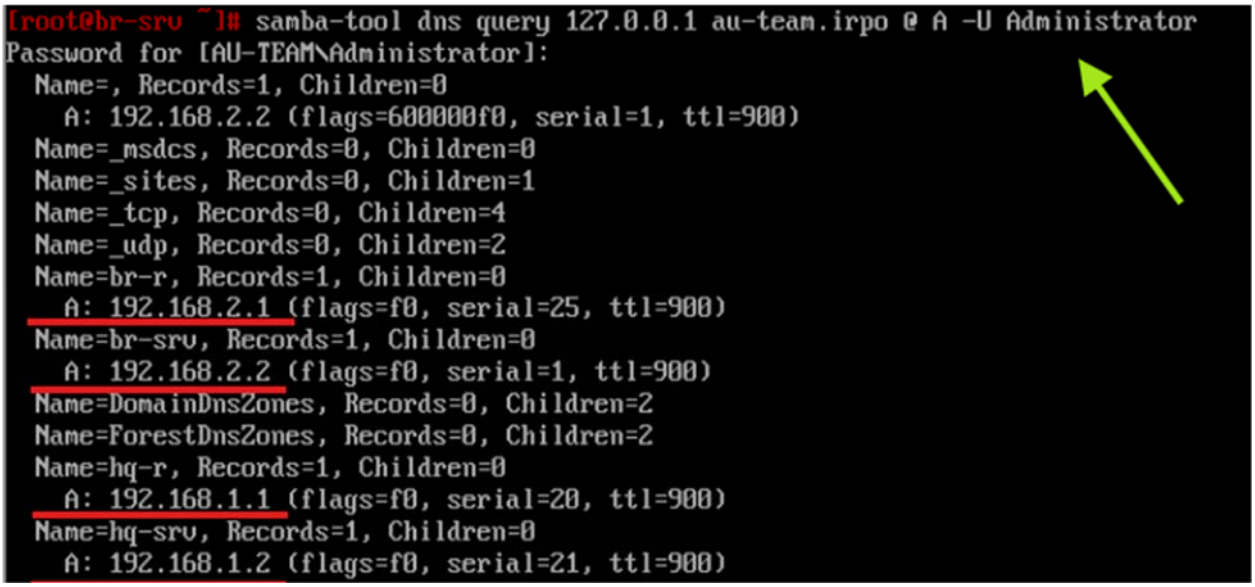
samba-tool dns add 127.0.0.1 au-team.irpo hq-srv A 192.168.1.2 -U Administrator

CLI введем с графического режима

Проверяем:

samba-tool dns query 127.0.0.1 au.team @ A -U Administrator

Результат:



Создаём зоны обратного просмотра для добавления PTR-записей:

Для сети офиса HQ:

samba-tool dns zonecreate 127.0.0.1 1.168.192.in-addr.arpa -U Administrator

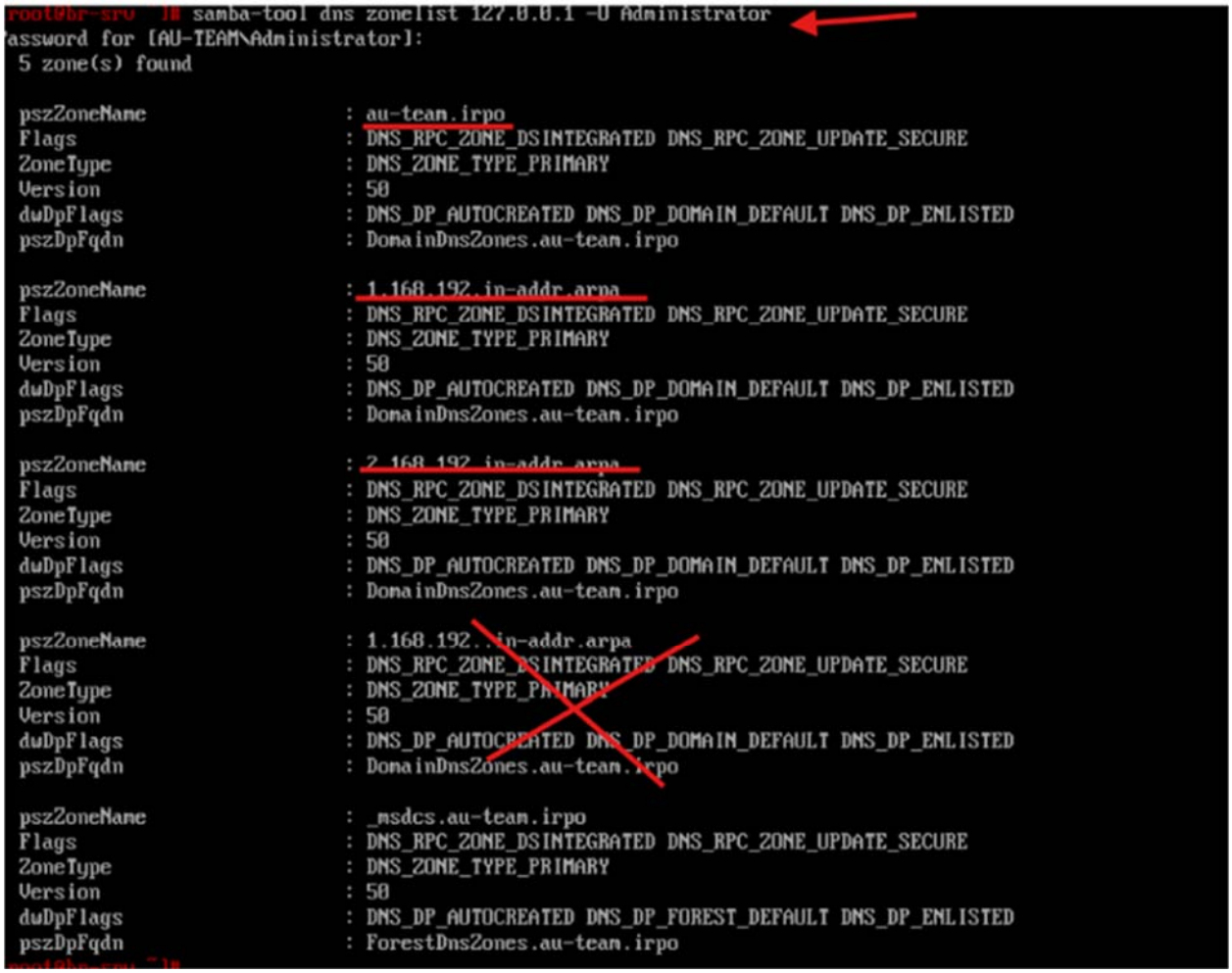
Для сети офиса BR:

samba-tool dns zonecreate 127.0.0.1 2.168.192.in-addr.arpa -U Administrator

Проверяем:

samba-tool dns zonelist 127.0.0.1 -U Administrator

Результат:

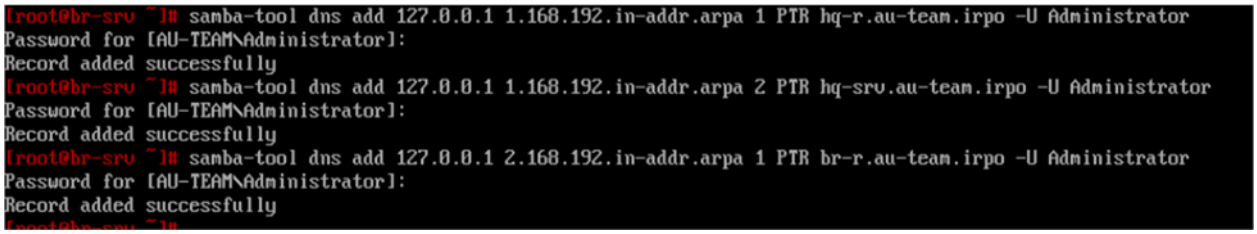


Добавляем записи типа PTR:

samba-tool dns add 127.0.0.1 1.168.192.in-addr.arpa 1 PTR hq-r.au-team.irpo -U Administrator

samba-tool dns add 127.0.0.1 1.168.192.in-addr.arpa 2 PTR hq-srv.au-team.irpo -U Administrator

samba-tool dns add 127.0.0.1 2.168.192.in-addr.arpa 1 PTR br-r.au-team.irpo



Проверяем:

```
[root@br-srv ~]# samba-tool dns query 127.0.0.1 1.168.192.in-addr.arpa @ PTR -U Administrator
Password for [AU-TEAM\Administrator]:
  Name=, Records=0, Children=0
  Name=1, Records=1, Children=0
    PTR: hq-r.au-team.irpo (flags=f0, serial=2, ttl=900)
  Name=2, Records=1, Children=0
    PTR: hq-srv.au-team.irpo (flags=f0, serial=3, ttl=900)
```

```
[root@br-srv ~]# samba-tool dns query 127.0.0.1 2.168.192.in-addr.arpa @ PTR -U Administrator
Password for [AU-TEAM\Administrator]:
  Name=, Records=0, Children=0
  Name=1, Records=1, Children=0
    PTR: br-r.au-team.irpo (flags=f0, serial=2, ttl=900)
[root@br-srv ~]#
```

Добавляем записи типа CNAME - для необходимых сервисов:

samba-tool dns add 127.0.0.1 au-team.irpo wiki CNAME br-srv.au-team.irpo -U administrator

samba-tool dns add 127.0.0.1 au-team.irpo moodle CNAME hq-srv1.au-team.irpo -U administrator

```
root@br-srv ~]# samba-tool dns add 127.0.0.1 au-team.irpo wiki CNAME br-srv.au-team.irpo -U Administrator
assword for [AU-TEAM\Administrator]:
ecord added successfully
root@br-srv ~]# samba-tool dns add 127.0.0.1 au-team.irpo moodle CNAME hq-srv.au-team.irpo -U Administrator
assword for [AU-TEAM\Administrator]:
ecord added successfully
```

Проверяем:

```
[root@br-srv ~]# samba-tool dns query 127.0.0.1  au-team.irpo  @ CNAME -U Administrator
Password for [AU-TEAM\Administrator]:
  Name=, Records=0, Children=0
  Name=_msdcs, Records=0, Children=0
  Name=_sites, Records=0, Children=1
  Name=_tcp, Records=0, Children=4
  Name=_udp, Records=0, Children=2
  Name=br-r, Records=0, Children=0
  Name=br-srv, Records=0, Children=0
  Name=cli, Records=0, Children=0
  Name=DomainDnsZones, Records=0, Children=2
  Name=ForestDnsZones, Records=0, Children=2
  Name=hq-r, Records=0, Children=0
  Name=hq-srv, Records=0, Children=0
  Name=moodle, Records=1, Children=0
    CNAME: hq-srv.au-team.irpo. (flags=f0, serial=22, ttl=900)
  Name=wiki, Records=1, Children=0
    CNAME: br-srv.au-team.irpo. (flags=f0, serial=26, ttl=900)
```

```
[root@br-r ens35]# ping wiki
PING br-srv.au-team.irpo (192.168.2.2) 56(84) bytes of data.
64 bytes from 192.168.2.2: icmp_seq=1 ttl=64 time=0.158 ms
64 bytes from 192.168.2.2: icmp_seq=2 ttl=64 time=0.168 ms
^C
--- br-srv.au-team.irpo ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 0.158/0.163/0.168/0.005 ms
[root@br-r ens35]# ping moodle
PING hq-srv.au-team.irpo (192.168.1.2) 56(84) bytes of data.
64 bytes from hq-srv.au-team.irpo (192.168.1.2): icmp_seq=1 ttl=63 time=0.580 ms
64 bytes from hq-srv.au-team.irpo (192.168.1.2): icmp_seq=2 ttl=63 time=0.559 ms
64 bytes from hq-srv.au-team.irpo (192.168.1.2): icmp_seq=3 ttl=63 time=0.710 ms
64 bytes from hq-srv.au-team.irpo (192.168.1.2): icmp_seq=4 ttl=63 time=0.725 ms
^C
--- hq-srv.au-team.irpo ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3053ms
rtt min/avg/max/mdev = 0.559/0.643/0.725/0.074 ms
[root@br-r ens35]#
```

Создаём группу hq:

samba-tool group add hq

Результат:

```
[root@br-srv ~]# samba-tool group add hq
Added group hq
[root@br-srv ~]#
```

Создаём необходимых пользователей и добавляем их в группу hq:

```
for i in {1..5};
do
  samba-tool user add user$i.hq P@ssw0rd;
  samba-tool user setexpiry user$i.hq --noexpiry;
  samba-tool group addmembers "hq" user$i.hq;
done
```

Проверить:

```
[root@br-srv ~]# samba-tool group listmembers hq
user3.hq
user4.hq
user1.hq
user2.hq
user5.hq
[root@br-srv ~]#
```

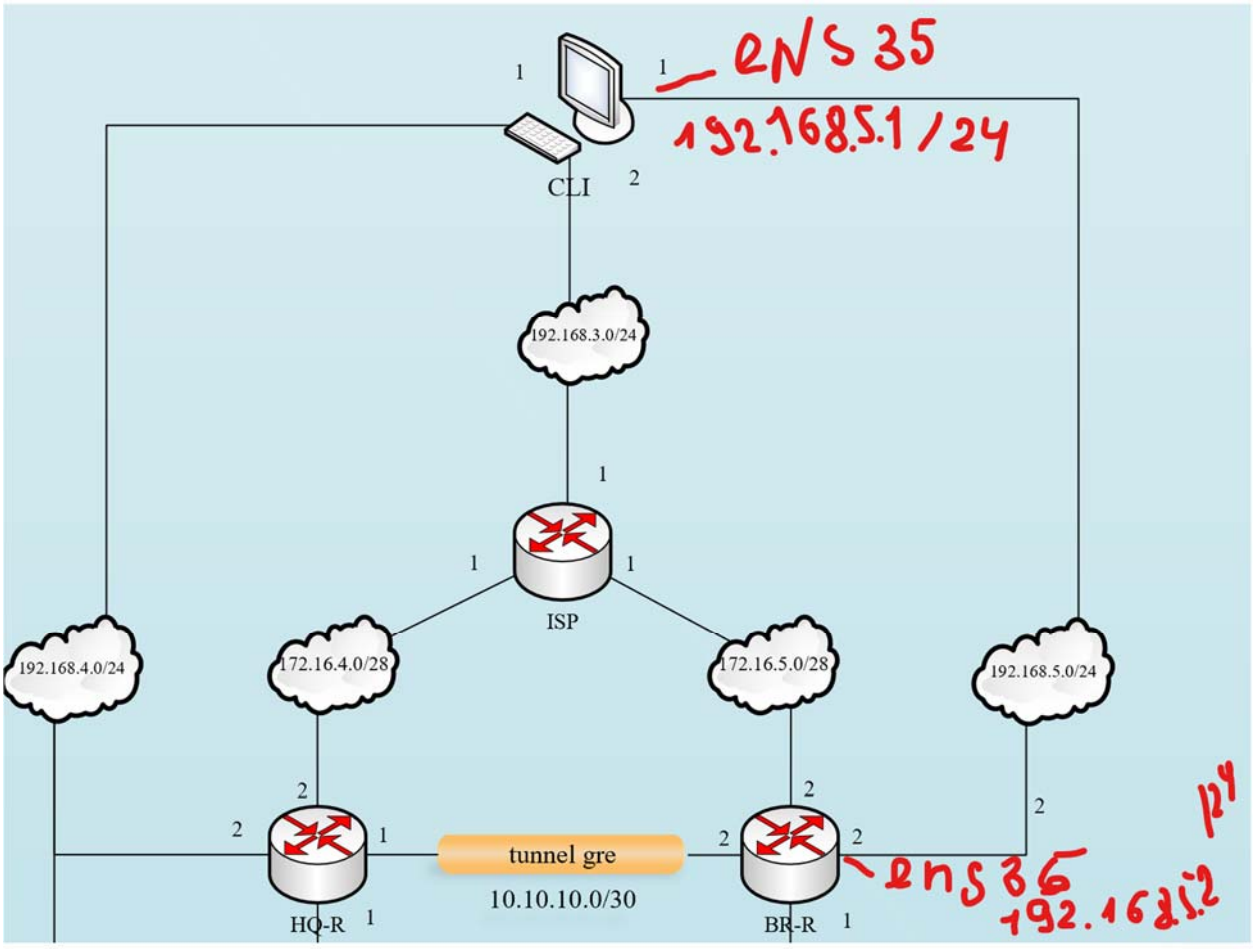
CLI

По заданию необходимо ввести ману CLI в контроллер домена BR-SRV.

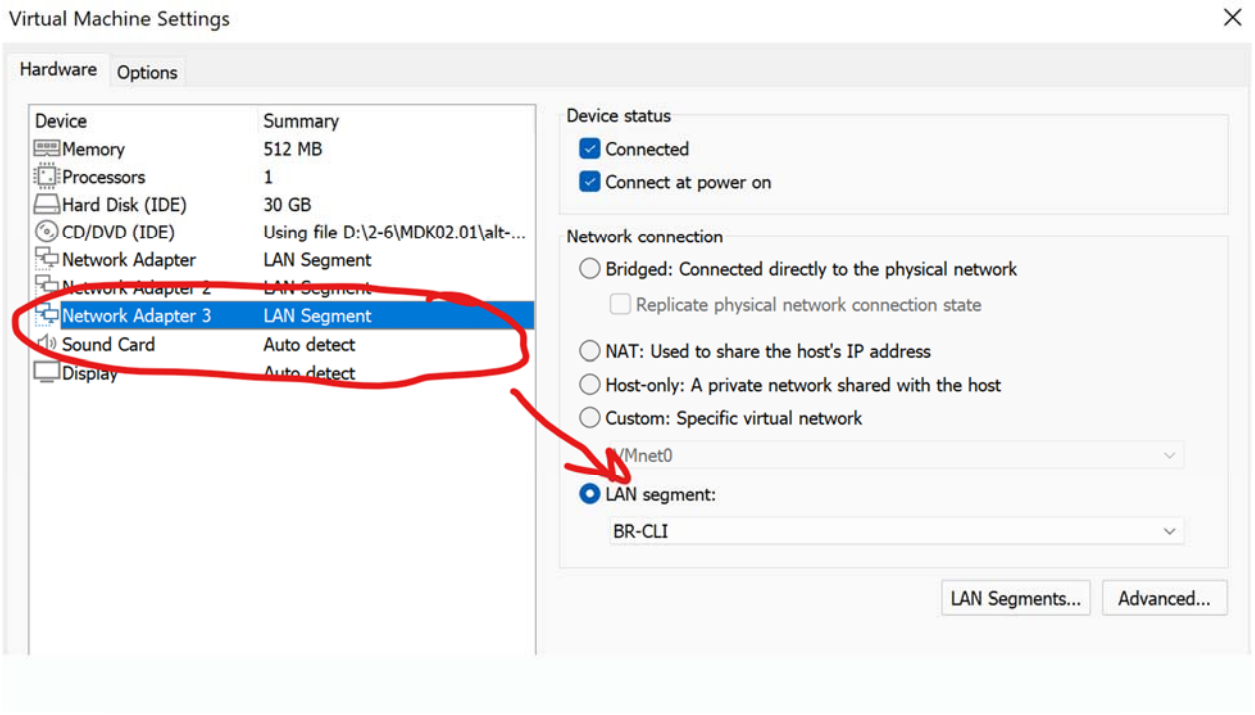
Сложность заключается в том что CLI по временному подключению находится в офисе HQ. Поэтому его надо временно подключить в офис BRANCH.

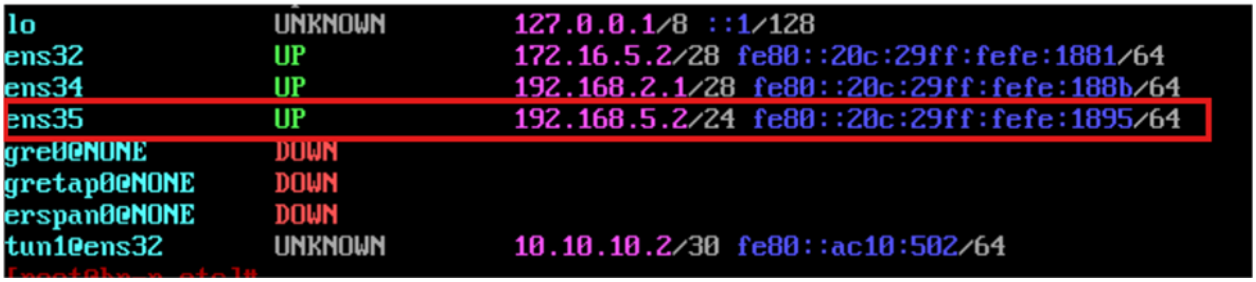
После подключения необходимо проложить маршруты по умолчанию для связности с офисами HQ и BTRANCH.

Создаем временное подключение с офисом BRANCH согласно данной схеме.

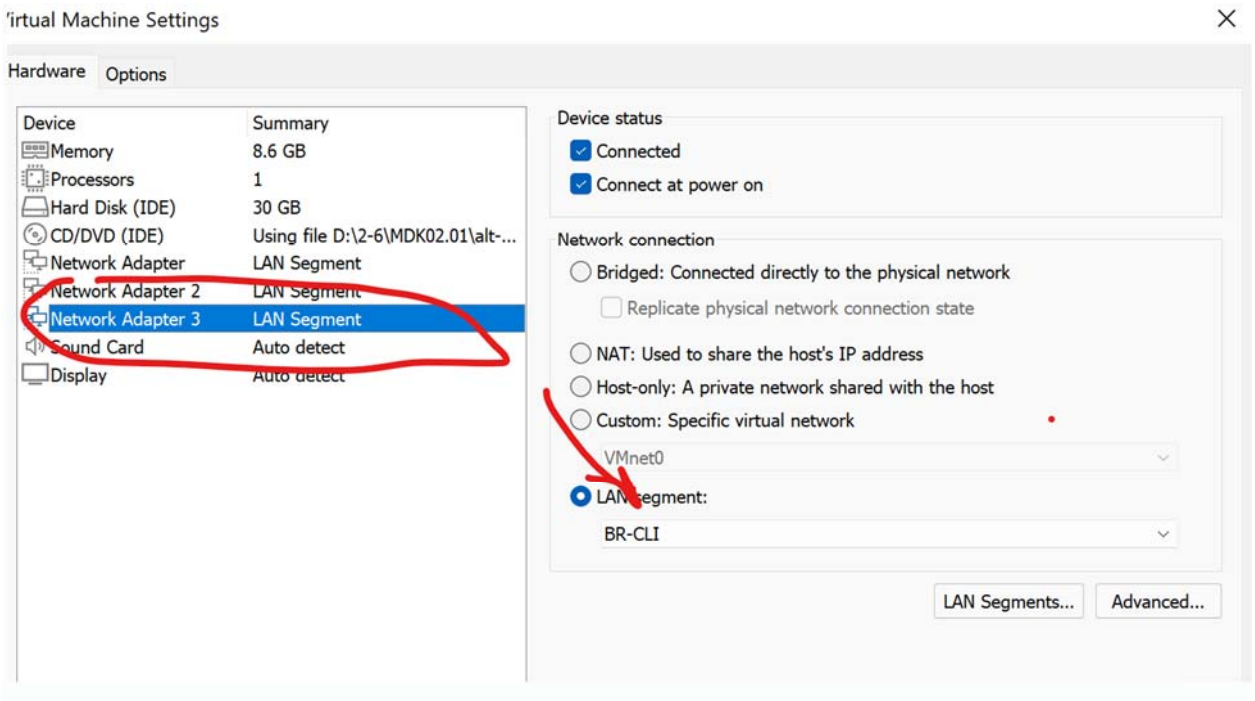


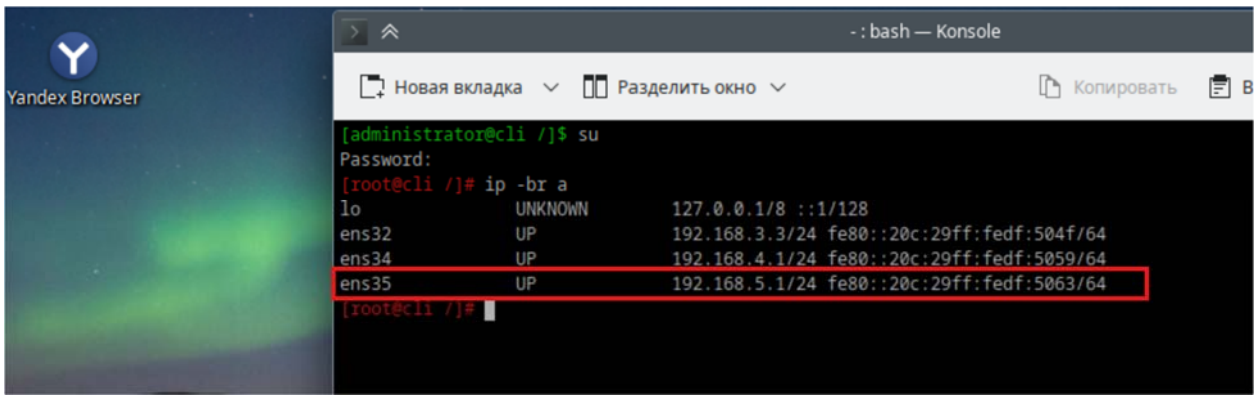
BR-R:


Virtual Machine Settings
Hardware
Options
Device
Summary
Memory
512 MB
Processors
1
Hard Disk (IDE)
30 GB
CD/DVD (IDE)
Using file D:\2-6\MDK02.01\alt-...
Network Adapter
LAN Segment
Network Adapter 3
LAN Segment
Sound Card
Auto detect
Display
Device status
Connected
Connect at power on
Network connection
Bridged: Connected directly to the physical network
Replicate physical network connection state
NAT: Used to share the host's IP address
Host-only: A private network shared with the host
Custom: Specific virtual network
VMnet0
LAN segment:
BR-CLI
LAN Segments...
Advanced...


lo UNKNOWN 127.0.0.1/8 ::1/128
ens32 UP 172.16.5.2/28 fe80::20c:29ff:fefe:1881/64
ens34 UP 192.168.2.1/28 fe80::20c:29ff:fefe:188b/64
ens35 UP 192.168.5.2/24 fe80::20c:29ff:fefe:1895/64
gre0@NONE DOWN
gretap0@NONE DOWN
erspan0@NONE DOWN
tun1@ens32 UNKNOWN 10.10.10.2/30 fe80::ac10:502/64

CLI:


'irtual Machine Settings
Hardware
Options
Device
Summary
Memory
8.6 GB
Processors
1
Hard Disk (IDE)
30 GB
CD/DVD (IDE)
Using file D:\2-6\MDK02.01\alt-...
Network Adapter
LAN Segment
Network Adapter 2
LAN Segment
Network Adapter 3
LAN Segment
Sound Card
Auto detect
Display
Device status
Connected
Connect at power on
Network connection
Bridged: Connected directly to the physical network
Replicate physical network connection state
NAT: Used to share the host's IP address
Host-only: A private network shared with the host
Custom: Specific virtual network
VMnet0
LAN segment:
BR-CLI
LAN Segments...
Advanced...



Прокладываем маршруты по умолчанию:

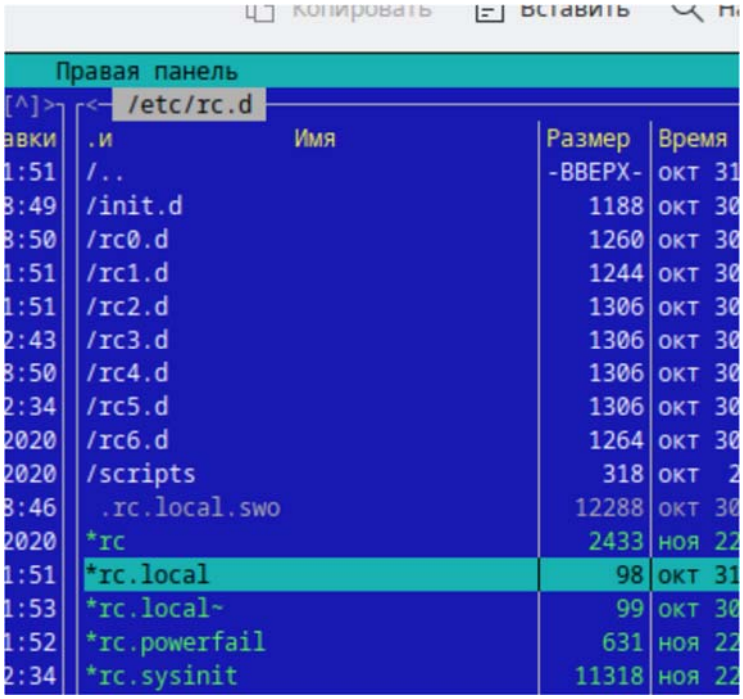
1 вариант rc.local

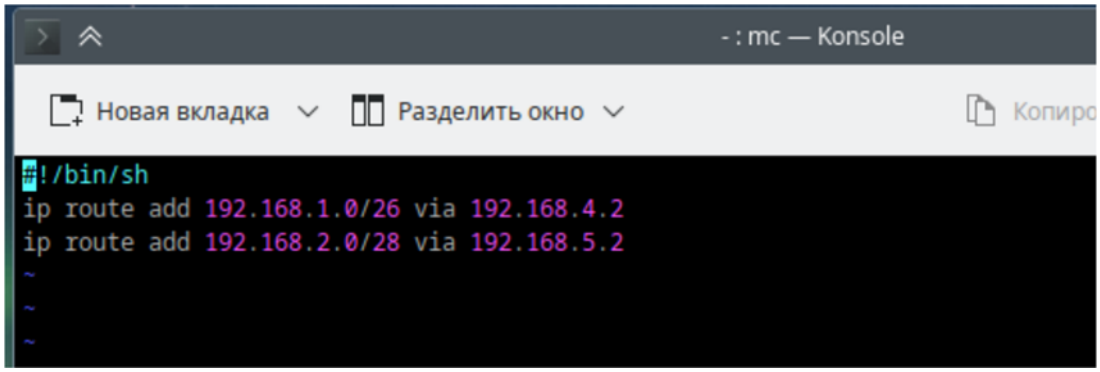
Для создания файла /etc/rc.d/rc.local можно применить следующие команды (с правами пользователя root):

echo '#!/bin/sh' > /etc/rc.d/rc.local

chmod +x /etc/rc.d/rc.local

После чего в этот файл можно помещать команды, которые необходимо выполнить после запуска системы. Однако в 95% случаев то, что вы собираетесь записать в этот файл, имеет более подходящее место в системе

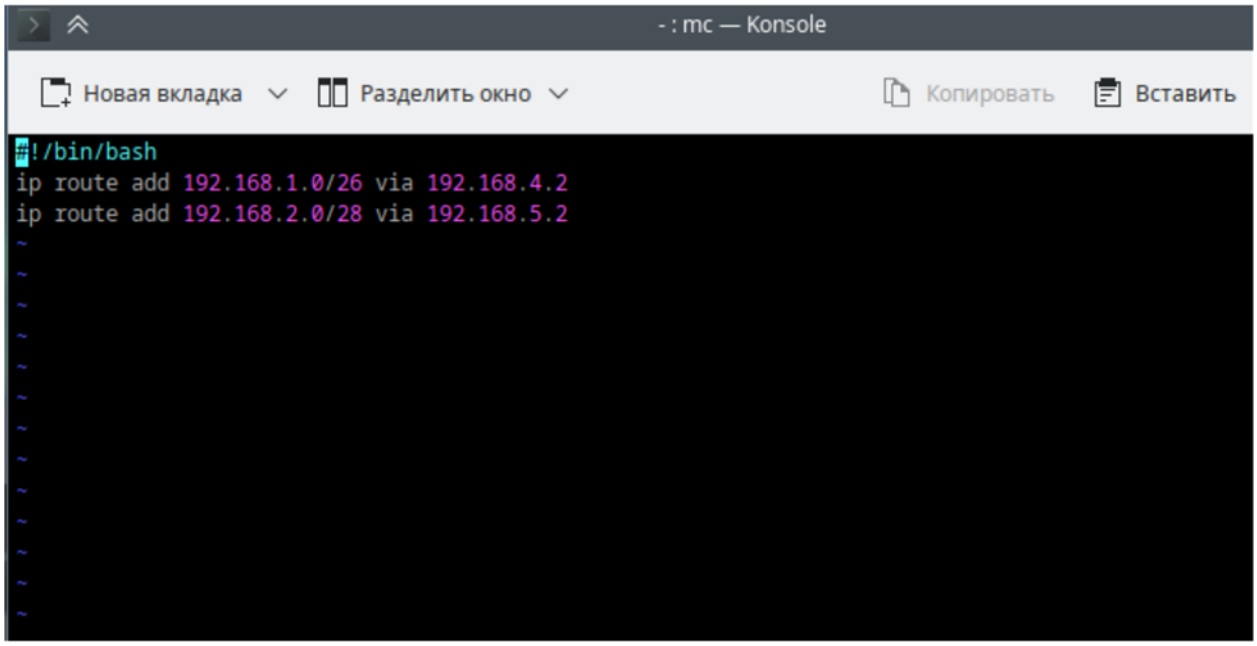




2 вариант crontabe

Создадим простой bash-скрипт:

vim rc.local.sh



Назначаем права на исполнения для данного файла:

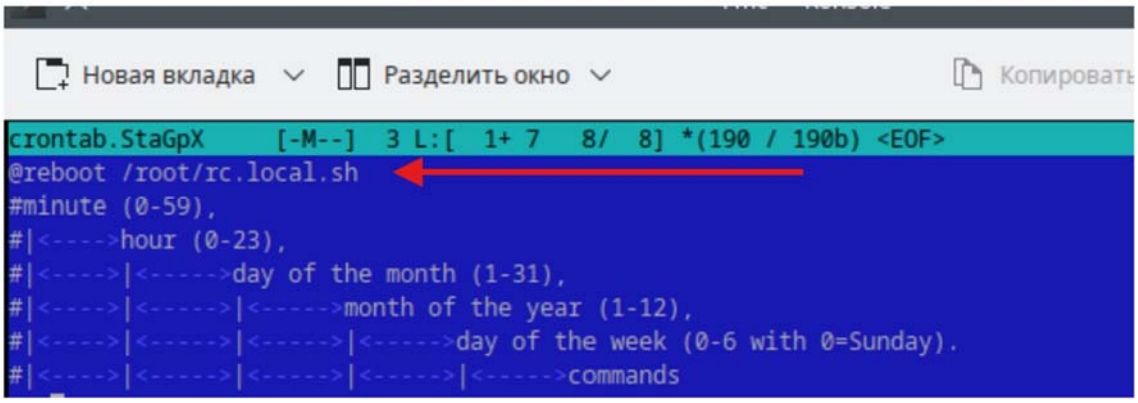
chmod +x rc.local.sh

где:

#!/bin/bash: Эта строка - это шебанг (shebang), она указывает на то, какую оболочку следует использовать для выполнения скрипта. В данном случае, скрипт выполняется с использованием оболочки Bash.

Помещаем скрипт в автозагрузку

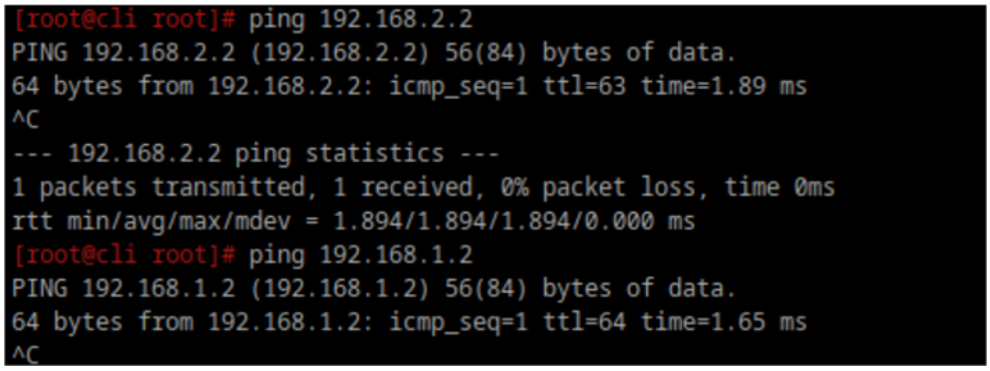
#crontab -e



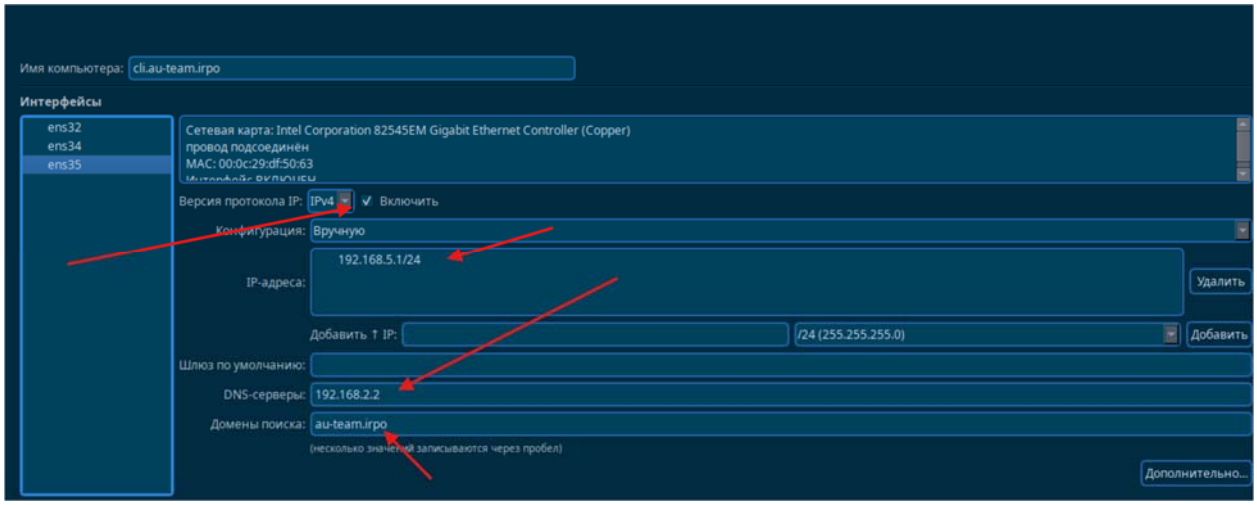
Проверяем

#./rc.local.sh

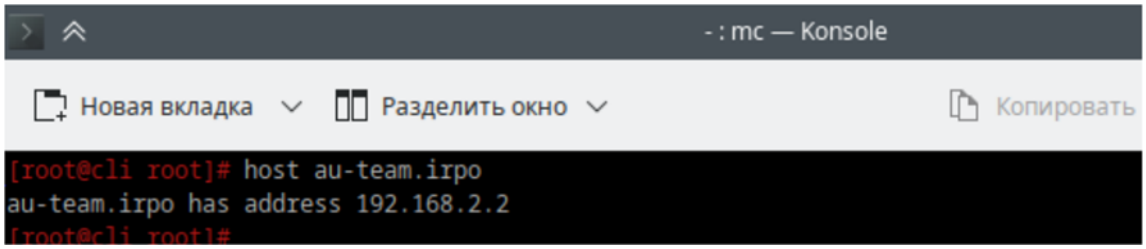
Проверка:



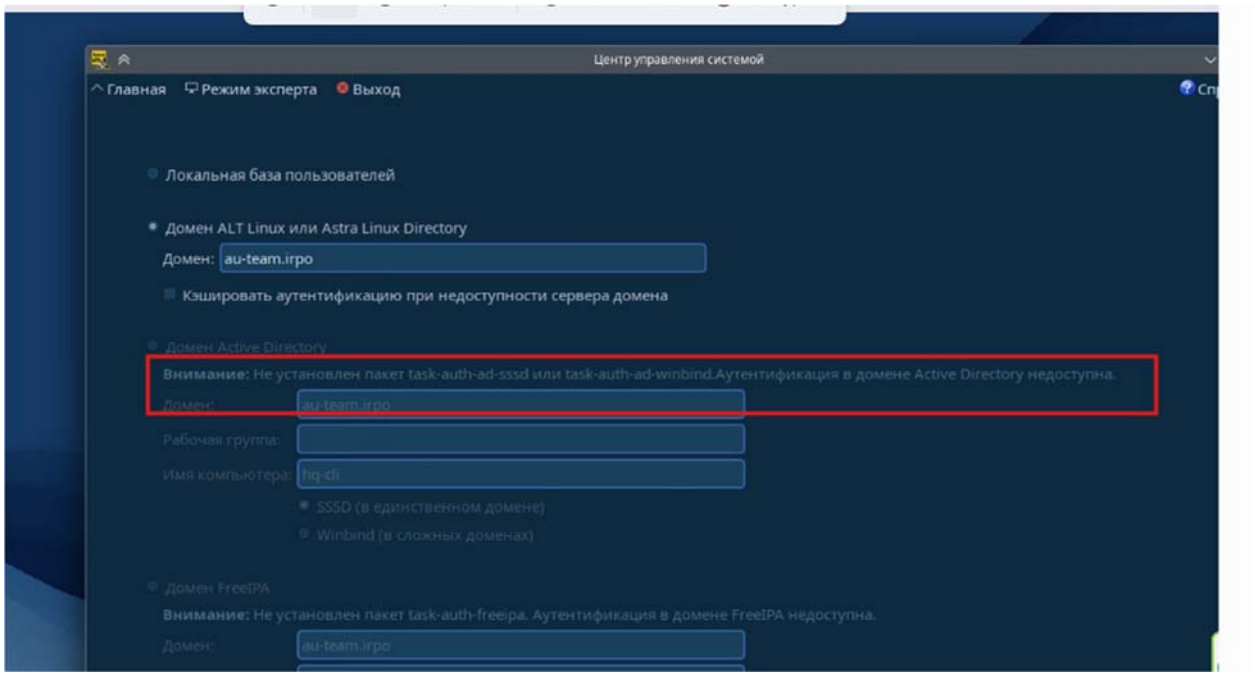
Для того чтобы ввести CLI в домен - задаём статические параметры адресации, чтобы явно указать в качестве DNS-сервера IP-адрес BR-SRV, или же правим данный параметр на DHCP-сервере:

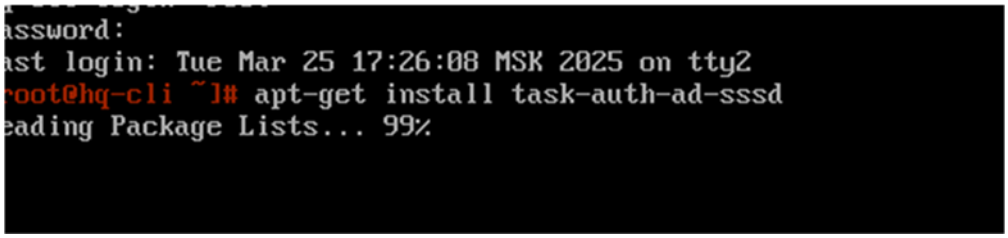


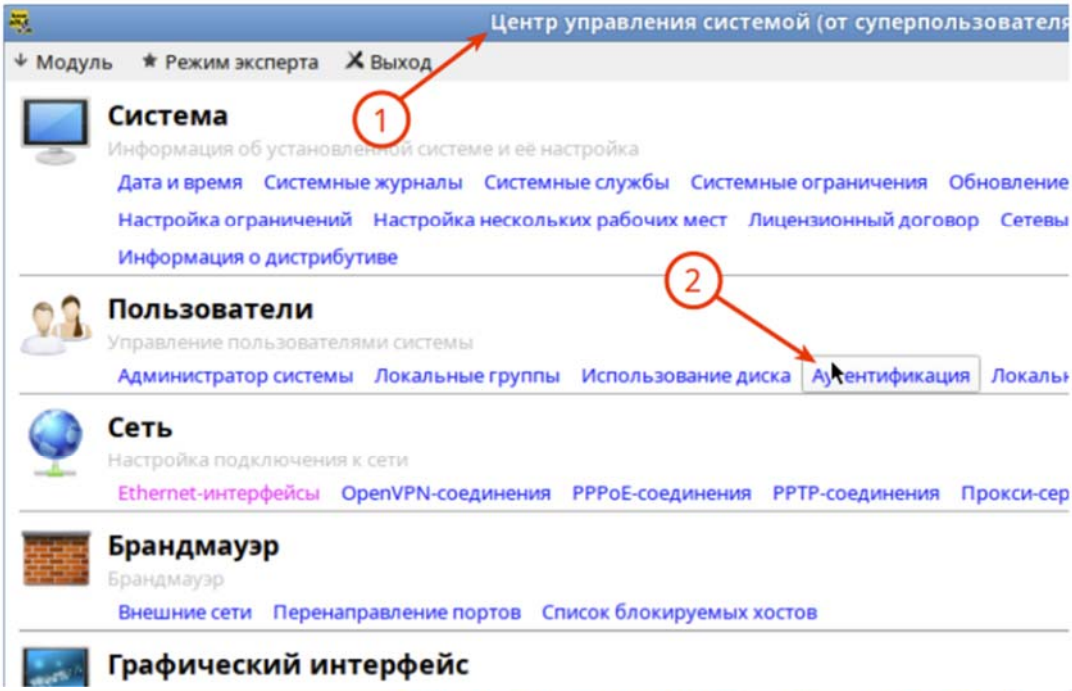
Проверить:

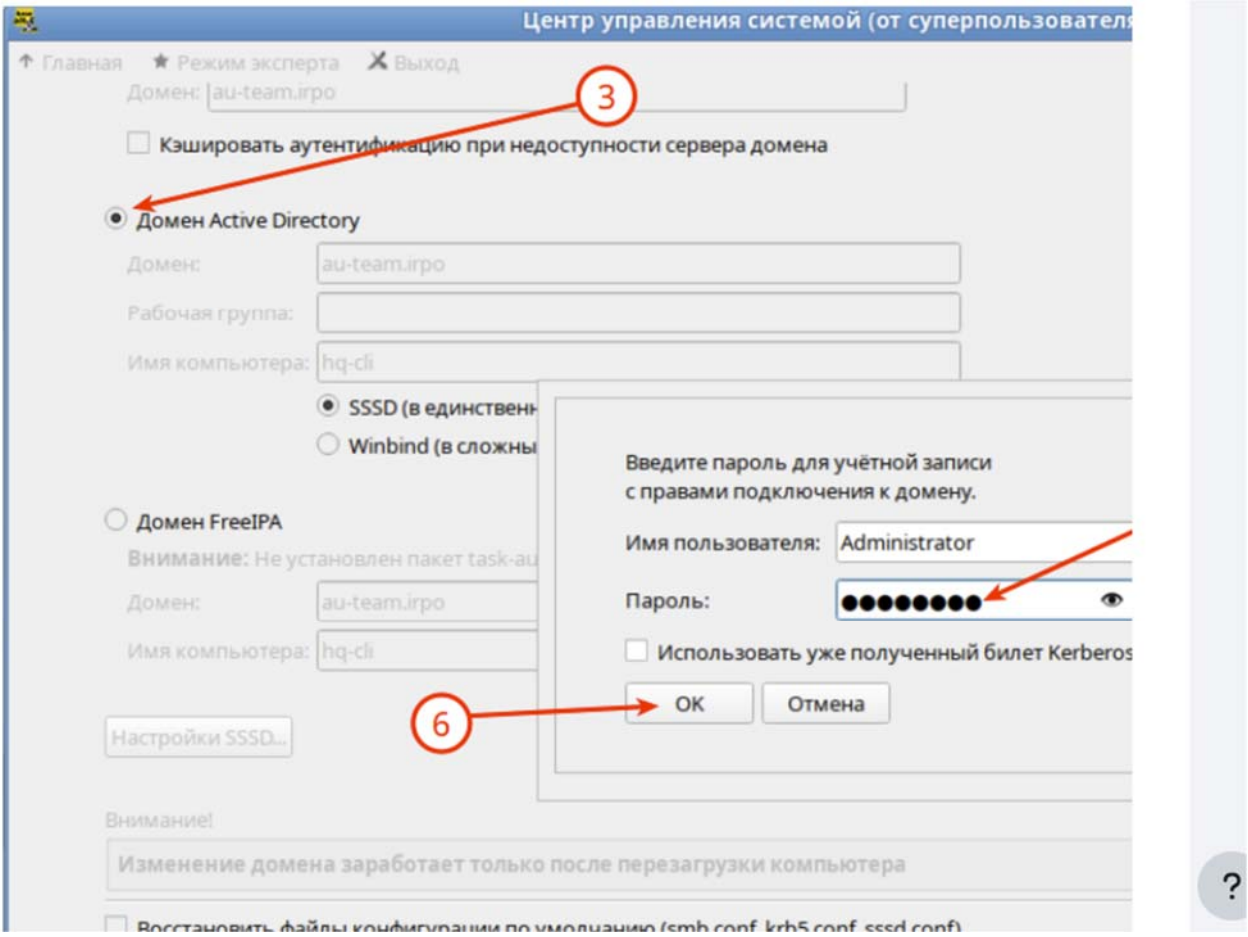


Используя Центр Управления Системой (ЦУС) вводим CLI в домен:



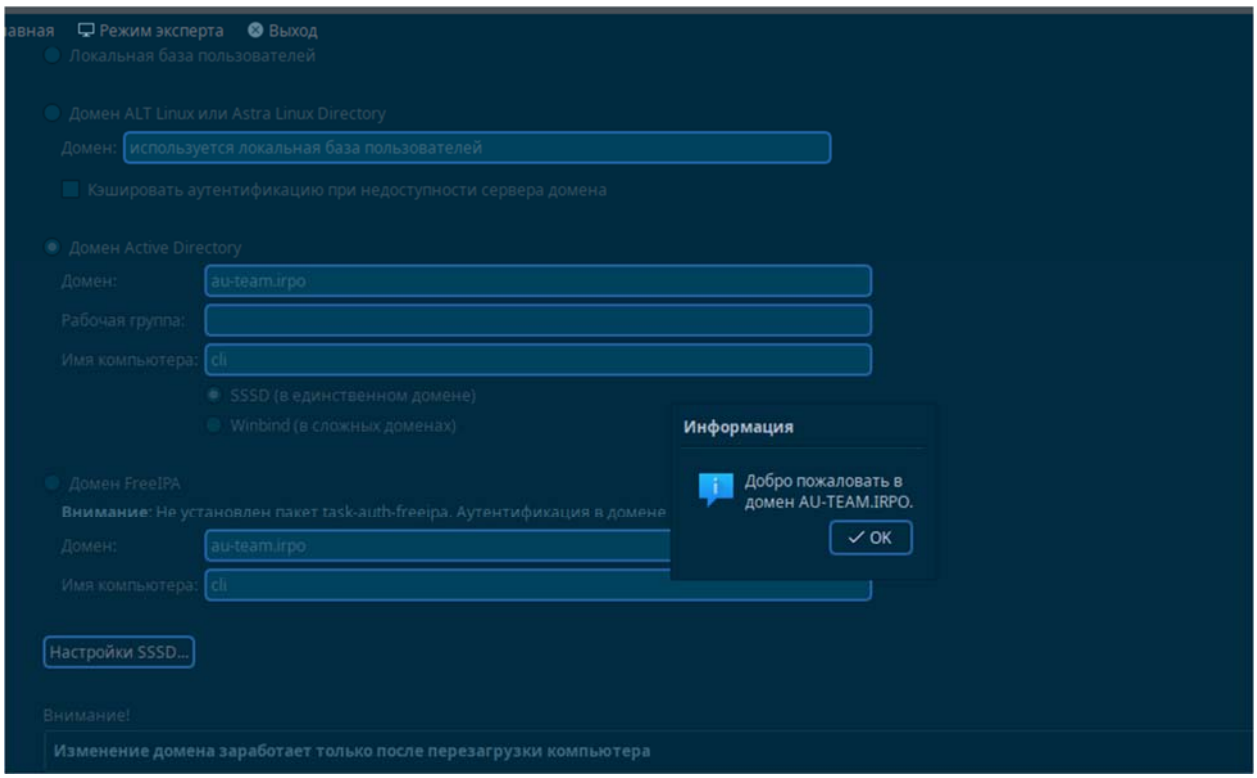




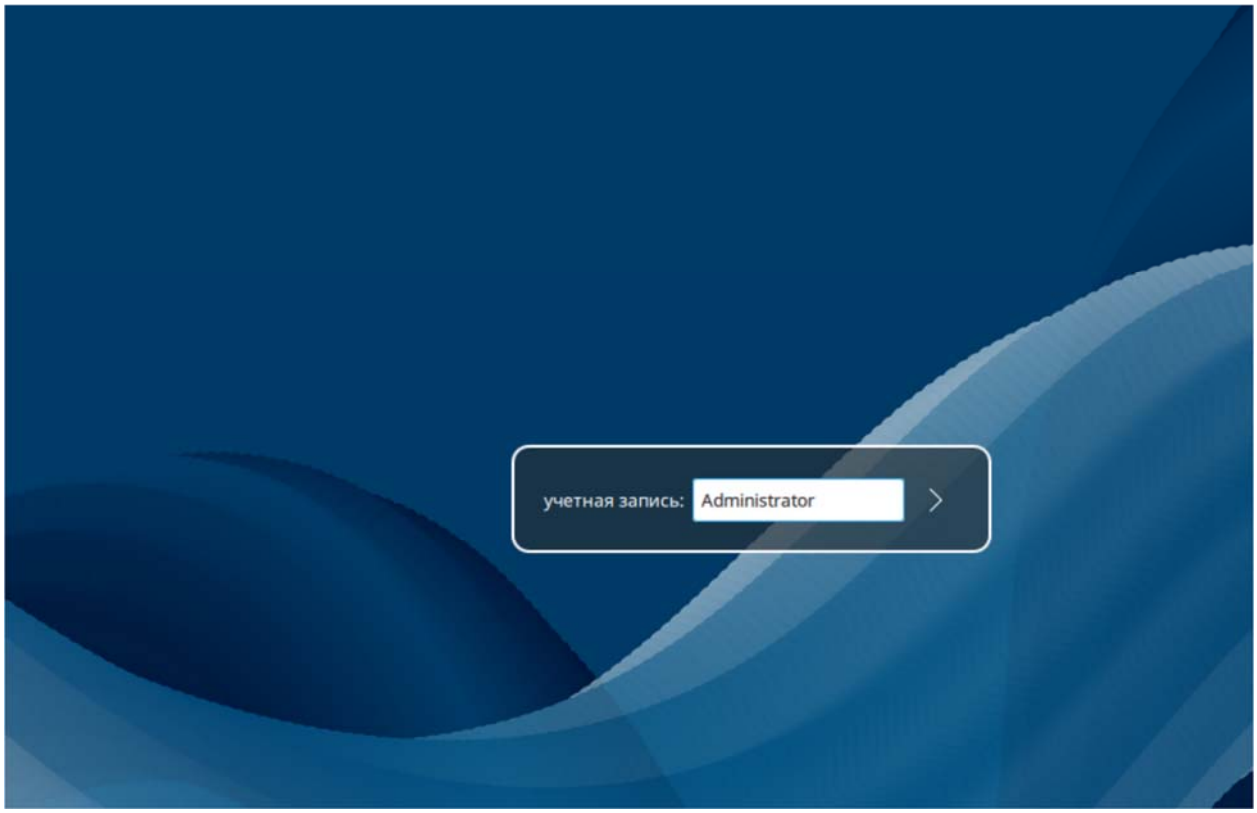


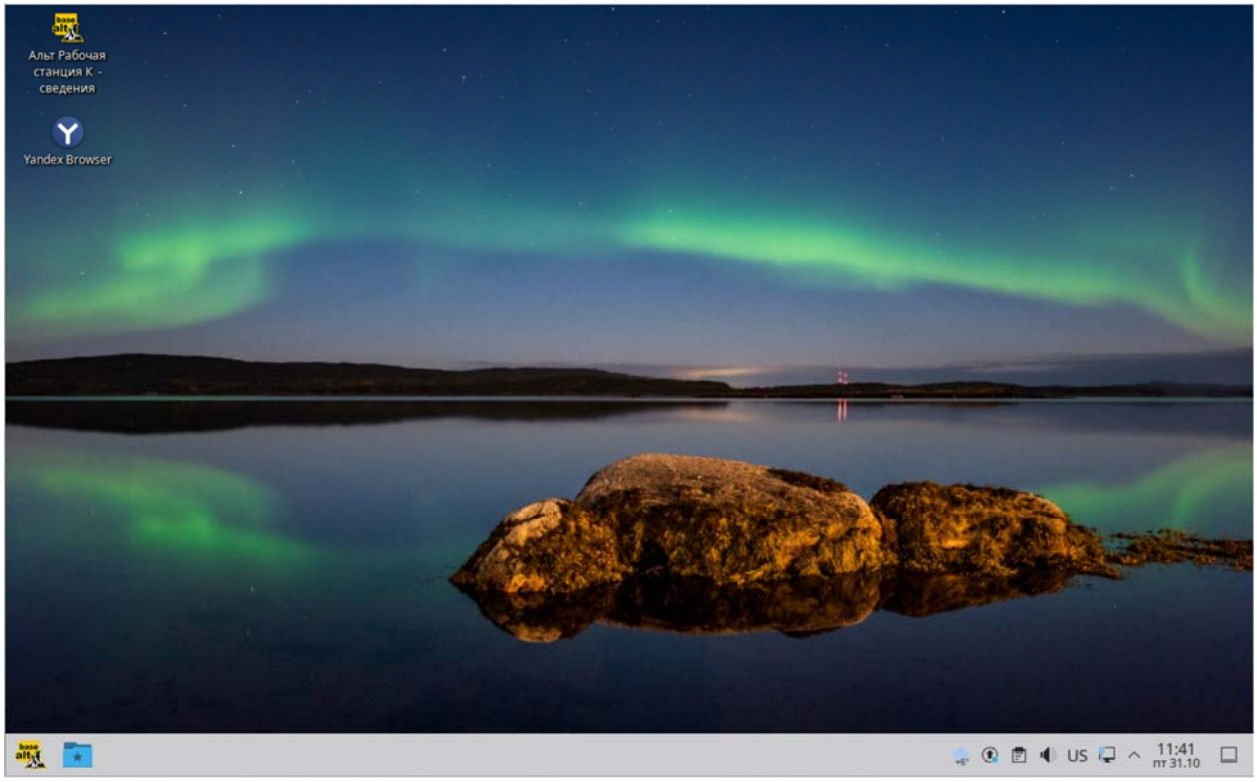
Результат:

необходимо перезагрузить виртуальную машину HQ-CLI:

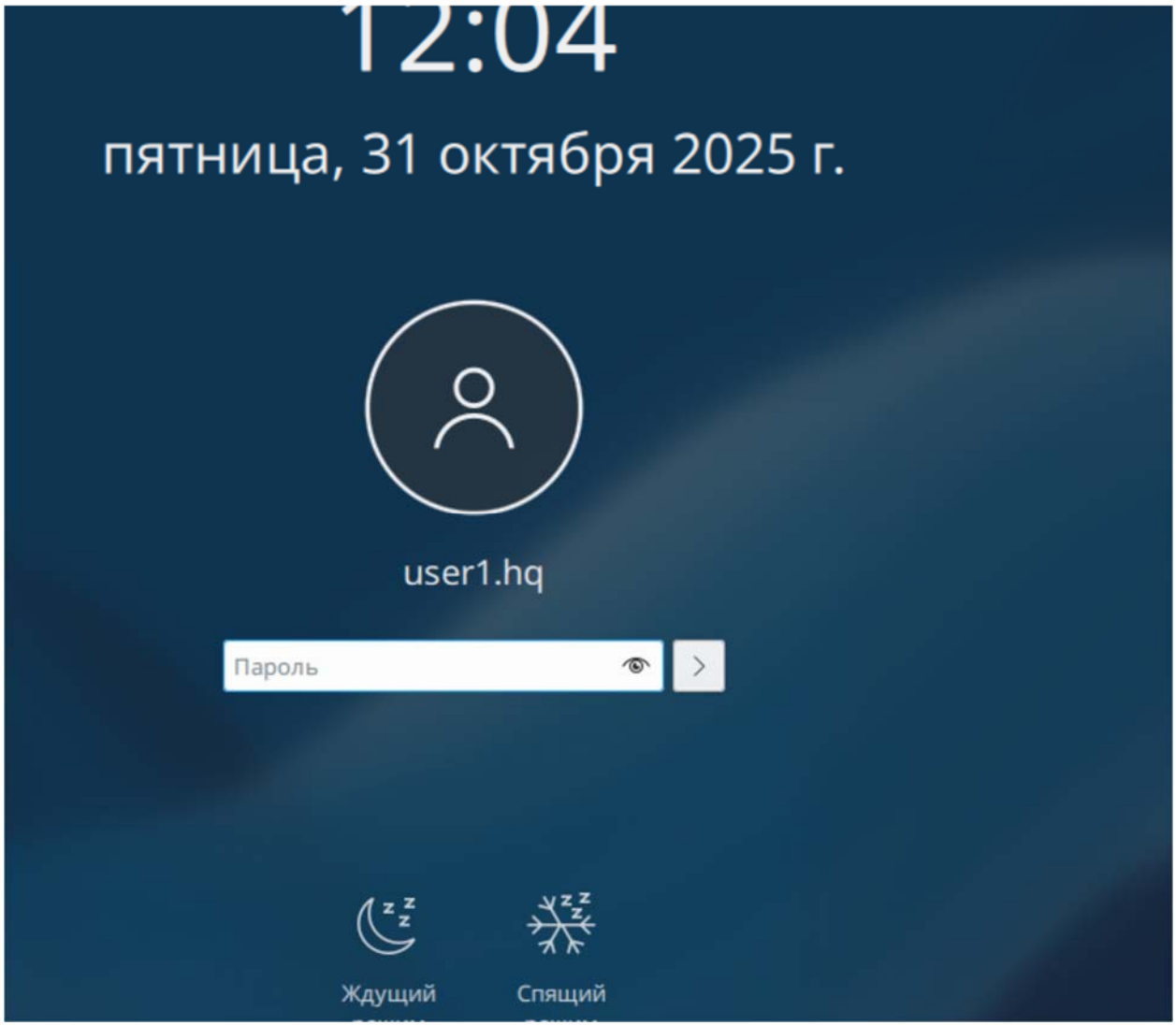


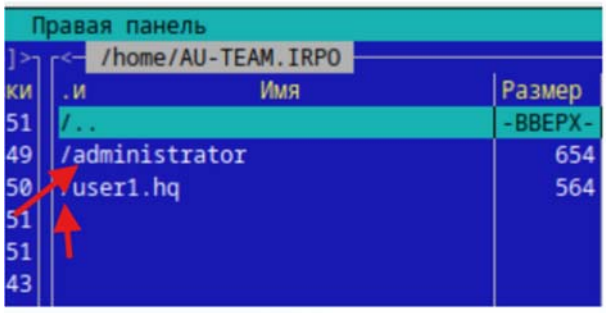
Зайдем на машину CLI под логином Administrator





Проверяем пользователя user1.hq





5.2 Запустите сервис moodle на сервере HQ-SRV1

Применение сервера Moodle в системе дистанционного образования

Введение

Цифровая трансформация образования стала одним из ключевых трендов XXI века, а дистанционное обучение превратилось из альтернативной формы в неотъемлемый компонент образовательного процесса. Этому способствовали как глобальные вызовы, так и объективное стремление к повышению доступности и гибкости образования. В этих условиях особую значимость приобретают системы управления обучением (LMS – Learning Management System). Среди них платформа Moodle (Modular Object-Oriented Dynamic Learning Environment) занимает лидирующие позиции благодаря своей открытости, гибкости и мощному функционалу. Применение сервера Moodle в системе дистанционного образования создает robustную, масштабируемую и педагогически ориентированную среду, которая эффективно решает задачи организации, доставки и контроля учебного контента.

1. Moodle как организационно-содержательный хаб образовательного процесса

Основная роль сервера Moodle заключается в структурировании и централизации всего учебного процесса. Он выступает в роли виртуального кампуса, где сосредоточены все необходимые ресурсы и инструменты.

Централизованное хранение материалов. Преподаватели могут размещать учебные материалы в различных форматах: лекции в виде текстовых документов (PDF, Word), презентаций, видео- и аудиозаписей, ссылок на внешние ресурсы. Это позволяет студенту в любое время иметь доступ к единой базе знаний, что является

фундаментом для асинхронного обучения.

Организация деятельности по времени. Используя такие элементы, как «Задание», «Форум», «Тест», «Лекция», преподаватель может выстраивать четкую временную линию курса. Настройка сроков сдачи заданий и открытия/закрытия модулей дисциплинирует студентов и помогает им рационально распределять время, что критически важно в условиях отсутствия очных встреч.

Коммуникационная платформа. Moodle предоставляет встроенные инструменты для синхронного и асинхронного общения. Форумы для обсуждений, личные сообщения, комментарии к заданиям и элементам курса создают образовательное сообщество, нивелируя эффект изоляции, присущий дистанционному формату. Преподаватель перестает быть удаленным и недоступным источником информации, превращаясь в модератора и наставника.

2. Инструменты оценки и контроля: от тестирования к формирующему оцениванию

Одна из самых сильных сторон Moodle – это мощный арсенал средств для оценки знаний и прогресса студентов.

Автоматизированное тестирование. Модуль «Тест» позволяет создавать вопросы различных типов (множественный выбор, верно/неверно, на соответствие, короткий ответ, эссе и др.). Система автоматически проверяет большинство из них, обеспечивая мгновенную обратную связь и значительно экономя время преподавателя. Возможность ограничения по времени, перемешивания вопросов и вариантов ответов повышает объективность оценки.

Разнообразие форматов сдачи работ. Элемент «Задание» позволяет студентам сдавать работы в виде файлов (документы, презентации, код), текста, введенного непосредственно в окне редактора, или даже аудио-/видеозаписей. Преподаватель может оценить работу, оставить развернутый комментарий непосредственно в системе, установить баллы и критерии оценивания (вплоть до использования рубрик).

Формирующее оценивание. Moodle поддерживает концепцию непрерывного обучения. Такие инструменты, как «Семинар» (Workshop), позволяют организовать взаимное рецензирование работ студентами, что развивает критическое мышление и

навыки самооценки. Журнал оценок, доступный и студенту, и преподавателю, дает наглядную картину успеваемости и помогает своевременно выявлять проблемы.

3. Гибкость, адаптивность и экономическая эффективность

Применение сервера Moodle выходит за рамки чисто технической реализации, оказывая влияние на педагогический дизайн и экономику образования.

Педагогическая гибкость. Платформа не навязывает единственно верную методику преподавания. Она является инструментом, который можно адаптировать под различные педагогические подходы: от традиционной знаниево-ориентированной модели до современных методов, таких как смешанное обучение (blended learning), перевернутый класс (flipped classroom) и проектная деятельность.

Масштабируемость. Установленный на собственном сервере (или арендованном виртуальном хостинге), Moodle может обслуживать как небольшую группу студентов (десятки человек), так и крупный университет или корпорацию (сотни тысяч пользователей). Это делает решение универсальным.

Экономическая целесообразность. Являясь open-source решением, Moodle не требует лицензионных отчислений. Затраты организации сводятся в основном к технической поддержке сервера и, возможно, кастомизации платформы. Это делает качественное дистанционное образование доступным для образовательных учреждений с разным бюджетом.

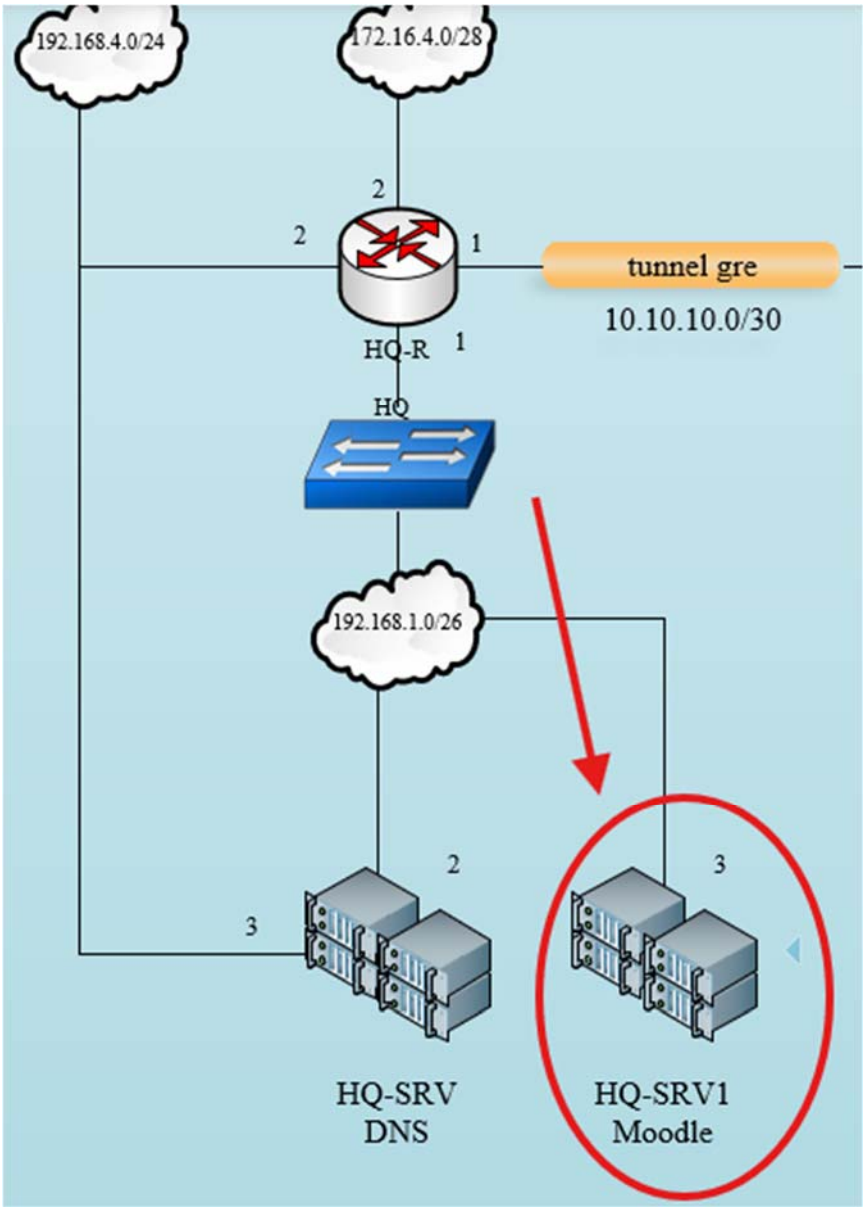
Заключение

Таким образом, сервер Moodle представляет собой не просто программное обеспечение, а целостную экосистему для построения эффективной системы дистанционного образования. Он успешно интегрирует в себе функции организации контента, управления учебным процессом, обеспечения коммуникации и всесторонней оценки знаний. Его открытый код, модульная архитектура и ориентация на социально-конструктивистскую педагогическую модель делают его идеальным выбором для образовательных учреждений, стремящихся идти в ногу со временем. Применение Moodle позволяет преодолеть пространственные и временные барьеры, обеспечивая при этом высокий уровень интерактивности, контроля и, в конечном счете, качества образования, что полностью соответствует вызовам

современной цифровой эпохи.

Установка

Добавляем в сеть машину HQ-SRV1



IPv4: 192.168.1.3/26

getway: 192.18.1.1

dns: 192.168.2.2

Задание:

Используйте веб-сервер apache

В качестве системы управления базами данных используйте mariadb

Создайте базу данных moodledb

Создайте пользователя moodle с паролем P@ssw0rd и предоставьте ему права

доступа к этой базе данных

У пользователя admin в системе обучения задайте пароль P@ssw0rd

На главной странице должен отражаться номер рабочего места в виде арабской цифры, других подписей делать не надо

Основные параметры отметьте в отчёте

Вариант реализации:

HQ-SRV1:

Устанавливаем необходимые пакеты:

moodle — код Moodle. По зависимостям вытягивает php8.2 и необходимые модули

moodle-apache2 — настройки apache2 для работы Moodle. По зависимостям вытягивает apache2 и apache2-mod_php8.2

apt-get install -y moodle moodle-apache2

Устанавливаем MariaDB:

apt-get install -y mariadb-server php8.2-mysqlnd-mysqli

Включаем и добавляем в автозагрузку:

systemctl enable --now mariadb

Создание базы данных и пользователя с правами на базу данных:

mariadb -u root

Создание базы данных:

CREATE DATABASE moodledb;

Создание пользователя:

CREATE USER 'moodle'@'%' IDENTIFIED BY 'P@ssw0rd';

Назначаем пользователю moodle права на полный доступ к базе данных moodledb:

GRANT ALL PRIVILEGES ON moodledb.* TO 'moodle'@'%' WITH GRANT OPTION;

Редактируем значение параметра max_input_vars:

sed -i "s/; max_input_vars = 1000/max_input_vars = 5000/g" /etc/php/8.2/apache2-mod_php/php.ini

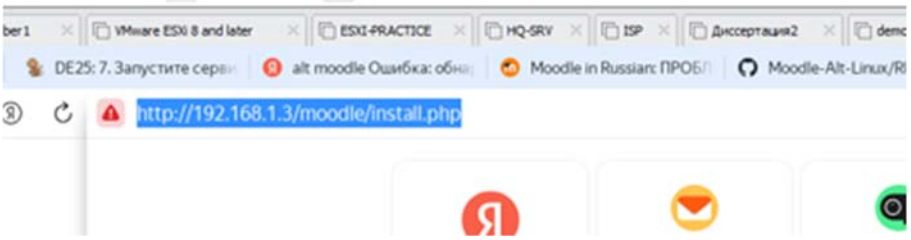
Включаем и добавляем в автозагрузку службу httpd2:

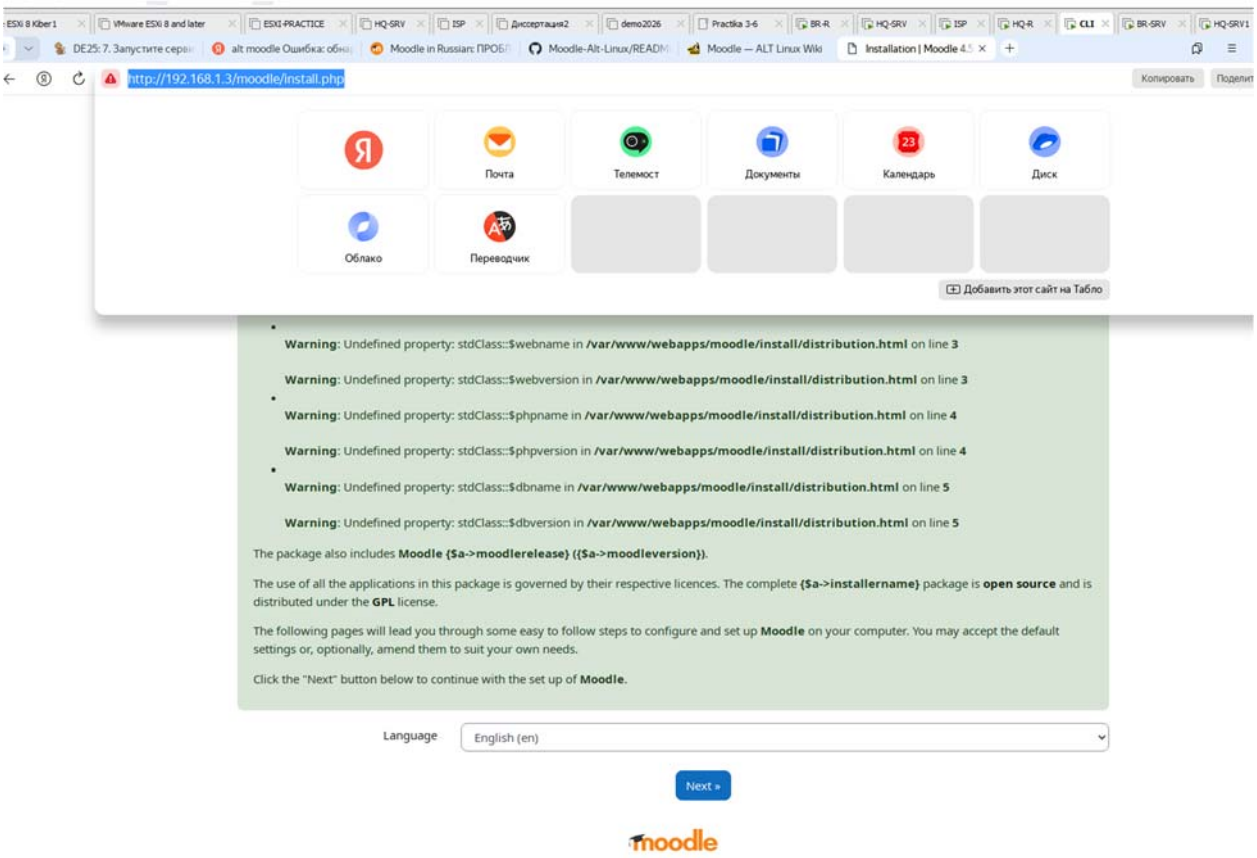
systemctl enable --now httpd2

CLI:

Переходим в браузере по http://<IP-адрес_HQ-SRV>/moodle:

Выполняем дальнейшую установку средствами веб-интерфейса:





Установка

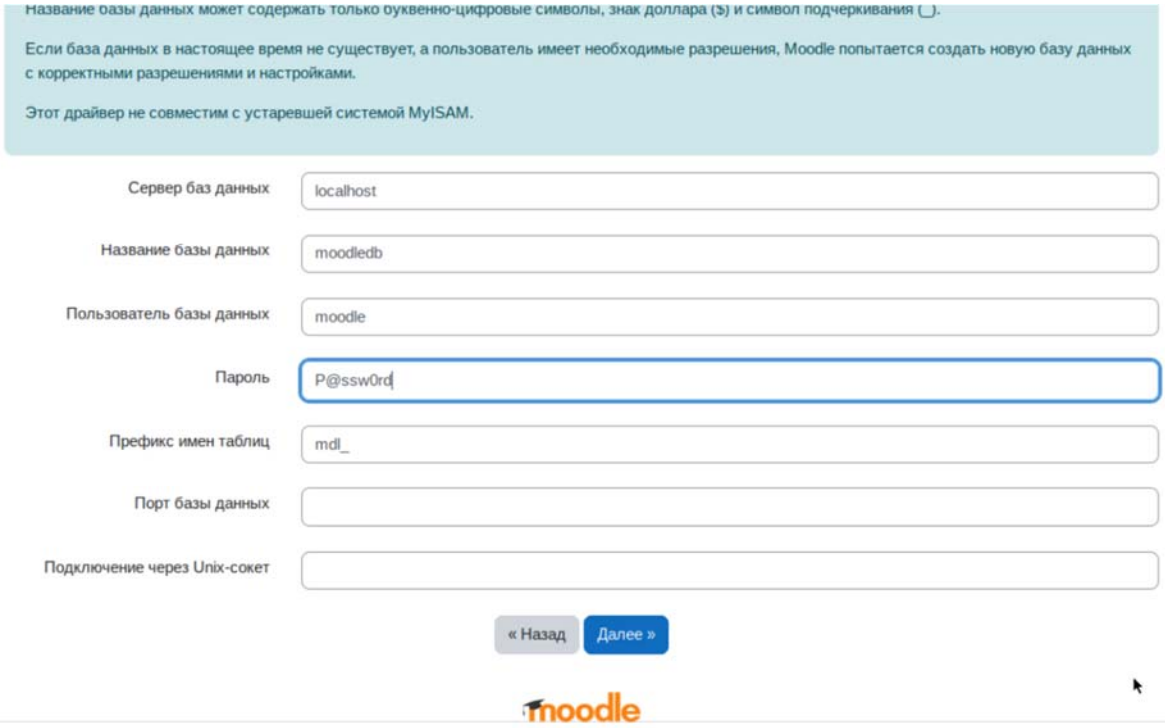
Moodle - Modular Object-Oriented Dynamic Learning Environment

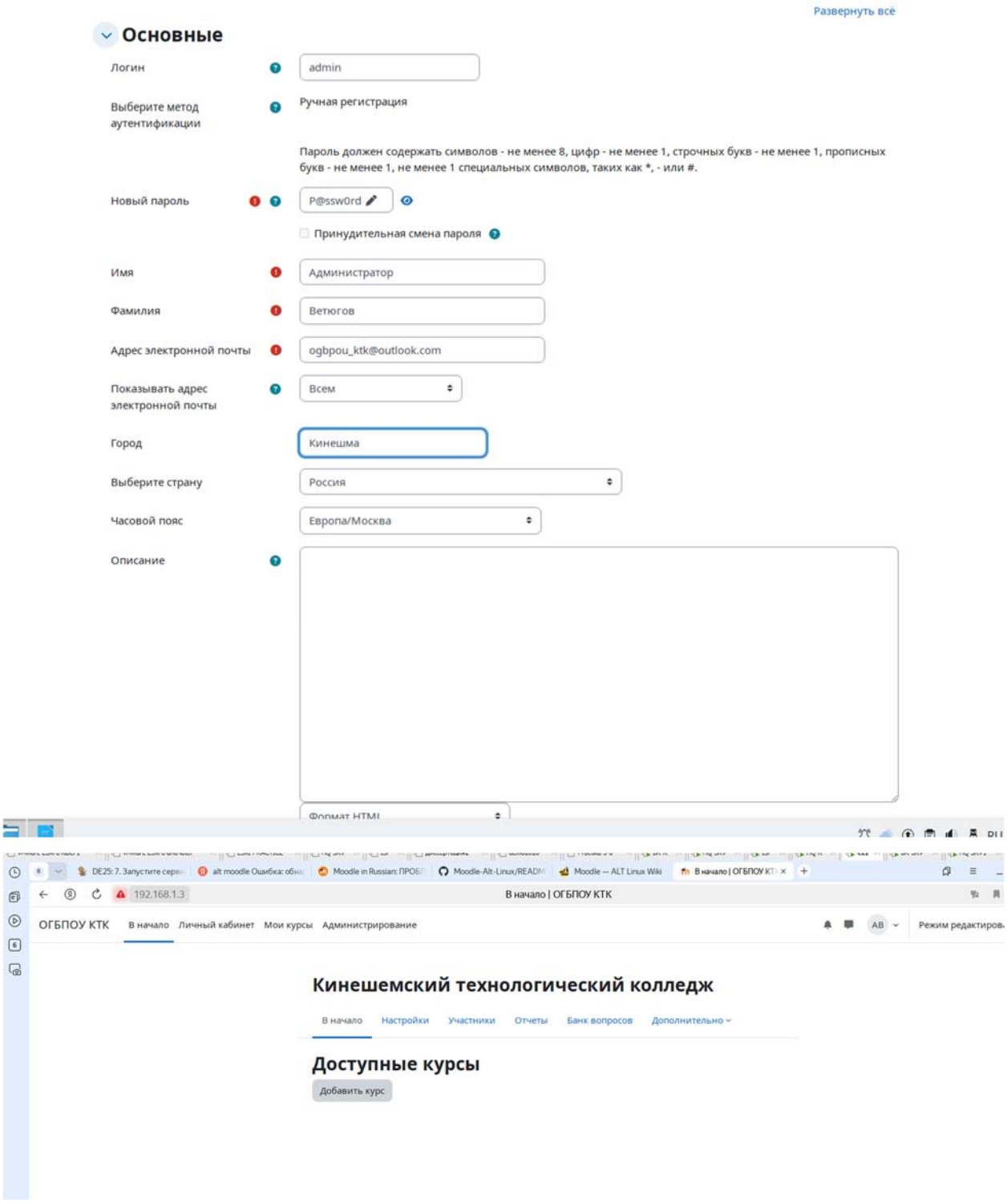
Заметка об авторском праве

Подтвердить

Прочитали ли Вы эти условия и поняли их?

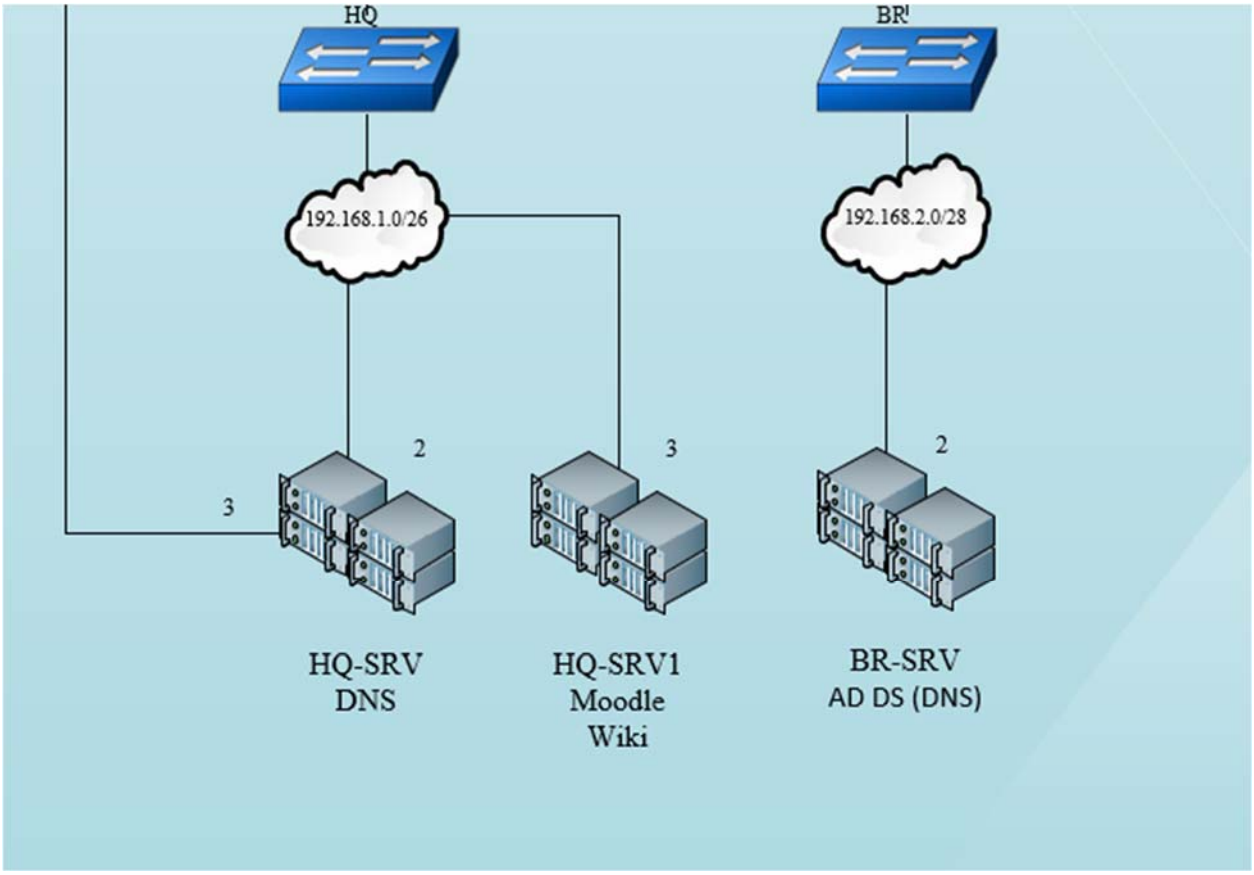
Отмена | Продолжить





Задание: Настроить свою специальность и курс

Развертывание приложений в Docker на сервере HQ-SRV1



Задание:

Создайте в домашней директории пользователя файл wiki.yml для приложения MediaWiki.

Средствами docker compose должен создаваться стек контейнеров с приложением MediaWiki и базой данных.

Используйте два сервиса

Основной контейнер MediaWiki должен называться wiki и использовать образ mediawiki

Файл LocalSettings.php с корректными настройками должен находиться в домашней папке пользователя и автоматически монтироваться в образ.

Контейнер с базой данных должен называться mariadb и использовать образ mariadb.

Он должен создавать базу с названием mediawiki, доступную по стандартному порту, пользователя wiki с паролем WikiP@ssw0rd должен иметь права доступа к этой базе данных

MediaWiki должна быть доступна извне через порт 8080.

Вариант реализации:

BR-SRV1:

Устанавливаем **Docker** и **Docker Compose**:

apt-get install -y docker-{engine,compose-v2}

Включаем и добавляем в автозагрузку службу **docker**:

systemctl enable --now docker.service

В домашней директории пользователя **root** создаём файл **wiki.yml** со следующим содержимым:

vim ~/wiki.yml

Добавляем следующую информацию, где:

services — основной раздел, где мы будем создавать и описывать наши сервисы (контейнеры docker). В данном примере сервиса два: **MediaWiki** - для приложения mediawiki и **database** - для базы данных;

container_name — имя, которое получит созданный контейнер;

image — имя образа, который будет использоваться для создания контейнера;

restart — поведения контейнера при падении;

ports (внешняя публикация). С помощью данной опции мы можем указывать, на каких портах должен слушать контейнер и на какие порты должны пробрасываться запросы;

environment — задаем переменные окружения;

volumes - проброс папок;

links - ссылайтесь на контейнеры в другом сервисе. Укажите либо имя сервиса, либо псевдоним ссылки (SERVICE:ALIAS), либо просто имя сервиса.

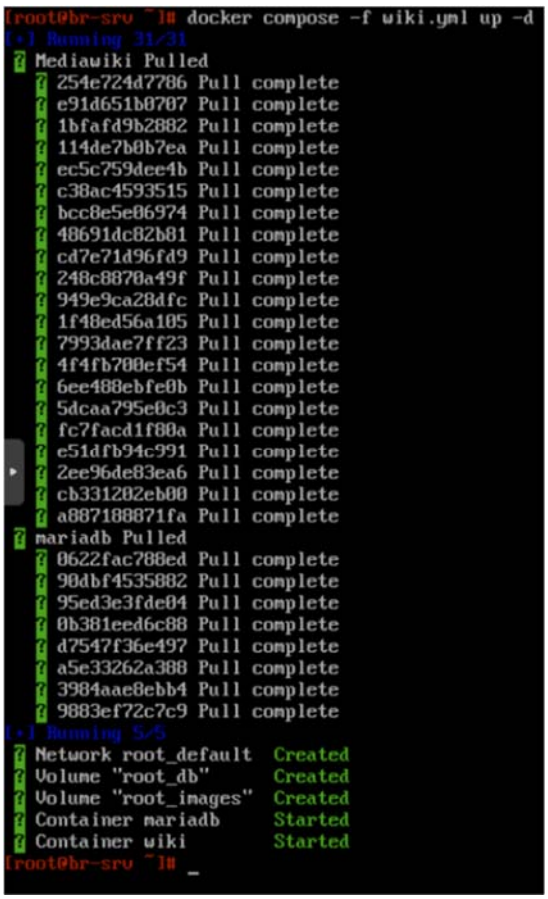
```
services:
  Mediawiki:
    container_name: wiki
    image: mediawiki
    restart: always
    ports:
```

```
      - 8080:80
    links:
      - mariadb
    volumes:
      - images:/var/www/html/images
      # - ./LocalSettings.php:/var/www/html/LocalSettings.php

  mariadb:
    container_name: mariadb
    image: mariadb
    restart: always
    environment:
      MYSQL_DATABASE: mediawiki
      MYSQL_USER: wiki
      MYSQL_PASSWORD: WikiP@ssw0rd
      MYSQL_RANDOM_ROOT_PASSWORD: 'yes'
    volumes:
      - db:/var/lib/mysql

volumes:
  images:
  db:
```

Выполняем сборку и запуск стека контейнеров с приложением MediaWiki и базой данных описанных в файле wiki.yml:

docker compose -f wiki.yml up -d

Результат:



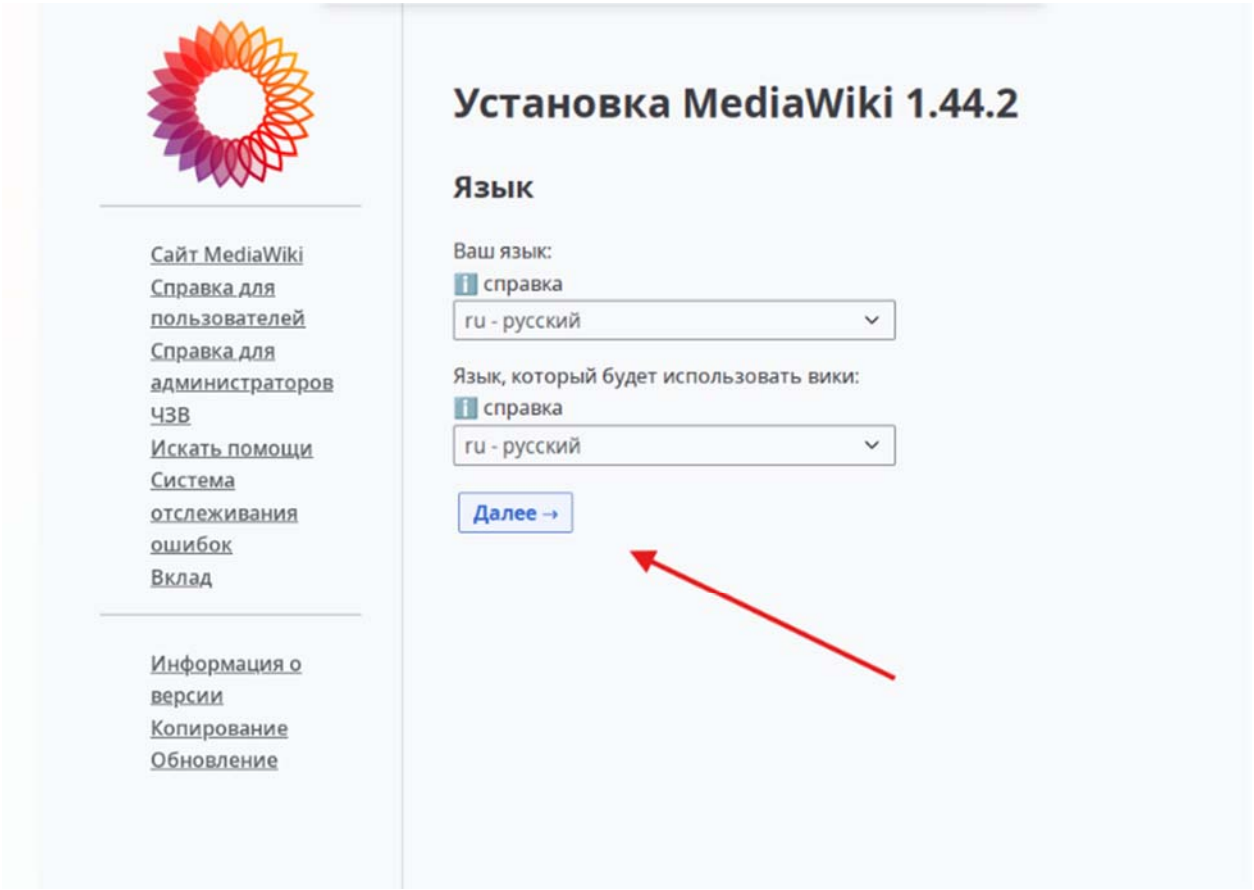
Проверить:

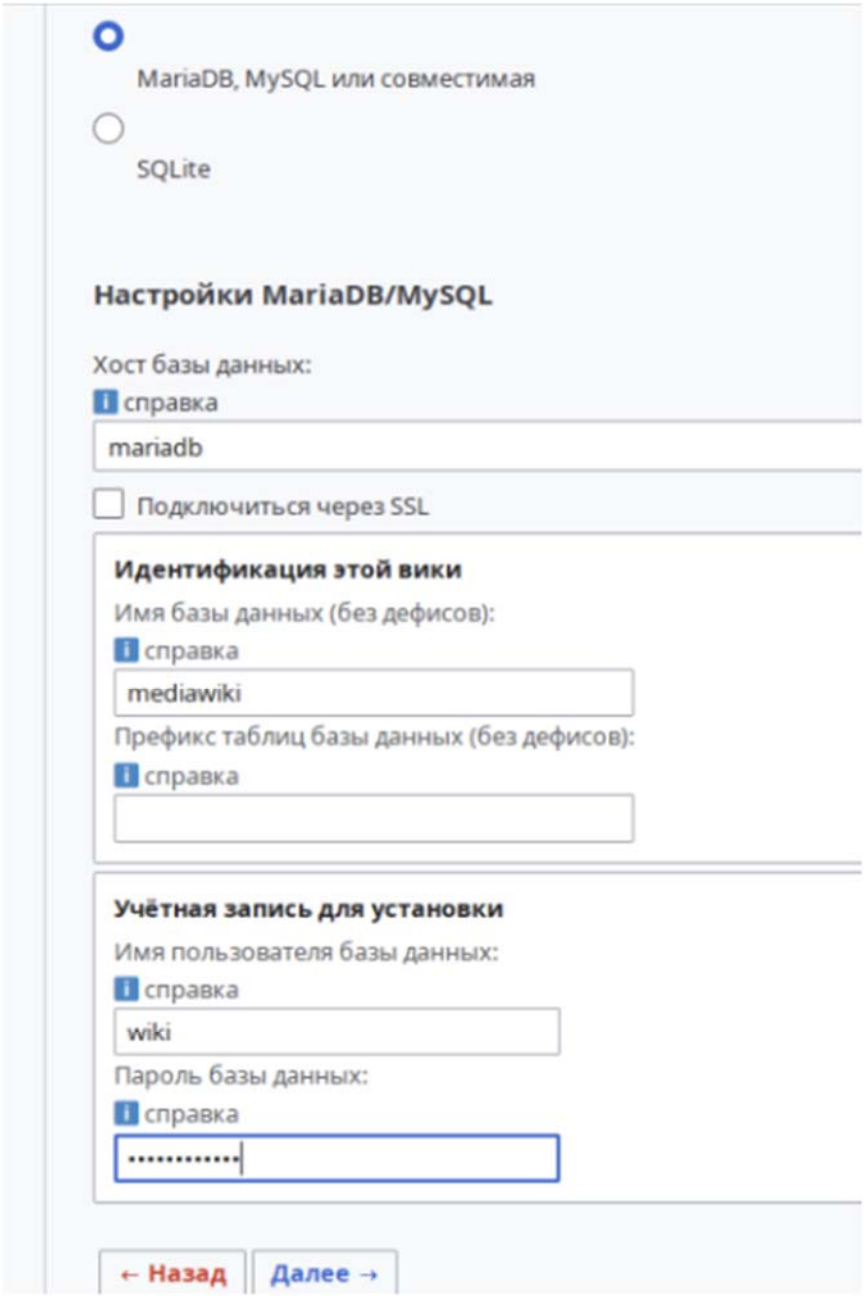
Проверить:

CLI:

Переходим в браузер с **CLI** http://<IP-адрес_BR-SRV1>:8080 для продолжения установки через веб-интерфейс - нажимаем **set up the wiki**:


DE25: 5. Развертывание
Telegram Web
192.168.1.3:8080 — Янде
MediaWiki 1.44.2
192.168.1.3:8080
MediaWiki 1.44.2
MediaWiki 1.44.2
LocalSettings.php not found.
Please set up the wiki first.

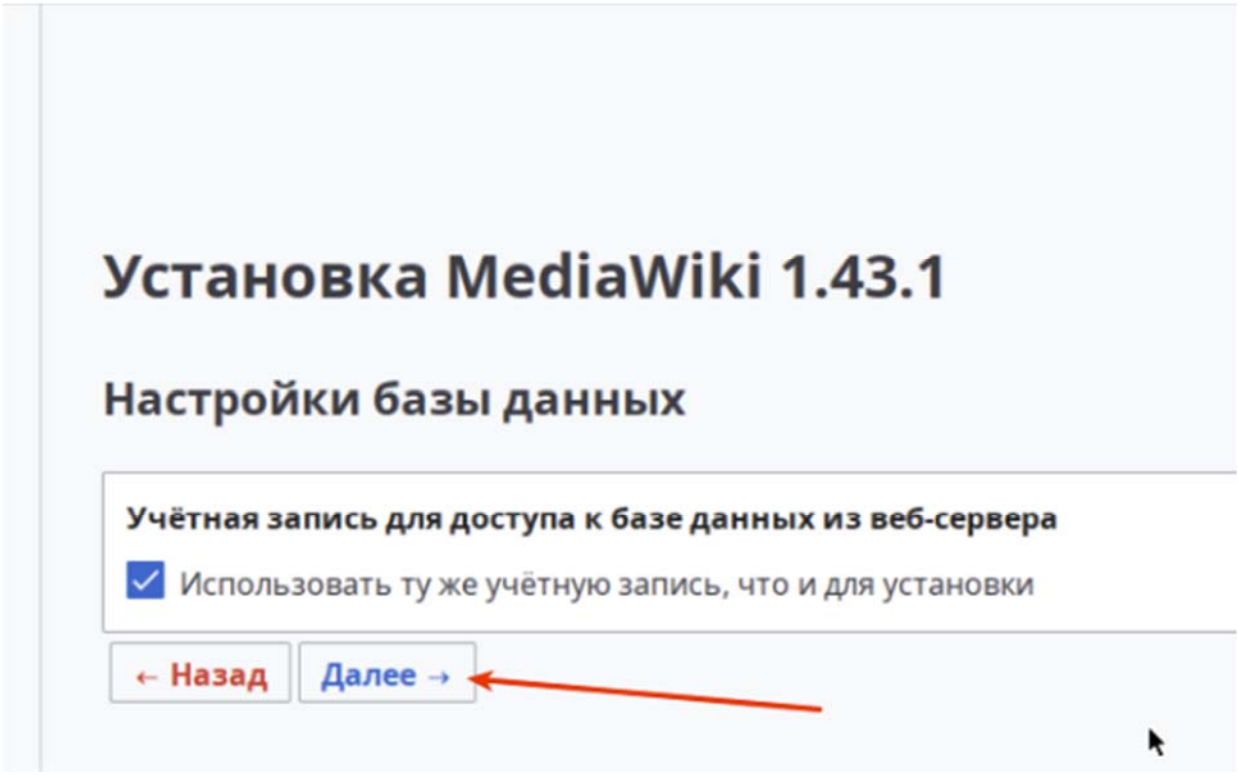

Установка MediaWiki 1.44.2
Язык
Ваш язык:
справка
ru - русский
Язык, который будет использовать вики:
справка
ru - русский
Далее →
Сайт MediaWiki
Справка для пользователей
Справка для администраторов
ЧЗВ
Искать помощи
Система отслеживания ошибок
Вклад
Информация о версии
Копирование
Обновление



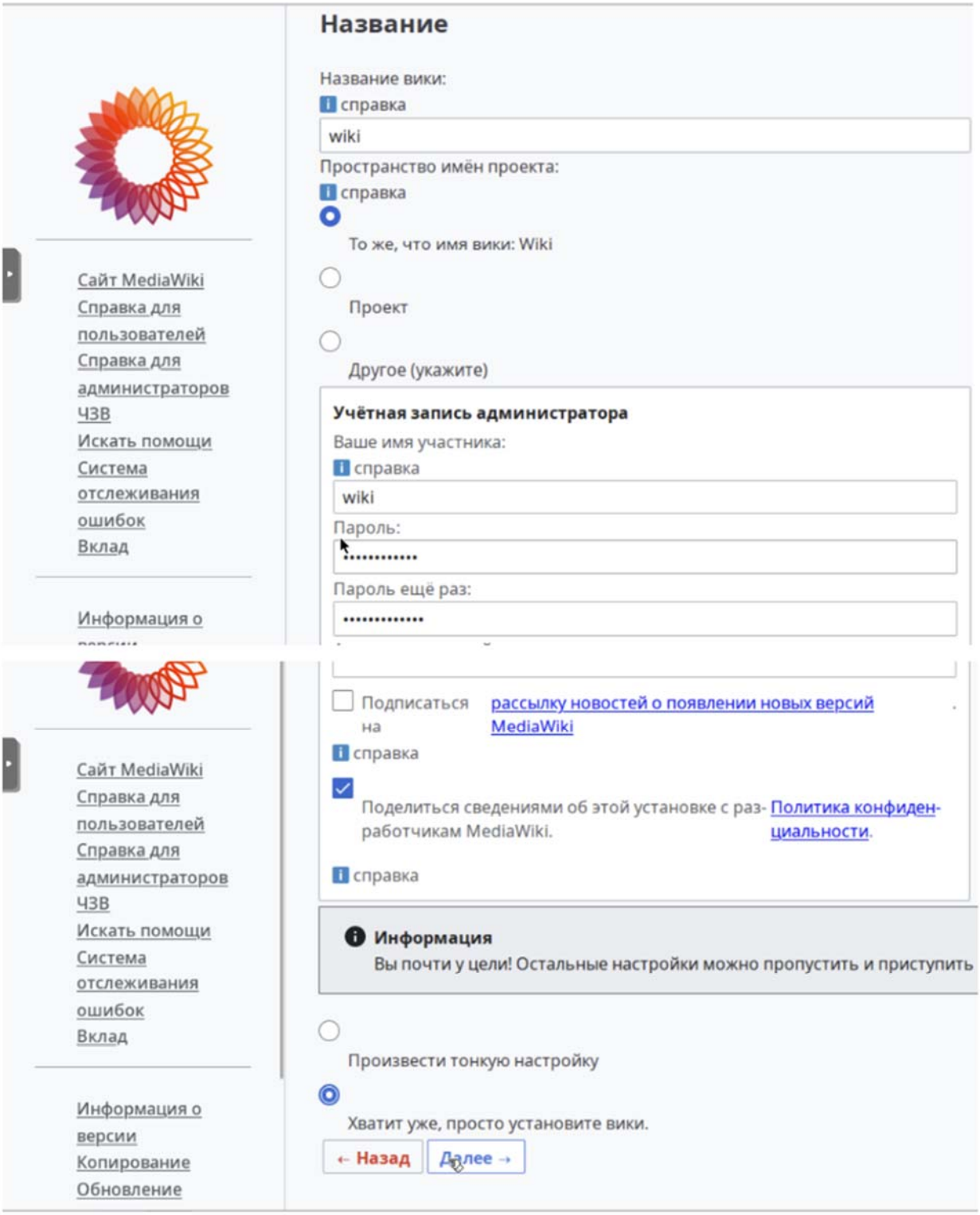
- Нажимаеем **Далее**:

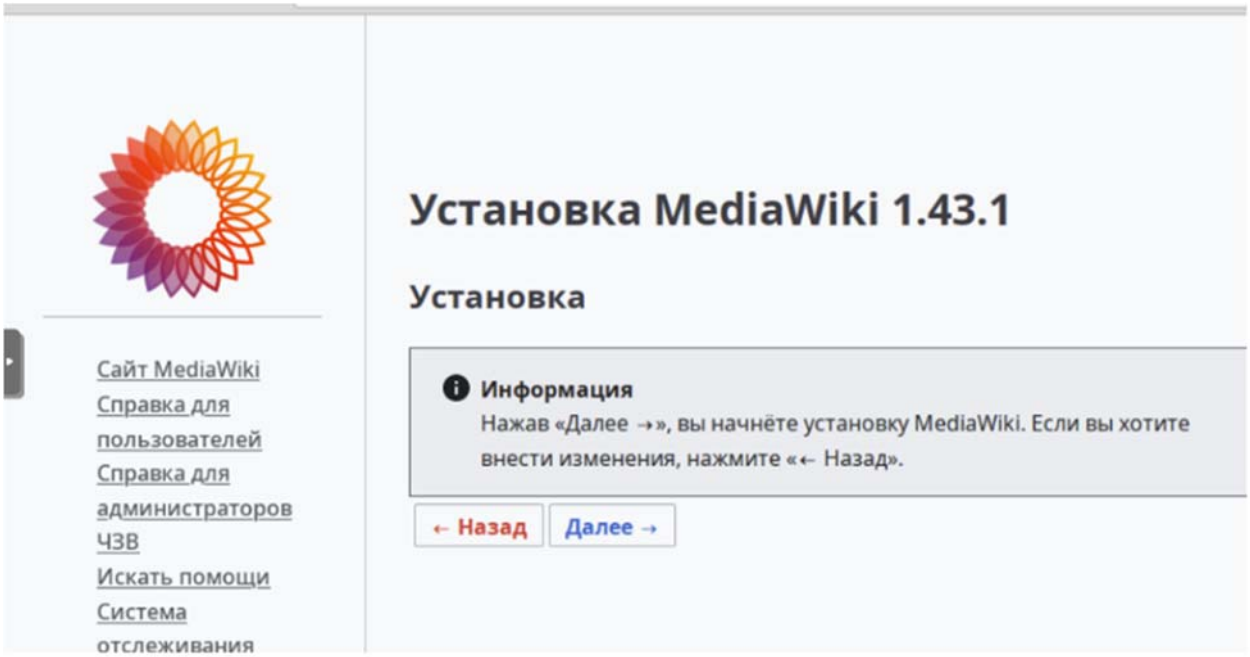
Пароль WikiP@ssw0rd

Нажимаеем Далее:



Заполняем необходимые сведения:


Название
Название вики:
справка
wiki
Пространство имён проекта:
справка
То же, что имя вики: Wiki
Проект
Другое (укажите)
Учётная запись администратора
Ваше имя участника:
справка
wiki
Пароль:
Пароль ещё раз:
Подписаться на рассылку новостей о появлении новых версий MediaWiki
справка
Поделиться сведениями об этой установке с разработчикам MediaWiki. Политика конфиденциальности.
справка
Информация
Вы почти у цели! Остальные настройки можно пропустить и приступить
Произвести тонкую настройку
Хватит уже, просто установите вики.
← Назад
Далее →
Сайт MediaWiki
Справка для пользователей
Справка для администраторов
ЧЗВ
Искать помощи
Система отслеживания ошибок
Вклад
Информация о версии
Копирование
Обновление



После чего будет автоматически скачен файл **LocalSettings.php** - который необходимо передать на **HQ-SRV1** в домашнюю директорию пользователя **root** туда же где лежим **wiki.yml**:

scp ~/Загрузки/LocalSettings.php user@192.168.1.3:/home/user

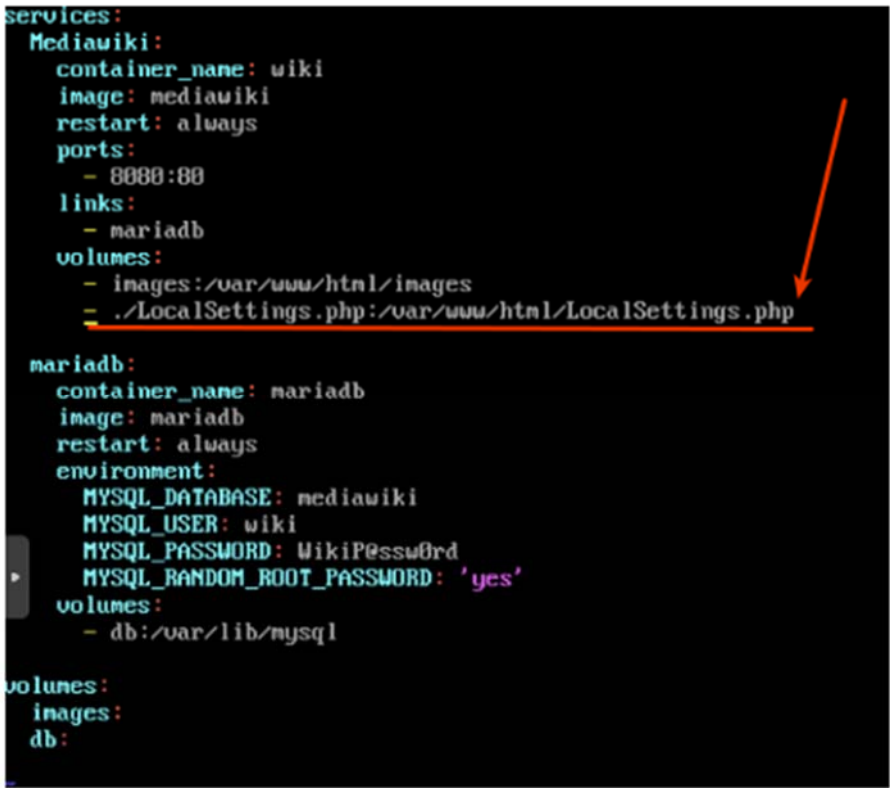
HQ-SRV1:

Забираем файл **LocalSettings.php** из /home/user и переносим в /root

Раскомментируем строку в файле wiki.yml:

vim wiki.yml

приводим файл к следующему виду:



ерезапускаем сервисы средствами docker compose:

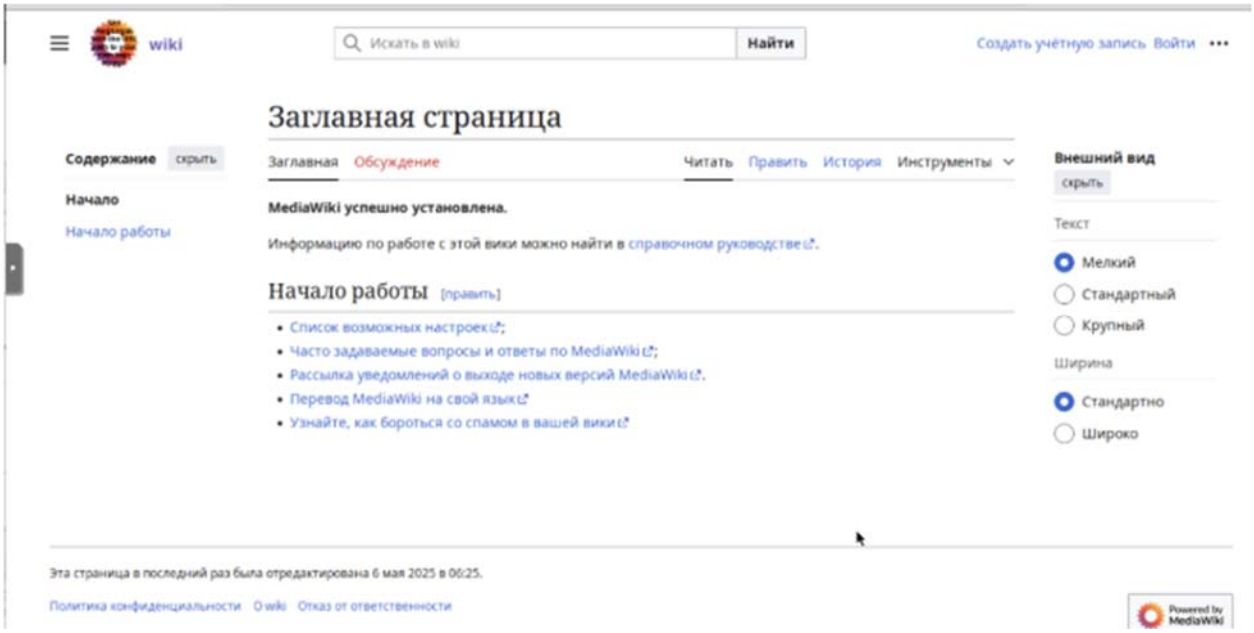
docker compose -f wiki.yml stop

docker compose -f wiki.yml up -d

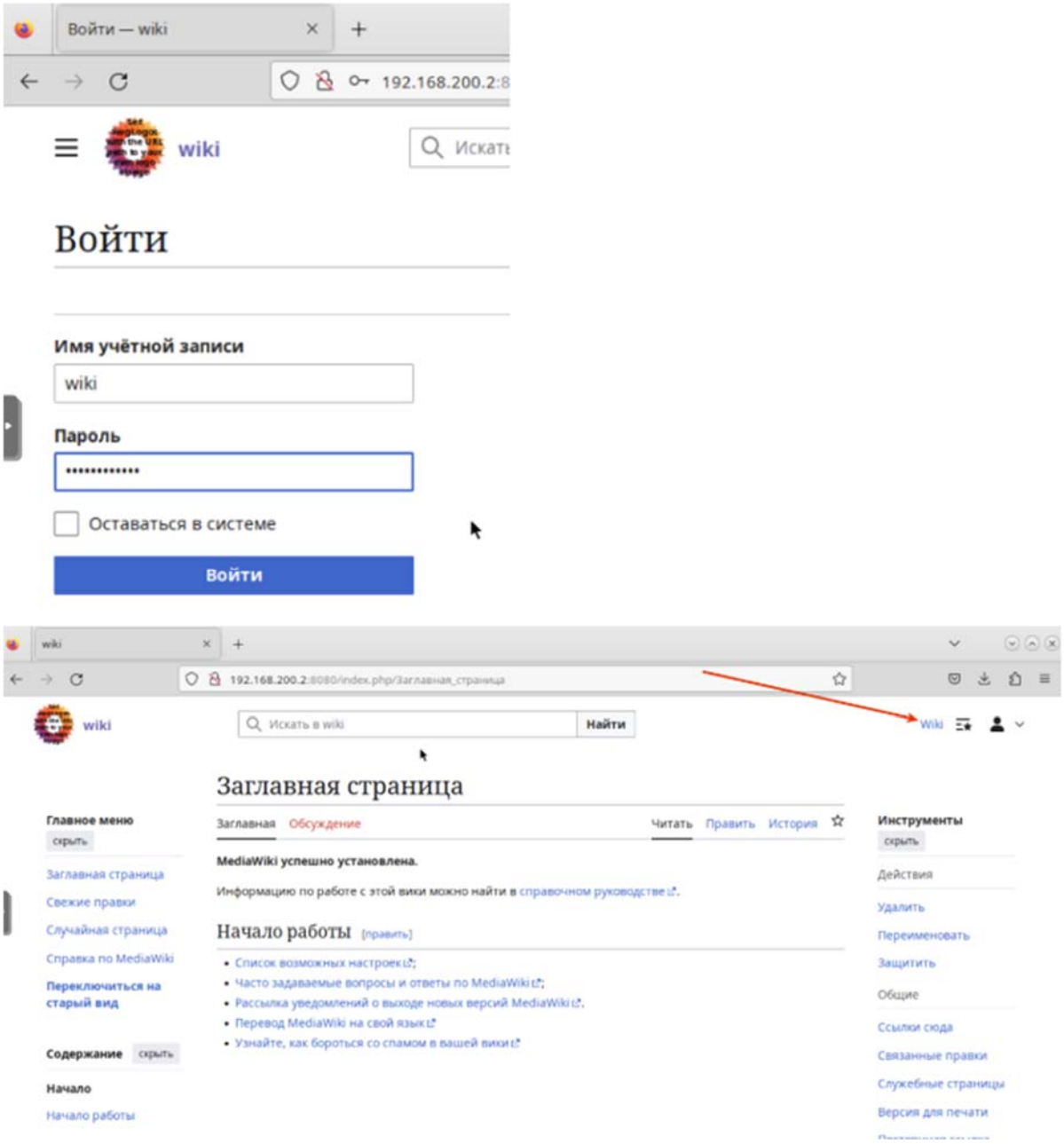
Результат:

CLI:

Проверяем доступ к http://<IP-адрес_BR-SRV>:8080:



вход из под пользователя созданного пользователя:



5.3 Сконфигурируйте файловое хранилище

Задание:

При помощи трёх дополнительных дисков, размером 1Гб каждый, на HQ-SRV сконфигурируйте дисковый массив уровня 5

Имя устройства – md0, конфигурация массива размещается в файле /etc/mdadm.conf

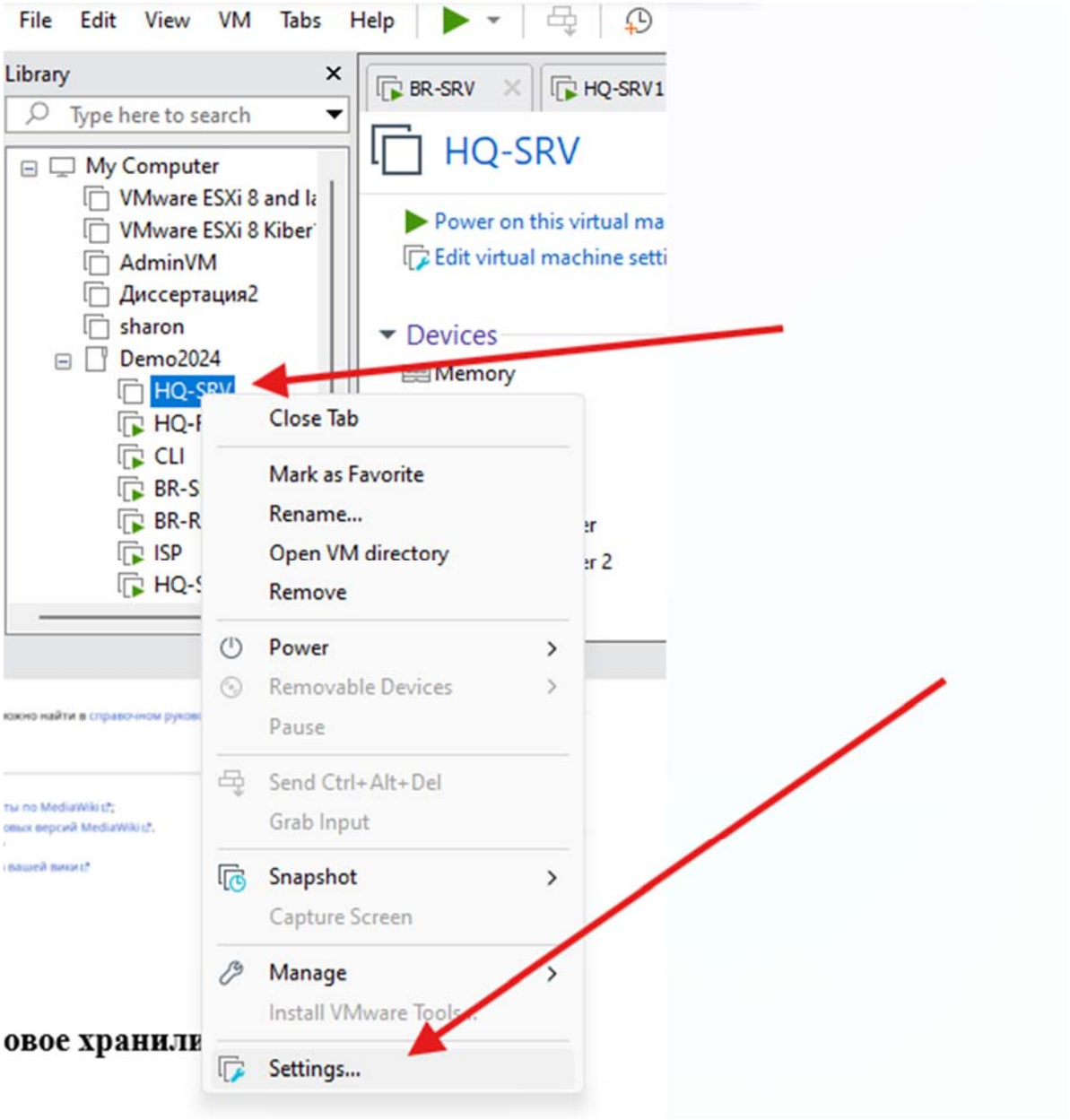
Обеспечьте автоматическое монтирование в папку /raid5

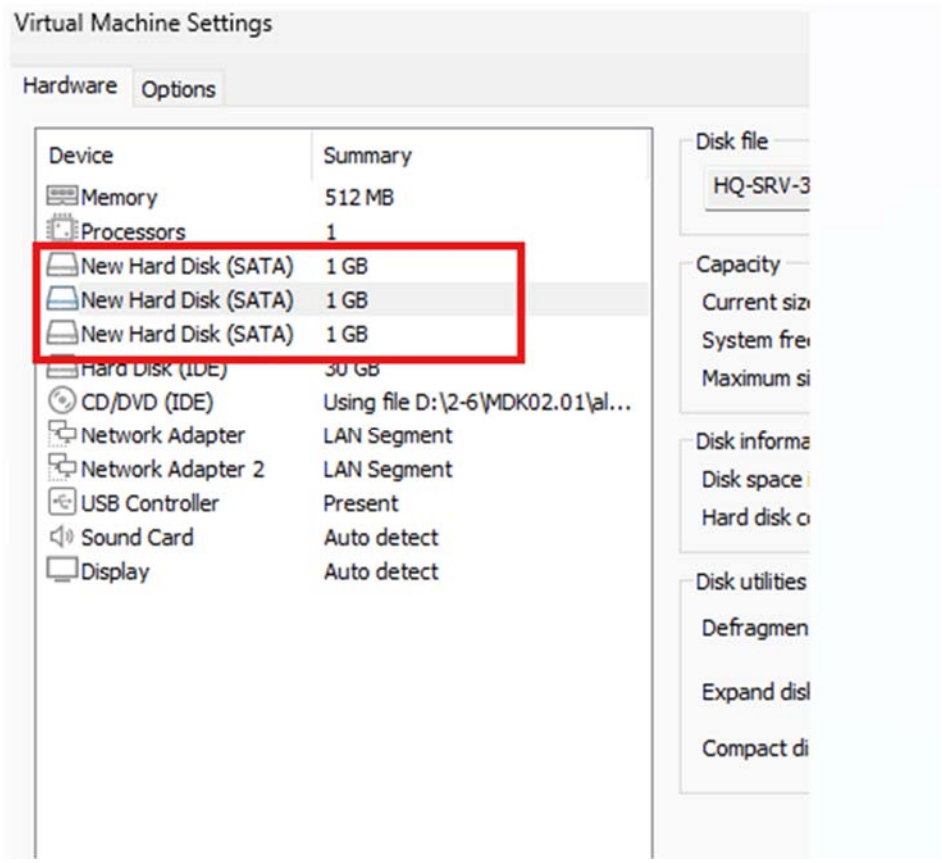
Создайте раздел, отформатируйте раздел, в качестве файловой системы используйте ext4

Настройте сервер сетевой файловой системы(nfs), в качестве папки общего доступа выберите /raid5/nfs, доступ для чтения и записи для всей сети в сторону CLI

На CLI настройте автомонтирование в папку /mnt/nfs

Основные параметры сервера отметьте в отчёте





Вариант реализации:

HQ-SRV:

Выполним установку пакета "mdadm":

mdadm — утилита для работы с программными RAID-массивами различных уровней

apt-get update && apt-get install -y mdadm

Подготовка носителей:

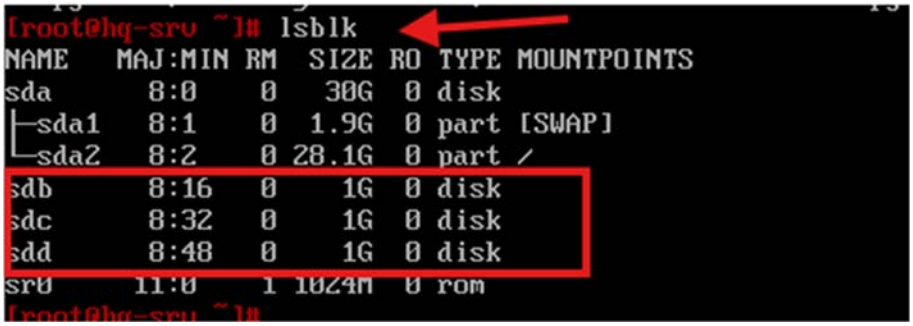
Сначала необходимо занулить суперблоки на дисках, которые мы будем использовать для построения RAID

при помощи утилиты "lsblk" - просматриваем наши фищические диски и определяемся какие будут использоваться в RAID - массиве

lsblk

Результат:

для работы будут использованы диски: **sdb**, **sdc** и **sdd**



Создание RAID-массива:

где:

/dev/md0 — устройство RAID, которое появится после сборки;

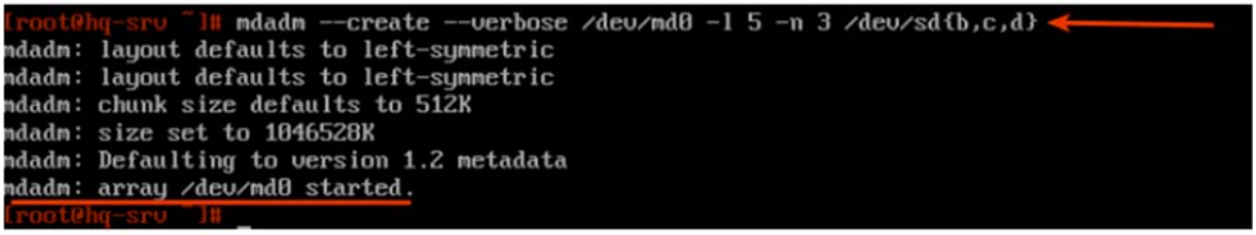
-l 5 — уровень RAID;

-n 3 — количество дисков, из которых собирается массив;

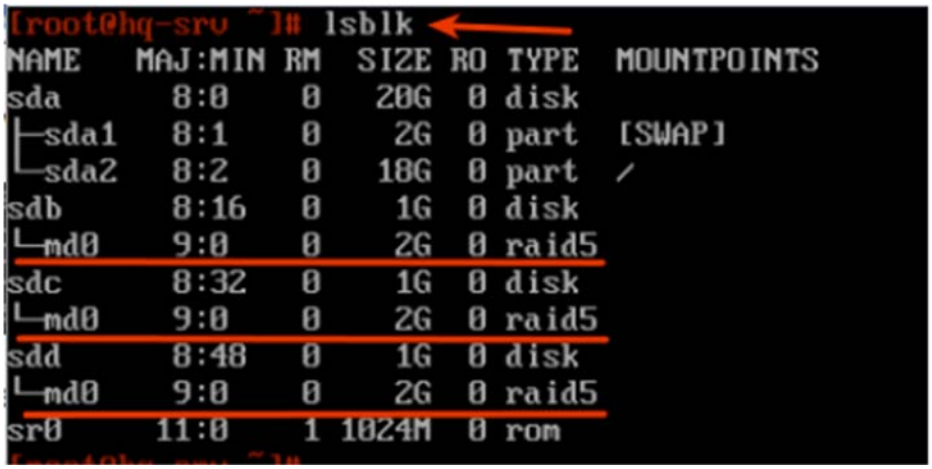
/dev/sd{b,c,d} — сборка выполняется из дисков sdb, sdc и sdd.

mdadm --create --verbose /dev/md0 -l 5 -n 3 /dev/sd{b,c,d}

Результат:



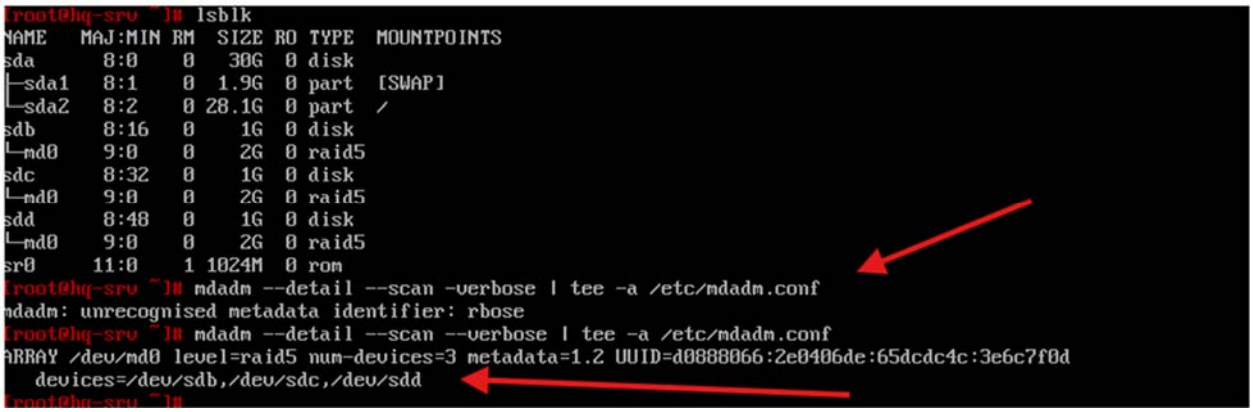
Проверяем:



Сохраняем конфигурацию массива в файле /etc/mdadm.conf:

mdadm --detail --scan --verbose | tee -a /etc/mdadm.conf

Результат:



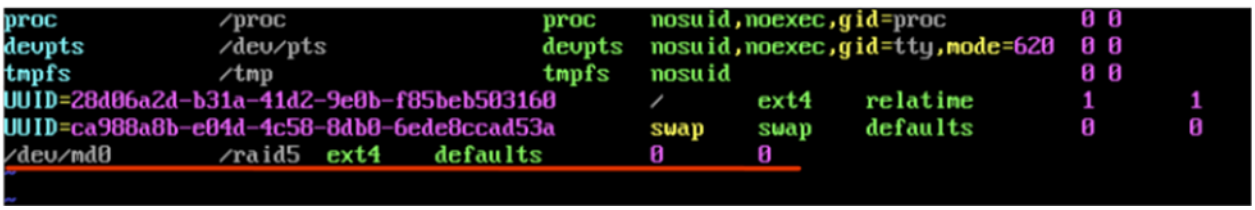
Создание файловой системы для массива

mkfs.ext4 /dev/md0

Чтобы данный раздел также монтировался при загрузке системы, добавляем в fstab

vim /etc/fstab

следующую информацию:



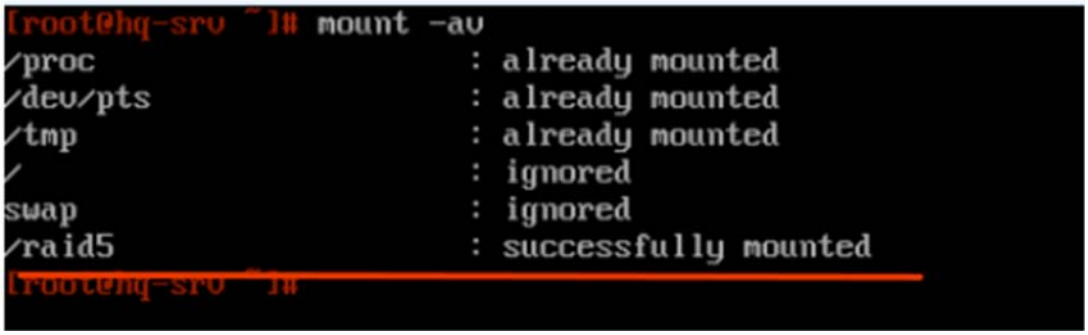
Создаём каталог /raid5:

mkdir /raid5

Выполняем монтирование:

mount -av

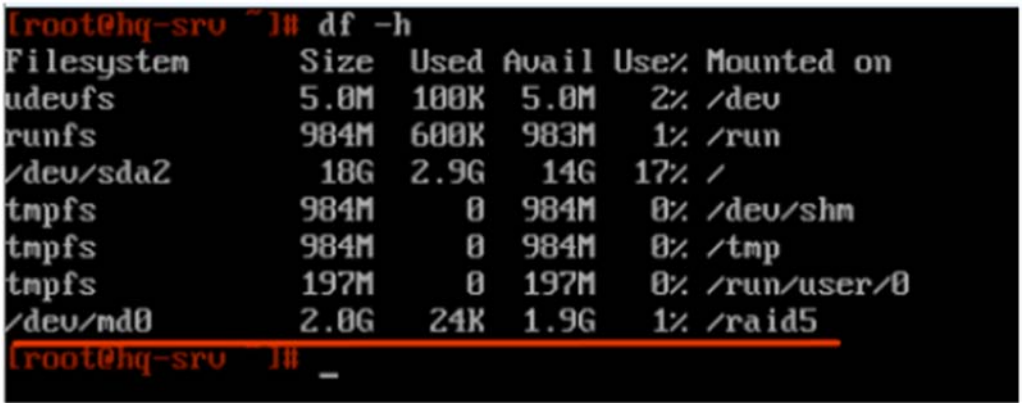
Результат:



Проверяем:

df -h

Результат:



Устанавливаем пакеты для NFS сервера:

apt-get install -y nfs-{server,utils}

Создаём директорию для общего доступа в директории /raid5/nfs, куда ранее был смонтирован RAID - массив:

mkdir /raid5/nfs

Назначаем права - полный доступ:

chmod 777 /raid5/nfs

3. Редактируем файл /etc/exports:

vim /etc/exports

Добавляем туда следующую информацию, где:

/raid5/nfs - общий ресурс

192.168.4.0/24 - клиентская сеть, которой разрешено монтирования общего ресурса

rw — разрешены чтение и запись

no_root_squash — отключение ограничения прав root

Экспортируем файловую систему, указанную выше в /etc/exports:

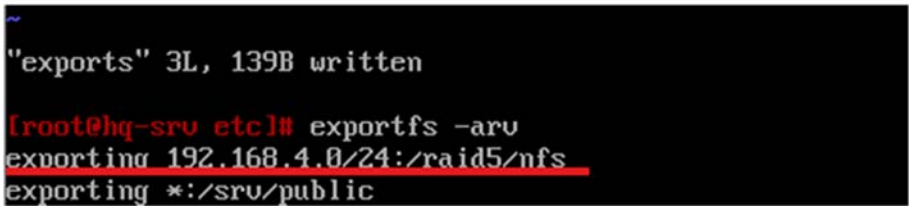
exportfs -arv

Результат:

exportfs с флагом -a, означающим экспортировать или отменить экспорт всех каталогов

-r означает повторный экспорт всех каталогов, синхронизируя /var/lib/nfs/etab с /etc/exports и файлами в /etc/exports.d

а флаг -v включает подробный вывод:



Запускаем и добавляем в автозагрузку NFS - сервер:

systemctl enable --now nfs-server

CLI:

Выполняем установку пакетов для NFS - клиента:

apt-get update && apt-get install -y nfs-{utils,clients}

Создадим директорию для монтирования общего ресурса:

mkdir /mnt/nfs

Задаём права на созданную директорию:

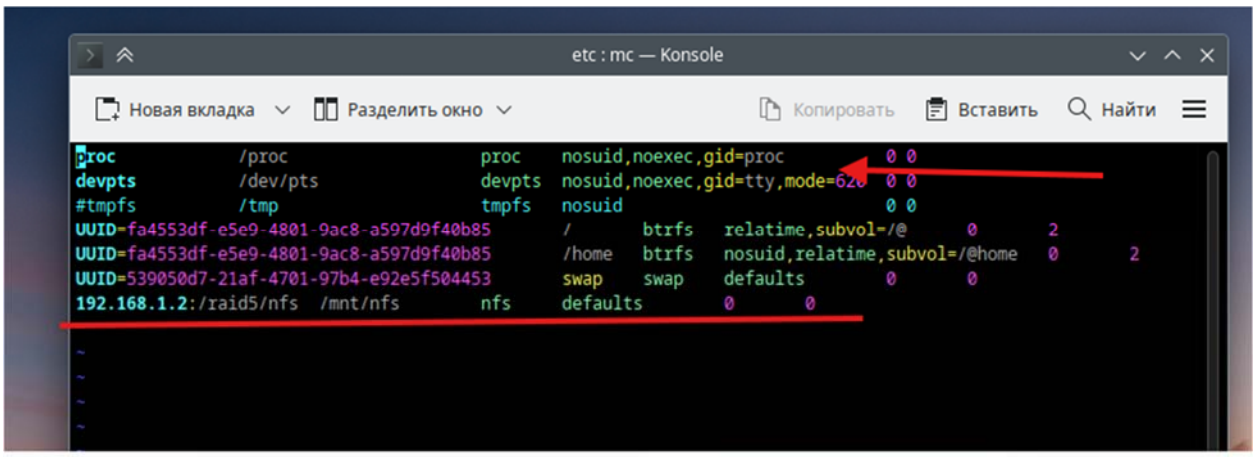
chmod 777 /mnt/nfs

Настраиваем автомонтирование общего ресурса через **fstab**:

vim /etc/fstab

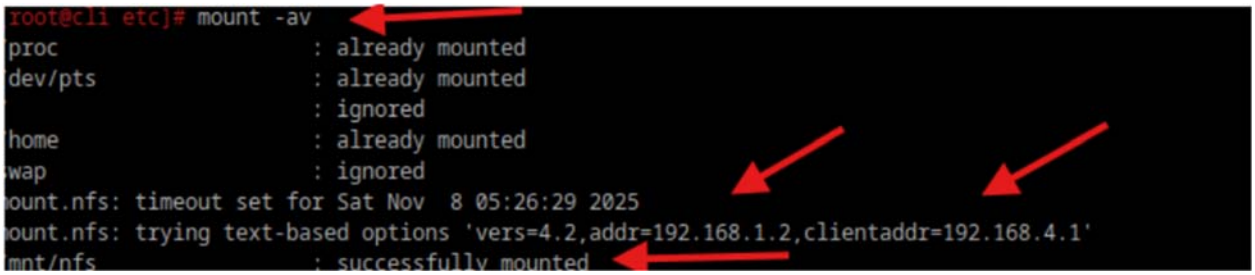
Добавляем следующую информацию:

где: **192.168.1.2** - адрес файлового сервера (**HQ-SRV**)



Выполняем монтирование общего ресурса:

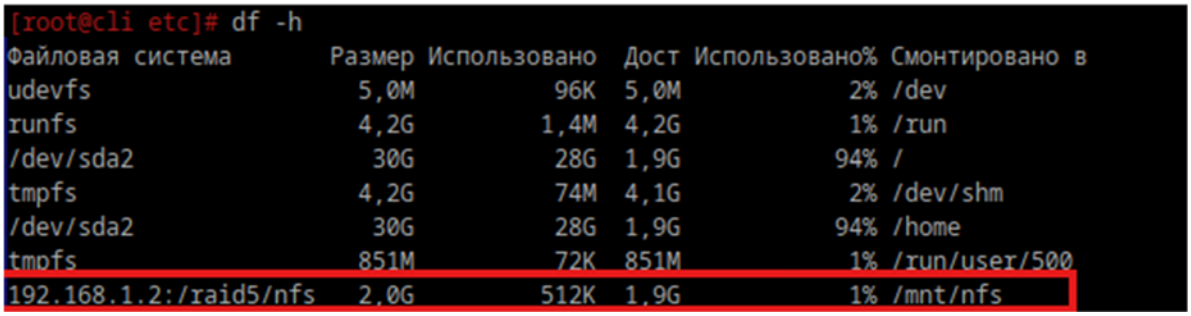
mount -av



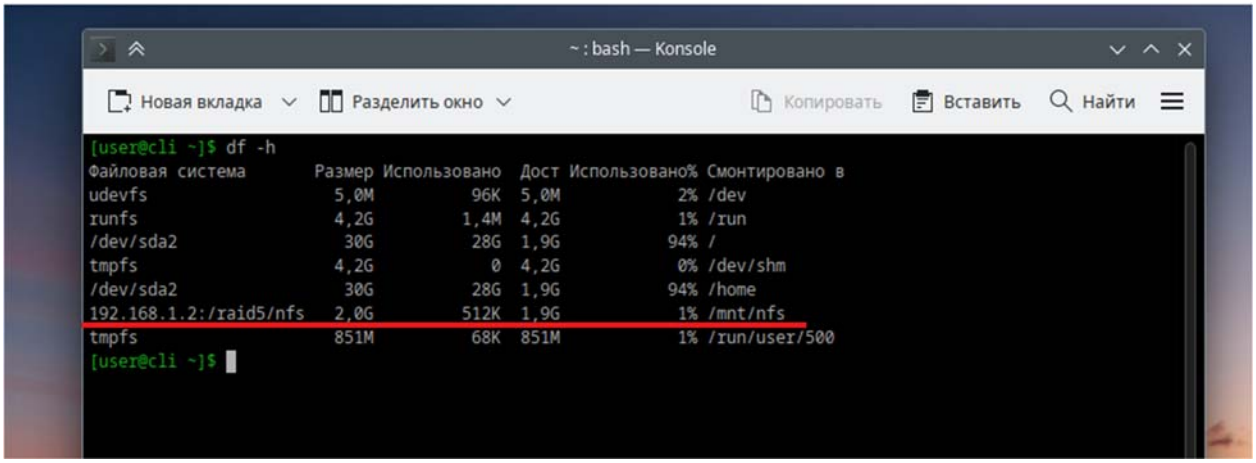
Проверяем:

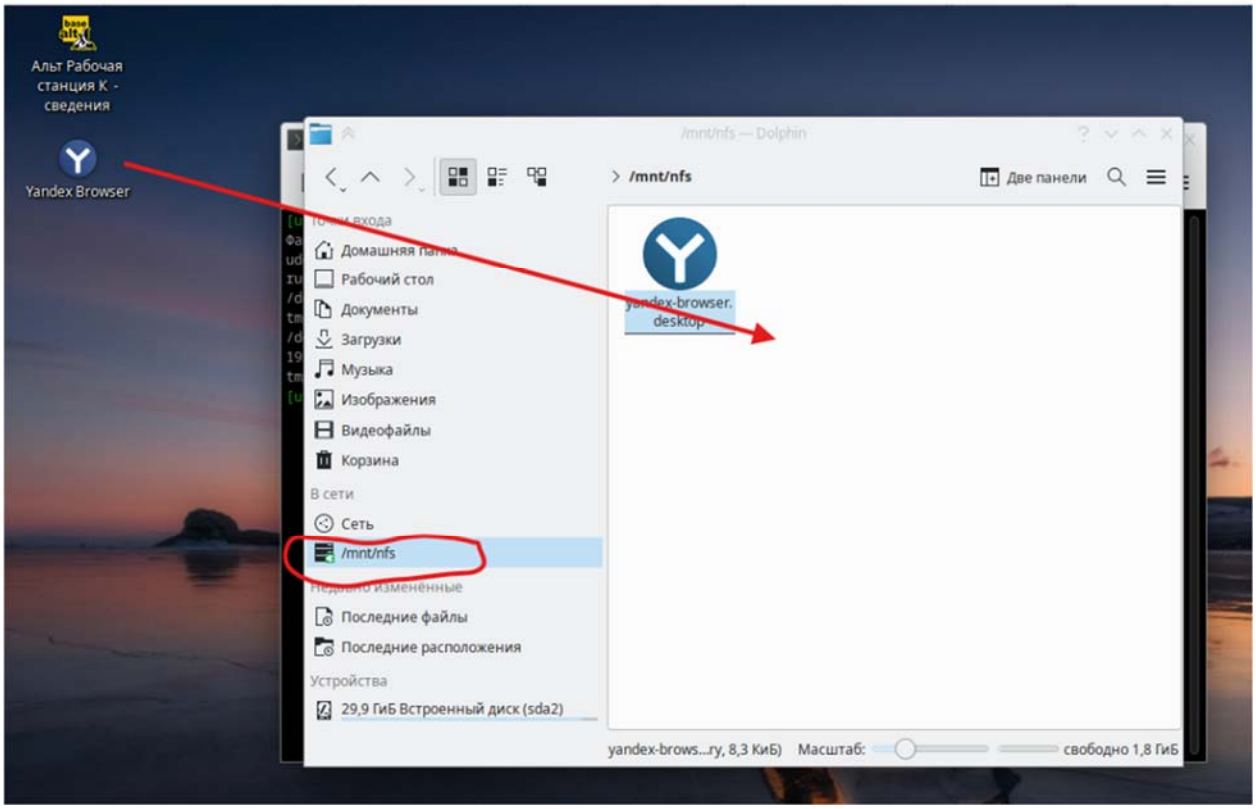
df -h

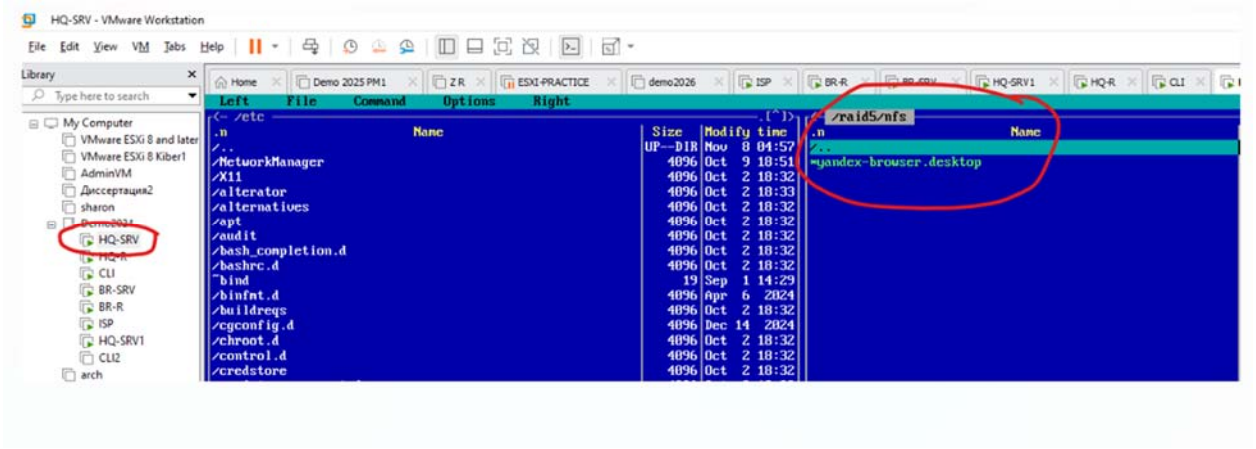
Результат:



Перезугружаем CLI и проверяем автомонтирование с правами на запись:


~ : bash — Konsole
Новая вкладка
Разделить окно
Копировать
Вставить
Найти
[user@cli ~]$ df -h
Файловая система Размер Использовано Дост Использовано% Смонтировано в
udevfs 5,0M 96K 5,0M 2% /dev
runfs 4,2G 1,4M 4,2G 1% /run
/dev/sda2 30G 28G 1,9G 94% /
tmpfs 4,2G 0 4,2G 0% /dev/shm
/dev/sda2 30G 28G 1,9G 94% /home
192.168.1.2:/raid5/nfs 2,0G 512K 1,9G 1% /mnt/nfs
tmpfs 851M 68K 851M 1% /run/user/500
[user@cli ~]$


Альт Рабочая станция К - сведения
Yandex Browser
/mnt/nfs — Dolphin
/mnt/nfs
Две панели
Домашняя папка
Рабочий стол
Документы
Загрузки
Музыка
Изображения
Видеофайлы
Корзина
В сети
Сеть
/mnt/nfs
Последние файлы
Последние расположения
Устройства
29,9 ГиБ Встроенный диск (sda2)
yandex-browser.desktop
yandex-brows...ry, 8,3 КиБ)
Масштаб:
свободно 1,8 ГиБ


HQ-SRV - VMware Workstation
File Edit View VM Tabs Help
Library
My Computer
VMware ESXi 8 and later
VMware ESXi 8 Kiber1
AdminVM
Диссертация2
sharon
HQ-SRV
BR-SRV
BR-R
ISP
HQ-SRV1
CLI2
arch
Left File Command Options Right
/etc
/raid5/nfs
/..
*yandex-browser.desktop

5.4Удобным способом установите приложение Яндекс Браузере для организаций на CLI

Установку браузера отметьте в отчёте

Если есть встроенный браузер - скачать Яндекс с его помощью

Если нет - установка при помощи **команды**:

$ su -

apt-get update

apt-get install yandex-browser-stable

rm -rf /var/cache – если не ставится

Список использованной литературы

1. Олифер, В. Г., Олифер, Н. А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. — 5-е изд. — СПб.: Питер, 2021. — 992 с.

2. Таненбаум, Э., Уэзеролл, Д. Компьютерные сети. — 5-е изд. — СПб.: Питер, 2021. — 960 с.

3. Куроуз, Дж., Росс, К. Компьютерные сети. Нисходящий подход. — М.: Эксмо, 2021. — 928 с.

4. Вишневский, В. М. Теоретические основы проектирования компьютерных сетей. — М.: Техносфера, 2021. — 512 с.

5. Столингс, В. Современные компьютерные сети. — 3-е изд. — СПб.: Питер, 2020. — 800 с.

6. Абрамов, В. А. Основы построения инфокоммуникационных сетей и систем: учебное пособие. — М.: Горячая линия-Телеком, 2020. — 396 с.

7. Андреев, А. М., Абрамов, М. В. Сети связи следующего поколения. — М.: Эко-Трендз, 2019. — 264 с.

8. Палмер, М., Синклер, Р. Б. Проектирование и внедрение компьютерных сетей. Учебный курс. — 2-е изд. — СПб.: БХВ-Петербург, 2018. — 752 с.

9. Рид, К. Настройка коммутаторов и маршрутизаторов Cisco. — М.: Диалектика, 2020. — 400 с.

10. Владимиров, А. Администрирование и безопасность компьютерных сетей. — М.: ДМК Пресс, 2022. — 450 с.

Приложение А (основные команды Linux)

To disable the GUI:

```
sudo systemctl set-default multi-user.target

sudo reboot
```

To re-enable the GUI:

```
sudo systemctl set-default graphical.target

sudo reboot
```

Команды Linux для управления файлами

1. ls – отображает список файлов и каталогов в текущей директории.
2. cd – изменяет текущую директорию.
3. pwd – выводит полный путь текущей директории.
4. mkdir – создает новый каталог.
5. rm – удаляет файлы или каталоги.
6. cp – копирует файлы и каталоги.
7. mv – перемещает или переименовывает файлы и каталоги.
8. touch – создает новый файл или обновляет время доступа и модификации существующего файла.
9. cat – выводит содержимое файла.
10. less – позволяет просматривать содержимое файла постранично.
11. head – выводит первые строки файла.
12. tail – выводит последние строки файла.
13. grep – ищет заданный текст в файлах или выводе команд.
14. find – находит файлы и каталоги на основе различных критериев.
15. chmod – изменяет права доступа к файлам и каталогам.
16. chown – изменяет владельца файлов и каталогов.
17. chgrp – изменяет группу файлов и каталогов.
18. tar – создает или распаковывает архивы.
19. zip – создает ZIP-архивы.
20. unzip – извлекает файлы из ZIP-архивов.

Команды Linux для управления пользователями

1. adduser – создает нового пользователя.
2. usermod – изменяет параметры существующего пользователя.
3. deluser – удаляет пользователя.
4. passwd – изменяет пароль пользователя.
5. su – переключается на другого пользователя или становится суперпользователем.
6. sudo – выполняет команду с привилегиями суперпользователя.
7. finger – отображает информацию о пользователе.

8. who – отображает информацию о вошедших пользователях.
9. id – отображает информацию о текущем пользователе или указанном пользователе.
10. groups – отображает группы, к которым принадлежит пользователь.
11. useradd – создает нового пользователя (альтернатива для adduser).
12. userdel – удаляет пользователя (альтернатива для deluser).
13. usermod – изменяет параметры существующего пользователя (альтернатива для usermod).
14. passwd – изменяет пароль пользователя (альтернатива для passwd).
15. last – отображает историю входа пользователей.
16. w – отображает текущих пользователей и их активность.
17. logout – выходит из текущей сессии пользователя.

Команды Linux для управления приложениями

1. apt-get install – устанавливает новое приложение или пакет.
2. apt-get remove – удаляет установленное приложение или пакет.
3. apt-get update – обновляет список доступных обновлений пакетов.
4. apt-get upgrade – обновляет установленные пакеты до последних версий.
5. apt-cache search – ищет пакеты по ключевому слову.
6. dpkg -i – устанавливает .deb пакет.
7. dpkg -r – удаляет .deb пакет.
8. dpkg -l – отображает список установленных пакетов.
9. snap install – устанавливает приложение из snap-пакета.
10. snap remove – удаляет установленное snap-приложение.
11. snap list – отображает список установленных snap-приложений.
12. systemctl start – запускает системную службу.
13. systemctl stop – останавливает системную службу.
14. systemctl restart – перезапускает системную службу.
15. systemctl enable – включает автозапуск системной службы при загрузке системы.
16. systemctl disable – отключает автозапуск системной службы при загрузке системы.
17. service <service> start – запускает службу.
18. service <service> stop – останавливает службу.
19. service <service> restart – перезапускает службу.
20. service <service> status – отображает статус службы.

Команды Linux для управления системой

1. shutdown – позволяет выключить или перезагрузить систему. Например, shutdown -h now выключает систему немедленно.
2. reboot – перезагружает систему. Просто запустите reboot в терминале.
3. halt – выключает систему. Просто запустите halt в терминале.
4. poweroff – выключает систему. Просто запустите poweroff в терминале.
5. systemctl – команда для управления системными сервисами. Например, systemctl start apache2 запускает службу Apache.
6. service – альтернативный способ управления системными службами. Например, service nginx restart перезапускает службу Nginx.
7. ifconfig – отображает и настраивает сетевые интерфейсы системы, включая IP-адреса, маски и шлюзы.
8. ip – альтернативный способ управления сетевыми интерфейсами и конфигурацией сети.
9. netstat – отображает сетевые соединения, открытые порты и другую связанную информацию.
10. ping – отправляет ICMP-пакеты на указанный IP-адрес для проверки доступности хоста в сети.
11. traceroute – отображает путь, по которому проходят пакеты до указанного IP-адреса в сети.
12. ssh – устанавливает безопасное соединение с удаленным сервером по протоколу SSH.
13. scp – копирует файлы между удаленным и локальным серверами по протоколу SSH.

14. rsync – выполняет синхронизацию и копирование файлов между удаленными и локальными серверами.
15. crontab – позволяет управлять cron-задачами, которые выполняются автоматически по заданному расписанию.
16. at – позволяет запускать команды или скрипты в определенное время в будущем.
17. shutdown – планирует выключение или перезагрузку системы по расписанию.
18. nohup – запускает команду с игнорированием сигналов завершения процесса. Это полезно для выполнения задач в фоновом режиме.
19. history – отображает историю команд, введенных пользователем в терминале.

Команды Linux для управления процессами

1. top – отображает список процессов и их характеристики, такие как использование CPU и памяти.
2. ps – выводит список текущих запущенных процессов с их идентификаторами (PID).
3. kill – отправляет сигнал процессу для его завершения. Например, kill PID завершит процесс с указанным идентификатором.
4. pkill – отправляет сигнал процессам по их имени или другим атрибутам. Например, pkill firefox завершит все процессы Firefox.
5. htop – интерактивное утилита мониторинга процессов, которая позволяет видеть дополнительную информацию и управлять процессами.
6. free – отображает общую, использованную и свободную память системы, включая физическую и подкачку.
7. vmstat – предоставляет информацию о использовании памяти, процессоре, вводе-выводе, планировании и других системных ресурсах.
8. killall – завершает все процессы с указанным именем. Например, killall firefox завершит все процессы Firefox.
9. renice – изменяет приоритет процесса в реальном времени. Например, renice -n -5 -p PID увеличит приоритет процесса с указанным идентификатором.
10. nice – запускает процесс с более низким приоритетом. Например, nice -n 10 command запустит команду с очень низким приоритетом.
11. pgrep – выводит идентификаторы процессов, соответствующие указанной строке. Например, pgrep firefox выведет идентификаторы процессов Firefox.
12. strace – отслеживает системные вызовы и сигналы, связываемые с процессом. Можно использовать для отладки или анализа процессов.
13. lsof – выводит открытые файлы и сетевые соединения для всех процессов на системе.
14. sar – собирает информацию о использовании ресурсов системы, таких как процессор, память, сеть и диски, и сохраняет ее для последующего анализа.
15. uptime – выводит информацию о времени работы системы, средней загрузке и количестве активных пользователей.
16. time – запускает команду и отображает время, затраченное на ее выполнение, включая CPU-время и время ввода-вывода.

Команды Linux для управления памятью

1. smem – отображает детальную информацию об использовании памяти процессами, группами процессов и системой в целом.
2. sync – записывает все буферы операционной системы на диск, чтобы обеспечить сохранность данных перед завершением работы.
3. swapoff – отключает файл подкачки, что позволяет освободить диск, но может увеличить использование оперативной памяти.
4. swapon – включает файл подкачки, добавляя дополнительную виртуальную память для использования системой.
5. sysctl – позволяет просматривать и изменять настройки ядра, включая параметры, связанные с памятью.
6. ulimit – устанавливает ограничения на использование ресурсов, включая память, для отдельного пользователя или процесса.

7. pmap – выводит карту памяти процесса, позволяя увидеть как процесс использует физическую и виртуальную память.
8. slabtop – отображает информацию о кэшах ядра, которые используют физическую память системы.
9. ulimit – устанавливает ограничения на использование ресурсов, включая память, для отдельного пользователя или процесса.
10. numactl – управляет доступом процессов к памяти и процессорам, особенно в многоядерных системах.
11. sysrq – позволяет отправлять системным вызовом определенные команды ядру Linux, в том числе сброс памяти (Memory Management).
12. mdb – интерактивный отладчик для системы Solaris, который может использоваться для анализа памяти.

Приложение Б (Ссылки)

IPv4 калькулятор

IPv6 калькулятор

draw.io

- Альт Сервер 10
- Альт Рабочая станция 10

Приложение В (Настройка и использование IP-туннелей)

IP-туннели — средство, позволяющее улучшить IP-сети. Поддерживаются IP-туннели трёх видов:

- IPIP
- GRE
- SIT
- VTI

Прежде всего следует определить необходимый вид туннеля для решаемой задачи.

- Туннели IPIP — самые простые.
- Туннели GRE (general incapsulation) обычно используются в маршрутизаторах Cisco. По туннелям этого типа могут передаваться broadcast и multicast пакеты. Кроме того, эти туннели поддерживают контрольные суммы и контроль упорядоченности пакетов. Также GRE-туннели обладают опциональным атрибутом key в виде произвольного 4-байтового числа, который позволяет конфигурировать несколько GRE туннелей между одной парой IP-адресов несущей сети (в отличие от IPIP-туннелей, с которыми это невозможно).

- Туннели SIT предназначены для транспортировки пакетов IPv6 через сети IPv4.
- Туннели VTI используются для построения IPsec туннелей. Работают используя один из демонов, strongswan или libreswan.

Тип туннеля определяется опцией TUNTYPE (ipip, gre, sit, vti). По умолчанию TUNTYPE=ipip. Кроме типа туннеля для конфигурации всегда требуется адрес удалённого хоста и почти всегда — локальный адрес. Эти адреса определяются опциями TUNREMOTE и TUNLOCAL соответственно. В некоторых случаях локальный адрес можно не указывать. В этом случае опция TUNLOCAL всё равно обязательна, но принимает значение any. Не забудьте назначить туннельному интерфейсу адреса и маршруты в соответствующих файлах.

Приложение Г (etcnet)

ОПИСАНИЕ

/etc/net - это система конфигурации сети. Она является одновременно простой в применении для новичка и действенной для эксперта. В первую очередь следует описать настройки и интерфейсы вашей сети в конфигурационных файлах. Однажды сделав это, вы сможете контролировать состояние вашего хоста с помощью трех скриптов: ifup, ifdown, network.init.

КОНФИГУРАЦИЯ СИСТЕМЫ

/etc/net поставляется с конфигурацией по умолчанию, которая подходит для большинства случаев. Более того, дистрибутивы Linux могут подстроить установки по умолчанию, но существуют вещи, которые можете настроить только вы. /etc/net сохраняет свою конфигурацию в файлах, большая часть которых постоянно хранится в каталоге /etc/net.

/etc/net/options.d

В этом каталоге по умолчанию хранится файл 00-default. Там же могут находиться и другие файлы, они будут читаться в алфавитном порядке.

/etc/net/sysctl.conf

файл запуска системных вызовов

/etc/net/ipv4rule

таблица правил ip ('ip -4 добавляет параметры)

/etc/net/vlantab

Таблица конфигурации VLAN. Если нужно настроить множество простых VLAN интерфейсов, это правильное место. Чтобы узнать подробности, смотрите раздел СИНТАКСИС VLANTAB.

/etc/net/iftab

Таблица назначения интерфейсов факультативна, но иметь ее настоятельно рекомендуется Этот файл используется ifrename. Формат файлов iftab описан в руководстве iftab. Обратите внимание, что /etc/iftab не используется, а данные хранятся в /etc/net/iftab. Это различие позволяет хранить /etc/net-специфичные профили и суффиксы хостов в отдельном каталоге, не создавая дополнительной путаницы в /etc. Кроме того, это оберегает систему от случайной смены имени интерфейса после запуска ifrename.

/etc/net/hosttab

Этот дополнительный файл может быть использован во время МУЛЬТИХОСТОВОЙ КОНФИГУРАЦИИ.

/etc/net/ifup-pre

Если существует и выполним, запускается перед запуском ЛЮБОГО интерфейса, но после того, как он будет создан.

/etc/net/ifup-post

Если существует и выполним, запускается после того, как ЛЮБОЙ интерфейс будет запущен и начнет работу.

/etc/net/ifdown-pre

Если существует и выполним, запускается перед тем, как ЛЮБОЙ интерфейс начнет подготовку к выключению.

/etc/net/ifdown-post

Если существует и выполним, запускается после того, как ЛЮБОЙ интерфейс полностью выключен.

/etc/net/netup-pre

Если существует и выполним, запускается перед началом работы сети.

/etc/net/netup-post

Если существует и выполним, запускается после начала работы сети.

/etc/net/netdown-pre

Если существует и выполним, запускается перед прекращением работы сети.

/etc/net/netdown-post

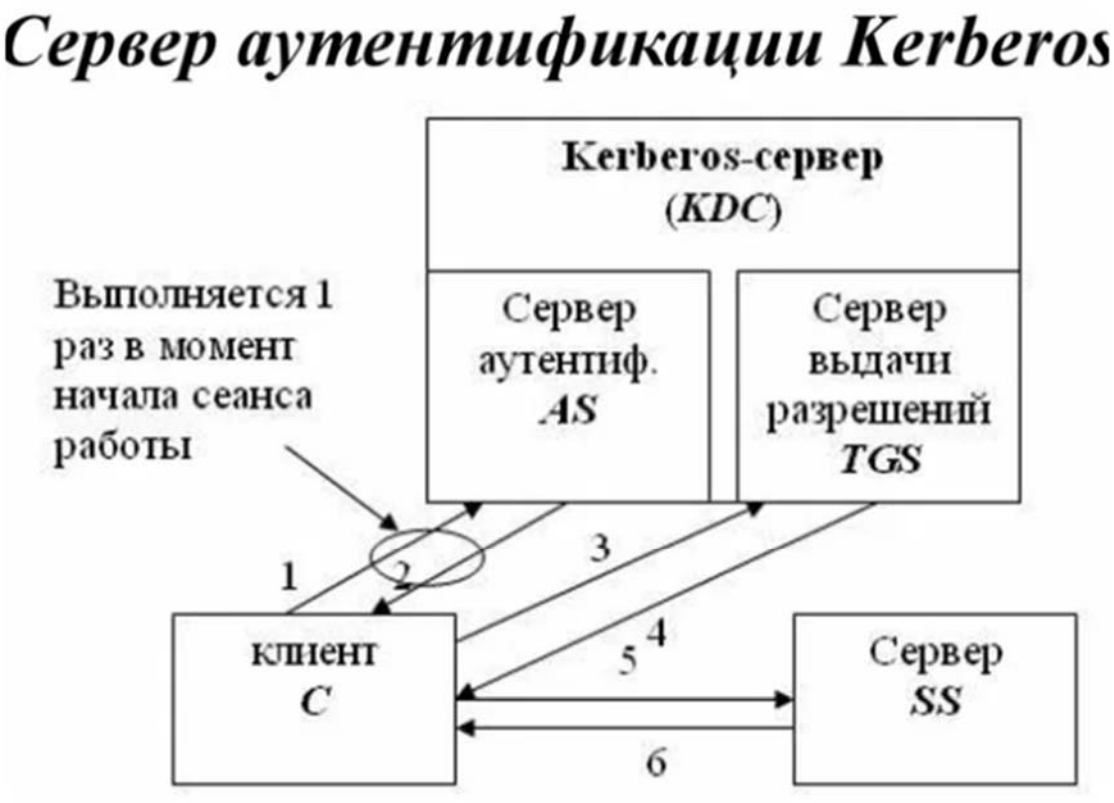
Если существует и выполним, запускается после прекращения работы сети.

Приложение Д (Kerberos)

Kerberos — **сетевой протокол аутентификации**, разработанный в MIT для проекта Athena в конце 1980-х годов. Позволяет клиентам и серверам безопасно проверять подлинность друг друга с помощью **Центра распределения ключей (KDC)** — доверенной третьей стороны. wiki.merionet.rugubin.systemsssl-team.comdzen.ru

Особенности:

- Использует криптографию с секретным ключом, не передаёт пароли по сети в явном виде.
- Позволяет пользователям аутентифицироваться один раз для доступа к нескольким сервисам (единая точка входа, Single Sign-On, SSO).
- Поддерживает взаимную аутентификацию: не только клиент, но и сервер может проверить подлинность друг друга.



Процесс аутентификации Kerberos включает несколько этапов:

1. **Аутентификация клиента**. Клиент отправляет запрос на Authentication Server (AS), AS проверяет учётные данные и выдаёт Ticket-Granting Ticket (TGT), зашифрованный ключом KDC.

2. **Запрос билета на доступ к сервису**. Клиент отправляет TGT вместе с запросом на доступ к определённому сервису (например, базе данных). TGS проверяет TGT и выдаёт Service Ticket, зашифрованный ключом этого сервиса.
3. **Доступ к сервису**. Клиент отправляет Service Ticket на сервер, сервер расшифровывает его своим ключом и проверяет подлинность. Если всё верно, клиент получает доступ к ресурсу.

Компоненты

Некоторые компоненты протокола Kerberos:

- **Клиент (Client)** — пользователь или приложение, запрашивающее доступ к сервису.
- **Сервер (Server)** — ресурс, к которому клиент хочет получить доступ (например, файловый сервер).
- **KDC (Key Distribution Center)** — центральный сервер, состоящий из двух частей: Authentication Server (AS) и Ticket Granting Server (TGS).
- **База данных принципалов (Principal Database)** — хранит информацию о пользователях и сервисах, их паролях и ключах.

Угрозы

Протокол Kerberos защищает от **перехвата учётных данных** злоумышленниками, так как «билеты» имеют отметку времени и действуют ограниченный период. Однако есть и уязвимости, например:

- **Атаки перебора паролей** — поскольку ответы AS зашифровываются ключом, производным от пароля пользователя, злоумышленник может попытаться расшифровать их с использованием слабо защищённых паролей.
- **Жёсткая зависимость от точной синхронизации времени** на всех узлах системы — при наличии возможности изменить системное время атакующий может повторно использовать просроченные тикеты, обходя механизмы контроля доступа.

Применение

Протокол Kerberos широко используется в различных системах, например:

- **Microsoft Active Directory** — Kerberos — стандартный протокол аутентификации в доменах Windows. wiki.merionet.rugubin.systems
- **Корпоративные и государственные организации** — для управления доступом к ресурсам, различным сервисам и приложениям, например к сетевым шарам, базам данных, веб-сервисам, почтовым службам.

Приложение E rc.local

Для создания файла **/etc/rc.d/rc.local** можно применить следующие команды (с правами пользователя *root*):

echo '#!/bin/sh' > /etc/rc.d/rc.local

chmod +x /etc/rc.d/rc.local

После чего в этот файл можно помещать команды, которые необходимо выполнить после запуска системы. Однако в 95% случаев то, что вы собираетесь записать в этот файл, имеет более подходящее место в системе

Лист регистрации изменений и дополнений ФОС по профессиональному модулю
ПМ 02. Организация сетевого администрирования

№ изме-нения	Номера листов		Основания для внесения изменений	Дата	№ протокола педсовета	Дата введения изменений	Подпись	Расшифровка подписи
	Замененных	Новых						