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
Государственной итоговой аттестации
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 Государственной итоговой аттестации 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 Государственной итоговой аттестации 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.

СОДЕРЖАНИЕ

1 ПАСПОРТ ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ИА

1.1. *Область применения программы ИА*

Целью итоговой аттестации (ИА) является комплексная оценка качества и уровня подготовки выпускника, а также соответствие его подготовки требованиям Федерального государственного образовательного стандарта по специальности среднего профессионального образования 09.02.06 «Сетевое и системное администрирование», требованиям работодателей.

Выполнение и защита ВКР является обязательным завершающим этапом среднего профессионального образования, предоставляет возможности для самореализации и творческого самовыражения. Его успешное прохождение является необходимым условием присвоения выпускникам квалификации дипломированного специалиста - Сетевой и системный администратор по специальности 09.02.06 «Сетевое и системное администрирование».

В соответствии с ФГОС СПО по специальности 09.02.06 «Сетевое и системное администрирование» при реализации программы подготовки специалистов среднего звена установлена форма итоговой аттестации: подготовка и защита выпускной квалификационной работы (далее ВКР) в виде дипломной работы и демонстрационный экзамен (ДЭ), который включается в выпускную квалификационную работу или проводится в виде государственного экзамена.

Объём времени на ИА (216 ч.), в том числе:

- на ВКР - 4 недели (144 ч.);
- на демонстрационный экзамен - 2 недели (72 ч.).

Сроки проведения ИА устанавливаются в соответствии с учебным планом по специальности 09.02.06 «Сетевое и системное администрированием графиком учебного процесса.

Ориентируясь на достижение общих целей образования в целом и целей среднего профессионального образования в частности, ВКР имеет свои специфические особенности, связанные с её основной функцией - итоговым контролем и оценкой качества образовательного процесса. При этом, предъявляются требования к качеству выполнения и защиты ВКР, а также определяющие уровень профессиональной подготовки студента, сводятся кследующему:

1) умение чётко формулировать рассматриваемую задачу, определять её актуальность и значимость, структурировать решаемую задачу;
2) обоснованно выбирать и корректно использовать наиболее эффективные методы решения задач;
3) уметь генерировать и анализировать альтернативные варианты и принимать оптимальные решения с учётом множественности критериев, влияющих факторов и характера информации;
4) использовать в работе современные информационные технологии, средства компьютерной техники и их программное обеспечение;
5) уметь осуществлять поиск научно-технической информации и работать со специальной литературой;
6) грамотно, с использованием специальной терминологии и лексики, чётко, в логической последовательности излагать содержание выполненных разработок.Работа над ВКР формирует у обучающихся специальности 09.02.06 «Сетевое и системное администрирование» общие компетенции:

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

профессиональные компетенции:

Код	Наименование видов деятельности и профессиональных компетенций
ВД 1.	Выполнение работ по проектированию сетевой инфраструктуры
ПК 1.1.	Выполнять проектирование кабельной структуры компьютерной сети.
ПК 1.2.	Осуществлять выбор технологии, инструментальных средств и средств вычислительной техники при организации процесса разработки и исследования объектов профессиональной деятельности
ПК 1.3.	Обеспечивать защиту информации в сети с использованием программно-аппаратных средств.
ПК 1.4.	Принимать участие в приемо-сдаточных испытаниях компьютерных сетей и сетевого оборудования различного уровня и в оценке качества и экономической эффективности сетевой топологии.

ПК 1.5.	Выполнять требования нормативно-технической документации, иметь опыт оформления проектной документации.
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.
ВД 3.	Эксплуатация объектов сетевой инфраструктуры
ПК 3.1.	Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей.
ПК 3.2.	Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях.
ПК 3.3.	Устанавливать, настраивать, эксплуатировать и обслуживать сетевые конфигурации
ПК 3.4.	Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное
ПК 3.5.	Организовывать инвентаризацию технических средств сетевой инфраструктуры, осуществлять контроль оборудования после его ремонта.
ПК 3.6.	Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры.

1.2. Цели и задачи итоговой аттестации

Целью проведения итоговой аттестации является: определение соответствия уровня подготовки выпускников требованиям Федерального государственного образовательного стандарта по специальности 09.02.06 «Сетевое и системное администрирование», готовности и способности решать профессиональные задачи.

Подготовка выпускной квалификационной работы является важнейшей составной частью учебного процесса, приобщает студентов к научно-исследовательской работе, обогащает опытом и знаниями, необходимыми для практической деятельности.

Цель выпускной квалификационной работы - систематизация и закрепление теоретических знаний студента по специальности при решении практических задач исследовательского и аналитического характера, а также выявление его способности к самостоятельной работе. Этим обуславливается необходимость творческого, а не формального подхода к выбору тематики, выполнению содержательной части работы, написанию и оформлению выпускной квалификационной работы.

В процессе написания выпускной квалификационной работы студент должен обстоятельно изучить литературные источники по теме исследования, ознакомиться с проблемами, поставленными отечественными и зарубежными специалистами в сфере юриспруденции и различными точками зрения на их решение. Далее студенту следует

показать, что он детально раскрыл содержание основных вопросов выбранной темы, умеет систематизировать и обобщать информацию, самостоятельно делать выводы и разрабатывать рекомендации.

Выпускные квалификационные работы должны содержать анализ деятельности конкретной организации, а также рекомендации по улучшению ее деятельности, повышению

эффективности.

Задачи итоговой аттестации:

- определение соответствия знаний, умений, навыков выпускников современным требованиям рынка труда, уточнение квалификационных требований конкретных работодателей;
- определение степени сформированности профессиональных компетенций, личностных качеств, наиболее востребованных на рынке труда;
- приобретение опыта взаимодействия выпускников с потенциальными работодателями, способствующего формированию презентационных навыков.

1.3. Количество часов, отводимое на итоговую аттестацию

всего - 6 недель, в том числе:

выполнение и защита выпускной квалификации работы - 4 недели,

подготовка и сдача демонстрационного экзамена - 2 недели.

2. СТРУКТУРА ПРОЦЕДУР ИА И ПОРЯДОК ПРОВЕДЕНИЯ 2.1. Форма(ы) и сроки проведения итоговой аттестации

Форма(ы) проведения ИА: ДЭ и ВКР

Сроки проведения каждой формы ИА регламентированы Календарным графиком учебного процесса на текущий учебный год.

2.2.Требования к определению тематики, содержания, объёма и структуры ВКР

Обязательным требованием является - соответствие тематики выпускной квалификационной работы содержанию одного или нескольких профессиональных модулей по специальности 09.02.06 «Сетевое и системное администрирование».

Требования к содержанию, объёму и структуре выпускной квалификационной работы определяются на основании Порядка проведения итоговой аттестации выпускников по образовательным программам СПО, утвержденного приказом Министерства образования и науки Российской Федерации от 16 августа 2013 г. N 968 в соответствии с частью 5 статьи 59 Федерального закона от 29 декабря 2012 г. N 273 -ФЗ «Об образовании в Российской Федерации» (Собрание законодательства Российской Федерации, 2012, N 53, ст. 7598; 2013, N 19, N 2326) а именно:

тематика выпускной квалификационной работы должна соответствовать содержанию одного или нескольких профессиональных модулей, входящих в образовательную программу среднего профессионального образования и отвечать современным требованиям развития науки, техники, производства, экономики, культуры и образования;

темы выпускных квалификационных работ рассматриваются на заседании предметной цикловой комиссии профессионального цикла специальности 09.02.06 «Сетевое и системное администрирование», а затем согласовываются с предприятиями (базами преддипломной практики), если ВКР выполняется по заказу предприятия (организации), то тема дипломной работы разрабатывается на основании технического задания заказчика;

студенту предоставляется право выбора темы выпускной квалификационной работы, в том числе предложения своей тематики с необходимым обоснованием целесообразности её разработки для практического применения;

после согласования тематики ВКР приказом директора проходит утверждение и закрепление за студентами темы выпускной квалификационной работы (с указанием сроков исполнения) и назначении руководителей ВКР из числа работников отраслевых предприятий и организаций, ведущих преподавателей предметной цикловой комиссии профессионального цикла специальности 09.02.06 «Сетевое и системное администрирование», а также консультантов по разделам ВКР и проведения нормоконтроля не позднее 01 марта.

2.3. Обязательные документы и материалы, необходимые для выполнения ВКР

Индивидуальное задание по теме ВКР, где в соответствующих разделах формулируются конкретные требования к каждой части, рассматривается на заседании ПЦК, подписывается руководителем ВКР и утверждается заместителем директора по учебно-производственной работе.

Выдача задания на ВКР студенту должна состояться не позднее, чем за две недели до начала преддипломной практики и должна сопровождаться консультацией со стороны руководителя, в ходе которой разъясняются задачи, структура, объём работы, принцип разработки и оформления.

До выхода на преддипломную практику студентом составляется календарный план работы над ВКР, где предусмотрены сроки выполнения всех отдельных частей ВКР, консультирования по разделам ВКР и предварительной защиты. Календарный план утверждается руководителем ВКР. Информация о выполнении календарного графика отражается в отзыве руководителя ВКР.

Для участников ДЭ тематика и содержание ВКР разрабатывается с учётом требований стандартов WSR, профессиональных стандартов и ФГОС СПО.

ВКР включает в себя разделы:

Введение

Теоретическая часть
Практическая часть
Заключение

Список использованных источников
Приложения

Участники ДЭ осуществляют разработку разделов в соответствии с требованиями указанными в п. 3.3.2, 3.3.3, 3.3.4.

Содержание практической части разрабатывается с учётом задания для ДЭ, которое отражает содержание актуальных заданий Национального чемпионата WSR (пункт 3).

Условия допуска обучающихся к ИА

Необходимым условием допуска к итоговой аттестации является: представление документов, подтверждающих освоение обучающимся компетенций при изучении теоретического материала и прохождении практики по каждому из основных видов деятельности;

наличие зачётной книжки (подтверждает отсутствие у обучающегося академических задолженностей и выполнение учебного плана или индивидуального учебного плана);
наличие оценочных листов экзаменов (квалификационных) по видам деятельности;

наличие документов, подтверждающих результаты завершения этапов учебной и производственной (по профилю специальности) и преддипломной практики (дневники, аттестационные листы, протоколы аттестации учебной практики, протоколы аттестации производственной и преддипломной практики, отчёт, ведомости, характеристики); наличие портфолио (презентация результатов освоения образовательной программы, сертификаты, удостоверения, свидетельства, дипломы, грамоты, фотосвидетельства участия в мероприятиях).

Необходимым условием допуска к защите ВКР является: наличие ВКР, выполненной в соответствии с индивидуальном заданием, в сроки, установленные графиком; наличие отзыва руководителя ВКР;

наличие рецензии специалиста отраслевой организации (предприятия) или другой образовательной организации;

наличие производственной характеристики с места прохождения преддипломной практики.

К участию в ДЭ допускаются студенты, завершающие обучение по имеющим аккредитацию образовательным программам СПО.

Для участия в ДЭ:

не менее чем за 2 месяца до даты проведения ДЭ направляется заявка для регистрации участников по компетенциям. Факт направления и регистрации заявки подтверждает участие в ДЭ и ознакомление заявителя с Положением о ДЭ, что является согласием на обработку, в том числе с применением автоматизированных средств обработки, персональных данных участников;

за неделю до начала участники проходят окончательную регистрацию в электронной системе интернет мониторинга eSim;

за день до проведения ДЭ участники встречаются на площадке, выбранной МЦКО для прохождения инструктажа по охране труда и технике безопасности, а также знакомства с инструментами, оборудованием, материалами и т.д.

Решение о допуске студентов к итоговой аттестации принимается педагогическим советом колледжа и утверждается приказом директора.

2.4. Порядок проведения процедуры

Защита ВКР проводится на открытых заседаниях ЭК с участием не менее двух третей ее состава.

Защита ВКР проводится в специально подготовленном помещении.

В случае участия студента в ДЭ, копия протокола Сертифицированного центра квалификаций (СЦК) представляется в ЭК. ЭК может учитывать результаты участия выпускников в ДЭ при выставлении оценки.

Результаты ИА определяются оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно» в соответствии с установленными критериями; объявляются в тот же день после оформления в установленном порядке протокола заседания ГЭК.

Заседания ЭК протоколируются. В протоколе записываются: итоговая оценка ВКР, присуждение квалификации и особые мнения членов комиссии. Протоколы подписываются председателем, заместителем председателя, членами ЭК, ответственным секретарем.

Лицам, не проходившим ИА по уважительной причине, предоставляется возможность пройти ЭК без отчисления из образовательной организации

Дополнительные заседания ЭК для лиц, не проходивших ИА по уважительной причине, организуются в установленные образовательной организацией сроки, но не позднее 4 месяцев после подачи заявления.

Лицам, не прошедшим ИА или получившим на итоговой аттестации неудовлетворительные результаты, а также лицам, освоившим часть образовательной программы среднего профессионального образования и (или) отчисленным из образовательной организации, выдается справка об обучении илио периоде обучения по образцу, самостоятельно устанавливаемому образовательной организацией.

Обучающиеся, не прошедшие ИА или получившие на итоговой аттестации неудовлетворительные результаты, проходят ИА не ранее чем через 6 месяцев после прохождения ИА впервые.

Повторное прохождение ИА не может быть назначено образовательной организацией для одного лица более двух раз.

Процедура проведения ДЭ.

ДЭ проводится на базе Сертифицированного центра квалификаций (СЦК).

По прибытию в день ДЭ на площадку студент должен предъявить студенческий билет и документ, удостоверяющий его личность.

ДЭ проводится в несколько этапов:

проверка и настройка оборудования экспертами (за 1 час до начала ДЭ);

инструктаж по охране труда и технике безопасности студентов на площадке проведения

ДЭ (за 1 день до начала ДЭ);

выполнение студентами заданий;

подведение итогов и оглашение результатов.

В случае опоздания студента к началу ДЭ по уважительной причине он допускается к выполнению заданий, но время на выполнение заданий не добавляется.

В случае поломки оборудования и его замены (не по вине студента) студенту предоставляется дополнительное время.

Выполнение задания оценивается в соответствии с процедурами оценки чемпионатов WSR по соответствующей компетенции.

Комиссия состоит из пяти экспертов, которые используют как объективные, так и субъективные критерии оценки.

Подведение итогов предусматривает:

решение экзаменационной комиссии об успешном освоении компетенции, которое принимается на основании критериев оценки. На итоговую оценку результатов ДЭ, в том числе влияет соблюдение студентом требований ОТ и ТБ; заполнение членами комиссии ведомости оценок;

занесение результатов в информационную систему CompetitionInformationSistem (далее - CIS);

оформление протоколов, обобщение результатов ДЭ с указанием балльного рейтинга студентов.

Дополнительные сроки для проведения ДЭ не предусматриваются.

Порядок подачи и рассмотрения апелляций

По результатам аттестации выпускник, участвовавший в итоговой аттестации, имеет право подать в апелляционную комиссию письменное апелляционное заявление о нарушении, по его мнению, установленного порядка проведения итоговой аттестации и (или) несогласии с ее результатами (далее - апелляция).

Апелляция подается лично выпускником или родителями (законными представителями) несовершеннолетнего выпускника в апелляционную комиссию образовательной организации.

Апелляция о нарушении порядка проведения итоговой аттестации подается непосредственно в день проведения итоговой аттестации.

Апелляция о несогласии с результатами итоговой аттестации подается не позднее следующего рабочего дня после объявления результатов итоговой аттестации.

Апелляция рассматривается апелляционной комиссией не позднее трёх рабочих дней с момента её поступления.

Состав апелляционной комиссии утверждается образовательной организацией одновременно с утверждением состава экзаменационной комиссии.

Апелляционная комиссия формируется в количестве не менее пяти человек из числа преподавателей образовательной организации, имеющих высшую или первую квалификационную категорию, не входящих в данном учебном году в состав государственных экзаменационных комиссий. Председателем апелляционной комиссии является руководитель образовательной организации либо лицо, исполняющее обязанности руководителя на основании распорядительного акта образовательной организации.

Апелляция рассматривается на заседании апелляционной комиссии с участием не менее двух третей ее состава.

На заседание апелляционной комиссии приглашается председатель соответствующей экзаменационной комиссии.

Выпускник, подавший апелляцию, имеет право присутствовать при рассмотрении апелляции.

С несовершеннолетним выпускником имеет право присутствовать один из родителей (законных представителей).

Указанные лица должны иметь при себе документы, удостоверяющие личность.

Рассмотрение апелляции не является пересдачей итоговой аттестации.

При рассмотрении апелляции о нарушении порядка проведения итоговой аттестации апелляционная комиссия устанавливает достоверность изложенных в ней сведений и выносит одно из решений:

об отклонении апелляции, если изложенные в ней сведения о нарушениях порядка проведения итоговой аттестации выпускника не подтвердились и/или не повлияли на результат итоговой аттестации;

об удовлетворении апелляции, если изложенные в ней сведения о допущенных нарушениях порядка проведения итоговой аттестации выпускника подтвердились и повлияли на результат итоговой аттестации.

В последнем случае результат проведения итоговой аттестации подлежит аннулированию, в связи с чем протокол о рассмотрении апелляции не позднее следующего рабочего дня передается в экзаменационную комиссию для реализации решения комиссии. Выпускнику предоставляется возможность пройти итоговую аттестацию в дополнительные сроки, установленные образовательной организацией.

Для рассмотрения апелляции о несогласии с результатами итоговой аттестации, полученными при защите выпускной квалификационной работы, секретарь экзаменационной комиссии не позднее следующего рабочего дня с момента поступления апелляции направляет в апелляционную комиссию выпускную квалификационную работу, протокол заседания экзаменационной комиссии и заключение председателя экзаменационной комиссии о соблюдении процедурных вопросов при защите подавшего апелляцию выпускника.

Для рассмотрения апелляции о несогласии с результатами итоговой аттестации, полученными при сдаче государственного экзамена, секретарь экзаменационной комиссии не позднее следующего рабочего дня с момента поступления апелляции направляет в апелляционную комиссию протокол заседания экзаменационной комиссии, письменные ответы выпускника (при их наличии) и заключение председателя экзаменационной комиссии о соблюдении процедурных вопросов при проведении государственного экзамена.

В результате рассмотрения апелляции о несогласии с результатами итоговой аттестации апелляционная комиссия принимает решение об отклонении апелляции и сохранении результата итоговой аттестации либо об удовлетворении апелляции и выставлении иного результата итоговой аттестации. Решение апелляционной комиссии не позднее следующего рабочего дня передаётся в экзаменационную комиссию. Решение апелляционной комиссии является основанием для аннулирования ранее выставленных результатов итоговой аттестации выпускника и выставления новых.

Решение апелляционной комиссии принимается простым большинством голосов. При равном числе голосов голос председательствующего на заседании апелляционной комиссии является решающим.

Решение апелляционной комиссии доводится до сведения подавшего апелляцию выпускника (под роспись) в течение трёх рабочих дней со дня заседания апелляционной комиссии.

Решение апелляционной комиссии является окончательным и пересмотру не подлежит.

Решение апелляционной комиссии оформляется протоколом, который подписывается председателем и секретарем апелляционной комиссии и хранится в архиве образовательной организации.

Для ДЭ апелляция не предусмотрена.

Критерии оценки ВКР

Объём выпускной квалификационной работы составляет не менее 35 страниц печатного текста.

К ВКР имеются приложения, в том числе копии документов, выдержки из отчётных материалов, статистические данные, схемы, таблицы, диаграммы, программы, положения и т.п. и подтверждающие освоение общих и профессиональных компетенций.

Тема ВКР соответствует содержанию одного или нескольких профессиональных модулей, компетенций Worldskills «Сетевое и системное администрирование»».

Структура ВКР соответствует выбранной форме (дипломная работа).

Теоретическая часть раскрывает теоретические аспекты изучаемого объекта и предмета. Практическая часть включает результаты исследования, выполненные обучающимся в со-

ответствии с заданием и (или) содержит расчёты, аналитические материалы, собранные в ходе производственной практики (преддипломной).

Текст ВКР, чертежи, схемы и приложения оформлены в соответствии с установленными требованиями.

Использование обучающимся во время доклада подготовленного наглядного материала.

Применение обучающимся во время доклада информационно-коммуникативных технологий, сопровождение доклада презентацией.

Владение обучающимся профессиональной терминологией, коммуникативной культурой.

Критерии оценки ДЭ соответствуют заданию национального чемпионата Worldskills по компетенции «Сетевое и системное администрирование»» (пункт 3).

По результатам защиты выставляются:

оценка 5 «отлично», если работа выполнена в полном объёме, в установленный срок в соответствии с графиком выполнения; точное выполнение технологических расчётов и показателей финансово-хозяйственной деятельности структурного подразделения; правильно составленная нормативнотехнологическая и учётно-отчётная документация; компьютерная презентация выполнена в соответствии с существующими требованиями к созданию презентаций, с достаточным количеством фото и видеоматериалов; доклад в «сжатом» виде полностью отражают содержание работы; печатный вариант работы выполнен аккуратно, оформлен в полном соответствии с требованиями ГОСТ; продемонстрировано знание профессиональной терминологии, владение информационно-компьютерными технологиями; полные ответы на дополнительные вопросы;

оценка 4 «хорошо», если работа выполнена в полном объёме, в установленный срок в соответствии с графиком выполнения; небольшие неточности при выполнении технологических расчётов, показателей финансово-хозяйственной деятельности структурного подразделения или составлении нормативно-технологической и учётно-отчётной документации; компьютерная презентация выполнена в соответствии с существующими требованиями к созданию презентаций, с достаточным количеством фото и видеоматериалов; доклад в «сжатом» виде отражают содержание работы; печатный вариант работы выполнен аккуратно, оформлен в соответствии с требованиями ГОСТ; продемонстрировано знание профессиональной терминологии, владение информационно-компьютерными технологиями; ответы на дополнительные вопросы достаточно полные;

оценка 3 «удовлетворительно», если работа выполнена в неполном объёме, с нарушением графика выполнения; грубые ошибки при выполнении технологических расчётов, показателей финансово-хозяйственной деятельности структурного подразделения или составлении нормативно-технологической и учётно-отчётной документации; выполнение компьютерной презентации не соответствует существующим требованиям к созданию презентаций, с недостаточным количеством фото и видеоматериалов; доклад не полностью отражает содержание работы; оформление печатного варианта работы не соответствует требованиям ГОСТ; не продемонстрировано знание профессиональной терминологии,

владение информационно-компьютерными технологиями; не на все дополнительные вопросы даны ответы;

оценка 2 «неудовлетворительно», если объём выполнения работы составил менее 50%

В случае участия обучающегося в ДЭ влияние полученного им количества баллов (балльный рейтинг) на результаты ИА определяется на заседании ЭК в рабочем порядке.

Документация по итогам ИА

Решение ЭК о присвоении квалификации «Сетевой и системный администратор» по специальности 09.02.06 «Сетевое и системное администрированием о выдаче диплома выпускникам, прошедшим ИА, оформляется протоколом ЭК и приказом директора

По окончании ИА председатель ЭК составляет отчёт о работе комиссии, который заслушивается на Совете.

Председатель ПЦК оформляет статистический отчёт результатов ИА по специальности.

Перечень документов, представляемых на заседание ЭК:

ФГОС СПО по специальности 09.02.06 «Сетевое и системное администрирование», утвержденного приказом Министерства образования и науки Российской Федерации 9 декабря 2016 года № 1548;

Приказ Министерства образования и науки Российской Федерации от 16 августа 2013 г. № 968 «Об утверждении порядка проведения итоговой аттестации по образовательным программам среднего профессионального образования»;

Приказ Министерства образования и науки Российской Федерации от 14 июня 2013 г. № 464 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам среднего профессионального образования»;

Приказ Министерства образования и науки Российской Федерации от 31 января 2014 г. № 74 «О внесении изменений в Порядок проведения итоговой аттестации по образовательным программам среднего профессионального образования, утвержденный Приказом Министерства образования и науки Российской Федерации от 16 августа 2013 г. № 968»; Приказ Министерства образования и науки Российской Федерации от 22 января 2014 года № 31 «О внесении изменений в Порядок организации и осуществления образовательной деятельности по образовательным программам среднего профессионального образования, утвержденный приказом Министерства образования и науки Российской Федерации от 14 июня 2013 года № 464»;

Приказ Министерства образования и науки Российской Федерации от 15 декабря 2014 года № 1580 «О внесении изменений в Порядок организации и осуществления образовательной деятельности по образовательным программам среднего профессионального образования, утвержденный приказом Министерства образования и науки Российской Федерации от 14 июня 2013 года № 464»;

Приказ Департамента образования города Москвы от 27 октября 2016 года № 1118 «Об утверждении Положения о проведении демонстрационного экзамена с учётом

требований стандартов Worldskills в рамках итоговой аттестации по образовательным программам среднего профессионального образования»;

Методические рекомендации о проведении аттестации с использованием механизма демонстрационного экзамена, утвержденные распоряжением Министерства просвещения Российской Федерации от 1 апреля 2019 г. №Р-42

Положение о итоговой аттестации выпускников, освоивших программы среднего профессионального образования;

Программа ИА по специальности 09.02.06 «Сетевое и системное администрирование»; Приказ колледжа ОмГТУ «Об утверждении председателей Государственных экзаменационных комиссий»;

Приказ колледжа ОмГТУ «Об утверждении состава апелляционной комиссии»;

Приказ о допуске выпускников к ИА;

Приказы о закреплении тем ВКР, назначении руководителей и консультантов по ним; Протокол ознакомления студентов с Программой ИА;

Г рафик контроля выполнения ВКР обучающимися;

документы, подтверждающие освоение обучающимися компетенций при изучении теоретического материала и прохождении практики по каждому из основных видов деятельности:

сводные ведомости результатов обучения студентов;

итоговые ведомости результатов обучения (для выпускников, осваивающих программы подготовки квалифицированных рабочих, служащих); зачётные книжки;

оценочные листы экзаменов (квалификационных) по видам деятельности; производственные характеристики обучающихся; аттестационные листы по практике;

копии протоколов ДЭ, которые являются подтверждением выполнения студентами части ВКР;

Книга протоколов заседаний ЭК.

3 ТИПОВОЕ ЗАДАНИЕ ДЛЯ ДЕМОНСТРАЦИОННОГО ЭКЗАМЕНА

Конкурсное задание включает в себя следующие разделы:

1. Формы участия в конкурсе
2. Задание для конкурса
3. Модули задания и необходимое время
4. Критерии оценки
5. Необходимые приложения

ФОРМЫ УЧАСТИЯ В КОНКУРСЕ

Индивидуальный конкурс.

ЗАДАНИЕ ДЛЯ КОНКУРСА

Содержанием конкурсного задания являются работы по пуско-наладке сетевой инфраструктуры на базе современного сетевого оборудования и операционных систем семейства Windows и Linux. Участники получают инструкцию, сетевые диаграммы и методические рекомендации по выполнению. Конкурсное задание имеет несколько модулей, выполняемых последовательно.

МОДУЛИ ЗАДАНИЯ И НЕОБХОДИМОЕ ВРЕМЯ

Модули и время приведены в таблице

Задание ДЭ представляет собой сочетание модулей в зависимости от вида аттестации и уровня ДЭ. Продолжительность выполнения каждого модуля задания представлена в таблице № 12.

Таблица № 12

Модули	Вид деятельности / Вид профессиональной деятельности	Продолжительность выполнения Модуля / совокупности Модулей и общее время на выполнение задания		
		ДЭ в рамках ПА	ГИА ДЭ БУ	ГИА ДЭ ПУ (инвариантная часть)
Модуль 1	Выполнение работ по проектированию сетевой инфраструктуры	1 ч. 00 мин.	1 ч. 00 мин.	1 ч. 00 мин.
Модуль 2	Организация сетевого администрирования		1 ч. 30 мин.	1 ч. 30 мин.
Модуль 3	Эксплуатация объектов сетевой инфраструктуры			1 ч. 30 мин.
Максимальная продолжительность демонстрационного экзамена:		1 ч. 00 мин.	2 ч. 30 мин.	4 ч. 00 мин.

1 Задание

1.1 Модуль 1: Настройка сетевой инфраструктуры

Необходимо разработать и настроить инфраструктуру информационно - коммуникационной системы согласно предложенной топологии (см. Рисунок 1)

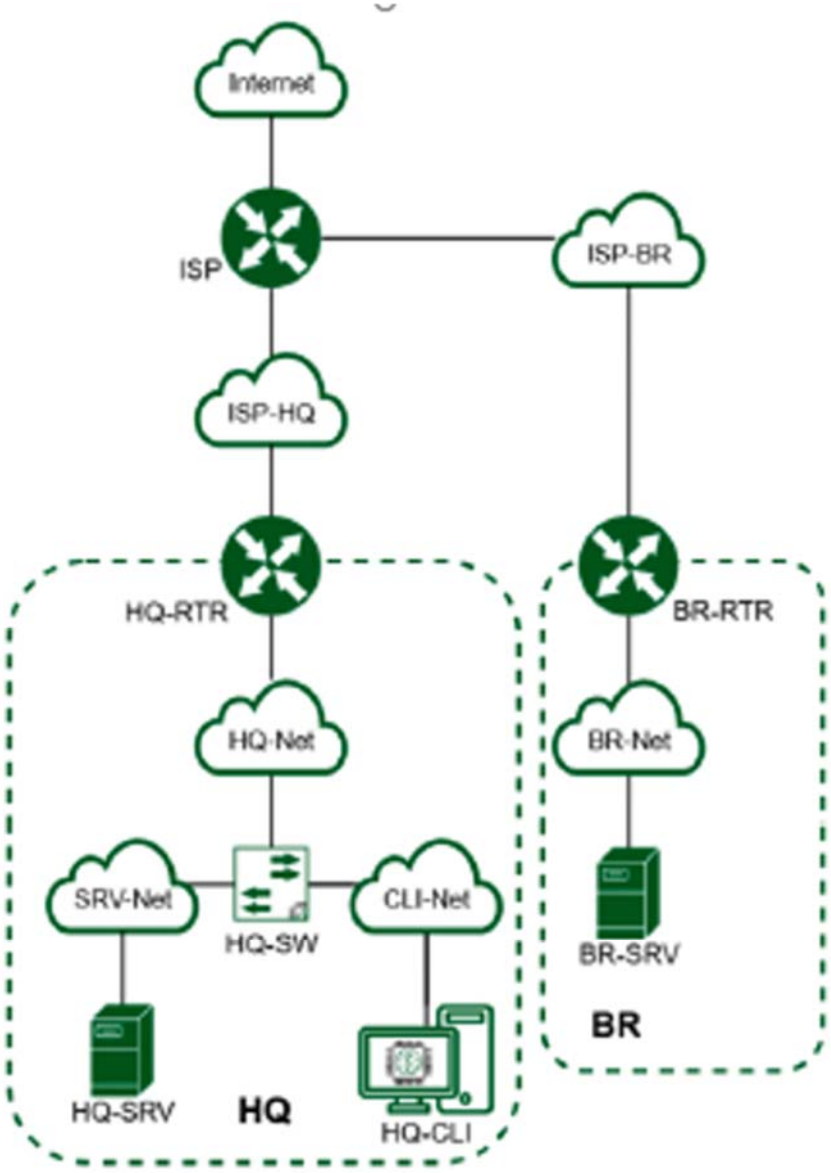


Рисунок 1. Топология сети

Задание включает базовую настройку устройств:

- присвоение имен устройствам
- расчет IP-адресации
- настройку коммутации и маршрутизации

В ходе проектирования и настройки сетевой инфраструктуры следует вести отчет о своих действиях, включая таблицы и схемы, предусмотренные в задании

По каждому пункту задания, требующего отчёт, составить текстовый документ, название которого должно содержать индекс пункта и краткое описание. Текстовый документ должен содержать текстовую информацию и может включать снимки экрана, кадрированные таким образом, чтобы относящаяся к выполнению задания информация на снимках была читаемой.

Итоговый отчет по окончании работы следует сохранить на диске рабочего места и задать имя файла - ФамилияУчастникаМодуль1 без учёта расширения

Задание модуль 1

1. Произведите базовую настройку устройств:

- Настройте имена устройств согласно топологии. Используйте полное доменное имя
- На всех устройствах необходимо сконфигурировать IPv4:
    - IP-адрес должен быть из приватного диапазона, в случае, если сеть локальная, согласно RFC1918
    - Локальная сеть в сторону HQ-SRV(VLAN 100) должна вмещать не более 32 адресов
    - Локальная сеть в сторону HQ-CLI(VLAN 200) должна вмещать не менее 16 адресов
    - Локальная сеть для управления(VLAN 999) должна вмещать не более 8 адресов
    - Локальная сеть в сторону BR-SRV должна вмещать не более 16 адресов
- Сведения об адресах занесите в **таблицу 2**, в качестве примера используйте

Прил_3_О1_КОД 09.02.06-1-2026-М1

2. Настройте доступ к сети Интернет, на маршрутизаторе ISP:

- Настройте адресацию на интерфейсах:
- Интерфейс, подключенный к магистральному провайдеру, получает адрес по DHCP
- Настройте маршрут по умолчанию, если это необходимо
- Настройте интерфейс, в сторону HQ-RTR, интерфейс подключен к сети 172.16.1.0/28
- Настройте интерфейс, в сторону BR-RTR, интерфейс подключен к сети 172.16.2.0/28
- На ISP настройте динамическую сетевую трансляцию портов для доступа к сети Интернет HQ-RTR и BR-RTR.

3. Создайте локальные учетные записи на серверах HQ-SRV и BR-SRV:

- Создайте пользователя sshuser
- Пароль пользователя sshuser с паролем P@ssw0rd
- Идентификатор пользователя 2026
- Пользователь sshuser должен иметь возможность запускать sudo без ввода пароля
- Создайте пользователя net_admin на маршрутизаторах HQ-RTR и BR- RTR
- Пароль пользователя net_admin с паролем P@ssw0rd
- При настройке ОС на базе Linux, запускать sudo без ввода пароля
- При настройке ОС отличных от Linux пользователь должен обладать максимальными привилегиями.

4. Настройте коммутацию в сегменте HQ следующим образом:

- Трафик HQ-SRV должен принадлежать VLAN 100
- Трафик HQ-CLI должен принадлежать VLAN 200
- Предусмотреть возможность передачи трафика управления в VLAN 999
- Реализовать на HQ-RTR маршрутизацию трафика всех указанных VLAN с использованием одного сетевого адаптера ВМ/физического порта
- Сведения о настройке коммутации внесите в отчёт

5. Настройте безопасный удаленный доступ на серверах HQ-SRV и BR- SRV:

- Для подключения используйте порт 2026
- Разрешите подключения исключительно пользователю sshuser
- Ограничьте количество попыток входа до двух
- Настройте баннер «Authorized access only».

6. Между офисами HQ и BR, на маршрутизаторах HQ-RTR и BR-RTR необходимо сконфигурировать ip туннель:
- На выбор технологии GRE или IP in IP
- Сведения о туннеле занесите в отчёт.
7. Обеспечьте динамическую маршрутизацию на маршрутизаторах HQ- RTR и BR-RTR: сети одного офиса должны быть доступны из другого офиса и наоборот. Для обеспечения динамической маршрутизации используйте link state протокол на усмотрение участника:
- Разрешите выбранный протокол только на интерфейсах ip туннеля
- Маршрутизаторы должны делиться маршрутами только друг с другом
- Обеспечьте защиту выбранного протокола посредством парольной защиты
- Сведения о настройке и защите протокола занесите в отчёт.
8. Настройка динамической трансляции адресов маршрутизаторах HQ- RTR и BR-RTR:
- Настройте динамическую трансляцию адресов для обоих офисов в сторону ISP, все устройства в офисах должны иметь доступ к сети Интернет
9. Настройте протокол динамической конфигурации хостов для сети в сторону HQ-CLI:
- Настройте нужную подсеть
- В качестве сервера DHCP выступает маршрутизатор HQ-RTR
- Клиентом является машина HQ-CLI
- Исключите из выдачи адрес маршрутизатора
- Адрес шлюза по умолчанию - адрес маршрутизатора HQ-RTR
- Адрес DNS-сервера для машины HQ-CLI - адрес сервера HQ-SRV
- DNS-суффикс - au-team.irpo
- Сведения о настройке протокола занесите в отчёт.
10. Настройте инфраструктуру разрешения доменных имён для офисов HQ и BR:
- Основной DNS-сервер реализован на HQ-SRV
- Сервер должен обеспечивать разрешение имён в сетевые адреса устройств и обратно в соответствии с **таблицей 3**
- В качестве DNS сервера пересылки используйте любой общедоступный DNS сервер(77.88.8.7, 77.88.8.3 или другие)
11. Настройте часовой пояс на всех устройствах (за исключением виртуального коммутатора, в случае его использования) согласно месту проведения экзамена

Таблица 2

Имя устройства	IP-адрес	Шлюз по умолчанию
HQ-RTR		
BR-RTR		
HQ-SRV		
HQ-CLI		
BR-SRV		

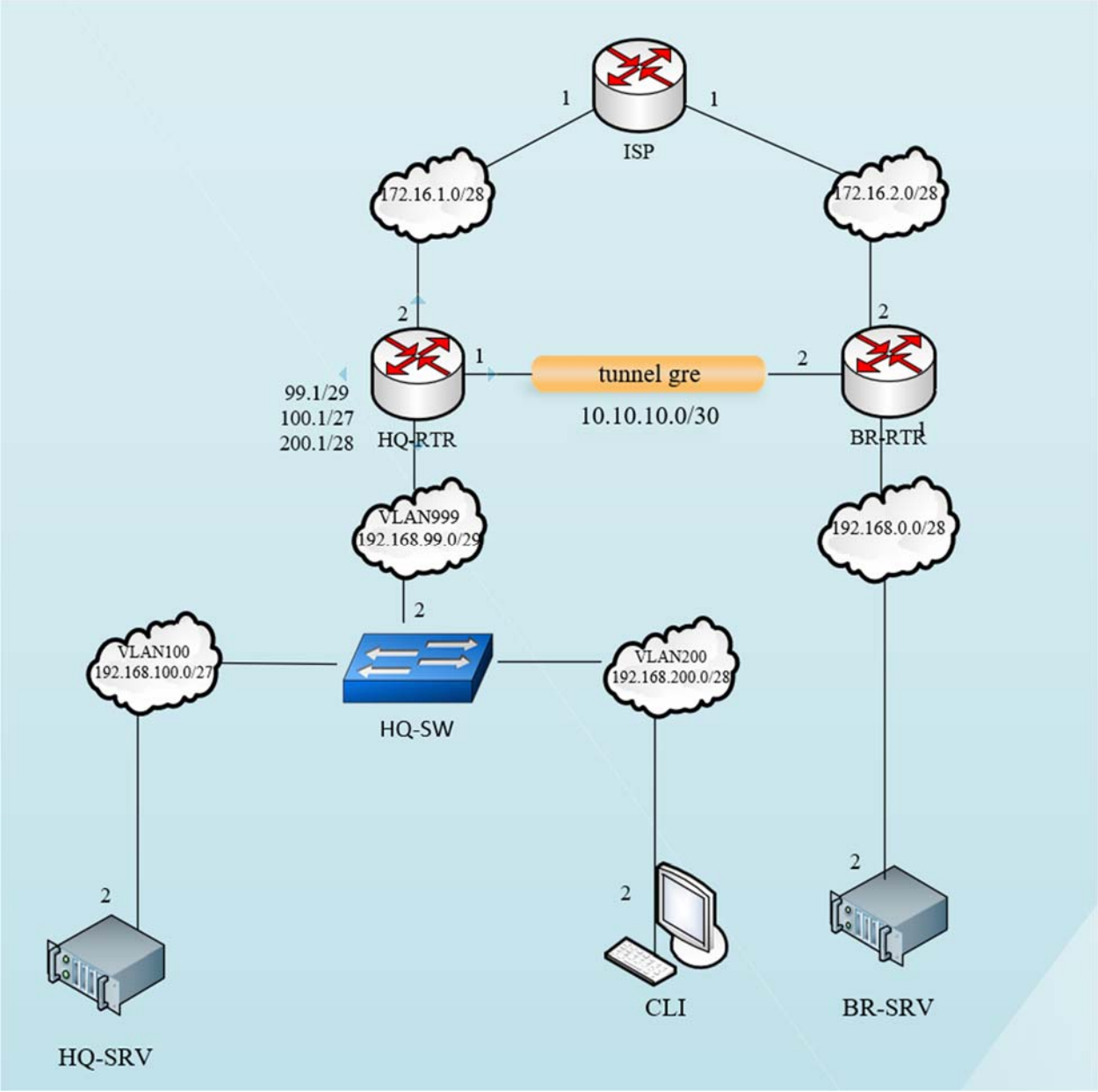
шина	**RAM, ГБ**	**CPU**	**HDD/SDD, ГБ**	**ОС**
ISP	1	1	10	Альт JeOS (p11)
HQ-RTR	4	2	6	EcoRouterOS (Jasmine)
BR-RTR	4	2	6	EcoRouterOS(Jasmine)
HQ-SRV	2	2	20	Альт Сервер 11
BR-SRV	2	2	20	Альт Сервер 11
HQ-CLI	2	2	20	Альт Рабочая Станция 11
HQ-SW	-			Виртуальный коммутатор
Итого	15	11	82	-

Имя устройства	**NIC**	**IP-адрес**	**Шлюз по умолчанию**
HQ-RTR	ISP <-> HQ-RTR	172.16.1.2/28	172.16.1.1

	HQ-RTR <-> HQ - SRV(VLAN100)	192.168.100.1/27	
	HQ-RTR <-> HQ - CLI(VLAN200)	192.168.200.1/28	
	HQ-RTR <-> HQ - SW(VLAN999)	192.168.99.1/29	
	Tunnel (GRE)	10.10.10.1/30	-
BR-RTR	ISP <-> BR-RTR	172.16.2.2/28	172.16.2.1
	BR-RTR <-> BR-SRV	192.168.0.1/28	
	Tunnel (GRE)	10.10.10.2/30	-
HQ-SRV	HQ-SW <-> HQ-CLI (VLAN100)	192.168.100.2/27	192.168.100.1
HQ-CLI	HQ-SW <-> HQ-CLI	192.168.200.2/28	192.168.200.1
BR-SRV	BR-SRV<-> BR-RTR	192.168.0.2/28	192.168.0.1
HQ-SW	ovs-internal (VLAN990)	192.168.99.2/29	192.168.99.1/29

Таблица 3

Устройство	Запись	Тип
HQ-RTR	hq-rtr.au-team.irpo	A,PTR
BR-RTR	br-rtr.au-team.irpo	A
HQ-SRV	hq-srv.au-team.irpo	A,PTR
HQ-CLI	hq-cli .au-team.irpo	A,PTR
BR-SRV	br-srv.au-team.irpo	A
ISP (интерфейс направленный в сторону HQ-RTR)	docker.au-team.irpo	A
ISP (интерфейс направленный в сторону BR-RTR)	web.au-team.irpo	A



Необходимые приложения:

Прил_1_О1_КОД 09.02.06-1-2026-М1: Шаблон отчета

Прил_2_О1_КОД 09.02.06-1-2026-М1: Инструкция по настройке оборудования для технического эксперта ДЭ

Прил_3_О1_КОД 09.02.06-1-2026-М1: Пример заполнения таблицы адресов

Прил_4_О1_КОД 09.02.06-1-2026-М1: Инструкции по оформлению отчёта

Необходимые приложения:

Прил_3_ОЗ_КОД 09.02.06-1-2026-М1.docx Прил_4_ОЗ_КОД 09.02.06-1-2026-М1 .docx Прил_1_ОЗ_КОД 09.02.06-1-2026-М1.docx Прил_2_ОЗ_КОД 09.02.06-1-2026-М1 .docx

Инструкции для ТЭ: Инструкция для технического администратора размещена в приложении

1.2 Модуль 2. Организация сетевого администрирования

Необходимо разработать и настроить инфраструктуру информационно - коммуникационной системы согласно предложенной топологии (см. **Рисунок 2**).

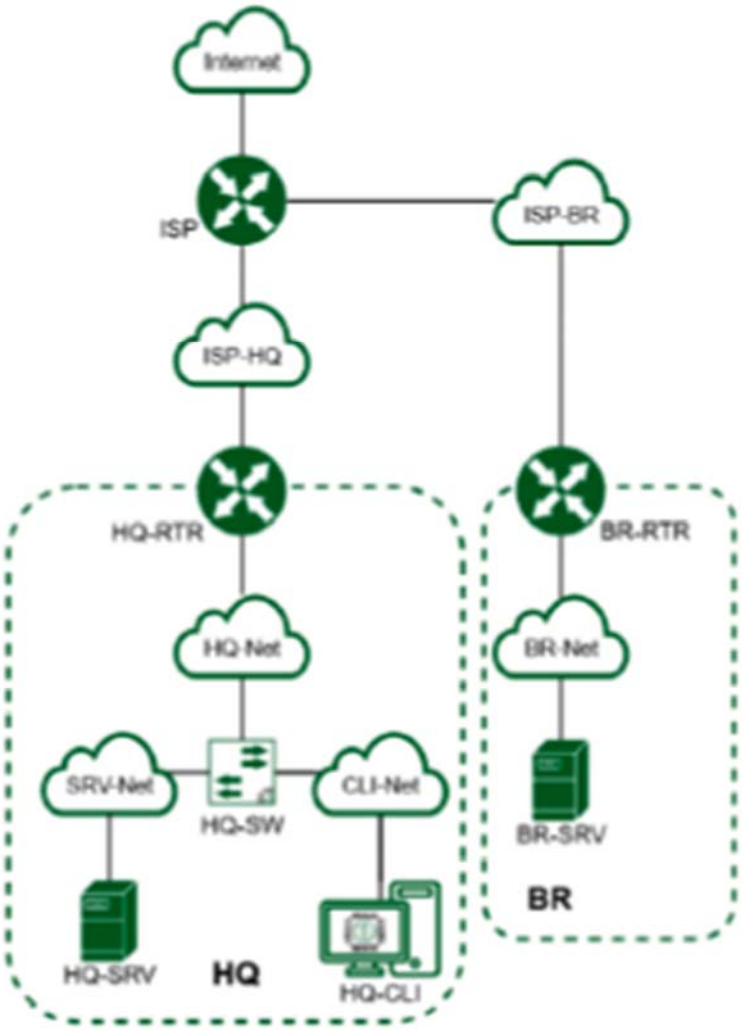
Для модуля 2 используется отдельный стенд. Инструкция по настройке стенда для технических администраторов площадки в отдельном файле.

В стенде преднастроены:

- IP-адреса, маски подсетей и шлюзы по умолчанию
- Сетевая трансляция адресов
- IP туннель
- Динамическая маршрутизация
- Созданы пользователи sshuser на серверах и net_admin на маршрутизаторах, им предоставлены административные привилегии
- Порты ssh на серверах
- DHCP-сервер
- DNS-сервер
- Сервер HQ-SRV имеет три дополнительных накопителя размером 1ГБ

По каждому пункту задания, требующего отчёт, составить текстовый документ, название которого должно содержать индекс пункта и краткое описание. Текстовый документ должен содержать текстовую информацию и может включать снимки экрана, кадрированные таким образом, чтобы относящаяся к выполнению задания информация на снимках была читаемой.

Итоговый отчет по окончании работы следует сохранить на диске рабочего места и задать имя файла - ФамилияУчастникаМодуль2 без учёта расширения



Задание модуль 2

1. Настройте контроллер домена Samba DC на сервере BR-SRV:

- Имя домена au-team.irpo
- Введите в созданный домен машину HQ-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 HQ-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.

2. Сконфигурируйте файловое хранилище на сервере HQ-SRV:

- При помощи двух подключенных к серверу дополнительных дисков размером 1 Гб

сконфигурируйте дисковый массив уровня 0

- Имя устройства - md0, при необходимости конфигурация массива размещается в файле /etc/mdadm.conf
- Создайте раздел, отформатируйте раздел, в качестве файловой системы используйте ext4
- Обеспечьте автоматическое монтирование в папку /raid

3. Настройте сервер сетевой файловой системы (nfs) на HQ-SRV:

- В качестве папки общего доступа выберите /raid/nfs, доступ для чтения и записи исключительно для сети в сторону HQ-CLI
- На HQ-CLI настройте автомонтирование в папку /mnt/nfs
- Основные параметры сервера отметьте в отчёте

4. Настройте службу сетевого времени на базе сервиса chrony на маршрутизаторе ISP:

- Вышестоящий сервер ntp на маршрутизаторе ISP - на выбор участника
- Стратум сервера - 5
- В качестве клиентов ntp настройте: HQ-SRV, HQ-CLI, BR-RTR, BR- SRV.

5. Сконфигурируйте ansible на сервере BR-SRV:

- Сформируйте файл инвентаря, в инвентарь должны входить HQ-SRV, HQ-CLI, HQ-RTR и BR-RTR
- Рабочий каталог ansible должен располагаться в /etc/ansible
- Все указанные машины должны без предупреждений и ошибок отвечать pong на команду ping в ansible посланную с BR-SRV.

6. Разверните веб приложение в docker на сервере BR-SRV:

- Средствами docker должен создаваться стек контейнеров с веб приложением и базой данных
- Используйте образы site_latesta mariadb_latestрасполагающиеся в директории docker в образе Additional.iso
- Основной контейнер testapp должен называться tespapp
- Контейнер с базой данных должен называться db
- Импортируйте образы в docker, укажите в yaml файле параметры подключения к СУБД, имя БД - testdb, пользователь teste паролем P@ssw0rd, порт приложения 8080, при необходимости другие параметры
- Приложение должно быть доступно для внешних подключений через порт 8080

7. Разверните веб приложение на сервере HQ-SRV:

- Используйте веб-сервер apache
- В качестве системы управления базами данных используйте mariadb
- Файлы веб приложения и дамп базы данных находятся в директории web образа Additional.iso
- Выполните импорт схемы и данных из файла dump.sql в базу данных webdb
- Создайте пользователя weta паролем P@ssw0rd и предоставьте ему права доступа к этой базе данных
- Файлы index.php и директорию images скопируйте в каталог веб сервера apache
- В файле index.php укажите правильные учётные данные для подключения к БД
- Запустите веб сервер и убедитесь в работоспособности приложения
- Основные параметры отметьте в отчёте

8. На маршрутизаторах сконфигурируйте статическую трансляцию портов:

- Пробросьте порт 8080 в порт приложения testapp BR-SRV на маршрутизаторе BR-RTR, для обеспечения работы приложения testapp извне
- Пробросьте порт 8080в порт веб приложения на HQ-SRV на маршрутизаторе HQ-RTR, для обеспечения работы веб приложения извне
- Пробросьте порт 2026 на маршрутизаторе HQ-RTR в порт 2026сервера HQ-SRV, для подключения к серверу по протоколу ssh из внешних сетей
- Пробросьте порт 2026 на маршрутизаторе BR-RTR в порт 2026сервера BR-SRV, для подключения к серверу по протоколу ssh из внешних сетей.

9. Настройте веб-сервер nginx как обратный прокси-сервер на ISP

- При обращении по доменному имени web.au-team.irpo у клиента должно открываться веб приложение на HQ-SRV
- При обращении по доменному имени docker.au-team.irpo клиента должно открываться веб приложение testapp

10. На маршрутизаторе ISP настройте web-based аутентификацию:

- При обращении к сайту web.au-team.irpo клиенту должно быть предложено ввести аутентификационные данные
    - В качестве логина для аутентификации выберите WEBс паролем P@ssw0rd
    - Выберите файл /etc/nginx/.htpasswd в качестве хранилища учётных записей
    - При успешной аутентификации клиент должен перейти на веб сайт.

11. Удобным способом установите приложение Яндекс Браузер на HQ-CLI

- Установку браузера отметьте в отчёте.

Необходимые приложения:

Прил_5_ОЗ_КОД 09.02.06-1 -2026-М2.txt

Инструкции для ТЭ: Инструкция для технического администратора размещена в приложении

4. ПОРЯДОК ОРГАНИЗАЦИИ И ПРОВЕДЕНИЯ ЗАЩИТЫ ВЫПУСКНЫХ КВАЛИФИКАЦИОННЫХ РАБОТ

Порядок оценки защиты выпускной квалификационной работы.

К итоговой аттестации допускается студент, не имеющий академической задолженности и в полном объеме выполнивший учебный план или индивидуальный учебный план по осваиваемой образовательной программе среднего профессионального образования (часть 6 статьи 59 Федерального закона от 29 декабря 2012 г. N 273-ФЗ "Обобразовании в Российской Федерации").

Вопрос о допуске ВКР к защите решается на расширенных заседаниях педагогического совета отделения с приглашением председателей соответствующих направлению ВКР предметных цикловых комиссий.

Защита выпускных квалификационных работ (за исключением работ по закрытой тематике) проводятся на открытых заседаниях экзаменационной комиссии (ЭК) с участием не менее двух третей ее состава.

На процедуру защиты ВКР отводится до 1 академического часа на одного обучающегося. Процедура защиты устанавливается председателем ЭК по согласованию с членами ЭК и как, правило, включает доклад обучающегося (не более 15 минут), чтение отзыва и рецензии, вопросы членов комиссии, ответы обучающегося. Обучающимся и лицам, привлекаемым к итоговой аттестации, во время ее проведения запрещается иметь при себе и использовать средства связи.

Результаты любой из форм итоговой аттестации определяются оценками "отлично", "хорошо", "удовлетворительно", "неудовлетворительно" и объявляются в тот же день после оформления в установленном порядке протоколов заседаний государственных экзаменационных комиссий.

Решения экзаменационных комиссий принимаются на закрытых заседаниях простым большинством голосов членов комиссии, участвующих в заседании, при обязательном присутствии Председателя комиссии или его заместителя. При равном числе голосов голос председательствующего на заседании экзаменационной комиссии является решающим.

Лицам, не проходившим итоговой аттестации по уважительной причине, предоставляется возможность пройти итоговую аттестацию без отчисления из Колледжа.

Дополнительные заседания экзаменационных комиссий организуются в установленные колледжем дополнительные сроки, но не позднее четырех месяцев после подачи заявления лицом, не проходившим итоговой аттестации по уважительной причине.

Обучающиеся, не прошедшие ИА или получившие на ИА неудовлетворительные результаты, проходят ИА не ранее, чем через шесть месяцев после прохождения ИА впервые.

Для прохождения ИА, лицо, не прошедшее итоговую аттестацию по неуважительной причине или получившее на итоговой аттестации неудовлетворительную оценку, восстанавливается в Колледже на период времени, установленный Колледжем, но не менее

предусмотренного календарным учебным графиком для прохождения итоговой аттестации соответствующей образовательной программы среднего профессионального образования.

Повторное прохождение итоговой аттестации для одного лица назначается колледжем не более двух раз.

Решение экзаменационной комиссии оформляется протоколом, который подписывается Председателем экзаменационной комиссии (в случае отсутствия Председателя - его заместителем) и секретарем экзаменационной комиссии и хранится в архиве колледжа.Защита выпускной квалификационной работы производится в установленное время на заседании экзаменационной комиссии (ЭК) по соответствующей специальности.

Защита начинается с доклада студента по содержанию выпускной квалификационной работы. Студент должен излагать основное содержание доклада свободно, не читая письменного текста. Доклад студента не должен занимать более 10 минут и должен содержать обоснование актуальности работы, изложение логики исследования (проблема, объект, предмет, цель и задачи и т.д.), основных результатов проведенного исследования и практических рекомендации по вопросам изучения.

Студенту следует отметить личный вклад в исследование, чем он руководствовался при работе над темой, какие методы использованы при изучении рассматриваемой проблемы, какие новые результаты достигнуты в ходе исследования и каковы вытекающие из исследования основные выводы.

Это общая схема доклада; более конкретно его содержание определяется дипломником совместно с научным руководителем.

После завершения доклада члены ЭК задают студенту вопросы, как непосредственно связанные с темой выпускной квалификационной работы, так и близко к ней относящиеся. При ответах на вопросы студент имеет право пользоваться своей работой.

После ответов дипломника на вопросы зачитывается внешняя рецензия и предоставляется заключительное слово дипломнику. В своем заключительном слове студент должен ответить на замечания внешнего рецензента и членов ЭК.

После заключительного слова студента процедура защиты выпускной квалификационной работы считается оконченной.

При выставлении окончательной оценки по результатам защиты выпускной квалификационной работы учитываются:

- мнение научного руководителя о качестве работы, степени ее соответствия требованиям, предъявляемым к работе;
- оценка рецензента за работу в целом, учитывая степень обоснованности выводов и рекомендаций, их новизны и практической значимости

оценки членов ЭК за содержание работы, ее защиту, включая доклад, ответы на замечания рецензента.

Итоговая оценка по результатам защиты выпускной квалификационной работы студента проставляется по пятибалльной системе и заносится в протокол заседания ко-

миссии и зачетную книжку студента, в которых расписывается председатель и члены экзаменационной комиссии.

№	Тема выпускной квалификационной работы	Наименование профес-сиональных модулей, от-ражаемых в работе
1.	Проектирование сети предприятия с использованием автоматиче-ского назначения IPv6 в SLAAC	ПМ 02
2.	Проектирование и администрирование компьютерной сети пред-приятия	ПМ 01 ПМ 02
3.	Проектирование и администрирование компьютерной сети офиса с обеспечением удаленного доступа	ПМ 01 ПМ 02
4.	Организация и конфигурирование локальных корпоративных сетей и их объединение с помощью VPN	ПМ 01 ПМ 02
5.	Проектирование и обслуживание VLAN на коммутаторах в ком-пьютерной сети офиса	ПМ 01
6.	Конфигурация сетевой инфраструктуры с использованием ОС LINUX	ПМ 03
7.	Проектирование и администрирование компьютерной сети офиса с обеспечением удаленного доступа	ПМ 01 ПМ 02
8.	Проектирование сети предприятия через NAT и анализ трансляции адресов	ПМ 03
9.	Организация и администрирование сети с применением Штелефо-нии	ПМ 01 ПМ 03
10.	Проектирование и администрирование сети отделов с разными операционными системами с использованием IPv6	ПМ 02 ПМ 03
11.	Проектирование и обеспечение защиты сети от внешних угроз и аналитика безопасности сетевой инфраструктуры	ПМ 01 ПМ 03
12.	Обеспечение безопасности компьютерной сети офиса	ПМ 02 ПМ 03
13.	Администрирование сегмента сети с использованием адресации IPv6 и анализ работы протокола NDP	ПМ 01 ПМ 03
14.	Проектирование и администрирование компьютерной сети пред-приятия с использованием бездисковых станций	ПМ 02 ПМ 03
15.	Проектирование инфраструктуры с использованием удаленных рабочих стволов	ПМ 01 ПМ 02
16.	Проектирование и администрирование сети с использованием разных дистрибутивов Linux	ПМ 01 ПМ 03
17.	Конфигурация служб хранения данных на ОС LINUX	ПМ 02 ПМ 03
18.	Проектирование сети предприятия с использованием автоматиче-ского назначения IPv6 в DHCPv6	ПМ 01 ПМ 02
19.	Администрирование сегмента сети с использованием адресации	ПМ 01

	IPv6	ПМ 02
20.	Проектирование сети с использованием протокола агрегирования каналов	ПМ 01 ПМ 02
21.	Проектирование сети с использованием протокола teredo	ПМ 01 ПМ 02
22.	Проектирование сети офисов с обеспечением беспроводных точек доступа	ПМ 01 ПМ 02
23.	Проектирование сети на базе маршрутизации IPv6 с обеспечением безопасности и использованием новейших трендов сети, и методом их разработки	ПМ 01 ПМ 03
24.	Описание процесса предоставления доступа и контроля над ним через AAA в корпоративной сети	ПМ 01 ПМ 03
25.	Проектирование сети с подключением маршрутизаторов через PPPoE	ПМ 01 ПМ 03
26.	Обеспечение безопасности удалённого доступа сети предприятия	ПМ 02 ПМ 03
27.	Проектирование сети с использованием зашифрованных паролей на пользовательский и привилегированный режимах, на виртуальных и консольных линиях	ПМ 02 ПМ 03
28.	Организация и обеспечение информационной безопасности ком-пьютерной сети	ПМ 02 ПМ 03
29.	Проектирование и обслуживание сети	ПМ 01 ПМ 02
30.	Создание и администрирование сегмента локальной сети пред-приятия	ПМ 01 ПМ 03
31.	Администрирование компьютерной сети предприятия с обеспече-нием стратегий групповых политик	ПМ 02 ПМ 03
32.	Организация и администрирование корпоративного сервера на базе Linux сервера	ПМ 02 ПМ 03

Структура и содержание выпускной квалификационной работы

Требования к выполнению выпускной квалификационной работы ВКР (дипломная работа) по структуре состоит из введения, двух разделов и заключения. Материалы дипломной работы располагаются в следующейпоследовательности: титульный лист;

оглавление с указанием разделов, подразделов и страниц; введение;

теоретическая часть ВКР; практическая часть ВКР; заключение;

список использованных источников; приложения.

Краткая характеристика разделов:

Содержание выпускной квалификационной работы.

Основную часть выпускной квалификационной работы составляют теоретические и практические разделы, разделённые на пункты. Общее количество пунктов, как в теоретической, так и в практической части должно быть не менее трех и не более пяти. Разделы и тема выпускной квалификационной работы не могут называться одинаково. Раздел или пункт не могут иметь название, состоящее из одного слова.

Введение - вступительная часть выпускной квалификационной работы. Объем введения должен быть небольшим - 1,5-2 страницы. Введение к выпускной квалификационной работе в обязательном порядке содержит следующие элементы: актуальность, цель, задачи, объект и предмет выпускной квалификационной работы.

Основная часть ВКР должна состоять из практической и теоретической.

В теоретической части дается теоретическое освещение темы на основе полученной информации, аспектов изучаемого объекта и предмета ВКР. В ней содержится обзор используемых источников информации, нормативной базы по теме ВКР.

В ***практической части*** проводится анализ практического материала, полученного во время преддипломной практики, а так же разрабатываются практические предложения и мероприятия по улучшению организации и контроля текущей деятельности работников различных служб (структурных подразделений) гостиничных и туристических комплексов (предприятий) с учётом инновационных изменений.

Изложение содержания работы должно быть строго логичным. Особое внимание следует обратить на переход от одного раздела к другому. Содержание основной части должно соответствовать тематике дипломной работы.

Заключение подводит итог решения тех задач, которые были поставлены в выпускной квалификационной работе (1 - 2 страницы).

Заключение - последовательное, логически стройное изложение полученных итогов и их соотношение с общей целью и конкретными задачами. Заключение должно содержать краткие выводы по результатам работы, отражающим новизну и практическую значимость, предложения по использованию ее результатов.

После заключения размещается ***список использованных источников и приложения,*** являющийся важной частью выпускной квалификационной работы и отражающий самостоятельность и творческий подход студента. При составлении списка источников и литературы необходимо соблюдать определенную последовательность в перечислении библиографических записей. Список использованных источников отражает перечень источников, которые использовались при написании ВКР (не менее 20).

Выпускная квалификационная работа должна быть выполнена на стандартных листах белой бумаги формата А4 и оформлена в соответствии с требованиями ГОСТ 7.322001 «Отчёт о научно-исследовательской работе. Структура и правила оформления»; ГОСТ Р 7.0.5-2008 «Библиографическая ссылка. Общие требования и правила составления»; ГОСТ 7.1-2003 «Библиографическая запись. Библиографическое описание. Общие требования и правила составления».

На титульном листе дипломной работы ставится подпись руководителя структурного подразделения по направлению подготовки о допуске работы к защите и подписи руководителя и консультанта дипломной работы.

Дипломная работа должна быть выполнена в соответствии с методическими рекомендациями к ВКР

Защита выпускной квалификационной работы проводится в аудитории образовательного комплекса, оснащенной мультимедийным оборудованием, и включает в себя доклад студента, мультимедийную презентацию и экономическое обоснование, чтение рецензии, вопросы членов комиссии, ответы студента, выступление руководителя выпускной квалификационной работы.

Электронная презентация должна помогать обучающемуся представить достоинства выполненной работы, подтвердить освоение общих и профессиональных компетенций. На слайдах должны быть отражены: цели и задачи ВКР, характеристика предмета и объекта исследования, основные этапы исследования, выводы о целесообразности и перспективах практического применения результатов ВКР.

Презентация создается в программе PowerPoint, выполняется в едином стиле. Цветовая гамма и использование анимации не должны препятствовать адекватному восприятию информации. Количество слайдов в презентации не более 25.

Выпускник предоставляет в экзаменационную комиссию дипломную работу на бумажном носителе в жёстком переплете, оформленную в соответствии с ГОСТом.

Общее руководство и контроль за ходом выполнения выпускной квалификационной работы осуществляет руководитель ППССЗ специальности, непосредственное руководство осуществляет руководитель ВКР.

Выполнение выпускной квалификационной работы осуществляется студентом с соблюдением сроков, установленных в календарном плане. В случае нарушения сроков выполнения одного из этапов выполнения ВКР руководитель ВКР ставит в известность руководителя ППССЗ специальности.

Выпускная квалификационная работа, выполненная в полном объёме в соответствии с заданием, подписанная выпускником, передается руководителю ВКР для заключительного контроля. Руководитель пишет отзыв, где отражает качество содержания выполненной ВКР, проводит анализ хода её выполнения, даёт характеристику работы выпускника и выставляет оценку. Отзыв руководителя ВКР о работе выпускника над дипломной работой является основанием для допуска студента к рецензированию ВКР.

Рецензирование выполненных ВКР осуществляется специалистами из числа работников отраслевых предприятий и организаций, которые определяли тематику ВКР, или преподавателями вузов.

Рецензия должна включать:

заключение о соответствии ВКР заданию на неё;

оценку качества выполнения каждого раздела ВКР;

оценку степени разработки перспективных вопросов, оригинальности и практической значимости ВКР;

оценку практической значимости и возможности внедрения (апробации) на предприятии, в организации; оценку ВКР.

Внесение изменений в ВКР после получения рецензии не допускается. Во время защиты студент вправе согласиться или не согласиться с рецензией, обосновав свой выбор.

Отзыв руководителя ВКР, рецензию на ВКР и саму дипломную работу студент сдает руководителю ППССЗ специальности для предоставления их в ЭК до начала её работы.

Приложение 1

ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ ИВАНОВСКОЙ ОБЛАСТИ

ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

«КИНЕШЕМСКИЙ ТЕХНОЛОГИЧЕСКИЙ КОЛЛЕДЖ»

2 Решение. Модуль 1: Настройка сетевой инфраструктуры

2.1. Произведите базовую настройку устройств:

Задание:

- Настройте имена устройств согласно топологии. Используйте полное доменное имя
- На всех устройствах необходимо сконфигурировать IPv4:
  - IP-адрес должен быть из приватного диапазона, в случае, если сеть локальная, согласно RFC1918
  - Локальная сеть в сторону HQ-SRV(VLAN 100) должна вмещать не более 32 адресов
  - Локальная сеть в сторону HQ-CLI(VLAN 200) должна вмещать не менее 16 адресов
  - Локальная сеть для управления(VLAN 999) должна вмещать не более 8 адресов
  - Локальная сеть в сторону BR-SRV должна вмещать не более 16 адресов
- Сведения об адресах занесите в таблицу 2, в качестве примера используйте Приложение Б.

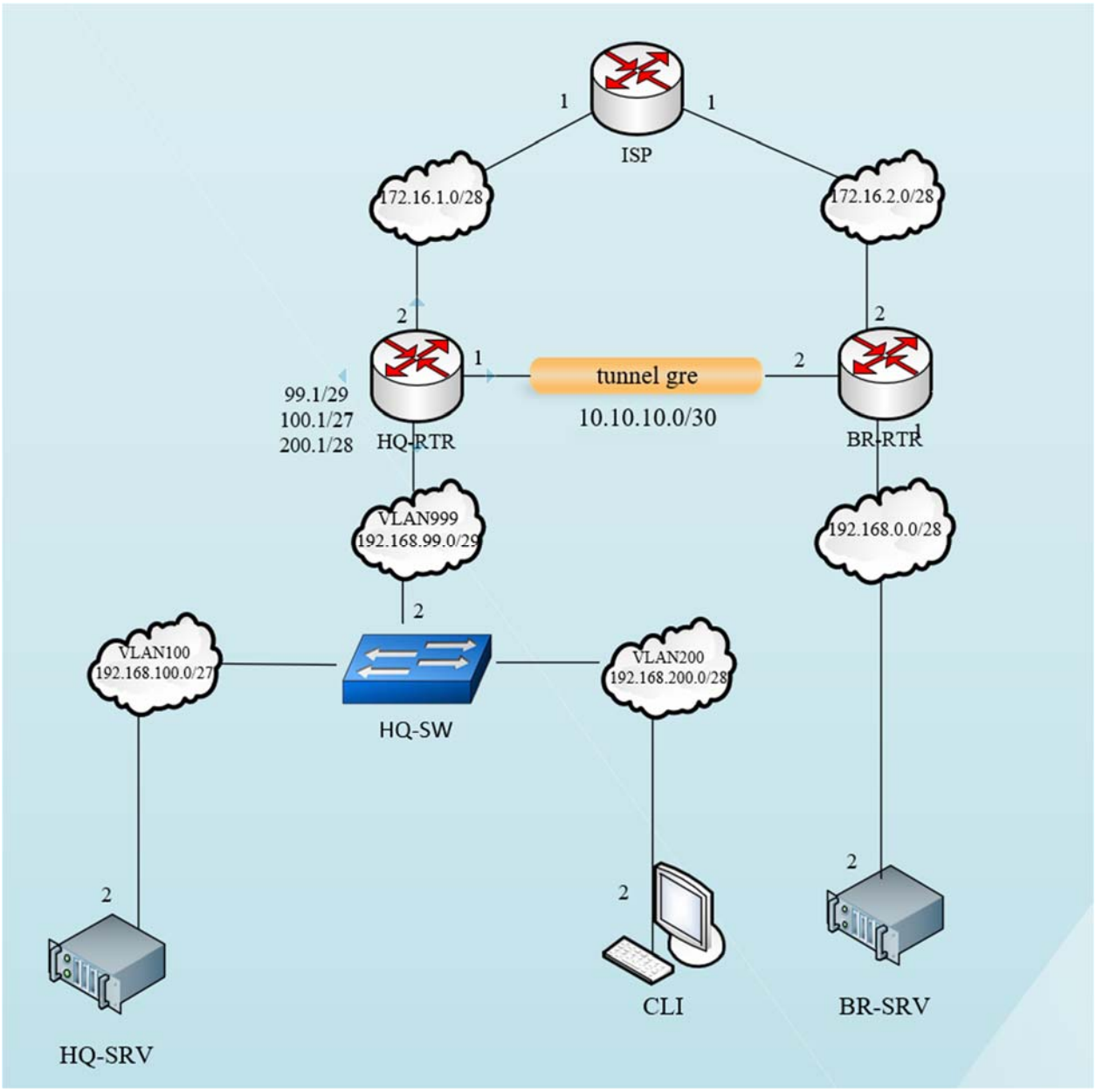
- Сведения об адресах занесите в отчёт, в качестве примера используйте Таблицу 3
  - IP-адрес должен быть из приватного диапазона, в случае, если сеть локальная, согласно RFC1918 (https://www.ietf.org/rfc/rfc1918.txt)

```
3. Private Address Space

   The Internet Assigned Numbers Authority (IANA) has reserved the
   following three blocks of the IP address space for private internets:

     10.0.0.0        -   10.255.255.255  (10/8 prefix)
     172.16.0.0      -   172.31.255.255  (172.16/12 prefix)
     192.168.0.0     -   192.168.255.255 (192.168/16 prefix)
```

- IP калькулятор (https://ipcalc.co/)

Имя устройства	**NIC**	**IP-адрес**	**Шлюз по умолчанию**
HQ-RTR	ISP <-> HQ-RTR	172.16.1.2/28	172.16.1.1
	HQ-RTR <-> HQ - SRV(VLAN100)	192.168.100.1/27	
	HQ-RTR <-> HQ - CLI(VLAN200)	192.168.200.1/28	
	HQ-RTR <-> HQ - SW(VLAN999)	192.168.99.1/29	
	Tunnel (GRE)	10.10.10.1/30	-
BR-RTR	ISP <-> BR-RTR	172.16.2.2/28	172.16.2.1
	BR-RTR <-> BR-SRV	192.168.0.1/28	
	Tunnel (GRE)	10.10.10.2/30	-
HQ-SRV	HQ-SW <-> HQ-CLI (VLAN100)	192.168.100.2/27	192.168.100.1
HQ-CLI	HQ-SW <-> HQ-CLI	192.168.200.2/28	192.168.200.1

BR-SRV	BR-SRV<-> BR-RTR	192.168.0.2/28	192.168.0.1
HQ-SW	ovs-internal (VLAN990)	192.168.99.2/29	192.168.99.1/29



Настройте имена устройств согласно топологии. Используйте полное доменное имя

Доменное имя - au-team.irpo видно в Таблице 2 (DNS - записи);

Исключением является виртуальная машина ISP - задавать полное доменное имя на Internet Service Provider нет смысла;

2.1.1 ISP:

Для назначения имени устройства согласно топологии используем следующую команду:

#hostnamectl set-hostname isp; exec bash

Проверить:

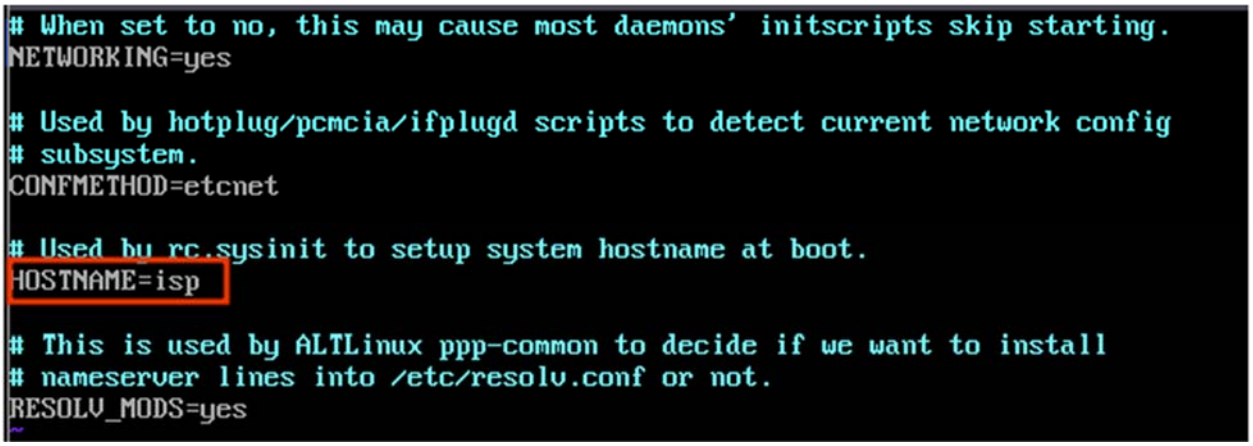
#hostname

Результат:

- Так же рекомендуется указать имя в файле **/etc/sysconfig/network**:

```
#vim /etc/sysconfig/network
```

- указать имя в параметре **HOSTNAME**:



2.1.2 HQ-RTR:

- Для назначения имени устройства согласно топологии используем следующие команды:
  - переходим в привилегированный режим;
  - переходим в режим администрирования;
  - задаём имя устройству;
  - задаём доменное имя;
  - сохраняем конфигурацию.

```
ecorouter>enable

ecorouter#configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

ecorouter(config)#hostname hq-rtr

hq-rtr(config)#ip domain-name au-team.irpo

hq-rtr(config)#write memory

Building configuration...


hq-rtr(config)#
```

- Проверить имя устройства:

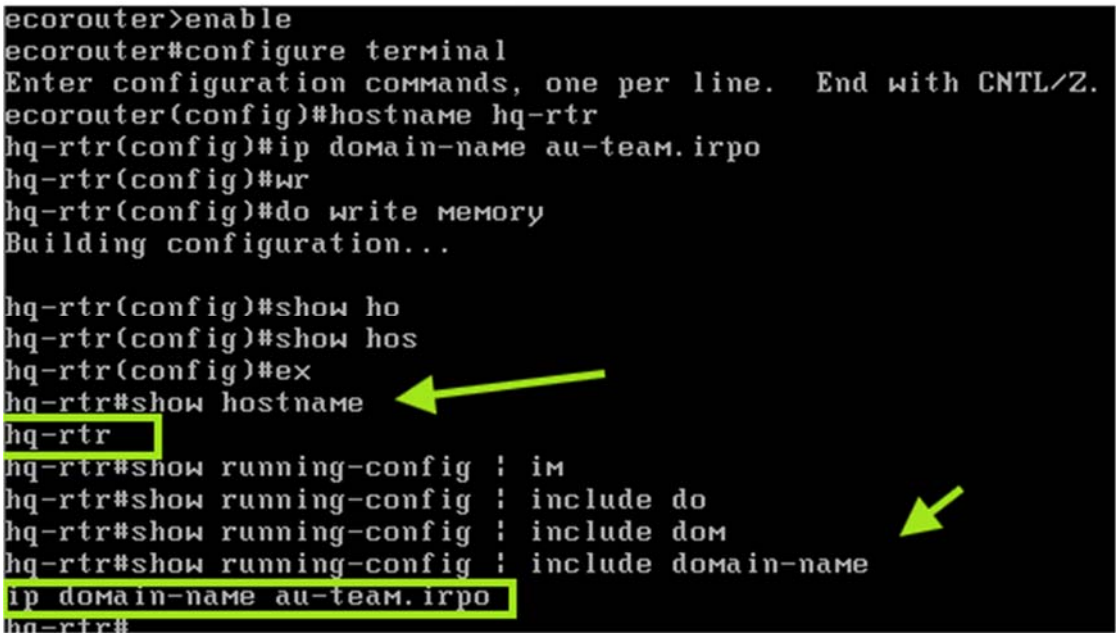
```
hq-rtr#show hostname
```

```
hq-rtr#sh host
hostname  hosts
hq-rtr#show hostname
hq-rtr
hq-rtr#
```

- Проверить доменное имя устройства:

```
hq-rtr#show running-config | include domain-name
```

- Результат:



2.1.3 BR-RTR:

- Аналогично **HQ-RTR**

```
ecorouter>enable

ecorouter#configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.

ecorouter(config)#hostname br-rtr

br-rtr(config)#ip domain-name au-team.irpo

br-rtr(config)#write memory
```

```
Building configuration...


br-rtr(config)#
```

-
  - ожидаемый результат:

2.1.4 HQ-SRV, BR-SRV:

HQ-SRV:

Для назначения имени устройства согласно топологии используем следующую команду:

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

Проверить:

#hostname -f

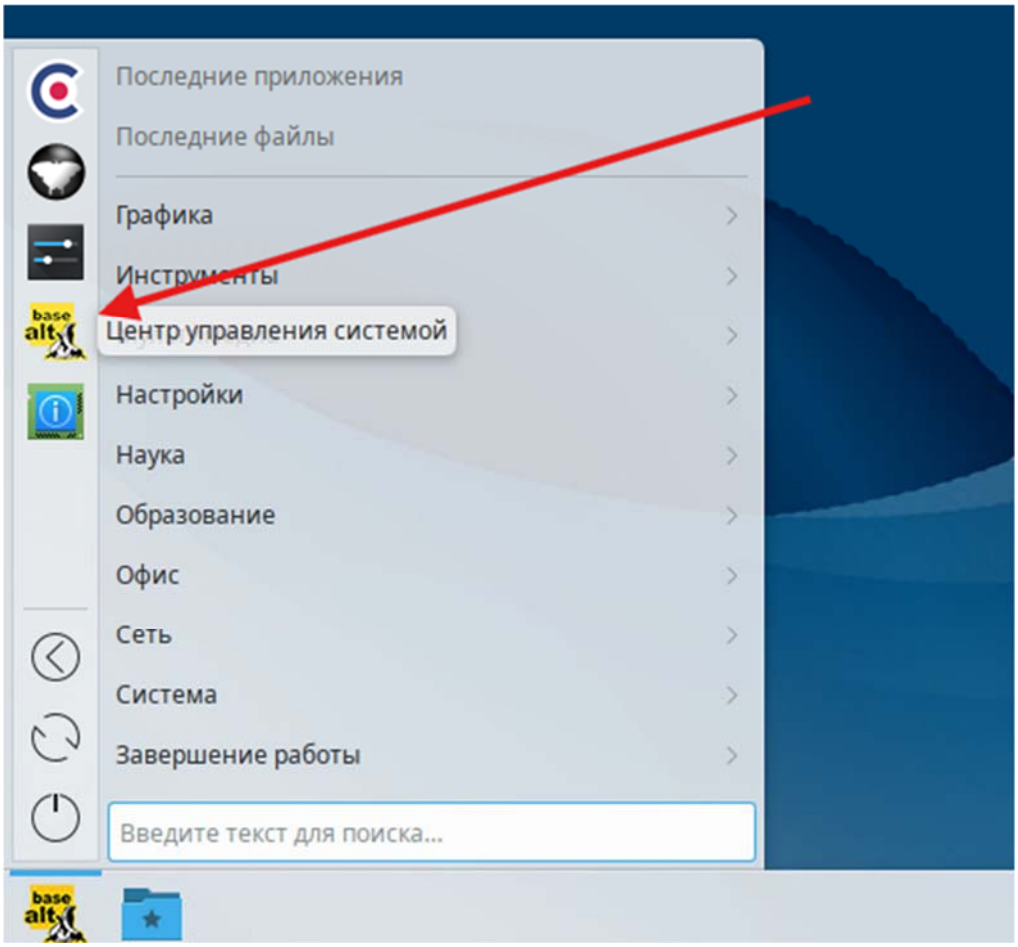
Результат:

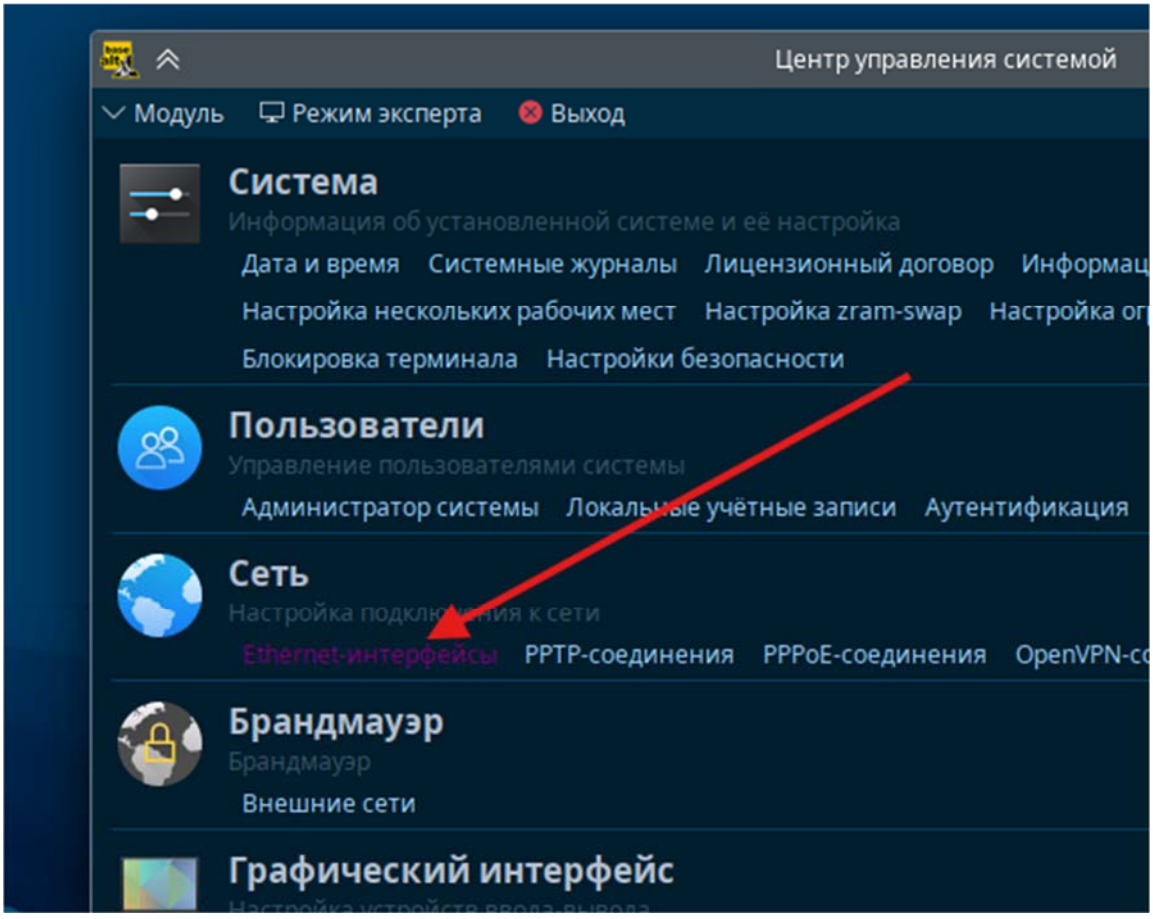
BR-SRV:

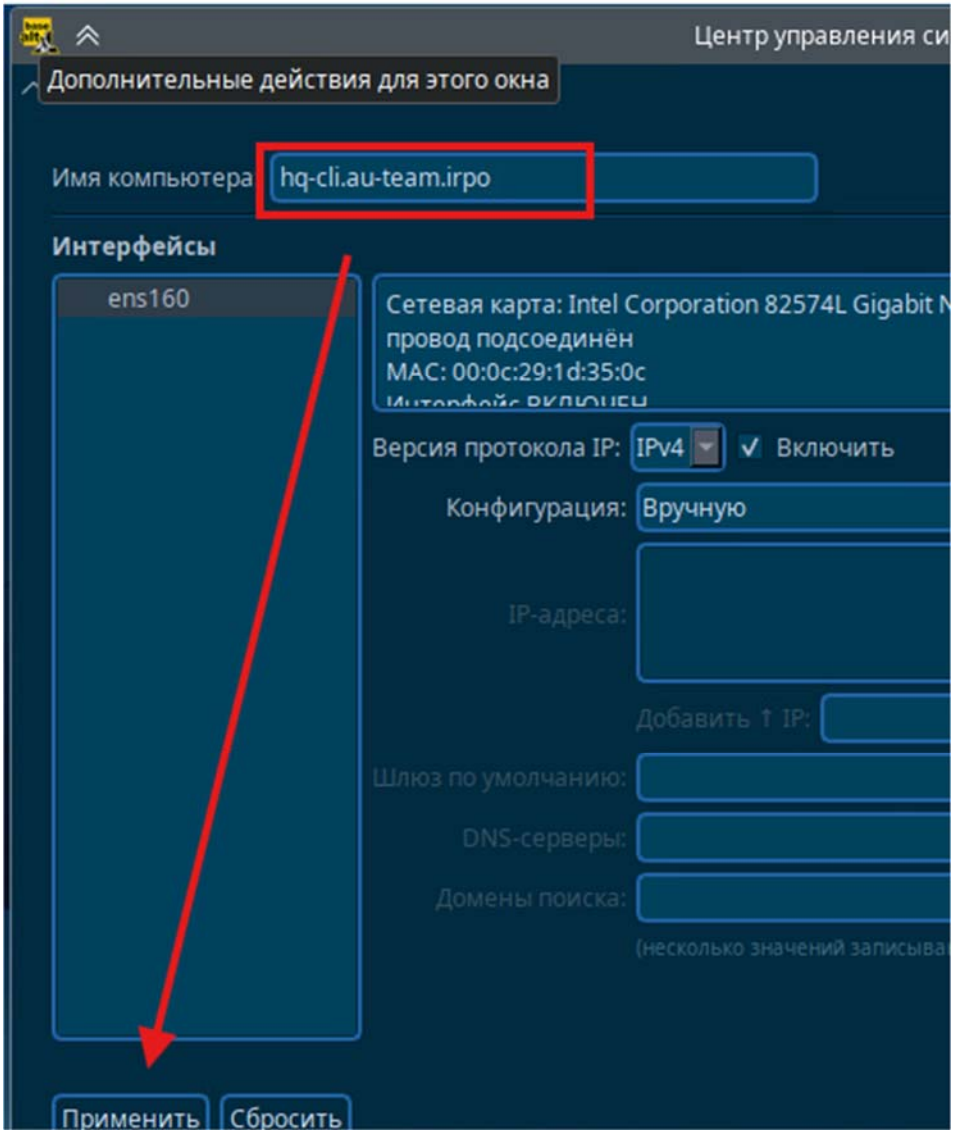
Аналогично **HQ-SRV**, ожидаемый результат:

2.1.5 HQ-CLI:

Для назначения имени устройства согласно топологии воспользуемся Центром Управления Системой (ЦУС):


Последние приложения
Последние файлы
Графика
Инструменты
Центр управления системой
Настройки
Наука
Образование
Офис
Сеть
Система
Завершение работы
Введите текст для поиска...


Центр управления системой
Модуль
Режим эксперта
Выход
Система
Информация об установленной системе и её настройка
Дата и время
Системные журналы
Лицензионный договор
Настройка нескольких рабочих мест
Настройка zram-swap
Блокировка терминала
Настройки безопасности
Пользователи
Управление пользователями системы
Администратор системы
Аутентификация
Сеть
Ethernet-интерфейсы
PPTP-соединения
PPPoE-соединения
Брандмауэр
Брандмауэр
Внешние сети
Графический интерфейс



2.1.6 На всех устройствах необходимо сконфигурировать IPv4

Основные понятия касающиеся EcoRouter:

- **Порт (port)** – это устройство в составе EcoRouter, которое работает на уровне коммутации (L2);
- **Интерфейс (interface)** – это логический интерфейс для адресации, работает на сетевом уровне (L3);
- **Service instance (Сабинтерфейс, SI, Сервисный интерфейс)** является логическим сабинтерфейсом, работающим между L2 и L3 уровнями:

- Данный вид интерфейса необходим для соединения физического порта с интерфейсами L3, интерфейсами bridge, портами;
- Используется для гибкого управления трафиком на основании наличия меток VLANов в фреймах, или их отсутствия;
- Сквозь сервисный интерфейс проходит весь трафик, приходящий на порт.

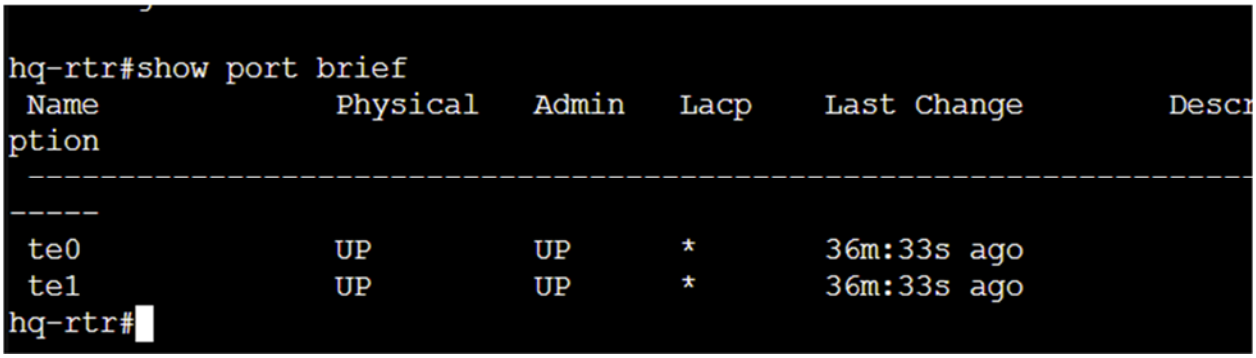
- Таким образом, для того чтобы назначить IPv4-адрес на EcoRouter - необходимо придерживаться следующего алгоритма в общем виде:
  - Создать интерфейс с произвольным именем и назначить на него IPv4;
  - В режиме конфигурирования порта создать service-instance с произвольным именем:
    - указать (инкапсулировать) что будет обрабатываться тегированный или не тегированный трафик;
    - указать в какой интерфейс (ранее созданный) нужно отправить обработанные кадры.

HQ-RTR:

- Посмотреть физические порты можно при помощи следующей команды:

```
hq-rtr#show port brief
```

-
  - где:
    - **te0** - порт в сторону **ISP**;
    - **te1** - порт в сторону **локальной сети офиса HQ** (виртуальный коммутатор HQ-SW);



- Создаём интерфейсы (подинтерфейсы/sub-interfaces) для назначения IP-адресов локальных подсетей офиса **HQ** для дальнейшей маршрутизации между VLAN-ами:
    - первым делом создаём интерфейсы для каждого VLAN-а:

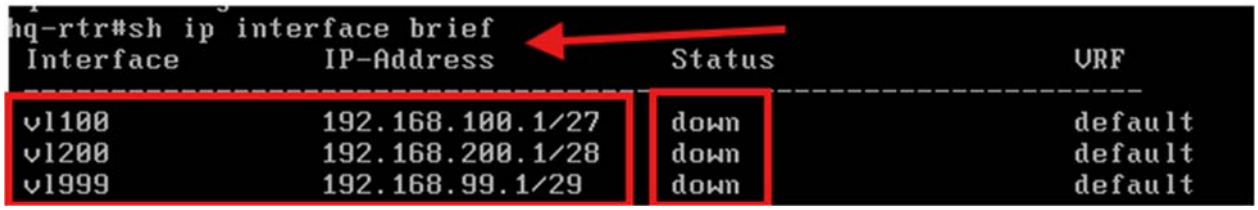
```
hq-rtr(config)#interface vl100
hq-rtr(config-if)#description "VLAN 100"
hq-rtr(config-if)#ip address 192.168.100.1/27
hq-rtr(config-if)#exit
hq-rtr(config)#interface vl200
hq-rtr(config-if)#description "VLAN 200"
hq-rtr(config-if)#ip address 192.168.200.1/28
hq-rtr(config-if)#exit
hq-rtr(config)#interface vl999
hq-rtr(config-if)#description "VLAN 999"
hq-rtr(config-if)#ip address 192.168.99.1/29
hq-rtr(config-if)#exit
hq-rtr(config)#write memory
Building configuration...


hq-rtr(config)#
```

- Проверить, назначенный IP-адреса на интерфейс:

```
hq-rtr#show ip interface brief
```

- Результат:

- созданные интрфейсы пока не добавлены какие-либо Service instance, а значит не привязаны и к порту, отсюда и статус **down**:



- на базе физического интерфейса **te1** для каждого VLAN-а создаём **service-instance** с инкапсуляцией соответствующих тегов (VID) и подключением необходимых интерфейсов:

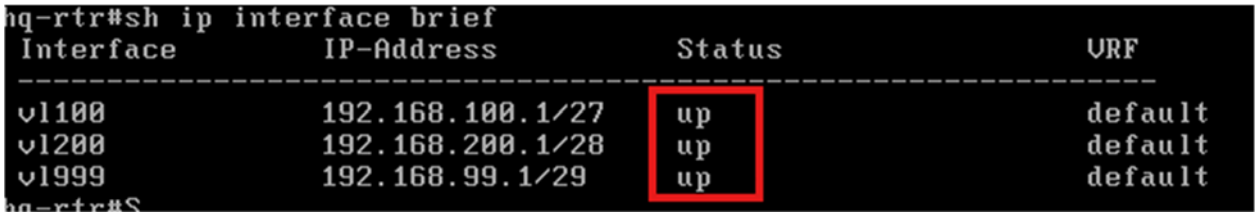
```
hq-rtr(config)#port te1
hq-rtr(config-port)#service-instance te1/vl100
hq-rtr(config-service-instance)#encapsulation dot1q 100 exact
hq-rtr(config-service-instance)#rewrite pop 1
hq-rtr(config-service-instance)#connect ip interface vl100

2025-10-23 05:07:20     INFO     Interface vl100 changed state to up
hq-rtr(config-service-instance)#exit
hq-rtr(config-port)#service-instance te1/vl200
hq-rtr(config-service-instance)#encapsulation dot1q 200 exact
hq-rtr(config-service-instance)#rewrite pop 1
hq-rtr(config-service-instance)#connect ip interface vl200

2025-09-04 05:07:51     INFO     Interface vl200 changed state to up
hq-rtr(config-service-instance)#exit
hq-rtr(config-port)#service-instance te1/vl999
hq-rtr(config-service-instance)#encapsulation dot1q 999 exact
hq-rtr(config-service-instance)#rewrite pop 1
```

```
hq-rtr(config-service-instance)#connect ip interface vl999


2025-09-04 05:08:14     INFO     Interface vl999 changed state to up
hq-rtr(config-service-instance)#exit
hq-rtr(config-port)#exit
hq-rtr(config)#write memory
Building configuration...


hq-rtr(config)#
```

- Проверить, назначенный IP-адреса на интерфейс и статус:

```
hq-rtr#show ip interface brief
```

  - Результат:



BR-RTR:

- Аналогично **HQ-RTR**:

```
br-rtr(config)#interface int1
br-rtr(config-if)#description "BR-Net"
br-rtr(config-if)#ip address 192.168.0.1/28
br-rtr(config-if)#exit
br-rtr(config)#port te1
br-rtr(config-port)#service-instance te1/int1
br-rtr(config-service-instance)#encapsulation untagged
br-rtr(config-service-instance)#connect ip interface int1


2025-09-04 05:13:37     INFO     Interface int1 changed state to up
```

```
br-rtr(config-service-instance)#exit

br-rtr(config-port)#exit

br-rtr(config)#do write memory

Building configuration...


br-rtr(config)#
```

- Ожидаемый результат:

```
br-rtr#sh ip in br
 Interface        IP-Address          Status                VRF
 ------------------------------------------------------------------
 int1             192.168.0.1/28      up                    default
br-rtr#
```

HQ-SRV:

Просмотр существующих интерфейсов выполняется командой **ip a**

```
[root@hq-srv ~]# ip -c a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens19: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether bc:24:11:85:50:89 brd ff:ff:ff:ff:ff:ff
    altname enp0s19
    inet 192.168.100.2/27 brd 192.168.100.31 scope global ens19
       valid_lft forever preferred_lft forever
    inet6 fe80::be24:11ff:fe85:5089/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
```

Для конфигурации IPv4 на устройствах, будут отредактированы файлы **options**

- созданы файлы **ipv4address, ipv4route**.
- в файле **/etc/net/ifaces/<ИМЯ_ИНТЕРФЕЙСА>/options**

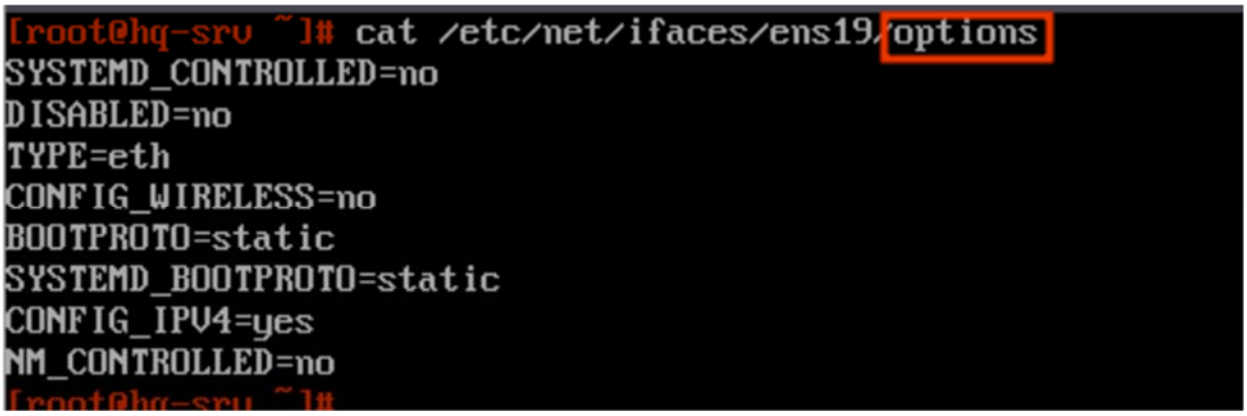
```
[root@hq-srv ~]# ls /etc/net/ifaces/
default  ens19  lo  unknown
[root@hq-srv ~]#
```

Должны быть заданы хотя бы два основных параметра:

Параметр TYPE=eth указывает на тип интерфейса – ethernet

Параметр BOOTPROTO=static означает, что настройка статического IP-адреса и маршрутов будет взята из файлов ipv4address и ipv4route

Проверяем содержимое конфигурационного файла /etc/net/ifaces/ens19/options:



Внимание! Для того, чтобы в качестве сетевой подсистемы корректно использовался etcnet и операционная система могла считывать и применять содержимое конфигурационных файлов: ipv4address, ipv4route, resolv.conf из директории /etc/net/ifaces/<ИМЯ_ИНТЕРФЕЙСА>/, необходимо, чтобы значение параметров DISABLED,NM_CONTROLLED,SYSTEMD_CONTROLLED были установлены в no или же указание данных параметров в файле options не является обязательным условием.

Режим из Alterator	Параметры в options
NetworkManager (native)	DISABLED=yes NM_CONTROLLED=yes BOOTPROTO=static
NetworkManager (etcnet)	DISABLED=no NM_CONTROLLED=yes
Etcnet	DISABLED=no NM_CONTROLLED=no

- Зададим IP-адрес:

```
echo "192.168.100.2/27" > /etc/net/ifaces/ens19/ipv4address
```

- Зададим IP-адрес шлюза по умолчанию:

```
echo "default via 192.168.100.1" > /etc/net/ifaces/ens19/ipv4route
```

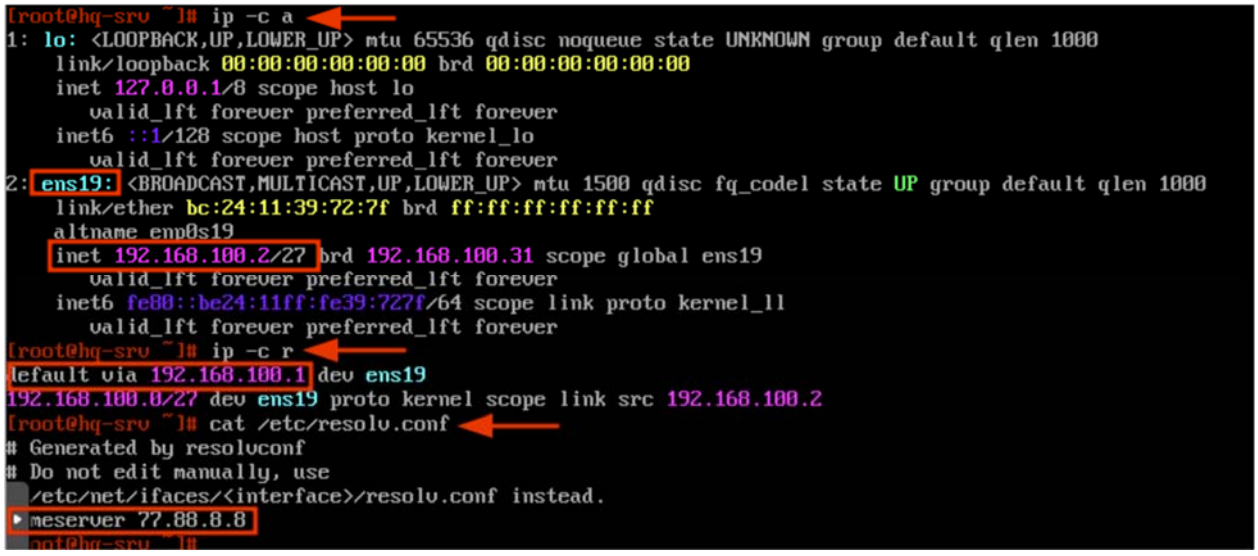
- Зададим (временно) IP-адрес DNS-сервера, для дальнейшей возможности выхода в сеть Интернет и установки необходимых пакетов:

```
echo "nameserver 77.88.8.8" > /etc/net/ifaces/ens19/resolv.conf
```

- Для применения настроек, необходимо перезагрузить службу **network**:

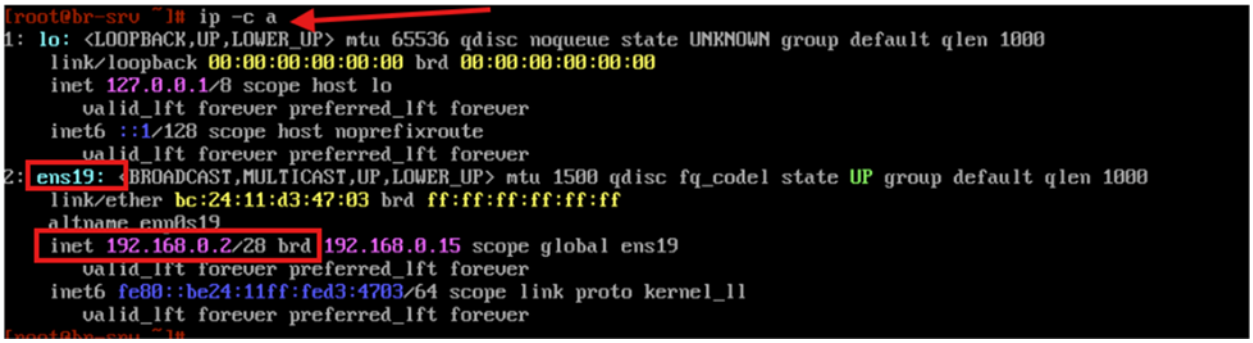
```
systemctl restart network
```

- Проверить:



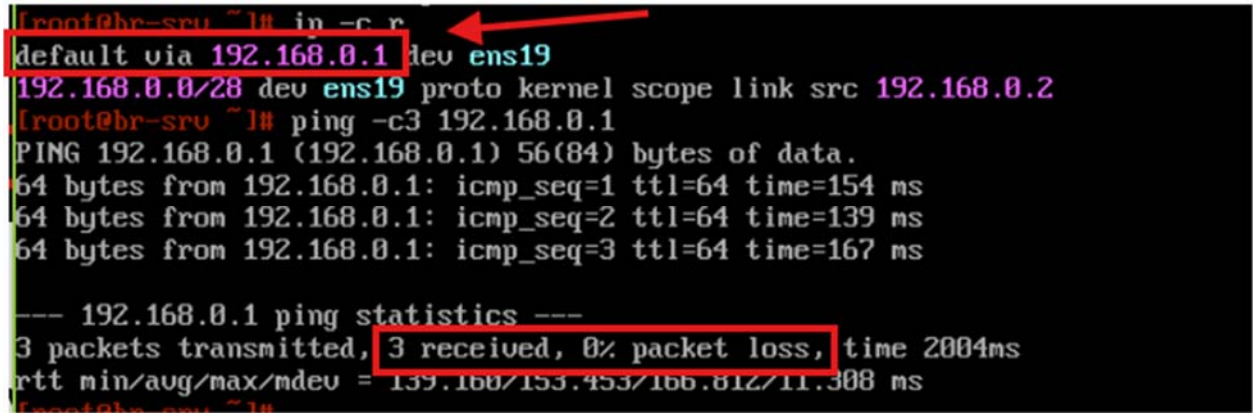
BR-SRV:

Аналогично **HQ-SRV**, ожидаемый результат:



В отличие от офиса HQ, в офисе BR с BR-SRV на текущем этапе можно проверить доступность шлюза по умолчанию

- в офисе HQ, с HQ-SRV шлюз пока не должен быть доступен, т.к. не реализована коммутация



2.2. Настройте доступ к сети Интернет, на маршрутизаторе ISP

Задание:

Настройте адресацию на интерфейсах:

Интерфейс, подключенный к магистральному провайдеру, получает адрес по DHCP;

Настройте маршрут по умолчанию, если это необходимо;

Настройте интерфейс, в сторону HQ-RTR, интерфейс подключен к сети 172.16.1.0/28;

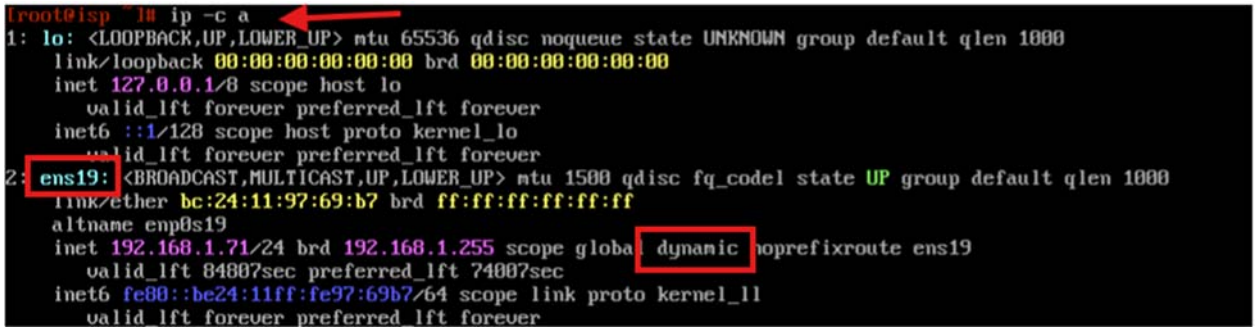
Настройте интерфейс, в сторону BR-RTR, интерфейс подключен к сети 172.16.2.0/28;

На ISP настройте динамическую сетевую трансляцию портов для доступа к сети Интернет HQ-RTR и BR-RTR.

Вариант реализации:

2.2.1 ISP:

Просмотр существующих интерфейсов выполняется командой ip a

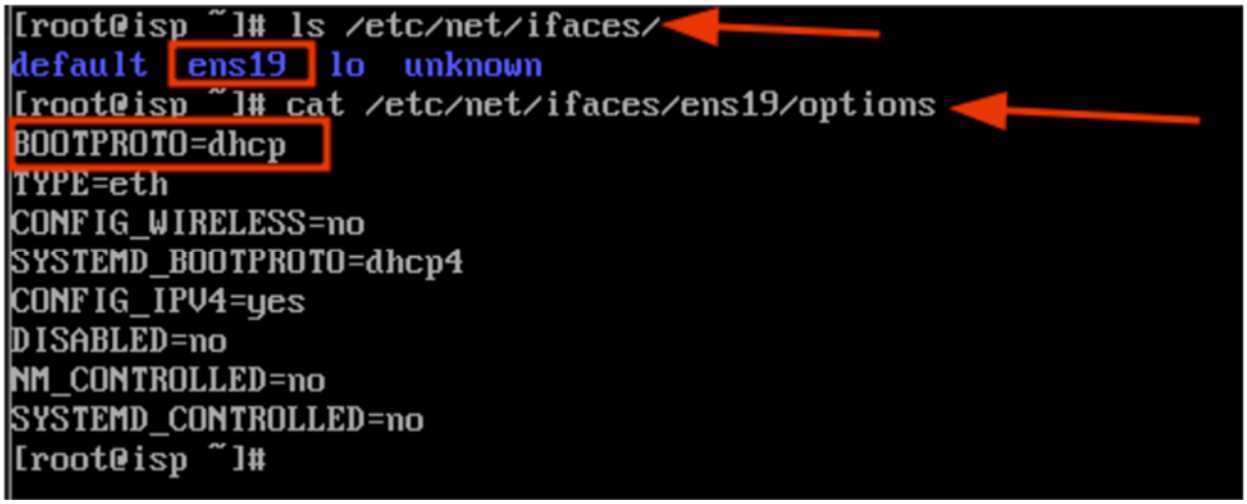


где:

ens19 - интерфейс подключённый к **магистральному провайдеру**;

Для того чтобы интерфейс, подключенный к магистральному провайдеру, получал адрес по DHCP:

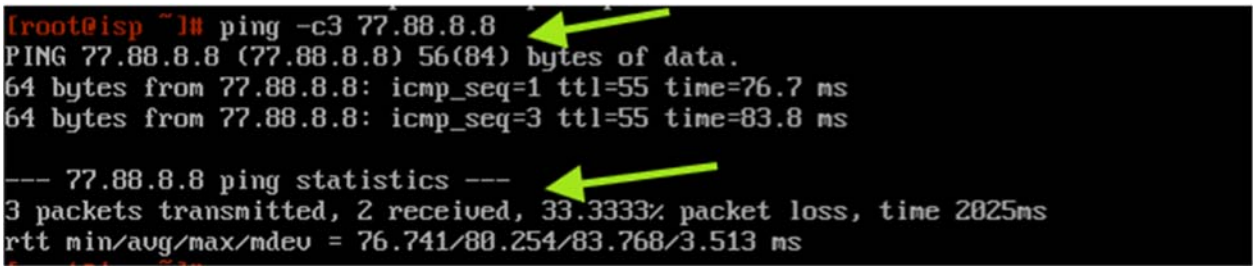
- необходимо в конфигурационном файле, расположенном по пути /etc/net/ifaces/<ИМЯ_ИНТЕРФЕЙСА>/options;
- в параметре BOOTPROTO указать значение dhcp.



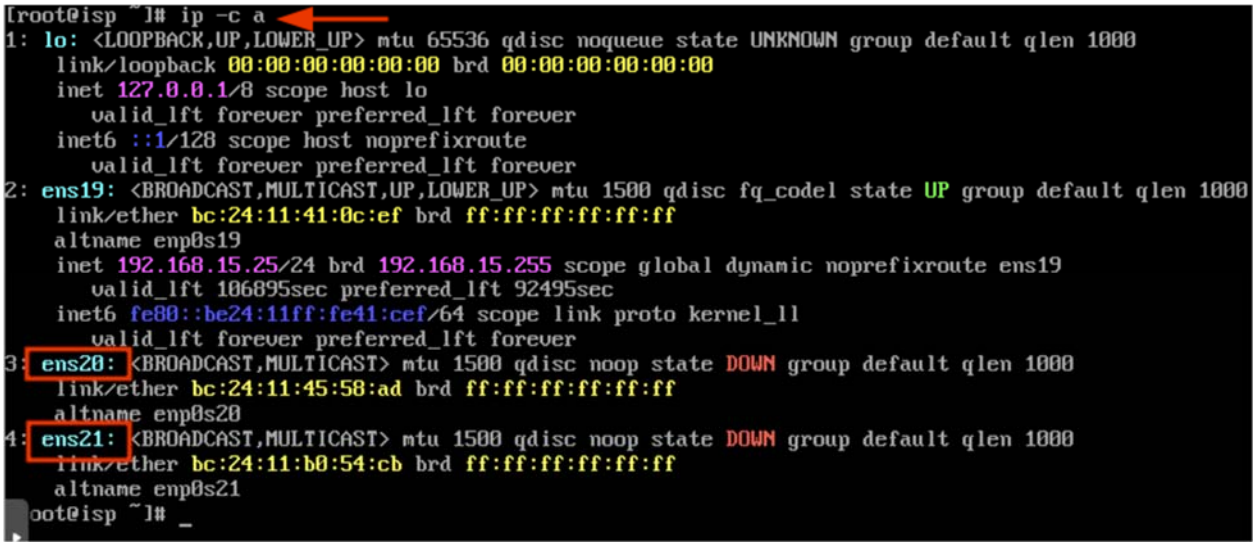
- Для применения настроек, необходимо перезагрузить службу **network**

```
systemctl restart network
```

- Проверить:
  - получение всех параметров по DHCP;
  - доступ в сеть Интернет.



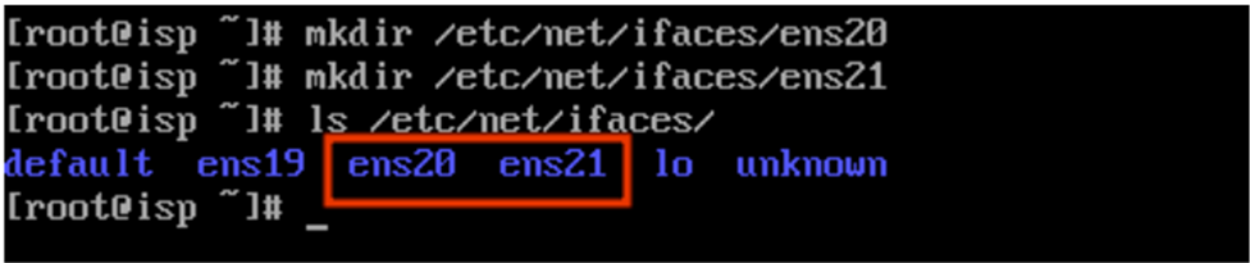
- Просмотр существующих интерфейсов выполняется командой ip a
  - где:
    - **ens20** - интерфейс подключённый к **HQ-RTR**;
    - **ens21** - интерфейс подключённый к **BR-RTR**.



Создадим директории в **/etc/net/ifaces/** для интерфейсов **ens192** и **ens224**:

```
mkdir /etc/net/ifaces/ens20

mkdir /etc/net/ifaces/ens21
```

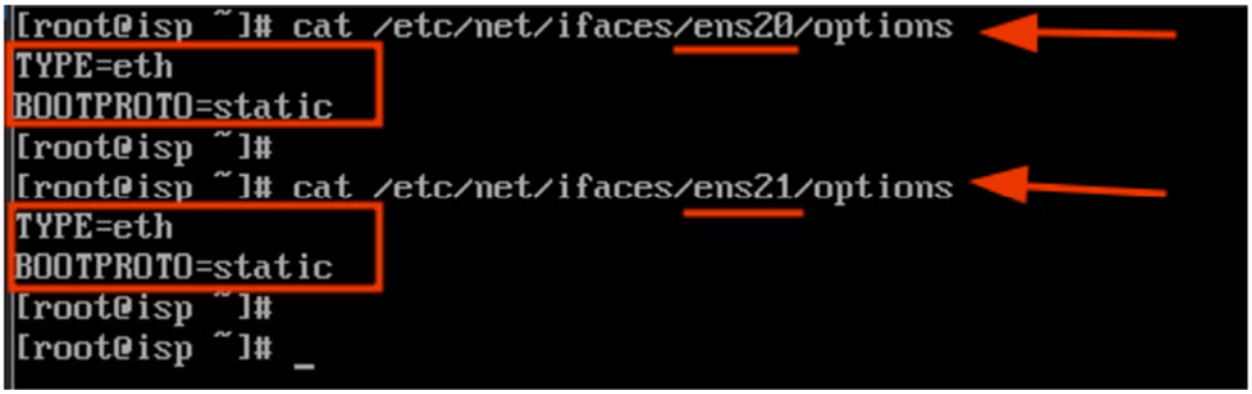
- Результат:



- Для каждого интерфейса, необходимо в директории /etc/net/ifaces/<ИМЯ_ИНТЕРФЕЙСА>/ создать конфигурационный файл options
- с минимально необходимыми параметрами, а именно:
  - **TYPE=eth** указывает на тип интерфейса – ethernet,
  - **BOOTPROTO=static** означает, что настройка статических параметров

```
echo "TYPE=eth" > /etc/net/ifaces/ens20/options

echo "BOOTPROTO=static" >> /etc/net/ifaces/ens20/options

cp /etc/net/ifaces/ens20/options /etc/net/ifaces/ens21/options
```

- Результат:



- Далее опишем содержимое конфигурационного файла **ipv4address** для каждого интерфейса:
    - в сторону **HQ-RTR**:

```
echo "172.16.1.1/28" > /etc/net/ifaces/ens20/ipv4address
```

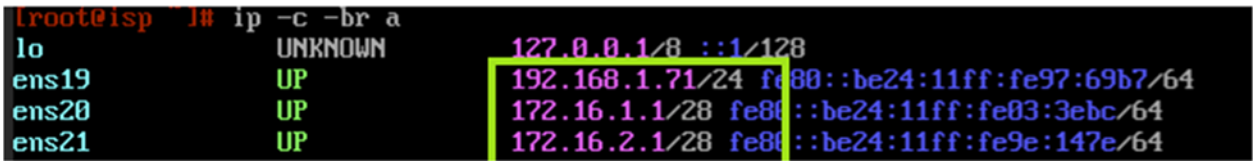
    - в сторону **BR-RTR**:

```
echo "172.16.2.1/28" > /etc/net/ifaces/ens21/ipv4address
```

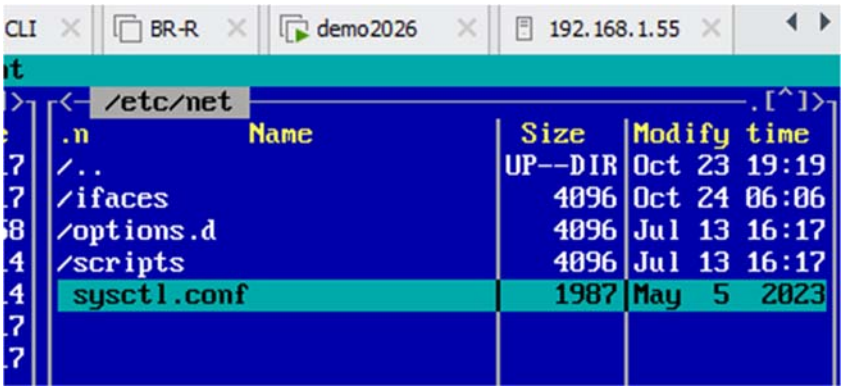
- Для применения настроек, необходимо перезагрузить службу **network**

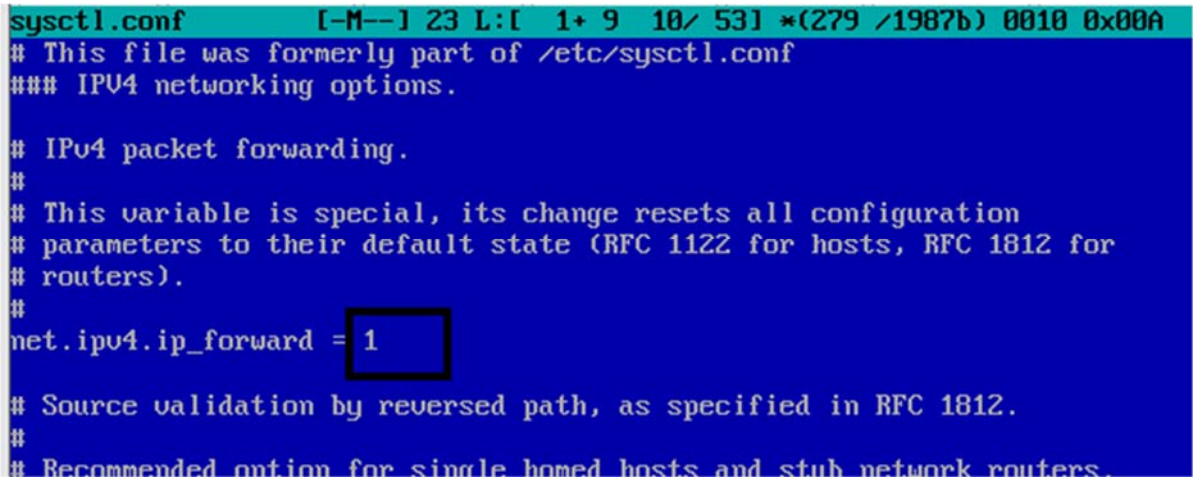
```
systemctl restart network
```

- Проверить:



- Для того чтобы устройство ISP могло пересылать пакеты с интерфейса на интерфейс, необходимо включить пересылку пакетов (маршрутизацию/forwarding)
    - Для этого следует в конфигурационном файле **/etc/net/sysctl.conf** в параметре **net.ipv4.ip_forward = 0** заменить значение с **0** на **1**

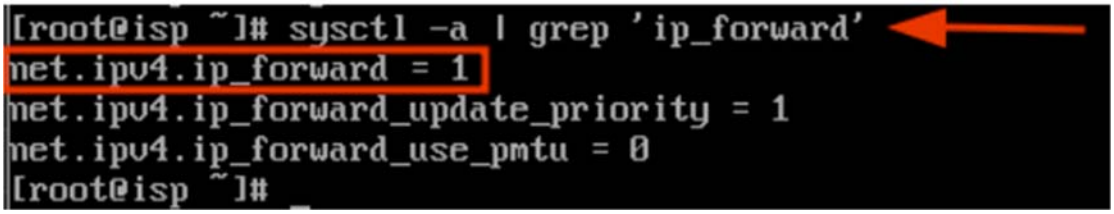




- Для применения настроек, необходимо перезагрузить службу **network**

```
systemctl restart network
```

- Проверить:



- Для динамической сетевой трансляции можно использовать iptables.
- В случае использования в качестве ОС на ВМ ISP «Альт Jeos» – пакет iptables необходимо установить:
    - предварительно обновив список пакетов с помощью команды **apt-get update**

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

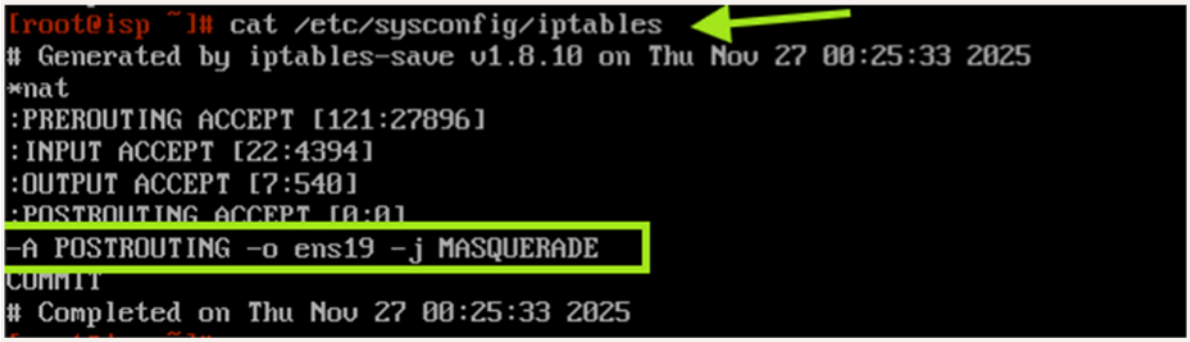
- Реализацию сетевой трансляции адресов с помощью iptables можно выполнить одной командой:

- где, **ens19** внешний интерфейс, подключённый к магистральному провайдеру
- также реализуем трансляцию адресов только из конкретных сетей HQ-RTR и BR-RTR

```
iptables –t nat –A POSTROUTING -s 172.16.1.0/28 –o ens19 –j MASQUERADE

iptables –t nat –A POSTROUTING -s 172.16.2.0/28 –o ens19 –j MASQUERADE

или

iptables –t nat –A POSTROUTING–o ens19 –j MASQUERADE (так проще)
```

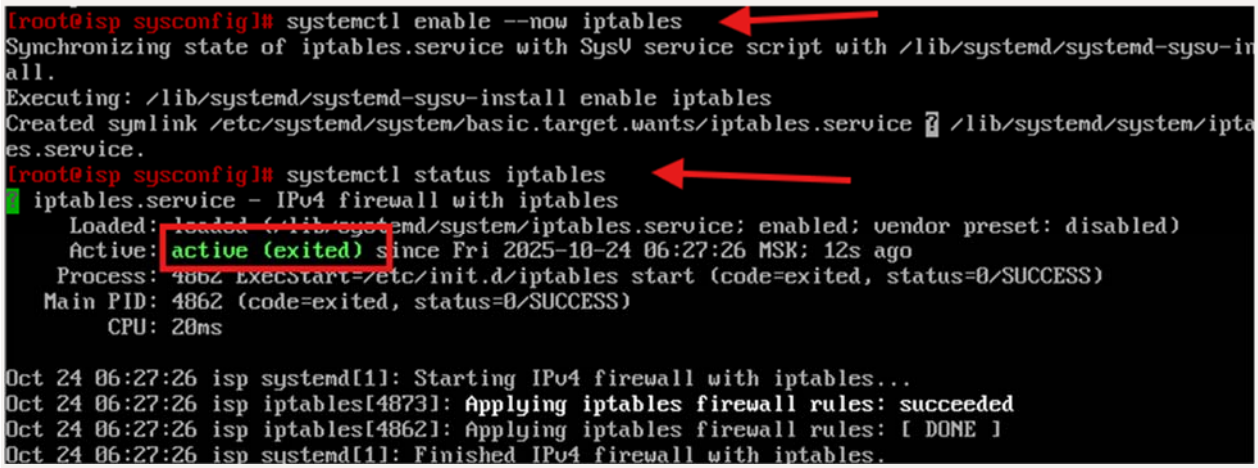
- Сохраняем правила iptables на постоянной основе (после перезагрузки):

```
iptables-save >> /etc/sysconfig/iptables
```

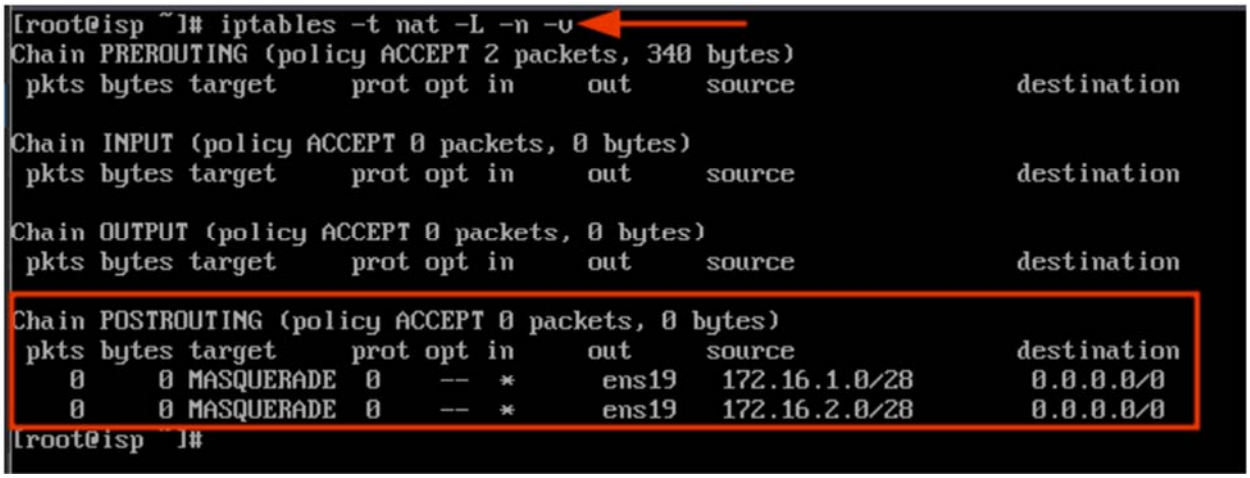


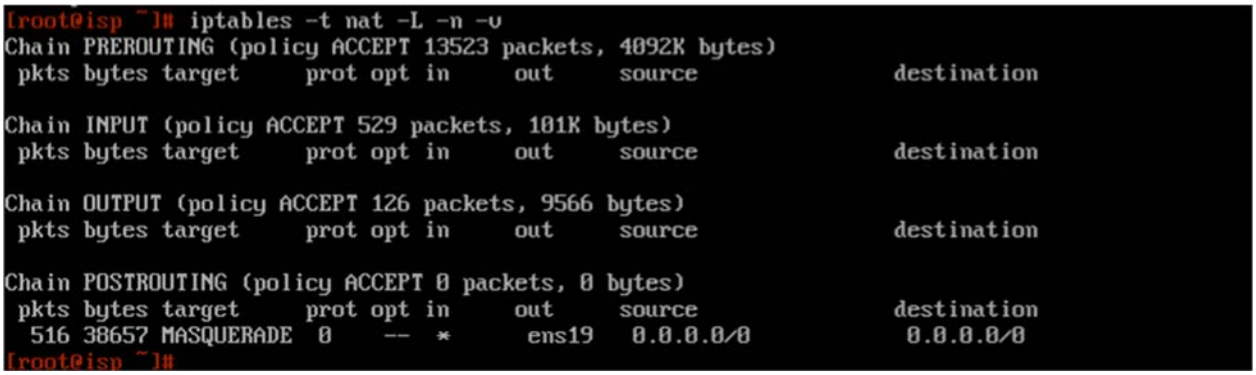
- Включаем и добавляем в автозагрузку службу **iptables**:

```
systemctl enable --now iptables
```



- Проверить, наличие правила в iptables, а именнов таблице **nat**, в цепочек **POSTROUTING**:





2.2.2 HQ-RTR:

- Создаём интерфейс с именем **isp** (произвольное имя) и назначаем на него IP-адрес согласно заполненной таблице адресации:

```
hq-rtr>enable
hq-rtr#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
hq-rtr(config)#interface isp
hq-rtr(config-if)#description "ISP"
hq-rtr(config-if)#ip address 172.16.1.2/28
hq-rtr(config-if)#exit
hq-rtr(config)#
```

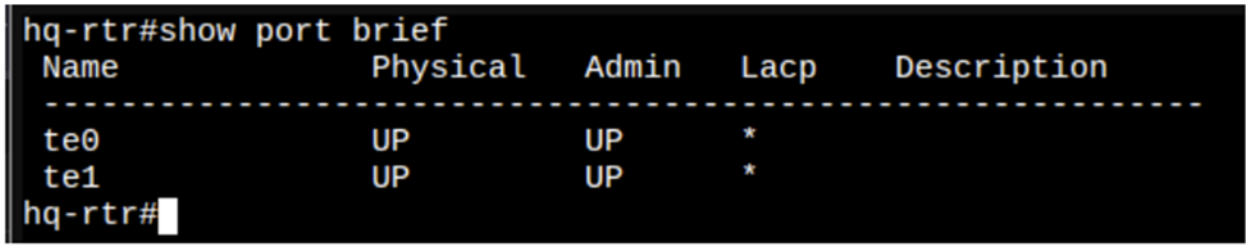
- Также зададим сразу же маршрут по умолчанию, указав в качестве шлюза по умолчанию IP-адрес ISP:

```
hq-rtr(config)#ip route 0.0.0.0/0 172.16.1.1
```

- Посмотреть физические порты можно при помощи следующей команды:

```
hq-rtr#show port brief
```

  - где:
    - **te0** - порт в сторону **ISP**;
    - **te1** - порт в сторону **локальной сети офиса HQ** (HQ-Net, виртуальный коммутатор HQ-SW);



- В режиме конфигурирования порта создим service-instance с произвольным именем:
  - укажем (инкапсулировать) что будет обрабатываться не тегированный трафик (untagget);
  - укажем в какой интерфейс (ранее созданный с именем isp) нужно отправить обработанные кадры;

```
hq-rtr(config)#port te0
hq-rtr(config-port)#service-instance te0/isp
hq-rtr(config-service-instance)#encapsulation untagged
hq-rtr(config-service-instance)#connect ip interface isp

2025-09-04 05:45:04 INFO Interface isp changed state to up
hq-rtr(config-service-instance)#exit
hq-rtr(config-port)#exit
hq-rtr(config)#do write memory
Building configuration...

hq-rtr(config)#
```

- Проверить, назначенный IP-адрес на интерфейс:

hq-rtr#show ip interface brief

```
hq-rtr#show ip interface brief
 Interface        IP-Address          Status                VRF
 ---------------------------------------------------------------
 vl100            192.168.100.1/27    up                    default
 vl200            192.168.200.1/24    up                    default
 vl999            192.168.99.1/29     up                    default
 isp              172.16.1.2/28       up                    default
hq-rtr#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
Gateway of last resort is 172.16.1.1 to network 0.0.0.0

S*      0.0.0.0/0 [1/0] via 172.16.1.1, isp
C       172.16.1.0/28 is directly connected, isp
C       192.168.99.0/29 is directly connected, vl999
C       192.168.100.0/27 is directly connected, vl100
C       192.168.200.0/24 is directly connected, vl200
hq-rtr#
```

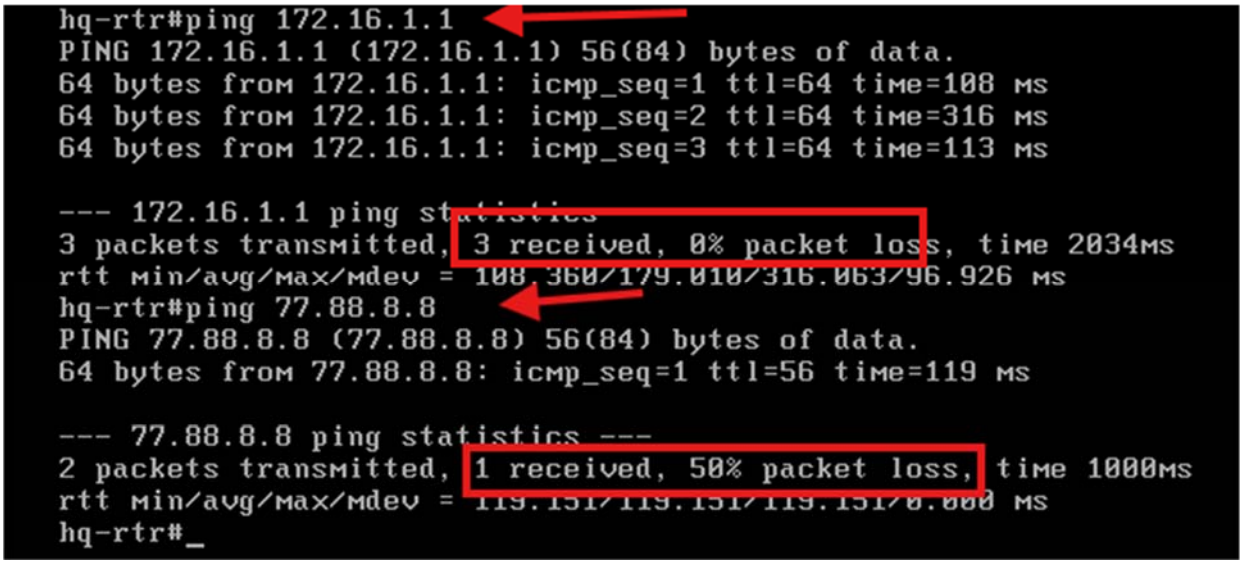
- Проверить, назначенный маршрут по умолчанию:

hq-rtr#show ip route static

  - Результат:

```
hq-rtr#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default

IP Route Table for VRF "default"
Gateway of last resort is 172.16.1.1 to network 0.0.0.0

S*      0.0.0.0/0 [1/0] via 172.16.1.1, isp
C       172.16.1.0/28 is directly connected, isp
C       192.168.99.0/29 is directly connected, vl999
C       192.168.100.0/27 is directly connected, vl100
C       192.168.200.0/28 is directly connected, vl200
```

- Проверить доступность шлюза и доступ в сеть Интернет:



2.2.3 BR-RTR:

- Аналогично **HQ-RTR**

```
br-rtr>enable

br-rtr#conf t

Enter configuration commands, one per line.  End with CNTL/Z.

br-rtr(config)#interface isp

br-rtr(config-if)#description "ISP"

br-rtr(config-if)#ip address 172.16.2.2/28

br-rtr(config-if)#exit

br-rtr(config)#ip route 0.0.0.0/0 172.16.2.1

br-rtr(config)#port te0

br-rtr(config-port)#service-instance ge0

br-rtr(config-service-instance)#encapsulation untagged

br-rtr(config-service-instance)#connect ip interface isp


2025-09-04 05:48:19      INFO      Interface isp changed state to up

br-rtr(config-service-instance)#exit

br-rtr(config-port)#exit

br-rtr(config)#write memory

Building configuration...
```

```
br-rtr(config)#
```

- Ожидаемый результат:

```
br-rtr#sh ip in br
 Interface        IP-Address          Status                VRF
 ---------------------------------------------------------------
 int1             192.168.0.1/28      up                    default
 isp              172.16.2.2/28       up                    default
br-rtr#sh ip route
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter are
       * - candidate default

IP Route Table for VRF "default"
Gateway of last resort is 172.16.2.1 to network 0.0.0.0

S*      0.0.0.0/0 [1/0] via 172.16.2.1, isp
C       172.16.2.0/28 is directly connected, isp
C       192.168.0.0/28 is directly connected, int1
br-rtr#
```

```
br-rtr#ping 172.16.2.1
PING 172.16.2.1 (172.16.2.1) 56(84) bytes of data.
64 bytes from 172.16.2.1: icmp_seq=2 ttl=64 time=41.3 ms
64 bytes from 172.16.2.1: icmp_seq=3 ttl=64 time=226 ms
64 bytes from 172.16.2.1: icmp_seq=4 ttl=64 time=85.2 ms

--- 172.16.2.1 ping statistics ---
4 packets transmitted, 3 received, 25% packet loss, time 3089ms
rtt min/avg/max/mdev = 41.267/117.538/226.148/78.865 ms
br-rtr#ping 77.88.8.8
PING 77.88.8.8 (77.88.8.8) 56(84) bytes of data.
64 bytes from 77.88.8.8: icmp_seq=1 ttl=56 time=53.9 ms
64 bytes from 77.88.8.8: icmp_seq=2 ttl=56 time=58.8 ms
64 bytes from 77.88.8.8: icmp_seq=3 ttl=56 time=319 ms

--- 77.88.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2144ms
rtt min/avg/max/mdev = 53.875/144.012/319.366/124.010 ms
```

2.3. Создайте локальные учетные записи на серверах HQ-SRV и BR-SRV, роутерах HQ-RTR, BR-RTR

Задание:

- Создайте пользователя remote_user
  - Пароль пользователя sshuser с паролем P@ssw0rd
  - Идентификатор пользователя 2026

- Пользователь sshuser должен иметь возможность запускать sudo без ввода пароля
- Создайте пользователя net_admin на маршрутизаторах HQ-RTR и BR-RTR
- Пароль пользователя net_admin с паролем P@ssw0rd
- При настройке ОС на базе Linux, запускать sudo без ввода пароля
- При настройке ОС отличных от Linux пользователь должен обладать максимальными привилегиями.

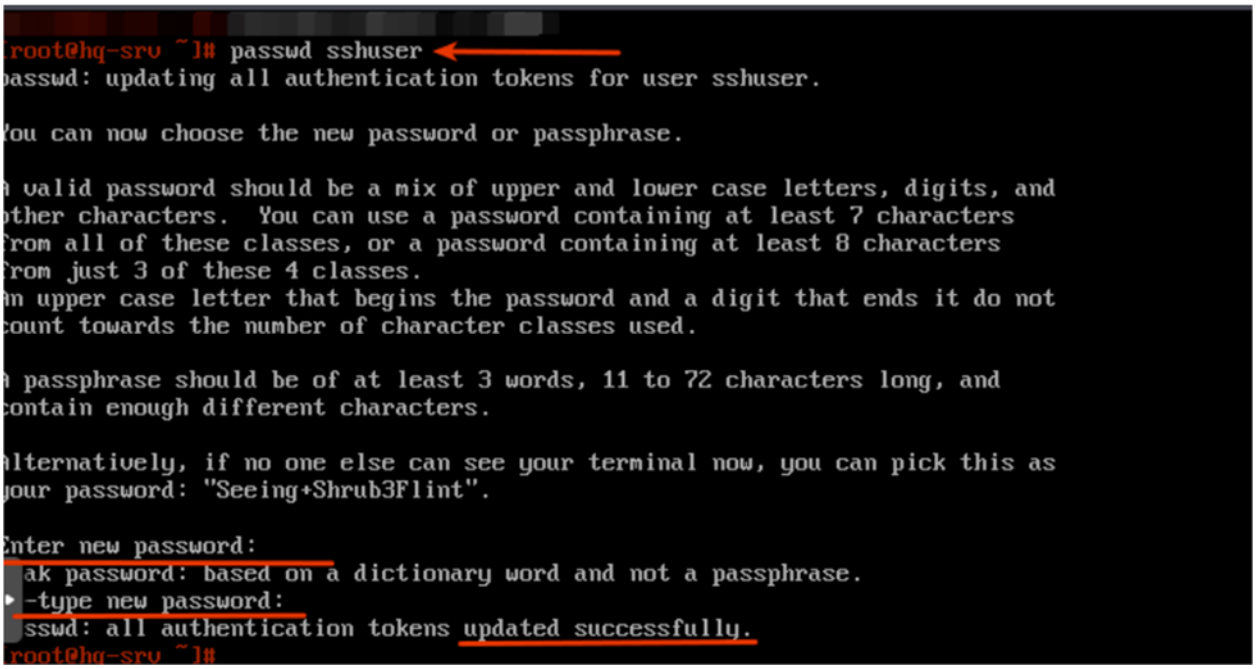
2.3.1 HQ-SRV и BR-SRV:

- Создать пользователя с явным указанием UID можно с помощью команды:

```
useradd sshuser –u 2026
```

- Проверить UID-пользователя **sshuser**:

Задать пароль пользователю можно с помощью утилиты passwd: результате запуска утилиты passwd необходимо будет задать пароль, а затем подтвердить заданный пароль



- Реализуем возможность запуска утилиты sudo пользователю sshuser без ввода пароля:
- Рекомендуется прочитать перед выполнением

- Добавляем пользователя **sshuser** в группу **wheel** для этого используем утилиту usermod
    - поскольку штатное состояние политики: **wheelonly** (Означает что пользователь из группы wheel имеет право запускать саму команду sudo, но не означает, что он через sudo может выполнить какую-то команду с правами root)
    - где:
        - **usermod** - утилита для изменения и работы с параметрами пользователя;
        - **-aG** - параметр чтобы добавить пользователя в дополнительную группу(ы). Использовать только вместе с параметром **-G;**
        - **wheel** - имя группы;
        - **sshuser** - имя пользователя:

```
usermod -aG wheel sshuser
```

- Добавляем следующую строку в файл в /etc/sudoers чтобы была возможность запуска **sudo** без дополнительной аутентификации:

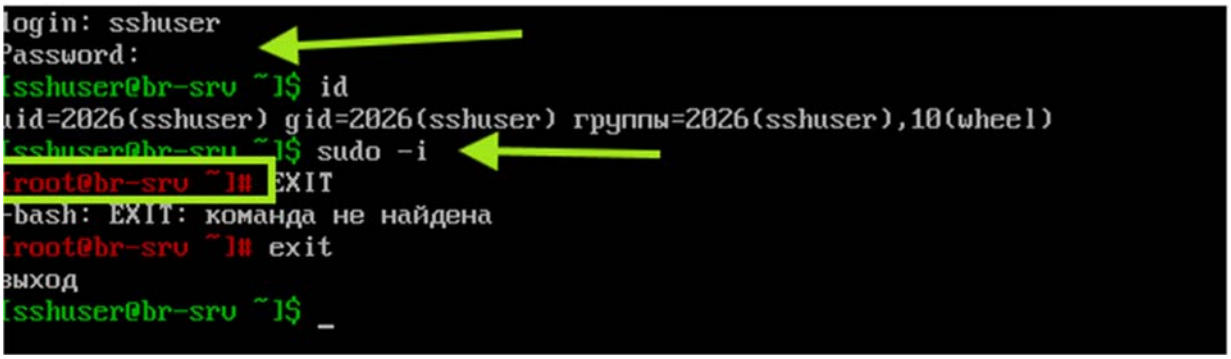
```
echo "sshuser ALL=(ALL:ALL) NOPASSWD: ALL" >> /etc/sudoers
```

```
sudoers            [-M--]  1 L:[102+34 136/136] *(4704/4704b) <EOF>                [*][X
# to only contain the fixed list of variables.
# See sudoers(5) for details.
#Defaults:WHEEL_USERS !env_reset

# Preserve DISPLAY and XAUTHORITY environment variables
# for "xgrp" group members.
Defaults:XGRP_USERS env_keep += "DISPLAY XAUTHORITY"

##
## Runas alias specification
##

##
## User privilege specification
##
# root ALL=(ALL:ALL) ALL

## Uncomment to allow members of group wheel to execute any command
# WHEEL_USERS ALL=(ALL:ALL) ALL

## Same thing without a password
# WHEEL_USERS ALL=(ALL:ALL) NOPASSWD: ALL

## Uncomment to allow members of group sudo to execute any command
# SUDO_USERS<-->ALL=(ALL:ALL) ALL

## Uncomment to allow any user to run sudo if they know the password
## of the user they are running the command as (root by default).
# Defaults targetpw  # Ask for the password of the target user
# ALL ALL=(ALL:ALL) ALL  # WARNING: only use this together with 'Defaults targetpw'

## Read drop-in files from /etc/sudoers.d
@includedir /etc/sudoers.d
sshuser ALL=(ALL:ALL) NOPASSWD: ALL
```


- Проверяем:
  - выполняем вход из под пользователя **sshuser** и пытаемся повысить привелегии:
    - **HQ-SRV:**

```
Hostname: hq-srv.au-team.irpo
IP: 192.168.100.2
hq-srv login: sshuser
Password:
[sshuser@hq-srv ~]$ id
uid=2026(sshuser) gid=2026(sshuser) группы=2026(sshuser),10(wheel)
[sshuser@hq-srv ~]$ sudo -i
[root@hq-srv ~]#
[root@hq-srv ~]# exit
выход
[sshuser@hq-srv ~]$ _
```

BR-SRV:



HQ-RTR и BR-RTR:

- Создаём пользователя **net_admin** на маршрутизаторах с паролем **P@$$word** и с максимальными привилегиями:
    - максимальным привилегиям в EcoRouter - соответствуем роль **admin**:

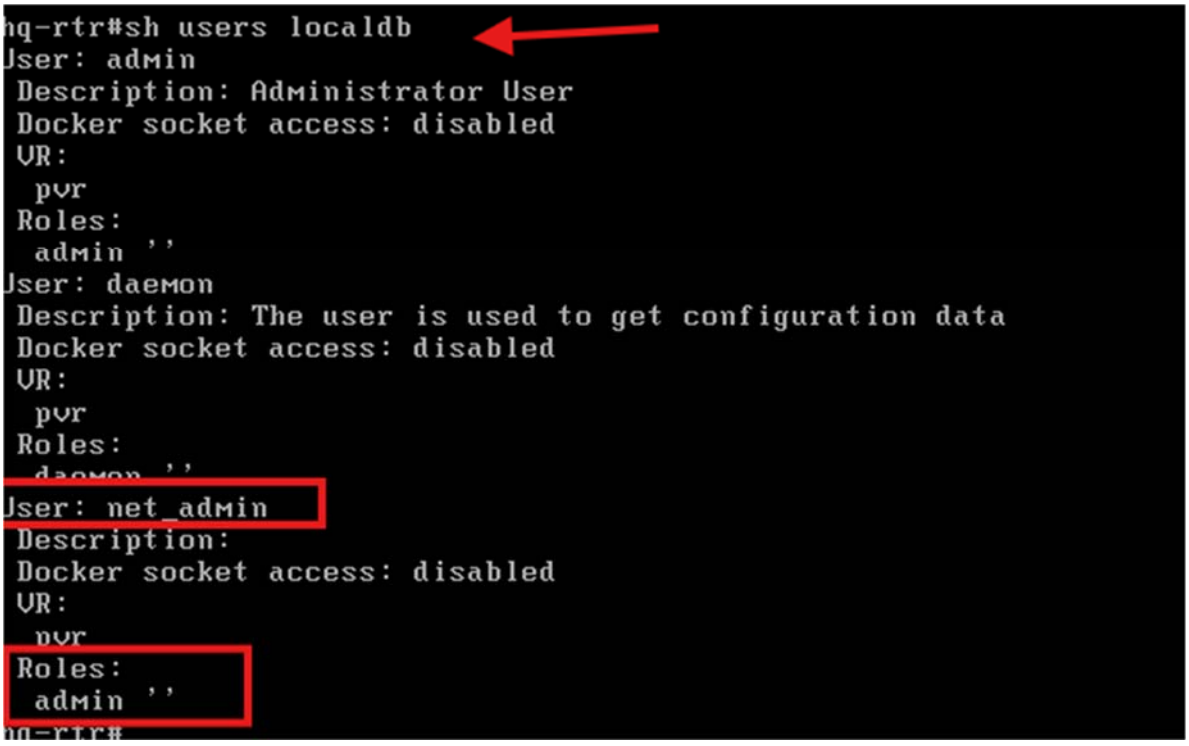
HQ-RTR

```
hq-rtr(config)#username net_admin
hq-rtr(config-user)#password P@ssw0rd
hq-rtr(config-user)#role admin
hq-rtr(config-user)#exit
hq-rtr(config)#write memory
Building configuration...
hq-rtr(config)#
```

BR-RTR

```
br-rtr(config)#username net_admin
br-rtr(config-user)#password P@ssw0rd
br-rtr(config-user)#role admin
br-rtr(config-user)#exit
br-rtr(config)#write memory
Building configuration...
br-rtr(config)#
```

- Проверяем:
  - наличие созданного пользователя и назначение соответствующей роли на **HQ-RTR** и выполняем вход из под пользователя **net_admin**:



2.4. Настройка коммутации в сегменте HQ (HQ-SW)

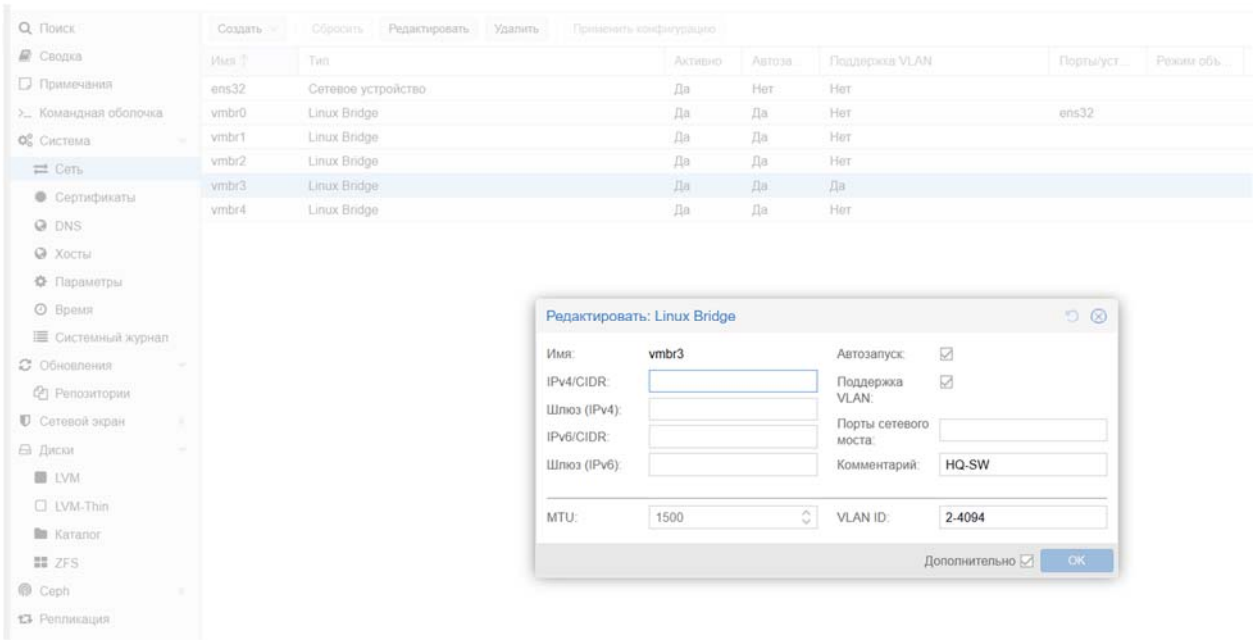
Задание:

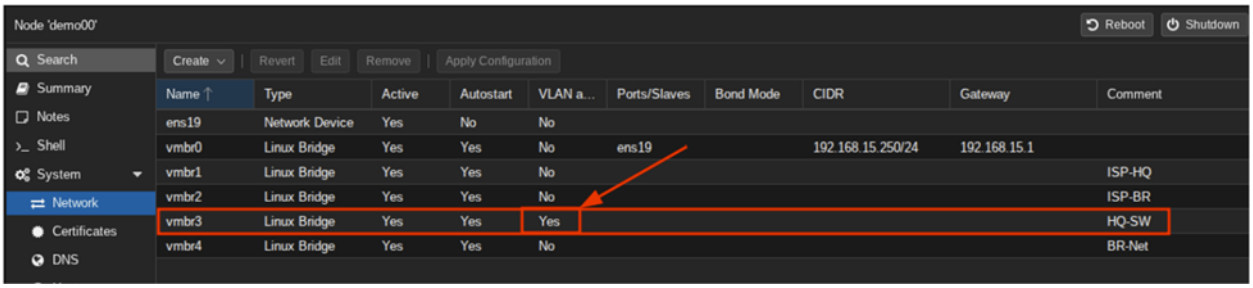
- Трафик HQ-SRV должен принадлежать VLAN 100
- Трафик HQ-CLI должен принадлежать VLAN 200
- Предусмотреть возможность передачи трафика управления в VLAN 999
- Реализовать на HQ-RTR маршрутизацию трафика всех указанных VLAN с использованием одного сетевого адаптера ВМ/физического порта
- Сведения о настройке коммутации внесите в отчёт

Вариант реализации:

Гипервизор:

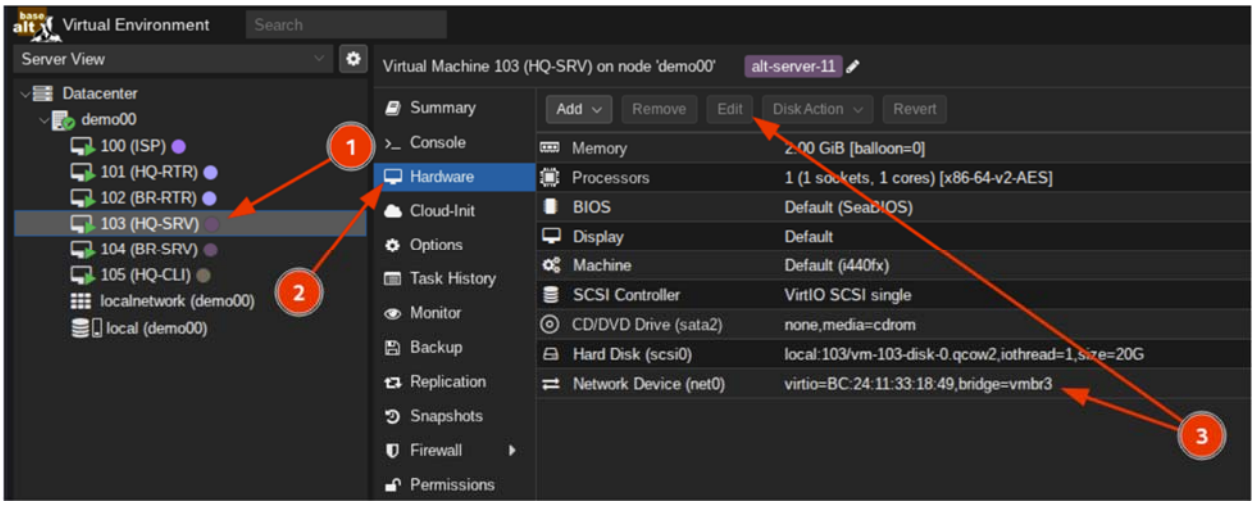
- В качестве коммутатора используется виртуальный коммутатор на уровне Альт Виртуализаци PVE (на котором развёрнут стенд) например **vmbr3**:
    - подразумевается что для **vmbr3** в текущем случае выставлен чек-бокс **VLAN aware**:

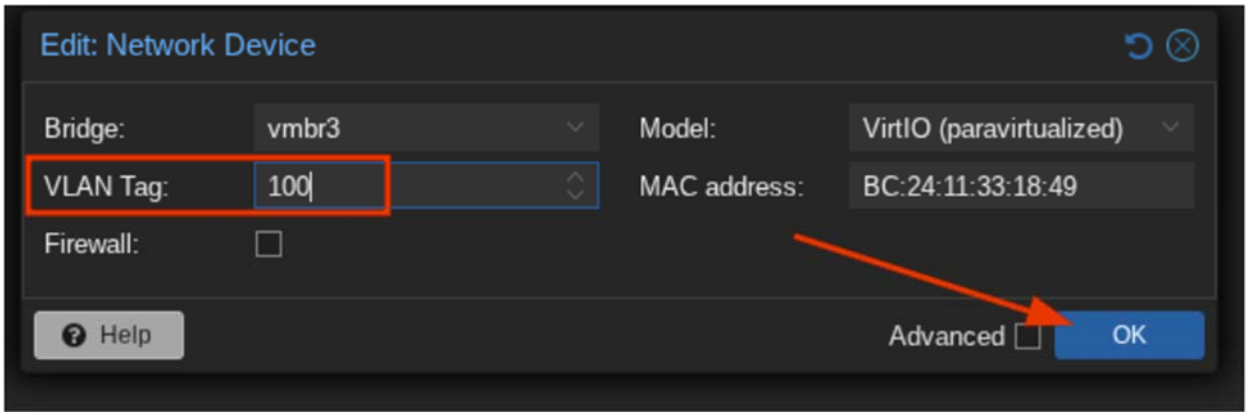


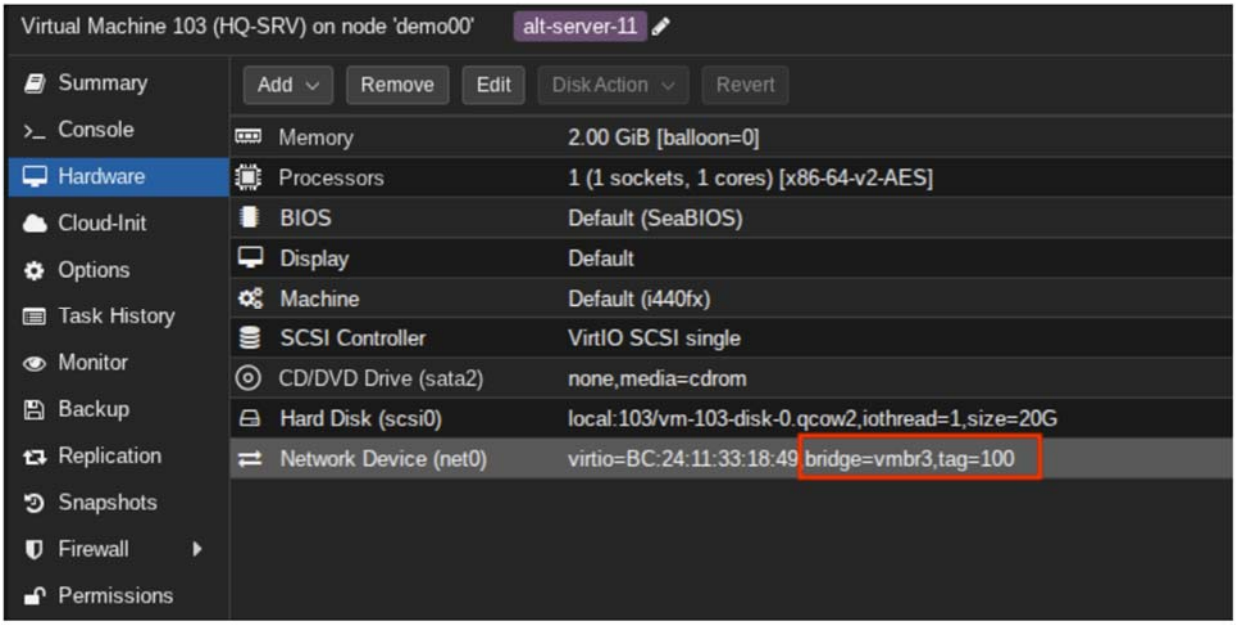


Реализуем необходимые порты "доступа (access)":

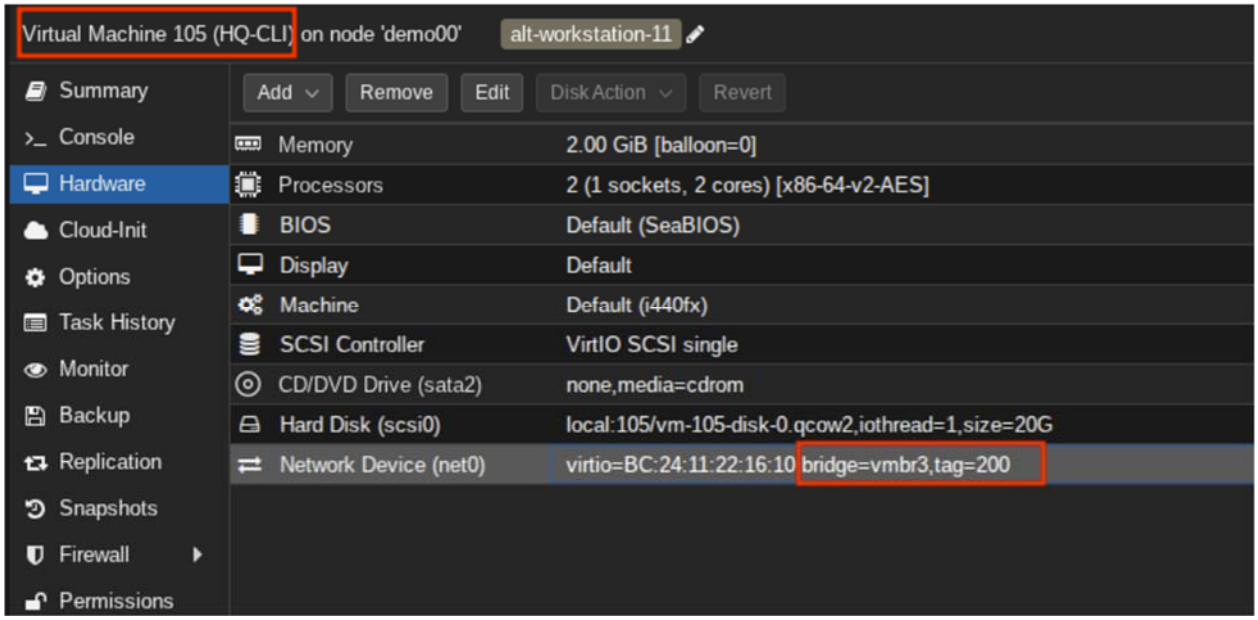
HQ-SRV (vlan 100 - Сервера):



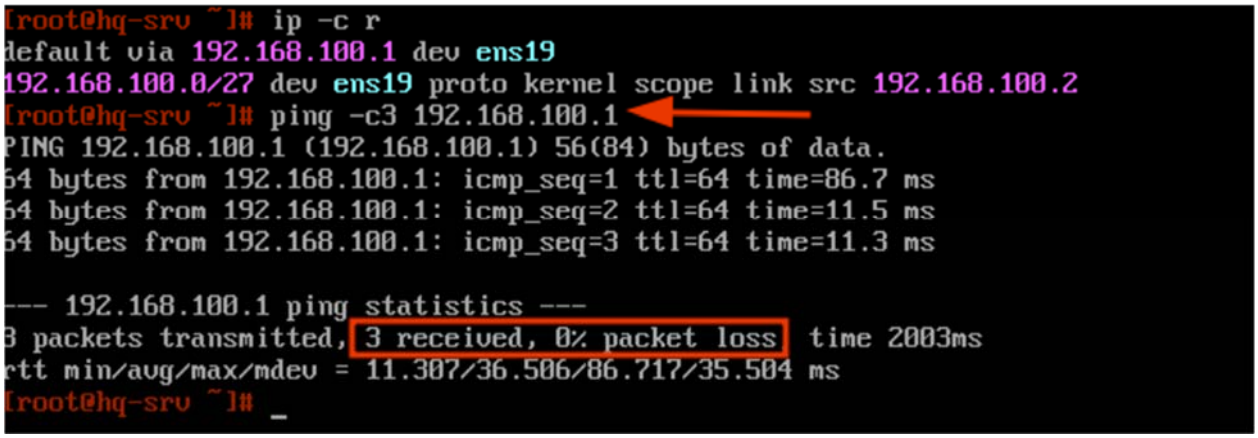


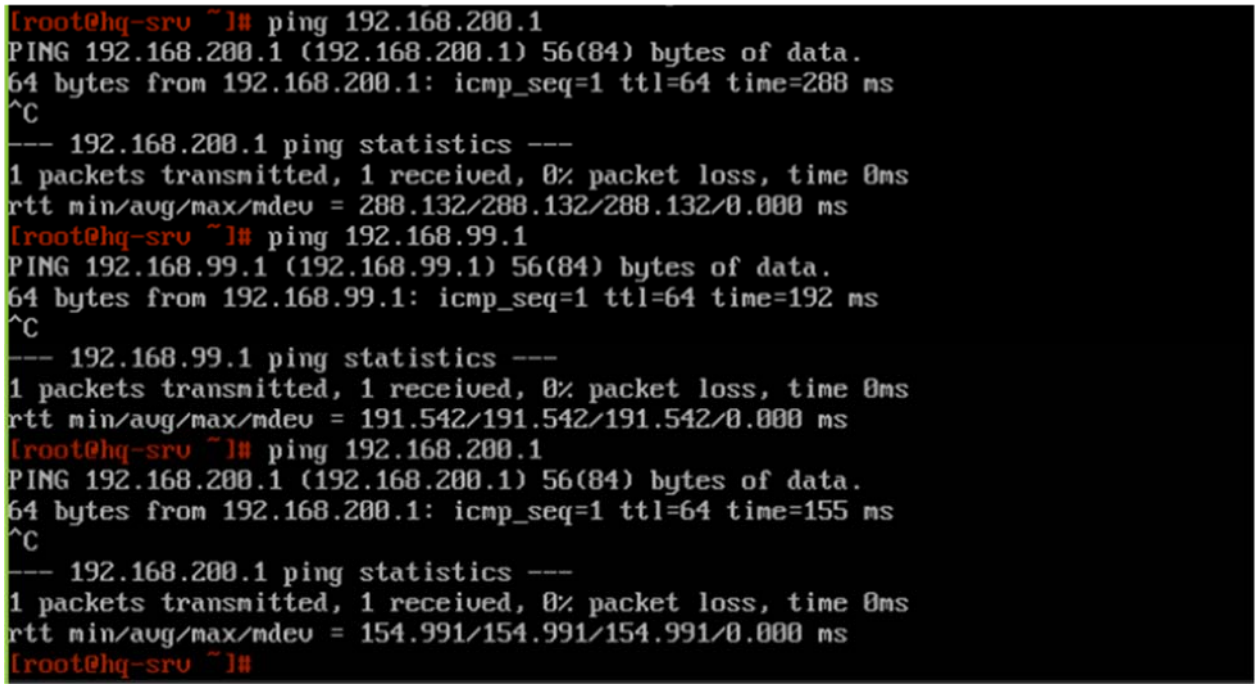


HQ-CLI (vlan 200 - Клиенты):



Проверить, с HQ-SRV должен быть доступен HQ-RTR:





2.5. Настройте безопасный удаленный доступ на серверах HQ-SRV и BR-SRV

Задание:

- Для подключения используйте порт 2026
- Разрешите подключения исключительно пользователю sshuser
- Ограничьте количество попыток входа до двух
- Настройте баннер «Authorized access only».

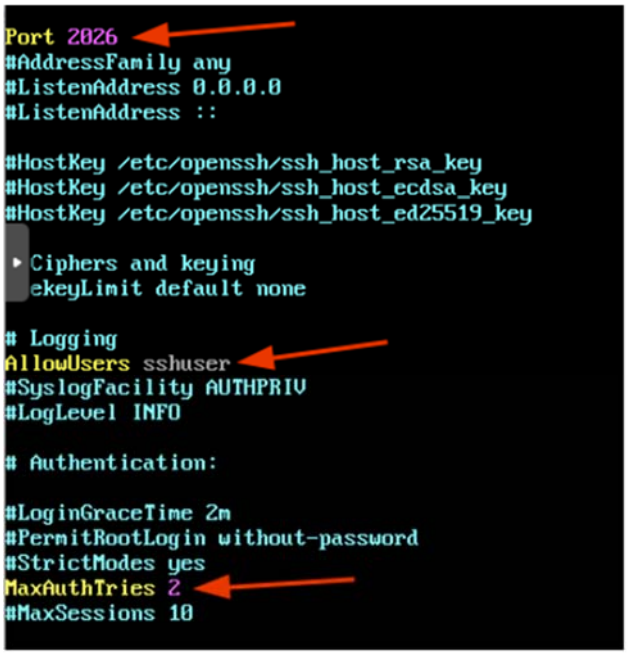
HQ-SRV и BR-SRV:

- Редактируем конфигурационный файл openssh, расположенный по пути **/etc/openssh/sshd_config**:

```
vim /etc/openssh/sshd_config
```

  - Вносим следующие изменения:

- **Port 2026** – Порт, на котором следует ожидать запросы на соединение. Значение по умолчанию – 22;
- **AllowUsers sshuser** – список имён пользователей через пробел. Если параметр определён, регистрация в системе будет разрешена только пользователям, чьи имена соответствуют одному из шаблонов;
- **MaxAuthTries 2** – ограничение на число попыток идентифицировать себя в течение одного соединения;
    - **Banner /etc/openssh/banner** – содержимое указанного файла будет отправлено удалённому пользователю прежде, чем будет разрешена аутентификация.



- Редактируем баннер, а именно файл по пути **/etc/openssh/banner**:

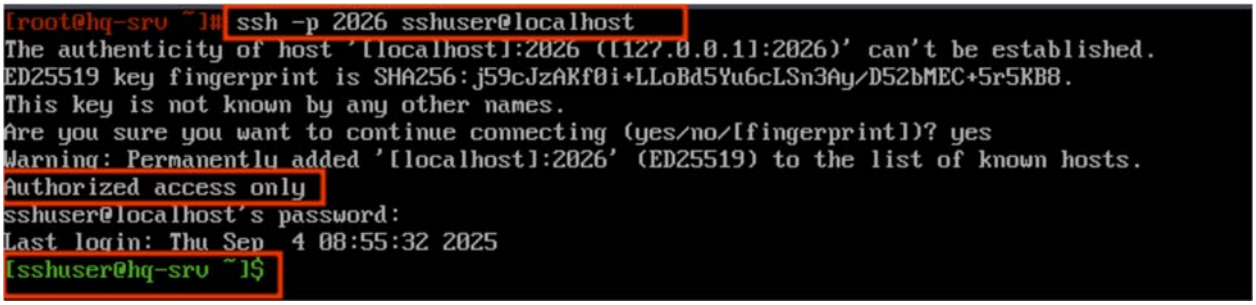
```
echo "Authorized access only" > /etc/openssh/banner
```

- Для применения всех изменений необходимо перезапустить службу **sshd**:

```
systemctl restart sshd
```

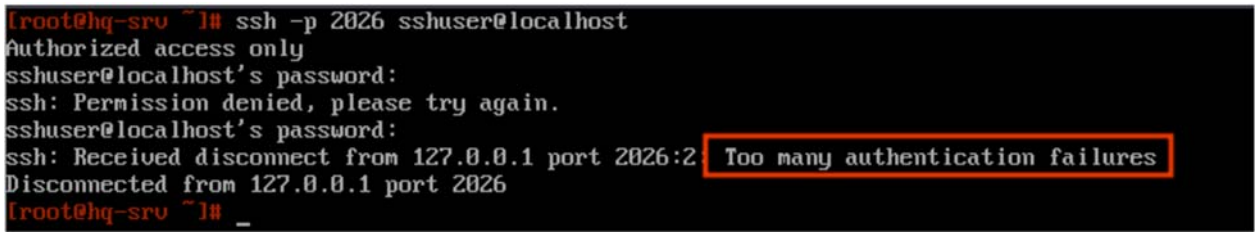
- Проверяем:

- Наличие **Banner** и доступ по порту **2026** из под пользователя **sshuser**, а также ограничение кол-во попыток входа до **2**:

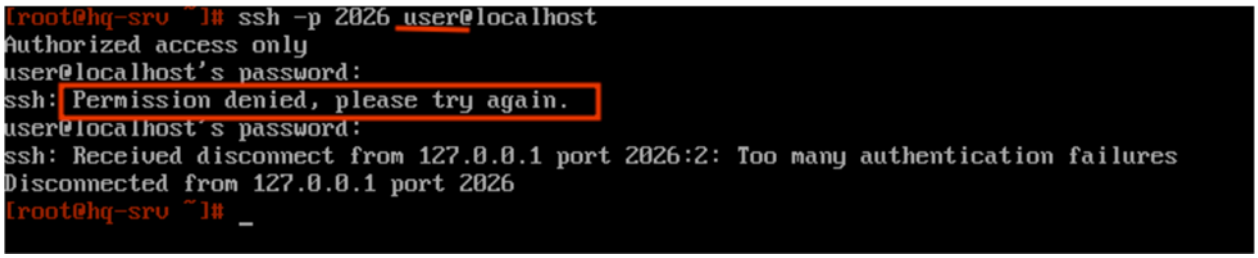


- Попытаться подключить под пользователем sshuser на стандартный порт ssh:

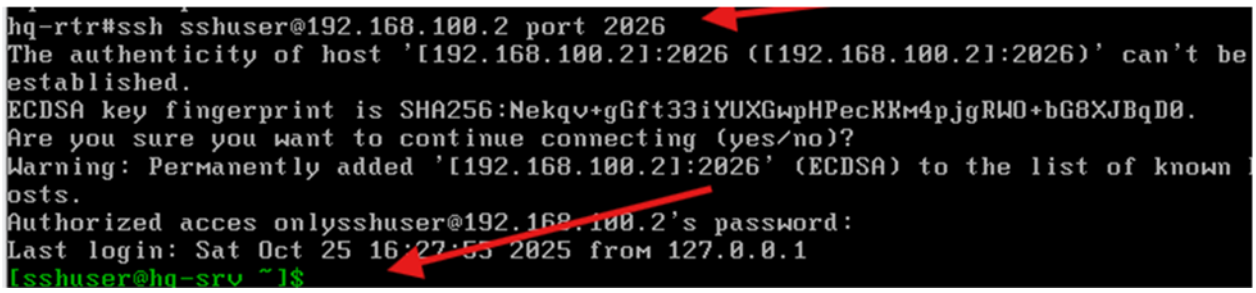
- Попытаться подключить под пользователем sshuser с указанием не верных паролей более чем 2 раза:

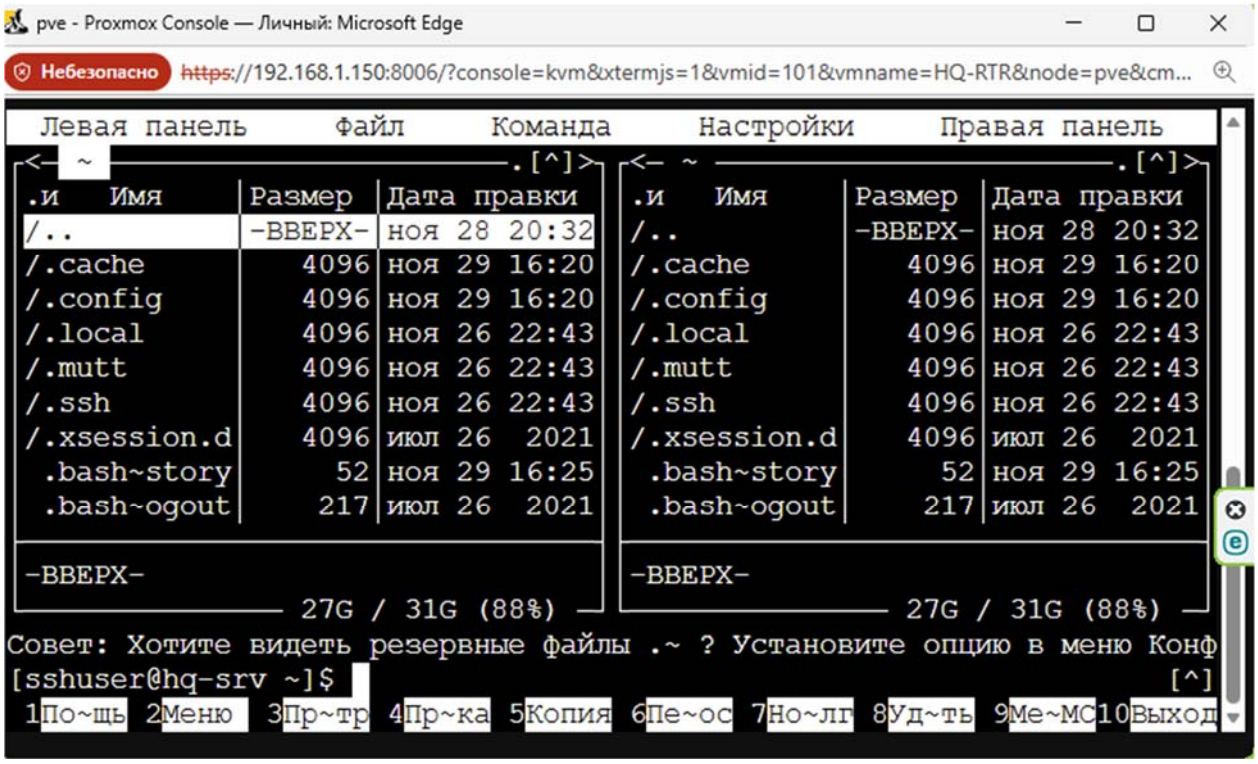


- Попытаться не из-под пользователя sshuser:

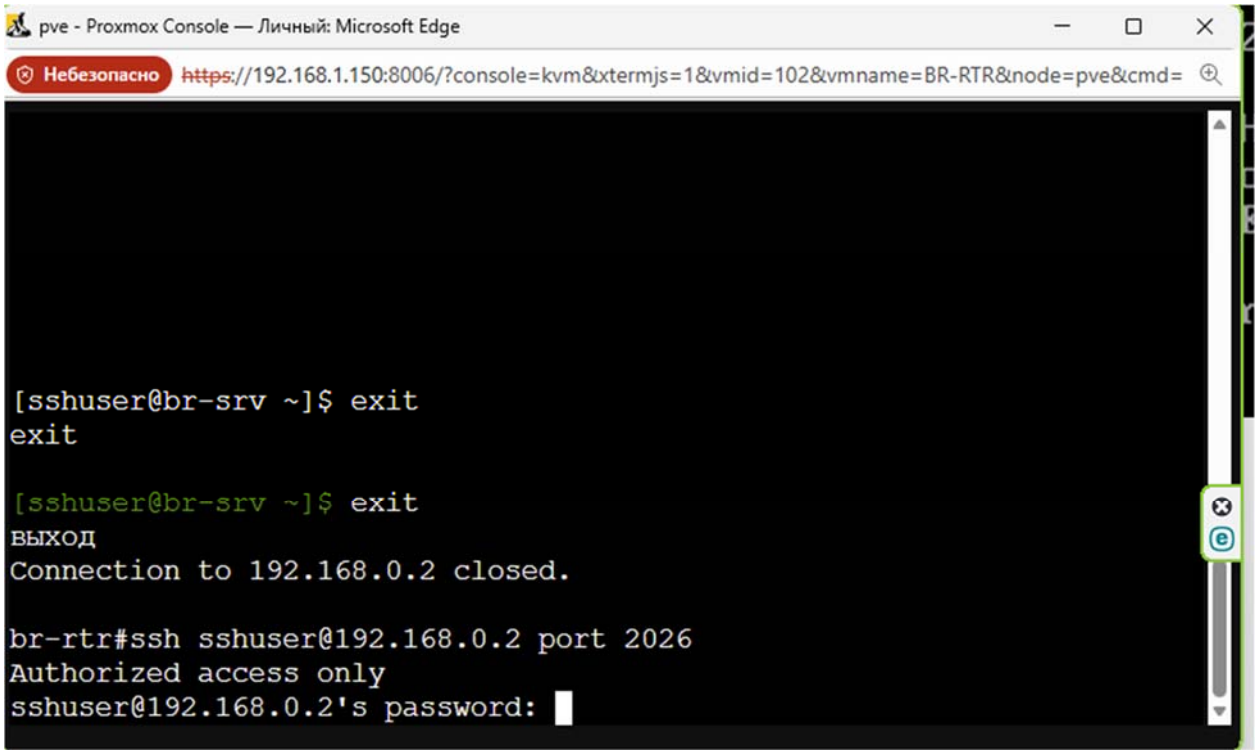


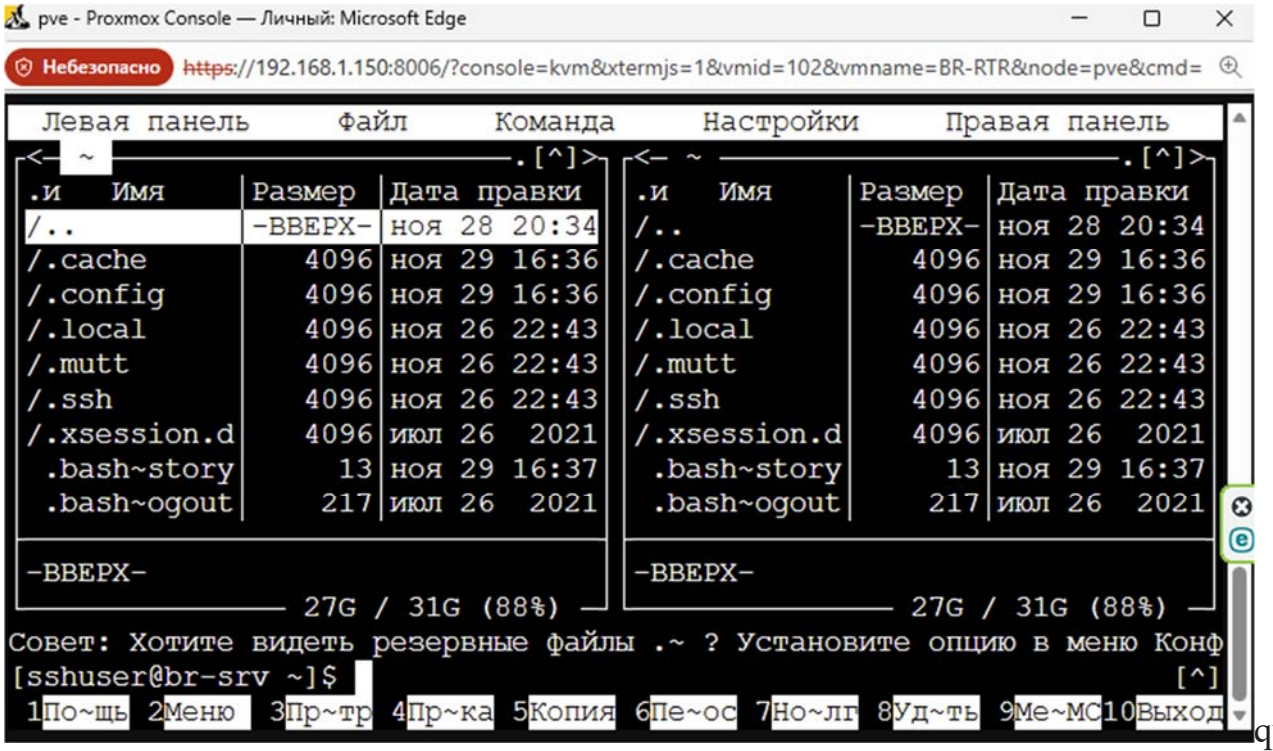
Доступ с HQ-RTR на HQ-SRV





Доступ с BR-RTR на BR-SRV





qw

2.6. Между офисами HQ и BR, на маршрутизаторах HQ-RTR и BR-RTR необходимо сконфигурировать ip gre туннель

Задание:

- На выбор технологии GRE или IP in IP
- Сведения о туннеле занесите в отчёт.

Вариант реализации:

HQ-RTR:

- Настраиваем **GRE** туннель в сторону офиса **BR (BR-RTR),**
    - где: i**nterface tunnel.<номер>** - номер это произвольное число

```
hq-rtr>enable
hq-rtr#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
hq-rtr(config)#interface tunnel.0
hq-rtr(config-if-tunnel)#description "GRE"
hq-rtr(config-if-tunnel)#ip address 10.10.10.1/30
hq-rtr(config-if-tunnel)#ip tunnel 172.16.1.2 172.16.2.2 mode gre

2025-09-04 06:23:20      INFO      Interface tunnel.0 changed state to up
hq-rtr(config-if-tunnel)#exit
hq-rtr(config)#write memory
Building configuration...

hq-rtr(config)#
```

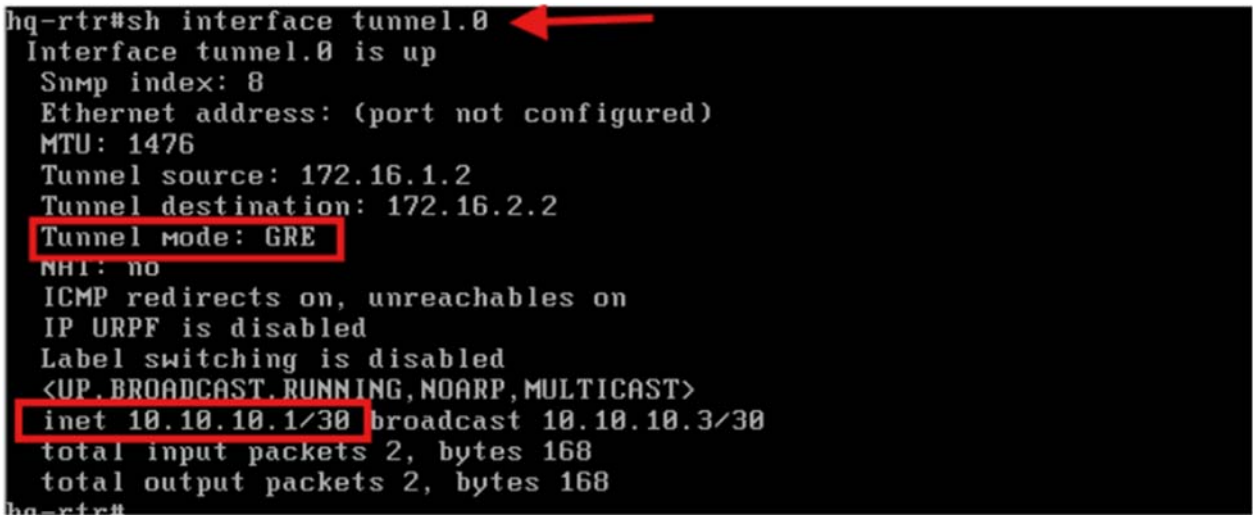
BR-RTR:

- Настраиваем **GRE** туннель в сторону офиса **HQ (HQ-RTR)**

```
br-rtr>enable
br-rtr#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
br-rtr(config)#interface tunnel.0
br-rtr(config-if-tunnel)#description "GRE"
```

```
br-rtr(config-if-tunnel)#ip address 10.10.10.2/30

br-rtr(config-if-tunnel)#ip tunnel 172.16.2.2 172.16.1.2 mode gre


2025-09-04 06:25:05      INFO      Interface tunnel.0 changed state to up

br-rtr(config-if-tunnel)#exit

br-rtr(config)#write memory

Building configuration...


br-rtr(config)#
```

- Проверить:
    - Режим работы туннеля и наличие IP-адреса на **HQ-RTR (GRE)**:



- Режим работы туннеля и наличие IP-адреса на **BR-RTR (GRE)**:

```
br-rtr#sh interface tunnel.0
 Interface tunnel.0 is up
  Snmp index: 6
  Ethernet address: (port not configured)
  MTU: 1476
  Tunnel source: 172.16.2.2
  Tunnel destination: 172.16.1.2
  Tunnel mode: GRE
  NAT: no
  ICMP redirects on, unreachables on
  IP URPF is disabled
  Label switching is disabled
  <UP,BROADCAST,RUNNING,NOARP,MULTICAST>
  inet 10.10.10.2/30 broadcast 10.10.10.3/30
  total input packets 2, bytes 168
  total output packets 2, bytes 168
```

- Связность по туннелю между **HQ-RTR <-> BR-RTR**:

```
hq-rtr#show ip interface brief
 Interface        IP-Address          Status                VRF
 ---------------------------------------------------------------
 vl100            192.168.100.1/27    up                    default
 vl200            192.168.200.1/28    up                    default
 vl999            192.168.99.1/29     up                    default
 isp              172.16.1.2/28       up                    default
 tunnel.0         10.10.10.1/30       up                    default
hq-rtr#ping 10.10.10.2
PING 10.10.10.2 (10.10.10.2) 56(84) bytes of data.
64 bytes from 10.10.10.2: icmp_seq=1 ttl=64 time=455 ms
64 bytes from 10.10.10.2: icmp_seq=2 ttl=64 time=478 ms
64 bytes from 10.10.10.2: icmp_seq=3 ttl=64 time=314 ms
64 bytes from 10.10.10.2: icmp_seq=4 ttl=64 time=517 ms

--- 10.10.10.2 ping statistics ---
5 packets transmitted, 4 received, 20% packet loss, time 4229ms
rtt min/avg/max/mdev = 314.436/440.966/517.165/76.390 ms
hq-rtr#D
```

2.7. Динамическая маршрутизация на маршрутизаторах HQ-RTR и BR-RTR

Задание:

- сети одного офиса должны быть доступны из другого офиса и наоборот. Для обеспечения динамической маршрутизации используйте link state протокол на усмотрение участника:
  - Разрешите выбранный протокол только на интерфейсах ip туннеля

- Маршрутизаторы должны делиться маршрутами только друг с другом
- Обеспечьте защиту выбранного протокола посредством парольной защиты
- Сведения о настройке и защите протокола занесите в отчёт.

HQ-RTR:

- Настраиваем OSPFv2:
  - Задаём router-id;
  - Переводим все интерфейсы в пассивный режим;
  - Объявляем сети;
  - На туннельном интерфейсе отключаем пассивный режим, чтобы можно было установить соседство:

```
hq-rtr>enable
hq-rtr#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
hq-rtr(config)#router ospf 1
hq-rtr(config-router)#ospf router-id 10.10.10.1
hq-rtr(config-router)#passive-interface default
hq-rtr(config-router)#no passive-interface tunnel.0
hq-rtr(config-router)#network 10.10.10.0/30 area 0
hq-rtr(config-router)#network 192.168.100.0/27 area 0
hq-rtr(config-router)#network 192.168.200.0/28 area 0
hq-rtr(config-router)#network 192.168.99.0/29 area 0
hq-rtr(config-router)#exit
```

- Обеспечиваем защиту протокола маршрутизации посредством парольной защиты:

```
hq-rtr(config)#interface tunnel.0
hq-rtr(config-if-tunnel)#ip ospf authentication message-digest
hq-rtr(config-if-tunnel)#ip ospf message-digest-key 1 md5 P@ssw0rd
hq-rtr(config-if-tunnel)#exit
hq-rtr(config)#write memory
Building configuration...
```

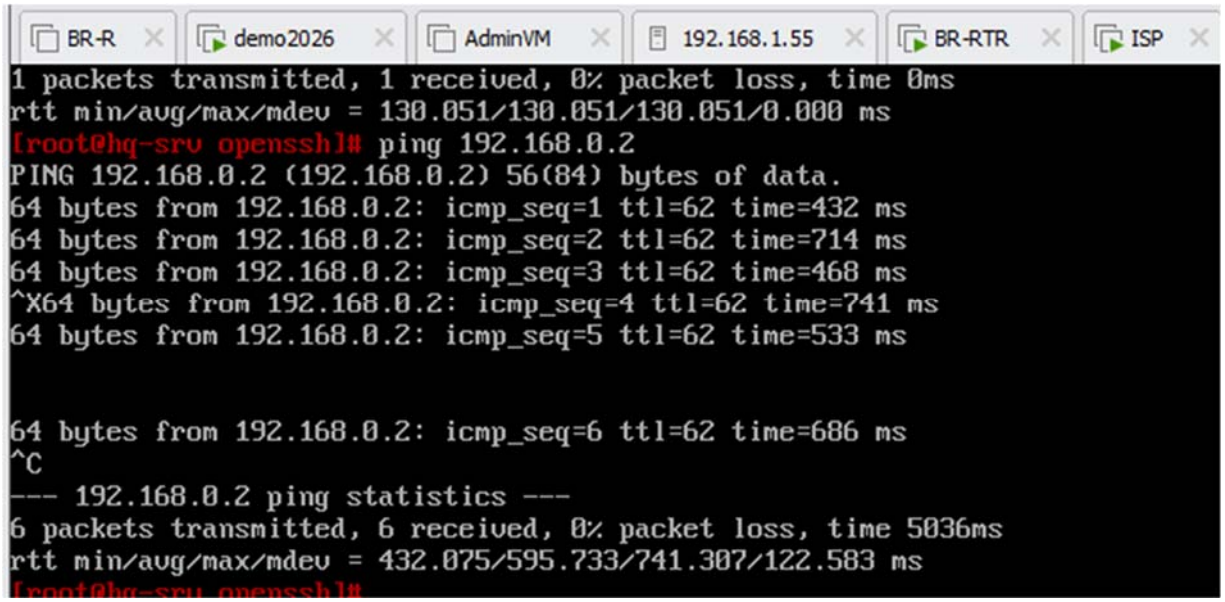
```
hq-rtr(config)#
```

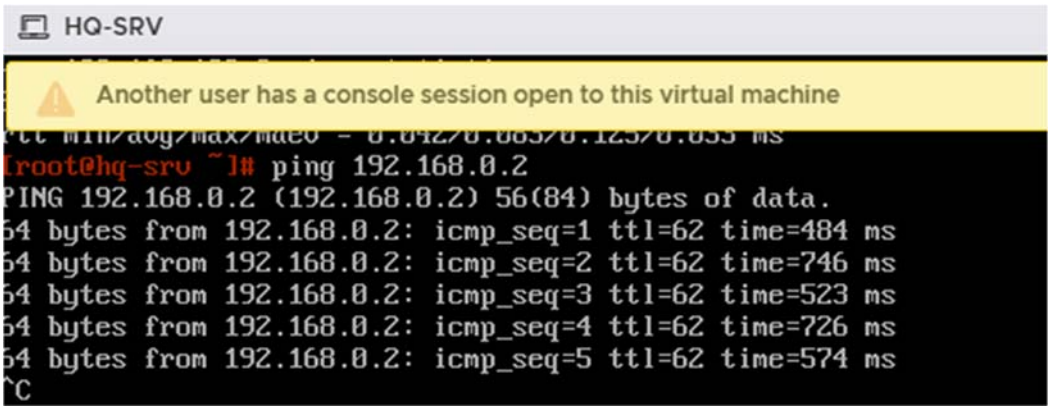
BR-RTR:

- Настраиваем OSPFv2, аналогично **HQ-RTR**:

```
br-rtr>enable
br-rtr#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
br-rtr(config)#router ospf 1
br-rtr(config-router)#ospf router-id 10.10.10.2
br-rtr(config-router)#passive-interface default
br-rtr(config-router)#no passive-interface tunnel.0
br-rtr(config-router)#network 192.168.0.0/28 area 0
br-rtr(config-router)#network 10.10.10.0/30 area 0
br-rtr(config-router)#exit
br-rtr(config)#interface tunnel.0
br-rtr(config-if-tunnel)#ip ospf authentication message-digest
br-rtr(config-if-tunnel)#ip ospf message-digest-key 1 md5 P@ssw0rd
br-rtr(config-if-tunnel)#exit
br-rtr(config)#write memory
Building configuration...

br-rtr(config)#
```

- Проверяем:
    - Наличие аутентификации на интерфейсе по которому предусмотрено установление соседства и обмен маршрутной информации:


BR-R
demo2026
AdminVM
192.168.1.55
BR-RTR
ISP
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 130.051/130.051/130.051/0.000 ms
[root@hq-srv openssh]# ping 192.168.0.2
PING 192.168.0.2 (192.168.0.2) 56(84) bytes of data.
64 bytes from 192.168.0.2: icmp_seq=1 ttl=62 time=432 ms
64 bytes from 192.168.0.2: icmp_seq=2 ttl=62 time=714 ms
64 bytes from 192.168.0.2: icmp_seq=3 ttl=62 time=468 ms
^X64 bytes from 192.168.0.2: icmp_seq=4 ttl=62 time=741 ms
64 bytes from 192.168.0.2: icmp_seq=5 ttl=62 time=533 ms
64 bytes from 192.168.0.2: icmp_seq=6 ttl=62 time=686 ms
^C
--- 192.168.0.2 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5036ms
rtt min/avg/max/mdev = 432.075/595.733/741.307/122.583 ms

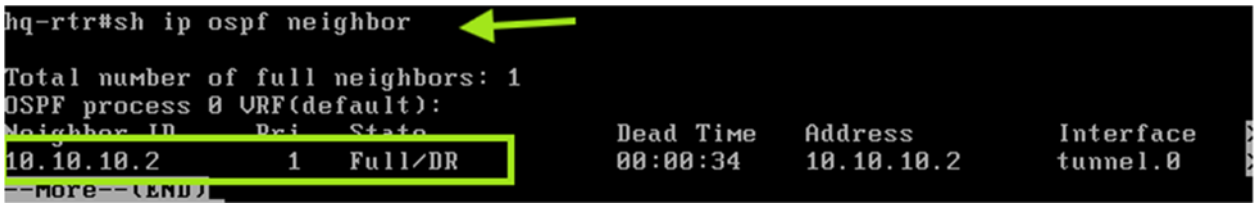

HQ-SRV
Another user has a console session open to this virtual machine
[root@hq-srv ~]# ping 192.168.0.2
PING 192.168.0.2 (192.168.0.2) 56(84) bytes of data.
64 bytes from 192.168.0.2: icmp_seq=1 ttl=62 time=484 ms
64 bytes from 192.168.0.2: icmp_seq=2 ttl=62 time=746 ms
64 bytes from 192.168.0.2: icmp_seq=3 ttl=62 time=523 ms
64 bytes from 192.168.0.2: icmp_seq=4 ttl=62 time=726 ms
64 bytes from 192.168.0.2: icmp_seq=5 ttl=62 time=574 ms
^C

```
hq-rtr#show ip ospf interface
vl100 is up, line protocol is up
  Internet Address 192.168.100.1/27, Area 0.0.0.0, MTU 1500
  Process ID 1, VRF (default), Router ID 10.10.10.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec,  State DROther, Priority 1, TE Metric 1
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    No Hellos (Passive interface)
  Neighbor Count is 0, Adjacent neighbor count is 0
  Hello received 0 sent 0, DD received 0 sent 0
  LS-Req received 0 sent 0, LS-Upd received 0 sent 0
  LS-Ack received 0 sent 0, Discarded 0
  No authentication
vl200 is up, line protocol is up
  Internet Address 192.168.200.1/24, Area 0.0.0.0, MTU 1500
  Process ID 1, VRF (default), Router ID 10.10.10.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec,  State DROther, Priority 1, TE Metric 1
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    No Hellos (Passive interface)
  Neighbor Count is 0, Adjacent neighbor count is 0
  Hello received 0 sent 0, DD received 0 sent 0
  LS-Req received 0 sent 0, LS-Upd received 0 sent 0
  LS-Ack received 0 sent 0, Discarded 0
  No authentication
vl999 is up, line protocol is up
  Internet Address 192.168.99.1/29, Area 0.0.0.0, MTU 1500
  Process ID 1, VRF (default), Router ID 10.10.10.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec,  State DROther, Priority 1, TE Metric 1
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    No Hellos (Passive interface)
  Neighbor Count is 0, Adjacent neighbor count is 0
  Hello received 0 sent 0, DD received 0 sent 0
  LS-Req received 0 sent 0, LS-Upd received 0 sent 0
  LS-Ack received 0 sent 0, Discarded 0
```

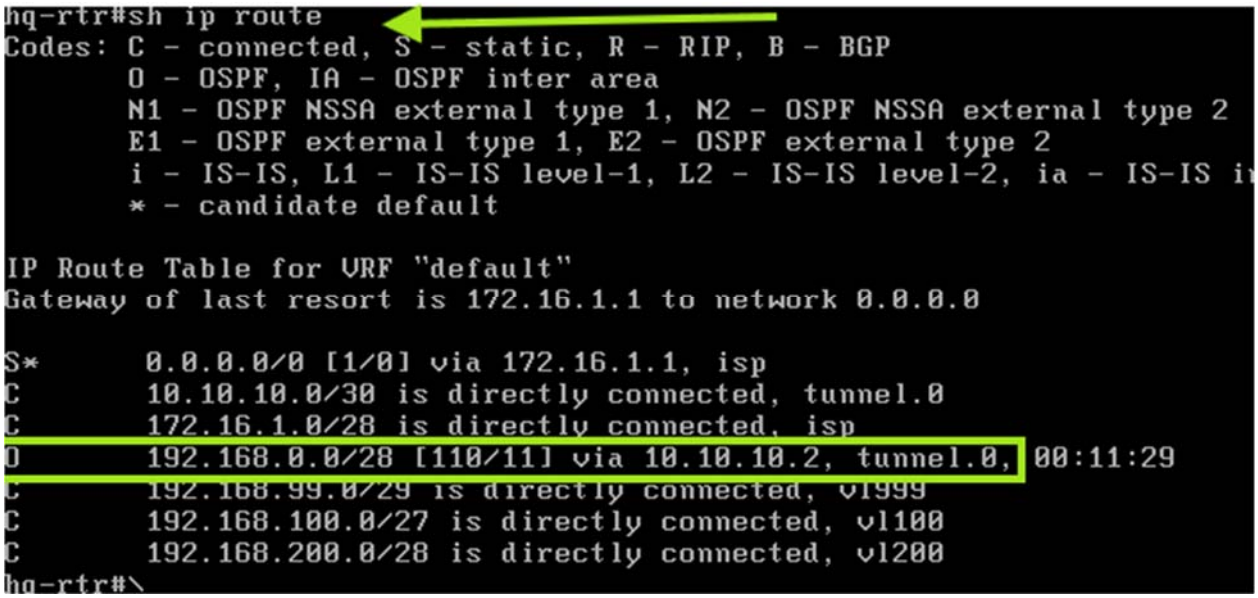
- **BR-RTR:**

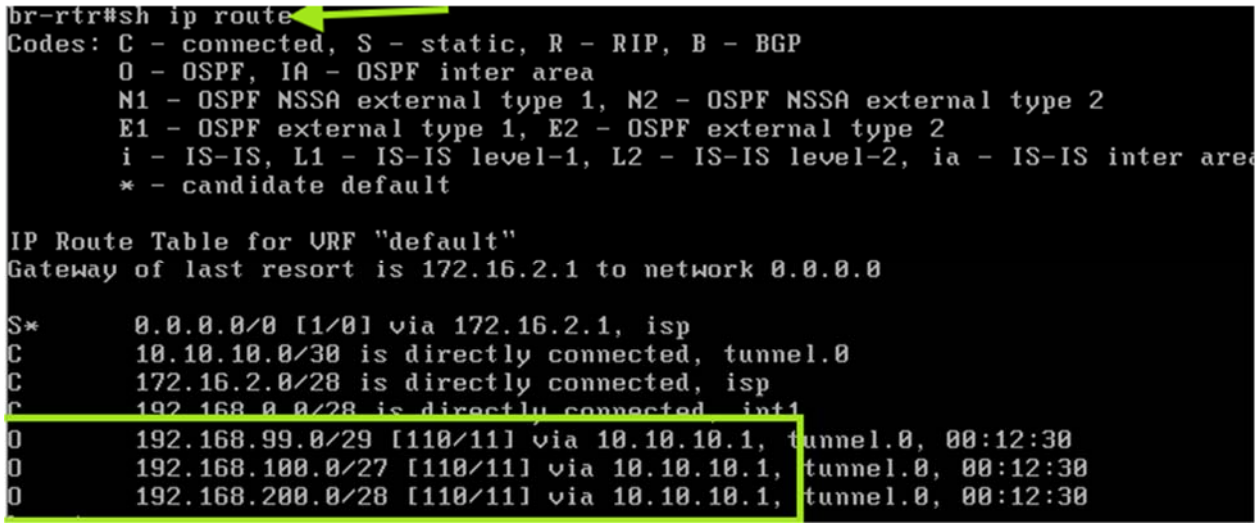
```
br-rtr#show ip ospf interface
int1 is up, line protocol is up
  Internet Address 192.168.0.1/28, Area 0.0.0.0, MTU 1500
  Process ID 1, VRF (default), Router ID 10.10.10.2, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec,  State DROther, Priority 1, TE Metric 1
  No designated router on this network
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    No Hellos (Passive interface)
  Neighbor Count is 0, Adjacent neighbor count is 0
  Hello received 0 sent 0, DD received 0 sent 0
  LS-Req received 0 sent 0, LS-Upd received 0 sent 0
  LS-Ack received 0 sent 0, Discarded 0
  No authentication
tunnel.0 is up, line protocol is up
  Internet Address 10.10.10.2/30, Area 0.0.0.0, MTU 1476
  Process ID 1, VRF (default), Router ID 10.10.10.2, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec,  State Backup, Priority 1, TE Metric 1
  Designated Router (ID) 10.10.10.1, Interface Address 10.10.10.1
  Backup Designated Router (ID) 10.10.10.2, Interface Address 10.10.10.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:08
  Neighbor Count is 1, Adjacent neighbor count is 1
  Crypt Sequence Number is 155602
  Hello received 3 sent 6, DD received 4 sent 3
  LS-Req received 1 sent 1, LS-Upd received 3 sent 3
  LS-Ack received 1 sent 2, Discarded 0
  Message-digest authentication, using key-id 1
br-rtr#
```

- Наличие установленного соседства:

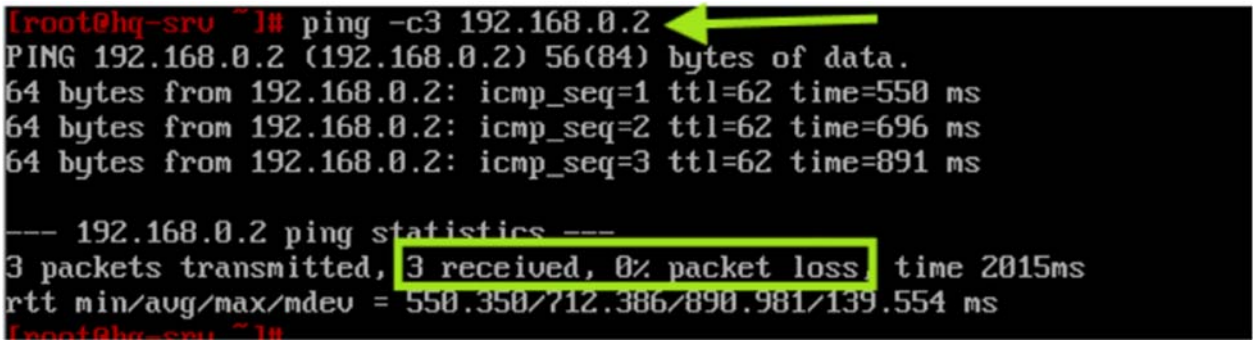


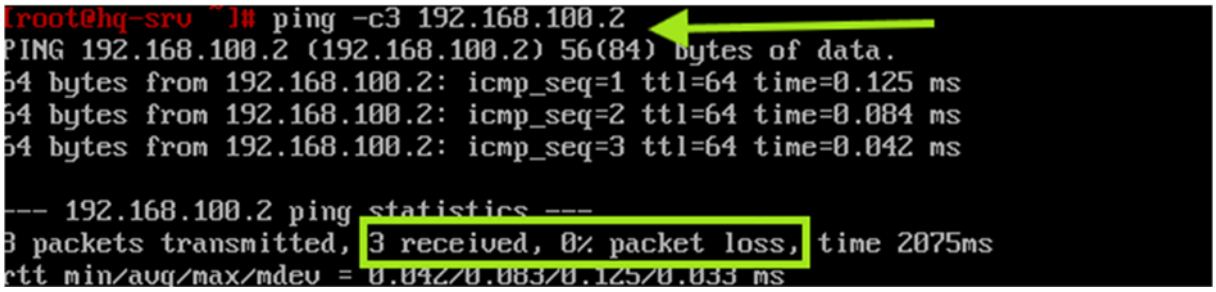
- Наличие полученных маршрутов по OSPF:





- Связность между устройствами офиса HQ и BR:





2.8. Настройка динамической трансляции адресов маршрутизаторах HQ-RTR и BR-RTR

Задание:

Настройте динамическую трансляцию адресов для обоих офисов в сторону ISP, все устройства в офисах должны иметь доступ к сети Интернет

Вариант реализации:

HQ-RTR:

С точки зрения **EcoRouter** - реализуем конфигурацию **static source PAT:**

Интерсейс в сторону **ISP** с именем **isp** - назначаем как **nat outside**:

```
hq-rtr>enable

hq-rtr#configure terminal

Enter configuration commands, one per line.  End with CNTL/Z.
```

```
hq-rtr(config)#interface isp
hq-rtr(config-if)#ip nat outside
hq-rtr(config-if)#exit
```

-
  - Подинтерфейсы **vl100, vl200, vl999** - назначаем как **nat inside**:

```
hq-rtr(config)#interface vl100
hq-rtr(config-if)#ip nat inside
hq-rtr(config-if)#exit
hq-rtr(config)#interface vl200
hq-rtr(config-if)#ip nat inside
hq-rtr(config-if)#exit
hq-rtr(config)#interface vl999
hq-rtr(config-if)#ip nat inside
hq-rtr(config-if)#exit
```

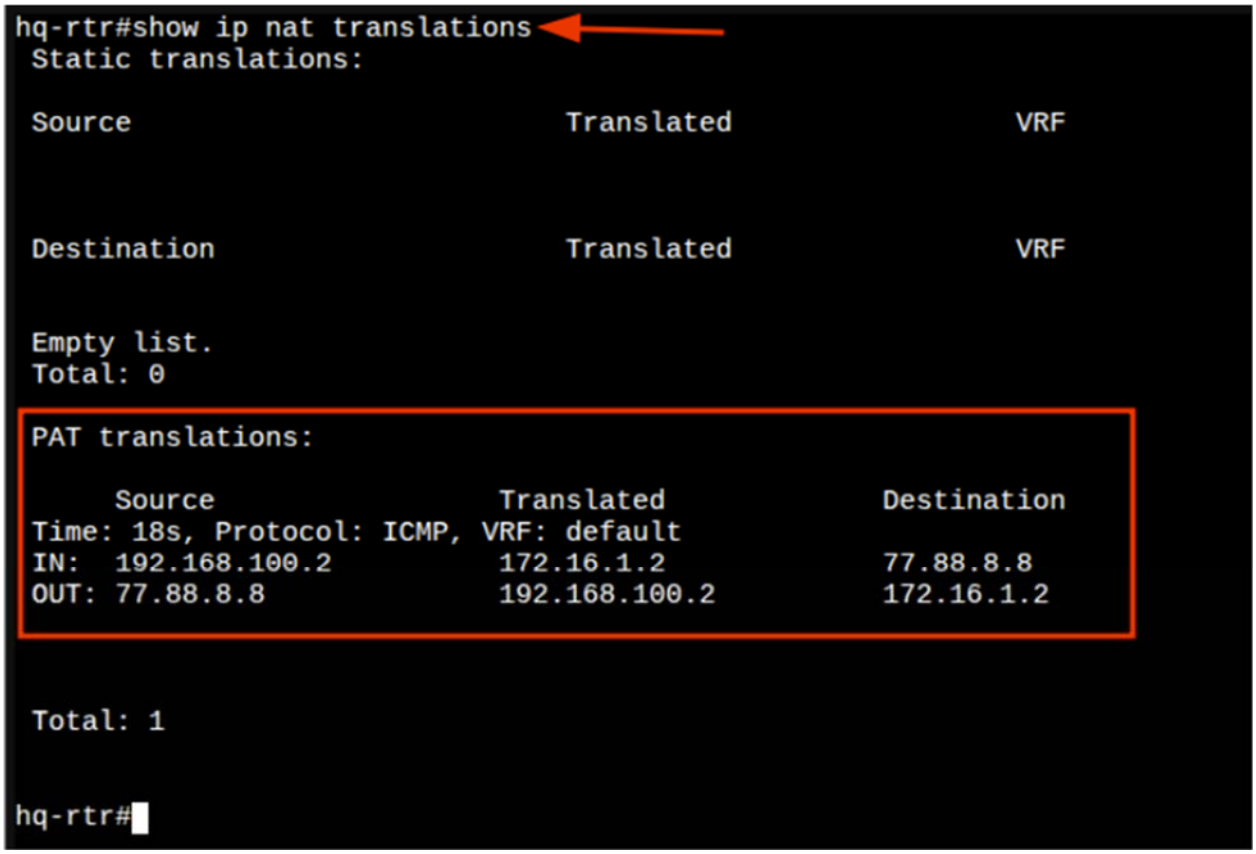
-
  - создаём пулы адресов для локальных подсетей офиса **HQ** для входящего трафика - указываем диапазон адресов из выделенных подсети:

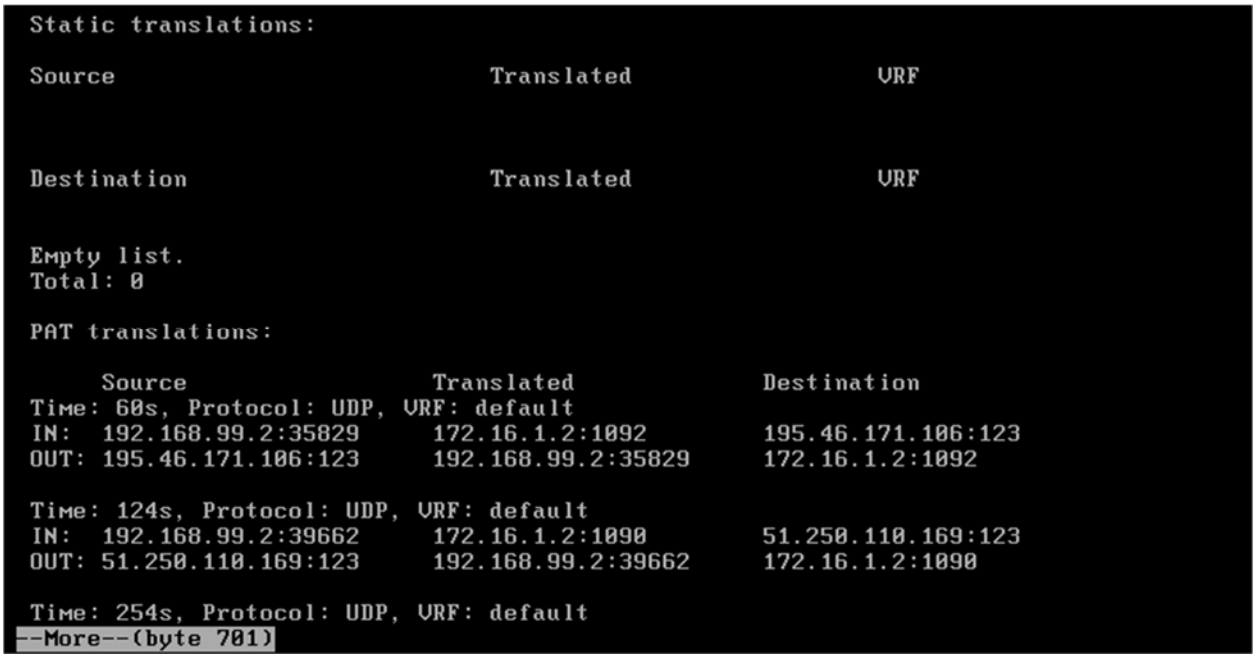
```
hq-rtr(config)#ip nat pool VLAN100 192.168.100.1-192.168.100.30
hq-rtr(config)#ip nat pool VLAN200 192.168.200.1-192.168.200.14
hq-rtr(config)#ip nat pool VLAN999 192.168.99.1-192.168.99.6
```

  - задаём правила для трансляции адресов:

```
hq-rtr(config)#ip nat source dynamic inside-to-outside pool VLAN100 overload interface isp
hq-rtr(config)#ip nat source dynamic inside-to-outside pool VLAN200 overload interface isp
hq-rtr(config)#ip nat source dynamic inside-to-outside pool VLAN999 overload interface isp
hq-rtr(config)#write memory
Building configuration...


hq-rtr(config)#
```

- Проверяем доступ в сеть Интернет с устройств офиса HQ - **HQ-SRV**:





BR-RTR:

- Настраиваем аналогично **HQ-RTR**:

```
br-rtr>enable

br-rtr#configure terminal
```

```
Enter configuration commands, one per line.  End with CNTL/Z.

br-rtr(config)#interface isp

br-rtr(config-if)#ip nat outside

br-rtr(config-if)#exit

br-rtr(config)#interface int1

br-rtr(config-if)#ip nat inside

br-rtr(config-if)#exit

br-rtr(config)#ip nat pool BR-Net 192.168.0.1-192.168.0.14

br-rtr(config)#ip nat source dynamic inside-to-outside pool BR-Net overload interface isp

br-rtr(config)#exit

br-rtr#write memory

Building configuration...


br-rtr#
```

- Проверяем доступ в сеть Интернет с устройств офиса BR - **BR-SRV**:

```
[root@br-srv ~]# ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=49.9 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=257 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=64 time=71.1 ms
^C
--- 192.168.0.1 ping statistics ---
4 packets transmitted, 3 received, 25% packet loss, time 3015ms
rtt min/avg/max/mdev = 49.878/125.965/256.881/92.977 ms
```

```
[root@br-srv ~]# ping -c3 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
64 bytes from 192.168.0.1: icmp_seq=1 ttl=64 time=237 ms
64 bytes from 192.168.0.1: icmp_seq=2 ttl=64 time=46.7 ms
64 bytes from 192.168.0.1: icmp_seq=3 ttl=64 time=293 ms

--- 192.168.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2015ms
rtt min/avg/max/mdev = 46.660/192.215/293.064/105.444 ms
```

```
br-rtr#sh ip nat translations_
```

```
Static translations:

Source                          Translated                  VRF



Destination                     Translated                  VRF


Empty list.
Total: 0

PAT translations:

     Source                  Translated            Destination
Time: 5s, Protocol: ICMP, VRF: default
IN:  192.168.0.2             172.16.2.2            77.88.8.8
OUT: 77.88.8.8               192.168.0.2           172.16.2.2



Total: 1


br-rtr#
```

2.9. Настройте протокол динамической конфигурации хостов для сети в сторону HQ-CLI

Задание:

- Настройте нужную подсеть
- В качестве сервера DHCP выступает маршрутизатор HQ-RTR
- Клиентом является машина HQ-CLI
- Исключите из выдачи адрес маршрутизатора
- Адрес шлюза по умолчанию – адрес маршрутизатора HQ-RTR
- Адрес DNS-сервера для машины HQ-CLI – адрес сервера HQ-SRV
- DNS-суффикс – au-team.irpo
- Сведения о настройке протокола занесите в отчёт.

Вариант реализации:

HQ-RTR:

- Задаём POOL адресов с именем **VLAN200**, затем задаём диапазон IP-адресов, который будет раздаваться DHCP сервером:
    - в данном случае раздаваться будет вся клиентская подсеть заисключением IP-адреса маршрутизатора HQ-RTR

```
hq-rtr#configure
Enter configuration commands, one per line.  End with CNTL/Z.
hq-rtr(config)#ip pool VLAN200
hq-rtr(config-ip-pool)#range 192.168.200.2-192.168.200.14
hq-rtr(config-ip-pool-range)#
```

Для настройки DHCP-сервера необходимо в режиме конфигурации ввести команду **dhcp-server <NUMBER>**

- где **NUMBER** – номер сервера в системе маршрутизатора:

```
hq-rtr(config)#dhcp-server 1
hq-rtr(config-dhcp-server)#
```

- Привязываем ранее созданный POOL раздаваемых адресов с именем **VLAN200** с номером DHCP-сервера в системе маршрутизатора **1**:

```
hq-rtr(config-dhcp-server)#pool VLAN200 1
hq-rtr(config-dhcp-server-pool)
```

- Задаём основные параметры для раздачи DHCP сервером:

```
hq-rtr(config-dhcp-server-pool)#mask 28
hq-rtr(config-dhcp-server-pool)#gateway 192.168.200.1
hq-rtr(config-dhcp-server-pool)#dns 192.168.100.2
hq-rtr(config-dhcp-server-pool)#domain-name au-team.irpo
hq-rtr(config-dhcp-server-pool)#exit
hq-rtr(config-dhcp-server)#exit
```

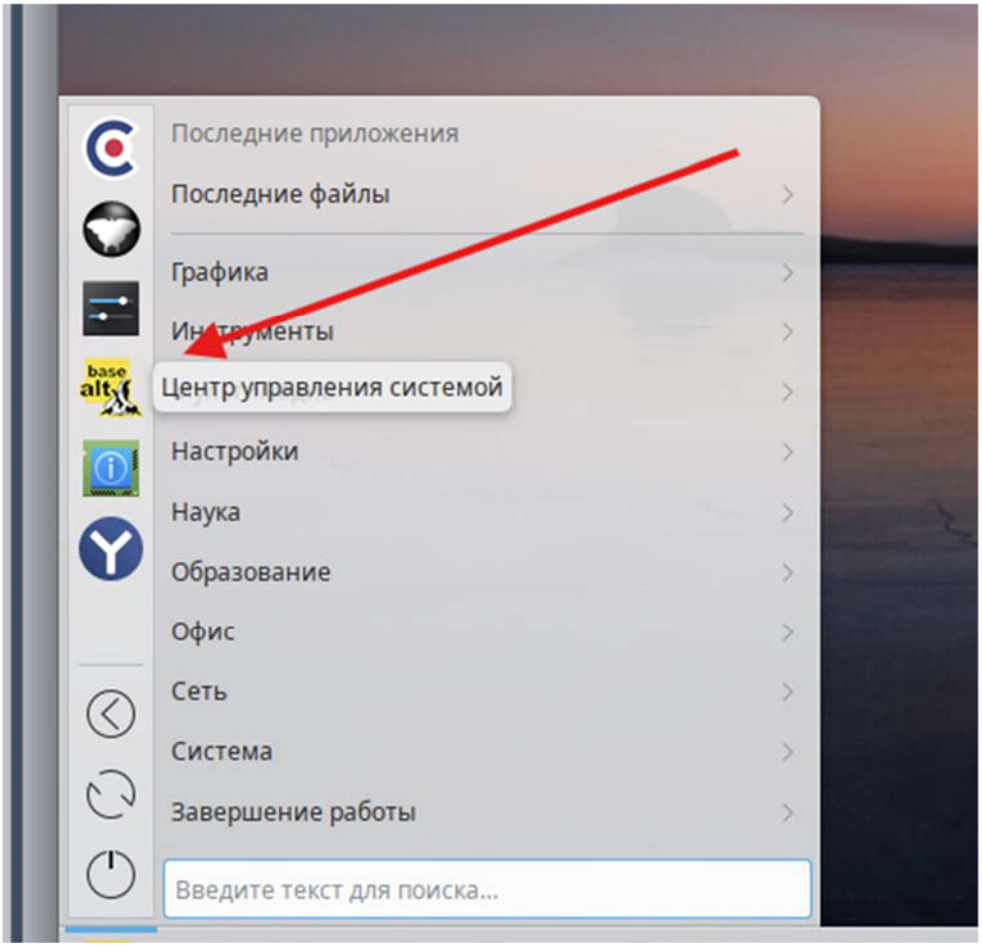
- После настройки сервера необходимо указать, на каком интерфейсе маршрутизатор будет принимать пакеты DHCP Discover и отвечать на них предложением с IP-настройками:
  - в данном случае подинтерфейс с именем **vl200** смотрит в сторону клиентской подсети (vlan200)

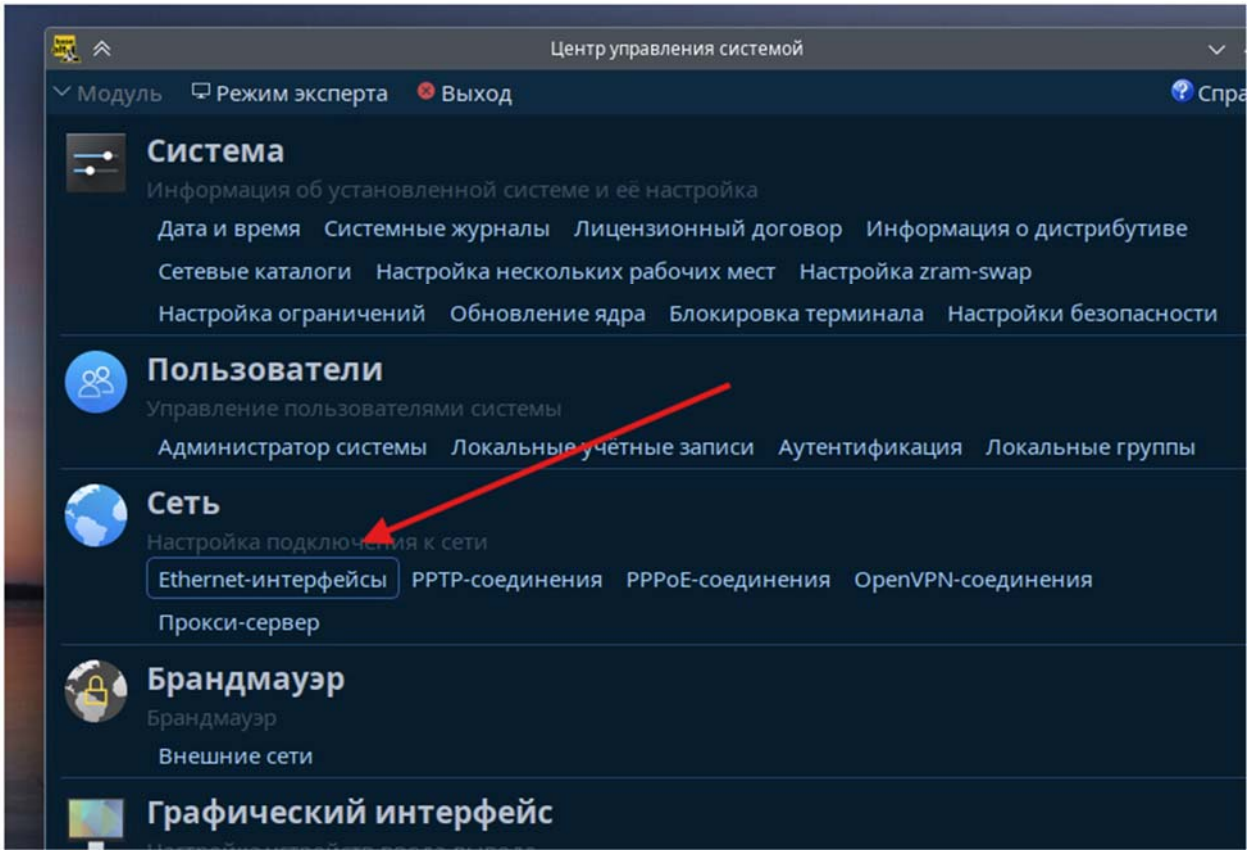
```
hq-rtr(config)#interface vl200
hq-rtr(config-if)#dhcp-server 1
hq-rtr(config-if)#exit
hq-rtr(config)#write memory
```

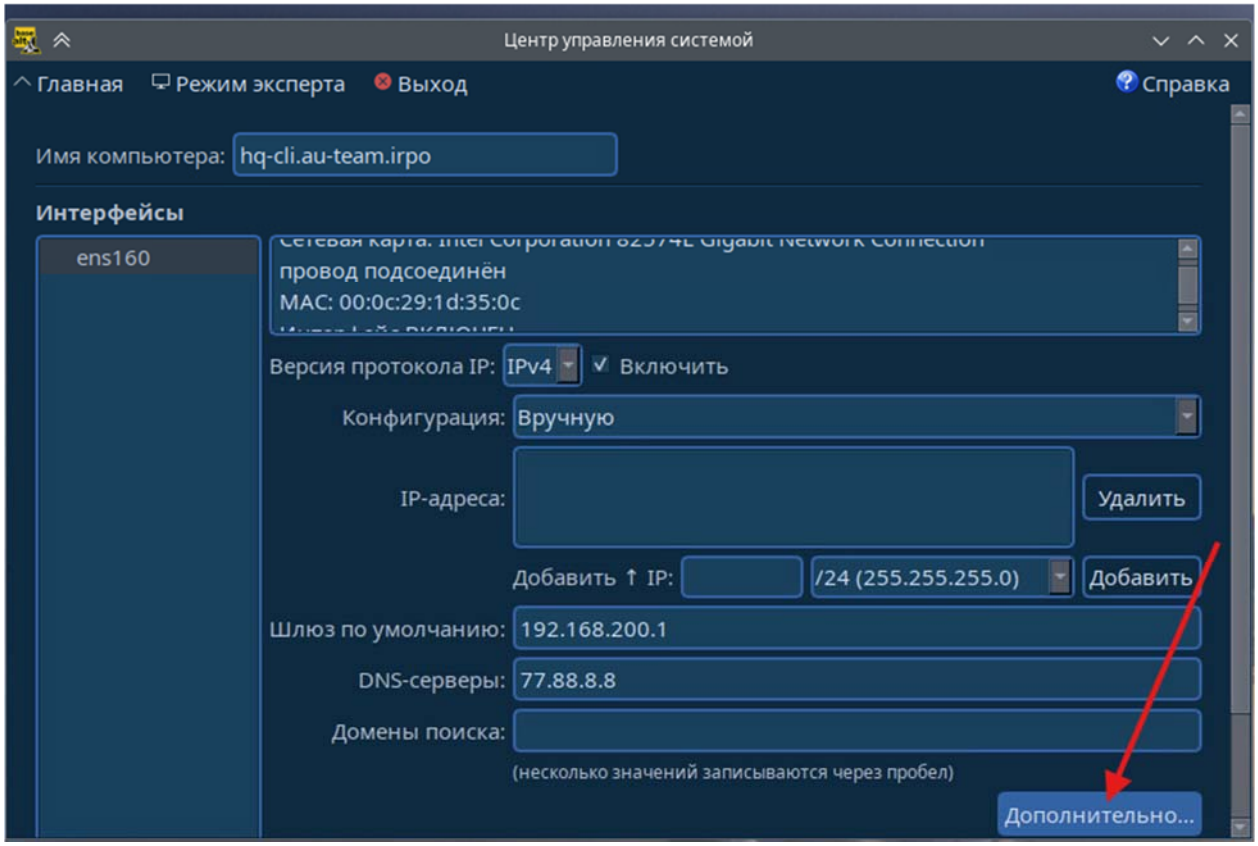
```
Building configuration...


hq-rtr(config)#
```

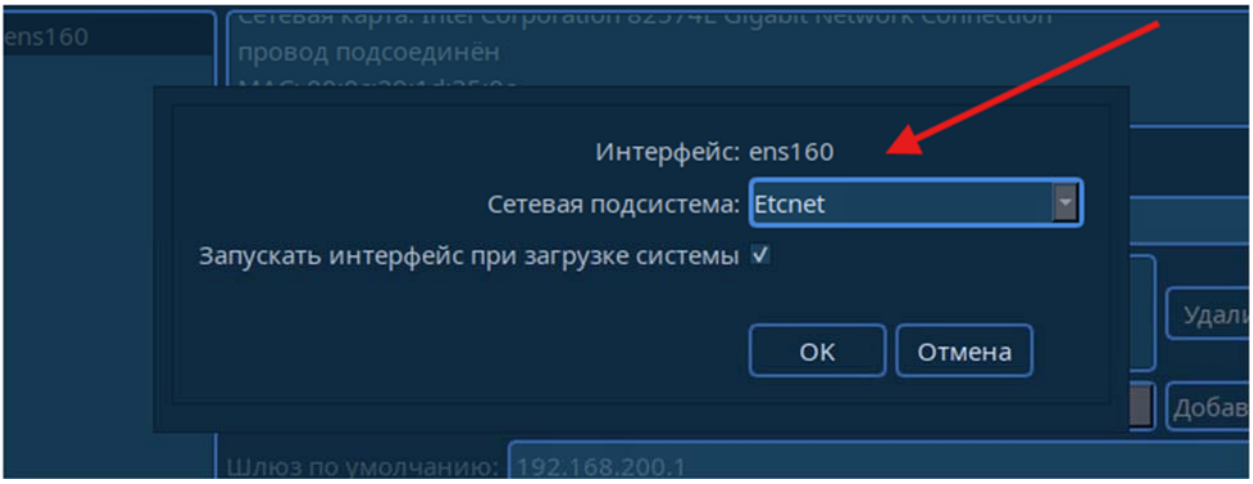
- Проверить, наличие полученных параметров по DHCP на **HQ-CLI**:
  - в Центре Управления Системой (ЦУС) выбрать в качестве режима работы сетевой подсистемы:

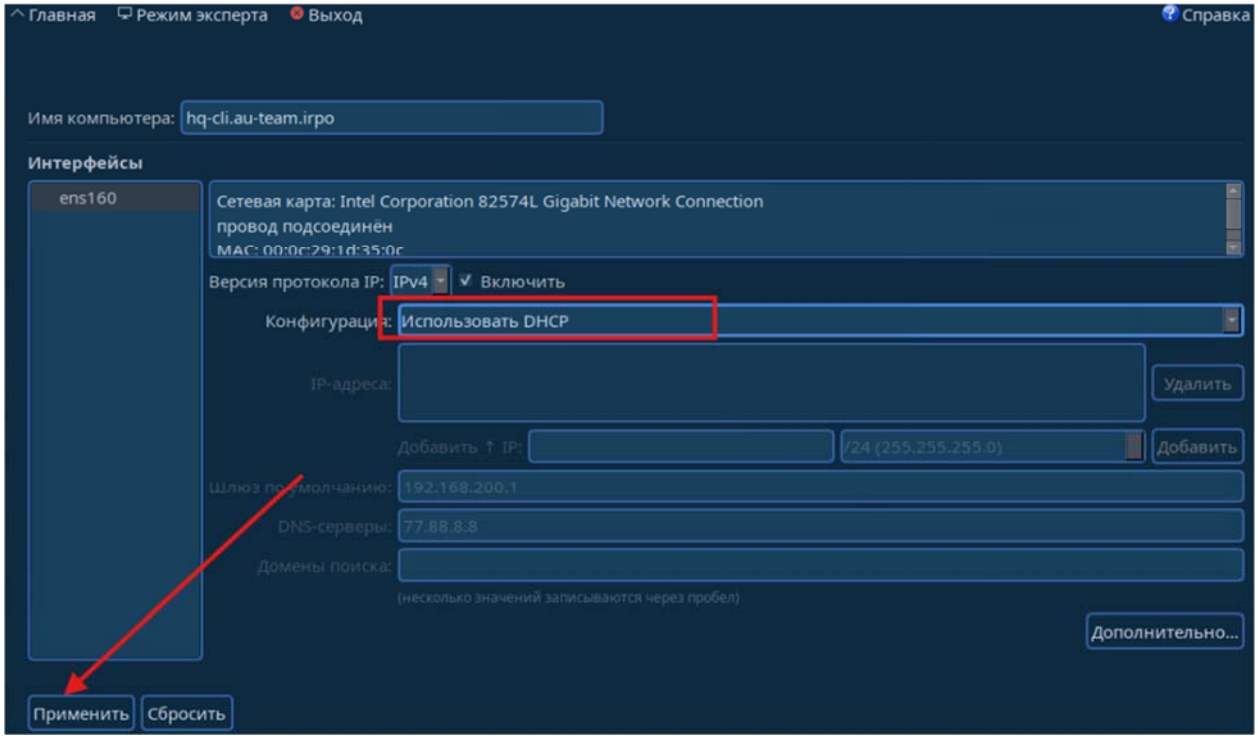
HQ-CLI

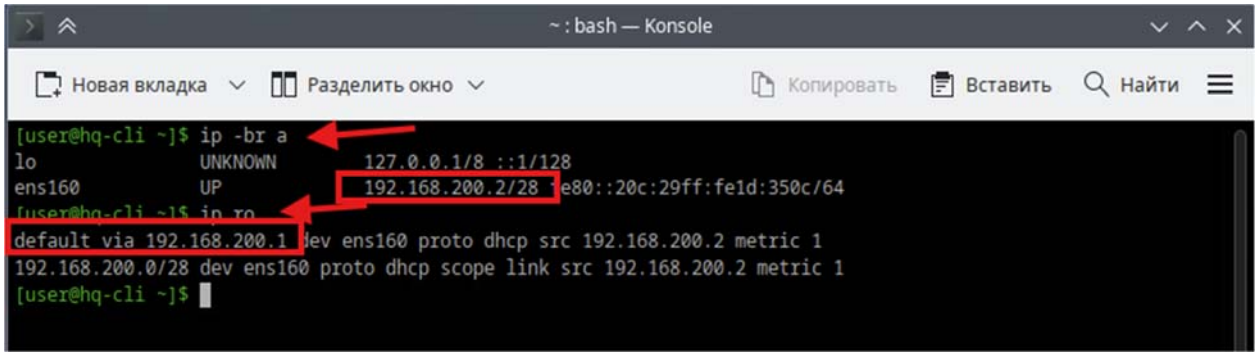


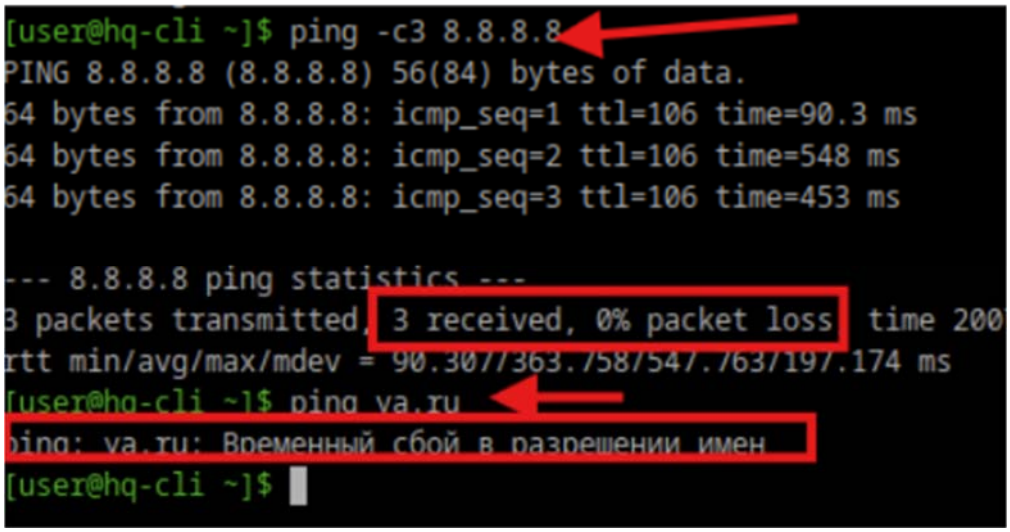

Центр управления системой
Модуль
Режим эксперта
Выход
Спра
Система
Информация об установленной системе и её настройка
Дата и время
Системные журналы
Лицензионный договор
Информация о дистрибутиве
Сетевые каталоги
Настройка нескольких рабочих мест
Настройка zram-swap
Настройка ограничений
Обновление ядра
Блокировка терминала
Настройки безопасности
Пользователи
Управление пользователями системы
Администратор системы
Локальные учётные записи
Аутентификация
Локальные группы
Сеть
Настройка подключения к сети
Ethernet-интерфейсы
PPTP-соединения
PPPoE-соединения
OpenVPN-соединения
Прокси-сервер
Брандмауэр
Брандмауэр
Внешние сети
Графический интерфейс


Центр управления системой
Главная
Режим эксперта
Выход
Справка
Имя компьютера:
hq-cli.au-team.irpo
Интерфейсы
ens160
провод подсоединён
MAC: 00:0c:29:1d:35:0c
Версия протокола IP:
IPv4
Включить
Конфигурация:
Вручную
IP-адреса:
Удалить
Добавить ↑ IP:
/24 (255.255.255.0)
Добавить
Шлюз по умолчанию:
192.168.200.1
DNS-серверы:
77.88.8.8
Домены поиска:
(несколько значений записываются через пробел)
Дополнительно...

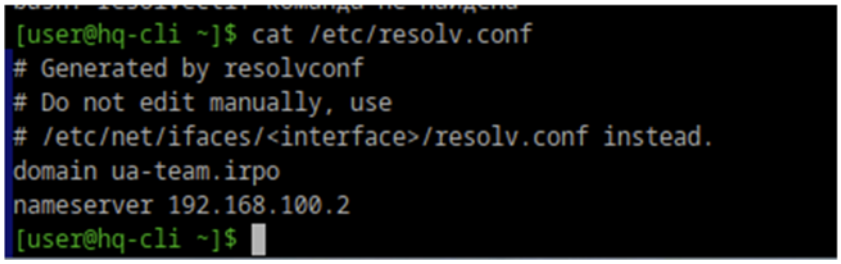

ens160
провод подсоединён
Интерфейс: ens160
Сетевая подсистема: Etcnet
Запускать интерфейс при загрузке системы
OK
Отмена
Шлюз по умолчанию: 192.168.200.1


Главная
Режим эксперта
Выход
Справка
Имя компьютера: hq-cli.au-team.irpo
Интерфейсы
ens160
Сетевая карта: Intel Corporation 82574L Gigabit Network Connection
провод подсоединён
MAC: 00:0c:29:1d:35:0c
Версия протокола IP: IPv4
Включить
Конфигурация: Использовать DHCP
IP-адреса:
Удалить
Добавить IP:
/24 (255.255.255.0)
Добавить
Шлюз по умолчанию: 192.168.200.1
DNS-серверы: 77.88.8.8
Домены поиска:
(несколько значений записываются через пробел)
Дополнительно...
Применить
Сбросить


~ : bash — Konsole
Новая вкладка
Разделить окно
Копировать
Вставить
Найти
[user@hq-cli ~]$ ip -br a
lo UNKNOWN 127.0.0.1/8 ::1/128
ens160 UP 192.168.200.2/28 e80::20c:29ff:fe1d:350c/64
[user@hq-cli ~]$ ip ro
default via 192.168.200.1 dev ens160 proto dhcp src 192.168.200.2 metric 1
192.168.200.0/28 dev ens160 proto dhcp scope link src 192.168.200.2 metric 1
[user@hq-cli ~]$



ВНИМАНИЕ DNS не работает пока не настроен DNS сервер HQ-SRV



2.10. Настройте инфраструктуру разрешения доменных имён для офисов HQ и BR

Задание:

- Основной DNS-сервер реализован на HQ-SRV
- Сервер должен обеспечивать разрешение имён в сетевые адреса устройств и обратно в соответствии с таблицей 3
- В качестве DNS сервера пересылки используйте любой общедоступный DNS сервер(77.88.8.7, 77.88.8.3 или другие)

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

ISP (интерфейс направленный в сторону HQ-RTR)	docker.au-team.irpo	A
ISP (интерфейс направленный в сторону BR-RTR)	web.au-team.irpo	A

Вариант реализации:

HQ-SRV:

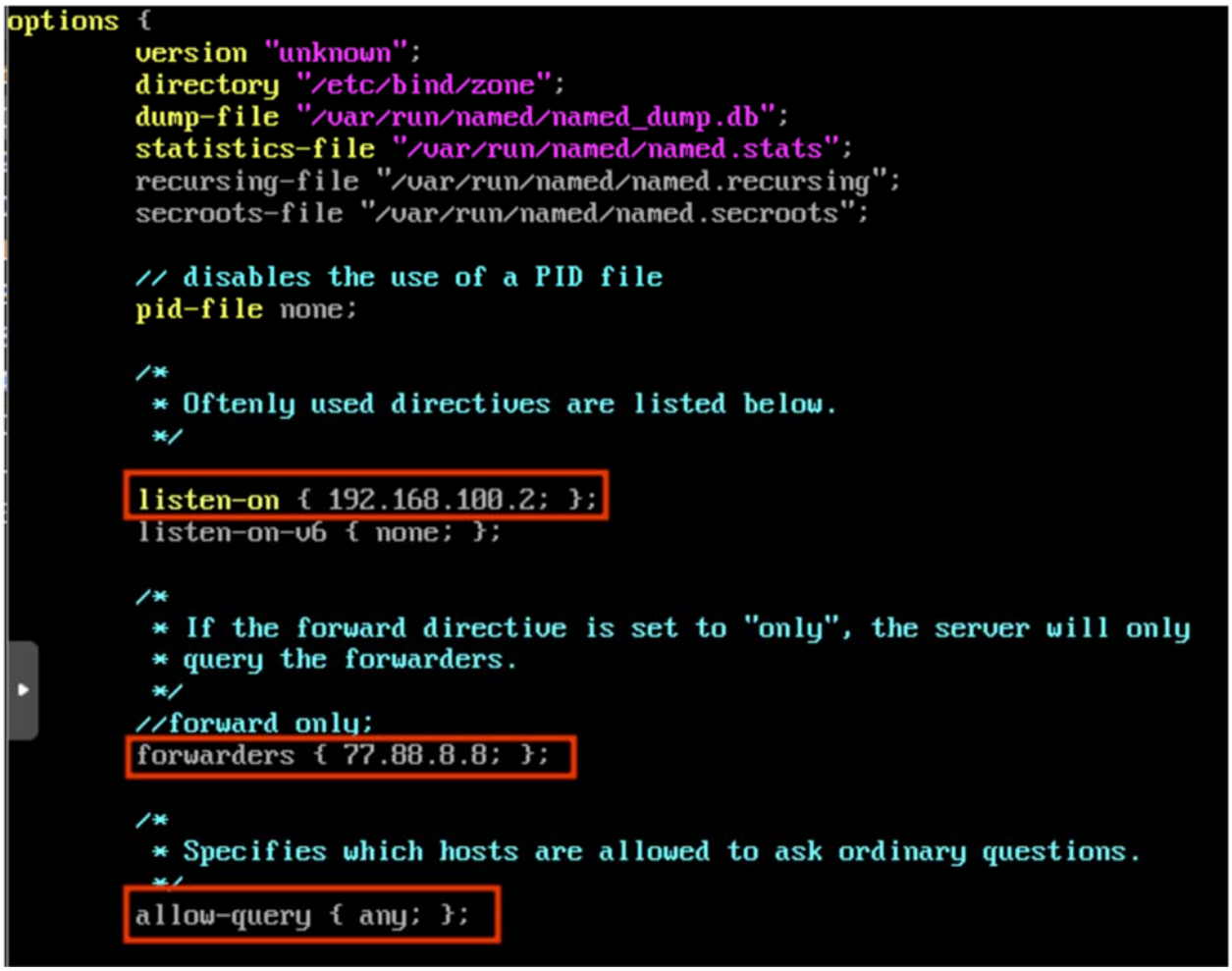
- Для установки и дальнейшей настройки DNS-сервера, необходимо выполнить установку пакета BIND:

```
apt-get update && apt-get install bind bind-utils -y
```

- Далее выполняется редактирование конфигурационного файла **/var/lib/bind/etc/options.conf** согласно скриншоту

```
vim /var/lib/bind/etc/options.conf
```

-
  - где:
    - **listen-on** параметр определяет адреса и порты, на которых DNS-сервер будет слушать запросы;
    - В параметре **forwarders** указываются сервера, куда будут перенаправляться запросы, на которые нет информации в локальной зоне;
    - **allow-query** – IP-адреса и подсети от которых будут обрабатываться запросы;



- Далее необходимо добавить зоны прямого и обратного просмотра в файл **/var/lib/bind/etc/rfc1912.conf:**

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

-
  - Добавляем следующее содержимое (в конец файла):

```
zone "au-team.irpo" {
        type master;
        file "au-team.irpo";
};

zone "100.168.192.in-addr.arpa" {
        type master;
        file "100.168.192.in-addr.arpa";
};

zone "200.168.192.in-addr.arpa" {
        type master;
        file "200.168.192.in-addr.arpa";
};
~
```

- Создаём файлы зон прямого и обратного просмотра из шаблона:

```
[root@hq-srv ~]# cp /var/lib/bind/etc/zone/empty /var/lib/bind/etc/zone/au-team.irpo
[root@hq-srv ~]# cp /var/lib/bind/etc/zone/empty /var/lib/bind/etc/zone/100.168.192.in-addr.arpa
[root@hq-srv ~]# cp /var/lib/bind/etc/zone/empty /var/lib/bind/etc/zone/200.168.192.in-addr.arpa
[root@hq-srv ~]# _
```

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

```
vim /var/lib/bind/etc/zone/au-team.irpo
```

-
  - который является прямой зоной следующим образом:

```
$TTL    1D
@       IN      SOA     au-team.irpo. root.au-team.irpo. (
                                2025062300      ; serial
                                12H             ; refresh
                                1H              ; retry
                                1W              ; expire
                                1H              ; ncache
                        )
        IN      NS      au-team.irpo.
        IN      A       192.168.100.2
hq-srv  IN      A       192.168.100.2
hq-cli  IN      A       192.168.200.2
hq-rtr  IN      A       192.168.100.1
hq-rtr  IN      A       192.168.200.1
hq-rtr  IN      A       192.168.99.1
docker  IN      A       172.16.1.1
web     IN      A       172.16.2.1
br-srv  IN      A       192.168.0.2
br-rtr  IN      A       192.168.0.1
~
```

- Далее необходимо настроить обратную зону и привести файл **100.168.192.in-addr.arpa**:

```
vim /var/lib/bind/etc/zone/100.168.192.in-addr.arpa
```

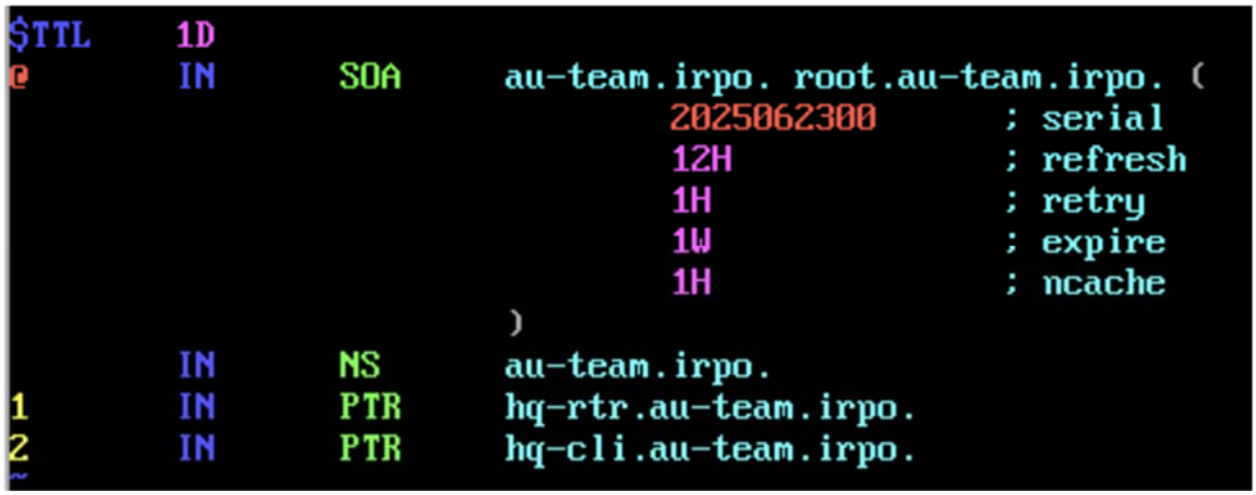
-
  - к следующему виду:

```
$TTL    1D
@       IN      SOA     au-team.irpo. root.au-team.irpo. (
                                2025062300      ; serial
                                12H             ; refresh
                                1H              ; retry
                                1W              ; expire
                                1H              ; ncache
                        )
        IN      NS      au-team.irpo.
1       IN      PTR     hq-rtr.au-team.irpo.
2       IN      PTR     hq-srv.au.team.irpo.
~
```

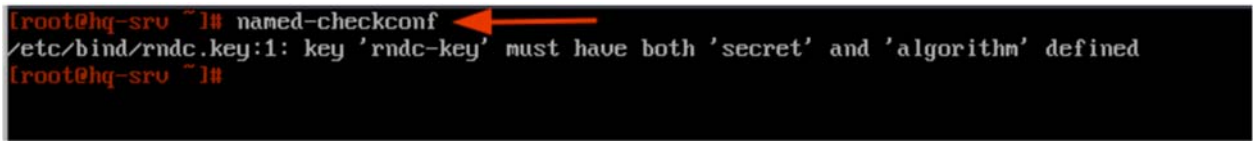
- Далее необходимо настроить обратную зону и привести файл **200.168.192.in-addr.arpa**:

```
vim /var/lib/bind/etc/zone/200.168.192.in-addr.arpa
```

-
  - к следующему виду:



- 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, 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
```

-
  -
    - Результат:

```
[root@hq-srv ~]# rndc-confgen > /etc/bind/rndc.key
[root@hq-srv ~]# sed -i '6,$d' /etc/bind/rndc.key
[root@hq-srv ~]# cat /etc/bind/rndc.key
# Start of rndc.conf
key "rndc-key" {
        algorithm hmac-sha256;
        secret "SKB1FfUzpWq44SPhErFg5+q5SiSvzp8fklbrZQvNvzs=";
};
[root@hq-srv ~]# _
```

- 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:

```
[root@hq-srv ~]# named-checkconf
[root@hq-srv ~]#
```

```
[root@hq-srv ~]# chown  -R root:named /etc/bind/zone/*
[root@hq-srv ~]# ls -l /etc/bind/zone/
total 32
-rw-r----- 1 root named  378 Sep  4 10:14 100.168.192.in-addr.arpa
-rw-r----- 1 root named  212 May 22 11:22 127.in-addr.arpa
-rw-r----- 1 root named  378 Sep  4 10:15 200.168.192.in-addr.arpa
-rw-r----- 1 root named  558 Sep  4 10:13 au-team.irpo
-rw-r----- 1 root named  309 May 22 11:22 empty
-rw-r----- 1 root named  208 May 22 11:22 localdomain
-rw-r----- 1 root named  178 May 22 11:22 localhost
drwx------ 2 root named 4096 May 22 11:22 slave
[root@hq-srv ~]#
```

```
[root@hq-srv ~]# named-checkconf -z
zone localhost/IN: loaded serial 2025062300
zone localdomain/IN: loaded serial 2025062300
zone 127.in-addr.arpa/IN: loaded serial 2025062300
zone 0.in-addr.arpa/IN: loaded serial 2025062300
zone 255.in-addr.arpa/IN: loaded serial 2025062300
zone au-team.irpo/IN: loaded serial 2025062300
zone 100.168.192.in-addr.arpa/IN: loaded serial 2025062300
zone 200.168.192.in-addr.arpa/IN: loaded serial 2025062300
[root@hq-srv ~]#
```

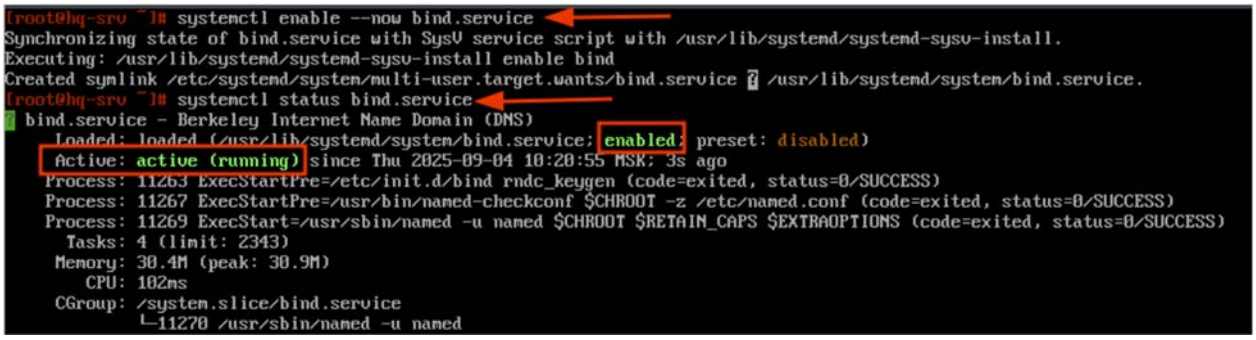
- После этого можно запустить службу **bind**:

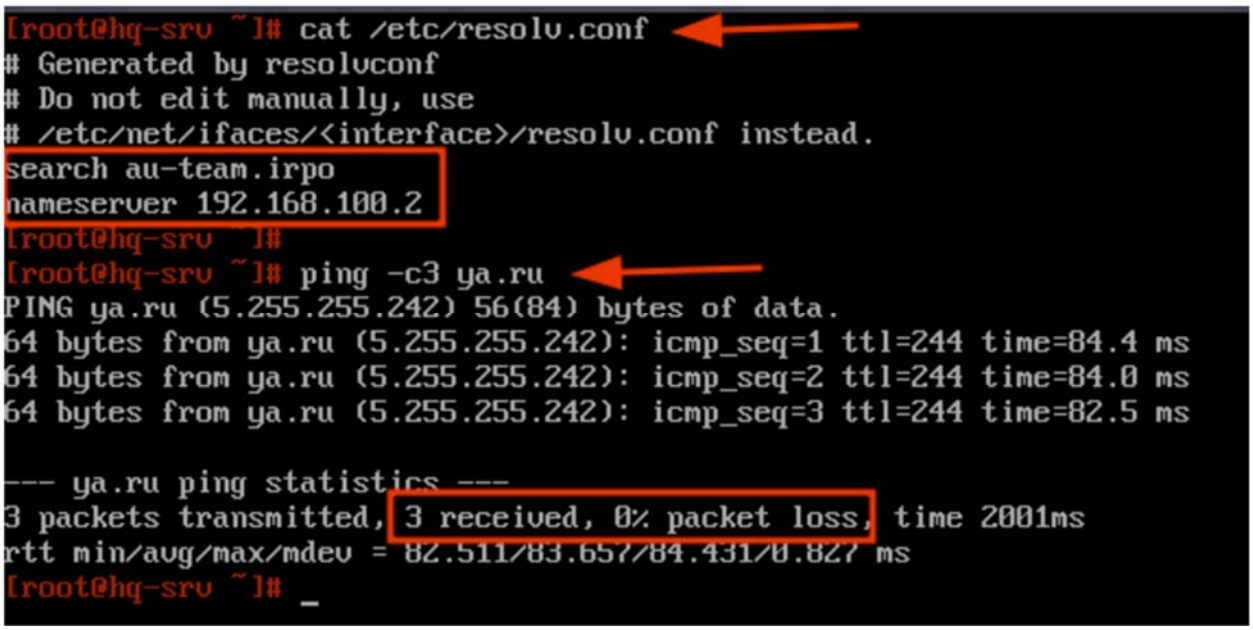
```
systemctl enable --now bind.service
```

- Проверить статус службы:

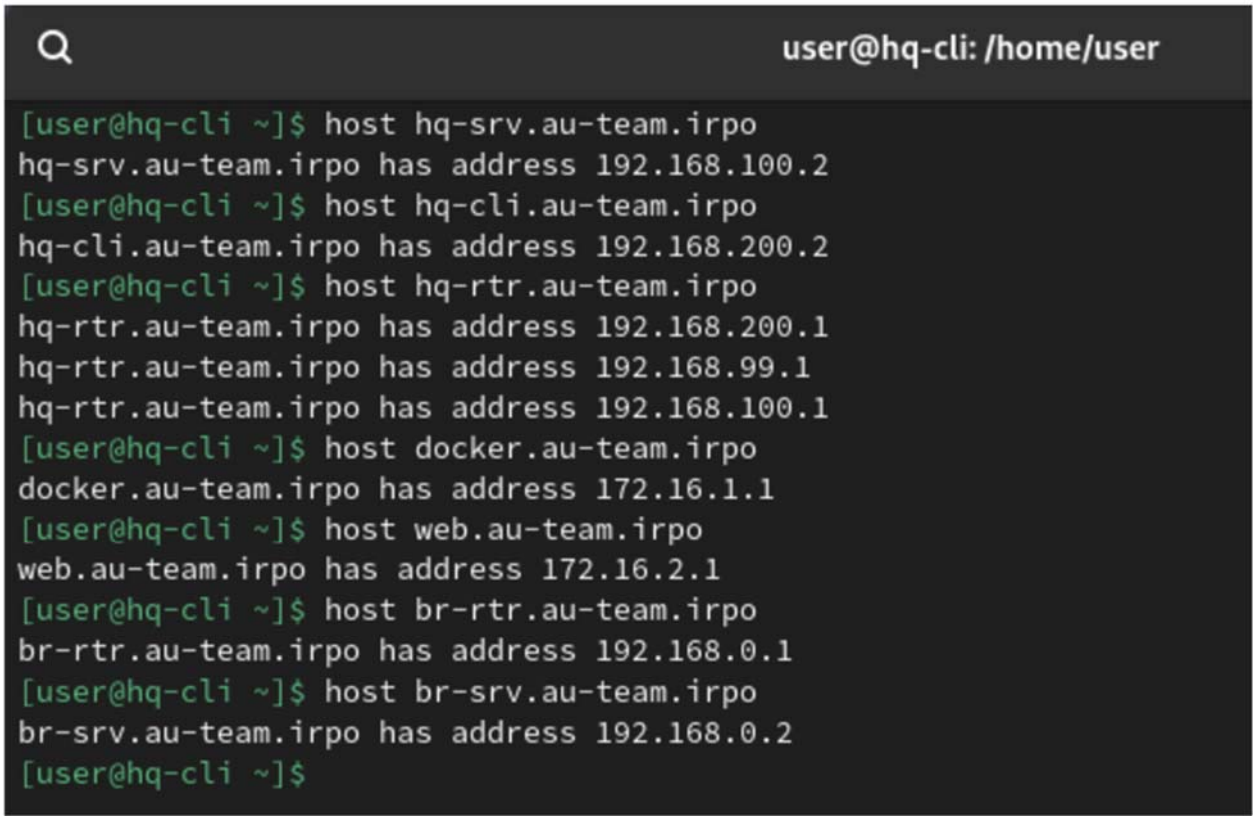
```
systemctl status bind.service
```

-
  - Результат:

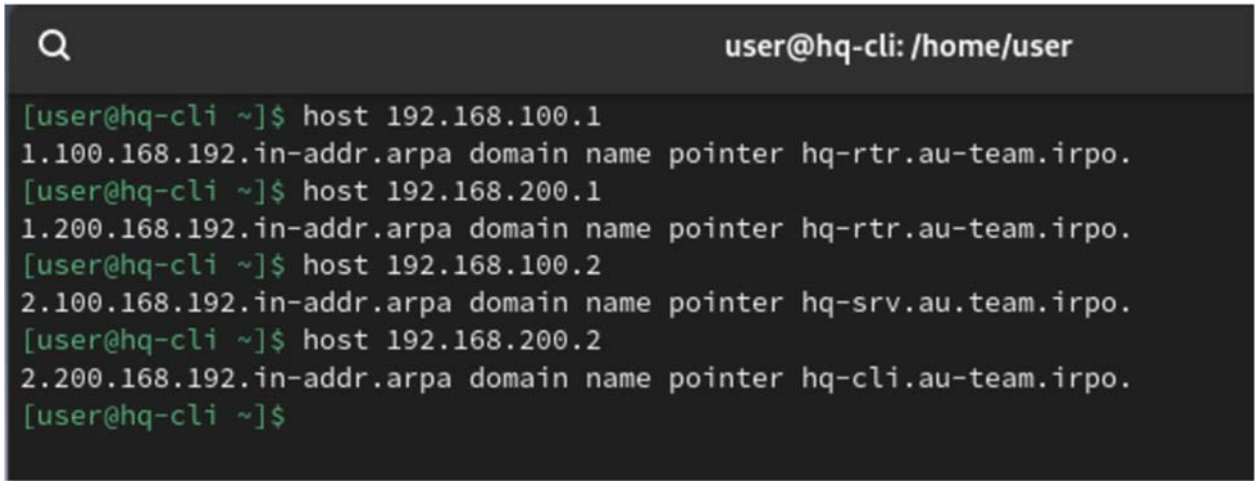




- Используя утилиту **host** или **nslookup** проверить записи типа **A**, **PTR**:
  - Записи типа **A**:



- Записи типа **PTR**:



BR-SRV

```
[root@br-srv etc]# ping -c3 br-rtr
PING br-rtr.au-team.irpo (192.168.0.1) 56(84) bytes of data.
64 bytes from _gateway (192.168.0.1): icmp_seq=1 ttl=64 time=161 ms
64 bytes from _gateway (192.168.0.1): icmp_seq=2 ttl=64 time=257 ms
64 bytes from _gateway (192.168.0.1): icmp_seq=3 ttl=64 time=181 ms

--- br-rtr.au-team.irpo ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 161.016/199.855/257.121/41.341 ms
[root@br-srv etc]# ping -c3 hq-rtr
PING hq-rtr.au-team.irpo (192.168.200.1) 56(84) bytes of data.
64 bytes from hq-rtr.au-team.ipro (192.168.200.1): icmp_seq=1 ttl=63 time=558 ms
64 bytes from hq-rtr.au-team.ipro (192.168.200.1): icmp_seq=2 ttl=63 time=485 ms
64 bytes from hq-rtr.au-team.ipro (192.168.200.1): icmp_seq=3 ttl=63 time=568 ms

--- hq-rtr.au-team.irpo ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2190ms
rtt min/avg/max/mdev = 485.020/536.848/567.583/36.858 ms
[root@br-srv etc]# ping -c3 isp
ping: isp: Name or service not known
[root@br-srv etc]# ping -c3 hq-cli
PING hq-cli.au-team.irpo (192.168.200.2) 56(84) bytes of data.
64 bytes from hq-cli.au-team.irpo (192.168.200.2): icmp_seq=1 ttl=62 time=485 ms
64 bytes from hq-cli.au-team.irpo (192.168.200.2): icmp_seq=2 ttl=62 time=708 ms
64 bytes from hq-cli.au-team.irpo (192.168.200.2): icmp_seq=3 ttl=62 time=336 ms

--- hq-cli.au-team.irpo ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2288ms
rtt min/avg/max/mdev = 336.253/509.832/708.101/152.806 ms
[root@br-srv etc]# ping -c3 hq-srv
PING hq-srv.au-team.irpo (192.168.100.2) 56(84) bytes of data.
64 bytes from hq-srv.au-team.irpo (192.168.100.2): icmp_seq=1 ttl=62 time=317 ms
64 bytes from hq-srv.au-team.irpo (192.168.100.2): icmp_seq=2 ttl=62 time=604 ms
64 bytes from hq-srv.au-team.irpo (192.168.100.2): icmp_seq=3 ttl=62 time=521 ms

--- hq-srv.au-team.irpo ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1999ms
rtt min/avg/max/mdev = 316.620/480.626/604.194/120.833 ms
```

HQ-CLI

HQ-RTR

```
hq-rtr#configure terminal
hq-rtr (config)#ip name-server 192.168.100.2
hq-rtr (config)#ip domain-name au-team.irpo
hq-rtr (config)#write
hq-rtr (config)#
```

```
hq-rtr#ping ya.ru
PING ya.ru (77.88.55.242) 56(84) bytes of data.
64 bytes from ya.ru (77.88.55.242): icmp_seq=1 ttl=55 time=219 ms
64 bytes from ya.ru (77.88.55.242): icmp_seq=2 ttl=55 time=305 ms
64 bytes from ya.ru (77.88.55.242): icmp_seq=3 ttl=55 time=216 ms

--- ya.ru ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2010ms
rtt min/avg/max/mdev = 215.898/246.731/305.327/41.452 ms
hq-rtr#
```

BR-RTR

```
br-rtr#configure terminal
hq-rtr (config)#ip name-server 192.168.100.2
br-rtr (config)#ip domain-name au-team.irpo
br-rtr (config)#write
r-rtr (config)#
```

```
br-rtr#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=197 ms
64 bytes from ya.ru (77.88.44.242): icmp_seq=2 ttl=55 time=204 ms

--- ya.ru ping statistics ---
3 packets transmitted, 2 received, 33.3333% packet loss, time 3066ms
rtt min/avg/max/mdev = 197.135/200.332/203.530/3.197 ms
br-rtr#
```

2.11. Настройте часовой пояс на всех устройствах

Задание:

- Настройте часовой пояс на всех устройствах (за исключением виртуального коммутатора, в случае его использования) согласно месту проведения экзамена

Вариант реализации:

HQ-RTR и BR-RTR:

- Настройте часовой пояс на всех устройствах, согласно месту проведения экзамена:
  - **HQ-RTR:**

```
hq-rtr(config)#ntp timezone utc+3
hq-rtr(config)#write memory
Building configuration...

hq-rtr(config)#
```

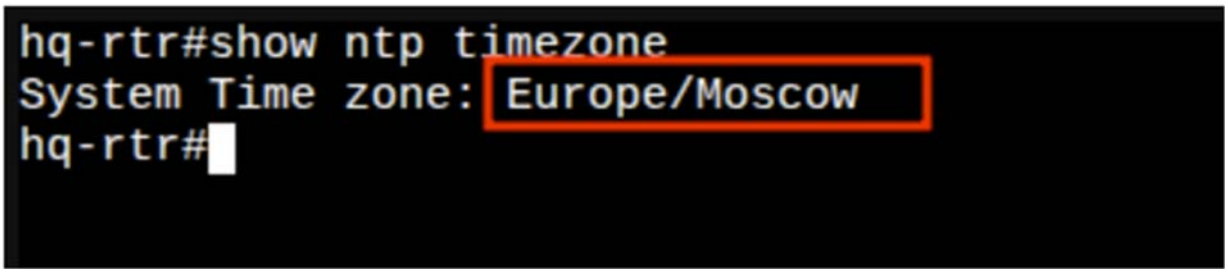
  -
  - **BR-RTR:**

```
br-rtr(config)#ntp timezone utc+3
```

```
br-rtr(config)#write memory

Building configuration...



br-rtr(config)#
```

- Проверить:

```
show ntp timezone
```



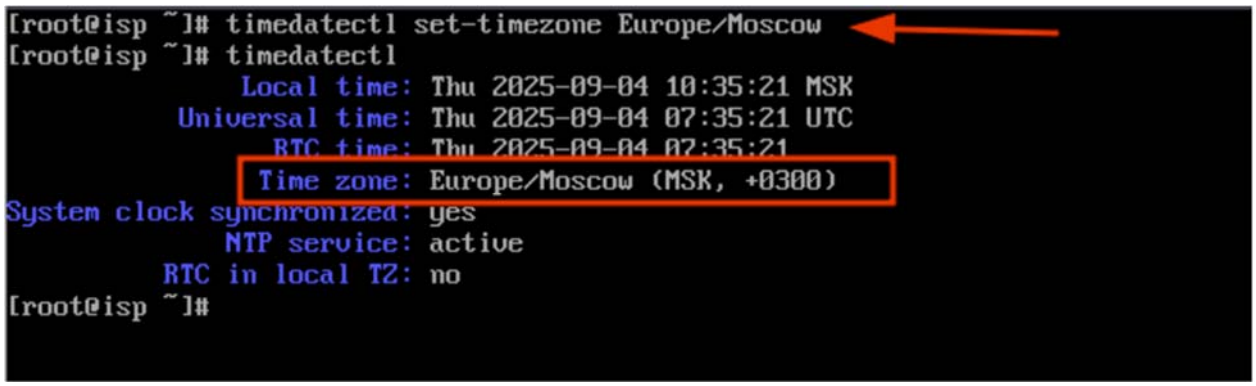
ISP | HQ-SRV | HQ-CLI | BR-SRV:

- Настройте часовой пояс на всех устройствах, согласно месту проведения экзамена:

```
timedatectl set-timezone Europe/Moscow
```

- Проверить:

```
timedatectl
```



3 Модуль 2. Организация сетевого администрирования

3.1. Настройте контроллер домена Samba DC на сервере BR-SRV

Задание:

- Имя домена au-team.irpo
- Введите в созданный домен машину HQ-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 HQ-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:

3.1.1. Настройка AD DS

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
```

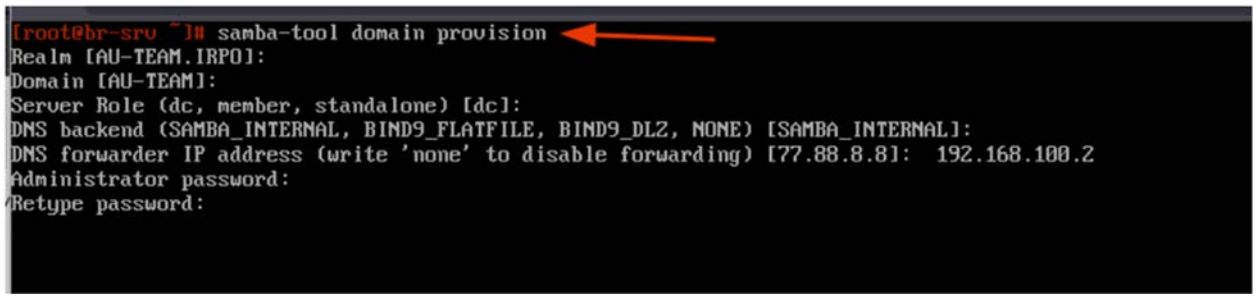
- Так как Samba в режиме контроллера домена (Domain Controller, DC) использует свой сервер LDAP, свой центр распределения ключей Kerberos и свой сервер DNS (если не включен плагин BIND9_DLZ), перед установкой необходимо остановить конфликтующие службы **krb5kdc** и **slapd**, а также **bind**:

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

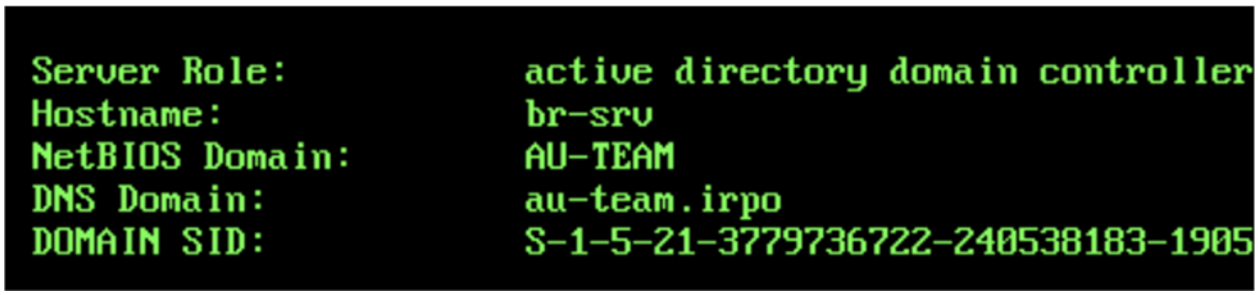
- Восстановление к начальному состоянию Samba:
  - Необходимо очистить базы и конфигурацию Samba (домен, если он создавался до этого, будет удалён):

```
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
```

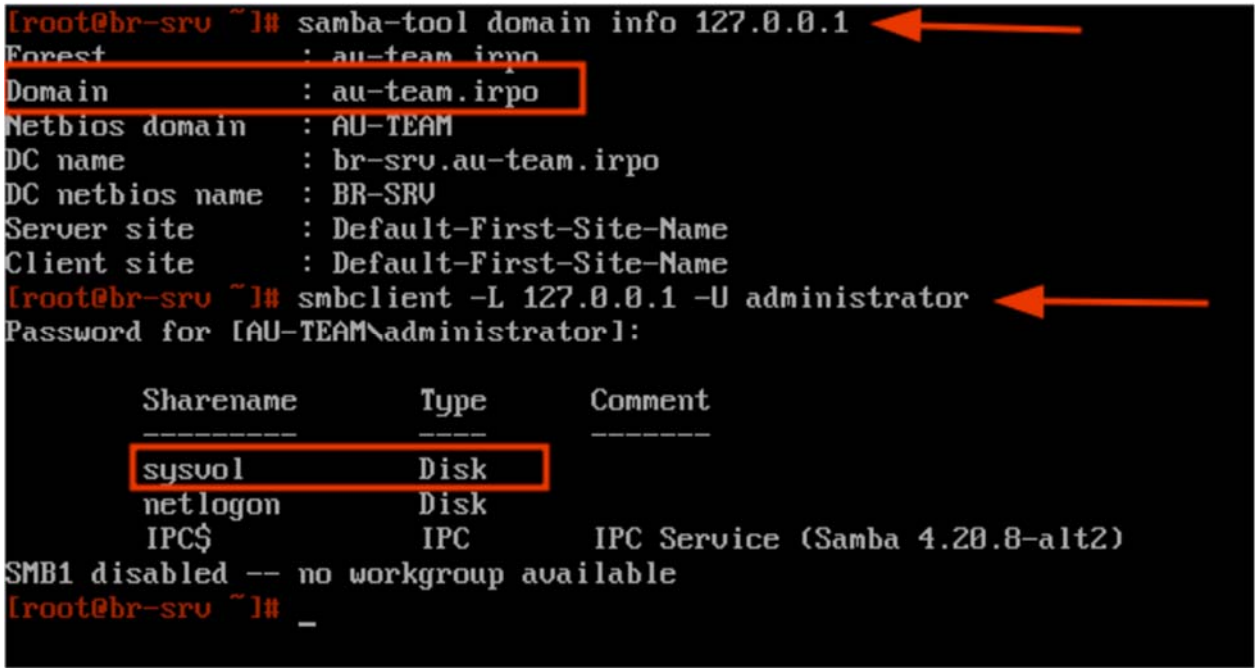
- Настройка Kerberos:

```
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

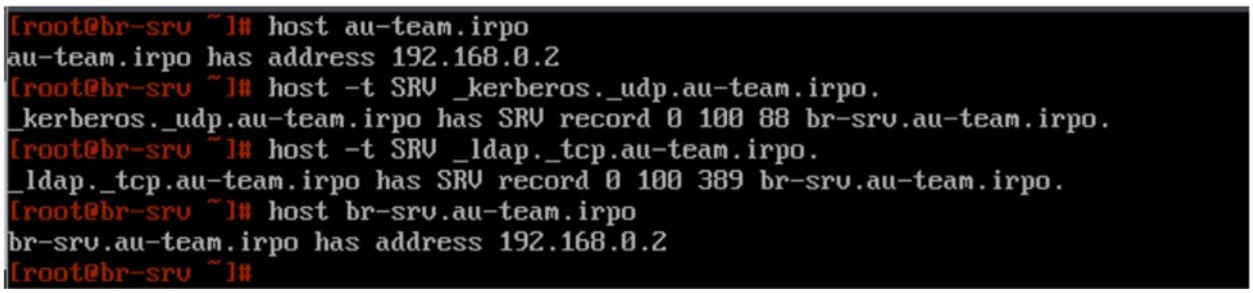


- Проверка конфигурации DNS:
  - Убедиться в наличии **nameserver 127.0.0.1** в **/etc/resolv.conf**:

```
echo "search au-team.irpo" > /etc/net/ifaces/ens19/resolv.conf

echo "nameserver 127.0.0.1" >> /etc/net/ifaces/ens19/resolv.conf

systemctl restart network
```

  -
  - Утилита **host** в пакете **bind-utils**

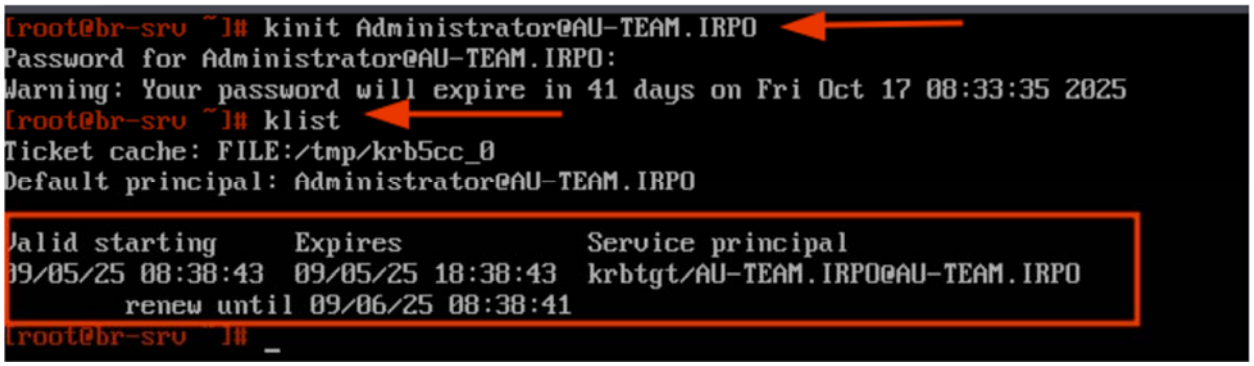
- Проверить имена хостов:



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

```
kinit administrator@AU-TEAM.IRPO
```

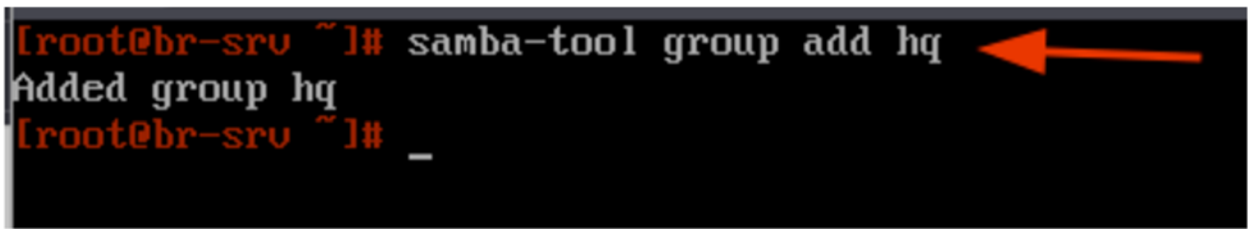
Просмотр полученного билета:



3.1.2 Создаём группу hq:

```
samba-tool group add hq
```

- Результат:

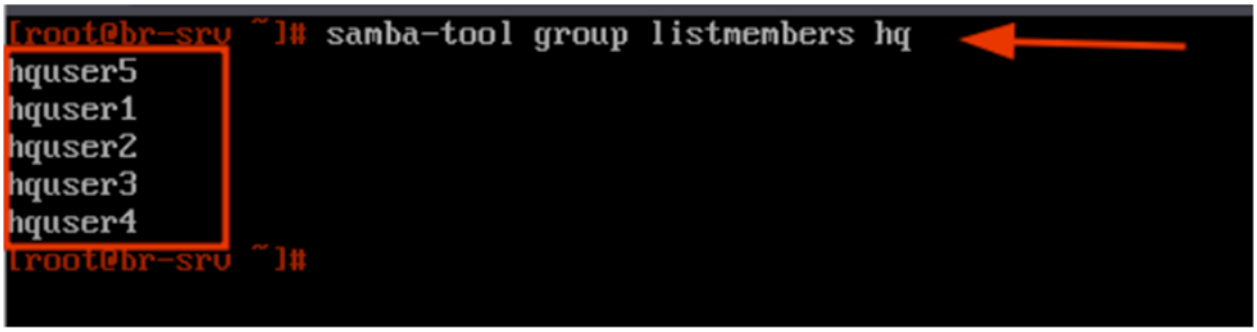


- Создаём необходимых пользователей и добавляем их в группу **hq**:

```
for i in {1..5};

do
```

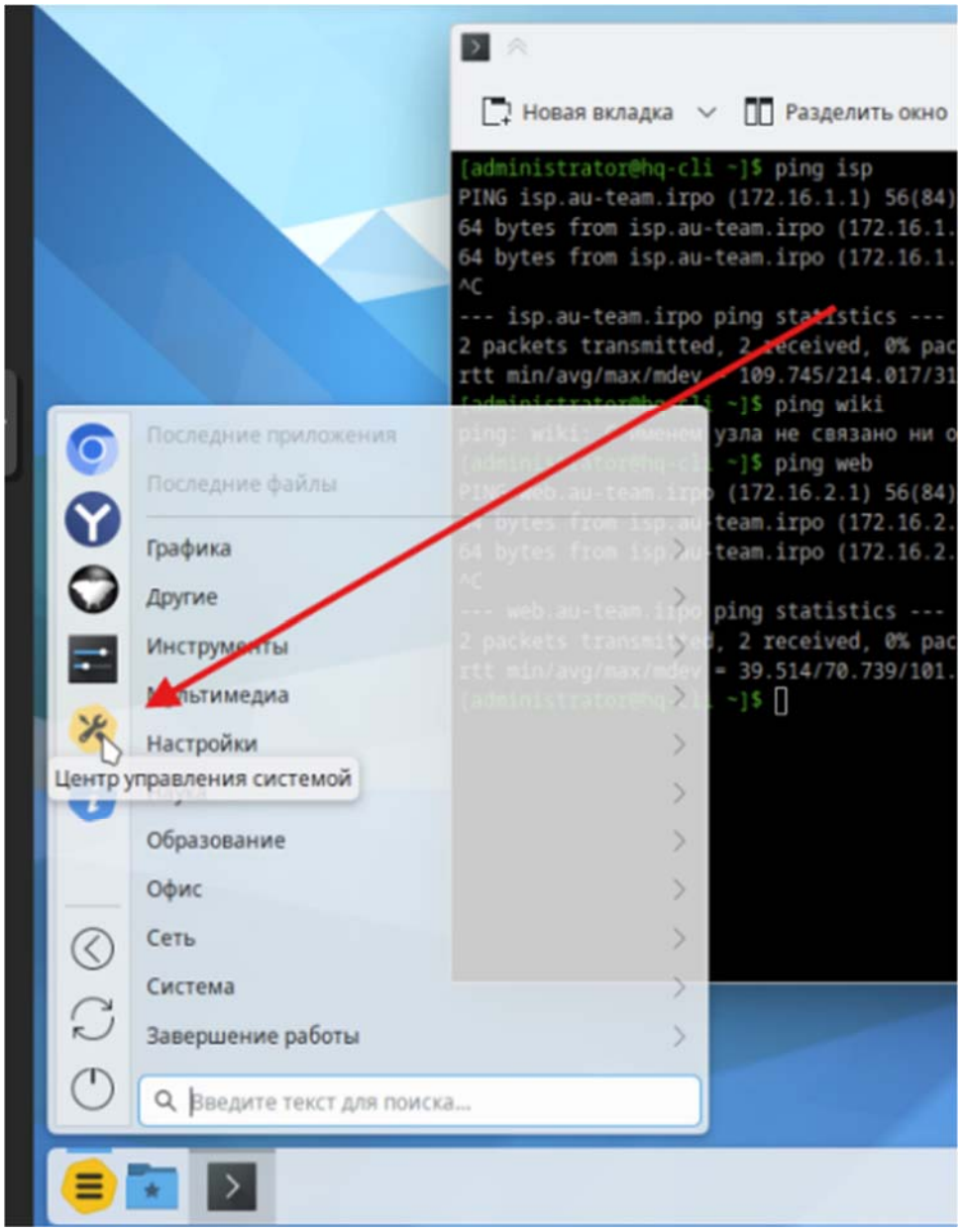
```
  samba-tool user add hquser$i P@ssw0rd;
  samba-tool user setexpiry hquser$i --noexpiry;
  samba-tool group addmembers "hq" hquser$i;
done
```

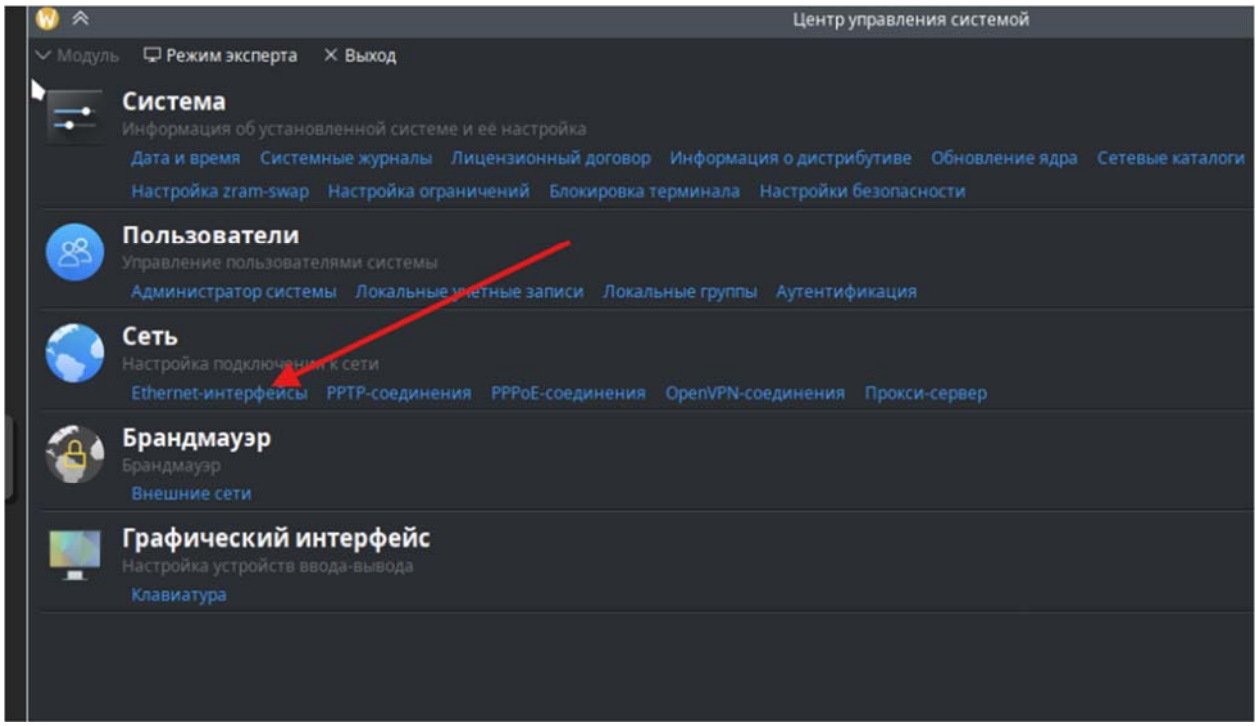
Проверить:

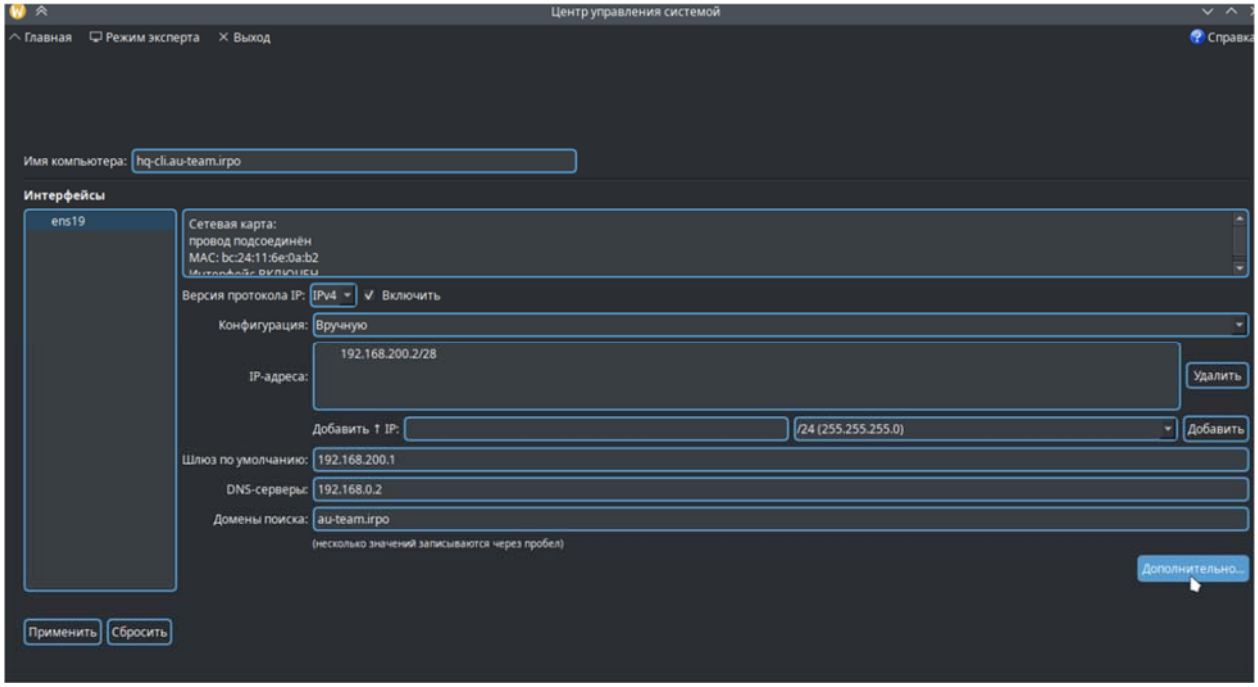


3.1.3 Подключение HQ-CLI к контроллеру домена

- Для того чтобы ввести HQ-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:





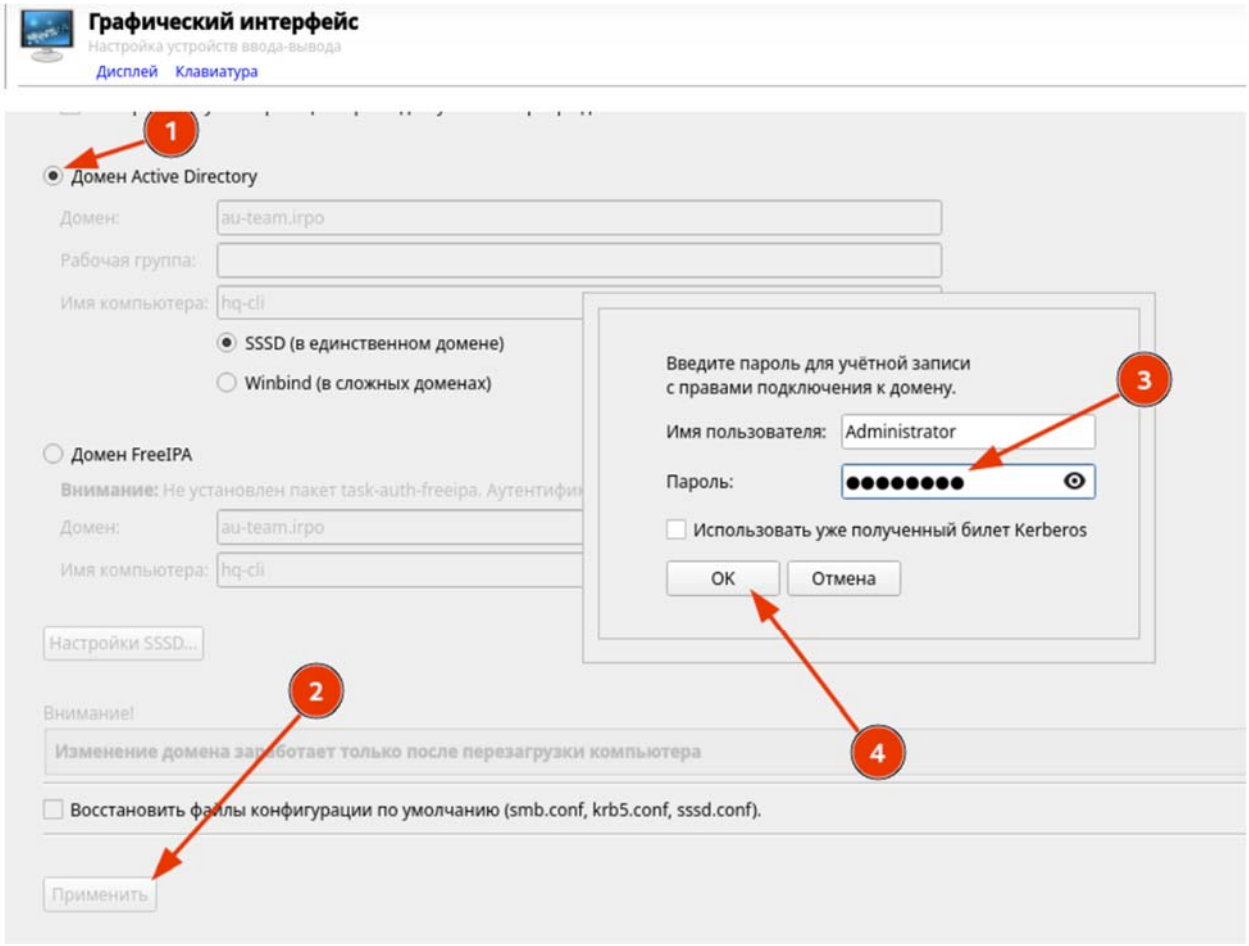


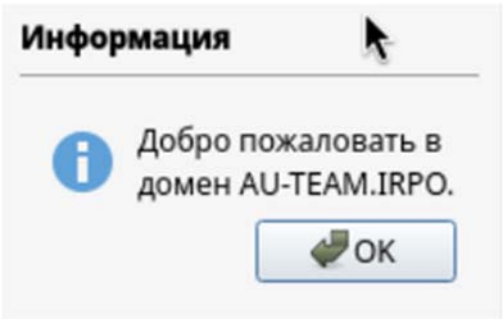
- Проверить что доменное имя резольвится:

- Установить пакет **task-auth-ad-winbind (task-auth-ad-sssd)**:

```
apt-get update && apt-get install -y task-auth-ad-winbind
```

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

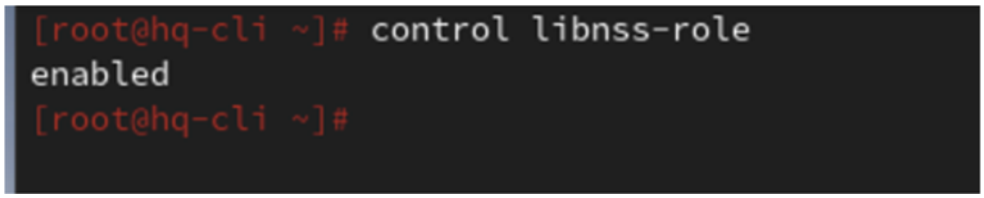




- Установим библиотеку **libnss-role** для NSS и набор инструментов для администрирования ролей и привилегий:

```
apt-get install -y libnss-role
```

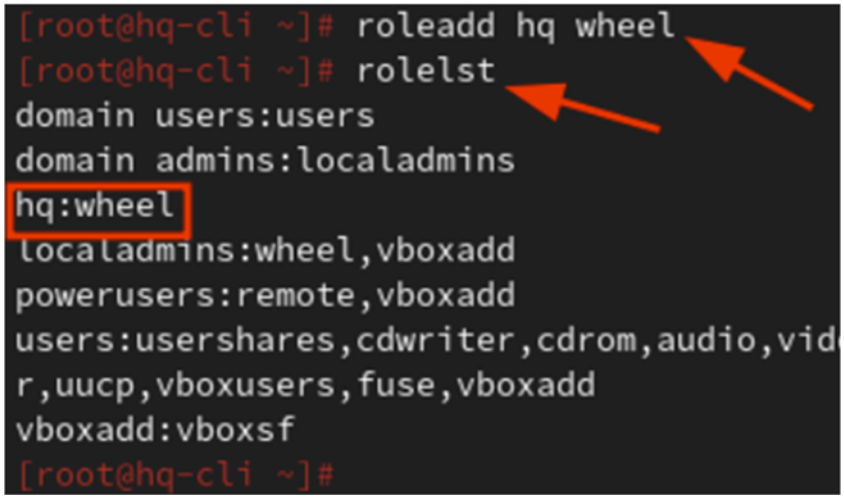
- Данный модуль должен быть включён:



- Связываем доменную группу **hq** с локальной группой **wheel**:

```
roleadd hq wheel
```

    - Проверить:



- Редактируем конфигурационный файл **/etc/sudoers**: (apt-get install sudo)

```
vim /etc/sudoers
```

    - добавляем следующее содержимое:

```
##
## Cmnd alias specification
##
## Groups of commands.  Often used to group related commands together.
# Cmnd_Alias    PROCESSES = /usr/bin/nice, /bin/kill, /usr/bin/renice, \
#                           /usr/bin/pkill, /usr/bin/top
Cmnd_Alias      SHELLCMD = /bin/cat, /bin/grep, /usr/bin/id
#
# Cmnd_Alias    REBOOT = /sbin/halt, /sbin/reboot, /sbin/poweroff
#
```

```
## User privilege specification
##
# root ALL=(ALL:ALL) ALL

## Uncomment to allow members of group wheel to execute any command
# WHEEL_USERS ALL=(ALL:ALL) ALL
WHEEL_USERS ALL=(ALL:ALL) SHELLCMD

## Same thing without a password
# WHEEL_USERS ALL=(ALL:ALL) NOPASSWD: ALL
```

- Проверяем, выполнив вход из под любого пользователя группы **hq**:
- проверяем **sudo** для необходимых команд:

```
hquser3@hq-cli: /home/AU-TEAM.IRPO/hquser3
[hquser3@hq-cli ~]$ sudo id
uid=0(root) gid=0(root) группы=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),19(proc)
[hquser3@hq-cli ~]$ sudo cat /etc/hosts
127.0.0.1       localhost.localdomain localhost
::1     localhost6.localdomain localhost6
[hquser3@hq-cli ~]$ sudo grep '127.0.0.1' /etc/hosts
127.0.0.1       localhost.localdomain localhost
[hquser3@hq-cli ~]$
```

- проверяем **sudo** для других команд:

```
[hquser3@hq-cli ~]$ sudo su -
Извините, пользователю hquser3 не разрешено выполнять «/bin/su -» как root на hq-cli.au-team.irpo.
[hquser3@hq-cli ~]$
```

3.2. Сконфигурируйте файловое хранилище на сервере HQ-SRV

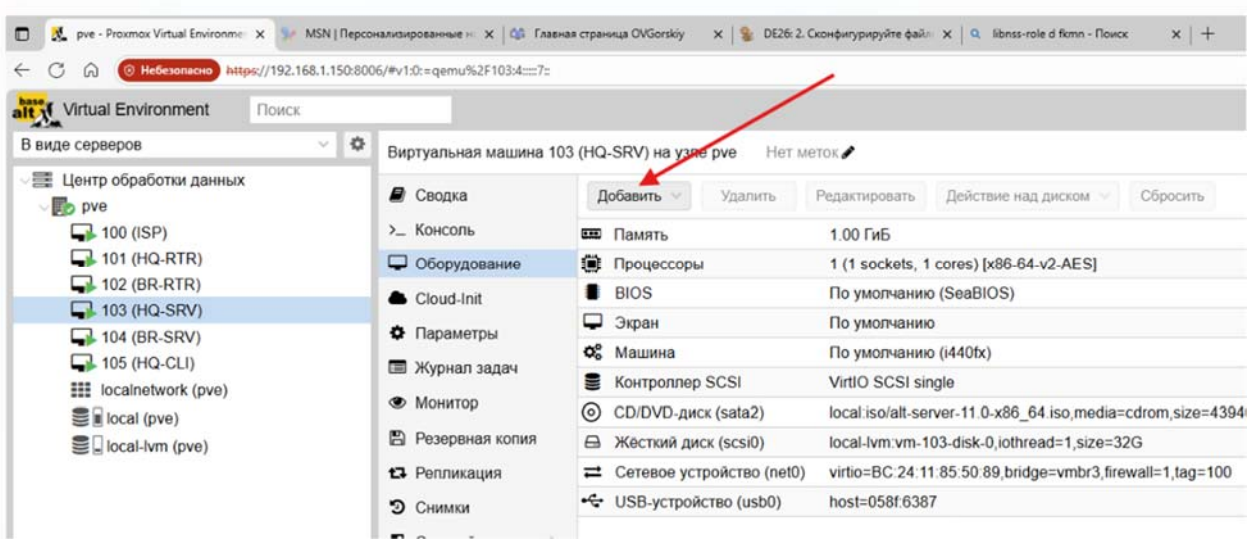
Задание:

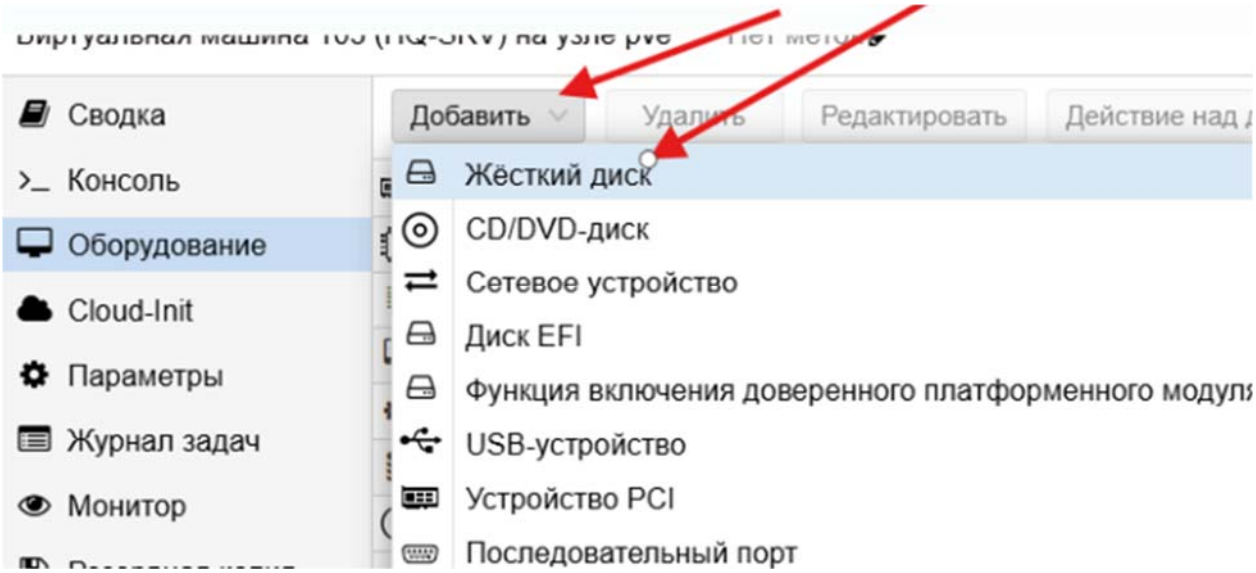
- При помощи двух подключенных к серверу дополнительных дисков размером 1 Гб сконфигурируйте дисковый массив уровня 0
- Имя устройства – md0, при необходимости конфигурация массива размещается в файле /etc/mdadm.conf
- Создайте раздел, отформатируйте раздел, в качестве файловой системы используйте ext4
- Обеспечьте автоматическое монтирование в папку /raid

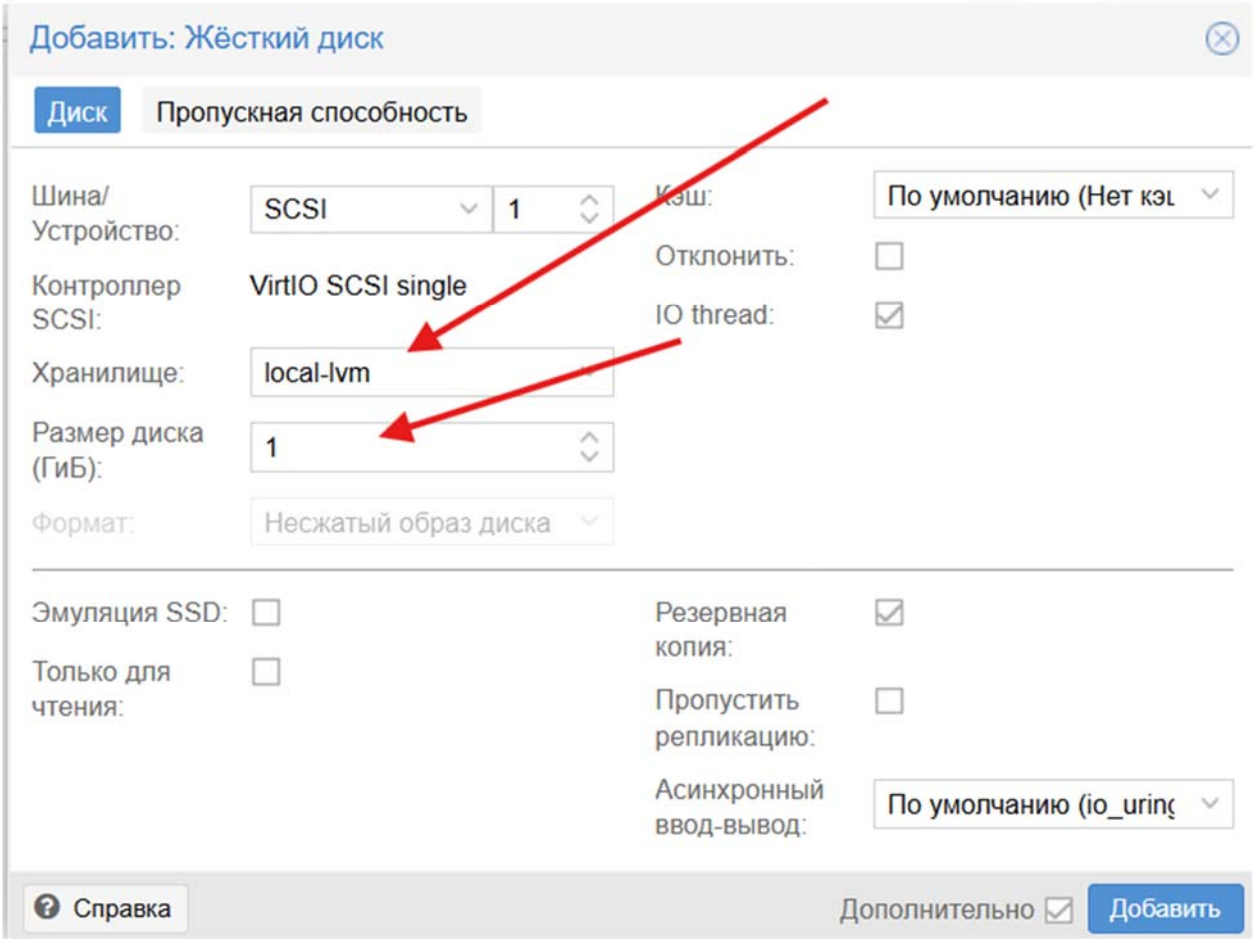
Вариант реализации:

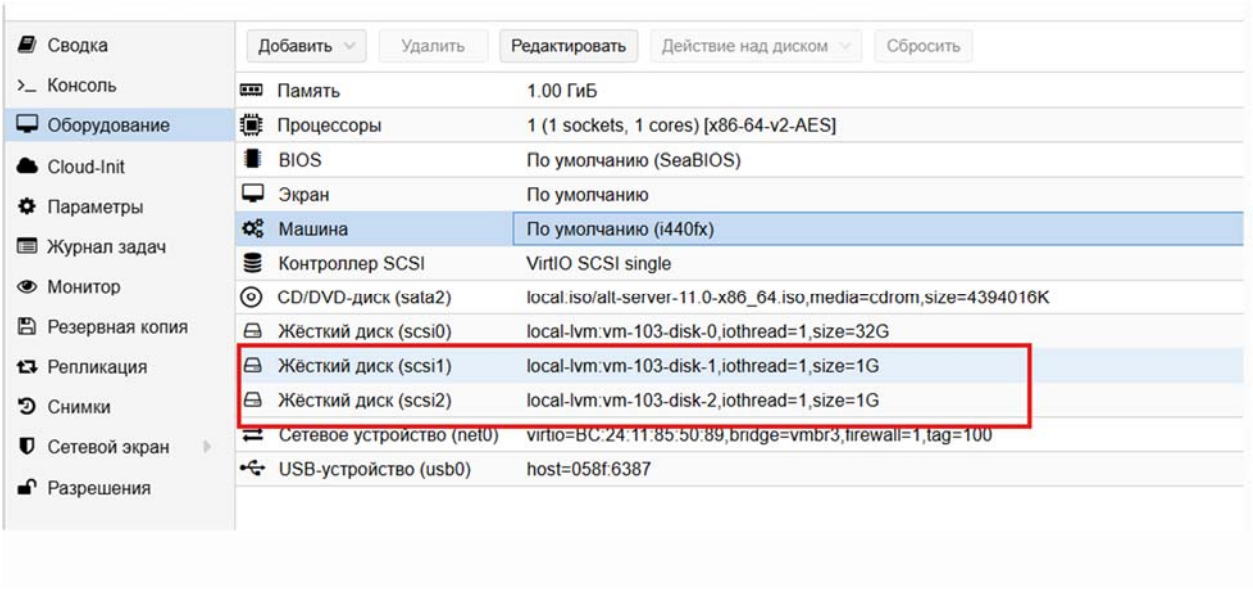
HQ-SRV:

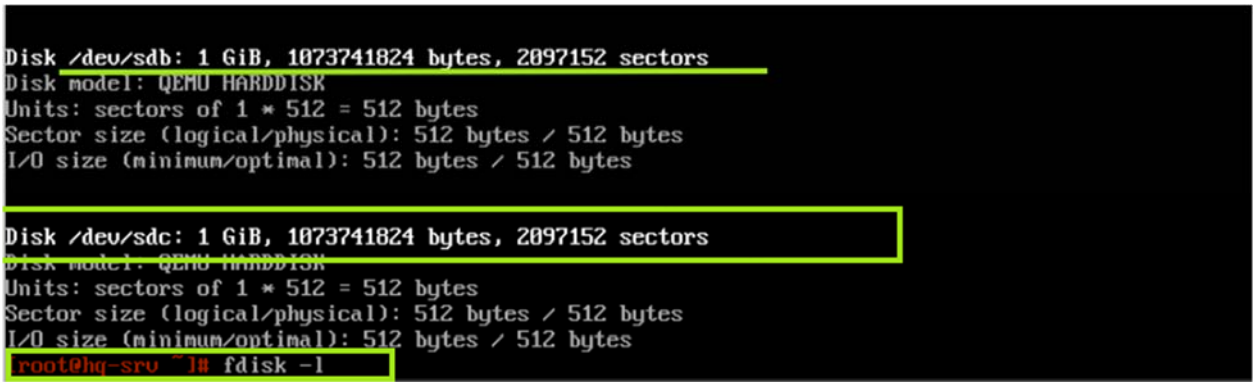
Создаем 2 диска




Сводка
Консоль
Оборудование
Cloud-Init
Параметры
Журнал задач
Монитор
Добавить
Удалить
Редактировать
Жёсткий диск
CD/DVD-диск
Сетевое устройство
Диск EFI
Функция включения доверенного платформенного модуля
USB-устройство
Устройство PCI
Последовательный порт


Добавить: Жёсткий диск
Диск
Пропускная способность
Шина/ Устройство:
SCSI
1
Контроллер SCSI:
VirtIO SCSI single
Хранилище:
local-lvm
Размер диска (ГиБ):
1
Формат:
Несжатый образ диска
Кэш:
По умолчанию (Нет кэ
Отклонить:
IO thread:
Эмуляция SSD:
Только для чтения:
Резервная копия:
Пропустить репликацию:
Асинхронный ввод-вывод:
По умолчанию (io_uring
Справка
Дополнительно
Добавить





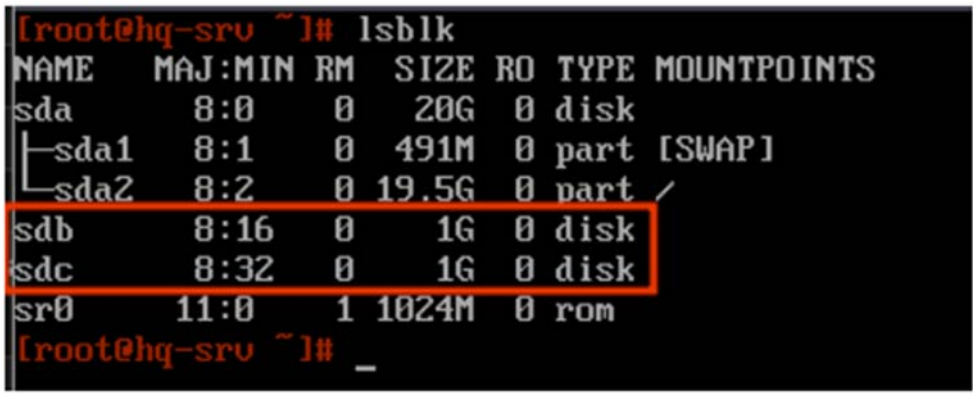
- Выполним установку пакета "mdadm":
  - mdadm — утилита для работы с программными RAID-массивами различных уровней

```
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 физические диски и определяемся какие будут использоваться в RAID - массиве

```
lsblk
```

- Результат:
  - для работы будут использованы диски: **sdb**, **sdc**

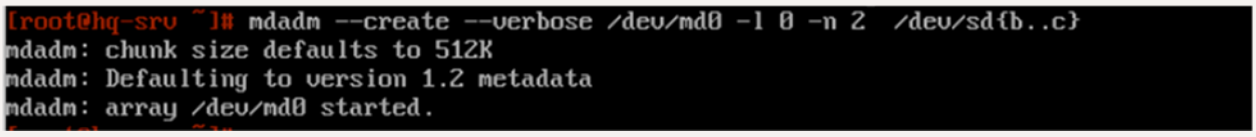


- Зануление суперблоков на дисках, которые будут использоваться для построения RAID-массива:

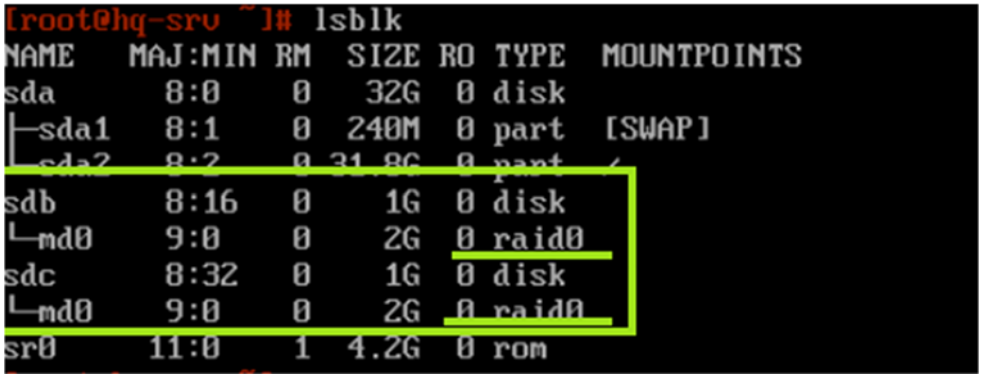
```
mdadm --zero-superblock --force /dev/sdb /dev/sdc
```

- Создание RAID-массива:
  - где:
    - **/dev/md0** — устройство RAID, которое появится после сборки;
    - **-l 0** — уровень RAID;
    - **-n 2** — количество дисков, из которых собирается массив;
    - **/dev/sd{b,c}** — сборка выполняется из дисков sdb, sdc и sdd.

```
mdadm --create --verbose /dev/md0 -l 0 -n 2 /dev/sdb /dev/sdc
```



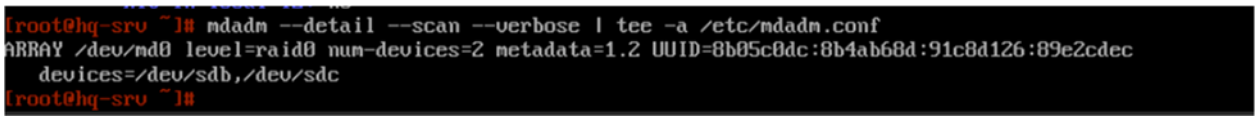
  - Результат:



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

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

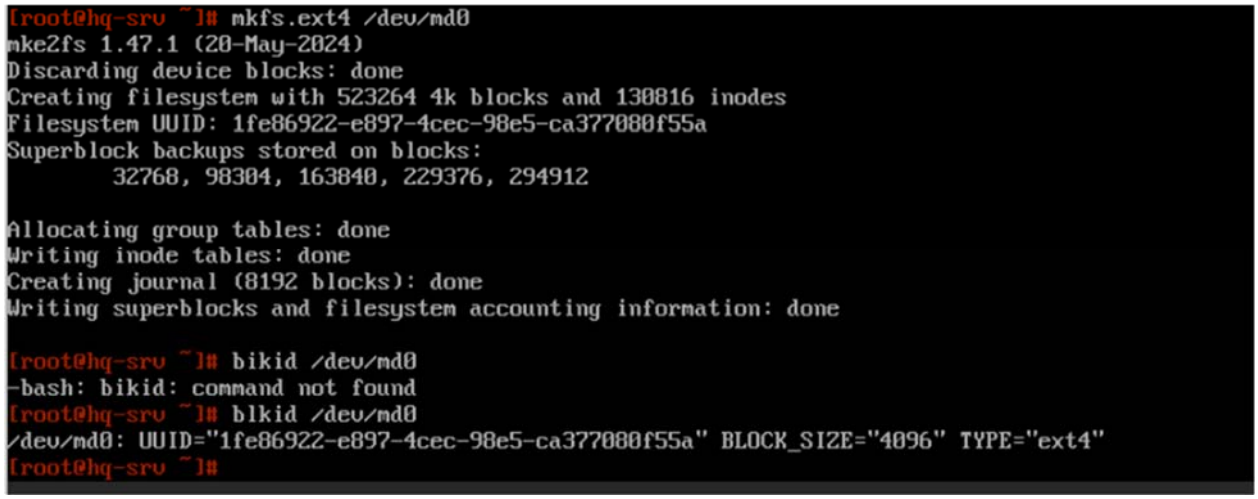
  - Результат:



- Создание файловой системы для массива

```
mkfs.ext4 /dev/md0
```

  - Результат:



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

```
vim /etc/fstab
```

  - следующую информацию:

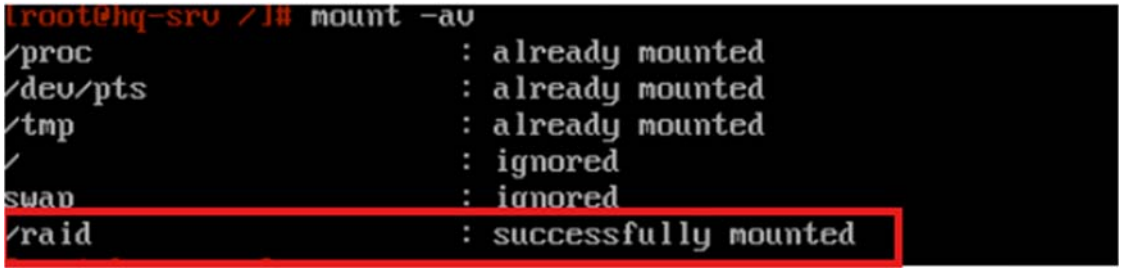
- Создаём каталог **/raid**:

```
mkdir /raid
```

- Выполняем монтирование:

```
mount -av
```

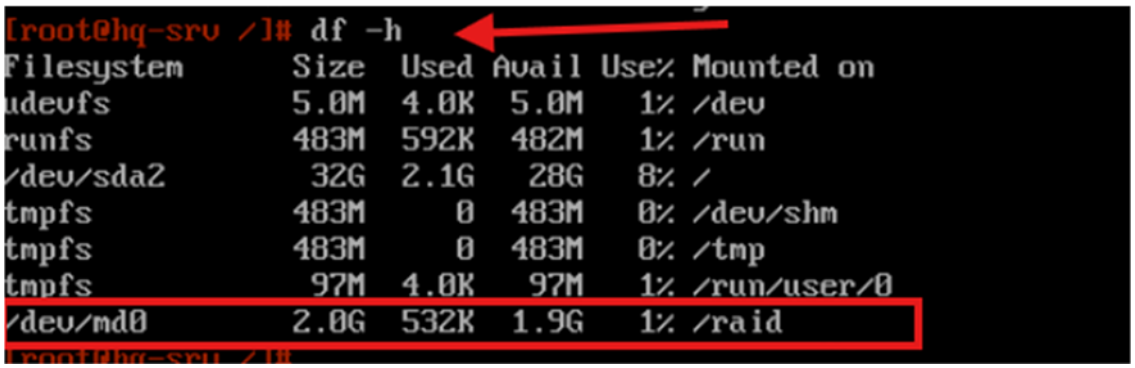
  - Результат:



- Проверяем:

```
df -h
```

  - Результат:

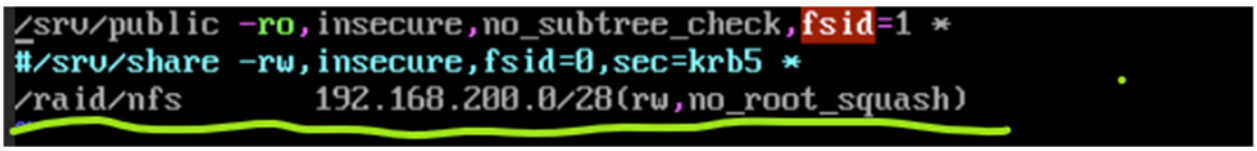


3.3. Настройте сервер сетевой файловой системы (nfs) на HQ-SRV

Задание:

- В качестве папки общего доступа выберите /raid/nfs, доступ для чтения и записи исключительно для сети в сторону HQ-CLI
- На HQ-CLI настройте автомонтирование в папку /mnt/nfs
- Основные параметры сервера отметьте в отчёте

Вариант реализации:

- HQ-SRV:
- Устанавливаем пакеты для NFS сервера:
- apt-get install -y nfs-server nfs-utils
- Создаём директорию для общего доступа /raid/nfs, куда ранее был смонтирован RAID - массив:
- mkdir /raid/nfs
- Назначаем права на созданную директорию (полный доступ):
- chmod 777 /raid/nfs
- Редактируем файл /etc/exports:
- vim /etc/exports
- Добавляем туда следующую информацию, где:
- /raid/nfs - общий ресурс
- 192.168.200.0/24 - 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
- a флаг -v включает подробный вывод:

```
[root@hq-srv ~]# exportfs -arv
exporting 192.168.200.0/24:/raid/nfs
exporting *:/srv/public
[root@hq-srv ~]#
```

-
-
- Запускаем и добавляем в автозагрузку NFS - сервер:
- systemctl enable --now nfs-server

HQ-CLI:

- Выполняем установку пакетов для NFS - клиента:

```
apt-get update && apt-get install -y nfs-utils nfs-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
```

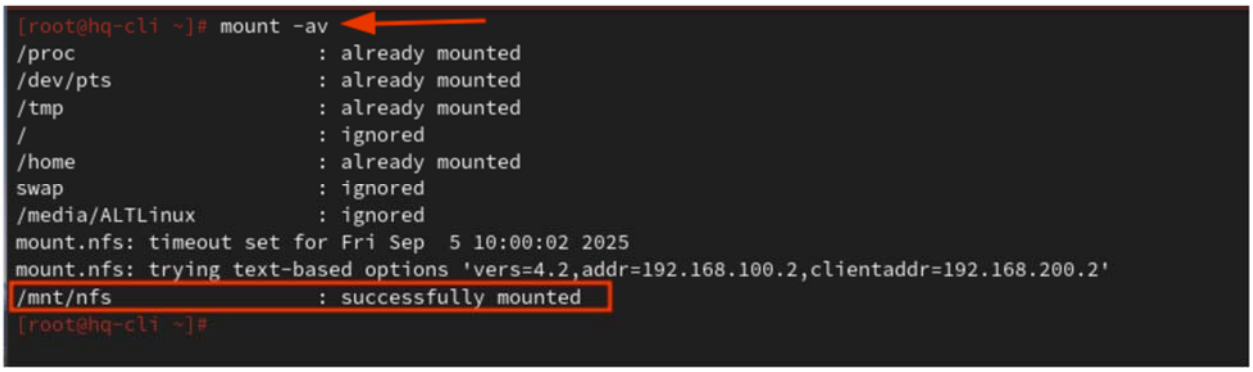
    - Добавляем следующую информацию:
        - где: **192.168.100.2** - адрес файлового сервера (**HQ-SRV**)

```
proc            /proc                   proc    nosuid,noexec,gid=proc                          0 0
devpts          /dev/pts                devpts  nosuid,noexec,gid=tty,mode=620,ptmxmode=0666    0 0
tmpfs           /tmp                    tmpfs   nosuid                                          0 0
UUID=265ae1fb-a7b0-4fbf-aa24-58c14cad9ad4       /       btrfs   relatime,subvol=/@      0       2
UUID=265ae1fb-a7b0-4fbf-aa24-58c14cad9ad4       /home   btrfs   nosuid,relatime,subvol=/@home   0
  2
UUID=66adcaab-b235-46f7-a549-f12ec370f957       swap    swap    defaults        0       0
/dev/sr0        /media/ALTLinux udf,iso9660     ro,noauto,user,utf8,nofail,comment=x-gvfs-show  0 0
192.168.100.2:/raid/nfs /mnt/nfs        nfs     defaults        0       0
~
```

- Выполняем монтирование общего ресурса:

```
mount -av
```

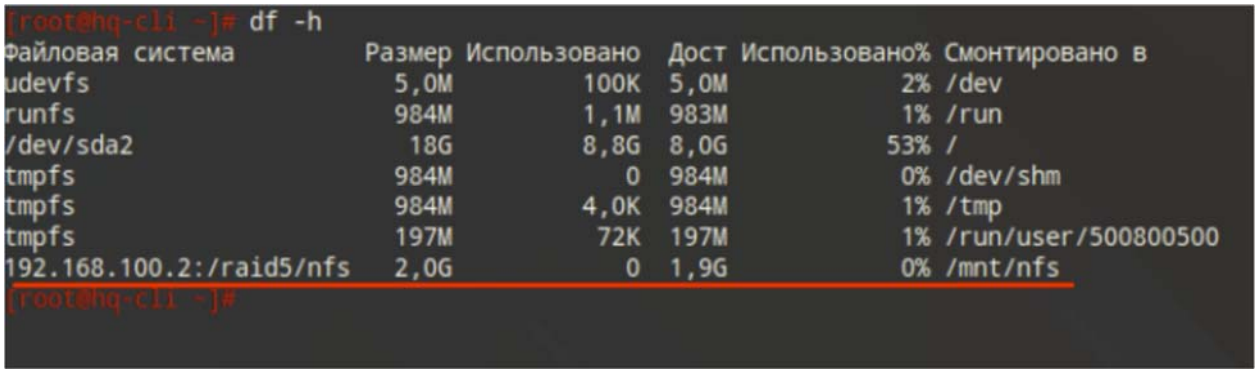
Результат:



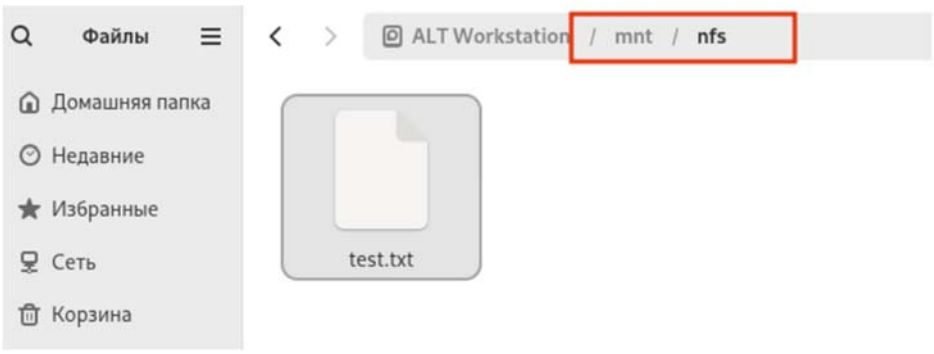
- Проверяем:

```
df -h
```

  - Результат:



- Перезугружаем **HQ-CLI** и проверяем автомонтирование с правами на запись:



- Результат на сервере HQ-SRV:

```
[root@hq-srv ~]# ls -l /raid/nfs/
total 0
-rw-r--r-- 1 user user 0 Sep  5 09:58 test.txt
[root@hq-srv ~]# _
```

`3.4. Настройте службу сетевого времени на базе сервиса chrony на маршрутизаторе ISP

Задание:

- Вышестоящий сервер ntp на маршрутизаторе ISP - на выбор участника
- Стратум сервера - 5
- В качестве клиентов ntp настройте: HQ-SRV, HQ-CLI, BR-RTR, BR-SRV.

Вариант реализации:

ISP:

- Редактируем конфигурационный файл **/etc/chrony.conf**:

```
vim /etc/chrony.conf
```

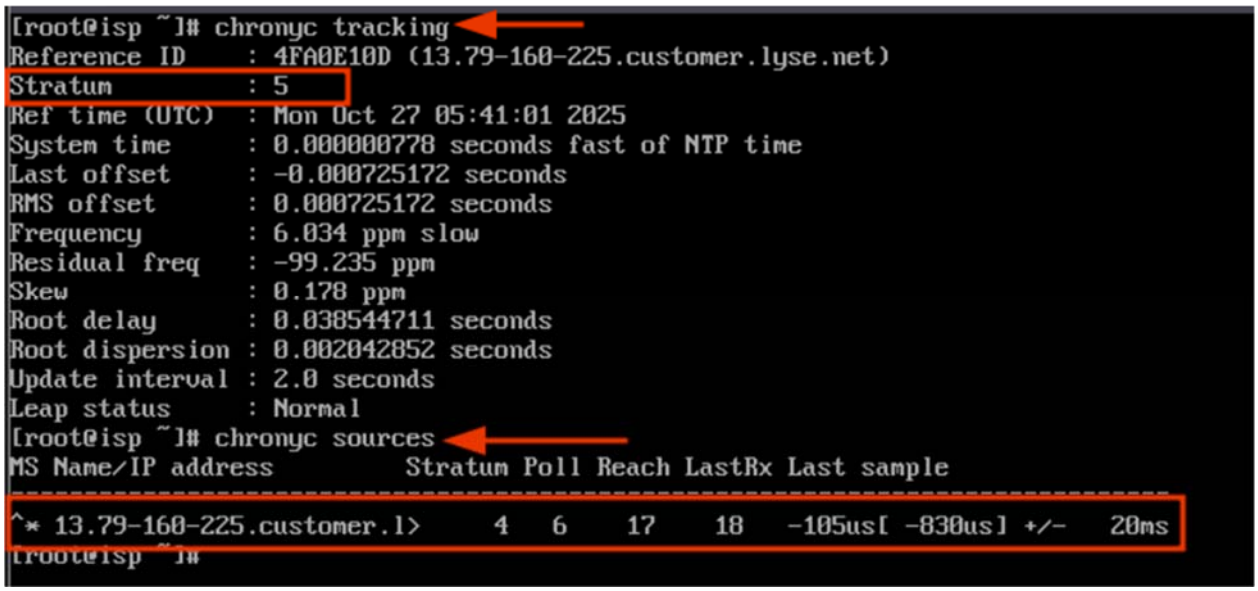
  - Добавляем следующую информацию:

```
# Use public servers from the pool.ntp.org project.
# Please consider joining the pool (https://www.pool.ntp.org/join.html).
#pool pool.ntp.org iburst
server ntp0.ntp-servers.net iburst prefer minstratum 4
local stratum 5
allow 0.0.0.0/0
```

- Перезагружаем службу **chronyd** для применения изменений:

```
systemctl restart chronyd
```

- Проверяем:



HQ-RTR:

- Указываем в качестве сервера времени **ISP**:

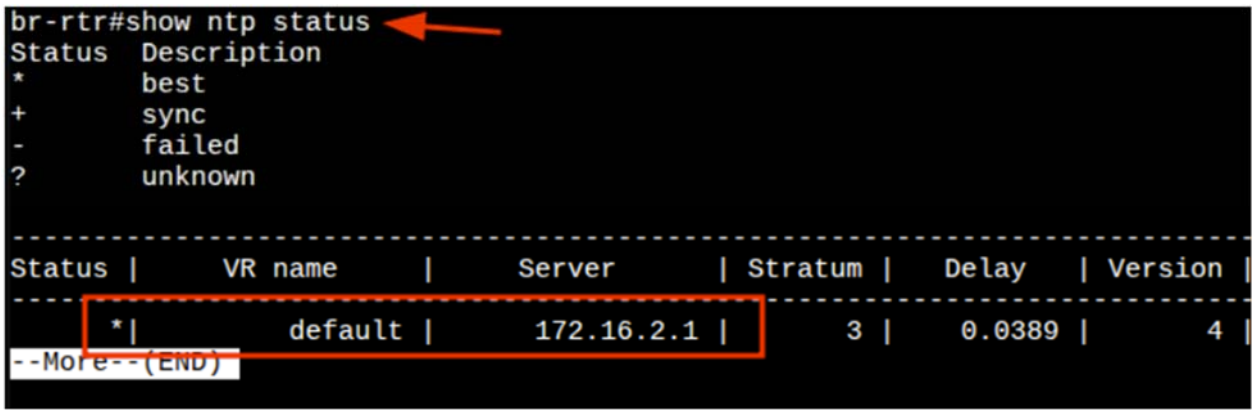
```
hq-rtr(config)#ntp server 172.16.1.1

hq-rtr(config)#write memory

Building configuration...


hq-rtr(config)#
```

BR-RTR:

- Указываем в качестве сервера времени **ISP**:

```
br-rtr(config)#ntp server 172.16.2.1

br-rtr(config)#write memory

Building configuration...


br-rtr(config)#
```

- Проверить:



HQ-CLI и HQ-SRV:

- Редактируем конфигурационный файл **/etc/chrony.conf**:

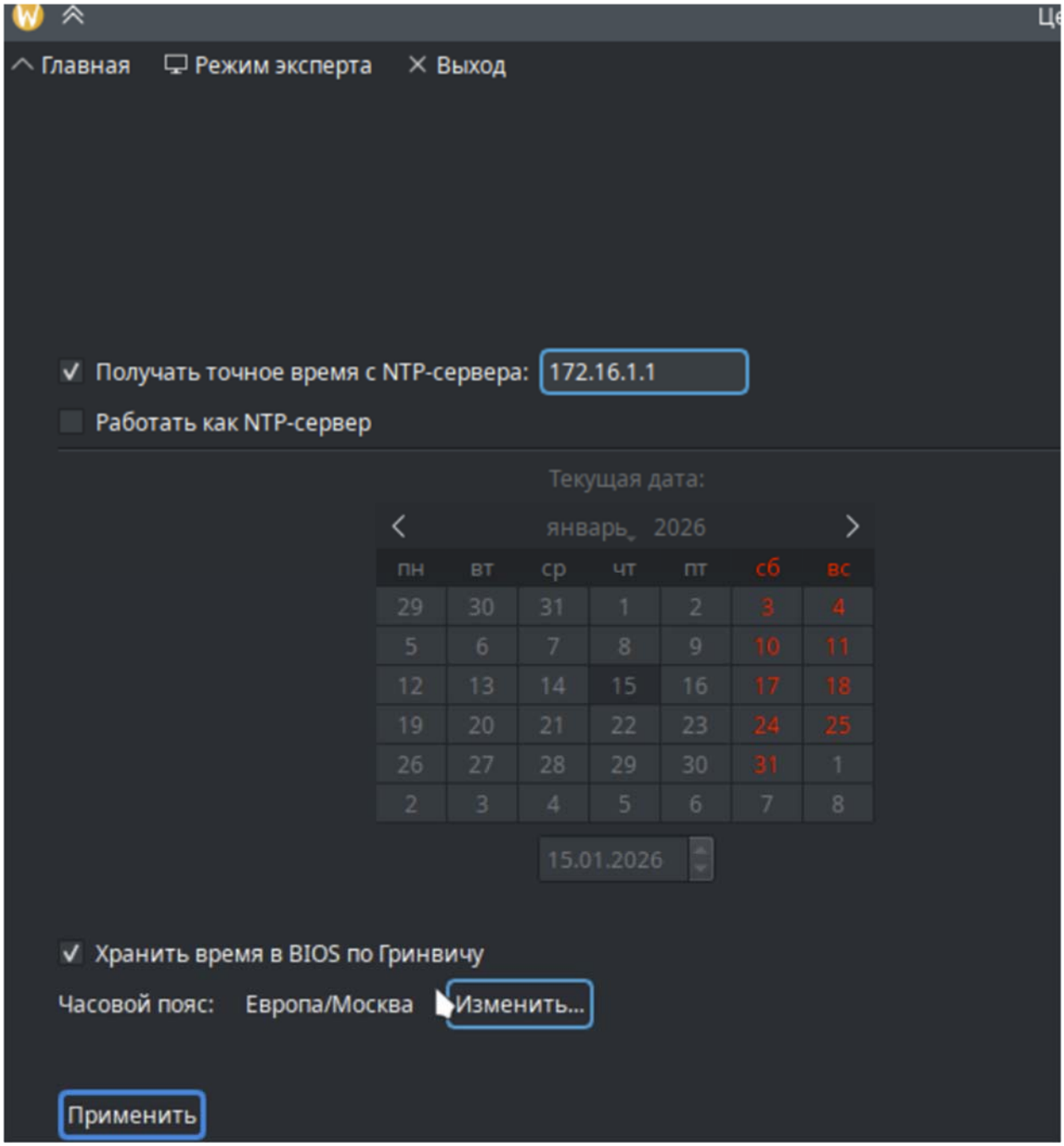
```
vim /etc/chrony.conf
```

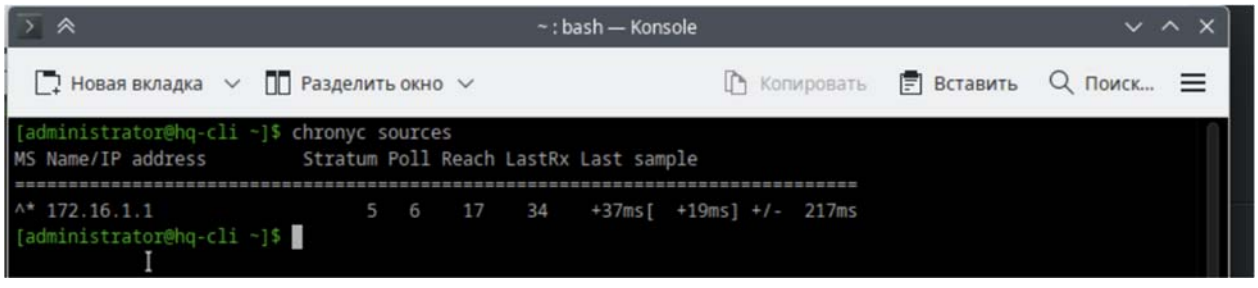
  -
  - Добавляем следующую информацию:

- Перезагружаем службу **chronyd** для применения изменений:

```
systemctl restart chronyd
```

- Проверяем:
  - **HQ-CLI:**

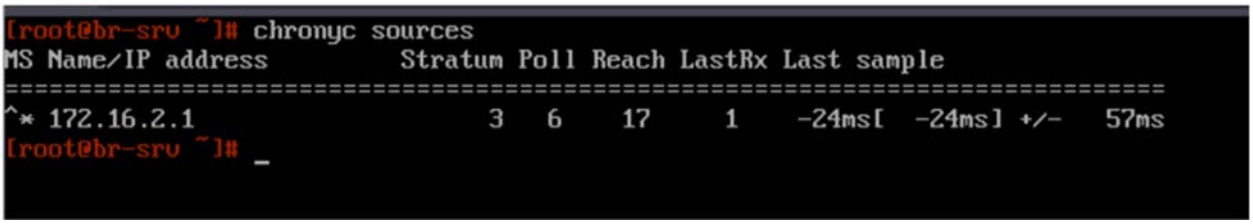

Главная
Режим эксперта
Выход
Получать точное время с NTP-сервера:
172.16.1.1
Работать как NTP-сервер
Текущая дата:
январь 2026
пн вт ср чт пт сб вс
29 30 31 1 2 3 4
5 6 7 8 9 10 11
12 13 14 15 16 17 18
19 20 21 22 23 24 25
26 27 28 29 30 31 1
2 3 4 5 6 7 8
15.01.2026
Хранить время в BIOS по Гринвичу
Часовой пояс: Европа/Москва
Изменить...
Применить


~ : bash — Konsole
Новая вкладка
Разделить окно
Копировать
Вставить
Поиск...
[administrator@hq-cli ~]$ chronyc sources
MS Name/IP address Stratum Poll Reach LastRx Last sample
^* 172.16.1.1 5 6 17 34 +37ms[+19ms] +/- 217ms
[administrator@hq-cli ~]$

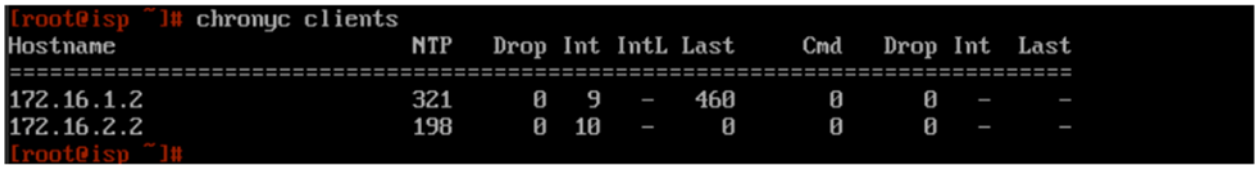
- **HQ-SRV:**

BR-SRV:

- Аналогично HQ-SRV:
- Проверяем:



ISP



3.5. Сконфигурируйте ansible на сервере BR-SRV

Требуемые условия завершения

Задание:

- Сформируйте файл инвентаря, в инвентарь должны входить HQ-SRV, HQ-CLI, HQ-RTR и BR-RTR
- Рабочий каталог ansible должен располагаться в /etc/ansible
- Все указанные машины должны без предупреждений и ошибок отвечать pong на команду ping в ansible посланную с BR-SRV.

Вариант реализации:

BR-SRV:

- Необходимо установить пакет **ansible** и **sshpass** выполнить это можно следующей командой:

```
apt-get update && apt-get install –y ansible sshpass
```

- Приведём файл инвентаря ansible к следующему виду, отредактировав конфигурационный файл по пути **/etc/ansible/hosts**:
    - в данном примере файл инвентаря описан в **ini** формате

```
vim /etc/ansible/hosts
```

```
HQ-RTR ansible_host=10.10.10.1 ansible_user=net_admin ansible_password=P@ssw0rd ansible_connection=network_cli ansible_network_os=ios
BR-RTR ansible_host=192.168.0.1 ansible_user=net_admin ansible_password=P@ssw0rd ansible_connection=network_cli ansible_network_os=ios
HQ-SRV ansible_host=192.168.100.2 ansible_user=sshuser ansible_password=P@ssw0rd ansible_ssh_port=2026
HQ-CLI ansible_host=192.168.200.2 ansible_user=user ansible_password=P@ssw0rd


[all:vars]
ansible_python_interpreter=/usr/bin/python3
```

- Редактируем файл **/etc/ansible/ansible.cfg**, приводя его к следующему виду:

```
vim /etc/ansible/ansible.cfg
```

```
# Since Ansible 2.12 (core):
# To generate an example config file (a "disabled" one with all default settings, commented out):
# ansible-config init --disabled > ansible.cfg
#
# Also you can now have a more complete file by including existing plugins:
# ansible-config init --disabled -t all > ansible.cfg
[defaults]

inventory = /etc/ansible/hosts
host_key_checking = False
```

- Устанавливаем необходимые коллекции для подключения к «EcoRouterOS»:

```
ansible-galaxy collection install ansible.netcommon

ansible-galaxy collection install cisco.ios
```

```
[root@br-srv ansible]# ansible-galaxy collection install ansible.netcommon
Starting galaxy collection install process
Process install dependency map
Starting collection install process
Downloading https://galaxy.ansible.com/api/v3/plugin/ansible/content/published/collections/artifacts/ansible-netcommon-8.2.1.tar.gz to /root/.ansible/tmp/ansibl
e-local-1326zbtyb4pu/tmpzr8fp5u8/ansible-netcommon-8.2.1-qjsrjj02
Installing 'ansible.netcommon:8.2.1' to '/root/.ansible/collections/ansible_collections/ansible/netcommon'
Downloading https://galaxy.ansible.com/api/v3/plugin/ansible/content/published/collections/artifacts/ansible-utils-6.0.1.tar.gz to /root/.ansible/tmp/ansible-lo
cal-1326zbtyb4pu/tmpzr8fp5u8/ansible-utils-6.0.1-lbxfdy3f
ansible.netcommon:8.2.1 was installed successfully
Installing 'ansible.utils:6.0.1' to '/root/.ansible/collections/ansible_collections/ansible/utils'
ansible.utils:6.0.1 was installed successfully
[root@br-srv ansible]#
```

```
[root@br-srv ansible]# ansible-galaxy collection install cisco.ios
Starting galaxy collection install process
Process install dependency map
Starting collection install process
Downloading https://galaxy.ansible.com/api/v3/plugin/ansible/content/published/collections/artifacts/cisco-ios-11.2.0.tar.gz to /root/.ansible/t
-1347fuwze6p_/tmp27_2axg3/cisco-ios-11.2.0-0hrx4q4b
Installing 'cisco.ios:11.2.0' to '/root/.ansible/collections/ansible_collections/cisco/ios'
cisco.ios:11.2.0 was installed successfully
'ansible.netcommon:8.2.1' is already installed, skipping.
'ansible.utils:6.0.1' is already installed, skipping.
```

- Устанавливаем пакет **python3-module-pip** для возможности установки библиотеки **ansible-pylibssh**:

```
apt-get install –y python3-module-pip
```

Под sshuser

```
br-srv login: sshuser
Password:
Last login: Sat Nov 29 16:37:20 MSK 2025 from 192.168.0.1 on pts/1
[sshuser@br-srv ~]$ pip3 install ansible-pylibssh
Defaulting to user installation because normal site-packages is not writeable
Requirement already satisfied: ansible-pylibssh in /usr/lib64/python3/site-packages (1.3.0)
[sshuser@br-srv ~]$
```

```
pip3 install ansible-pylibssh
```

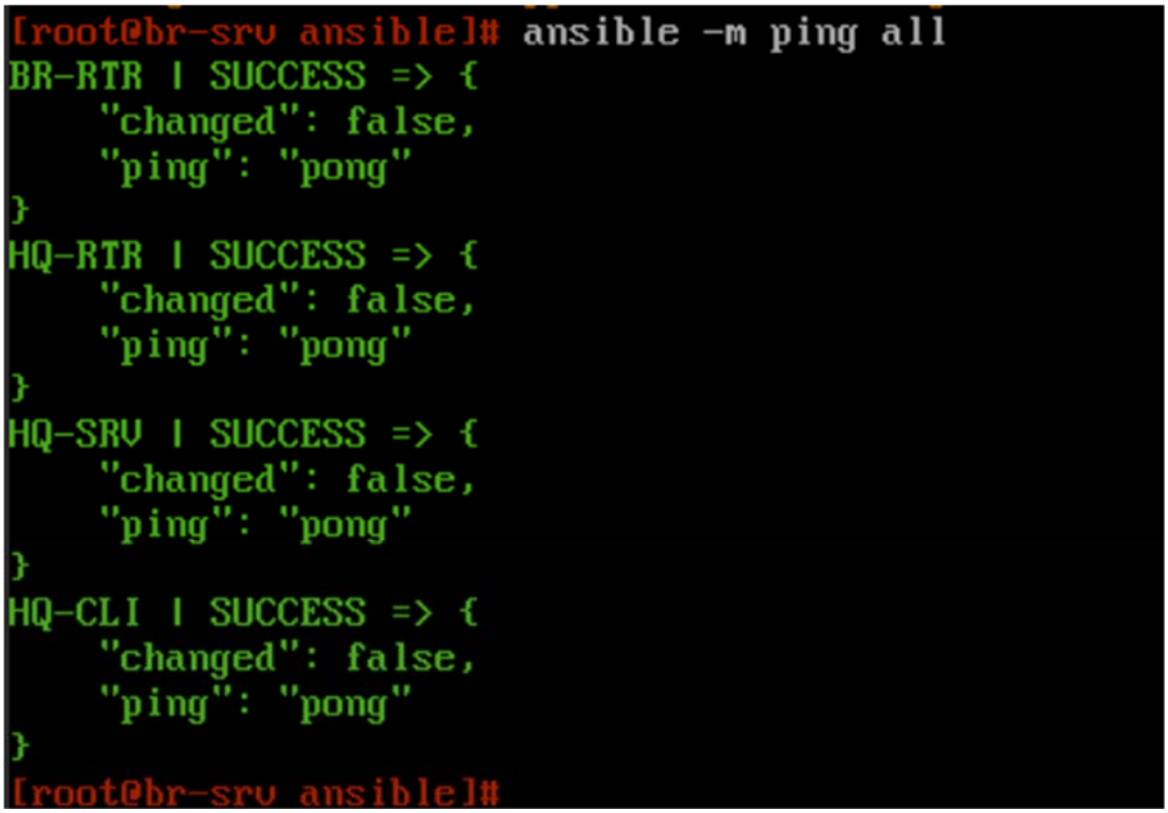
HQ-RTR | BR-RTR:

- На виртуальных машинах с ОС «EcoRouterOS» из режима администрирования (conf t) разрешить подключения к устройству по ssh:

```
(config)# security none
```

BR-SRV:

- Проверяем, ответы от машин должны быть зелёного цвета и содержать значение **pong** в поле **ping**:

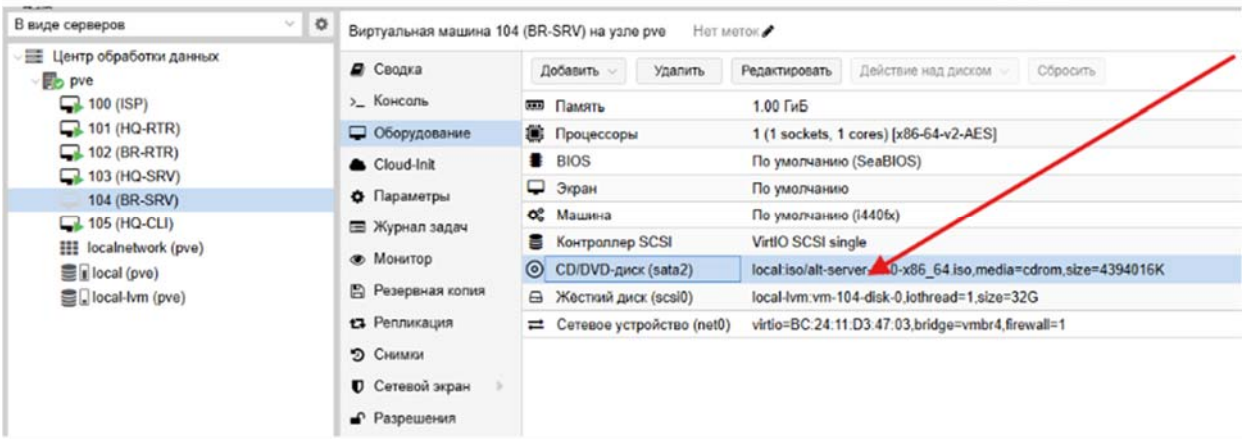


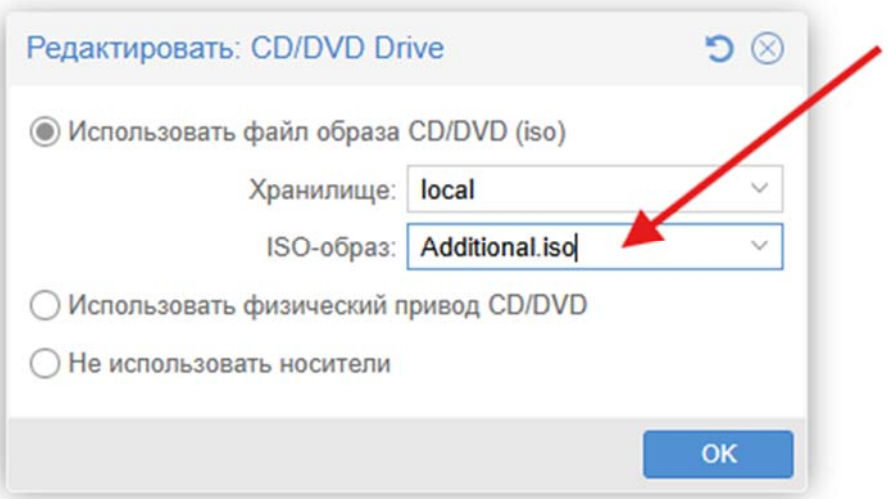
3.6. Разверните веб-приложение testapp с использованием средств контейнеризации на сервере BR-SRV

Задание:

- Средствами docker должен создаваться стек контейнеров с веб приложением и базой данных
- Используйте образы site_latest и mariadb_latest располагающиеся в директории docker в образе Additional.iso
- Основной контейнер testapp должен называться tespapp
- Контейнер с базой данных должен называться db
- Импортируйте образы в docker, укажите в yaml файле параметры подключения к СУБД, имя БД - testdb, пользователь testc паролем P@ssw0rd, порт приложения 8080, при необходимости другие параметры
- Приложение должно быть доступно для внешних подключений через порт 8080

Подключить диск





BR-SRV:

- Установить необходим пакеты для работы с Docker и Docker Compose можно воспользовавшись следующей командой:

```
apt-get install –y docker-engine docker-compose-v2
```

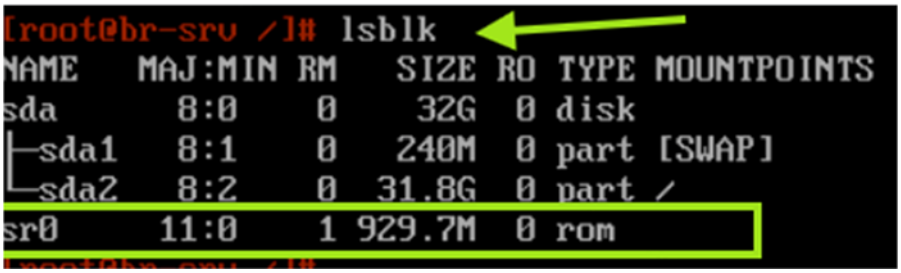
- После установки необходимых пакетов стоит запустить службу docker:

```
systemctl enable --now docker.service
```

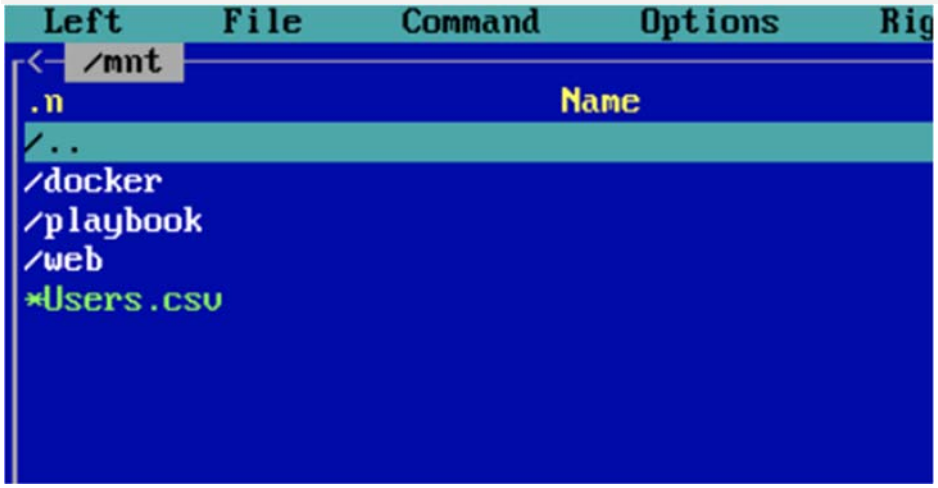
- Выполнить монтирование Additional.iso в директорию /mnt:

  #mount /dev/sr0 /mnt/

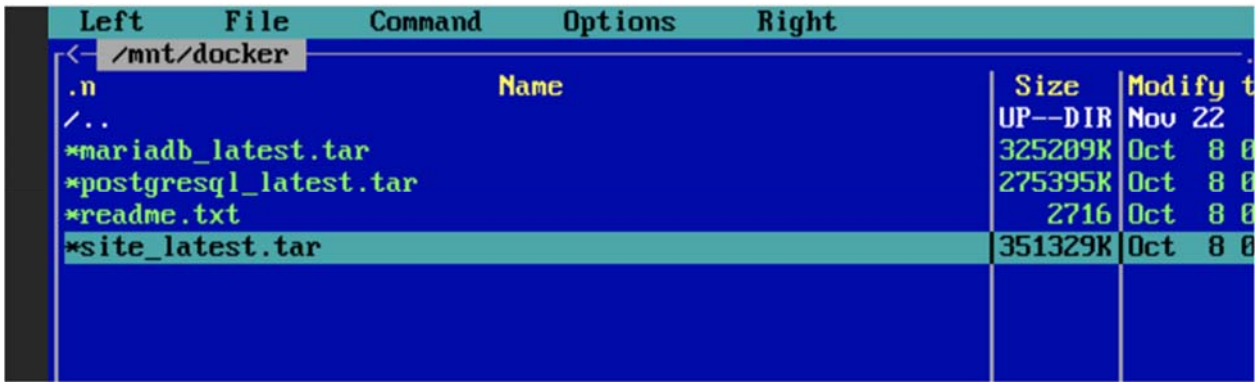
#lsblk




```
#mount /dev/sr0 /mnt/
```



Выполнить импорт образа mariadb_latest и site_latest:




```
docker load < /mnt/docker/site_latest.tar
```

```
root@br-srv mnt]# docker load  < /mnt/docker/site_latest.tar
18dccb7d85a: Loading layer [==================================================>]  8.596MB/8.596MB
09e09bc9ce7: Loading layer [==================================================>]  1.676MB/1.676MB
b5dfdbd0211: Loading layer [==================================================>]  43.22MB/43.22MB
6dadb8c55d7: Loading layer [==================================================>]  5.12kB/5.12kB
a6ab270dfc4: Loading layer [==================================================>]  1.536kB/1.536kB
296fa7d3e68: Loading layer [==================================================>]  176.4MB/176.4MB
7d44a5452c6: Loading layer [==================================================>]  3.072kB/3.072kB
a221749f04b: Loading layer [==================================================>]  129MB/129MB
737b3a43bb8: Loading layer [==================================================>]  836.1kB/836.1kB
oaded image: site:latest
```

docker load < /mnt/docker/mariadb_latest.tar

```
[root@br-srv mnt]# docker load  < /mnt/docker/mariadb_latest.tar
767e56ba346a: Loading layer [==================================================>]  80.42MB/80.42MB
f30f8fd94399: Loading layer [==================================================>]  337.9kB/337.9kB
29698e3a4235: Loading layer [==================================================>]  16.33MB/16.33MB
1a569e551418: Loading layer [==================================================>]  1.536kB/1.536kB
63e39b3459b1: Loading layer [==================================================>]  5.12kB/5.12kB
599b2700498c: Loading layer [==================================================>]  235.8MB/235.8MB
adf17a73d7f3: Loading layer [==================================================>]  13.82kB/13.82kB
64b59101975d: Loading layer [==================================================>]  29.7kB/29.7kB
Loaded image: mariadb:10.11
[root@br-srv mnt]#
```

Проверить:

```
[root@br-srv ~]# docker image ls
REPOSITORY   TAG       IMAGE ID       CREATED         SIZE
site         latest    015b4b821098   2 weeks ago     353MB
mariadb      10.11     bc52d24721da   2 months ago    327MB
[root@br-srv ~]#
```

Также у данного веб приложения есть инструкция в виде файла readme.txt:

```
[root@br-srv ~]# cat /mnt/docker/readme.txt
Разработчик приложения testapp приветствует вас!

Наше приложение выполняет очень важную бизнес-задачу и поставляется в виде набора TAR-архивов с образами контейнеров для Docker.

site_latest.tar - основной контейнер веб-приложения, использующего порт tcp/8000

        переменные для запуска
                DB_TYPE - [maria|postgres]
                DB_HOST - <IPv4 СУБД>
                DB_NAME - <название БД>
                DB_PORT - <порт TCP подключения к БД>
                DB_USER - <пользователь СУБД>
                DB_PASS - <пароль пользователя СУБД>

mariadb_latest.tar - контейнер СУБД MariaDB, используемый порт tcp/3306

        переменные для запуска
                MARIADB_DATABASE - <название БД>
                MARIADB_USER - <пользователь СУБД>
                MARIADB_PASSWORD - <пароль пользователя СУБД>
                MARIADB_ROOT_PASSWORD/MARIADB_RANDOM_ROOT_PASSWORD - обязательные параметры

postgresql_latest.tar  - контейнер СУБД PostgeSQL, используемый порт tcp/5432

        переменные для запуска
                POSTGRES_DB - <название БД>
                POSTGRES_USER - <пользователь СУБД>
                POSTGRES_PASSWORD - <пароль пользователя СУБД>

Все заявленные переменные являются обязательными для запуска и должны быть согласованы по значениям.

Проверка работоспособности приложения проводится путём заполнения 3 строк данными с последующим перезапуском узла. Записи должны сохраниться при повторном обра
ении к сайту. Так же, контроль может быть произведён путем проверки записи в БД вносимых через веб-интерфейс данных.

Данное приложение поставляется as is, разработчик не несёт никакой ответственности за возможные убытки с чьей-либо стороны, запрещает вносить изменения или ком
ентировать его исходный ход где бы то ни было.

Использовать только для нужд сдачи ДЭ или подготовки к ДЭ.
[root@br-srv ~]#
```

Создадать файл compose.yaml и поместить в него следующее содержимое:

```
vim /root/compose.yml
```

```
services:
  database:
    container_name: db
    image: mariadb:10.11
    restart: always
    ports:
      - "3306:3306"
    environment:
      MARIADB_DATABASE: "testdb"
      MARIADB_USER: "testc"
      MARIADB_PASSWORD: "P@ssw0rd"
      MARIADB_ROOT_PASSWORD: "toor"

  app:
    container_name: testapp
    image: site:latest
    restart: always
    ports:
      - "8080:8000"
    environment:
      DB_TYPE: "maria"
      DB_HOST: "192.168.0.2"
      DB_PORT: "3306"
      DB_NAME: "testdb"
      DB_USER: "testc"
      DB_PASS: "P@ssw0rd"
    depends_on:
      - database
```

```
services:
  database:
    container_name: db
    image: mariadb:10.11
    restart: always
    ports:
      - "3306:3306"
    environment:
      MARIADB_DATABASE: "testdb"
      MARIADB_USER: "testc"
      MARIADB_PASSWORD: "P@ssw0rd"
      MARIADB_ROOT_PASSWORD: "toor"

  app:
    container_name: testapp
    image: site:latest
    restart: always
    ports:
      - "8080:8000"
    environment:
      DB_TYPE: "maria"
      DB_HOST: "192.168.0.2"
      DB_PORT: "3306"
      DB_NAME: "testdb"
      DB_USER: "testc"
      DB_PASS: "P@ssw0rd"
    depends_on:
      - database
```

Запустить набор контейнеров с веб приложением и базой данных:

#docker compose up -d

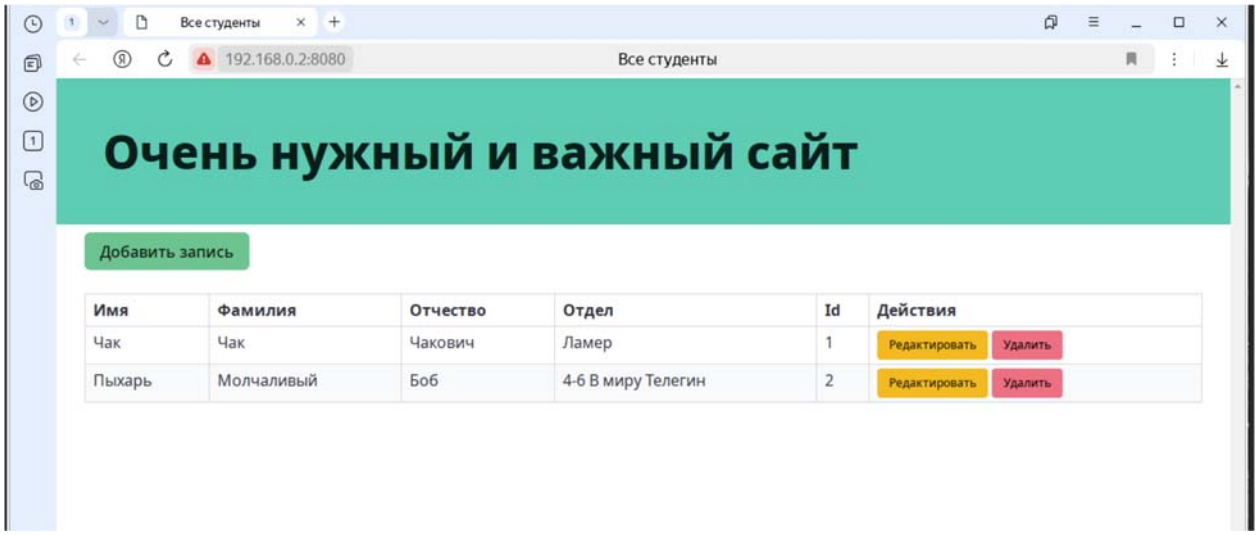
```
[root@br-srv ~]# docker compose up -d
[+] Running 3/3
 ? Network root_default  Created
 ? Container db          Started
 ? Container testapp     Started
```

Проверяем набор контейнеров с веб приложением и базой данных:

```
[root@br-srv ~]# docker ps
CONTAINER ID   IMAGE          COMMAND                  CREATED              STATUS              PORTS                                                  NAMES
ec9445c9a408   site:latest    "sh -c 'python3 -m a…"   About a minute ago   Up About a minute   0.0.0.0:8080->8080/tcp, [::]:8080->8080/tcp            testa
87c9b5e337b4   mariadb:10.11  "docker-entrypoint.s…"   About a minute ago   Up About a minute   0.0.0.0:3306->3306/tcp, [::]:3306->3306/tcp            db
```

Проверяем доступ до веб приложения с браузера:

HQ-CLI


Все студенты
192.168.0.2:8080
Все студенты
Очень нужный и важный сайт
Добавить запись
Имя
Фамилия
Отчество
Отдел
Id
Действия
Чак
Чак
Чакович
Ламер
1
Редактировать
Удалить
Пыхарь
Молчаливый
Боб
4-6 В миру Телегин
2
Редактировать
Удалить

3.7. Разверните веб приложение на сервере HQ-SRV

Задание:

- Используйте веб-сервер apache
- В качестве системы управления базами данных используйте mariadb
- Файлы веб приложения и дамп базы данных находятся в директории web образа Additional.iso
- Выполните импорт схемы и данных из файла dump.sql в базу данных webdb
- Создайте пользователя web с паролем P@ssw0rd и предоставьте ему права доступа к этой базе данных
- Файлы index.php и директорию images скопируйте в каталог веб сервера apache
- В файле index.php укажите правильные учётные данные для подключения к БД
- Запустите веб сервер и убедитесь в работоспособности приложения
- Основные параметры отметьте в отчёте

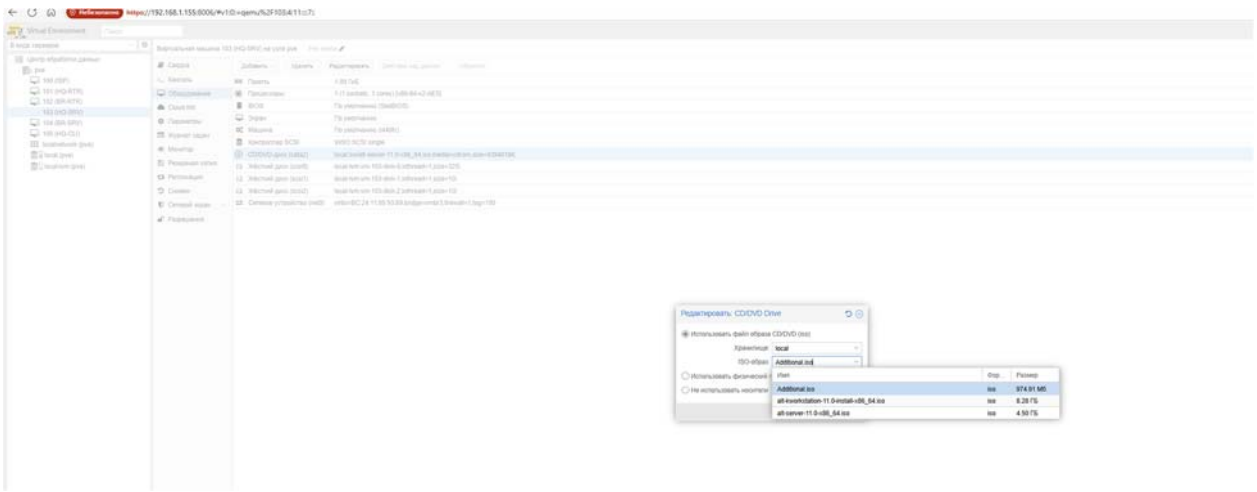
Вариант реализации:

HQ-SRV:

Установить метапакет который содержит в себе всё необходимое для работы стека LAMP (Linux+Apache+MariaDB+PHP):

```
apt-get install lamp-server –y
```

- Выполнить монтирование **Additional.iso** в директорию **/mnt**:



mount /dev/sr0 /mnt/

Произвести копирование файлов веб приложения **index.php** и **logo.png** в директорию **/var/www/html**:

cp /mnt/web/index.php /var/www/html

cp /mnt/web/logo.png /var/www/html

В файле **/var/www/html/index.php** указать правильные учётные данные для подключения к БД:

vim /var/www/html/index.php

```php
<?php
$servername = "localhost";
$username = "webc";
$password = "P@ssw0rd";
$dbname = "webdb";

$conn = new mysqli($servername, $username, $password, $dbname);
```

Включить и добавить в автозагрузку службу mariadb:

systemctl enable --now mariadb

Перейти в интерфейс управления MariaDB:

mariadb –u root

Создать базу данных с именем webdb:

CREATE DATABASE webdb;

Создать пользователя webc с паролем P@ssw0rd:

CREATE USER ‘webc’@’localhost’ IDENTIFIED BY ‘P@ssw0rd’;

Назначить пользователю webc полные права на базу данных webdb, после чего выйти из интерфейса управления MariaDB:

GRANT ALL PRIVILEGES ON webdb.* TO ‘webc’@’localhost’ WITH GRANT OPTION;

EXIT;

Выполнить импорт схемы и данных из файла dump.sql в базу данных webdb:

mariadb –u webc –p –D webdb < /mnt/web/dump.sql

Проверить:

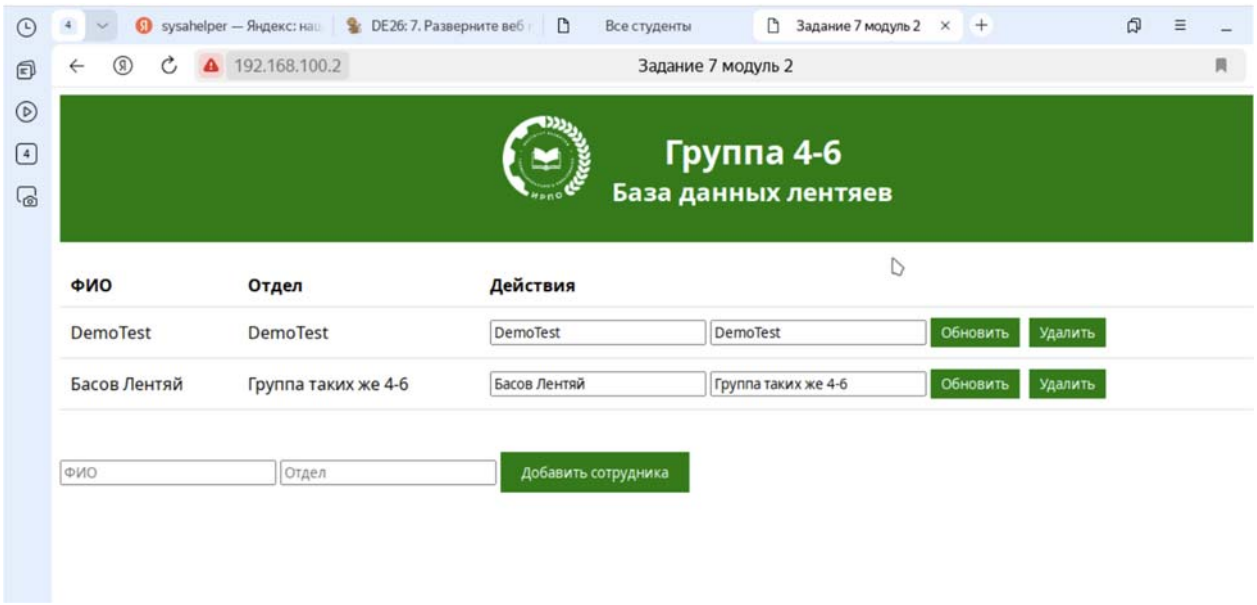
```
[root@hq-srv ~]# mariadb
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 34
Server version: 10.11.14-MariaDB-alt1 (ALT p11)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> USE webdb;
Database changed
MariaDB [webdb]> SHOW TABLES;
+-----------------+
| Tables_in_webdb |
+-----------------+
| employees       |
+-----------------+
1 row in set (0.000 sec)

MariaDB [webdb]> _
```

Включить и добавить в автозагрузку службу **httpd2**:

systemctl enable --now httpd2

Проверяем доступ до веб приложения с браузера:

HQ-CLI



3.8. На маршрутизаторах сконфигурируйте статическую трансляцию портов

Задание:

- Пробросьте порт 8080 в порт приложения testapp BR-SRV на маршрутизаторе BR-RTR, для обеспечения работы приложения testapp извне
- Пробросьте порт 8080 в порт веб приложения на HQ-SRV на маршрутизаторе HQ-RTR, для обеспечения работы веб приложения извне
- Пробросьте порт 2026 на маршрутизаторе HQ-RTR в порт 2026 сервера HQ-SRV, для подключения к серверу по протоколу ssh из внешних сетей
- Пробросьте порт 2026 на маршрутизаторе BR-RTR в порт 2026 сервера BR-SRV, для подключения к серверу по протоколу ssh из внешних сетей.

Вариант реализации:

- Из режима администрирования (conf t) выполнить следующую команду:

  ip nat source static tcp <IP-АДРЕС_УСТРОЙСТВА_ЛОКАЛЬНОЙ_СЕТИ> <ПОРТ_УСТРОЙСТВА_ЛОКАЛЬНОЙ_СЕТИ> <ВНЕШНИЙ_IP-АДРЕС_УСТРОЙСТВА> <ПОРТ_ДЛЯ_ОБРАЩЕНИЯ_ИЗ_ВНЕШНЕЙ_СЕТИ>

  HQ-RTR:

  hq-rtr(config)#ip nat source static tcp 192.168.100.2 80 172.16.1.2 8080

  hq-rtr(config)#ip nat source static tcp 192.168.100.2 2026 172.16.1.2 2026

  hq-rtr(config)#write memory

  BR-RTR:

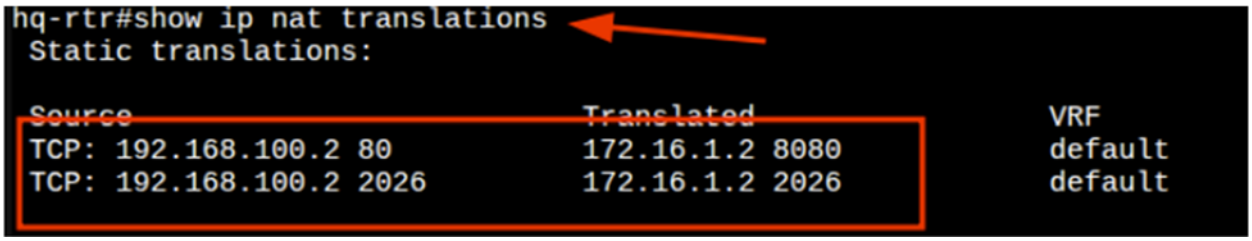
  br-rtr(config)#ip nat source static tcp 192.168.0.2 8080 172.16.2.2 8080

  br-rtr(config)#ip nat source static tcp 192.168.0.2 2026 172.16.2.2 2026

br-rtr(config)#write memory

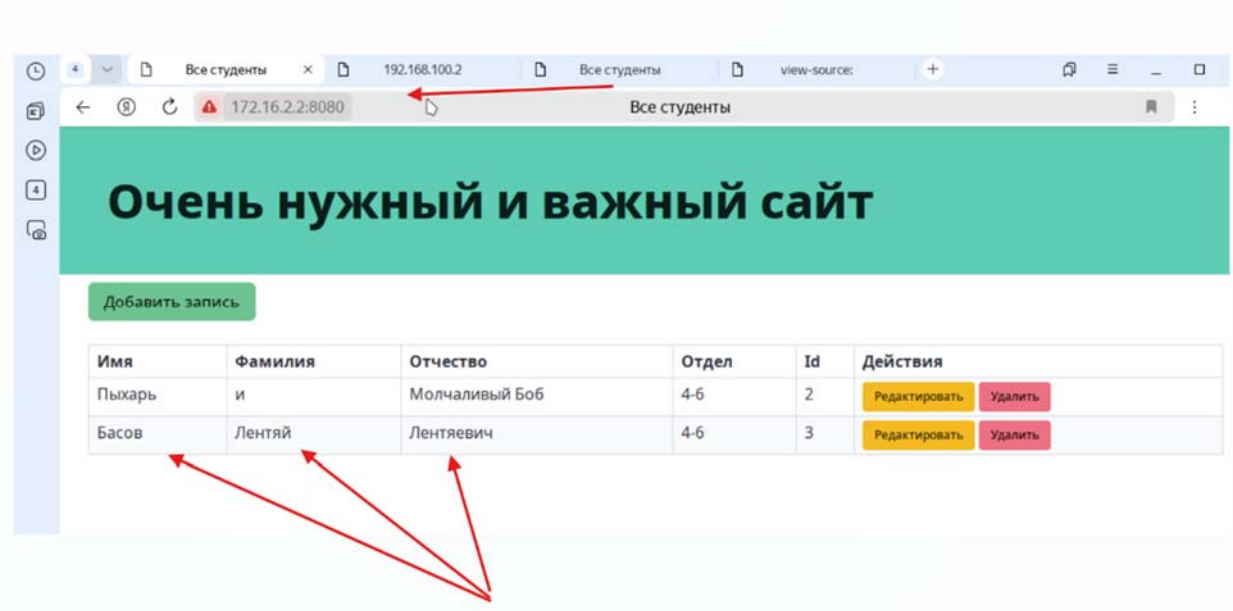
Проверяем статическую трансляцию портов:

HQ-RTR

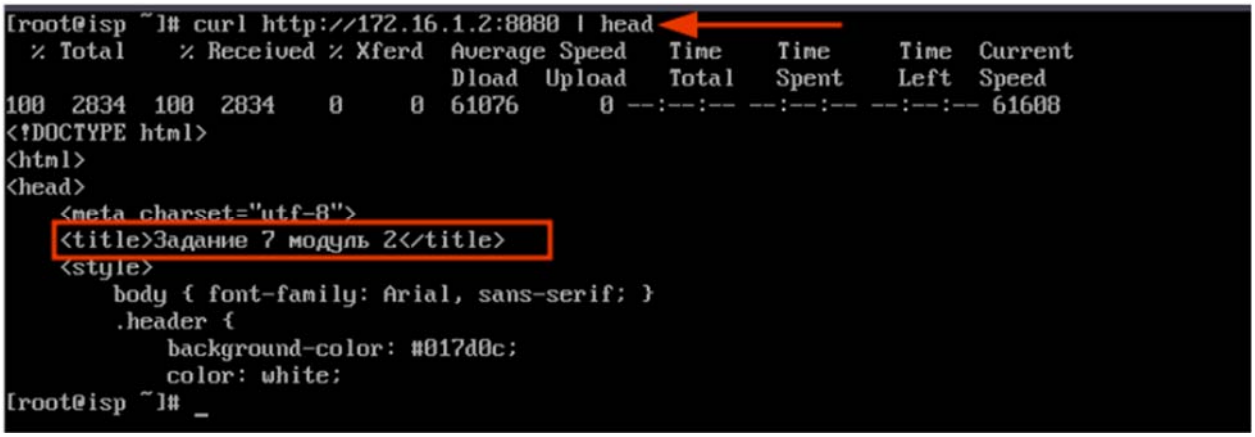


BR-RTR

Проверяем возможность доступа из-вне до веб приложения развёрнутого на базе стека контейнеров с браузера на клиенте:

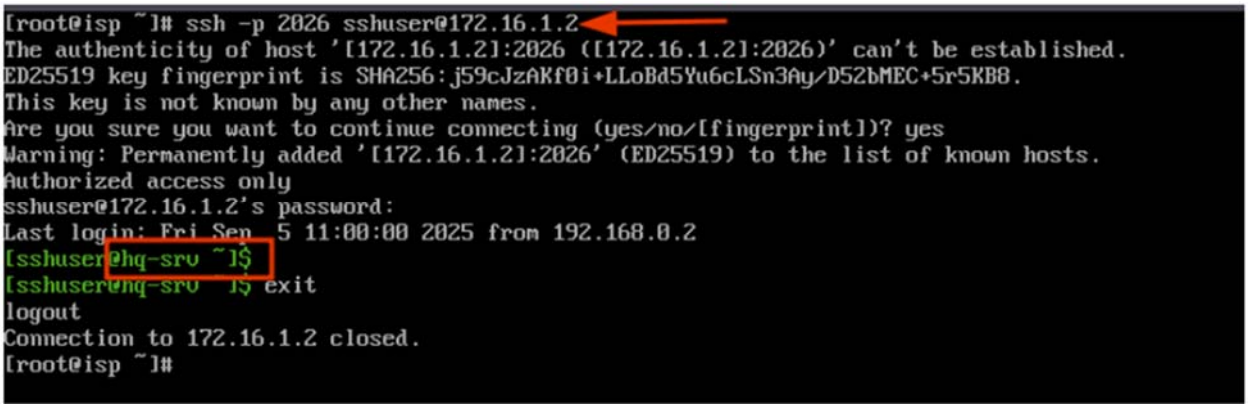


Проверяем возможность доступа из-вне до веб приложения развёрнутого на базе веб сервера Apache с виртуальной машины ISP:

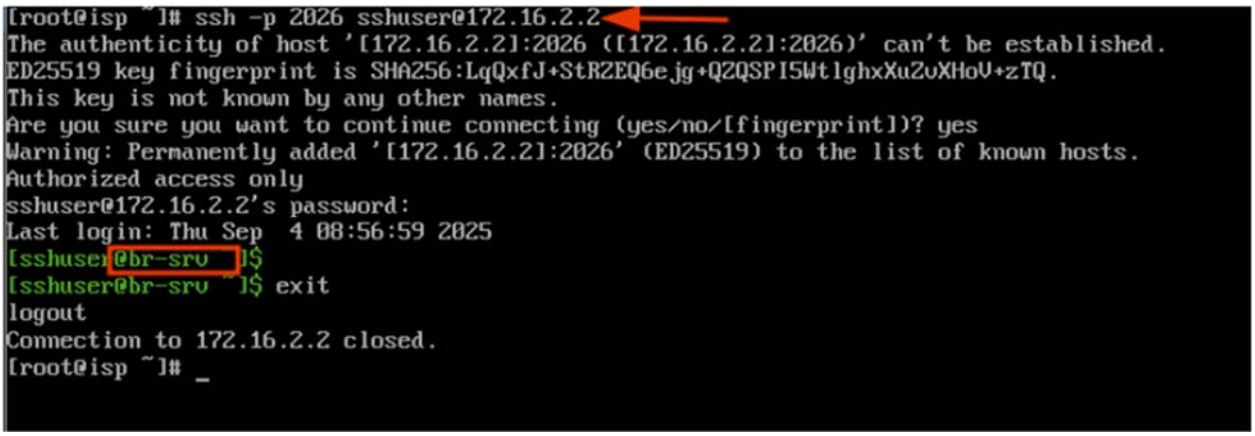


Проверяем возможность доступа из-вне по SSH с виртуальной машины ISP:

до HQ-SRV:



до BR-SRV:

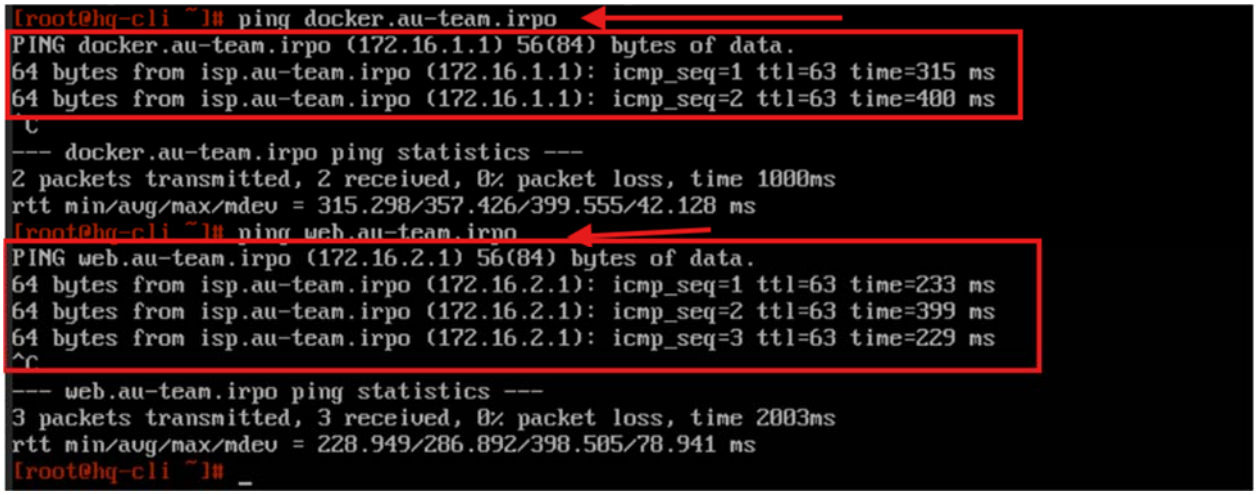


3.9. Настройте веб-сервер nginx как обратный прокси-сервер на ISP

Задание:

- При обращении по доменному имени web.au-team.irpo у клиента должно открываться веб приложение на HQ-SRV
- При обращении по доменному имени docker.au-team.irpo клиента должно открываться веб приложение testapp.

Проверка



ISP:

- Установить пакет **nginx**:

```
apt-get install -y nginx
```

- Настроить nginx как реверсивный прокси сервер, приведя файл **/etc/nginx/sites-available.d/default.conf** к следующему виду:

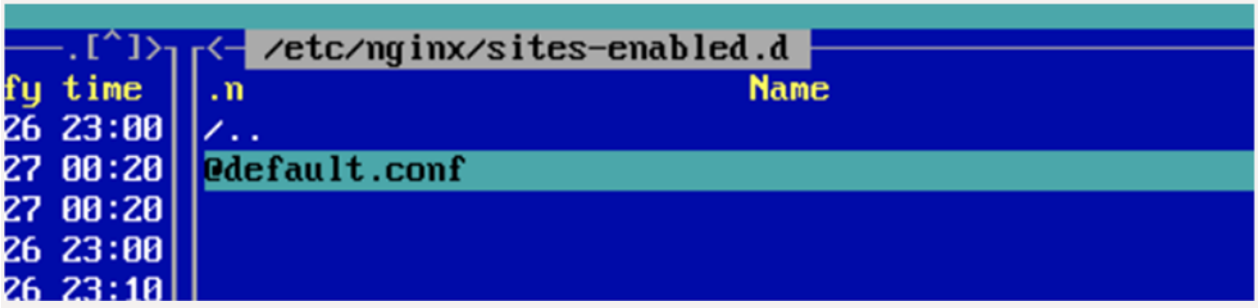
```
vim /etc/nginx/sites-available.d/default.conf
```

кщще

```
server {
        listen 80;
        server_name web.au-team.irpo;

        location / {
                proxy_pass http://172.16.1.2:8080;
                proxy_set_header Host $host;
                proxy_set_header X-Real-IP $remote_addr;
                proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
                proxy_set_header X-Forwarded-Proto $scheme;
        }
}

server {
        listen 80;
        server_name docker.au-team.irpo;

        location / {
                proxy_pass http://172.16.2.2:8080;
                proxy_set_header Host $host;
                proxy_set_header X-Real-IP $remote_addr;
                proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
                proxy_set_header X-Forwarded-Proto $scheme;
        }
}
```

- Добавить символическую ссылку на данный файл:

```
ln -s /etc/nginx/sites-available.d/default.conf /etc/nginx/sites-enabled.d/
```



- Проверить наличие ошибок в конфигурационных файлах:

- Запустить и активировать службу nginx:

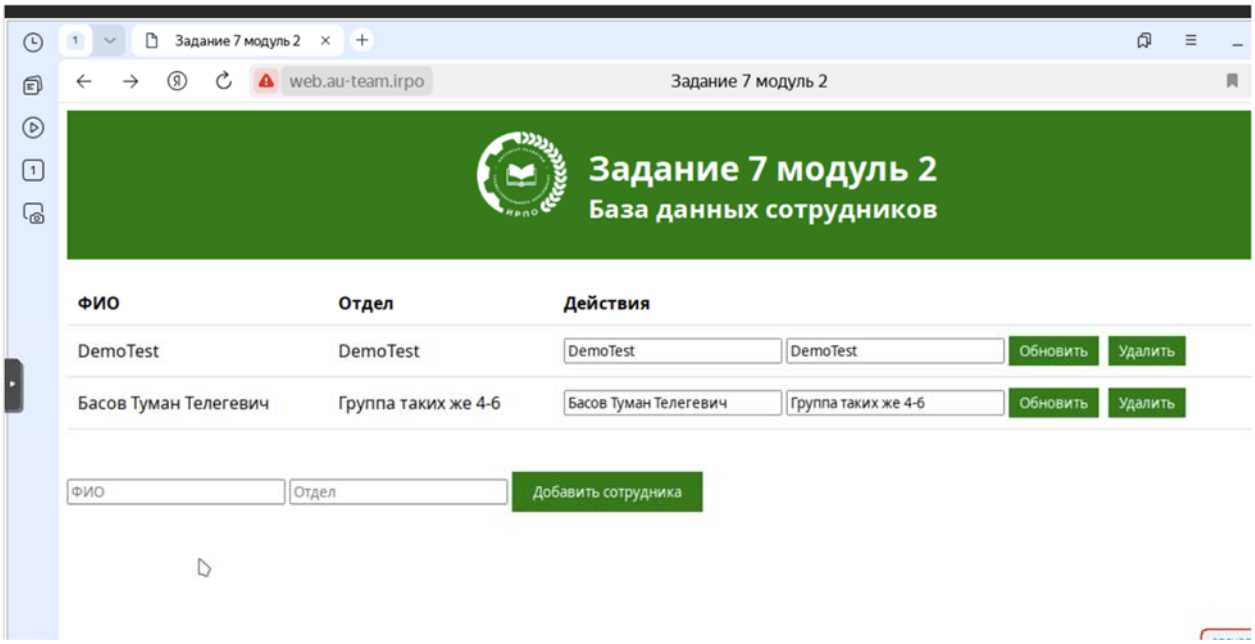
```
systemctl enable --now nginx
```

HQ-CLI:

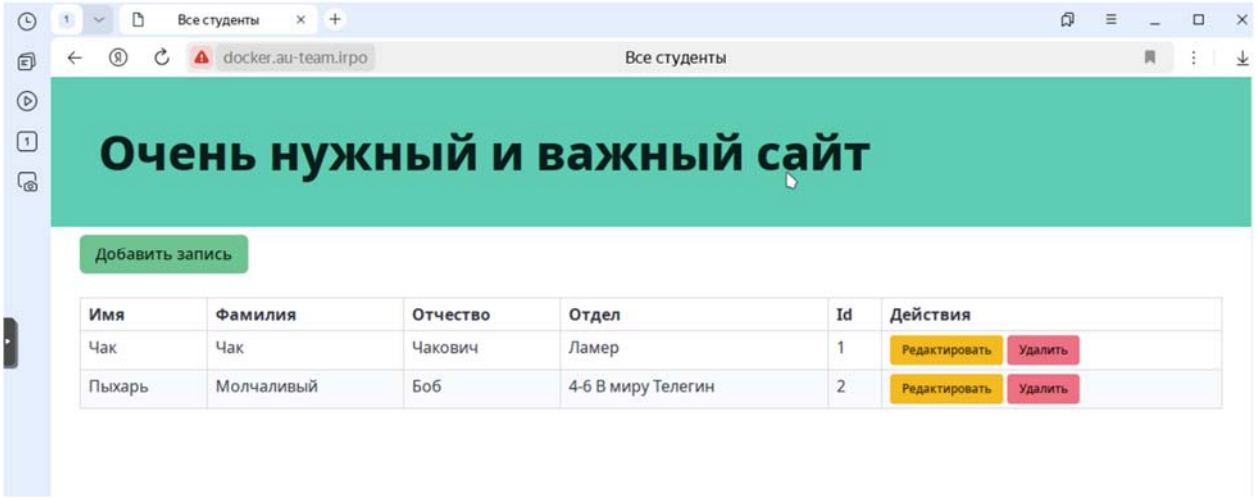
- Поскольку в домене SambaDC нет DNS записей ссылающихся на необходимые имена, а на HQ-CLI в качестве DNS-сервера задан адрес именно контроллера домена, поэтому необходимо добавить записи в файл /etc/hosts на виртуальной машине HQ-CLI:
    - или же используя утилиту **samba-tool** добавить необходимые записи на DNS-сервере BR-SRV;

```
[root@hq-cli ~]# cat /etc/hosts
127.0.0.1       localhost.localdomain localhost
::1     localhost6.localdomain localhost6
172.16.1.1      web.au-team.irpo
172.16.2.1      docker.au-team.irpo
[root@hq-cli ~]#
```

- Проверяем возможность доступа до веб ресурсов с браузера на клиенте:
    - http://web.au-team.irpo



- http://docker.au-team.irpo



3.10. На маршрутизаторе ISP настройте web-based аутентификацию

Задание:

- При обращении к сайту web.au-team.irpo клиенту должно быть предложено ввести аутентификационные данные
  - В качестве логина для аутентификации выберите WEB с паролем P@ssw0rd
  - Выберите файл /etc/nginx/.htpasswd в качестве хранилища учётных записей
  - При успешной аутентификации клиент должен перейти на веб сайт.

Вариант реализации:

ISP:

- Установить пакет **apache2-htpasswd**:

```
apt-get install -y apache2-htpasswd
```

- Средствами утилиты **htpasswd** создать пользователя **WEB** и добавить информацию о нём в файл **/etc/nginx/.htpasswd**, задав пароль **P@ssw0rd:**

```
htpasswd –c /etc/nginx/.htpasswd WEB
```

```
[root@isp ~]# htpasswd -c /etc/nginx/.htpasswd WEB
New password:
Re-type new password:
Adding password for user WEB
[root@isp ~]# _
```

- Добавить web-based аутентификацию для доступа к сайту **web.au-team.irpo** в конфигурационный файл **/etc/nginx/sites-available.d/default.conf**:

```
vim /etc/nginx/sites-available.d/default.conf
```

```
server {
        listen 80;
        server_name web.au-team.irpo;

        location / {
                proxy_pass http://172.16.1.2:8080;
                proxy_set_header Host $host;
                proxy_set_header X-Real-IP $remote_addr;
                proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
                proxy_set_header X-Forwarded-Proto $scheme;
                auth_basic "Restricted area";
                auth_basic_user_file /etc/nginx/.htpasswd;
        }
}

server {
        listen 80;
        server_name docker.au-team.irpo;

        location / {
                proxy_pass http://172.16.2.2:8080;
                proxy_set_header Host $host;
                proxy_set_header X-Real-IP $remote_addr;
                proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
                proxy_set_header X-Forwarded-Proto $scheme;
        }
}
```

- Проверить наличие ошибок в конфигурационных файлах:

```
[root@isp ~]# nginx -t
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
[root@isp ~]#
```

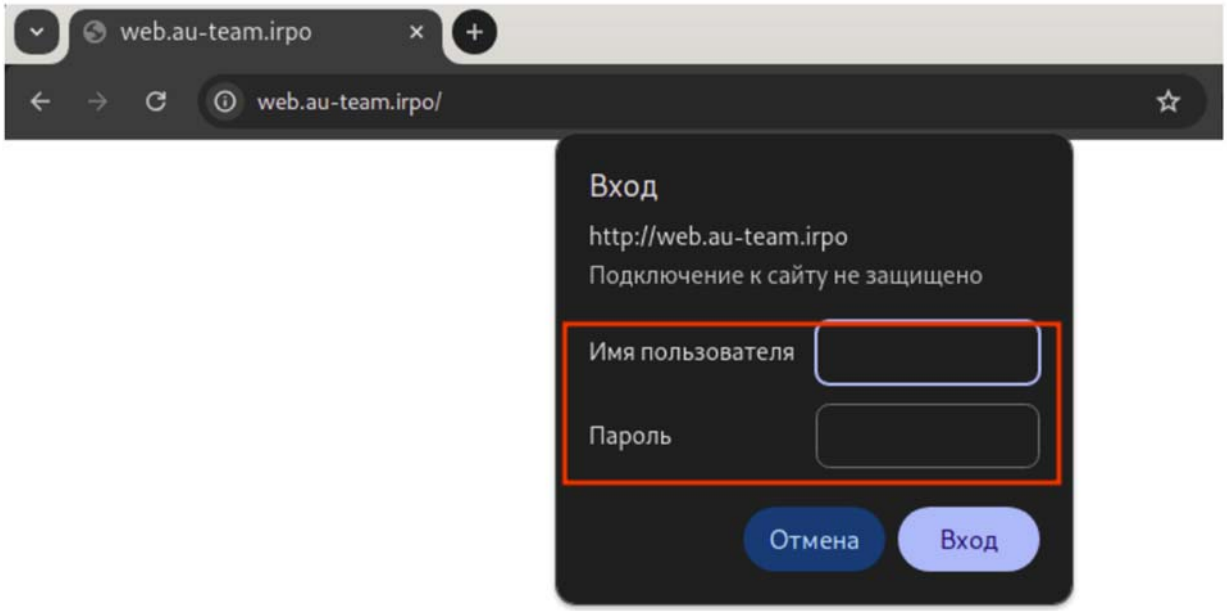
- Перезапустить службу **nginx**:

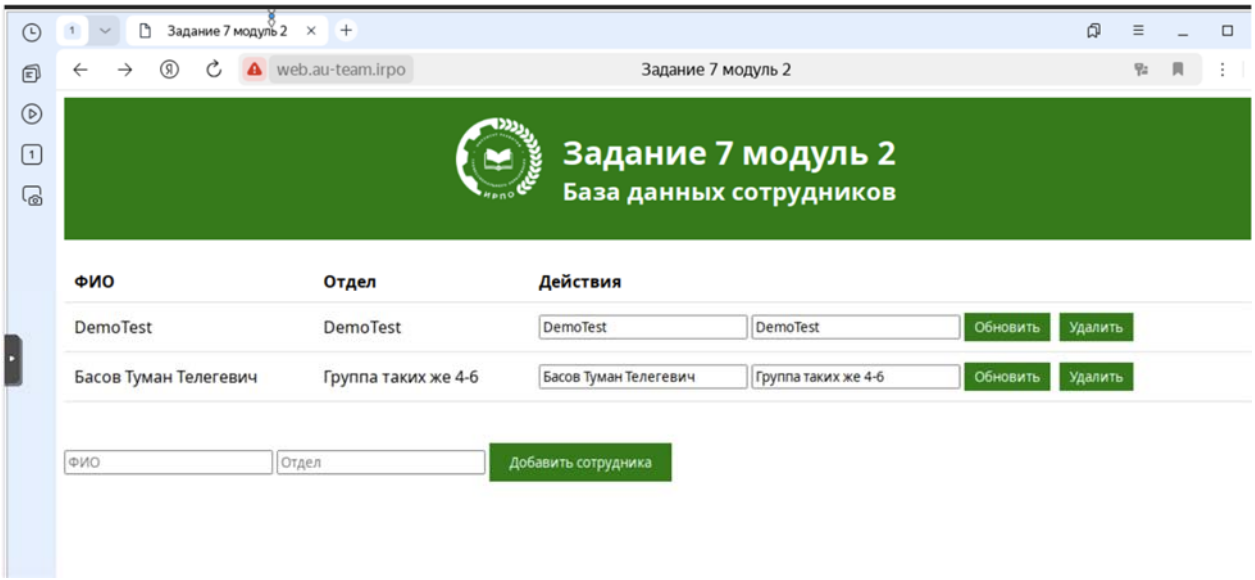
```
systemctl restart nginx
```

HQ-CLI:

- Проверяем возможность доступа до веб ресурса с браузера на клиенте:

- Имя пользователя: **WEB**
- Пароль: **P@ssw0rd**





3.11. Удобным способом установите приложение Яндекс Браузер на HQ-CLI

Задание:

Установку браузера отметьте в отчёте.

3.11.1 Вариант 1

HQ-CLI:

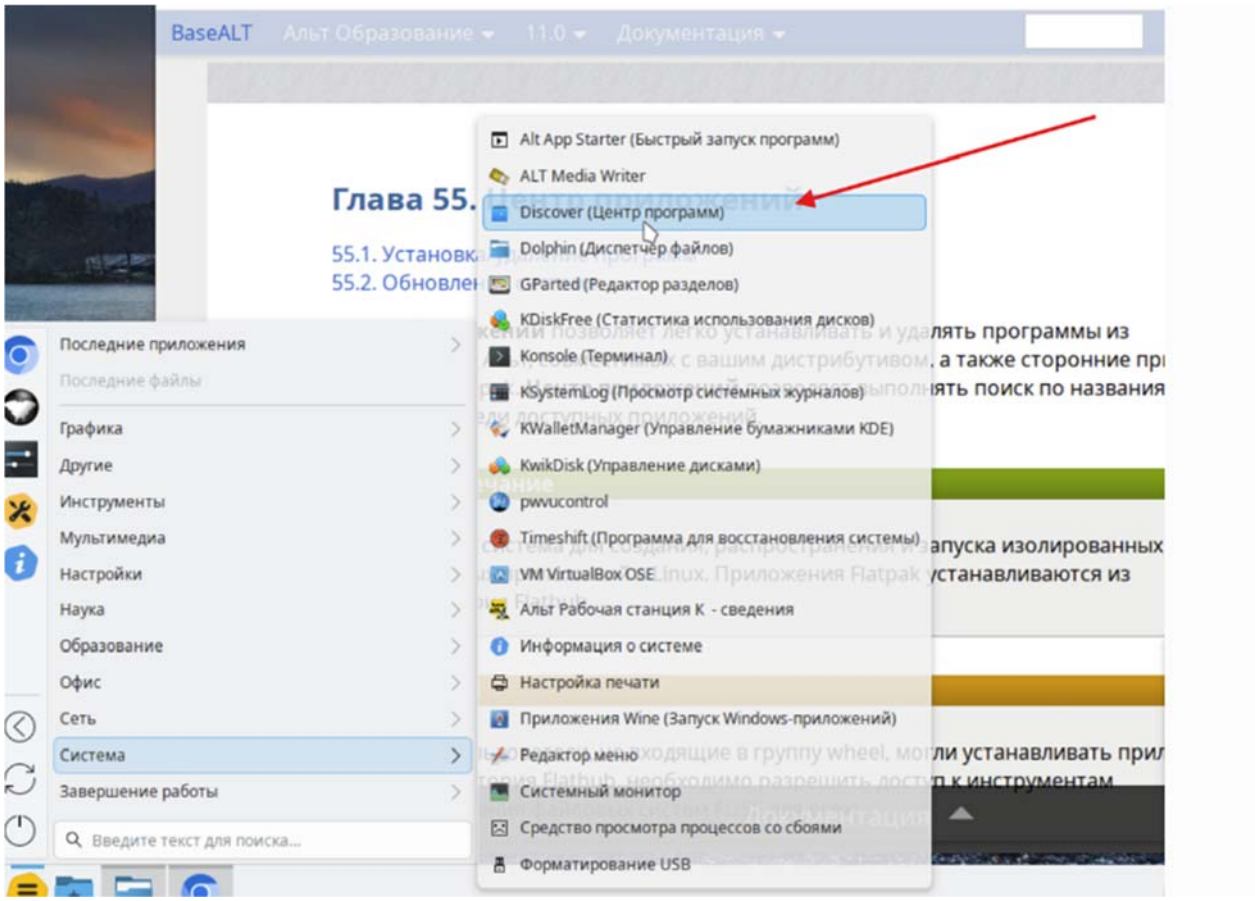
От имени суперпользователя выполнить:

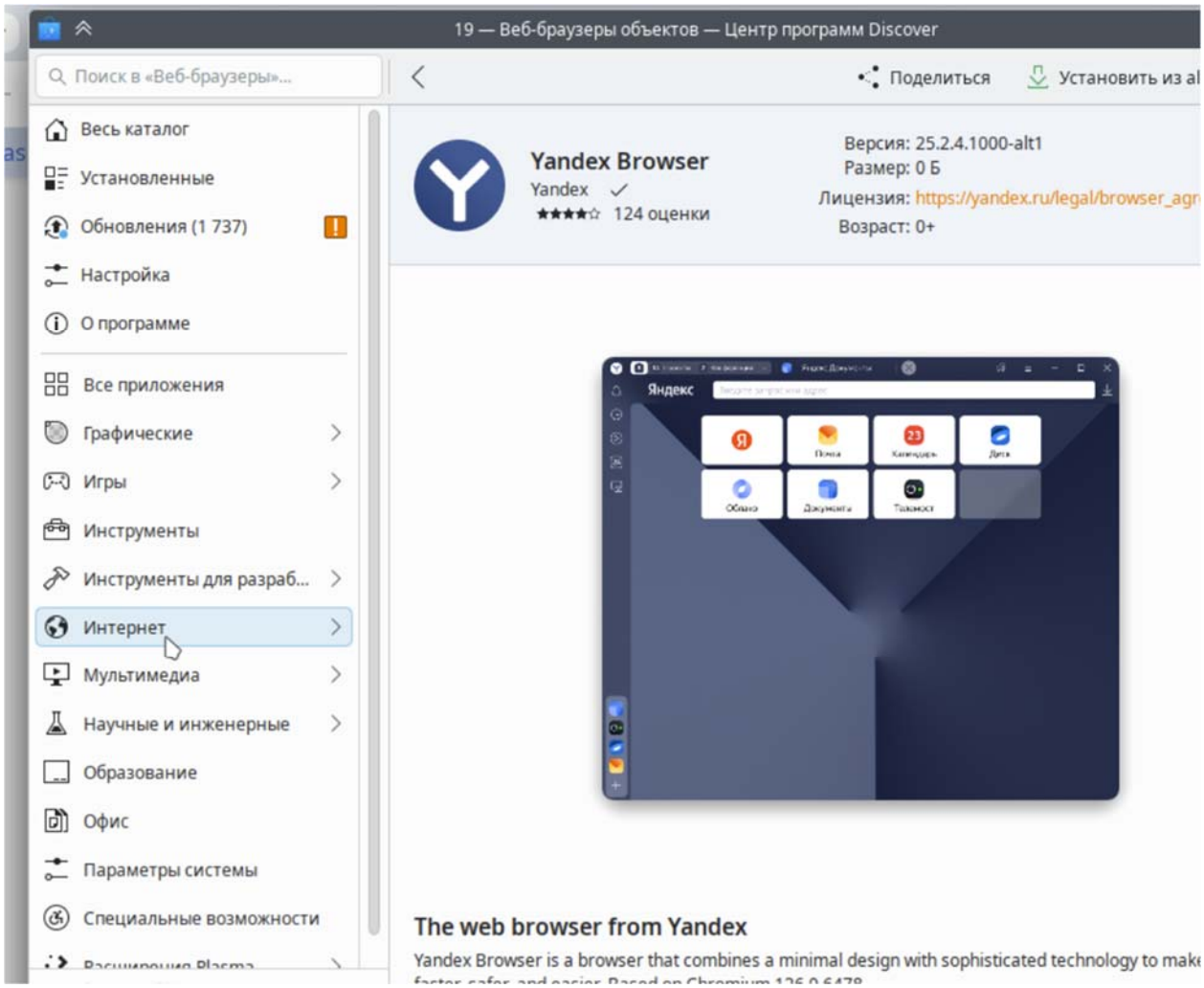
apt-get install –y yandex-browser-stable

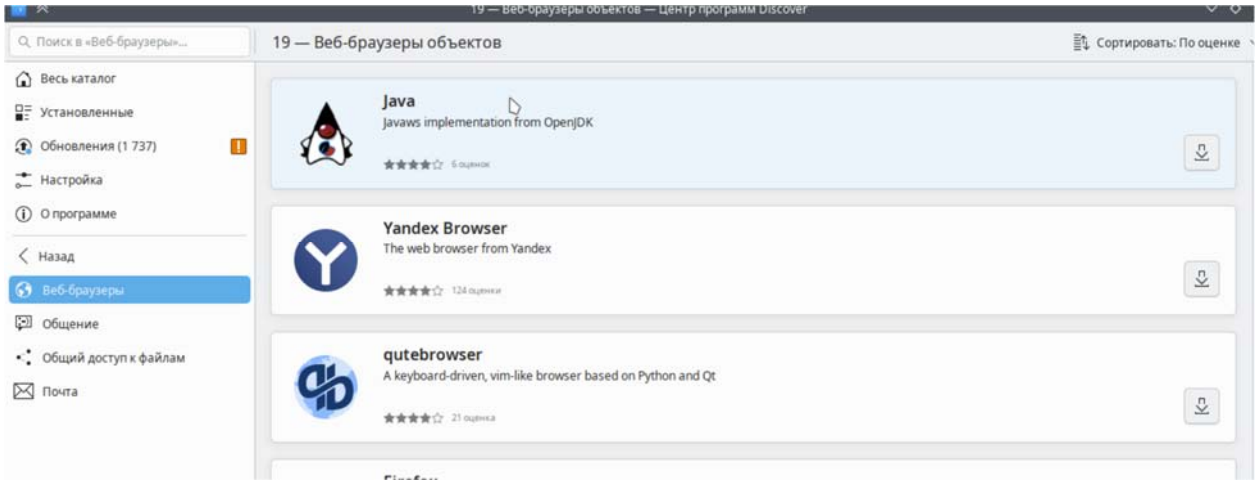
```
[root@hq-cli ~]# apt-get install yandex-browser-stable
Чтение списков пакетов... Завершено
Построение дерева зависимостей... Завершено
Следующие НОВЫЕ пакеты будут установлены:
  yandex-browser-stable
0 будет обновлено, 1 новых установлено, 0 пакетов будет удалено и 1449 не будет обновлено.
Необходимо получить 0B/218MB архивов.
После распаковки потребуется дополнительно 587MB дискового пространства.
Совершаем изменения...
Подготовка...                          ############################################################ [100%]
Обновление / установка...
1: yandex-browser-stable-25.2.4.1000-alt#########################
```

%

3.11.1 Вариант 2




19 — Веб-браузеры объектов — Центр программ Discover
Поиск в «Веб-браузеры»...
Поделиться
Установить из al
Весь каталог
Установленные
Обновления (1 737)
Настройка
О программе
Все приложения
Графические
Игры
Инструменты
Инструменты для разраб...
Интернет
Мультимедиа
Научные и инженерные
Образование
Офис
Параметры системы
Специальные возможности
Yandex Browser
Yandex
124 оценки
Версия: 25.2.4.1000-alt1
Размер: 0 Б
Возраст: 0+
Яндекс
The web browser from Yandex
Yandex Browser is a browser that combines a minimal design with sophisticated technology to mak


19 — Веб-браузеры объектов
Поиск в «Веб-браузеры»...
Сортировать: По оценке
Весь каталог
Установленные
Обновления (1 737)
Настройка
О программе
Назад
Веб-браузеры
Общение
Общий доступ к файлам
Почта
Java
Javaws implementation from OpenJDK
Yandex Browser
The web browser from Yandex
qutebrowser
A keyboard-driven, vim-like browser based on Python and Qt

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 (sudo)

Команда **sudo** может использоваться [1] для выполнения пользователем какой-либо команды, требующей права суперпользователя (**root**), то есть получение прав **root** для выполнения какой-либо команды на время её выполнения.

Перед выполнением команды **sudo** запрашивает пароль пользователя, а не пароль **root**, как у команды **su -**.

После выполнения **sudo** существует временной отрезок, в течение которого повторное выполнение команды **sudo** не требует пароль (что удобно для взлома вашего компьютера со стороны **rootkits** и хакерских атак).

С другой стороны, команда **sudo** удобна для распределения прав между несколькими администраторами компьютера (например, кому можно обновлять и устанавливать программы, а кому настраивать работу аппаратуры компьютера), не предоставляя прав **root** на все другие действия и не выдавая пользователю пароля **root**.

Особенности sudo в дистрибутивах ALT Linux

Штатным способом временного получения прав **root** в большинстве дистрибутивах ALT Linux, является команда su -. Команда **sudo** в большинстве дистрибутивов ALT Linux требует предварительной настройки, так как в **/etc/sudoers** не описан ни один пользователь, включая **root**. Исключением является дистрибутив Simply, где **sudo** уже настроена для первого пользователя. В дополнение к **/etc/sudoers** могут использоваться отдельные файлы из каталога **/etc/sudoers.d/**.

Для ограничения прав на выполнение самой команды **sudo** используется особый механизм **control**.

Настройка control для работы sudo

В ALT Linux sudo используется фреймворк control, который задаёт права на выполнение команды **sudo**.

С его помощью можно дать или отнять права на использование команды **sudo**.

Возможные значения **control sudo** можно посмотреть командой **control sudo help**:

```
$ su -
# control sudo help
```

На текущий момент существуют следующие **политики** у команды **sudo**:

```
public — любой пользователь может получить доступ к команде /usr/bin/sudo
wheelonly — только пользователи из группы wheel имеют право получить доступ к команде /usr/bin/sudo
restricted — только root имеет право выполнять команду /usr/bin/sudo
```

Штатное состояние политики:

```
# control sudo
wheelonly
```

Означает что пользователь из группы **wheel** имеет право запускать саму команду **sudo**, но не означает, что он через **sudo** может выполнить какую-то команду с правами **root**.

Для разрешения получения прав на выполнение конкретных команд с правами **root** надо отредактировать настройки правил **/etc/sudoers** [2] при помощи специальной команды **visudo** (которая не портит права на файлы):

```
$ su -
# EDITOR=mcedit visudo
```

Грубая настройка sudo

Раскомментировать (убрать '#' в начале строки) в **/etc/sudoers** строчку, дав права выполнять через **sudo** любую команду с любого компьютера (например через ssh), пользователям входящим в группу **wheel**, запрашивая их пароль:

```
WHEEL_USERS ALL=(ALL) ALL
```

С точки зрения безопасности **правильнее** давать права на выполнение **sudo** не всей группе **wheel**, а *конкретному пользователю*, например **petya**, входящего в группу **localhost**:

```
petya localhost=(ALL) ALL
```

и не на все **команды** , а на те, которые ему **необходимы** для быстрого получения прав **root**:

```
petya localhost=(ALL) /usr/bin/apt-get,/usr/bin/rpm,/sbin/fdisk
```

Это особенно важно потому, что после выполнения команды **sudo** с запросом пароля есть определённый временный отрезок, в течение которого **sudo** выполняет следующие команды, не запрашивая повторно пароль пользователя.

Также может понадобиться добавление требуемых пользователей в группу **wheel** (созданный при установке системы аккаунт добавляется в неё автоматически, можно посмотреть в **/etc/group**):

```
# gpasswd -a имя_пользователя wheel
```

Примечание: Для быстрого разрешения запуска произвольной программы пользователям группы wheel можно выполнить под правами суперпользователя:

```
# control sudowheel enabled
```

Что является **безрассудством** с точки зрения безопасности ;-)

Тонкая настройка sudo

Для того, чтобы настроить работу **sudo**, необходимо с применением административных привилегий отредактировать файл **/etc/sudoers** при помощи специальной команды **visudo** (подробности смотри выше) и внести туда записи о том, каким пользователям какие команды можно выполнять.

Пример:

```
user1 ALL = (ALL) ALL
user1 ALL = NOPASSWD: /usr/bin/apt-get  update
```

Позволяет пользователю **user1** запускать все приложения через **sudo** с правами суперпользователя (**root**) с запросом пароля, а при выполнении команды **sudo apt-get update** пароль не будет спрашиваться.

Полная документация по формату конфигурационного файла находится в **man-странице sudoers**, начинать читать может быть проще с секции **EXAMPLES**.

- Sudo cancer

Внимание! Используйте команду sudo только если без неё нельзя обойтись!

- Синтаксис правил sudo довольно сложен — можно выстрелить себе в ногу
- Исходный код sudo тяжело вычитать до конца на предмет безопасности — возможность несанкционированного повышения прав маловероятна, но присутствует
- В большинстве случаев sudo в действительности не нужно
    - Например, при сборке ПО всевозможные команды, типа configure, make, не говоря уже о редактировании исходных текстов, надо запускать с правами обычного пользователя, и только установку (*если вам это вообще понадобится*) делать от root-а.

Если вы запустили процесс из-под sudo, все файлы, которые он породит и, возможно, отредактирует, будут принадлежать не вам, а другому пользователю (скорее всего — root-у). Это значит, что *никакой* процесс с правами вашего пользователя больше не сможет их изменять — а возможно, и читать из них. Сами файлы могут создаваться неявно (просто посмотрите, сколько их наплодилось, например, в **~/.cache**), и сложно предсказать, как поведут себя приложения, неожиданно получив отказ в доступе.