КОМПЛЕКТ ОЦЕНОЧНОЙ ДОКУМЕНТАЦИИ №2.1 ДЛЯ ДЕМОНСТРАЦИОННОГО ЭКЗАМЕНА ПО СТАНДАРТАМ ВОРЛДСКИЛЛС РОССИЯ ПО КОМПЕТЕНЦИИ № 39 «СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ» (ДАЛЕЕ – ДЕМОНСТРАЦИОННЫЙ ЭКЗАМЕН)

СОДЕРЖАНИЕ

Паспорт комплекта оценочной документации (КОД) № 2.1 по компетенции № 39 «Сетевое и системное администрирование» 3

Задание для демонстрационного экзамена по комплекту оценочной документации № 2.1 по компетенции № «Сетевое и системное администрирование (образец)38

Примерный план работы Центра проведения демонстрационного экзамена по КОД № 2.1 по компетенции № 39 «Сетевое и системное администрирование»..... 89

План застройки площадки для проведения демонстрационного экзамена по КОД № 2.1 по компетенции № 39 «Сетевое и системное администрирование»..... 91

ПРИЛОЖЕНИЕ 92

Паспорт комплекта оценочной документации (КОД) № 2.1 по компетенции № 39 «Сетевое и системное администрирование»

Комплект оценочной документации (КОД) № 2.1 разработан в целях организации и проведения демонстрационного экзамена по компетенции № 39 «Сетевое и системное администрирование» и рассчитан на выполнение заданий продолжительностью 12 часов.

КОД № 2.1 может быть рекомендован для оценки освоения основных профессиональных образовательных программ и их частей, дополнительных профессиональных программ и программ профессионального обучения, а также на соответствие уровням квалификации согласно Таблице (Приложение).

1. Перечень знаний, умений, навыков в соответствии со Спецификацией стандарта компетенции № 39 «Сетевое и системное администрирование» (WorldSkills Standards Specifications, WSSS), проверяемый в рамках комплекта оценочной документации (Таблица 1).

Таблица 1.

Раздел WSSS	Наименование раздела WSSS	**Важность (%)**
1	**Организация работы и управление**	**6,1**
	Специалист должен знать и понимать: • Регламентирующие документы в области охраны труда и безопасности жизнедеятельности; • В каких ситуациях необходимо применять персональные защитные средства; • Порядок работы, хранения, и обслуживания оборудования в условиях антистатического окружения; • Важность соблюдения техники безопасности и аккуратности при работе с клиентским оборудованием и информацией; • Важность безопасной переработки отходов; • Методы планирования и определения приоритетов; • Важность точной работы, проверки выполненной работы, а также внимания к деталям во всех аспектах своей работы; • Важность организации труда в соответствии с методиками;	

	• Методы и технологии исследования; • Важность управления собственным профессиональным развитием; • Скорость изменения ИТ-сферы и важности соответствия современному уровню.	
	Специалист должен уметь: • Следовать предписаниям в области охраны труда и безопасности жизнедеятельности; • Поддерживать безопасную рабочую среду; • Определять и применять подходящие персональные защитные средства для организации антистатического окружения; • Выбирать, применять и обслуживать инструментарий и оборудование в соответствии с правилами техники безопасности; • Планировать свою работу для достижения максимальной эффективности и поддерживать чистоту на рабочем месте; • Регулярно планировать и корректировать планы в соответствии с изменяющимися приоритетами; • Работать эффективно и регулярно оценивать результаты своего труда; • Соответствовать различным требованиям таких отраслевых систем сертификаций как Cisco, Microsoft, Linux (со специализацией хотя бы в одной из этих областей); • Соответствовать требованиям, предъявляемым к носителям данной компетенции, соответствовать современному уровню; • Демонстрировать эффективные и всеобъемлющие методы получения знаний; • Демонстрировать энтузиазм в области внедрения новых методов, систем, быть готовым к изменениям; • Эффективно работать в составе команды.	
4	**Поиск и устранение неисправностей**	**7,5**
	Специалист должен знать и понимать:	

	• Важность спокойного и сфокусированного подхода к решению проблемы; • Значимость IT-систем и зависимость пользователей и организаций от их доступности; • Популярные аппаратные и программные ошибки; • Аналитический и диагностический подходы к решению проблем; • Границы собственных знаний, навыков и полномочий; • Ситуации, требующие эскалации инцидентов; • Стандартное время решения наиболее популярных проблем.	
	Специалист должен уметь: • Подходить к проблеме с необходимым уровнем уверенности для успокоения пользователя в случае необходимости; • Регулярно проверять результаты собственной работы во избежание проблем на последующих этапах; • Уточнять некорректную информацию для предотвращения или минимизации проблем; • Демонстрировать уверенность и упорство в решении проблем • Быстро узнавать и понимать суть неисправностей и разрешать их в ходе самостоятельной управляемой работы • Тщательно расследовать и анализировать сложные, комплексные ситуации и проблемы, применять методики поиска неисправностей; • Выбирать и принимать диагностирующее ПО и инструменты для поиска неисправностей; • Поддерживать пользователей в решении проблем через советы, указания и инструкции; • Искать помощь в тех случаях, когда требуется более тщательная экспертиза, избегать чрезмерного увлечения проблемой; • Уточнять уровень удовлетворенности пользователя после решения проблемы;	

	• Точно описывать инцидент и документировать решение проблемы.	
5	**Дизайн**	**11,4**
	Специалист должен знать и понимать: • Сетевые топологии и окружения; • Логические и функциональные диаграммы; • Типы активных сетевых устройств (маршрутизаторов и коммутаторов и т.д.) и требования к их расположению; • Решения в области безопасности и их влияние; • Схемы адресации; • Документацию по настройке оборудования и программ.	
	Специалист должен уметь: • Сетевые топологии и окружения; • Логические и функциональные диаграммы; • Типы активных сетевых устройств (маршрутизаторов и коммутаторов и т.д.) и требования к их расположению; • Решения в области безопасности и их влияние; • Схемы адресации; • Документацию по настройке оборудования и программ.	
6	**Настройка, обновление и конфигурация операционных систем**	**25**
	Специалист должен знать и понимать: • Разнообразие операционных систем, их возможности к удовлетворению пользовательских требований; • Процесс выбора подходящих драйверов для разных типов аппаратных средств; • Базовые функции аппаратного обеспечения и процесс начальной загрузки; • Важность следования инструкциям и последствия, цену пренебрежения ими; • Меры предосторожности, рекомендуемые к принятию перед установкой ПО или обновлением системы;	

	• Цель документирования процессов обновления и установки.	
	Специалист должен уметь: • Внимательно слушать и определять пользовательские запросы для удовлетворения ожиданий; • Выбирать операционную систему – проприетарную или открытую; • Точно определять устройство и соответствующий ему драйвер; • Последовательно проверять указанные производителем инструкции при выполнении обновления; • Выбирать роли и возможности операционных систем (такие как Контроллер Домена и т.д.); • Обсуждать предложенные решения для выбранных ролей и возможностей, соглашаться с конструктивными предложениями от пользователей, менеджеров и коллег; • Подготовить технический документ, отражающий принятое решение для согласования и подписи; • Конфигурировать необходимые роли\возможности в соответствии с инструкциями разработчиков или в соответствии с наилучшими практиками; • Тестировать системы, устранять проблемы и проводить контрольные проверки; • Добиваться пользовательского одобрения.	
7	**Конфигурация сетевых устройств**	**25**
	Специалист должен знать и понимать: • Сетевое окружение; • Сетевые протоколы; • Процесс построения сети и как сетевые устройства могут быть настроены для эффективного взаимодействия; • Типы сетевых устройств.	

	Специалист должен уметь: • Интерпретировать пользовательские запросы и требования с точки зрения индустриальных сертификационных требований; • Применять все типы конфигураций, программные и аппаратные обновления на все типы сетевых устройств, которые могут быть в сетевом окружении; • Проектировать и реализовывать процедуры ликвидации инцидентов; • Поддерживать базу данных конфигураций.	

---

2. Форма участия:

Индивидуальная

3. Обобщенная оценочная ведомость.

В данном разделе определяются критерии оценки и количество начисляемых баллов (судейские и объективные) (Таблица 2).

Общее максимально возможное количество баллов задания по всем критериям оценки составляет 75.

Таблица 2.

п/п	Критерий	Модуль, в котором используется критерий	Проверяемые разделы WSSS	Баллы		
				Судейская (если это применимо)	Объективная	Общая
1	A Linux Enviroments	A Linux Enviroments	6	0	25	25
2	B Windows Enviroments	B Windows Enviroments	1, 4, 5	0	25	25
3	C Cisco Enviroments	C Cisco Enviroments	7	0	25	25
				ИТОГО:	**75**	**75**

4. Количество экспертов, участвующих в оценке выполнения задания, и минимальное количество рабочих мест на площадке.

4.1. Минимальное количество экспертов, участвующих в оценке демонстрационного экзамена по компетенции № 39 «Сетевое и системное администрирование» - 3 чел.

4.2. Минимальное количество рабочих мест составляет 9.

4.3. Расчет количества экспертов исходя из количества рабочих мест и участников осуществляется по схеме согласно Таблице 3:

Таблица 3.

Количество постов-рабочих мест / Количество участников	1	2	3	..	..	25
От 1 до 3	3	3	3	3	3	3

5. Список оборудования и материалов, запрещенных на площадке (при наличии)

К проносу запрещаются такие электронные устройства как мобильные телефоны, смартфоны, плееры, наушники, диктофоны, камеры, ноутбуки, планшетные компьютеры и прочие персональные электронные устройства.

Таблица соответствия
знаний, умений и практических навыков, оцениваемых в рамках демонстрационного экзамена по компетенции №39«Сетевое и системное администрирование» по КОД № 2.1 профессиональным компетенциям, основным видам деятельности, предусмотренным ФГОС СПО и уровням квалификаций в соответствии с профессиональными стандартами

Уровень аттестации (промежуточная/ ГИА)	Код и наименование ФГОС СПО	Основные виды деятельности ФГОС СПО (ПМ)	Профессиональные компетенции (ПК) ФГОС СПО	Наименование профессионального стандарта (ПС)	Наименование и уровень квалификаций ПС	WSSS/модули/критерии оценки по КОД (по решению разработчика)
Комплект оценочной документации №2.1, продолжительность 12 час., максимально возможный балл - 75б.						
ГИА	09.01.02 Наладчик компьютерных сетей	4.3.1. Выполнение работ по монтажу, наладке, эксплуатации и обслуживанию локальных компьютерных сетей. 4.3.2. Выполнение работ по подключению к глобальным компьютерным сетям. 4.3.3. Обеспечение информационной безопасности компьютерных сетей.	ПК 1.1. Осуществлять монтаж кабельной сети и оборудования локальных сетей различной топологии. ПК 1.2. Осуществлять настройку сетевых протоколов серверов и рабочих станций. ПК 1.3. Выполнять работы по эксплуатации и обслуживанию сетевого оборудования. ПК 1.4. Обеспечивать работу системы регистрации и авторизации пользователей сети. ПК 1.5. Осуществлять системное администрирование локальных сетей. ПК 2.1.		Мониторинг СКС с целью локализации неисправностей, 4	

			Устанавливать и настраивать подключения к сети Интернет с помощью различных технологий и специализированного оборудования. ПК 2.2. Осуществлять выбор технологии подключения и тарифного плана у провайдера доступа к сети Интернет. ПК 2.3. Устанавливать специализированные программы и драйверы, осуществлять настройку параметров подключения к сети Интернет. ПК 2.4. Осуществлять управление и учет входящего и исходящего трафика сети. ПК 2.5. Интегрировать локальную сеть в сеть Интернет. ПК 2.6. Устанавливать и настраивать программное обеспечение серверов сети Интернет. ПК 3.1. Обеспечивать резервное копирование данных. ПК			

			3.2. Осуществлять меры по защите компьютерных сетей от несанкционированного доступа. ПК 3.3. Применять специализированные средства для борьбы с вирусами, несанкционированными рассылками электронной почты, вредоносными программами. ПК 3.4. Осуществлять мероприятия по защите персональных данных.			
промежуточная/ ГИА	09.02.02 Компьютерные сети	4.3. Техник по компьютерным сетям готовится к следующим видам деятельности: 4.3.1. Участие в проектировании сетевой инфраструктуры. 4.3.2. Организация сетевого администрирования 4.3.3. Эксплуатация объектов сетевой инфраструктуры. 4.3.4. Выполнение работ по одной или	5.2.1. Участие в проектировании 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.	Приказ Минтруда России от 05.10.2015 N 684н"Об утверждении профессионального стандарта "Системный администратор информационно-коммуникационных систем"	Администрирование прикладного программного обеспечения инфокоммуникационной системы организации, Управление программно-аппара тными средствами информационных служб инфокоммуникацио нной системы организации, Администрирование сетевой	

		нескольким профессиям рабочих, должностям служащих (приложение к настоящему ФГОС СПО). 4.4. Специалист по администрированию сети готовится к следующим видам деятельности: 4.4.1. Участие в проектировании сетевой инфраструктуры. 4.4.2. Организация сетевого администрирования 4.4.3. Эксплуатация объектов сетевой инфраструктуры. 4.4.4. Управление сетевыми сервисами. 4.4.5. Участие в модернизации сетевой инфраструктуры.	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. 5.2.2. Организация сетевого администрирования. ПК 2.1. Администрировать локальные вычислительные сети и принимать меры по		подсистемы инфокоммуникацио нной системы организации, Администрировани е системного программного обеспечения инфокоммуникацио нной системы организации, Управление развитием инфокоммуникацио нной системы организации,	

		4.4.6. Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих (приложение к настоящему ФГОС СПО).	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. 5.2.3. 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. Эксплуатация сетевых конфигураций. ПК 3.4. Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации. 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. 5.4.4. Управление сетевыми сервисами. ПК 4.1. Принимать меры по отслеживанию, предотвращению и устранению нештатных ситуаций. ПК 4.2. Контролировать сетевую инфраструктуру с использованием инструментальных средств эксплуатации сетевых конфигураций. ПК 4.3. Обеспечивать максимальную стабильность предоставляемых сетевых сервисов. ПК 4.4. Предоставлять согласованные с информационно-технологическими подразделениями сетевые сервисы и			

			выполнять необходимые процедуры поддержки. ПК 4.5. Восстанавливать нормальную работу сетевых сервисов в соответствии с требованиями регламентов. ПК 4.6. Вести учет плановой потребности в расходных материалах и комплектующих. 5.4.5. Участие в модернизации сетевой инфраструктуры. ПК 5.1. Идентифицировать проблемы в процессе эксплуатации программного обеспечения. ПК 5.2. Разрабатывать предложения по совершенствованию и повышению эффективности работы сетевой инфраструктуры. ПК 5.3. Разрабатывать сетевые топологии в соответствии с			

			требованиями отказоустойчивости и повышения производительности корпоративной сети. ПК 5.4. Составлять отчет по выполненному заданию, участвовать во внедрении результатов разработок. ПК 5.5. Проводить эксперименты по заданной методике, выполнять анализ результатов. 5.4.6. Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих.			
ГИА	09.02.06 Сетевое и системное администрирование	Выполнение работ по проектированию сетевой инфраструктуры Организация сетевого администрирования Эксплуатация объектов сетевой инфраструктуры	3.4.1. Выполнение работ по проектированию сетевой инфраструктуры: ПК 1.1. Выполнять проектирование кабельной структуры компьютерной сети. ПК 1.2. Осуществлять выбор технологии,	Приказ Минтруда России от 05.10.2015 N 684н "Об утверждении профессионального стандарта "Системный администратор информационно-коммуникационных систем"	Администрирование прикладного программного обеспечения инфокоммуникационной системы организации, Управление программно-аппаратными	

		Управление сетевыми сервисами Сопровождение модернизации сетевой инфраструктуры	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.		средствами информационных служб инфокоммуникационной системы организации, Администрирование сетевой подсистемы инфокоммуникационной системы организации, Администрирование системного программного обеспечения инфокоммуникационной системы организации, Управление развитием инфокоммуникационной системы организации,	

			3.4.2. 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.			

			3.4.3. 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 копирование информации.			

			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. 3.4.4. Управление сетевыми сервисами: ПК 4.1. Принимать меры по отслеживанию, предотвращению и устранению нештатных ситуаций. ПК 4.2. Контролировать сетевую инфраструктуру с использованием инструментальных средств эксплуатации сетевых конфигураций.			

			ПК 4.3. Обеспечивать максимальную стабильность предоставляемых сетевых сервисов. ПК 4.4. Представлять согласованные с информационно-технологическими подразделениями сетевые сервисы и выполнять необходимые процедуры поддержки. ПК 4.5. Восстанавливать нормальную работу сетевых сервисов в соответствии с требованиями регламентов. ПК 4.6 Вести учет плановой потребности в расходных материалах и комплектующих. 3.4.5. Сопровождение модернизации сетевой инфраструктуры; ПК 5.1. Идентифицировать проблемы в процессе эксплуатации			

			программного обеспечения. ПК 5.2. Разрабатывать предложения по совершенствованию и повышению эффективности работы сетевой инфраструктуры. ПК 5.3. Разрабатывать сетевые топологии в соответствии с требованиями отказоустойчивости и повышения производительности корпоративной сети. ПК 5.4. Составлять отчет по выполненному заданию, участвовать во внедрении результатов разработок. ПК 5.5. Проводить эксперименты по заданной методике, выполнять анализ результатов.			
промежуточная/ ГИА	09.02.07 Информационные	Сопровождение и обслуживание программного	3.4.4. Сопровождение и обслуживание программного	Приказ Минтруда России от 05.10.2015 N	Администрирование прикладного программного	

	системы и программирование	обеспечения компьютерных систем Сопровождение информационных систем Администрирование информационных ресурсов	обеспечения компьютерных систем: ПК 4.1. Осуществлять инсталляцию, настройку и обслуживание программного обеспечения компьютерных систем. ПК 4.2. Осуществлять измерения эксплуатационных характеристик программного обеспечения компьютерных систем. ПК 4.3. Выполнять работы по модификации отдельных компонент программного обеспечения в соответствии с потребностями заказчика. ПК 4.4. Обеспечивать защиту программного обеспечения компьютерных систем программными средствами.	684н"Об утверждении профессионального стандарта "Системный администратор информационно-коммуникационных систем"	обеспечения инфокоммуникацио нной системы организации,	

			3.4.6. Сопровождение информационных систем: ПК 6.1. Разрабатывать техническое задание на сопровождение информационной системы. ПК 6.2. Выполнять исправление ошибок в программном коде информационной системы. ПК 6.4. Оценивать качество и надежность функционирования информационной системы в соответствии с критериями технического задания. ПК 6.5. Осуществлять техническое сопровождение, обновление и восстановление данных информационной системы в соответствии с техническим заданием.			

			3.4.10.Администрирование информационных ресурсов: ПК 10.1. Обрабатывать статический и динамический информационный контент.			
промежуточная	10.02.02 Информационная безопасность телекоммуникационных систем	4.3.1. Техническое обслуживание оборудования защищенных телекоммуникационных систем. 4.3.2. Применение программно-аппаратных, инженерно-технических методов и средств обеспечения информационной безопасности телекоммуникационных систем. 4.3.3. Участие в организации работ по обеспечению информационной безопасности телекоммуникационных систем.	ПК 1.1. Устанавливать, конфигурировать оборудование защищенных телекоммуникационных систем. ПК 1.2. Эксплуатировать оборудование защищенных телекоммуникационных систем. ПК 2.1. Осуществлять установку (монтаж), настройку (наладку) и запуск в эксплуатацию программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности телекоммуникационных систем. ПК 2.2. Обеспечивать эксплуатацию и содержание в	Приказ Минтруда России от 05.10.2015 N 684н "Об утверждении профессионального стандарта "Системный администратор информационно-коммуникационных систем	Администрирование сетевой подсистемы инфокоммуникационной системы организации	

			работоспособном состоянии программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности телекоммуникационных систем, их диагностику, обнаружение отказов, формировать предложения по их устранениюпринадлежностей. ПК 3.3. Участвовать во внедрении разработанных технических решений и проектов во взаимодействии с другими специалистами, оказывать техническую помощь исполнителям при изготовлении, монтаже, настройке, испытаниях и эксплуатации технических средств.			
промежуточная/ ГИА	10.02.03 Информационная безопасность автоматизир	4.3.1. Эксплуатация подсистем безопасности автоматизированных систем. 4.3.2. Применение программно-	ПК 1.1. Участвовать в эксплуатации компонентов подсистем безопасности автоматизированных систем, в проверке их технического состояния,	Приказ Минтруда России от 05.10.2015 N 684н"Об утверждении профессионального стандарта "Системный администратор	Администрировани е сетевой подсистемы инфокоммуникацио нной системы организации	

	ованных систем	аппаратных средств обеспечения информационной безопасности в автоматизированных системах. 4.3.3. Применение инженерно-технических средств обеспечения информационной безопасности.	в проведении технического обслуживания и текущего ремонта, устранении отказов и восстановлении работоспособности. ПК 1.2. Выполнять работы по администрированию подсистем безопасности автоматизированных систем. ПК 1.3. Производить установку и адаптацию компонентов подсистем безопасности автоматизированных систем. ПК 2.1. Применять программно-аппаратные средства обеспечения информационной безопасности в автоматизированных системах. ПК 2.2. Участвовать в эксплуатации программно-аппаратных средств обеспечения информационной безопасности, в проверке их технического состояния, в проведении технического обслуживания и	информационно-коммуникационных систем		

			текущего ремонта, устранении отказов и восстановлении работоспособности. ПК 2.3. Участвовать в мониторинге эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в автоматизированных системах.			
промежуточная/ ГИА	10.02.05 Обеспечение информационной безопасности автоматизированных систем	Эксплуатация автоматизированных (информационных) систем в защищенном исполнении; Защита информации в автоматизированных системах программными и программно-аппаратными средствами	ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации. ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами. ПК 2.4. Осуществлять обработку, хранение и	06.030 Профессиональный стандарт «Специалист по защите информации в телекоммуникационных системах и сетях», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 3 ноября 2016 г. № 608н (зарегистрирован Министерством юстиции Российской Федерации 25 ноября 2016 г., регистрационный № 44449) 06.032 Профессиональный	Выполнение комплекса мер по обеспечению функционирования СССЭ исключением сетей связи специального назначения) и средств их защиты от НСД, 5 Обслуживание средств защиты информации в компьютерных системах и сетях, Обслуживание систем защиты информации в	

			передачу информации ограниченного доступа. ПК 3.2. Осуществлять эксплуатацию технических средств защиты информации в соответствии с требованиями эксплуатационной документации.	стандарт «Специалист по безопасности компьютерных систем и сетей», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. № 598н (зарегистрирован Министерством юстиции Российской Федерации 28 ноября 2016 г., регистрационный № 44464) 06.033 Профессиональный стандарт «Специалист по защите информации в автоматизированных системах», утвержден приказом Министерства труда и социальной зашиты Российской Федерации от 15 сентября 2016 г. № 522н (зарегистрирован Министерством юстиции Российской Федерации 28 сентября 2016 г., регистрационный № 43857)	автоматизированных системах, 5	

промежуточная/ ГИА	10.05.02 Информационная безопасность телекоммуникационных систем	эксплуатационная	способностью выполнять установку, настройку, обслуживание, диагностику, эксплуатацию и восстановление работоспособности телекоммуникационного оборудования и приборов, технических и программно-аппаратных средств защиты телекоммуникационных сетей и систем (ПК-14); способностью проводить инструментальный мониторинг защищенности телекоммуникационных систем, обеспечения требуемого качества обслуживания (ПК-15).	06.030 Профессиональный стандарт «Специалист по защите информации в телекоммуникационных системах и сетях», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 3 ноября 2016 г. № 608н (зарегистрирован Министерством юстиции Российской Федерации 25 ноября 2016 г., регистрационный № 44449) 06.032 Профессиональный стандарт «Специалист по безопасности компьютерных систем и сетей», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. № 598н (зарегистрирован Министерством юстиции Российской Федерации 28 ноября 2016 г.,	Выполнение комплекса мер по обеспечению функционирования СССЭ исключением сетей связи специального назначения) и средств их защиты от НСД, Обслуживание средств защиты информации в компьютерных системах и сетях, Обслуживание систем защиты информации в автоматизированных системах, 5	

				регистрационный № 44464) 06.033 Профессиональный стандарт «Специалист по защите информации в автоматизированных системах», утвержден приказом Министерства труда и социальной зашиты Российской Федерации от 15 сентября 2016 г. № 522н (зарегистрирован Министерством юстиции Российской Федерации 28 сентября 2016 г., регистрационный № 43857)		
промежуточная	10.02.04 Обеспечение информационной безопасности телекоммуникационных систем	4.3.3. Участие в организации работ по обеспечению информационной безопасности телекоммуникационных систем.	ПК 3.3. Участвовать во внедрении разработанных технических решений и проектов во взаимодействии с другими специалистами, оказывать техническую помощь исполнителям при изготовлении, монтаже, настройке, испытаниях и эксплуатации технических средств.	06.030 Профессиональный стандарт «Специалист по защите информации в телекоммуникационных системах и сетях», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 3 ноября 2016 г. № 608н (зарегистрирован Министерством юстиции Российской	Выполнение комплекса мер по обеспечению функционирования СССЭ исключением сетей связи специального назначения) и средств их защиты от НСД, Обслуживание средств защиты информации в компьютерных	

				Федерации 25 ноября 2016 г., регистрационный № 44449) 06.032 Профессиональный стандарт «Специалист по безопасности компьютерных систем и сетей», утвержден приказом Министерства труда и социальной защиты Российской Федерации от 1 ноября 2016 г. № 598н (зарегистрирован Министерством юстиции Российской Федерации 28 ноября 2016 г., регистрационный № 44464) 06.033 Профессиональный стандарт «Специалист по защите информации в автоматизированных системах», утвержден приказом Министерства труда и социальной зашиты Российской Федерации от 15 сентября 2016 г. № 522н (зарегистрирован Министерством	системах и сетях, Обслуживание систем защиты информации в автоматизированных системах,	

				юстиции Российской Федерации 28 сентября 2016 г., регистрационный № 43857)		
промежуточная/ ГИА	11.02.11 Сети связи и системы коммутации	4.3.1. Техническая эксплуатация информационно-коммуникационных сетей связи. 4.3.2. Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи. 4.3.3. Техническая эксплуатация телекоммуникационных систем.	ПК 1.1. Выполнять монтаж и производить настройку сетей проводного и беспроводного абонентского доступа. ПК 1.2. Осуществлять работы с сетевыми протоколами. ПК 1.4. Выполнять монтаж и первичную инсталляцию компьютерных сетей. ПК 1.6. Производить администрирование сетевого оборудования. ПК 2.1. Использовать программно-аппаратные средства защиты информации в телекоммуникационных системах и сетях связи. ПК 2.2. Применять системы анализа защищенности для обнаружения уязвимости	Приказ Минтруда России от 05.10.2015 N 684н"Об утверждении профессионального стандарта "Системный администратор информационно-коммуникационных систем"	Администрирование прикладного программного обеспечения инфокоммуникацио нной системы организации, Управление программно-аппара тными средствами информационных служб инфокоммуникацио нной системы организации, Администрирование сетевой подсистемы инфокоммуникацио нной системы организации, Администрирование системного программного обеспечения инфокоммуникационной	

			в сетевой инфраструктуре, выдавать рекомендации по их устранению. ПК 2.3. Обеспечивать безопасное администрирование телекоммуникационных систем и информационно-коммуникационных сетей связи. ПК 3.1. Выполнять монтаж оборудования телекоммуникационных систем. ПК 3.2. Проводить мониторинг и диагностику телекоммуникационных систем. ПК 3.3. Управлять данными телекоммуникационных систем. ПК 3.4. Устранять аварии и повреждения оборудования телекоммуникационных систем, выбирать		системы организации, Управление развитием инфокоммуникацио нной системы организации,	

			методы восстановления его работоспособности. ПК 3.5. Выполнять монтаж и обеспечивать работу линий абонентского доступа и оконечных абонентских устройств. ПК 3.6. Решать технические задачи в области эксплуатации телекоммуникационных систем.			

Задание для демонстрационного экзамена по комплекту оценочной документации № 2.1 по компетенции № «Сетевое и системное администрирование (образец)

Задание включает в себя следующие разделы:

1. Формы участия
2. Модули задания, критерии оценки и необходимое время
3. Необходимые приложения

Продолжительность выполнения задания: 12 ч.

1. ФОРМЫ УЧАСТИЯ

Индивидуальный.

2. МОДУЛИ ЗАДАНИЯ И НЕОБХОДИМОЕ ВРЕМЯ

Модули и время приедены в таблице 1

Таблица 1 – Время выполнение модуля

п/п	**Критерий**	**Модуль, в котором используется критерий**	**Время на выполнения модуля**	**Проверяемые разделы WSSS**	**Баллы**		
					Судейская (если это применимо)	**Объективная**	**Общая**
1	A Linux Environments	A Linux Enviroments	4 часа	6	0	25	25
2	B Windows Environments	B Windows Enviroments	4 часа	1, 4, 5	0	25	25
3	C Cisco Environments	C Cisco Enviroments	4 часа	7	0	25	25
				Итого =	**0**	**75**	**75**

Модуль A: «Пуско-наладка инфраструктуры на основе ОС семейства Linux»
Версия 1 от 01.04.19.

ВВЕДЕНИЕ

Умение работать с системами на основе открытого исходного кода становится все более важным навыком для тех, кто желает построить успешную карьеру в ИТ. Данное экзаменационное задание содержит множество задач, основанных на опыте реальной эксплуатации информационных систем, в основном, интеграции и аутсорсинге. Если вы можете выполнить задание с высоким результатом, то вы точно сможете обслуживать информационную инфраструктуру большого предприятия.

Описание экзаменационного задания

Данное экзаменационное задание разработано с использованием различных открытых технологий, с которыми вы должны быть знакомы по сертификационным курсам LPIC и Red Hat. Задания поделены на следующие секции:

- Базовая конфигурация
- Конфигурация сетевой инфраструктуры
- Службы централизованного управления и журналирования
- Конфигурация служб удаленного доступа
- Конфигурация веб- и почтовых служб
- Конфигурация служб хранения данных
- Конфигурация параметров безопасности и служб аутентификации

Секции независимы друг от друга, но вместе они образуют достаточно сложную инфраструктуру. Некоторые задания достаточно просты и понятны, некоторые могут быть неочевидными. Можно заметить, что некоторые технологии должны работать в связке или поверх других технологий. Например, динамическая маршрутизация должна выполнять поверх настроенного между организациями туннеля. Важно понимать, что если вам не удалось настроить полностью технологический стек, то это не означает что работа не будет оценена. Например, для удаленного доступа необходимо настроить IPsec-туннель, внутри которого организовать GRE-туннель. Если, например, вам не удалось настроить IPsec, но вы смогли настроить GRE, то вы все еще получите баллы за организацию удаленного доступа.

Инструкции для участника

В первую очередь необходимо прочитать задание полностью. Следует обратить внимание, что задание составлено не в хронологическом порядке. Некоторые секции могут потребовать действий из других секций, которые изложены ниже. Например, задание 6 в секции «Базовая конфигурация» предписывает автоматизировать удаленный доступ, который, разумеется, не будет работать без предварительной конфигурации, изложенной в секции «Маршрутизация и удаленный доступ». На вас возлагается ответственность за распределение своего рабочего времени. Не тратьте время, если у вас возникли проблемы с некоторыми заданиями. Вы можете использовать временные решения (если у вас есть зависимости в технологическом

стеке) и продолжить выполнение других задач. Рекомендуется тщательно проверять результаты своей работы.

Доступ ко всем виртуальным машинам настроен по аккаунту root:toor.

Если Вам требуется установить пароль, не указанный в задании используйте: P@ssw0rd

Виртуальная машина ISP преднастроена. Управляющий доступ участника к данной виртуальной машине для выполнения задания не предусмотрен. При попытке его сброса возникнут проблемы.

Организация LEFT включает виртуальные машины: L-SRV, L-FW, L-RTR-A, L-RTR-B, L-CLI-A, L-CLI-B.

Организация RIGHT включает виртуальные машины: R-SRV, R-FW, R-RTR, R-CLI.

НЕОБХОДИМОЕ ОБОРУДОВАНИЕ, ПРИБОРЫ, ПО И МАТЕРИАЛЫ

Ожидается, что экзаменационное задание выполнимо Участником с привлечением оборудования и материалов, указанных в Инфраструктурном Листе.

В качестве системной ОС в организации LEFT используется Debian

В качестве системной ОС в организации RIGHT используется CentOS

Вам доступен диск CentOS-7-x86_64-Everything-XXXX.iso

Вам доступен диск debian-9.X.0-amd64-BD-1.iso

Вам доступен диск debian-9.X.0-amd64-BD-2.iso

Вам доступен диск AdditionalPackages.iso, на котором располагаются недостающие RPM и deb пакеты

Внимание! Все указанные компоненты предоставляются участникам в виде ISO-файлов на локальном или удаленном хранилище.

Участники не имеют права пользоваться любыми устройствами, за исключением находящихся на рабочих местах устройств, предоставленных организаторами.

Участники не имеют права приносить с собой на рабочее место заранее подготовленные текстовые материалы.

В итоге участники должны обеспечить наличие и функционирование в соответствии с заданием служб и ролей на указанных виртуальных машинах. При этом участники могут самостоятельно выбирать способ настройки того или иного компонента, используя предоставленные им ресурсы по своему усмотрению.

Необходимое Оборудование, приборы, ПО и материалы

Ожидается, что экзаменационное задание выполнимо Участником с привлечением оборудования и материалов, указанных в Инфраструктурном Листе.

В качестве Системной ОС используется **CentOS 7**

Вам доступен диск CentOS-7-x86_64-Everything-XXXX.iso

Вам доступен диск AdditionalPackages.iso на котором располагаются недостающие RPM пакеты

Схема оценки

Каждый субкритерий имеет приблизительно одинаковый вес. Пункты внутри каждого критерия имеют разный вес, в зависимости от сложности пункта и количества пунктов в субкритерии.

Схема оценка построена таким образом, чтобы каждый пункт оценивался только один раз. Например, в секции «Базовая конфигурация» предписывается настроить имена для всех устройств, однако этот пункт будет проверен только на одном устройстве и оценен только 1 раз. Одинаковые пункты могут быть проверены и оценены больше чем 1 раз, если для их выполнения применяются разные настройки или они выполняются на разных классах устройств.

Подробное описание методики проверки должно быть разработано экспертами, принимающими участие в оценке экзаменационного задания, и вынесено в отдельный документ. Данный документ, как и схема оценки, является объектом внесения 30% изменений.

Конфигурация хостов

1) Настройте имена хостов в соответствии с диаграммой.
2) Установите следующее ПО на ВСЕ виртуальные машины:
    a. Пакет tcpdump
    b. Пакет net-tools
    c. Редактор vim
    d. lynx
    e. dhclient
    f. bind-utils
    g. nfs-utils
    h. cifs-utils
3) На хостах сформируйте файл /etc/hosts в соответствии с диаграммой (кроме адреса хоста L-CLI-A). Данный файл будет применяться во время проверки в случае недоступности DNS-сервисов. Проверка по IP-адресам выполняться не будет.
4) В случае корректной работы DNS-сервисов ответы DNS должны иметь более высокий приоритет.

Конфигурация сетевой инфраструктуры

1) Настройте IP-адресацию на ВСЕХ хостах в соответствии с **диаграммой**.
2) Настройте сервер протокола динамической конфигурации хостов для L-CLI-A и L-CLI-B
    a. В качестве DHCP-сервера организации LEFT используйте L-RTR-A
        i. Используйте пул адресов 172.16.100.60 — 172.16.100.75 для сети L-RTR-A
        ii. Используйте пул адресов 172.16.200.60 — 172.16.200.75 для сети L-RTR-B
        iii. Используете адрес L-SRV в качестве адреса DNS-сервера
    b. Настройте DHCP-сервер таким образом, чтобы L-CLI-B всегда получал фиксированный IP-адрес в соответствии с **диаграммой.**

c. В качестве шлюза по умолчанию используйте адрес интерфейса соответствующего маршрутизатора в локальной сети

d. Используйте DNS-суффикс **skill39.wsr**

e. DNS-записи типа A соответствующего хоста должны обновляться при получении им адреса от DHCP-сервера.

3) На L-SRV настройте службу разрешения доменных имен

a. Сервер должен обслуживать зону **skill39.wsr**

b. Сопоставление имен организовать в соответствии с **Таблицей 1**

c. Настройте на R-SRV роль вторичного DNS сервера для зоны **skill39.wsr**

i. Используете адрес R-SRV в качестве адреса DNS-сервера для R-CLI

d. Запросы, которые выходят за рамки зоны **skill39.wsr** должны пересылаться DNS-серверу ISP. Для проверки используйте доменное имя ya.ru.

e. Реализуйте поддержку разрешения обратной зоны.

f. Файлы зон располагать в **/opt/dns/**

g. Делегируйте поддомен ext.skill39.wsr серверу ISP.

4) На L-FW настройте интернет-шлюз для организации коллективного доступа в интернет.

a. Настройте трансляцию сетевых адресов из внутренней сети в адрес внешнего интерфейса.

b. Организуйте доступность сервиса DNS на L-SRV по внешнему адресу L-FW.

c. Сервер L-FW должен перенаправлять внешние DNS запросы от OUT-CLI на L-SRV. Важно преобразовывать только www.skill39.wsr во внешний адрес R-FW.

Службы централизованного управления и журналирования

1) Разверните LDAP-сервер для организации централизованного управления учетными записями

a. В качестве сервера выступает L-SRV

b. Учетные записи создать в соответствии с **Таблицей 2**.

c. Группы и пользователей создать в соответствии с **Таблицей 2**

d. Пользователи должны быть расположены в OU Users

e. Группы должны быть расположены в OU Groups

f. L-SRV, L-CLI-A и L-CLI-B должны аутентифицироваться через LDAP

g. Только группы Admin и Guest могут аутентифицироваться на клиентах

2) Реализуйте централизованное хранение домашних каталогов пользователей LDAP

a. Сервером домашних каталогов выступает L-SRV

b. Подключите 4 диска по 1Гб и объедините их в RAID5 используйте файловую систему ext4

c. Хранение домашних каталогов выполнять в /opt/homes/ монтируемой с собранного RAID5 массива

d. Определите квоту на хранение в 10 MB

e. Доступ к каталогам осуществлять по протоколу NFS

3) На L-SRV организуйте централизованный сбор журналов с хостов L-CLI-A, R-CLI, L-FW, L-SRV, R-RTR

a. Журналы должны храниться в директории **/opt/logs/**

b. Журналирование должно производится в соответствии с **Таблицей 3.**

c. Размеры файлов логов не должны превышать **10Кб**.

d. Должна быть настроена циклическая запись журналов, не более 10 файлов для каждого лога.

Конфигурация служб удаленного доступа

1) На L-FW настройте сервер удаленного доступа на основе технологии OpenVPN:

a. В качестве сервера выступает L-FW

b. Параметры туннеля

i. Устройство TUN

ii. Протокол UDP

iii. Применяется сжатие

iv. Порт сервера 1122

c. Ключевая информация должна быть сгенерирована на R-FW

d. Должна быть реализована аутентификация средствами LDAP-сервера, развернутого на L-SRV

i. Только LDAP-пользователи в группе VPN должны получать доступ к VPN-службе

e. В качестве адресного пространства подключаемых клиентов использовать сеть 5.5.5.0/27

f. Хранение всей необходимой (кроме конфигурационных файлов) информации организовать в **/opt/vpn**

2) На OUT-CLI настройте клиент удаленного доступа на основе технологии OpenVPN:

a. Запуск удаленного подключения должен выполняться скриптом **start_vpn.sh**

i. Скрипт принимает на вход следующие параметры(последовательно):

1. Имя пользователя OpenVPN
2. Пароль в открытом виде

ii. Отключение VPN-туннеля должно выполняться скриптом **stop_vpn.sh**

iii. Скрипты должны располагаться в **/opt/vpn**.

iv. Скрипты должны вызываться из любого каталога без указания пути

v. Используйте следующий каталог для расположения файлов скриптов **/opt/vpn/start_vpn.sh**

3) Настройте защищенный канал передачи данных между L-FW и R-FW с помощью технологии IPSEC:

a. Параметры политики первой фазы IPSec:

i. Проверка целостности SHA-1

ii. Шифрование 3DES

iii. Группа Диффи-Хелмана — 14 (2048)

iv. Аутентификация по общему ключу WSR-2018

b. Параметры преобразования трафика для второй фазы IPSec:

i. Протокол ESP
ii. Шифрование AES
iii. Проверка целостности SHA-2

c. В качестве трафика, разрешенного к передаче через IPsec-туннель, должен быть указан только GRE-трафик между L-FW и R-FW

4) Настройте GRE-туннель между L-FW и R-FW:
   a. Используйте следующую адресацию внутри GRE-туннеля:
      i. L-FW: 10.5.5.1/30
      ii. R-FW: 10.5.5.2/30
5) Настройте динамическую маршрутизацию по протоколу OSPF с использованием пакета Quagga:
   a. Анонсируйте все сети, необходимые для достижения полной связности
   b. Применение статических маршрутов не допускается
   c. В обмене маршрутной информацией участвуют L-RTR-A, L-RTR-B, R-RTR, L-FW и R-FW
   d. Соседство и обмен маршрутной информацией между L-FW и R-FW должно осуществляться исключительно через настроенный GRE-туннель
   e. Анонсируйте сети локальных интерфейсов L-RTR-A и L-RTR-B.
6) На L-FW настройте удаленный доступ по протоколу SSH:
   a. Доступ ограничен пользователями **ssh_p** и **ssh_c**
      i. В качестве пароля использовать **ssh_pass**
   b. SSH-сервер должен работать на порту **1022**
7) На OUT-CLI настройте клиент удаленного доступа SSH:
   a. Доступ к серверу L-FW должен происходить автоматически по правильному порту, без его явного указания номера порта в команде подключения
   b. Для других серверов по умолчанию должен использоваться порт **22**
   c. Доступ к L-FW под учетной записью **ssh_p** должен происходить с помощью аутентификации на основе открытых ключей.

Конфигурация веб- и почтовых служб

1) На R-SRV установите и настройте веб-сервер apache:
    a. Настройте веб-сайт для внешнего пользования www.skill39.wsr
        i. Используйте директорию **/var/www/html/out**
        ii. Используйте порт 8088
    b. Настройте веб-сайт для внутреннего пользования intra.skill39.wsr
        i. Используйте директорию **/var/www/html/intra**
        ii. Обеспечьте работу сайтов по протоколам http и https (сертификат должен быть сгененрирован на R-FW)
        iii. В случае доступности https должен происходить автоматическое перенаправление с http
2) На R-FW настройте пакет HAProxy
    a. Сайт www.skill39.wsr должен быть доступен из внешней сети по внешнему адресу R-FW
    b. Настройте SSL

Конфигурация служб хранения данных

1) Создайте LVM-том на R-RTR и разместите на нём каталог **/opt/lvm**
    a. Виртуальные диски для размещения LVM-тома создайте самостоятельно
    b. Обеспечьте создание снапшотов по расписанию раз в час с именем <Date>.<Time>
        i. Убедитесь, что на время проверки хотя бы один снапшот создан

Конфигурация параметров безопасности и служб аутентификации

1) Настройте CA на R-FW, используя OpenSSL.
    a. Используйте **/etc/ca** в качестве корневой директории CA
    b. Атрибуты CA должны быть следующими:
        i. Страна RU
        ii. Организация WorldSkills Russia
        iii. CN должен быть установлен как WSR CA
    c. Создайте корневой сертификат CA

d. Все клиентские операционные системы должны доверять CA

3) Настройте межсетевой экран **iptables** на L-FW и R-FW

a. Запретите прямое попадание трафика из сетей в **Internal**

b. Разрешите удаленные подключения с использованием OpenVPN на внешний интерфейс маршрутизатора L-FW

c. Разрешите необходимый трафик для создания IPSec и GRE туннелей между организациями

d. Разрешите SSH подключения на соответствующий порт

e. Для VPN-клиентов должен быть предоставлен полный доступ к сети **Internal**

f. Разрешите необходимый трафик к серверам L-SRV и R-SRV по транслированным IP-адресам

g. Настройте ограничение доступа к сайту www.skill39.wsr при подключении по Remote-Access VPN. Разрешите доступ только к intra.wsr.right

h. Остальные сервисы следует запретить.

i. В отношении входящих (из внешней сети) ICMP запросов поступать по своему усмотрению

Таблица 1 – DNS-имена

Хост	**DNS-имя**
L-CLI-A	A,PTR: l-cli-a.skill39.wsr
L-CLI-B	A,PTR: l-cli-b.skill39.wsr
L-RTR-A	A: l-rtr-a.skill39.wsr
L-RTR-B	A: l-rtr-b.skill39.wsr
L-SRV	A,PTR: l-srv.skill39.wsr CNAME: server.skill39.wsr CNAME: center.skill39.wsr
L-FW	A: l-fw.skill39.wsr CNAME: vpn.skill39.wsr
R-FW	A: r-fw.skill39.wsr
R-SRV	A,PTR: r-srv.skill39.wsr CNAME: intra.skill39.wsr
R-RTR	A,PTR: r-rtr.skill39.wsr
R-CLI	A: r-cli.skill39.wsr

Таблица 2 – Учетные записи LDAP

Группа	**CN**	**Пароль**	**Доступ**
Admin	tux	toor	L-SRV, L-CLI-A L-CLI-B
Guest	user1 – **user99**	P@ssw0rd	L-CLI-A L-CLI-B
VPN	vpn1 – vpn99	Passw0rd	только для VPN
webuser	webuser1 – webuser99	P@ssword	только для доступа к сайту intra.skill39.wsr

Таблица 3 – Правила журналирования

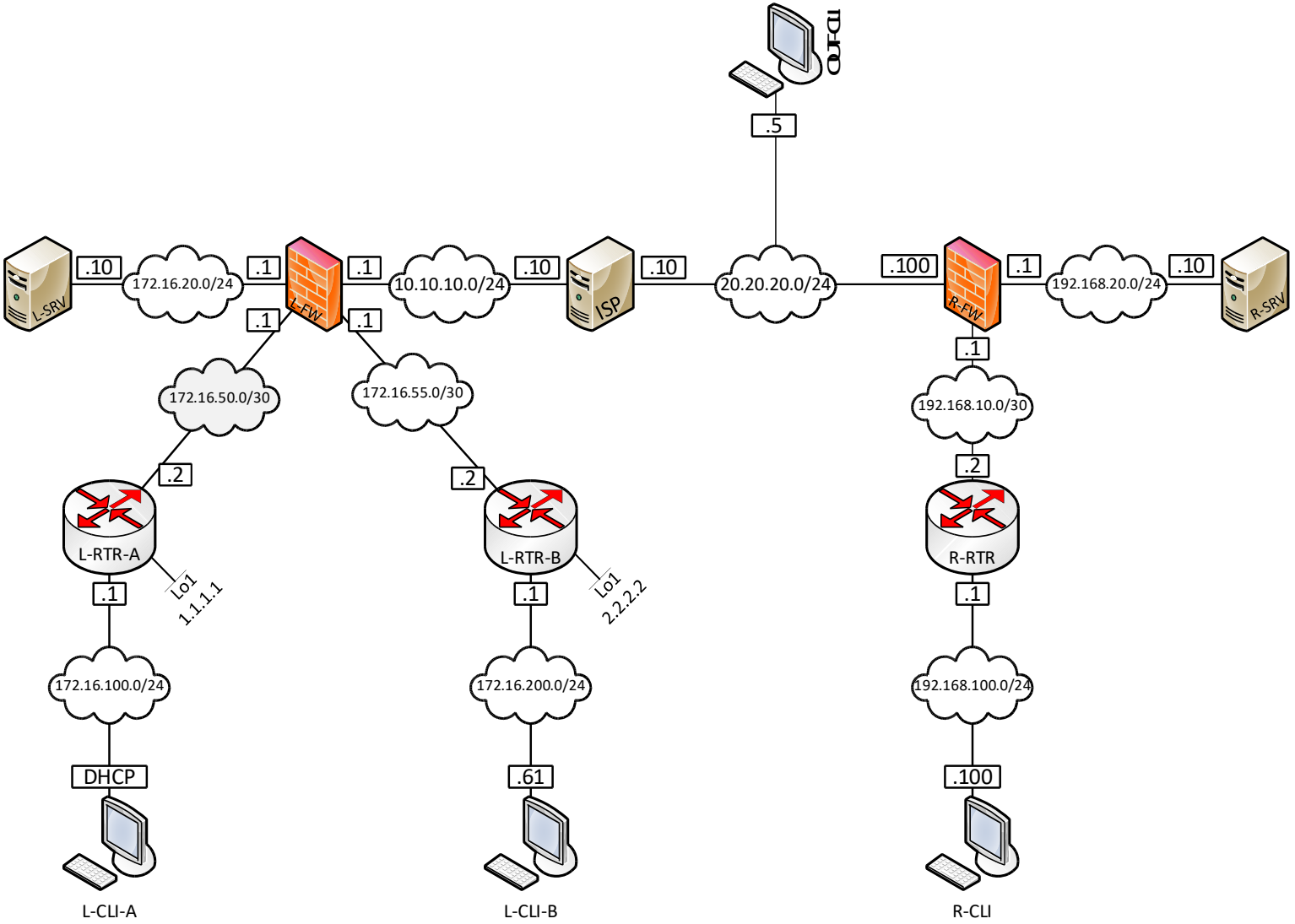
Источник	**Уровень журнала (строгое соответствие)**	**Файл**
Все хосты	critical	/opt/logs/<HOSTNAME>/crit.log

L-SRV	auth.*	/opt/logs/<HOSTNAME>/auth.log
L-FW	*.err	/opt/logs/<HOSTNAME>/error.log
R-RTR	alert	/opt/logs/<HOSTNAME>/alert.log
Все клиенты	*.err	/opt/logs/err.log

*<HOSTNAME> - название директории для журналируемого хоста

**В директории /opt/logs/ не должно быть файлов, кроме тех, которые указаны в таблице

ДИАГРАММА ВИРТУАЛЬНОЙ СЕТИ



Модуль B: «Пуско-наладка инфраструктуры на основе ОС семейства Windows»

Версия 1 от 01.04.19

ВВЕДЕНИЕ

На выполнение задания отводится ограниченное время – подумайте, как использовать его максимально эффективно. Составьте план выполнения работ. Вполне возможно, что для полной работоспособности системы в итоге действия нужно выполнять не строго в той последовательности, в которой они описаны в данном экзаменационном задании.

В рамках легенды экзаменационного задания Вы – системный администратор вновь создаваемой московской компании. Вам необходимо настроить сервисы в локальной сети головного офиса.

Также учтите, что компания приобрела одно из малых предприятий в Ижевске. В ижевском офисе сеть уже функционировала, но системный администратор (из-за скандала при увольнении) не предоставил доступа к действующему там контроллеру домена. Вам придется восстановить доступ к ижевскому домену.

Также Вам предстоит настроить защищенный канал связи между офисами, доверие между доменами и удаленное подключение клиентов, предварительно смоделировав наличие провайдера Интернета.

Внимательно прочтите задание от начала до конца – оно представляет собой целостную систему. При первом доступе к операционным системам либо следуйте указаниям мастера, либо используйте следующие реквизиты: **Administrator/P@ssw0rd.**

Обратите внимание что брандмауэр должен быть включен!

Если предоставленные виртуальные машины начнут самопроизвольно отключаться в процессе работы, попробуйте выполнить на них команду **slmgr /rearm** или обратитесь к техническому эксперту.

КОМПЛЕКТАЦИЯ ЭКЗАМЕНАЦИОННОГО ЗАДАНИЯ

1. Текстовые файлы:

1. данный файл с экзаменационным заданием;
2. файл дополнений к экзаменационному заданию, содержащий: описание вида предустановок, описание используемых операционных систем, рекомендации по выделению ресурсов для виртуальных машин, рекомендации возможных изменений к заданию в рамках 30%.

2. Предоставляемые участникам компоненты проекта:

1. файл для импорта пользователей в домен Moscow (.xlsx);
2. стартовая страница сайта managers.moscow.ru (.htm);
3. стартовая страница сайта www.moscow.ru (.htm);
4. стартовая страница сайта www.izhevsk.ru (.htm).

3. Программное обеспечение:

1. Windows server 2016;
2. Microsoft Office;
3. RSAT tools for Windows 10;
4. Windows10.ADMX.

Внимание! Все указанные компоненты предоставляются участникам в виде
ISO-файлов на локальном или удаленном хранилище.

Участники не имеют права пользоваться любыми устройствами, за исключением находящихся на рабочих местах устройств, предоставленных организаторами.

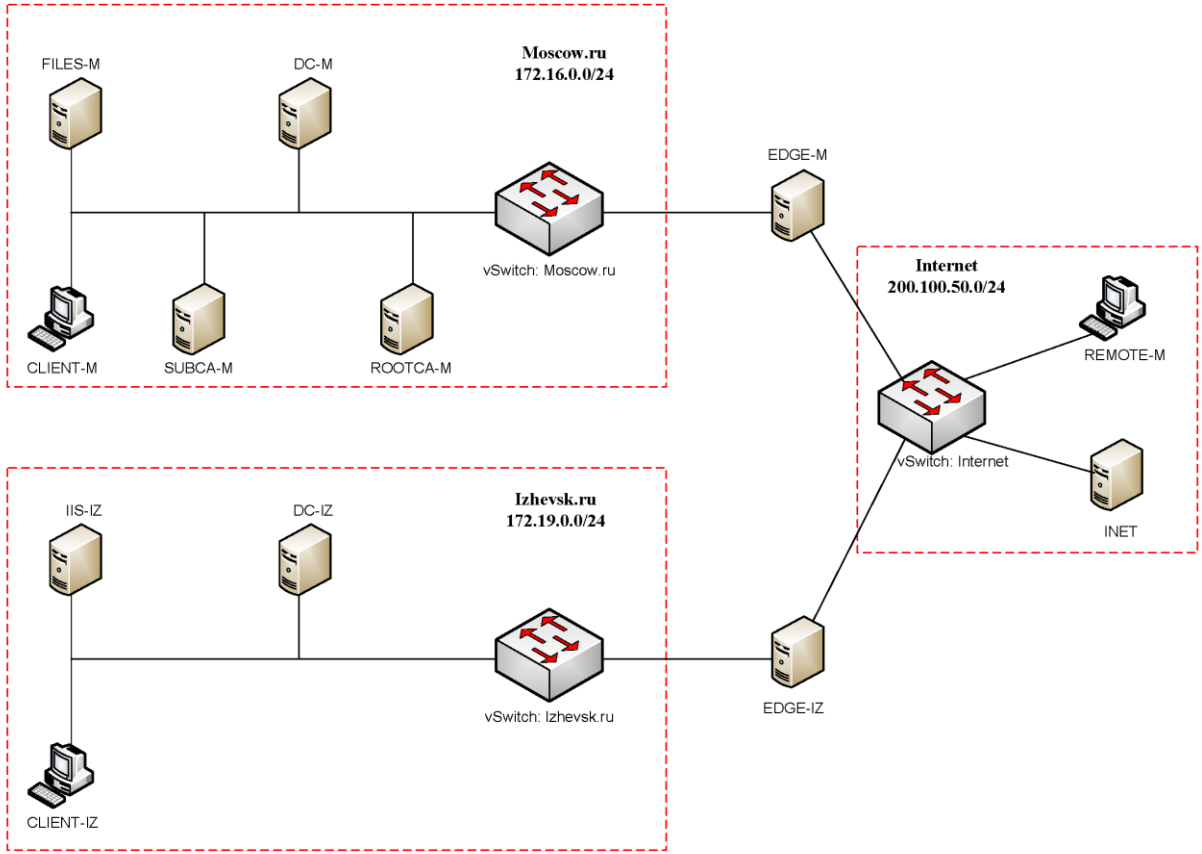
Участники не имеют права приносить с собой на рабочее место заранее подготовленные текстовые материалы.

В итоге участники должны обеспечить наличие и функционирование в соответствии с заданием служб и ролей на указанных виртуальных машинах. При этом участники могут самостоятельно выбирать способ настройки того

или иного компонента, используя предоставленные им ресурсы по своему усмотрению

1

Диаграмма виртуальной сети



Настройка DC-M

Базовая настройка

1. переименуйте компьютер в DC-M;
2. задайте настройки сети в соответствии с таблицей 1;
3. обеспечьте работоспособность протокола ICMP (для использования команды ping).

Active Directory

1. сделайте сервер основным контроллером домена Moscow.ru;
2. настройте одностороннее нетранзитивное доверие с доменом Izhevsk.ru – пользователи домена Moscow.ru должны иметь доступ к ресурсам домена Izhevsk.ru, но не наоборот.

DHCP

1. настройте протокол DHCP для автоконфигурации клиентов;
2. настройте failover: mode – Load balancer, partner server – FILES-M, state swithover – 10 min;
3. диапазон выдаваемых адресов: 172.16.0.100-200/24;
4. настройте дополнительные свойства области (адреса обоих DNS-серверов и основного шлюза).

DNS

1. настройте необходимые зоны прямого и обратного просмотра, обеспечьте их согласованную работу со службой DNS на FILES-M;
2. создайте вручную все необходимые записи типа A и PTR для серверов домена и необходимых web-сервисов;
3. сделайте необходимые настройки для работоспособности доверия с доменом Izhevsk.ru (при появлении в сети новых DNS серверов они должны автоматически получать необходимые для работоспособности доверия настройки).

GPO

1. запретите анимацию при первом входе пользователей в систему на всех клиентских компьютерах домена;
2. члены группы IT должны быть членами группы локальных администраторов на всех клиентских компьютерах домена;
3. в браузерах IE Explorer и Microsoft Edge (установите и используйте windows10.admx) должна быть настроена стартовая страница – www.moscow.ru;
4. запретите изменение экранной заставки и Корзину на рабочем столе для всех пользователей домена, кроме членов группы локальных администраторов клиентских компьютеров;
5. для членов группы Experts настройте перенаправление папок my Documents и Desktop по адресу FILES-M→d:\shares\redirected.

Элементы доменной инфраструктуры

1. создайте подразделения: Experts, Competitors, Managers, Visitors, IT и Project;
2. в соответствующих подразделениях создайте доменные группы: Experts, Competitors, Managers, Visitors, IT, Project_Budget-R, Project_Budget-W, Project_Intranet-R, Project_Intranet-W, Project_Logistics-R, Project_Logistics-W;
3. также создайте доменную группу DAClients;

Внимание! Указанные выше подразделения и группы должны быть созданы в домене обязательно. Если Вы считаете, что для выполнения задания необходимы дополнительные элементы доменной инфраструктуры, Вы можете создать их.

4. создайте пользователей, используя прилагаемый excel-файл (вся имеющаяся в файле информация о пользователях должна быть внесена в Active Directory); поместите пользователей в соответствующие подразделения и группы; все созданные учетные записи должны быть включены и доступны;

5. для каждого пользователя создайте автоматически подключаемую в качестве диска U:\ домашнюю папку по адресу FILES-M→d:\shares\users.

Настройка FILES-M

Базовая настройка

4. переименуйте компьютер в FILES-M;
5. задайте настройки сети в соответствии с таблицей 1;
6. обеспечьте работоспособность протокола ICMP (для использования команды ping);
7. присоедините компьютер к домену Moscow.ru;
8. из четырех имеющихся жестких дисков создайте RAID-5 массив; назначьте ему букву D:\.

Active Directory

3. сделайте сервер дополнительным контроллером домена Moscow.ru;
4. контроллер не должен выполнять функцию глобального каталога.

DHCP

5. настройте протокол DHCP для автоконфигурации клиентов;
6. настройте failover: mode – Load balancer, partner server – DC-M, state swithover – 10 min;

DNS

4. сделайте сервер дополнительным DNS-сервером в домене Moscow.ru;
5. загрузите с DC-M все зоны прямого и обратного просмотра.

Общие папки

6. создайте общие папки для подразделений (Competitors, Experts and Managers) по адресу FILES-M→d:\shares\departments;
7. обеспечьте привязку общей папки подразделения к соответствующей группе в качестве диска G:\;
8. создайте общую папку проектов по адресу FILES-M→d:\shares\projects;

9. в папке d:\shares\projects создайте следующие папки: Budget, Intranet, Logistics; настройте разрешения этих папок в соответствии с таблицей 2;

10. создайте привязку общей папки проектов для всех пользователей, кроме членов группы Visitors, в качестве диска P:\; пользователи должны видеть только те папки внутри диска P:\, к которым им разрешен доступ.

Квоты/Файловые экраны

1. установите максимальный размер в 5Gb для каждой домашней папки пользователя (U:\);
2. запретите хранение в домашних папках пользователей файлов с расширениями .cmd и .exe; учтите, что файлы остальных типов пользователи вправе хранить в домашних папках.

IIS

1. создайте сайт для менеджеров компании (используйте предоставленный htm-файл в качестве документа по умолчанию);
2. сайт должен быть доступен по имени managers.moscow.ru только по протоколу https исключительно для членов группы Managers по их пользовательским сертификатам.

Настройка ROOTCA-M

Базовая настройка

9. переименуйте компьютер в ROOTCA-M;
10. задайте настройки сети в соответствии с таблицей 1;
11. обеспечьте работоспособность протокола ICMP (для использования команды ping);
12. не присоединяйте компьютер к какому-либо домену.

Службы сертификации

1. установите службы сертификации;
2. настройте одиночный корневой сервер сертификации (длина ключа и алгоритмы шифрования значения не имеют);
3. имя центра сертификации – Moscow Root CA;
4. срок действия сертификата – 10 лет;
5. CRL location: http://SUBCA-M.Moscow.ru/certenroll/<caname><crlnamesuffix><deltacrlallowed>.crl
6. AIA location: http://SUBCA-M.Moscow.ru/certenroll/<serverdnsname>_<caname><certificatename>.crt

7. создайте список отзыва сертификатов и сертификат корневого центра сертификации для SUBCA-M;

8. выпустите сертификат подчиненного центра сертификации для SUBCA-M, одобрив соответствующий запрос;

9. после всех настроек отключите сетевой интерфейс.

Настройка SUBCA-M

Базовая настройка

13. переименуйте компьютер в SUBCA-M;

14. задайте настройки сети в соответствии с таблицей 1;

15. обеспечьте работоспособность протокола ICMP (для использования команды ping);

16. присоедините компьютер к домену Moscow.ru.

Службы сертификации

10. установите службы сертификации;

11. настройте подчиненный доменный центр сертификации;

12. имя центра сертификации – Moscow Sub CA;

13. срок действия сертификата – 5 лет;

14. импортируйте и опубликуйте список отзыва сертификатов с ROOTCA-M;

15. настройте шаблон выдаваемого сертификата для клиентских компьютеров MoscowClients: subject name=common name, автозапрос для всех клиентских компьютеров домена;

16. настройте шаблон выдаваемого сертификата для группы Managers MoscowUsers: subject name=common name, автозапрос только для пользователей – членов группы Managers.

Настройка CLIENT-M

Базовая настройка

17. переименуйте компьютер в CLIENT-M;
18. обеспечьте работоспособность протокола ICMP (для использования команды ping);
19. присоедините компьютер к домену Moscow.ru;
20. установите набор компонентов удаленного администрирования RSAT;
21. запретите использование «спящего режима»;
22. используйте компьютер для тестирования настроек в домене Moscow.ru: пользователей, общих папок, групповых политик, в том числе – тестирования удаленных подключений через Direct Access (временно переключаю компьютер в сеть Internet).

Работа с DC-IZ

Восстановление доступа

1. получите (восстановите) доступ к контроллеру домена и реплике Active Directory; помните – на сервере хранится важная информация, поэтому просто переустановить операционную систему нельзя!

Поиск пользователей и ресурсов

2. найдите всех пользователей домена Izhevsk.ru, у которых в графе Job Title проставлено значение Expert;
3. переместите всех найденных пользователей в специальное подразделение Migration (при необходимости создайте его) и отключите учетные записи в домене Izhevsk.ru;
4. найдите в домене Izhevsk.ru и скопируйте на FILES-M→d:\shares\migrated все домашние папки ранее найденных пользователей;
5. в домене Moscow.ru в подразделении Migrated (при необходимости создайте это подразделение) создайте новые учетные записи, соответствующие найденным ранее и отключенным учетным записям; задайте для них пароль NewP@ssw0rd;
6. для вновь созданных учетных записей обеспечьте привязку домашних папок в качестве диска S:\; проследите, что вновь созданные в домене

Moscow.ru пользователи имеют доступ к скопированным из домена Izhevsk.ru файлам, находящимся в их домашних папках.

DNS

1. сделайте необходимые настройки для работоспособности доверия с доменом Moscow.ru (при появлении в сети новых DNS серверов они должны автоматически получать необходимые для работоспособности доверия настройки);
2. обеспечьте разрешение имен сайтов www.moscow.ru и www.izhevsk.ru.

Службы удаленных рабочих столов

1. разверните терминальный сервер, не устанавливайте и не настраивайте компоненты лицензирования;
2. сконфигурируйте web-доступ RemoteApp к службам терминалов сервера;
3. опубликуйте программу Wordpad на web-портале RemoteApp для членов группы Domain Admins;
4. опубликуйте программу Notepad на web-портале RemoteApp для членов группы Domain Users;
5. web-интерфейс сервера должен быть настроен таким образом, чтобы пользователи могли автоматически получать доступ к форме входа на web-интерфейс удаленных рабочих столов при указании адресов http://rds.izhevsk.ru и https://rds.izhevsk.ru;
6. с помощью доменного центра сертификации на сервере SUBCA-M сгенерируйте и используйте для терминальных служб соответствующий SSL-сертификат. Сертификат должен быть использован для всех установленных компонентов терминальных служб. При обращении с любого компьютера в домене Moscow.ru или Izhevsk.ru к сайту по имени https://rds.izhevsk.ru сертификат должен распознаваться как доверенный и действительный.

Работа с IIS-IZ

IIS

1. создайте сайт www.moscow.ru (используйте предоставленный htm-файл в качестве документа по умолчанию);
2. создайте сайт www.izhevsk.ru (используйте предоставленный htm-файл в качестве документа по умолчанию);
3. оба сайта должны быть доступны по протоколу https с использованием сертификатов, выданных SUBCA-M.

Работа с CLIENT-IZ

Базовая настройка

1. переименуйте компьютер в CLIENT-IZ;
2. обеспечьте работоспособность протокола ICMP (для использования команды ping);
3. присоедините компьютер к домену Izhevsk.ru;
4. запретите использование «спящего режима»;
5. используйте компьютер для тестирования настроек в домене Izhevsk.ru.

Настройка INET

Базовая настройка

1. переименуйте компьютер в INET;
2. задайте настройки сети в соответствии с таблицей 1;
3. обеспечьте работоспособность протокола ICMP (для использования команды ping);
4. не присоединяйте компьютер к какому-либо домену.

DNS/IIS

1. настройте эмуляцию подключения к Интернету, принимая во внимание версии используемых операционных систем;
2. создайте в DNS соответствующие записи для удаленного подключения клиентов к серверу Direct Access в домене Moscow.ru, а также записи для доступа внешних клиентов к сайтам www.moscow.ru и www.izhevsk.ru.

DHCP

1. настройте протокол DHCP для клиентов в сети Internet;
2. диапазон выдаваемых адресов: .170-190/24;
3. остальные необходимые параметры области сконфигурируйте по вашему выбору.

Настройка EDGE-IZ

Базовая настройка

1. переименуйте компьютер в EDGE-IZ;
2. задайте настройки сети в соответствии с таблицей 1;
3. обеспечьте работоспособность протокола ICMP (для использования команды ping);
4. присоедините компьютер к домену Izhevsk.ru.

Настройка RRAS

1. установите службу RRAS;
2. настройте защищенное VPN-соединение с доменом Moscow.ru с использованием аутентификации по сертификатам компьютеров; сертификаты должны быть выданы SUBCA-M; весь трафик между доменами должен передаваться через это соединение;
3. настройте проброс портов для доступа удаленных клиентов (проверяется из сети Internet) к сайтам www.moscow.ru и www.izhevsk.ru, развернутым на IIS-IZ.

Настройка EDGE-M

Базовая настройка

1. переименуйте компьютер в EDGE-M;
2. задайте настройки сети в соответствии с таблицей 1;
3. обеспечьте работоспособность протокола ICMP (для использования команды ping);
4. присоедините компьютер к домену Moscow.ru.

Настройка RRAS

1. установите службу RRAS;

2. настройте защищенное VPN-соединение с доменом Izhevsk.ru с использованием аутентификации по сертификатам компьютеров; сертификаты должны быть выданы SUBCA-M; весь трафик между доменами должен передаваться через это соединение.

Настройка REMOTE-M

Базовая настройка

1. переименуйте компьютер в REMOTE-M;

2. обеспечьте работоспособность протокола ICMP (для использования команды ping);

3. запретите использование «спящего режима»;

4. не меняя сетевых настроек (сетевой интерфейс должен быть соединен с сетью Internet) присоедините компьютер к домену Moscow.ru в режиме OFFLINE;

5. сохраните созданный на DC-M файл ответов для offline-присоединения к домену по адресу C:\Remote.txt.

Таблица 1 – Реквизиты

Имя компьютера	Имя домена	IP-адреса
DC-IZ	Izhevsk.ru	172.19.0.1/24
CLIENT-IZ		DHCP
IIS-IZ		172.19.0.3/24
EDGE-IZ		172.19.0.250/24 200.100.50.101/24
DC-M	Moscow.ru	172.16.0.1/24
FILES-M		172.16.0.2/24
SUBCA-M		172.16.0.4/24
EDGE-M		172.16.0.250/24 200.100.50.100/24
CLIENT-M		DHCP
REMOTE-M		DHCP
ROOTCA-M	None	172.16.0.3/24
INET		200.100.50.200/24

Таблица 2 – Файловый доступ

Имя общего ресурса	Расположение	Доступ только для чтения	Доступ для чтения и записи
Budget	FILES-M→D:\shares\projects	Project_Budget-R	Project_Budget-W
Intranet		Project_Intranet-R	Project_Intranet-W
Logistics		Project_Logistics-R	Project_Logistics-W

Модуль С: «Пуско-наладка телекоммуникационного оборудования»

Версия: 1.3 01.04.19

ВВЕДЕНИЕ

Знание сетевых технологий на сегодняшний день становится незаменимым для тех, кто хочет построить успешную карьеру в области ИТ. Данное экзаменационное задание содержит множество задач, основанных на опыте реальной эксплуатации информационных систем, в основном интеграции и аутсорсинге. Если вы можете выполнить задание с высоким результатом, то вы точно сможете обслуживать информационную инфраструктуру большого предприятия.

ОПИСАНИЕ ЭКЗАМЕНАЦИОННОГО ЗАДАНИЯ

Данное экзаменационное задание разработано с учетом различных сетевых технологий, соответствующих уровням сертификации CCNA R\S, CCNA Security, CCNA Collaboration, CCNP R\S Задание разбито на следующие секции:

- Базовая настройка
- Настройка коммутации
- Настройка подключений к глобальным сетям
- Настройка маршрутизации
- Настройка служб
- Настройка механизмов безопасности
- Настройка параметров мониторинга и резервного копирования
- Конфигурация виртуальных частных сетей
- Конфигурация подсистемы телефонной связи

Все секции являются независимыми друг от друга, но вместе образуют достаточно сложную сетевую инфраструктуру. Некоторые задания достаточно просты и понятны, некоторые могут быть неочевидными. Можно заметить, что некоторые технологии должны работать в связке или поверх других технологий. Например, может подразумеваться, что IPv6 маршрутизация должна работать поверх настроенной виртуальной частной сети, которая, в свою очередь, должна работать поверх IPv4 маршрутизации, которая, в свою очередь, должна работать поверх PPPoE и L2TP и т.д. Очень важно понимать, что если вам не удается решить

какую-либо из задач по середине такого технологического стека, это не значит, что решенные задачи не будут оценены. Например, если вы не можете настроить динамическую маршрутизацию IPv4, которая необходима для работы виртуальной частной сети, вы можете использовать статическую маршрутизацию и продолжать работу над настройкой виртуальной частной сети и всем что должно работать поверх нее. В этом случае вы не получите баллы за динамическую маршрутизацию, но вы получите баллы за всё что должно работать поверх нее (в случае если функциональные тесты пройдены успешно).

ИНСТРУКЦИИ ДЛЯ УЧАСТНИКА

В первую очередь необходимо прочитать задание полностью и составить алгоритм выполнения работы. Вам предстоит вносить изменения в действующую, преднастроенную сетевую инфраструктуру предприятия, состоящую из головного офиса HQ и двух удаленных офисов BR1 и BR2. Офисы имеют связь через двух провайдеров ISP1 и ISP2. Вы не имеете доступа к оборудованию провайдеров, оно полностью настроено и не требует дополнительного конфигурирования. Вам необходимо настраивать оборудование предприятия, а именно: SW1, SW2, HQSW1, HQSW2, HQ1, ASA, BR1 и BR2.

У вас отсутствует консольный доступ к устройствам, будьте очень внимательны при выполнении задания! В случае потери связи с оборудованием, вы будете виноваты сами. **Разрешается перезагрузка оборудования** – только техническими экспертами. Например, применили неправильный ACL, который закрыл доступ по telnet, но вы не успели сохранить конфигурацию.

Руководствуйтесь пословицей: **Семь раз отмерь, один раз отрежь**. Для выполнения задания у вас есть одна физическая машина (PC1 с доступом по Telnet и установленным ASDM), которую вы должны использовать в качестве:

PC2 Виртуальный ПК, Windows 10 с предустановленным Cisco IP Communicator, Cisco AnyConnect, Putty. Пользователь User пароль P@ssw0rd

PC3 Виртуальный ПК, Windows 10 с предустановленным Cisco IP Communicator, Cisco AnyConnect, Putty. Пользователь User пароль P@ssw0rd

SRV1 Виртуальный ПК, CentOS7 пользователь root пароль toor, с предустановленными сервисами

1) SysLog папка для проверки /Cisco_Log

2) RADIUS - FreeRadius

3) SNMP – для проверки используется пакет Net-SNMP используйте команду snmp_test

4) NTP

5) TFTP папка для проверки /Cisco_TFTP

Следует обратить внимание, что задание составлено не в хронологическом порядке. Некоторые секции могут потребовать действий из других секций, которые изложены ниже. Например, задание 3 в секции «Настройка служб» предписывает вам настроить службу протокола автоматической конфигурации хостов, которая, разумеется, не будет работать пока не будут выполнены необходимые настройки в секции «Конфигурация коммутации». На вас возлагается ответственность за распределение своего рабочего времени.

Не тратьте время, если у вас возникли проблемы с некоторыми заданиями. Вы можете использовать временные решения (если у вас есть зависимости в технологическом стеке) и продолжить выполнение других задач. Рекомендуется **тщательно проверять** результаты своей работы.

Убедитесь в том, что ваши настройки на всех устройствах функционируют после перезагрузки всего оборудования.

ПОДКЛЮЧЕНИЕ К УСТРОЙСТВАМ

Для первоначального подключения используйте протокол Telnet. Для подключения к ASA используете учетную запись с логином: **cisco** и паролем: **cisco**, для входа в привилегированный режим используйте пароль **cisco**. Для подключения к остальным сетевым устройствам используйте пароль: **cisco** и пароль для привилегированного режима: **cisco**

Для подключения к устройствам в главном офисе HQ, подключите рабочую станцию к порту F0/10 коммутатора SW2 и настройте адрес в соответствии с диаграммой L3, устройства доступны по следующим адресам:

SW1 – **192.168.254.10**

SW2 – **192.168.254.20**

HQSW1 – **192.168.254.1**

HQSW2 – **192.168.254.2**

HQ1 – **192.168.254.100**

ASA – **192.168.254.200**

Для подключения к устройствам в удаленном офисе BR1, подключите рабочую станцию в порт GigabitEthernet0/0/1 маршрутизатора BR1. BR1 доступен по адресу **192.168.1.3**.

Для подключения к устройствам в удаленном офисе BR2, подключите рабочую станцию в порт PC телефона Phone2 или напрямую в порт GigabitEthernet0/0/1 маршрутизатора BR2. BR2 доступен по адресу **192.168.2.1**.

ОЦЕНКА

Для оценки выполненного задания используется автоматизированный метод. Проверочный модуль будет включен в порт F0/11 коммутатора SW2, поэтому следует убедиться, что он настроен корректно.

Важно! Убедитесь в возможности удаленного подключения с порта F0/11 ко ВСЕМ сетевым устройствам компании, в том числе к BR1 и BR2, если к каким-либо из устройств будет отсутствовать доступ, эти устройства оцениваться не будут.

Если порт F0/11 находится во VLAN по умолчанию, то IP адрес сервиса проверки 192.168.245.11 и если порт переведен в VLAN 300, то ip адрес 192.168.3.11.

Сервис проверки подключается ко всем устройствам, сначала по SSH, затем по Telnet, перебирая варианты адресов:

SW1 - 172.16.10.10 или 192.168.254.10

SW2 - 172.16.10.20 или 192.168.254.20

HQSW1 - 192.168.3.1 или 192.168.254.1

HQSW2 - 192.168.3.2 или 192.168.254.2

HQ1 - 172.16.0.6 или 192.168.254.100

ASA - 172.16.0.14 или 192.168.254.200

BR1 - 33.33.33.2 или 5.5.5.2

BR2 - 40.15.4.2 или 5.5.5.3

Базовая настройка

1. Задайте имя всех устройств в соответствии с топологией.
2. Назначьте для всех устройств доменное имя **wsr2018.ru.**
3. Создайте на всех устройствах пользователей **wsr2018** с паролем **cisco**

    a. Пароль пользователя должен храниться в конфигурации в виде результата хэш-функции.

    b. Пользователь должен обладать максимальным уровнем привилегий.

4. На всех устройствах установите пароль **wsr** на вход в привилегированный режим.

    a. Пароль должен храниться в конфигурации НЕ в виде результата хэш-функции.

    b. На межсетевом экране ASA настройте вход в привилегированный режим по паролю пользователя (без запроса имени пользователя).

    c. Настройте режим, при котором все пароли в конфигурации хранятся в зашифрованном виде. На ASA используйте шифрование AES.

5. Для всех устройств реализуйте модель AAA.

    a. Аутентификация на линиях виртуальных терминалов с 0 по 15 должна производиться с использованием локальной базы учётных записей. (кроме маршрутизатора HQ1)

    b. После успешной аутентификации при удалённом подключении пользователи сразу должен получать права, соответствующие их уровню привилегий или роли (кроме межсетевого экрана ASA).

    c. Настройте необходимость аутентификации на локальной консоли.

    d. При успешной аутентификации на локальной консоли пользователи должны сразу должен получать права, соответствующие их уровню привилегий или роли.

6. На устройствах, к которым разрешен доступ, в соответствии с топологиями L2 и L3, создайте виртуальные интерфейсы, подынтерфейсы и интерфейсы типа петля, назначьте IP-адреса.

7. На маршрутизаторе HQ1 на виртуальных терминальных линиях с 0 по 15 настройте аутентификацию с использованием RADIUS-сервера.

a. Используйте на линиях vty с 0 по 15 отдельный список методов с названием **method_man**

b. Порядок аутентификации:

i. По протоколу RADIUS

ii. Локальная

c. Используйте общий ключ **cisco**

d. Используйте номера портов 1812 и 1813 для аутентификации и учета соответственно

e. Адрес RADIUS-сервера 172.16.0.10

f. Настройте авторизацию при успешной аутентификации

g. Проверьте аутентификацию по протоколу RADIUS при удаленном подключении к маршрутизатору HQ1, используя учетную запись **radius** с паролем **cisco**

8. Все устройства должны быть доступны для управления по протоколу SSH версии 2.

Настройка коммутации

1. Для централизованного конфигурирования VLAN в коммутируемой сети предприятия используйте протокол VTP версии 3.

a. В качестве основного сервера VTP настройте HQSW1.

b. Коммутаторы SW1, SW2 и HQSW2 настройте в качестве VTP клиента.

c. В качестве домена используйте **wsr2018.ru**

d. Используйте пароль **VTPPass** для защиты VTP.

e. Таблица VLAN должна содержать следующие сети:

i. VLAN100 с именем **MGT**.

ii. VLAN200 с именем **DATA**.

iii. VLAN300 с именем **OFFICE**.

iv. VLAN400 с именем **VOIP**.

2. Между всеми коммутаторами настройте транки с использованием протокола IEEE 802.1q.

a. Транки между коммутаторами HQSW1 и HQSW2, а также между SW1 и SW2 должны быть настроены без использования согласования. Отключите протокол DTP явным образом.

b. Транки между коммутаторами HQSW1 и SW1, SW2, а также между HQSW2 и SW1, SW2 должны быть согласованы по DTP, коммутаторы HQSW1 и HQSW2 должны инициировать создание транка, а коммутаторы SW1 и SW2 должны ожидать начала согласования параметров от соседа, но сами не инициировать согласование.

3. Настройте агрегирование каналов связи между коммутаторами.

a. Номера портовых групп:

1 – между коммутаторами HQSW1 (G1/0/6-7) и SW1 (F0/6-7);

2 – между коммутаторами HQSW2 (G1/0/6-7) и SW2 (F0/6-7);

3 – между коммутаторами HQSW1 (G1/0/1-2) и HQSW2 (G1/0/1-2);

b. Агрегированный канал между HQSW1 и SW1 должен быть организован с использованием протокола согласования LACP. HQSW1 должен быть настроен в активном режиме, SW1 в пассивном.

c. Агрегированный канал между HQSW2 и SW2 должен быть организован с использованием протокола согласования PAgP. HQSW2 должен быть настроен в предпочтительном, SW2 в автоматическом.

d. Агрегированный канал между HQSW1 и HQSW2 должен работать без использования протоколов согласования.

e. Агрегированные каналы 1 и 2 должны работать в режиме L2.

f. Агрегированный канал 3 должен работать в режиме L3.

4. Конфигурация протокола остовного дерева:

a. Используйте протокол совместимый с IEEE 802.1s.

b. Необходимо обеспечить два экземпляра деревьев во всей сети центрального офиса (не считая нулевой экземпляр).

i. Экземпляр под номером 1 для VLAN 100,200

ii. Экземпляр под номером 2 для VLAN 300,400

c. Коммутатор HQSW1 должен являться корнем связующего дерева в сетях VLAN 100 и 200, в случае отказа HQSW1, корнем должен стать коммутатор HQSW2.

d. Коммутатор HQSW2 должен являться корнем связующего дерева в сетях VLAN 300 и 400, в случае отказа HQSW2, корнем должен стать коммутатор HQSW1.

e. Настройте используемые порты коммутаторов HQSW1 и HQSW2 так, чтобы во всех VLAN корнем связующего дерева могли стать только HQSW1 или HQSW2, а при получении BPDU пакета с лучшим приоритетом корня, порт должен перейти в состояние root-inconsistent.

f. Настройте порты G1/0/24 коммутатора HQSW1 и F0/10 коммутатора SW1, таким образом, что при включении они сразу переходили в состояние forwarding не дожидаясь пересчета остовного дерева. При получении BPDU пакета данные порты должны переходить в состояние error-disabled.

5. Настройте порты F0/10 на коммутаторах SW1 и SW2, а также G1/0/8 на коммутаторах HQSW1 и HQSW2 в соответствии с L2 диаграммой. Порты должны работать в режиме доступа.

6. Настройте протокол IEEE 802.1AB таким образом, чтобы приём служебных сообщений был возможен на всех портах устройств HQSW1 и HQSW2, а передача только на портах между данными устройствами.

Настройка подключений к глобальным сетям

1. Настройте подключение PPPoE между ISP1 и маршрутизатором BR1.

a. Настройте PPPoE клиент на BR1.

b. Используйте имя пользователя **cisco** и пароль **cisco**

c. Устройства походят одностороннюю аутентификацию по протоколу CHAP, только ISP1 проверяет имя пользователя и пароль.

d. BR1 должен автоматически получать адрес от ISP1.

2. Провайдер ISP1 использует протокол L2TP для подключения офиса HQ1.

a. Настройте HQ1 в качестве L2TP-клиента.

i. Используйте адрес 10.1.3.1 в качестве сервера L2TP.

ii. Настройте VirtualPPP с номером 100.

iii. HQ1 должен автоматически получать адрес от ISP1.

iv. Настройте взаимную аутентификацию по протоколу CHAP. Используйте логин **client65000** и пароль **L2TPass**

v. Аутентифицируйте провайдера по логину **ISP1**

vi. Используйте MTU 1450

3. Настройте подключение HQ1 к ISP2 с помощью Frame Relay.

a. Используйте тип LMI cisco.

b. Используйте DLCI 102.

4. Настройте подключение BR2 к провайдеру ISP2 с помощью протокола PPP.

a. Настройте Multilink PPP с использованием двух Serial-интерфейсов.

b. Используйте 1 номер интерфейса.

c. Не используйте аутентификацию.

d. BR2 должен автоматически получать адрес от ISP2.

5. Для подключения BR2 к провайдеру ISP1 настройте туннель GRE. Используйте туннельный интерфейс с номером 10. В качестве транспорта используйте адреса в соответствии с диаграммой L3.

6. ASA подключена к провайдеру ISP1 и ISP2 с помощью IPoE и имеет статические адреса.

Настройка маршрутизации

1. В офисе HQ, на устройствах HQSW1, HQSW2, HQ1 и ASA настройте протокол динамической маршрутизации OSPF.

a. Включите в обновления маршрутизации сети в соответствии с Routing-диаграммой.

b. Используйте область с номером 51 для всех сетей центрального офиса.

c. HQSW1 и HQSW2 должны устанавливать соседство только в сети 172.16.0.0/30.

d. Отключите отправку обновлений маршрутизации на всех интерфейсах, где не предусмотрено формирование соседства.

2. Настройте протокол динамической маршрутизации OSPF в офисах BR1 и BR2 с главным офисом HQ.

a. Включите в обновления маршрутизации сети в соответствии с Routing-диаграммой.

b. Используйте магистральную область для сети DMVPN.

c. В сети DMVPN маршрутизатор HQ1 должен исполнять роль DR.

d. Соседства между офисами (HQ, BR1 и BR2) должны устанавливаться через защищенную DMVPN сеть.

e. В офисе BR1 используйте область с номером 1.

f. В офисе BR2 используйте область с номером 2.

g. Отключите отправку обновлений маршрутизации на всех интерфейсах, где не предусмотрено формирование соседства.

3. ISP1 предоставляет подсеть PA (Provider Aggregatable) адресов (11.31.31.31/32) для офиса BR1. На маршрутизаторе BR1 настройте протокол динамической маршрутизации EIGRP с номером автономной системы 2018.

a. Включите в обновления маршрутизации сети в соответствии с Routing-диаграммой.

b. Используйте аутентификацию MD5 с помощью связки ключей **EIGRP** с ключом **WSR** и номером ключа **2**.

c. Провайдер ISP1 выполняет редистрибуцию маршрута 11.31.31.31/32 в сеть BGP, убедитесь в том, что вы корректно анонсируете данный маршрут провайдеру.

4. Офисы HQ и BR2 имеют подсети PI (Provider Independent) адресов и автономную систему 65000 и 65020 соответственно. На маршрутизаторах настройте протокол динамической маршрутизации BGP в соответствии с таблицей.

Устройство	AS
HQ1	65000
ASA	65000
ISP1	65001
ISP2	65002

a. Настройте автономные системы в соответствии с Routing-диаграммой.

b. Маршрутизатор HQ1 и ASA должны быть связаны с помощью iBGP. Используйте для этого соседства интерфейс Loopback1 на HQ1.

c. Включите в обновления маршрутизации сети в соответствии с Routing-диаграммой.

d. На HQ1 и ASA настройте редистрибуцию маршрутов к сетям 10.10.10.10/32, 20.20.20.20/32 и 30.30.30.0/27 из OSPF в BGP

5. Настройте прокол динамической маршрутизации OSPFv3 поверх сети DMVPN. На маршрутизаторах HQ1, BR1, BR2 и на коммутаторах HQSW1, HQSW2 настройте протокол динамической маршрутизации OSPFv3 с номером процесса 1.

a. Включите в обновления маршрутизации сети в соответствии с Routing-диаграммой.

b. Маршрутизатор HQ1 должен исполнять роль DR в сети DMVPN.

c. Используйте зону с номером 0

Настройка служб

1. В сетевой инфраструктуре сервером синхронизации времени является SRV1. Все остальные сетевые устройства должны использовать в качестве сервера времени HQ1.

a. Передача данных между HQ1 и SRV1 осуществляется без аутентификации.

b. Настройте временную зону с названием SAKT, укажите разницу с UTC +11 часов.

c. Настройте сервер синхронизации времени. Используйте стратум 2.

d. Используйте для синхронизации клиентов с HQ1 аутентификацию MD5 с ключом **WSR**.

2. Настройте динамическую трансляцию портов (PAT):

a. На маршрутизаторе HQ1 настройте динамическую трансляцию портов (PAT) для сети OFFICE в адрес петлевого интерфейса 1.3.1.3.

b. На маршрутизаторе BR1 настройте динамическую трансляцию портов (PAT) для сети 192.168.1.0/24 в адрес петлевого интерфейса 11.31.31.31.

c. На маршрутизаторе BR2 настройте динамическую трансляцию портов (PAT) для сети 192.168.2.0/24 в адрес петлевого интерфейса 22.22.22.22.

d. На ASA настройте PAT для сетей центрального офиса в адреса внешних интерфейсов, ведущих на ISP1 и ISP2 соответственно.

3. На коммутаторе HQSW1 и HQSW2 настройте службу отказоустойчивости внутреннего шлюза.

a. Настройте HSRP группу для подсети OFFICE

i. Номер группы — 300

ii. В качестве виртуального IP-адреса используйте адрес 192.168.3.254

iii. Настройте приоритет 100 для маршрутизатора HQSW1, для HQSW2 — 120.

iv. Настройте аутентификацию по паролю **hsrp**

v. Разрешите перехват роли активного шлюза устройством с большим приоритетом

4. Настройте протокол динамической конфигурации хостов со следующими характеристиками

a. На маршрутизаторе HQ1 для подсети OFFICE:

i. Адрес сети – 192.168.3.0/24.

ii. Адрес шлюза по умолчанию — виртуальный IP-адрес настроенной HSRP группы.

iii. Адрес TFTP-сервера 172.16.0.10.

iv. Компьютер PC1 должен получать адрес 192.168.3.10.

v. На коммутаторах HQSW1 и HQSW2 настройте DHCP-relay.

Настройка механизмов безопасности

1. На маршрутизаторе BR2 настройте пользователей с ограниченными правами.

a. Создайте пользователей **user1** и **user2** с паролем **cisco**

b. Назначьте пользователю user1 уровень привилегий 5. Пользователь должен иметь возможность выполнять все команды пользовательского режима, а также выполнять перезагрузку и отладку с помощью команд **debug**.

c. Создайте и назначьте view-контекст **sh_view** на пользователя

i. Команду show cdp neighbor

ii. Все команды show ip *

iii. Команду who

d. Создайте view-контекст **ping_view**. Включите в него

i. Команду ping

ii. Команду traceroute

e. Создайте view-контекст wan_view. Разрешите с помощью него настройку на интерфейсе Multilink1 инкапсуляции, аутентификации PPP, IP-адресации и выключения интерфейса.

f. Создайте superview-контекст с именем super, объединяющий эти 3 контекста. При входе на маршрутизатор пользователь user2 должен попадать в данный контекст

g. Убедитесь, что пользователи не могут выполнять другие команды в рамках присвоенных контекстов и уровней привилегий.

2. На порту F0/10 коммутатора SW1, включите и настройте Port Security со следующими параметрами:

a. не более 2 адресов на интерфейсе

b. адреса должны динамически определяться, но не сохраняться в конфигурации.

c. при попытке подключения устройства с адресом, нарушающим политику, на консоль должно быть выведено уведомление, порт не должен быть отключен.

3. На коммутаторе SW2 включите DHCP Snooping для подсети OFFICE. Используйте флеш-память в качестве места хранения базы данных.

4. На коммутаторе SW2 включите динамическую проверку ARP-запросов в сети OFFICE. Сделайте порт Fa0/11 доверенным.

Настройка параметров мониторинга и резервного копирования

1. На маршрутизаторе HQ1 и межсетевом экране ASA настройте журналирование системных сообщений на сервер SRV1, включая информационные сообщения.

2. На маршрутизаторе HQ1 и межсетевом экране ASA настройте возможность удаленного мониторинга по протоколу SNMP v3.

a. Задайте местоположение устройств YEKT, Russia

b. Задайте контакт admin@wsr.ru

c. Используйте имя группы WSR.

d. Создайте профиль только для чтения с именем RO.

e. Используйте для защиты SNMP шифрование AES128 и аутентификацию SHA1.

f. Используйте имя пользователя: **snmpuser** и пароль: **snmppass**

g. Для проверки вы можете использовать команду snmp_test на SRV1.

3. На маршрутизаторе HQ1 настройте резервное копирование конфигурации

a. Резервная копия конфигурации должна сохраняться на сервер SRV1 по протоколу TFTP при каждом сохранении конфигурации в памяти устройства

b. Для названия файла резервной копии используйте шаблон <hostname>-<time>.cfg

Конфигурация виртуальных частных сетей

1. На маршрутизаторах HQ1, BR1 и BR2 настройте DMVPN:
   a. Используйте в качестве VTI интерфейс Tunnel1
   b. На каждом интерфейсе установите значение MTU равное 1400 для IPv4 и IPv6.
   c. Используйте адресацию в соответствии с VPN-диаграммой
   d. Режим — GRE Multipoint
   e. Интерфейс-источник — Loopback-интерфейс на каждом маршрутизаторе.
   f. Настройки NHRP:
      i. Идентификатор сети — **111**
      ii. Пароль для аутентификации NHRP – **WSR2018**
   g. В качестве DMVPN-хаба и NHS-сервера используйте маршрутизатор HQ1.
2. Защита туннелей DMVPN должна обеспечиваться с помощью IPsec.
   a. Параметры политики первой фазы:
      i. Проверка целостности – SHA-384
      ii. Шифрование – AES-192

iii. Группа Диффи-Хэлмана – 14

iv. Используйте аутентификацию по парольной фразе

v. Обеспечьте работу IKEv2

b. Параметры преобразования трафика для второй фазы:

i. Протокол – ESP

ii. Шифрование – AES

iii. Проверка целостности – MD5

3. На межсетевом экране ASA настройте возможность подключения удаленных клиентов с помощью SSL-VPN

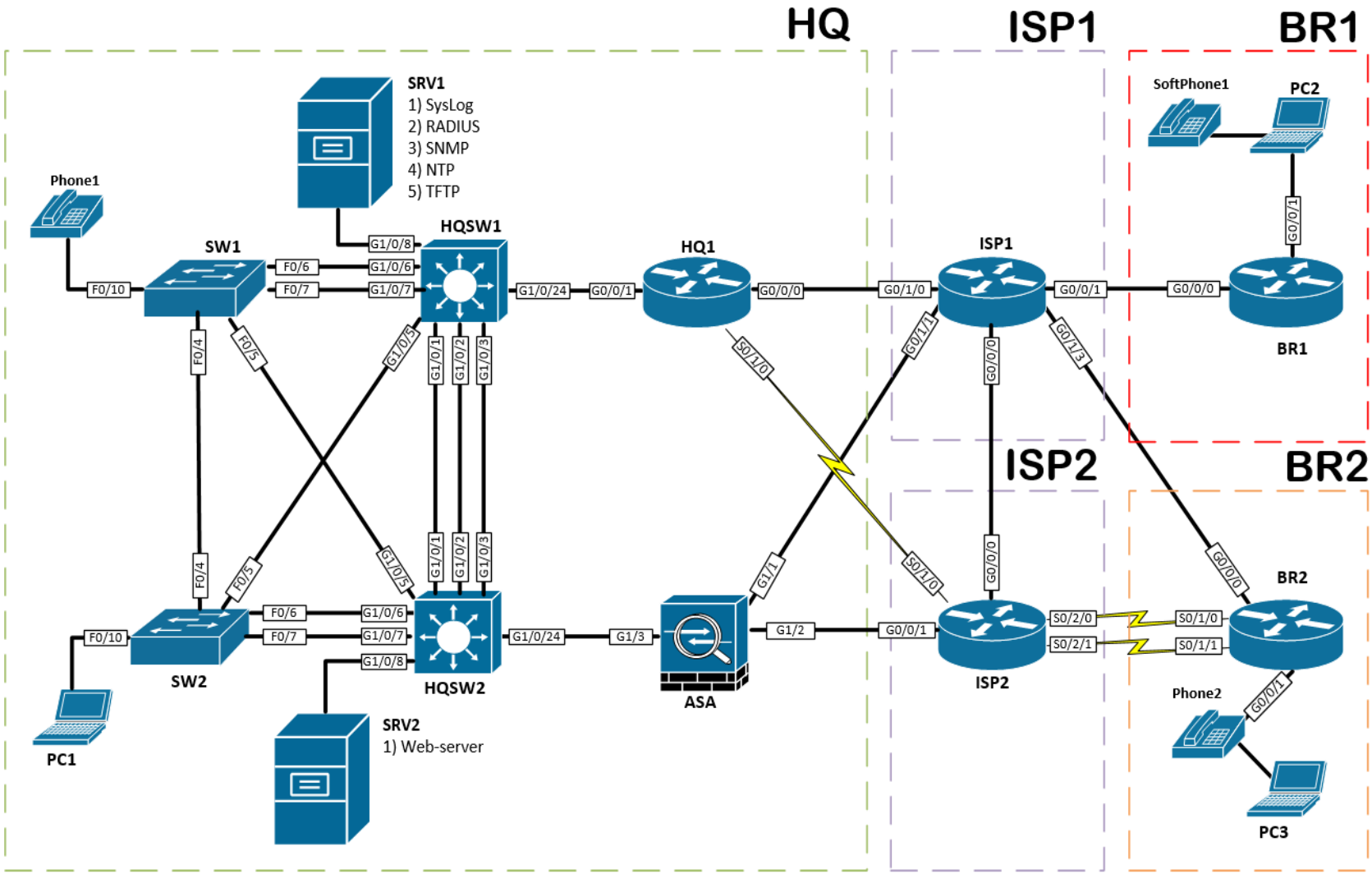
a. Создайте на ASA локального пользователя **vpnuser** с паролем **cisco**

b. Клиенты должны подключаться с помощью клиента AnyConnect, образ для установки которого находится во флеш-памяти межсетевого экрана ASA.

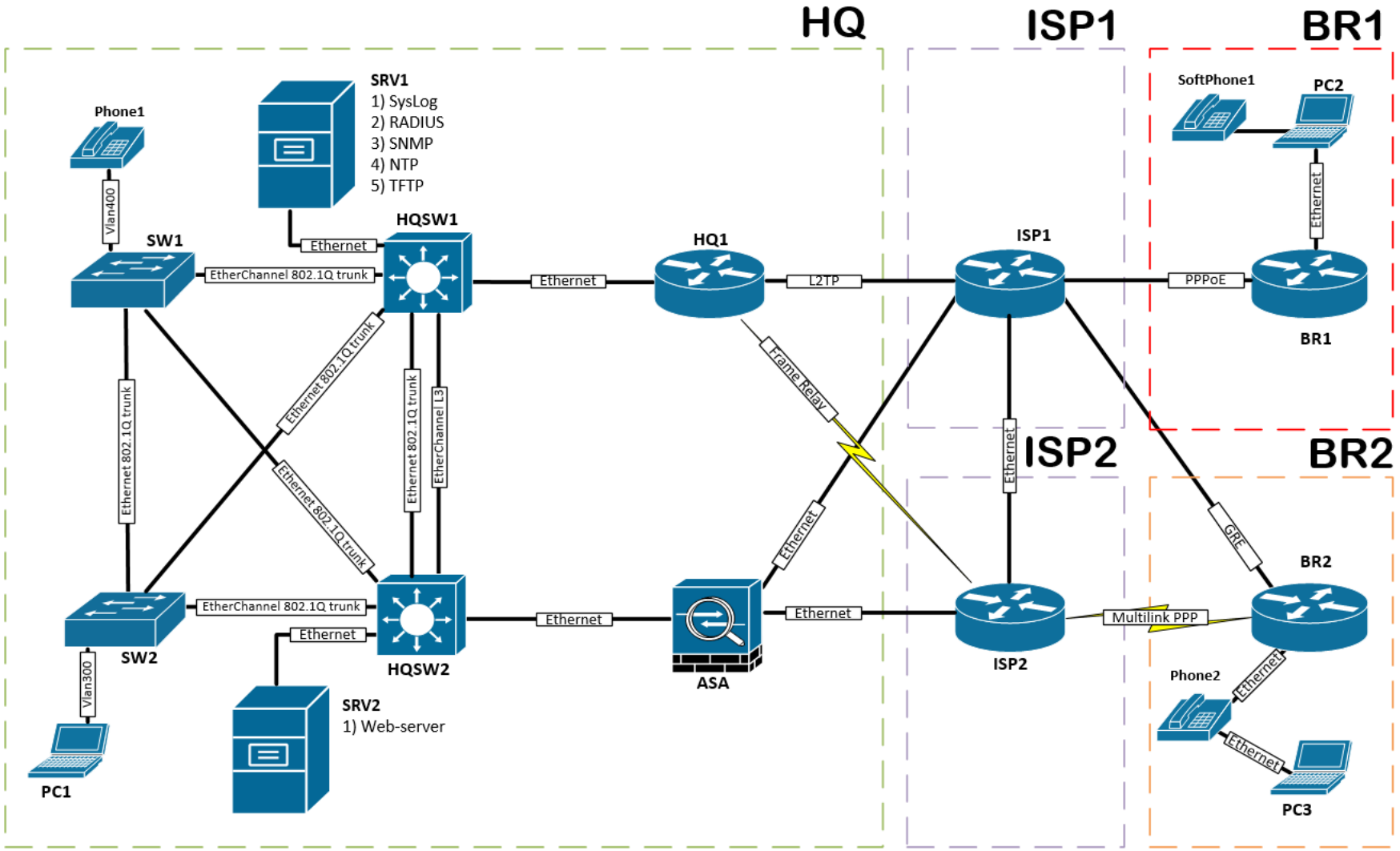
c. Подключение должно происходить по адресу 40.15.5.2.

d. Подключение проверять с PC3.

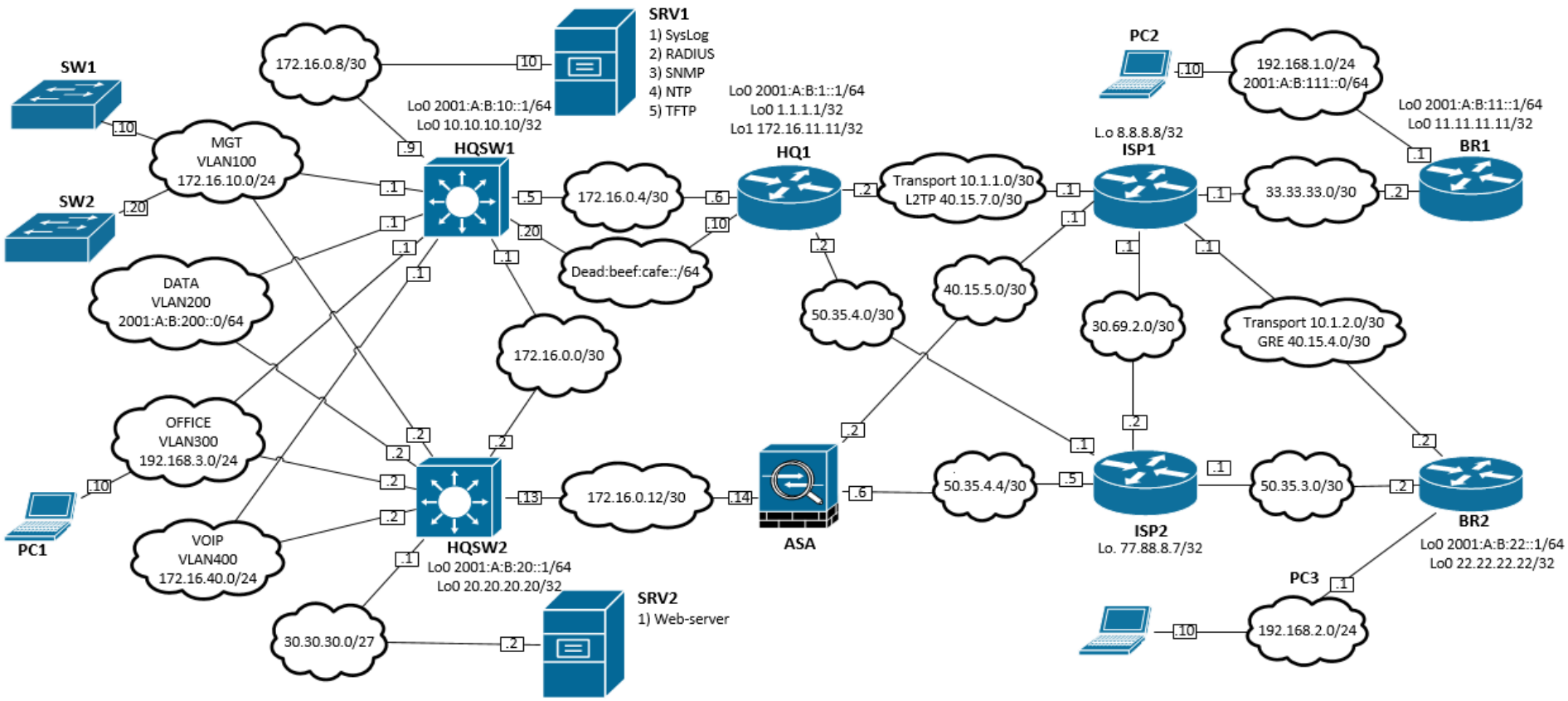
Топология L1



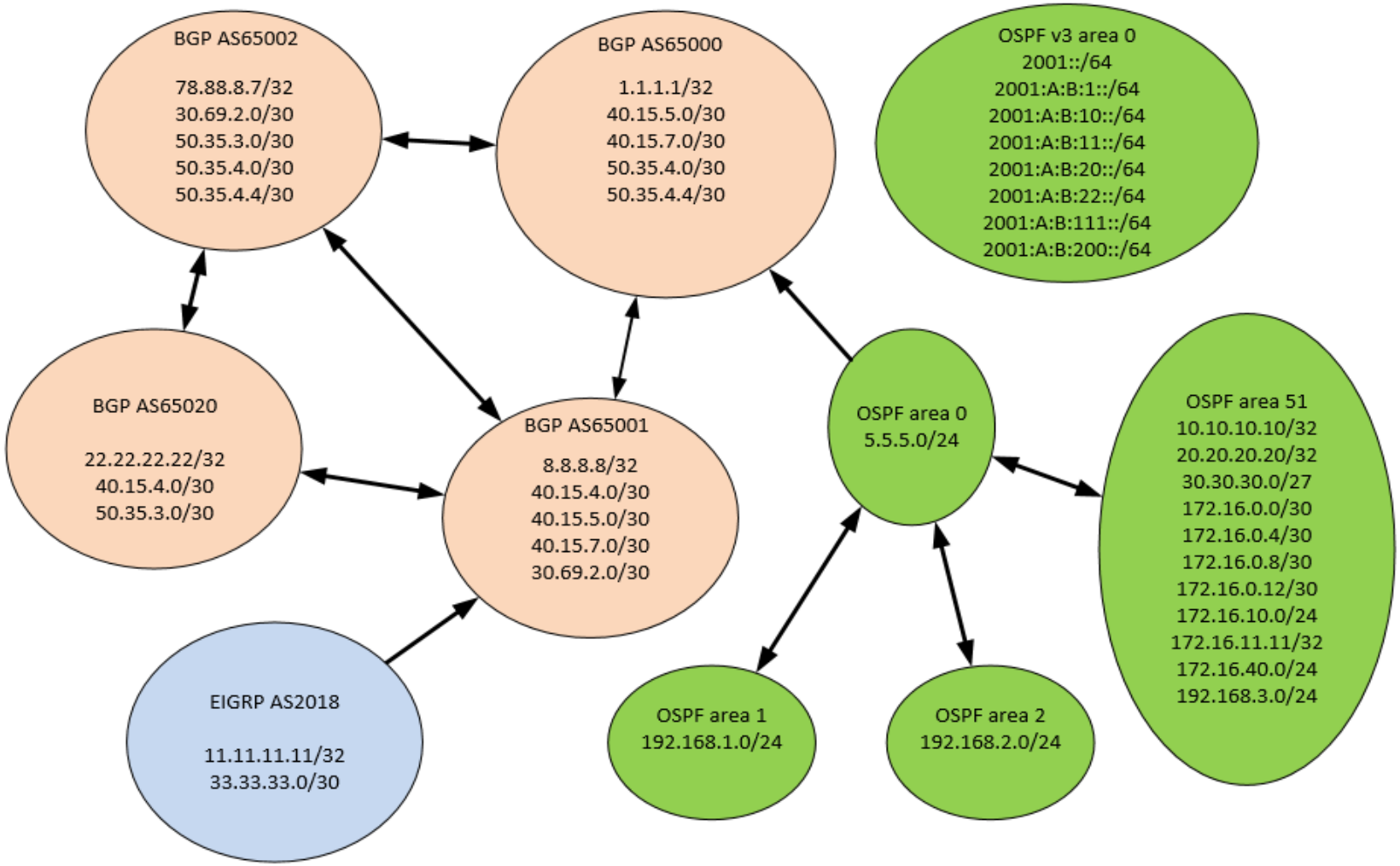
Топология L2



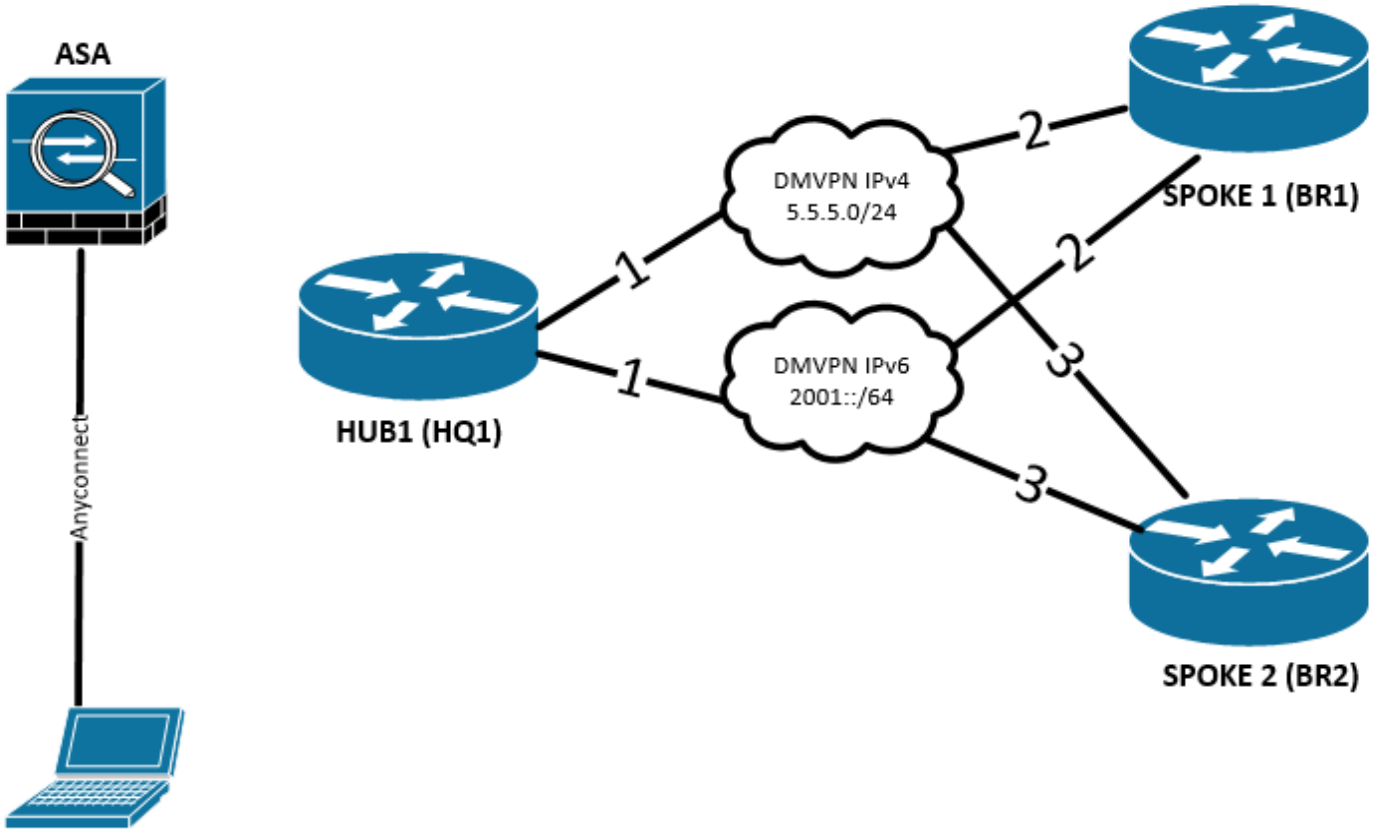
Топология L3



Routing-диаграмма



VPN диаграмма


ASA
Anyconnect
HUB1 (HQ1)
DMVPN IPv4
5.5.5.0/24
DMVPN IPv6
2001::/64
SPOKE 1 (BR1)
SPOKE 2 (BR2)
1
1
2
2
3
3

2

Примерный план работы Центра проведения демонстрационного экзамена по КОД № 2.1 по компетенции № 39 «Сетевое и системное администрирование»

	Примерное время	Мероприятие
Подготовительный день	08:00	Получение главным экспертом задания демонстрационного экзамена
	08:00 – 08:20	Проверка готовности проведения демонстрационного экзамена, заполнение Акта о готовности/не готовности
	08:20 – 08:30	Распределение обязанностей по проведению экзамена между членами Экспертной группы, заполнение Протокола о распределении
	08:30 – 08:40	Инструктаж Экспертной группы по охране труда и технике безопасности, сбор подписей в Протоколе об ознакомлении
	08:40 – 09:00	Регистрация участников демонстрационного экзамена
	09:00 – 09:30	Инструктаж участников по охране труда и технике безопасности, сбор подписей в Протоколе об ознакомлении
	09:30 – 11:00	Распределение рабочих мест (жеребьевка) и ознакомление участников с рабочими местами, оборудованием, графиком работы, иной документацией и заполнение Протокола
День 1	09:00 – 09:30	Ознакомление с заданием и правилами

	09:30 – 10:00	Брифинг экспертов
	10:00 – 14:00	Выполнение модуля A
	14:00 – 18:00	Выполнение модуля B
	18:00 – 19:00	Обед
	19:00 – 20:00	Работа экспертов, заполнение форм и оценочных ведомостей
День 2	09:30 – 10:00	Брифинг экспертов
	10:00 – 14:00	Выполнение модуля C
	14:00 – 15:00	Обед
	15:00 – 18:00	Работа экспертов, заполнение форм и оценочных ведомостей
	18:00 – 20:00	Подведение итогов, внесение главным экспертом баллов в CIS, блокировка, сверка баллов, заполнение итогового протокола

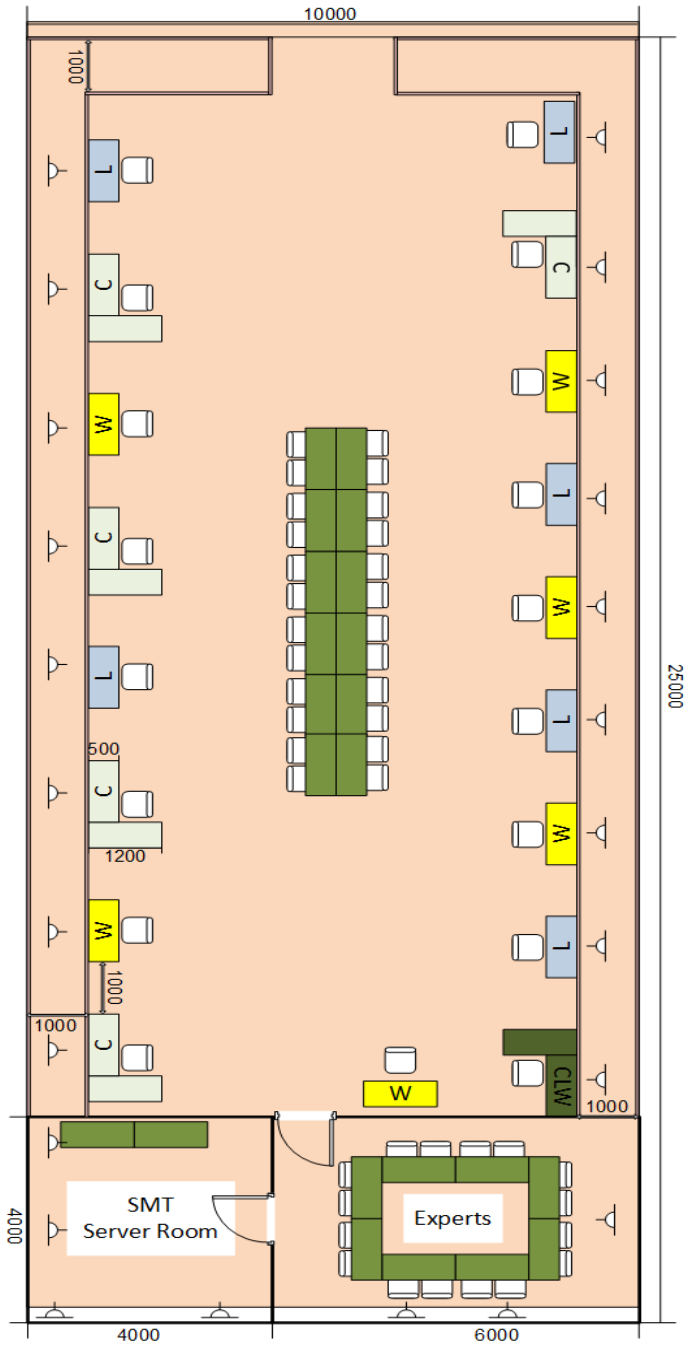
План застройки площадки для проведения демонстрационного экзамена по КОД № 2.1 по компетенции № 39 «Сетевое и системное администрирование»

Компетенция: Сетевое и системное администрирование

Номер компетенции: 39

Общая площадь площадки: 250 м^2

План застройки площадки:



ПРИЛОЖЕНИЕ

Инфраструктурный лист для КОД № 2.1